MANUALE PER LA PROGETTAZIONE DELLA *CYBERSECURITY*

GUIDA PER **PROGETTARE** E **REALIZZARE** IL SISTEMA DI SICUREZZA AZIENDALE [SECURITY ASSESSMENT]

NOME FILE: *5 - CYBERSECURITY - MANUALE.DOCX*
CREAZIONE: *27/02/2020*
AGGIORNAMENTO: *7 JULY 2022*

INDICE DEGLI ARGOMENTI

Titolo _____ *Pag.*

PARTE I: INTRODUZIONE ALLA CYBERSECURITY

1. CHE COSA È LA CYBERSECURITY

CYBER: «sono i processi (insieme di programmi) automatizzati (siti web, telecomunicazioni, trasmissioni, posta elettronica, computer, cellulari, ecc.) e tutti i dati da essi trattati sia personali sia aziendali (in formato digitale) » [NON è la CIBERNETICA! Scienza che studia l'applicazione ai sistemi automatici (robot, ecc.) dei processi mentali ed è UNA delle applicazioni della I.A. (un'altra è la cybersecurity, ecc.)]

NIST SP 800-160 AFFERMA: «Le strutture artificiali di calcolo e di comunicazione, rappresentate dal prefisso "cyber", formano un sistema distribuito che interagisce direttamente e dinamicamente con il mondo reale che le circonda ..»

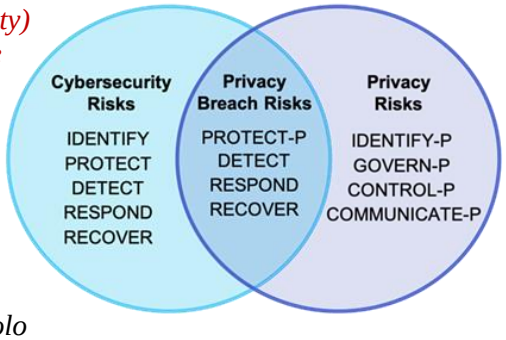
SECURITY: protezione dei **dati** *(personali e aziendali) e delle* **attività** *allo scopo di garantire sia la sicurezza degli individui [Reg. UE 2016/679] sia la continuità dei servizi aziendali.*

2. QUALI DIFFERENZE E PUNTI IN COMUNE CON LA PRIVACY

Attenzione!

Sebbene la gestione del rischio per la sicurezza informatica (cybersecurity) contribuisca a gestire il rischio per la privacy (la persona), essa non è sufficiente a coprire tutti i rischi.

La Cybersecurity e la Privacy hanno esigenze di gestione del rischio uniche e sovrapposte, come illustrato nella figura.



Da NIST SP 800-211 - 2019 NIST/ITL Cybersecurity Program Annual Report.

Per ulteriori approfondimenti sui controlli della Privacy, consultare il capitolo "Appendix J Privacy Control Catalog" del manuale "NISP SP 800-53"

3. PERCHÉ È NECESSARIA LA CYBERSECURITY

… Per tutelare le Esigenze aziendali e personali, rispondendo alle sfide globali e fronteggiare in modo adeguato il terrorismo, la criminalità organizzata e gli attacchi di ordine generale sin … (dal 2009)

[Tratto dall'articolo «Il Paradigma: Modelli 231/2001 e Sistema Qualità Cibersicurezza» dell'Avvocato Costanza Matteuzzi e Aldo Pedico]

Ransomware, malware distruttivo, minacce (threats) interne e persino errori onesti degli utenti rappresentano minacce continue per le organizzazioni e per le persone

[From: NIST Cybersecurity White Paper – Securing Data Integrity Against Ransomware Attacks: Using the NIST Cybersecurity Framework and NIST Cybersecurity Practice Guides – Data Set: NIST CWP Sec. Data Int. against Ransomware.pdf]

4. IMPORTANZA O RILEVANZA DELLA CYBERSECURITY

Essa è caratterizzata e analizzata utilizzando le seguenti designazioni:

- ✓ FUNZIONI DI RAFFORZAMENTO*: sono direttamente responsabili della fornitura della capacità di protezione della sicurezza, includendola in conformità con l'adozione o l'applicazione delle decisioni relative alle Politiche; un esempio di una funzione di rafforzamento della sicurezza è quella che prende la decisione di concedere o negare l'accesso a una risorsa.*
- ✓ FUNZIONI DI SUPPORTO*: contribuiscono alla capacità delle funzioni di applicazione di fornire le capacità specificate; queste funzioni forniscono dati, servizi oppure eseguono operazioni da cui dipendono le funzioni di Rafforzamento; in generale, la dipendenza è a livello funzionale; la gestione della memoria è un esempio di una funzione di supporto della sicurezza.*

4A. OVERVIEW OF THE CYBERSECURITY FRAMEWORK

The Profile defines specific practices to address the Framework Core.

It is the next layer of detail for implementing cybersecurity best practices for each category expressed in the Framework.

1 FRAMEWORK CORE

[From: NIST - Framework for Improving Critical Infrastructure – February 12, 2014]

The Framework Core is a set of cybersecurity activities and desired outcomes determined to be essential across critical infrastructure sectors.

The Core presents industry standards, guidelines, and practices in a manner that allows for communication of cybersecurity activities and outcomes across the organization from the executive level to the implementation/operations level.

The Framework Core consists of five concurrent and continuous Functions—Identify, Protect, Detect, Respond, Recover.

When considered together, these Functions provide a high-level, strategic view of the organization's management of cybersecurity risk.

The Framework Core then identifies underlying key Categories and Subcategories for each Function and matches them with example Informative References such as existing standards, guidelines, and practices for each Subcategory.

Il Framework (struttura) è composto da:

1. *FUNCTIONS*
   - ✓ *5 funzioni: {Identify, Protect, Detect, Respond, Recover};*
   - ✓ *organizzano attività di cybersecurity di base al loro massimo livello;*
2. *CATEGORIES*
   - ✓ *sono le suddivisioni di una Funzione in gruppi di risultati di cyber sicurezza strettamente legati a esigenze programmatiche e attività particolari (es.: Gestione Risorse, Controllo Accessi e Processi di Rilevamento).*
3. *SUBCATEGORIES*
   - ✓ *dividono ulteriormente una Categoria in risultati specifici delle attività tecniche e/o gestionali;*
   - ✓ *forniscono una serie di risultati che aiutano a supportare il raggiungimento dei risultati in ciascuna categoria.*
   - ✓ *Es. di sottocategorie: sono catalogati i sistemi d'informazione esterni, sono protetti i dati a riposo, sono investigate le notifiche dai sistemi di rilevamento.*
4. *INFORMATIVE REFERENCES*
   - ✓ *sono sezioni specifiche di standard, linee guida e pratiche comuni ai settori delle infrastrutture critiche;*
   - ✓ *sono illustrativi e non esaustivi.*

The five Framework Functions can be performed concurrently and continuously to form an operational culture that addresses the dynamic cybersecurity risk.

Table 1 Cybersecurity Framework Functions and Categories

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
PR	Protect	PR.AC	Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

*Le 5 "***funzioni***" del Framework Core sono:*

1. *Identify (ID) [NIST SP 1800-25: permette all'organizzazione di **progettare** e **pianificare** la gestione di un attacco, in tale situazione è necessario disporre delle capacità per rilevare e rispondere agli eventi distruttivi]*
   - ✓ *sviluppa la comprensione organizzativa per gestire il rischio di cyber sicurezza verso sistemi, risorse, dati e potenzialità.*
   - ✓ *comprensione del contesto aziendale, delle risorse che supportano le funzioni critiche e dei relativi rischi di cyber sicurezza, consente all'organizzazione di concentrarsi e prioritizzare i propri sforzi, coerentemente con la propria strategia di gestione del rischio e le esigenze aziendali;*
   - ✓ *le **Categorie** all'interno di questa funzione sono: **Gestione delle Risorse; Ambiente di Business; Governance; Valutazione del Rischio; Strategia di Gestione del Rischio**.*
   - ✓ ***Funzioni: Identify Assets; Vulnerability Identification**.*
2. *Protect (PR) [NIST SP 1800-25: permette all'organizzazione di **progettare** e **pianificare** la gestione di un attacco, in tale situazione è necessario disporre delle capacità per rilevare e rispondere agli eventi distruttivi]*
   - ✓ *sviluppa e implementa le opportune misure di salvaguardia per assicurare la fornitura di servizi di infrastruttura critici;*
   - ✓ *supporta la capacità di limitare o contenere l'impatto di un potenziale evento di sicurezza informatica;*
   - ✓ *le **Categorie** all'interno di questa funzione sono: Controllo Accessi; Consapevolezza e Formazione; Scurezza dei Dati; Processi e Procedure per la Protezione delle Informazioni; **Manutenzione; Tecnologia Protettiva**.*
   - ✓ ***Funzioni: Backup; Integrity Baseline; Denylist; Patching Vulnerabilities; Policy.***
1. *Detect (DE) [NIST SP 1800-26: permette all'organizzazione di **rilevare** e **rispondere** a ransomware e altri eventi distruttivi]*
   - ✓ *sviluppa e implementa le attività appropriate per identificare il verificarsi di un evento di sicurezza informatica.*
   - ✓ *consente la scoperta tempestiva di eventi di sicurezza informatica;*
   - ✓ *le **Categorie** incluse in questa funzione sono: **Anomalie ed Eventi; Monitoraggio Continuo della Sicurezza; Processi di Rilevamento**.*
   - ✓ ***Funzioni: Integrity Monitoring; Event Detection.***
2. *Respond (RS) [NIST SP 1800-26: permette all'organizzazione di **rilevare** e **rispondere** a ransomware e altri eventi distruttivi]*
   - ✓ *sviluppare e implementare le attività appropriate per intraprendere azioni in merito a un evento di sicurezza rilevato;*
   - ✓ *supporta la capacità di contenere l'impatto di un potenziale evento di sicurezza informatica;*
   - ✓ *le **Categorie** incluse in questa funzione sono: **Pianificazione della Risposta; Comunicazioni; Analisi; Mitigazione; Miglioramenti**.*

- ✓ ***Funzioni: Analytics; Malware Analysis; Logging.***

3. Recover (RC) *[NIST SP 1800-11: permette all'organizzazione di* ***disporre*** *della* ***capacità di ripristino*** *nel caso in cui un attacco all'integrità dei dati ha esito positivo]*
   - ✓ *sviluppa e implementa le attività appropriate per mantenere i piani di Resilienza;*
   - ✓ *supporta il ripristino tempestivo delle normali operazioni per ridurre l'impatto;*
   - ✓ *le* ***Categorie*** *incluse in questa funzione sono:* ***Pianificazione del Recupero; Miglioramenti; Comunicazioni****.*
   - ✓ ***Funzioni: Restore; Identify Last Known Good.***

2 ELENCO DELLE TECHNICAL CAPABILITY

CAPABILITY	DESCRIPTION
Hardware Inventory Management	*Hardware inventory management tools enable a manufacturer to track computing and network devices within the manufacturing system, including device details and location information*
Software and Firmware Inventory Management	*Software and firmware inventory management tools enable a manufacturer to track software and firmware installed within the manufacturing system computing and network devices, including identification, version numbers, and location information*
Systems Development Lifecycle Management	*Systems development lifecycle management tools enable a manufacturer to track the scope of activities associated with hardware and software components of the manufacturing system, encompassing each component's initiation, development and acquisition, implementation, operation and maintenance, and its ultimate decommissioning and disposal*
Network Architecture Documentation	*Network architecture documentation tools enable a manufacturer to identify, document, and diagram the interconnections between networked manufacturing system devices, corporate networks, and other external network connections.*
Configuration Management	*Configuration management tools enable a manufacturer to establish and maintain the integrity of manufacturing system hardware and software components by control of processes for initializing, changing, monitoring, and auditing the configurations of the components throughout the system development life cycle*
Baseline Establishment	*Baseline establishment tools enable a manufacturer to support the management of baseline configurations of the manufacturing system. The tools track information about the manufacturing system components (e.g. software license information, software version numbers, Human Machine Interface (HMI) and other ICS component applications, software, operating systems), current version numbers and patch information on operating systems and applications; and configuration settings/parameters), network topology, and the logical placement of those components within the system architecture*
Change Control	*Change control tools enable a manufacturer to document, track, and coordinate changes to manufacturing system hardware and software components*
Configuration Backups	*Configuration backup tools enable a manufacturer to gather and archive configuration settings from hardware and software components within the manufacturing system, typically in a data format specified by the original equipment manufacturer (OEM) of the component*
Data Backup	*Data backup tools enable a manufacturer to collect and store files and programs from the manufacturing system to facilitate recovery after an incident*
Data Replication	*Data replication tools enable a manufacturer to copy and transfer backup data to a physical location external to the manufacturing system*
Network Segmentation and Segregation	*Network segmentation and segregation solutions enable a manufacturer to separate the manufacturing system network from other networks (e.g., corporate networks, guest networks), segment the internal manufacturing system network into smaller networks, and control the communication between specific hosts and services*
Network Boundary Protection	*Network boundary protection solutions enable a manufacturer to restrict data communication traffic to and from manufacturing system network(s). Network boundary protection capabilities include, but are not limited to, the use of firewalls, demilitarized zones (DMZ), and intrusion detection and prevention systems.*
Secure Remote Access	*Secure remote access solutions enable a manufacturer to establish secure communications channels through which information can be transmitted over untrusted networks, including public networks such as the Internet.*
Managed Network Interfaces	*Managed network interface solutions enable a manufacturer to control connections and information transmitted and received through individual physical ports on a network device*
Map Data Flows	*Data flow diagrams enable a manufacturer to understand the flow of data between networked components of the manufacturing system*

CAPABILITY	DESCRIPTION
Time Synchronization	*Time synchronization solutions enable a manufacturer to synchronize time for all manufacturing system components to generate accurate timest*
Credential Management	*Credential management tools enable a manufacturer to manage the life cycle of user authentication and authorization credentials*
Authentication and Authorization	*Authentication and authorization tools enable a manufacturer to verify user identities and enforce the principles of least privilege. The tools and techniques supporting authentication and authorization enable a manufacturer to set user privileges and positively determine if a user has permission to access a system resource. Where feasible, centralized authentication and authorization mechanisms should be considered as part of the system architecture*
Anti-virus/malware	*Anti-virus/malware tools enable a manufacturer to monitor computing devices to identify major types of malware and prevent or contain malware incidents*
Risk Assessment	*Risk assessment tools enable a manufacturer to perform risks assessments of the manufacturing*
Vulnerability Scanning	*Vulnerability scanning tools enable a manufacturer to scan, detect, and identify software flaws or misconfigurations that cause a weakness in the security of the manufacturing system*
Vulnerability Management	*Vulnerability management tools enable a manufacturer to document, manage, and mitigate vulnerabilities discovered in the manufacturing system*
Incident Management	*Incident management tools enable a manufacturer to document, track, and coordinate the mitigation of an adverse event in manufacturing system devices or networks*
Network Monitoring	*Network monitoring tools enable a manufacturer to capture, store, and audit network traffic from the manufacturing system networks, and monitor for indicators of potential cybersecurity incidents*
System Use Monitoring	
Maintenance Tracking	*Maintenance tracking solutions enable a manufacturer to schedule, track, authorize, monitor, and audit maintenance and repair activities to manufacturing system computing devices*
Physical Access Control	*Physical access control solutions enable a manufacturer to deny or restrict access to the manufacturing system by unauthorized individuals*
Physical Access Monitoring	*Physical access monitoring solutions enable a manufacturer to record, monitor, archive, and audit physical access to the manufacturing system by all individuals*
Ports and Services Lockdown	*Ports and services lockdown solutions enable a manufacturer to discover and disable nonessential physical and logical network ports and services*
Media Protection	*Media protection solutions enable a manufacturer to restrict the use of portable media within the manufacturing system*
Encryption	*Encryption solutions enable a manufacturer to protect sensitive manufacturing system data so that only authorized users can access it*
Data Loss Prevention	*Data loss prevention solutions enable a manufacturer to detect and prevent the unauthorized access and transmission of sensitive manufacturing system data*
Media Sanitization	*Media sanitization solutions enable a manufacturer to render data written on media unrecoverable*
Event Logging	*Event logging solutions enable a manufacturer to capture, store, archive, and audit the events occurring within the manufacturing system and its networks*
Forensics	*Forensic solutions enable a manufacturer to identify, collect, examine, and analyze data from the manufacturing system to determine the cause of an incident.*

4B. ENTERPRISE CYBERSECURITY PROCESS

[Da: 1) NIST SP 800-34, capitolo “Contingency Planning and Resilience” e Appendix B; 2) NIST IR 8286; 3) NIST SP 800-30]

PIANO DI CONTINGENCY (EMERGENZA)

Un’organizzazione deve avere la capacità di resistere a tutti i pericoli e sostenere la propria missione attraverso i cambiamenti ambientali.

Questi cambiamenti possono essere graduali, come cambiamenti economici o di missione, o improvvisi, come in un evento disastroso.

Piuttosto che lavorare solo per identificare e mitigare minacce, vulnerabilità e rischi, le organizzazioni possono lavorare per costruire un'infrastruttura resiliente, riducendo al minimo l'impatto di qualsiasi interruzione sulle funzioni essenziali della missione.

Una pianificazione di emergenza efficace inizia con lo sviluppo di una politica di pianificazione di emergenza dell'organizzazione e l'assoggettamento di ciascun sistema informativo a un'analisi dell'impatto aziendale (BIA).

Ciò facilita la definizione delle priorità dei sistemi e dei processi in base al livello di impatto (vedi FIPS 199 - Federal Information Processing Standard) e sviluppa strategie di ripristino prioritarie per ridurre al minimo le perdite.

FIPS 199 fornisce le linee guida per determinare le informazioni e l'impatto del sistema informativo su operazioni e risorse dell'organizzazione, individui, altre organizzazioni e nazione attraverso una formula che esamina tre obiettivi di sicurezza: **riservatezza, integrità e disponibilità**.

DEFINIZIONE. *Si parla quindi di* INFORMATION SYSTEM CONTINGENCY PLANNING (ISCP)*: pianificazione per la gestione dell'emergenza che include l'integrazione dei controlli di sicurezza nelle prime fasi dello sviluppo di un sistema informativo e il mantenimento di tali controlli su base continuativa.*

ISCP *praticamente include anche* **BCP** *(Business Continuity Plan: interruzioni locali o circoscritte) e* **DRP** *(Disaster Recovery Plan: distruzione del sito primario).*

ISCP *è composto dai seguenti processi:*

1) Develop the Contingency Planning Policy;

2) Conduct the Business Impact Analysis (**BIA**);

3) Identify Preventive Controls;

4) Create Contingency Strategies;

5) Develop Contingency;

6) Plan Testing, Training, and Exercises (**TT&E**);

7) Plan Maintenance.

In sintesi, lo scopo dei suddetti processi è il seguente:

1°. il piano di gestione dell'emergenza si basa chiare policy (scopo, risorse necessarie, addestramento del personale, prove schedulate, manutenzione, backup);

*2°. realizzazione dell'analisi d'impatto (**BIA**); **BIA** ha lo scopo di:*

- *determinare i processi di business e la ripartenza delle applicazioni critiche;*
- *identificare le risorse hw e sw che vincolano la ripartenza dei processi critici;*
- *stabilire le priorità della ripartenza delle risorse di sistema;*

3rd. identificare i controlli preventivi;

4°. creare le strategie d'emergenza: requisiti per mitigare i rischi;

5°. esecuzione dei test di verifica delle procedure di ripartenza, delle risorse e dei tempi di ripristino;

6th. addestramento del personale.

SCHEMA PROCESSI ENTERPRISE CYBERSECURITY GOVERNANCE

In questo capitolo, ho voluto riportare solo i processi necessari alla gestione della sicurezza all'interno del ciclo di vita dell'intero sistema. L'elenco completo dei processi componenti il ciclo di vita del sistema è visibile nel capitolo SYSTEMS SECURITY IN SYSTEM LIFE CYCLE PROCESSES PARTE II.

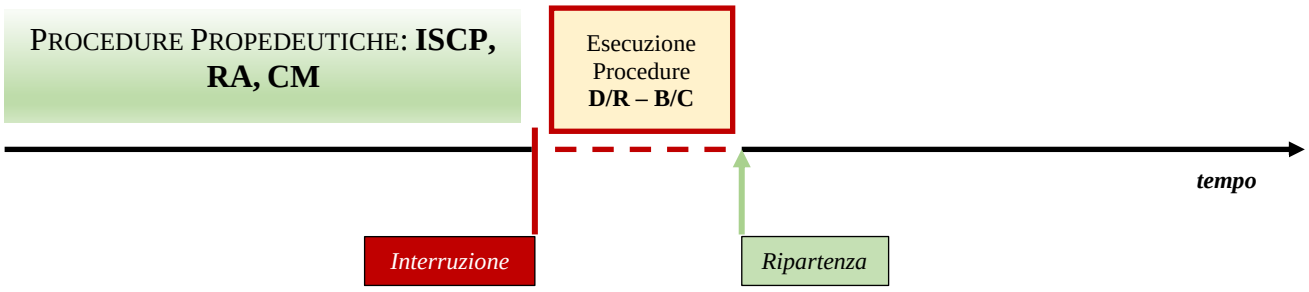
S L C P *[System Life Cycle Process]*

PROCESSI PROPEDEUTICI	PROCESSI ON GOING
1. **ISCP** {**DC** *[Data Classification – vedi capitoli 65A. Data Classification and Practices nella Parte XI: Zero Trust (ZT) e Data Security (DS) nella Parte II: Progettazione della Cybersecurity]*, **BCP**, **DRP**, **BIA**, ...} *[Information System Contingency Planning]* 2. **RA** {**FR** Framing Risk, *vedi NIST SP 800-30 e cap. 7. Parte I*} *[Risk Assessment]* 3. **CM** {**SLC** Software Life Cycle, **HLC** Hardware Life Cycle, **QA** Quality Assurance, ...} *[Change Management]*	1. **MONITORING** {**IDS** Intrusion Detection System, **Control**, ecc.} 2. **BC**, **DR** *[Business Continuity, Disaster Recovery]* 3. **RM** {**MR** Monitoring Risk, **RR** Responding Risk, *vedi NIST SP 800-30 e cap. 7. Valutazione del Rischio (Risk Assessment - RA) Parte I*} *[Risk Management]*

S L C P

PROCEDURE ONGOING: **MONITORING, RISK MANAGEMENT**

PROCEDURE PROPEDEUTICHE: **ISCP, RA, CM**



BUSINESS IMPACT ANALYSIS (BIA)

[Da NIST SP 800-34, capitolo "Conduct the Business Impact Analysis (BIA)" e Appendix B]

BIA è un passaggio chiave nell'implementazione dei controlli CP in NIST SP 800-53 e nel processo di pianificazione delle emergenze in generale. Inoltre, consente di caratterizzare i componenti del sistema, i processi di missione/business supportati e le interdipendenze e deve essere eseguita durante la fase di avvio del System Development Life Cycle (SDLC).

Scopo di BIA è correlare il sistema con la missione critica/processi aziendali e servizi forniti e, sulla base di tali informazioni, caratterizzare le conseguenze di un'interruzione.

Il coordinatore ISCP deve utilizzare i risultati BIA per determinare i requisiti e le priorità della pianificazione di emergenza.

I risultati della BIA devono essere adeguatamente incorporati nell'analisi e negli sforzi di sviluppo della strategia per BCP e DRP dell'organizzazione.

Man mano che la progettazione del sistema si evolve e i componenti cambiano, potrebbe essere necessario eseguire nuovamente la BIA durante la fase di sviluppo / acquisizione dell'SDLC.

Tre passaggi sono tipicamente coinvolti nella realizzazione del BIA:

1) DETERMINARE LA MISSIONE/PROCESSI AZIENDALI E CRITICITÀ DI RECUPERO.

Sono identificati i processi aziendali supportati dal sistema e è determinato l'impatto di un'interruzione del sistema su tali processi insieme agli impatti delle interruzioni e al tempo di inattività stimato.

Il tempo di inattività dovrebbe riflettere il tempo massimo che un'organizzazione può tollerare pur mantenendo la missione.

2) IDENTIFICARE I REQUISITI DELLE RISORSE.

Gli sforzi realistici di ripristino richiedono una valutazione approfondita delle risorse necessarie per riprendere i processi di business e le relative interdipendenze il più rapidamente possibile.

Esempi di risorse che dovrebbero essere identificate includono strutture, personale, attrezzature, software, file di dati, componenti di sistema e registrazioni vitali.

3) IDENTIFICARE LE PRIORITÀ DI RECUPERO PER LE RISORSE DI SISTEMA.

Sulla base dei risultati delle attività precedenti, le risorse di sistema possono essere collegate in modo più chiaro a funzioni e processi aziendali critiche.

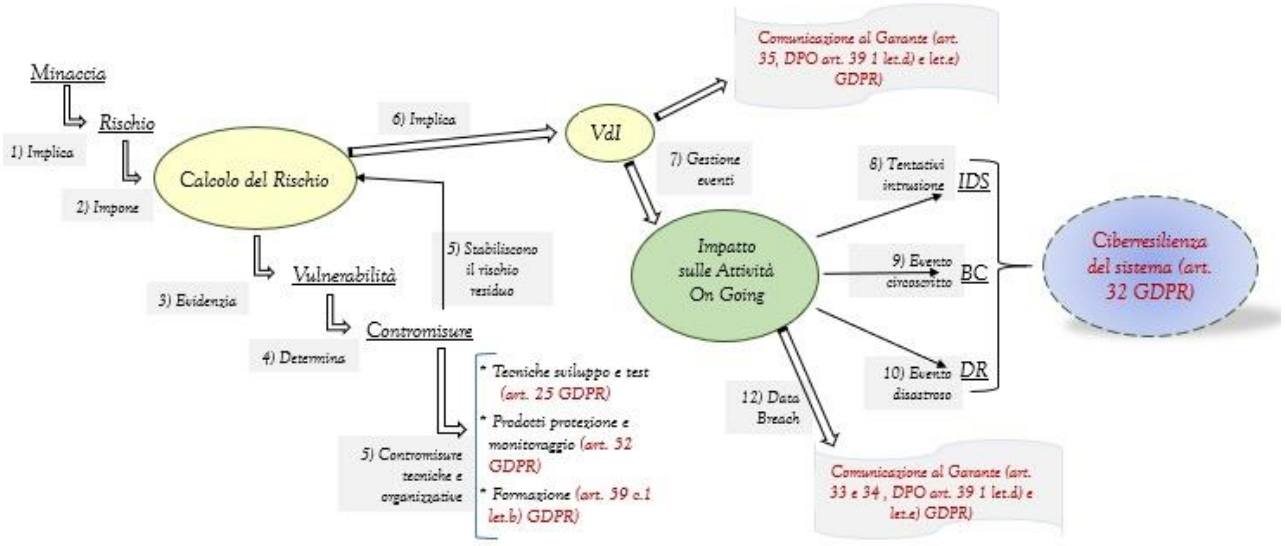
È possibile stabilire livelli di priorità per il sequenziamento delle attività e delle risorse di ripristino.

Per maggiori dettagli si rimanda al manuale indicato nel sottotitolo.

5. MAPPA CONCETTUALE DEL «SISTEMA SICUREZZA» O DEL PROCESSO DI SECURITY ASSESSMENT (SA)

[Mio percorso mentale]

[mia] MAPPA CONCETTUALE DEL «SISTEMA SICUREZZA» O DEL PROCESSO DI SECURITY ASSESSMENT



6. FASI E PROCESSI DEL SECURITY ASSESSMENT

Dettagli leggere: NIST SP 800-160 Vol.1 Fare riferimento al Capitolo "The Controls" all'interno del manuale "NIST SP 800-160 SSE Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems".

- ✓ *Capitolo "**System Life cycle Processes**", contiene:*
  1. *Elenco dei processi del ciclo di vita a gli ambienti (stage) che compongono il ciclo di vita del sistema necessari a realizzare sistemi sicuri*
  2. *Elenco dei 30 processi del ciclo di vita del sistema definiti in ISO/IEC/IEEE 15288*
- ✓ *Capitolo "**Summary of Systems Security Activities and Task**", contiene:*
  1. *Elenco dei task e delle attività per la progettazione della sicurezza associati ai processi del ciclo di vita del sistema definiti in ISO/IEC/IEEE 15288*
- ✓ *Capitolo "**Design Principles for Security**", contiene:*
  1. *I principi e concetti di progettazione della sicurezza usati come base affidabile per la progettazione di sistemi sicuri.*
  2. *Elenco e descrizione dei principi.*

Figure G-2 illustrates the two types of requirements and their relationship to the verification and validation of the system.

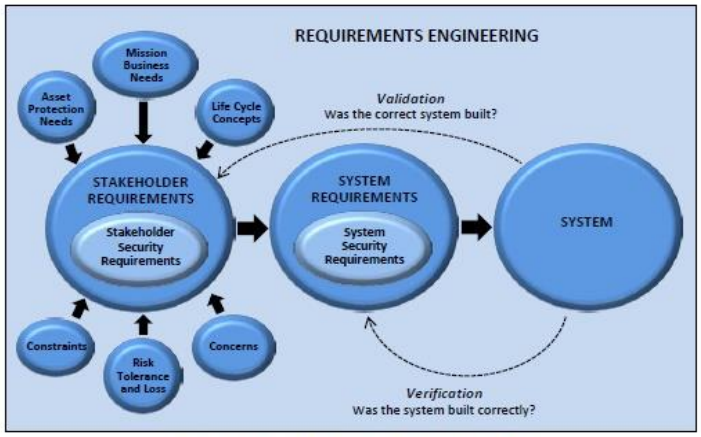


FIGURE G-2: STAKEHOLDER AND SYSTEM REQUIREMENTS

- ✓ *Capitolo "**Engineering and Security Fundamental**", contiene:*
  1. *Applicazione dei principi e concetti di progettazione della sicurezza.*
  2. *Requisiti della sicurezza*
  3. *Policy*

APPLICAZIONE DEL RA (RISK ASSESSMENT)

[Rif.: NIST SP 800-30, capitolo 2.4]

Le valutazioni del rischio possono essere condotte a tutti e tre i livelli (Tier) nella gerarchia di gestione del rischio:

1) *livello dell'organizzazione,*
2) *livello della missione/processo aziendale*
3) *livello del sistema informativo.*

La figura 4 illustra la gerarchia di gestione del rischio definita nella pubblicazione speciale del NIST 800-39, che fornisce molteplici prospettive di rischio dal livello strategico al livello tattico.

Le valutazioni del rischio tradizionali si concentrano generalmente a livello di Tier 3 (ossia, a livello di sistema informativo) e, di conseguenza, tendono a trascurare altri fattori di rischio significativi che possono essere valutati in modo più appropriato a Tier 1 o Tier 2 (ad es. missione/funzione aziendale a una minaccia antagonista basata sulle interconnessioni del sistema informativo).

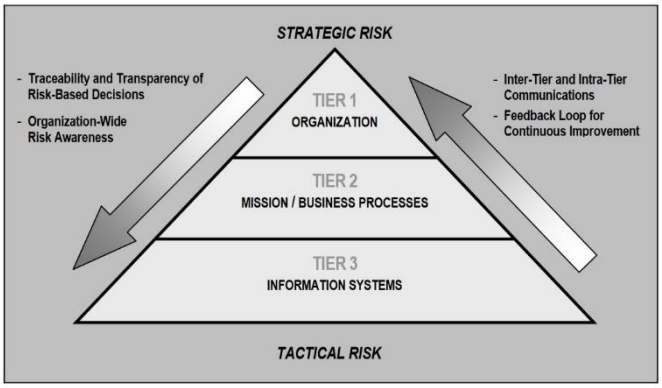


FIGURE 4: RISK MANAGEMENT HIERARCHY

Le valutazioni del rischio supportano le decisioni di risposta al rischio ai diversi livelli della gerarchia di gestione del rischio.

AL LIVELLO 1, *le valutazioni del rischio possono influenzare, ad esempio:*

(i) programmi, politiche, procedure e linee guida per la sicurezza delle informazioni a livello di organizzazione;

(ii) i tipi di risposte appropriate al rischio (cioè, accettazione del rischio, evitamento, mitigazione, condivisione o trasferimento);

(iii) decisioni di investimento per tecnologie/sistemi informatici

(iv) appalti;

(v) controlli di sicurezza minimi a livello di organizzazione;

(vi) conformità alle architetture aziendali/di sicurezza;

(vii) strategie di monitoraggio e autorizzazioni in corso di sistemi informativi e controlli comuni.

AL LIVELLO 2, *le valutazioni del rischio possono influenzare, ad esempio:*

(i) le decisioni di progettazione dell'architettura aziendale/dell'architettura di sicurezza;

(ii) la selezione di controlli comuni;

(iii) la selezione di fornitori, servizi e appaltatori a supporto di missioni organizzative/funzioni aziendali;

(iv) lo sviluppo di mission/processi aziendali risk-aware;

(v) l'interpretazione delle politiche di sicurezza delle informazioni rispetto ai sistemi informativi dell'organizzazione e agli ambienti in cui tali sistemi operano.

AL LIVELLO 3, *le valutazioni del rischio possono influenzare, ad esempio:*

(i) le decisioni di progettazione (inclusa la selezione, l'adattamento e l'integrazione dei controlli di sicurezza e la selezione dei prodotti di tecnologia dell'informazione per i sistemi informativi dell'organizzazione);

(ii) decisioni di implementazione (incluso se specifici prodotti informatici o configurazioni di prodotti soddisfano i requisiti di controllo della sicurezza);

(iii) decisioni operative (compreso il livello richiesto di attività di monitoraggio, la frequenza delle autorizzazioni in corso del sistema informativo e le decisioni di manutenzione del sistema).

Le valutazioni del rischio possono anche informare altre attività di gestione del rischio sui tre livelli che non sono correlate alla sicurezza.

Ad esempio, AL LIVELLO 1, *le valutazioni del rischio possono fornire input utili per:*

(i) determinazioni del rischio operativo (inclusa la continuità operativa per missioni organizzative e funzioni aziendali);

(ii) determinazioni del rischio organizzativo (inclusi rischio finanziario, rischio di conformità, rischio normativo, rischio di reputazione e rischio di acquisizione cumulativa in progetti su larga scala);

(iii) rischio a impatto multiplo (compreso il rischio della catena di approvvigionamento e il rischio che coinvolge le partnership).

A LIVELLO 2, *le valutazioni del rischio possono fornire gli stessi input utili ai rischi operativi, organizzativi e a impatto multiplo, specifici per i processi di missione aziendale.*

AL LIVELLO 3, *le valutazioni dei rischi possono fornire informazioni sulle valutazioni dei costi, della pianificazione e dei rischi legati alle prestazioni associati ai sistemi informativi, con esperti di sicurezza delle informazioni che si coordinano con i responsabili dei programmi, i proprietari dei sistemi informativi e i funzionari incaricati delle autorizzazioni.*

Questo tipo di coordinamento è essenziale all'interno delle organizzazioni al fine di eliminare stoccaggio (silos) e/o attività condotte per bloccare le informazioni (stovepipes) che producono soluzioni informatiche e di sicurezza

non ottimali o inefficienti, influenzando così la capacità delle organizzazioni di svolgere le missioni/funzioni aziendali assegnate con la massima efficienza ed efficacia in termini di costi.

È importante notare che il rischio per la sicurezza delle informazioni contribuisce ai rischi non legati alla sicurezza a ciascun livello. *Pertanto, i risultati di una valutazione del rischio a un determinato livello servono come input per e sono allineati con le attività di gestione del rischio non legate alla sicurezza a quel livello.*

Inoltre, i risultati delle valutazioni del rischio a livelli inferiori servono come input per le valutazioni del rischio a livelli superiori.

PROCESSI DEL SA (SECURITY ASSESSMENT)

Dettagli leggere: NIST SP 800-160 Vol.1 Fare riferimento al Capitolo "The Controls" all'interno del manuale "NIST SP 800-160 SSE Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems".

1. VALUTAZIONE DEL RISCHIO O RISK ASSESSMENT (RA)
   a) *Valutazione delle Minacce*
   b) *Calcolo del Rischio*
   c) *Valutazione della Vulnerabilità o Vulnerability Assessment (VA)*
   d) *Applicazione delle Contromisure, Valutazione d'Impatto o Gestione del Rischio Residuo*

2. GESTIONE DELLE ATTIVITÀ ON GOING
   a) *Monitoraggio*
   b) *Ciberresilienza*
      - ✓ *Intrusion Detection System (IDS)*
      - ✓ *Business Continuity (BC)*
      - ✓ *Disaster Recovery (DR)*

In sintesi, la tabella seguente estratta dal "NIST IR 8286 Integrating Cybersecurity and Enterprise Risk Management (ERM)" schematizza i processi della Risk Management ed il loro riferimento all'interno degli standard internazionali.

Table 1: Notional Crosswalk Among Selected ERM and Risk Management Frameworks

ERM Playbook	ISO 31000:2009		OMB A-123	GAO Green Book	NIST Risk Management Framework		
					SP 800-30 Rev. 1	SP 800-37 Rev. 2	SP 800-39
Identify the Context	Establish External Context (5.3.2), Establish Internal Context (5.3.3)		Establish Context	Define objectives and risk tolerances (6.01)	Preparing for the Risk Assessment (3.1)	Prepare (3.1)	Framing Risk (3.1)
Identify the Risks	Risk Assessment	Risk Identification (5.4.2)	Identify Risks	Identification of Risks (7.02)	Task 2-1: Identify and characterize threat sources of concern (3.2), Task 2-2: Identify potential threat events, threat sources (3.2), Task 2-3: Identify vulnerabilities/predisposing conditions (3.2)	Prepare (3.1), Task P-14, Risk Assessment - System, Risk Assessment Report (RAR) Assess (3.5)	
Analyze the Risks		Risk Analysis (5.4.3)	Analyze and Evaluate	Analysis of Risks (7.05)	Task 2-5: Determine the adverse impacts from threat events (3.2), Task 2-4: Determine the likelihood (3.2), Task 2-6: Determine the risk to the organization (3.2) Risk Assessment Report (Appendix K)		Assessing Risk (3.2)
Assess Impact Assess Likelihood Prioritize Risks Calculate Exposure		Calculate Level of Risk		Management estimates the significance of a risk, considering the magnitude of impact, likelihood of occurrence, and nature of the risk			
Plan and Execute Response Strategies		Risk Evaluation (5.4.4)	Develop Alter-natives	Response to Risks (7.08)	Task 3-1: Communicate Risk Assessment Results Task 3-2: Share Risk-Related Information (3.3) Also See 800-37 Rev. 2 See 800-39	Categorize (3.2), Select (3.3), and Implement (3.4)	Responding to Risk (3.3)
	Risk Treatment (5.5)		Respond to Risks			Implement (3.4), Authorize (3.6), Residual Risk reflected in POA&M	
Monitor, Evaluate, and Adjust	Monitoring and review (5.6)		Monitor and Review	Identification of Change (9.02)	Task 4-1: Conduct ongoing monitoring of the risk factors (3.4) Task 4-2: Update Risk Assessment	Monitor (3.7)	Monitoring Risk (3.4)
				Analysis of and Response to Change (9.04)			

TASK DEI PROCESSI

[Rif.: 1) NIST SP 800-30; 2) NIST SP 800-37; 3) NIST SP 800-39]

1) IDENTIFICARE IL CONTESTO

- ✓ *Preparing for the Risk Assessment (Chapter 3.1 del NIST SP 800-30), è composto dai seguenti passi:*
  - **Task 1-1: Identify the purpose** *of the risk assessment in terms of the information that the assessment is intended to produce and the decisions the assessment is intended to support.*
  - **Task 1-2: Identify the scope** *of the risk assessment in terms of organizational applicability, time frame supported, and architectural/technology considerations.*
  - **Task 1-3: Identify the specific assumptions and constraints** *under which the risk assessment is conducted.*
  - **Task 1-4: Identify the sources** *of descriptive, threat, vulnerability, and impact information to be used in the risk assessment.*
  - **Task 1-5: Identify the risk model and analytic approach** *to be used in the risk assessment.*
- ✓ *Prepare tasks – Organization level (3.1)*
  - **Task P-1 Risk Management Roles:** *Identify and assign individuals to specific roles associated with security and privacy risk management. Individuals are identified and assigned key roles for executing the Risk Management Framework.[Cybersecurity Framework: ID.AM-6; ID.GV-2]*

- **Task P-2 Risk Management Strategy**: *Establish a risk management strategy for the organization that includes a determination of risk tolerance. A risk management strategy for the organization that includes a determination and expression of organizational risk tolerance is established.[Cybersecurity Framework: ID.RM; ID.SC]*
- **Task P-3 Risk Assessment Organization**: *Assess organization-wide security and privacy risk and update the risk assessment results on an ongoing basis. An organization-wide risk assessment is completed or an existing risk assessment is updated.[Cybersecurity Framework: ID.RA; ID.SC-2]*
- **Task P-4 Organizationally-tailored control baselines and/or Cybersecurity Framework Profiles**: *Establish, document, and publish organizationally-tailored control baselines and/or Cybersecurity Framework Profiles. These are established and made available. [Cybersecurity Framework: Profile]*
- **Task P-5 Common Control Identification:** *Identify, document, and publish organization-wide common controls that are available for inheritance by organizational systems. Common controls that are available for inheritance by organizational systems are identified, documented, and published.*
- **Task P-6 Impact Level Prioritization**: *Prioritize organizational systems with the same impact level. A prioritization of organizational systems with the same impact level is conducted. [Cybersecurity Framework: ID.AM-5]*
- **Task P-7 Continuous Monitoring Strategy Organization**: *Develop and implement an organization-wide strategy for continuously monitoring control effectiveness. An organization-wide strategy for monitoring control effectiveness is developed and implemented. [Cybersecurity Framework: DE.CM; ID.SC-4]*

✓ *Framing Risk (3.1) – vedi NIST SP 800-39*

2) IDENTIFICARE I RISCHI

- **Task 2-1: Identify and characterize threat sources** *of concern, including capability, intent, and targeting characteristics for adversarial threats and range of effects for non-adversarial threats.*
- **Task 2-2: Identify potential threat events**, *relevance of the events, and the threat sources that could initiate the events*
- **Task 2-3:** *Identify vulnerabilities and predisposing conditions that affect the likelihood that threat events of concern result in adverse impacts.*
- **Task P-14 Risk Assessment – System:** *Conduct a system-level risk assessment and update the risk assessment results on an ongoing basis. A system-level risk assessment is completed or an existing risk assessment is updated. [Cybersecurity Framework: ID.RA; ID.SC-2]*

✓ *Prepare tasks - System level (3.1)*

- **Task P-8 Mission or Business Focus**: *Identify the missions, business functions, and mission/business processes that the system is intended to support. Missions, business functions, and mission/business processes that the system is intended to support are identified. [Cybersecurity Framework: Profile; Implementation Tiers; ID.BE]*
- **Task P-9 System Stakeholders:** *Identify stakeholders who have an interest in the design, development, implementation, assessment, operation, maintenance, or disposal of the system. The stakeholders having an interest in the system are identified.[Cybersecurity Framework: ID.AM; ID.BE]*
- **Task P-10 Asset Identification:** *Identify assets that require protection. Stakeholder assets are identified and prioritized. [Cybersecurity Framework: ID.AM]*
- **Task P-11 Authorization Boundary:** *Determine the authorization boundary of the system. The authorization boundary (i.e., system) is determined.*
- **Task P-12 Information Types:** *Identify the types of information to be processed, stored, and transmitted by the system. The types of information processed, stored, and transmitted by the system are identified. [Cybersecurity Framework: ID.AM-5]*
- **Task P-13 Information Life Cycle:** *Identify and understand all stages of the information life cycle for each information type processed, stored, or transmitted by the system. All stages of the information life cycle are identified and understood for each information type processed, stored, or transmitted by the system. [Cybersecurity Framework: ID.AM-3; ID.AM-4]*

- **Task P-14 Risk Assessment – System:** *Conduct a system-level risk assessment and update the risk assessment results on an ongoing basis. A system-level risk assessment is completed or an existing risk assessment is updated.[Cybersecurity Framework: ID.RA; ID.SC-2]*
- **Task P-15 Requirements Definition:** *Define the security and privacy requirements for the system and the environment of operation. Security and privacy requirements are defined and prioritized. [Cybersecurity Framework: ID.GV; PR.IP]*
- **Task P-16 Enterprise Architecture:** *Determine the placement of the system within the enterprise architecture. The placement of the system within the enterprise architecture is determined.*
- **Task P-17 Requirements Allocation**: *Allocate security and privacy requirements to the system and to the environment of operation. Security and privacy requirements are allocated to the system and to the environment in which the system operates. [Cybersecurity Framework: ID.GV]*
- **Task P-18 System Registration:** *Register the system with organizational program or management offices. The system is registered for purposes of management, accountability, coordination, and oversight.[Cybersecurity Framework: ID.GV*

✓ *Assess (3.5)*

- **Task A-1 Assessor Selection:** *Select the appropriate assessor or assessment team for the type of control assessment to be conducted.*
  - *An assessor or assessment team is selected to conduct the control assessments.*
  - *The appropriate level of independence is achieved for the assessor or assessment team selected.*
- **Task A-2 Assessment Plan:** *Develop, Review, and Approve plans to assess implemented controls.*
  - *Documentation needed to conduct the assessments is provided to the assessor or assessment team.*
  - *Security and privacy assessment plans are developed and documented.*
  - *Security and privacy assessment plans are reviewed and approved to establish the expectations for the control assessments and the level of effort required.*
- **Task A-3 Control Assessment:** *Assess the controls in accordance with the assessment procedures described in assessment plans.*
  - *Control assessments are conducted in accordance with the security and privacy assessment plans.*
  - *Opportunities to reuse assessment results from previous assessments to make the risk management process timely and cost-effective are considered.*
  - *Use of automation to conduct control assessments is maximized to increase speed, effectiveness, and efficiency of assessments*
- **Task A-4 Assessment Report:** *Prepare the assessment reports documenting the findings and recommendations from the control assessments. Security and privacy assessment reports that provide findings and recommendations are completed.*
- **Task A-5 Remediations Actions:** *Conduct initial remediation actions on the controls and re assess remediated controls.*
  - *Remediation actions to address deficiencies in the controls implemented in the system and environment of operation are taken.*
  - *Security and privacy plans are updated to reflect control implementation changes made based on the assessments and subsequent remediation actions. [Cybersecurity Framework: Profile]*
- **Task A-6 plan of Action and Milestones:** *Prepare the plan of action and milestones based on the findings and recommendations of the assessment reports. A plan of action and milestones detailing remediation plans for unacceptable risks identified in security and privacy assessment reports is developed. [Cybersecurity Framework: ID.RA-6]*

3) ANALIZZARE I RISCHI E VALUTARE L'IMPATTO O L'ENTITÀ DEL DANNO CHE UN EVENTO GENERA

- **Task 2-5: Determine the adverse impacts** *from threat events of concern considering:*

  (i) the characteristics of the threat sources that could initiate the events;

(ii) the vulnerabilities/predisposing conditions identified;

(iii) the susceptibility reflecting the safeguards/countermeasures planned or implemented to impede such events.

✓ *Assessing Risk (3.2) – vedi NIST SP 800-39*

4) VALUTARE LE PROBABILITÀ CHE UN EVENTO ACCADA

➢ **Task 2-4: Determine the likelihood** that threat events of concern result in adverse **impacts,** considering:

(i) the characteristics of the threat sources that could initiate the events;

(ii) the vulnerabilities/predisposing conditions identified;

(iii) the organizational susceptibility reflecting the safeguards/countermeasures planned or implemented to impede such events.

5) DISPORRE LA PRIORITÀ DEI RISCHI

➢ **Task 2-6: Determine the risk** *to the organization from threat events of concern considering:*

(i) the impact that would result from the events;

(ii) the likelihood of the events occurring.

6) CALCOLARE LE ESPOSIZIONE AL RISCHIO

✓ *Risk Assessment Report (Appendix K del NIST SP 800-30)*

7) PIANIFICARE ED ESEGUIRE RISPOSTE STRATEGICHE

➢ **Task 3-1: Communicate risk assessment results** *to organizational decision makers to support risk responses.*

➢ **Task 3-2: Share risk-related information** *produced during the risk assessment with appropriate organizational personnel. See also 800-37 See 800-39.*

✓ *Categorize (3.2)*

➢ **Task C-1 System Description:** *Document the characteristics of the system. The characteristics of the system are described and documented.[Cybersecurity Framework: Profile]*

➢ **Task C-2 Security Categorization:** *Categorize the system and document the security categorization results.*

- *A security categorization of the system, including the information processed by the system represented by the organization-identified information types, is completed. [Cybersecurity Framework: ID.AM-1; ID.AM-2; ID.AM-3; ID.AM-4; ID.AM-5]*
- *Security categorization results are documented in the security, privacy, and SCRM plans. [Cybersecurity Framework: Profile]*
- *Security categorization results are consistent with the enterprise architecture and commitment to protecting organizational missions, business functions, and mission/business processes. [Cybersecurity Framework: Profile]*
- *Security categorization results reflect the organization's risk management strategy.*

➢ **Task C-3 Security Categorization Review and Approval:** *Review and approve the security categorization results and decision. The security categorization results are reviewed and the categorization decision is approved by senior leaders in the organization.*

✓ *Select (3.3)*

➢ **Task S-1 Control Selection:** *Select the controls for the system and the environment of operation. Control baselines necessary to protect the system commensurate with risk are selected. [Cybersecurity Framework: Profile]*

- **Task S-2 Control Tailoring**: *Tailor the controls selected for the system and the environment of operation. Controls are tailored producing tailored control baselines.[Cybersecurity Framework: Profile]*
- **Task S-3 Control Allocation:** *Allocate security and privacy controls to the system and to the environment of operation.*
  - *Controls are designated as system-specific, hybrid, or common controls*
  - *Controls are allocated to the specific system elements (i.e., machine, physical, or human elements). [Cybersecurity Framework: Profile; PR.IP]*
- **Task S-4 Documentation of Planned Control Implementations:** *Document the controls for the system and environment of operation in security and privacy plans. Controls and associated tailoring actions are documented in security and privacy plans or equivalent documents.[Cybersecurity Framework: Profile]*
- **Task S-5 Continuous Monitoring Strategy System:** *Develop and implement a system-level strategy for monitoring control effectiveness that is consistent with and supplements the organizational continuous monitoring strategy. A continuous monitoring strategy for the system that reflects the organizational risk management strategy is developed.[Cybersecurity Framework: ID.GV; DE.CM]*
- **Task S-6 Plan Review and Approval:** *Review and approve the security and privacy plans for the system and the environment of operation. Security and privacy plans reflecting the selection of controls necessary to protect the system and the environment of operation commensurate with risk are reviewed and approved by the authorizing official*

✓ *Implement (3.4)*

- **Task I-1 Control Implementation:** *Implement the controls in the security and privacy plans*
  - *Controls specified in the security and privacy plans are implemented. [Cybersecurity Framework: PR.IP-1]*
  - *Systems security and privacy engineering methodologies are used to implement the controls in the system security and privacy plans. [Cybersecurity Framework: PR.IP-2]*
- **Task I-2 Update control Implementation Information: Implemented Control**
  - *Changes to the planned implementation of controls are documented. [Cybersecurity Framework: PR.IP-1]*
  - *The security and privacy plans are updated based on information obtained during the implementation of the controls. [Cybersecurity Framework: Profile]*

✓ *Authorize (3.6)*

- **Task R-1 Authorization Package:** *Assemble the authorization package and submit the package to the authorizing official for an authorization decision. An authorization package is developed for submission to the authorizing official.*
- **Task R-2 Risk Analisys and determination:** *Analyze and determine the risk from the operation or use of the system or the provision of common controls. A risk determination by the authorizing official that reflects the risk management strategy including risk tolerance, is rendered.*
- **Task R-3 Risk Response:** *Identify and implement a preferred course of action in response to the risk determined. Risk responses for determined risks are provided. [Cybersecurity Framework: ID.RA-6]*
- **Task R-4 Authorization Decision:** *Determine if the risk from the operation or use of the information system or the provision or use of common controls is acceptable. The authorization for the system or the common controls is approved or denied.*
- **Task R-5 Authorization reporting:** *Report the authorization decision and any deficiencies in controls that represent significant security or privacy risk. Authorization decisions, significant vulnerabilities, and risks are reported to organizational officials.*

✓ *Responding to Risk (3.3) – vedi NIST SP 800-39*

8) MONITORARE, VALUTARE, REGOLARE

- **Task 4-1: Conduct ongoing monitoring of the risk factors** *that contribute to changes in risk to organizational operations and assets, individuals, other organizations, or the Nation.*
- **Task 4-2: Update existing risk assessment** *using the results from ongoing monitoring of risk factors.*

✓ *Monitor (3.7)*

- **Task M-1 System and Environment Changes:** *Monitor the information system and its environment of operation for changes that impact the security and privacy posture of the system. The information system and environment of operation are monitored in accordance with the continuous monitoring strategy. [Cybersecurity Framework: DE.CM;ID.GV]*
- **Task M-2 Ongoing Assessment:** *Assess the controls implemented within and inherited by the system in accordance with the continuous monitoring strategy. Ongoing assessments of control effectiveness are conducted in accordance with the continuous monitoring strategy. [Cybersecurity Framework: ID.SC-4]*
- **Task M-3 Ongoing Risk Response:** *Respond to risk based on the results of ongoing monitoring activities, risk assessments, and outstanding items in plans of action and milestones. The output of continuous monitoring activities is analyzed and responded to appropriately. [Cybersecurity Framework: RS.AN]*
- **Task M-4 Authorization Package Update:** *Update plans, assessment reports, and plans of action and milestones based on the results of the continuous monitoring process. Risk management documents are updated based on continuous monitoring activities. [Cybersecurity Framework: RS.IM]*
- **Task M-5 Security and Privacy Reporting:** *Report the security and privacy posture of the system to the authorizing official and other organizational officials on an ongoing basis in accordance with the organizational continuous monitoring strategy. A process is in place to report the security and privacy posture to the authorizing official and other senior leaders and executives.*
- **Task M-6 Ongoing Authorization:** *Review the security and privacy posture of the system on an ongoing basis to determine whether the risk remains acceptable. Authorizing officials conduct ongoing authorizations using the results of continuous monitoring activities and communicate changes in risk determination and acceptance decisions.*
- **Task M-7 System Disposal:** *Implement a system disposal strategy and execute required actions when a system is removed from operation. A system disposal strategy is developed and implemented, as needed.*

✓ *Monitoring Risk (3.4) – vedi NIST SP 800-39*

6A. ONTOLOGY FOR AUTHENTICATION (IDENTITY)

[Rif.: NIST IR 8344]

SINTESI

Questo capitolo descrive l'implementazione della componente di autenticazione di un processo di gestione dell'autenticazione e dell'autorizzazione (Identity Authorization and Authentication - IAA) dell'identità.

Viene presentata una tassonomia dell'autenticazione per entrambe le autenticazioni incentrate sull'entità e sugli oggetti.

L'autenticazione dell'entità è suddivisa in tre aree:

1) **uomo-macchina;**
2) **macchina-macchina;**
3) **uomo-uomo**.

Affrontando la necessità di misurare definitivamente la forza dell'autenticazione, sono identificate quattro aree:

1) **Sicurezza***;*
2) **Usabilità***;*

3) **Distribuibilità**;
4) **Gestibilità**.

Per ogni area viene discussa una serie di fattori ambientali adatti alla misurazione.

La figura 1 fornisce una mappa concettuale dell'ontologia.

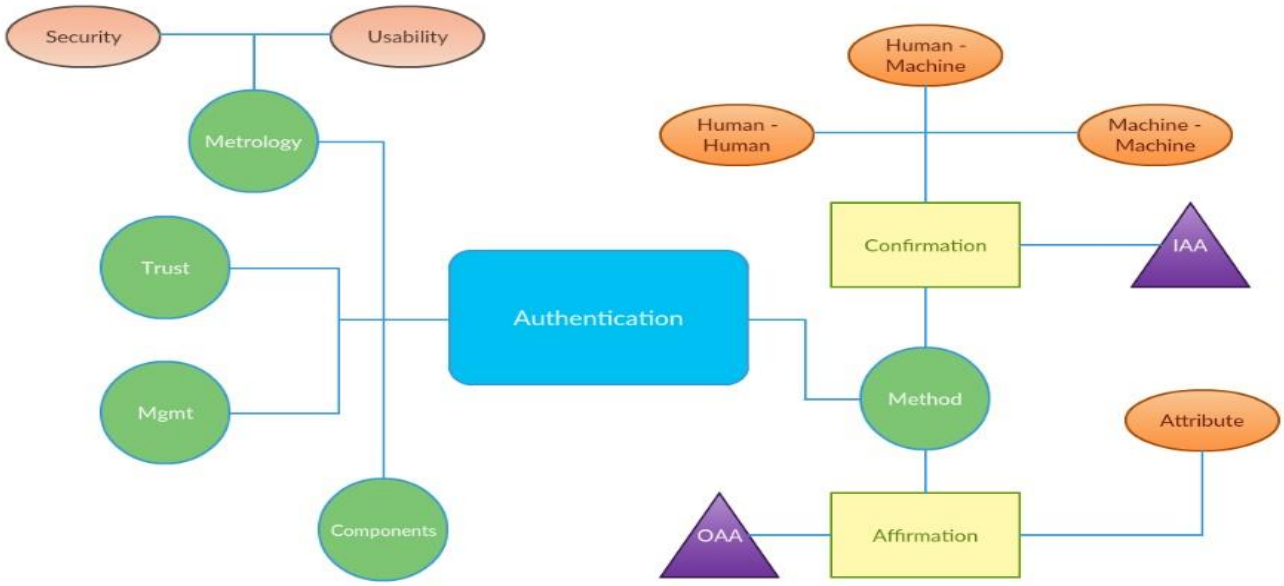


Figure 1 - Concept Map for Authentication Properties

Per affermare la questione in un altro modo, sembra esserci una relazione tra quanto è chiesto all'operatore e quanto è disposto l'operatore a supportare la sicurezza piuttosto che a gestirla (male).

INTRODUZIONE

L'autenticazione ha un impatto su diverse aree di un'organizzazione, in particolare la Generazione e il Coordinamento delle politiche.

Un insieme comune di misurazioni che riguardano tutti i meccanismi di autenticazione include:

- ✓ *l'unicità dell'hardware, del software o dei processi che rappresentano l'entità per l'entità che viene autenticata;*
- ✓ *la resistenza della rappresentazione ad essere duplicata o altrimenti compromessa;*
- ✓ *la protezione della rappresentazione durante la consegna al meccanismo di convalida e la protezione del meccanismo contenente il riferimento di autenticazione;*
- ✓ *l'usabilità dell'autenticazione uomo-macchina.*

L'autenticazione è la componente del processo IAA che fornisce un certo grado di garanzia che l'identità assegnata all'entità sia verificata.

La comprensione del processo per ottenere correttamente l'accesso a un sistema è spesso complicata dall'uso incoerente della terminologia.

DESCRIZIONE DELL'ONTOLOGIA DELL'AUTENTICAZIONE

La mappa concettuale mostrata nella Figura 1 identifica i fattori chiave osservati dalla valutazione delle metodologie di autenticazione.

Alcuni aspetti dell'ontologia sono di natura gerarchica o strutturale, come la tassonomia dei meccanismi di autenticazione fornita nella Figura 2.

La gestione dell'autenticazione include la relazione tra la gestione dell'identità (Identity Management - IM) e l'autorizzazione.

La tassonomia raggruppa alcuni meccanismi in base alle loro somiglianze e aiuta nella comprensione di ulteriori proprietà identificate da questo studio.

TASSONOMIA DEI MECCANISMI DI AUTENTICAZIONE

SCHEMA TASSONOMIA

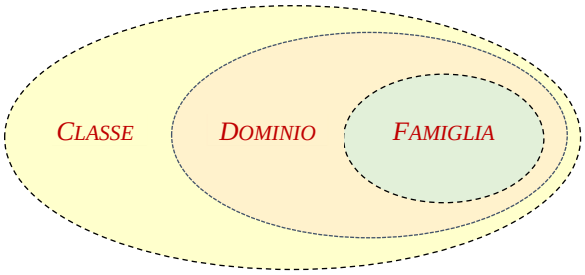


TABELLA CLASSI/DOMINI/FAMIGLIE

CLASSE (AUTENTICAZIONE)	DOMINIO	FAMIGLIA	ATTRIBUTO
1) ***Confirmation**: per gestire autorizzazioni e accessi (entità)*	*Uomo-Macchina (iniziale, multimodale e continua)*	1) *Segreto memorizzato* 2) *Biometrica* 3) *Apparato* 4) *Multimodale*	*Per la Famiglia Multimodale:* 1) *Tempo* 2) *Posizione*
	Macchina-Macchina	-	
	Uomo-Uomo	-	
2) ***Attestation**: per verifica attributi (oggetti)*	*Attributo*	1) *Crittografia* 2) *Archiviazione* 3) *Filigrana*	

DESCRIZIONE TASSONOMIA

Una tassonomia dei meccanismi di autenticazione fornisce una struttura per classificare tipi diversi ma correlati di meccanismi di autenticazione.

Questo documento propone una tassonomia composta da due classi principali di autenticazione:

1) **conferma**;
2) **attestazione**.

La **conferma** *è generalmente utilizzata come verifica di un'entità per gestire le autorizzazioni o l'accesso.*

*L'***attestazione** *è generalmente la verifica di un attributo diretto o indiretto dell'oggetto (non entità) di interesse.*

Ulteriori analisi hanno portato alla creazione di tre domini sotto la classe di conferma:

1) **uomo-macchina** *(ad esempio, un utente umano che si autentica su un dispositivo);*
2) **macchina-macchina** *(ad esempio, un accesso Internet aziendale automatizzato);*

1) *autenticazione* **uomo-uomo** *(ad esempio, recupero della password).*

*L'***attestazione** *è la seconda classe di autenticazione; il suo scopo è verificare l'oggetto piuttosto che utilizzare l'oggetto per verificare l'entità che rappresenta, inoltre, è utilizzata su oggetti, dalla filigrana digitale e fisica alle firme digitali.*

Questa classe di autenticazione ha una vasta gamma di obiettivi di garanzia, dalle indicazioni che un oggetto non è stato modificato per impedire la duplicazione. Attualmente esiste un solo dominio per l'attestazione: attributo.

La figura 2 presenta la struttura attuale della tassonomia dell'autenticazione con le classi di **conferma** *e* **attestazione**, *nonché i domini* **uomo-macchina, macchina-macchina, uomo-uomo** *e* **attributo**.

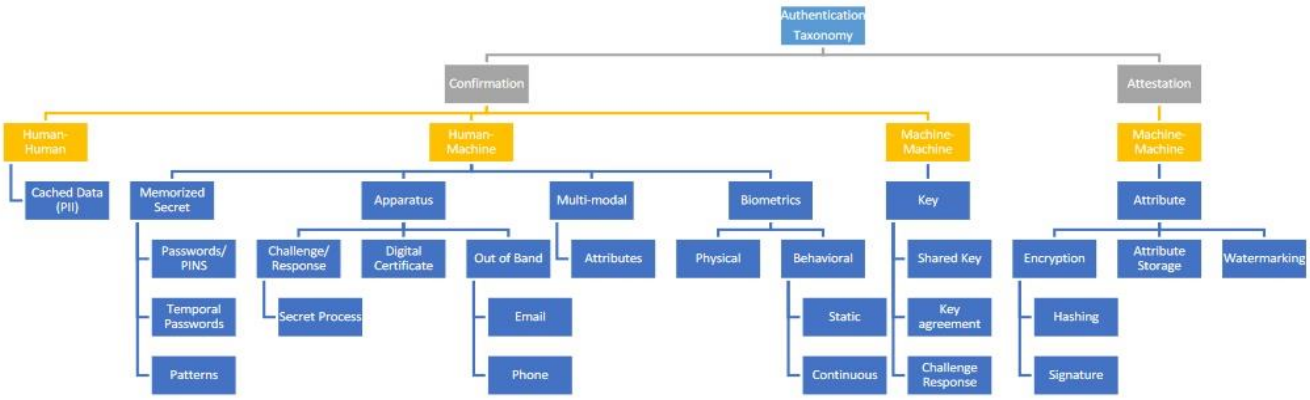


Figure 2 - Authentication taxonomy

CLASSE: CONFIRMATION

Conferma che l'hardware, il software o il processo fornito che rappresenta l'entità è valido per l'accesso.

Attualmente ci sono tre domini sotto la conferma:

1) **uomo-macchina***;*
2) **macchina-macchina***;*
3) **uomo-uomo**.

DOMINI DI CONFIRMATION

Autentica un'entità che è tipicamente rappresentata da una ma a volte da un gruppo di entità.

L'autenticazione più conosciuta dal pubblico è un essere umano che interagisce con qualche interfaccia o sensore che consente l'accesso da parte di un individuo.

Questo dominio è **uomo-macchina**.

I meccanismi di autenticazione sono spesso necessari per supportare le connessioni attraverso e all'interno di ogni livello del modello OSI (Open Systems Interconnection). Anche rimanendo all'interno delle comunicazioni TCP/IP, le autenticazioni sono state ottimizzate per e attraverso i livelli di astrazioni, come quelle presentate nella Figura 3 di seguito.

La figura 3 mostra la gerarchia IP comune dei computer moderni.

La tecnologia di autenticazione **macchina-macchina** *spesso cancella l'interfaccia di diversi livelli di comunicazione. Il livello dell'applicazione si trova in genere all'interno di un singolo sistema e spesso richiede almeno l'accesso a livello di console.*

L'accesso dell'utente alla console è gestito dall'amministratore del sistema, sebbene possa richiedere anche i permessi della rete interna tramite Active Directory o simili.

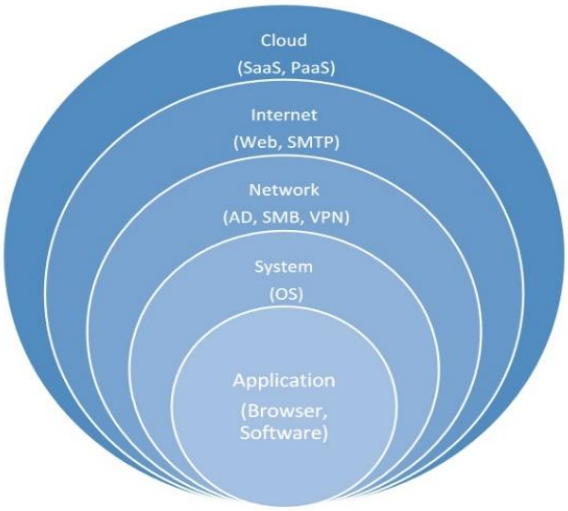


Figure 3 - Authentication Implementation Complexity (not user experience)

Quando si utilizzano servizi web sotto il controllo di un provider, l'utente e le entità aziendali devono accettare le politiche del provider. Tuttavia, i servizi cloud possono fornire piattaforme, servizi e applicazioni pur essendo strettamente legati a ciascuna politica aziendale che servono. Questo è il dominio dell'autenticazione di conferma **macchina-macchina**.

Un utente in genere considera l'autenticazione a un sito Web da una rete aziendale come un semplice processo di autenticazione. Tuttavia, la Figura 4 mostra le complessità nell'intreccio delle autenticazioni uomo-macchina e macchina-macchina, comprese le opzioni per il **Single Sign-On** *per i servizi che possono supportare l'azienda al di fuori della rete.*

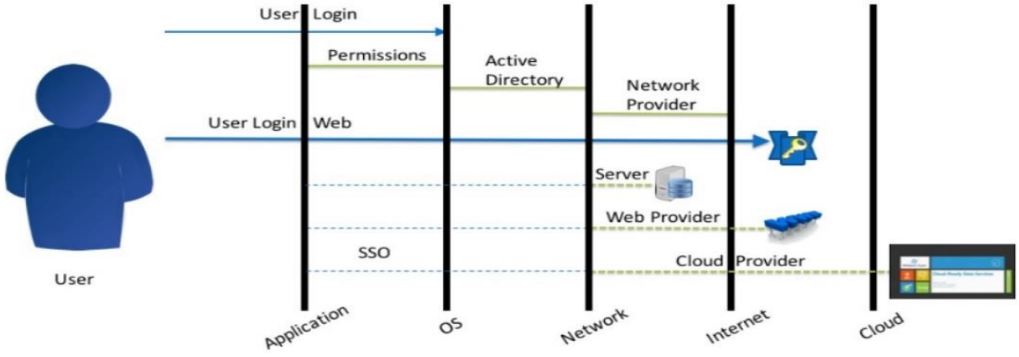


Figure 4 - Human-Machine and Machine-Machine Resources

L'ultimo dominio è solitamente il meno considerato ma il più costoso da gestire. L'autenticazione **uomo-uomo** *è spesso utilizzata come ultima risorsa dopo che l'***uomo-macchina** *ha fallito.*

È noto che gli hacker bloccano intenzionalmente un account di autenticazione **uomo-macchina** *per tentare di manipolare gli amministratori che supportano l'autenticazione* **uomo-uomo** *per fornire all'hacker l'accesso all'account.*

DOMINIO: UOMO-MACCHINA

Nel dominio **uomo-macchina**, *un essere umano ha il controllo dell'hardware, del software o del processo che rappresenta l'entità. Per adattarsi alla moltitudine di meccanismi diversi, l'autenticazione* **uomo-macchina** *è stata ulteriormente suddivisa in* **Iniziale**, **Multimodale** *e* **Continua**.

INIZIALE

La maggior parte dei meccanismi di autenticazione odierni sono considerati un tipo di meccanismo di autenticazione **iniziale**, *che risponde con una singola risposta:* **cioè sì o no**.

Tre categorie principali di meccanismi di **autenticazione iniziale** *attualmente utilizzati oggi includono password, dispositivi di autenticazione dedicati e biometria, con il loro utilizzo principalmente una volta per sessione.*

CONTINUA

*L'***autenticazione continua** *è attualmente rara nell'ambiente di oggi, ma offre molte promesse. Utilizza un meccanismo che è spesso basato sulla biometria comportamentale utilizzata in una modalità di campionamento continuo.*

MULTIMODALE

*Il sottodominio finale dell'***autenticazione uomo-macchina**, **multimodale**, *è qualsiasi combinazione di* **autenticazione iniziale e/o continua**.

Una volta che l'utente si è autenticato con successo, il meccanismo di autenticazione può memorizzare nella cache credenziali alternative per alleviare l'onere dell'autenticazione su ciascun sistema quando si prevede che il livello di rischio sia sufficientemente basso. In questi casi, si tratta di un'autenticazione **macchina-macchina** *che rappresenta l'uomo al posto di un'autenticazione* **uomo-macchina**.

FAMIGLIA: SEGRETO MEMORIZZATO

*La definizione più generica di segreto memorizzato è "***qualcosa che conosci***" che viene condiviso solo con la macchina che conferma l'utente. Sebbene esistano diverse forme di segreti memorizzati, tra cui password, numero di identificazione personale (PIN), immagine e suono, sono tutti utilizzati per dimostrare la conoscenza dell'utente delle informazioni segrete da condividere solo con il server di autenticazione. Le organizzazioni che utilizzano segreti memorizzati per l'autenticazione spesso seguono le ultime tendenze senza valutarne l'usabilità, rendendo difficile se non onerosa la selezione e l'utilizzo dei segreti memorizzati.*

PERSONAL INFORMATION

Le password cognitive sono talvolta utilizzate come meccanismo di autenticazione secondario o di backup. L'interfaccia presenta domande con risposte precedenti e spesso poste di frequente che potrebbero essere facilmente richiamate e risposte dalla memoria.

In alternativa, il server può richiedere all'utente di selezionare domande a scelta multipla sulla base di record storici e pubblicamente disponibili per integrare la prova dell'identità come forma di autenticazione.

Tuttavia, questo ha l'effetto collaterale negativo di raccogliere ulteriori informazioni sulla privacy, che in genere sono considerate di scarso valore.

FAMIGLIA: BIOMETRICA

*L'autenticazione basata su "****qualcosa che sei****" si riferisce spesso all'autenticazione biometrica. Esempi comuni includono impronta digitale, viso, iride e riconoscimento vocale.*

I dati biometrici utilizzati nell'autenticazione iniziale determinano una tantum la certezza che la scansione attiva e i dati biometrici raccolti prima dell'autenticazione provengano dallo stesso utente.

Un biometrico crea tipicamente un modello che incapsula i dettagli dell'oggetto in un hardware, software o processo che rappresenta l'entità, che viene confrontata con un riferimento.

Un esempio di raccomandazioni del NIST per l'uso della biometria nei meccanismi di autenticazione è SP 800-76-2.

CATEGORIA: INIZIALE

Attualmente, l'autenticazione **uomo-macchina** *più comune è l'autenticazione iniziale, questa convalida rapidamente una credenziale (come un'impronta digitale) che l'utente ha fornito in precedenza in modo che l'autorizzazione possa consentire all'utente di accedere alle informazioni o funzionalità richieste. Una volta completata l'autenticazione iniziale, la connessione rimane finché non viene interrotta dall'utente o da un altro meccanismo di monitoraggio.*

CATEGORIA: CONTINUO

Occasionalmente, gli utenti intenzionalmente o accidentalmente lasciano l'accesso aperto e disponibile ad altri. Diverse applicazioni basate sulla temporizzazione o altro hardware dedicato tentano di ridurre al minimo questa esposizione. Quando il fattore raggiunge una soglia predeterminata, l'utente viene autenticato per un certo periodo di tempo, legando più strettamente l'autenticazione all'utente. Tuttavia, questi meccanismi di autenticazione continua sono spesso limitati nel loro utilizzo a causa della non uniformità degli utenti (ad esempio, limitazioni o cambiamenti mentali o fisici).

BIOMETRIA COMPORTAMENTALE

La biometria comportamentale valuta continuamente l'utente monitorando alcune sue attività, come la digitazione, analizzando gli aspetti della digitazione per assicurarsi che l'operatore non sia cambiato.

A differenza dell'autenticazione iniziale, l'autenticazione continua valuta ripetutamente l'utente corrente per attività e identità.

La biometria cognitiva può essere considerata una forma di biometria comportamentale che si concentra sull'analisi delle emanazioni del cervello. Può essere utilizzata direttamente o tramite traduttore, a seconda della modalità biometrica. La biometria cognitiva interpreta i dati biometrici nell'azione umana, come qualcosa di sentito o visualizzato. Un esempio di ciò è il campionamento elettromagnetico dell'attività cerebrale in azioni come il movimento o la parola "virtuale", aggiungendo un aspetto veramente dinamico all'autenticazione.

FAMIGLIA: APPARATO

*Un apparato di autenticazione è spesso considerato "***qualcosa che possiedi***" e può includere PIN o password che cambiano in base all'ora o agli eventi in dispositivi hardware, smartcard o dispositivi basati su RFID.*

Un punto debole comune è che è relativamente facile perdere il dispositivo. Questo è in genere contrastato dall'uso di un meccanismo di autenticazione aggiuntivo, come i PIN, raggruppati in una soluzione più forte.

Ad esempio, una smartcard potrebbe supportare un'infrastruttura PKI ed è generalmente considerata una delle forme di autenticazione più efficaci.

La forma di realizzazione fisica ha reso difficile per gli aggressori replicare il dispositivo, ma non avrebbe necessariamente resistito a sofisticate tecniche di valutazione. I dispositivi di memoria sembrano essere sempre più difficili da trovare.

Va notato che i dispositivi hardware che agiscono per il server di convalida non sono considerati un autenticatore utente per questa tassonomia.

FAMIGLIA: MULTIMODALE

L'autenticazione multimodale è definita come la combinazione di due o più metodi di autenticazione **uomo-macchina***, sia iniziale sia continua, per aumentare la robustezza di un sistema.*

L'aggiunta di ulteriori forme di autenticazione per aumentare la difficoltà di compromettere un sistema è definita autenticazione a più fattori.

Questo si basa sui tre tipi di autenticazione: 1) ***qualcosa che conosci****, 2)* ***qualcosa che hai****, 3)* ***qualcosa che sei****.*

L'autenticazione a più fattori fa spesso riferimento a un token della smartcard con l'utente che immette una password o un PIN per sbloccare la smartcard.

I fattori che dovrebbero essere considerati includono compensazioni di vulnerabilità o esposizioni note, nonché impatti sull'usabilità.

L'autenticazione multimodale può aggiungere flessibilità a molti dei sistemi di autenticazione attualmente in uso.

ATTRIBUTI

L'aggiunta di determinati attributi può anche aiutare a rafforzare il processo di autenticazione.

La prescrizione dell'ambiente dell'utente in modo significativo può fornire maggiore sicurezza.

Gli attributi possono essere utilizzati per l'autenticazione e l'autorizzazione o solo l'autorizzazione, a seconda dei meccanismi di ciascuno e di quanto possa essere necessario compartimentare l'accesso.

- ✓ **TEMPO**

L'autenticazione controllata in determinati giorni della settimana o in alcune ore del giorno è stata supportata in molti sistemi ma viene utilizzata raramente. Allo stesso modo, le organizzazioni possono scegliere di disabilitare l'autenticazione per determinati utenti durante le vacanze o una malattia prolungata.

I limiti di tempo sono spesso impiegati e accoppiati con monitor di attività per ridurre al minimo l'esposizione dell'accessibilità se sembra che l'utente abbia abbandonato l'accesso.

I limiti di tempo possono essere implementati nell'autenticazione, autorizzazione o in entrambi.

- ✓ **POSIZIONE**

Ulteriori verifiche possono essere ottenute da attributi relativi alla posizione geografica. Le posizioni fisiche possono includere GPS, sensori di prossimità e indirizzi IP interni (controllati).

Le posizioni logiche possono includere indirizzo IP identificato o previsto, tempo previsto per la risposta o VPN affidabile.

Anche il numero di accessi simultanei può essere un fattore di limitazione, sebbene ora venga utilizzato meno spesso a causa del numero di dispositivi a cui gli utenti accedono quotidianamente.

DOMINIO: MACCHINA-MACCHINA

Un altro dominio nella classe di conferma è l'autenticazione **macchina-macchina**. *Questo dominio è spesso utilizzato per l'autenticazione del sistema organizzativo o di rete, come connessioni di rete per workstation e dispositivi mobili, VPN o comunicazioni business to business.*

L'autenticazione basata su macchina è spesso basata su uno schema crittografico, come PKI o altro accordo chiave o schema di negoziazione chiave. Anche gli schemi Single Sign-On che supportano più autenticazioni per un utente dopo l'accesso utente iniziale dovrebbero essere considerati in questo dominio.

L'autenticazione **macchina-macchina** *viene utilizzata per:*

- ✓ *Autenticazione tramite un collegamento di comunicazione;*
- ✓ *Supportare una rete di dispositivi affidabili;*
- ✓ *Supportare un'autenticazione uomo-macchina automatizzata (cache);*
- ✓ *Fornire altri dati di autenticazione, come la posizione (ad esempio, accesso aziendale ai servizi);*
- ✓ *Fornire servizi affidabili (ad esempio, DNS, NTS, posizione, ecc.).*

Inoltre, l'autenticazione **macchina-macchina***:*

- ✓ *di solito è di natura crittografica:*
  - ➢ *utilizza spesso i protocolli consigliati dal NIST (ad es. IPSEC, TLS);*
  - ➢ *utilizza una chiave pre-condivisa (simmetrica) o una firma digitale;*
- ✓ *è impostato da un amministratore.*
- ✓ *è spesso trasparente per l'utente;*
- ✓ *può essere un'autenticazione uomo-macchina memorizzata nella cache;*
- ✓ *può collegarsi temporalmente (ricorrente o meno) o può essere autocontrollato (vedere l'attestazione).*

DOMINIO: **UOMO-UOMO**

Il dominio finale nella classe di Confirmation è l'autenticazione **uomo-uomo**. *È spesso utilizzato quando un utente non è in grado di accedere tramite il sistema uomo-macchina.*

È considerato l'obiettivo più facile e più suscettibile agli attacchi, principalmente dall'ingegneria sociale.

Se le informazioni utilizzate come autenticatori non sono sufficientemente protette, il "database" dell'autenticatore diventa un'altra fonte di attacco.

Esistono due utilizzi principali per l'autenticazione uomo-uomo.

***Nel primo caso**, è stabilita un'identità tramite credenziali provenienti da altre fonti approvate. Un aspetto importante di questa autenticazione uomo-uomo di gestione delle identità è che le credenziali, sebbene fornite dall'utente, sono state autenticate da fonti riconosciute al di fuori dello schema di autenticazione.*

CLASSE: ATTESTAZIONE

Autentica un oggetto piuttosto che un'entità. Un esempio comune potrebbe essere l'hash di un file per verificare in seguito che non sia cambiato.

DOMINIO: **ATTRIBUTO**

Questo dominio conferma un oggetto verificando un attributo dell'oggetto.

Sebbene un'attestazione possa essere semplice come un controllo CRC (Cyclic Redundancy Check), la garanzia spesso si basa su un'operazione crittografica, come un seme o una chiave predeterminata, per rendere più difficile la sostituzione di un nuovo oggetto e determinare un nuovo valore.

Gli attributi dovrebbero essere selezionati in modo tale che maggiore è la fiducia necessaria, più difficile è cambiare l'oggetto senza essere in grado di rilevare il cambiamento nell'attributo. Ciò non significa necessariamente che non sia consentito modificare altri attributi. Ad esempio, un hash con chiave o una firma digitale di un file può accertare se il file rimane invariato, ma non impedisce a un utente di modificare l'associazione del file modificando l'estensione del nome del file.

Tre famiglie di attestazione degli attributi sono **crittografia**, **archiviazione** *e* **filigrana**.

La famiglia dipende dal focus dell'attributo piuttosto che dal meccanismo utilizzato.

FAMIGLIA: CRITTOGRAFIA

CATEGORIA: HASHING

L'hashing è spesso utilizzato per identificare i dati che non sono stati modificati da quando è stato acquisito l'hash ed è generalmente scelto quando l'uso del file è consentito ma le modifiche al file non lo sono.

*Una volta che un hash è stato generato dal file, le informazioni risultanti non possono essere invertite e la dimensione "**dell'impronta digitale**" è ridotta a una lunghezza dipendente dall'algoritmo di hash.*

La protezione dell'hash è importante per evitare che il file venga modificato o che venga generato un nuovo hash per sostituire il vecchio.

- ✓ **FIRME DIGITALI**

Le firme digitali forniscono la verifica che un file non sia stato modificato. In genere, questo tipo di attestazione esegue l'hashing del file di interesse prima di crittografare l'hash con una firma digitale che può essere ricondotta all'utente e all'autorità di certificazione.

Due forme principali di firme digitali sono DSA e PKI.

- ✓ **CRITTOGRAFIA SIMMETRICA**

Se non è necessario avere accesso illimitato al file di interesse, è possibile utilizzare anche la crittografia di un file per assicurarsi che non sia stato inconsapevolmente modificato. Qualsiasi modifica al file crittografato comporterà l'interruzione e il ripristino della crittografia a meno che la modifica non è identificata e annullata.

Ciò è particolarmente utile per il trasferimento dei dati, che può includere la crittografia prima del trasferimento o uno schema di trasporto come TLS o SSH.

FAMIGLIA: ARCHIVIAZIONE (STORAGE)

Questo è uno dei pochi metodi di attributo di attestazione che non si basa necessariamente sulla crittografia per la protezione ma piuttosto sulla separazione dall'oggetto.

Un attributo può essere memorizzato separatamente dall'oggetto, di solito in uno schema di protezione IAA o in un formato che non può essere facilmente modificato, come l'utilizzo di un hash con chiave o un meccanismo simile.

FAMIGLIA: FILIGRANA (WATERMARKING)

Il Watermarking differisce dalle altre attestazioni in quanto tipicamente si concentra sulla rappresentazione incorporata dai dati piuttosto che sui dati stessi. Ad esempio, una fotografia a colori digitalizzata spesso non viene riconosciuta guardando i dati.

La filigrana crea tipicamente un oggetto incorporato sulla rappresentazione dei dati, come un'immagine.

Sebbene la filigrana non sia necessariamente crittografica, la crittografia viene spesso utilizzata per impedire la manipolazione della filigrana.

PROCESSO IAA PER LA **CONFIRMATION**

L'autenticazione è un componente del processo IAA, come mostrato nella Figura 5.

Il processo IAA è costituito da tre attività uniche:

1) IDENTIFICARE;
2) AUTENTICARE;
3) AUTORIZZARE.

Figure 5 - IAA process

IDENTIFY (IM-IDENTITY MANAGEMENT)

*Scopo della gestione dell'***Identify** *è il rilascio o l'adozione di un'identità digitale che è logicamente legata a un'entità fisica; tale entità si basa sulla ricezione di credenziali di identificazione da parti attendibili, come un passaporto, una licenza o una registrazione aziendale.*

L'identità digitale è un artefatto prodotto per stabilire una presenza i sistemi di interesse ed è questa entità digitale che effettua l'autenticazione e che il componente di autorizzazione consente o limita una volta autenticato.

La garanzia di fiducia per l'entità fisica è solitamente correlata alla quantità e alla qualità della documentazione di terze parti, mentre la garanzia di fiducia per l'autenticazione dell'entità digitale è relativa alla forza dell'autenticazione utilizzata e al livello di protezione delle risorse a cui accedere.

Oltre ai problemi di identità, IM deve comunicare con entrambi i componenti di Authenticate e Authorize per applicare i diritti dell'entità digitale.

L'IM stabilisce i requisiti per una prova di identità sufficiente per un utente.

L'IM può anche far parte di una rete federata o gerarchica che gestisce le autorizzazioni degli utenti al di là delle risorse controllate direttamente.

Di fondamentale importanza per l'autenticazione è la comunicazione e l'accordo tra la gestione dell'identità e l'autenticazione.

Come minimo, la comunicazione tra IM e autenticazione dovrebbe supportare la richiesta di autorizzazione, revoca e riconoscimento delle richieste.

AUTHENTICATE

Scopo dell'autenticazione è confermare un'identità digitale attraverso la manipolazione di un hardware, software o processo che rappresenta l'entità.

In caso di manipolazione riuscita dell'hardware, del software o del processo che rappresenta l'entità, il componente di autenticazione comunica al componente di autorizzazione una conferma o un rifiuto per consentire l'accesso.

L'autenticazione può non consentire ulteriori tentativi di autenticazione quando viene superata la soglia di un tentativo non riuscito.

La sensibilità operativa e temporale può dettare la scelta della nuova autenticazione.

Gli attuali punti di forza dell'autenticazione dipendono dal tipo di meccanismo utilizzato: la biometria dipende da un basso numero di falsi positivi; le password dipendono da tentativi non riusciti; e le implementazioni PKI dipendono da forti chiavi pubbliche e private.

L'hardware, il software, la fonte biometrica o la conoscenza sotto il controllo dell'utente sono spesso indicati come token o autenticatore. Può assumere molte forme diverse a seconda del processo di autenticazione e dei meccanismi utilizzati; nell'autenticazione **uomo-macchina**, *ci sono tre forme di base che vengono spesso discusse: 1)* ***qualcosa che conosci****, 2)* ***qualcosa che hai*** *e 3)* ***qualcosa che sei****.*

Sebbene questi non siano direttamente associati al livello di autenticazione, la combinazione di queste diverse forme di autenticazione è stata storicamente utilizzata per aumentare la fiducia nel processo di autenticazione.

AUTHORIZE

L'ultimo passaggio del processo IAA è l'applicazione delle autorizzazioni.

Dopo aver ricevuto un rapporto di successo dal componente d'autenticazione IAA, l'autorizzazione consente all'entità digitale di accedere per eseguire programmi o manipolare informazioni.

Spesso, le autorizzazioni offrono una certa granularità, come la sola lettura, il permesso di eseguire o consentono all'entità di modificare le informazioni.

I controlli e i vincoli dell'autorizzazione vengono risolti tramite implementazioni del controllo degli accessi basato sui ruoli (RBAC - Role-Based Access Control) e del controllo degli accessi basato sugli attributi (ABAC - Attribute-Based Access Control).

Il controllo di accesso obbligatorio (MAC - Mandatory Access Control) e il controllo di accesso discrezionale (DAC - Discretionary Access Control) erano le prime implementazioni del controllo di accesso che negava tutto a meno che non fosse consentito (ad esempio, MAC) o consentiva tutto a meno che non fosse negato (ad esempio, DAC).

Va notato che i controlli di cui sopra sono sotto la componente di autorizzazione IAA.

Le comunicazioni tra i componenti si concentrano principalmente sul consentire o negare l'accesso a un'identità digitale.

Insieme all'autorizzazione, la gestione dell'identità consente o nega l'accesso all'entità digitale.

METROLOGIA PER L'AUTENTICAZIONE

Storicamente, la forza di un'autenticazione è stata attribuita direttamente alla crittografia utilizzata nel processo decisionale. Ciò non si applica ai meccanismi **uomo-macchina** *non basati sulla crittografia, come password o dati biometrici.*

Usare la forza della crittografia come misura è un valore ottimistico.

Basare solo sulla crittografia, all'interno del processo decisionale, si ignora qualsiasi:

1) *protezione utilizzata per il trasferimento delle informazioni di autenticazione;*
2) *protezione dei dati segreti durante l'archiviazione;*
3) *difetto di implementazione o configurazione che possa comportare la compromissione.*

Nell'autenticazione con un'interfaccia uomo-macchina basata sulla crittografia, sono adottate soluzioni alternative per affrontare i limiti umani.

Gli utenti sono spesso limitati quando si tratta di ricordare lunghezze di chiavi sufficientemente potenti e il numero di chiavi che dovrebbero conservare per i sistemi a cui accedono.

*Sono state sviluppate alternative che non si basano sul fatto che gli esseri umani ricordino direttamente i componenti di crittografia, ma piuttosto implichino un passaggio aggiuntivo, come "**qualcosa che hai**".*

Per i sistemi che supportano un'interfaccia umana ma non sono basati sulla crittografia, la crittografia può essere utilizzata per aggiungere complessità al sistema e renderlo più difficile per l'attaccante. Ad esempio, sistemi alternativi possono essere basati su una qualche forma di password o dati biometrici.

SICUREZZA

Sebbene non siano stati finora identificati metodi metrologici specifici per l'autenticazione, alcuni candidati sono discussi di seguito.

RAPPRESENTAZIONE

Questa è una misura del collegamento tra il token e l'entità da autenticare.

Si prevede che quanto più strettamente il token possa essere legato all'entità, tanto maggiore è la garanzia.

Tuttavia, il token deve essere selezionato in modo tale da poter rappresentare un aspetto dell'entità affinché non sia confuso con un altro.

INIMITABILE

Questa è una misura della resistenza del token a essere duplicato o altrimenti compromesso. Un compromesso è spesso correlato al tipo di autenticazione.

Ciò che conta è la resistenza al compromesso, non necessariamente il compromesso specifico applicato.

Poiché possono esserci più suscettibilità applicabili, la misura della minore resistenza dovrebbe essere associata alla forza di sicurezza dell'implementazione del meccanismo.

CONSEGNA SICURA

Dovrebbe misurare la protezione del token dal punto di ingresso da parte dell'entità al punto di valutazione dell'autenticazione e la decisione della valutazione alla gestione dell'autorizzazione.

La protezione dovrebbe affrontare una combinazione di vulnerabilità dovute a compromissioni, sostituzioni e omissioni non intenzionali dell'utente.

ARCHIVIAZIONE SICURA

È una misura della protezione delle informazioni di riferimento che il meccanismo di autenticazione utilizza per verificare l'entità. La misura di protezione dovrebbe applicarsi sia all'archivio attivo che a qualsiasi archivio di backup. Poiché possono essere utilizzati metodi diversi, è possibile prevedere misurazioni diverse.

Il livello di protezione deve essere commisurato al livello di rischio massimo per l'intero sistema.

USABILITÀ

L'usabilità si concentra sulle autenticazioni **uomo-macchina** *ed è relativamente nuova per i metodi di autenticazione.*

Di fronte a compiti difficili o impegnativi per soddisfare i requisiti di sicurezza, gli utenti spesso utilizzano strategie di coping che possono indebolire la sicurezza.

Gli sviluppatori e gli implementatori tentano di affrontare i limiti delle capacità umane attraverso le scelte e le politiche del meccanismo di autenticazione.

Un più stretto allineamento delle barriere di sicurezza al flusso di lavoro renderà più facile per gli utenti supportare e adottare i requisiti operativi imposti.

La misurazione dell'usabilità di un flusso di processo che contiene l'autenticazione è più rappresentativa di ciò che l'utente deve affrontare nel proprio ambiente.

Maggiore è la pressione del tempo, dell'offuscamento o dell'accuratezza che grava sull'utente durante l'autenticazione, maggiore è la possibilità di errore.

Se è possibile progettare l'autenticazione in modo che sia allineata con il lavoro e non l'ostacolo da superare per fare il lavoro, c'è un maggior grado di usabilità.

L'usabilità viene spesso valutata in base alla misura in cui gli utenti possono raggiungere obiettivi specifici con efficacia, efficienza e soddisfazione in uno specifico contesto di utilizzo.

Ad oggi, la maggior parte del lavoro nella valutazione dell'usabilità dell'autenticazione ha utilizzato uno standard che affronta l'usabilità dei display video, ISO 9241-11.

ESSERE **EFFICACI** SIGNIFICA FARE LE COSE GIUSTE; ESSERE **EFFICIENTI** SIGNIFICA FARE GIUSTE LE COSE**.**

EFFICACIA

L'efficacia è una misura dell'accuratezza e della completezza con cui gli utenti raggiungono obiettivi specifici.

Questa misurazione è spesso ottenuta collezionando errori dell'operatore, come errori di battitura, inserimento di carte al contrario o errori biometrici dovuti alle abitudini dell'utente.

Ulteriori misure potrebbero includere la disponibilità di ausili, come procedure e aspettative, utilizzo di casseforti per password o implementazioni single sign-on.

EFFICIENZA

L'efficienza è misurata come le risorse spese in relazione all'accuratezza e completezza con cui gli utenti raggiungono gli obiettivi.

La memorizzazione di password, le password scritte e il riutilizzo delle password sono esempi che influiscono sull'efficienza dell'autenticazione.

Il livello di impegno di Bitcoin per elaborare la blockchain è un esempio in cui l'efficienza è compromessa per aumentare la sicurezza.

SODDISFAZIONE

La soddisfazione è un obiettivo per raggiungere la libertà dal disagio e atteggiamenti positivi nei confronti dell'uso del prodotto.

La misurazione della soddisfazione è una misurazione qualitativa e, come tale, è più soggettiva.

Può essere meno affidabile dell'efficacia o dell'efficienza nel processo decisionale, ma è una misura importante della volontà dell'utente di supportare l'autenticazione.

7. VALUTAZIONE DEL RISCHIO (RISK ASSESSMENT - RA)

SCOPO DELLA VALUTAZIONE DEL RISCHIO (RISK ASSESSMENT)

Come introdotto nella Guida del NIST per la conduzione delle valutazioni dei rischi (NIST 800-30):

La valutazione del rischio è una delle componenti fondamentali di un processo di gestione del rischio organizzativo...

> Lo scopo delle valutazioni del rischio è informare i decisori e supportare le risposte al rischio identificando:
>
> (i) minacce rilevanti alle organizzazioni o minacce dirette attraverso organizzazioni contro altre organizzazioni;
>
> (ii) vulnerabilità sia interne che esterne alle organizzazioni;
>
> (iii) impatto (vale a dire, danno) alle organizzazioni che può verificarsi dato il potenziale di minacce che sfruttano le vulnerabilità; e
>
> (iv) probabilità che si verifichi un danno.

VALUTAZIONE DELLE MINACCE (THREAT ASSESSMENT)

[Rif.: NIST SP 800-160 Vol.1]

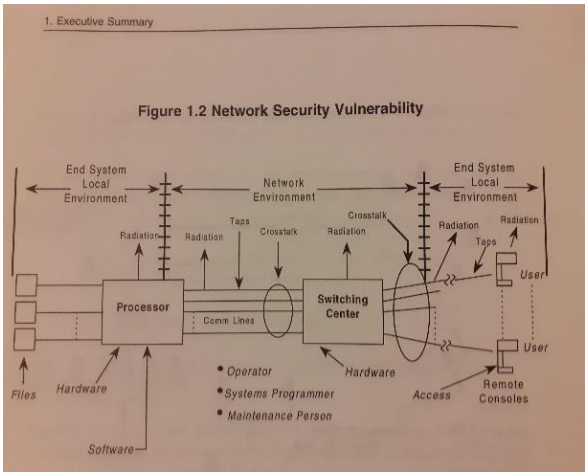
> *«Valutazione della misura dell'effetto reale o potenziale di una minaccia al sistema.»*
> *Nota: la valutazione della minaccia può includere l'identificazione e la descrizione della natura della minaccia.*

CHE COSA È UNA **MINACCIA**

NIST SP 800-30 la definisce come:

> *«Qualsiasi circostanza o evento che potrebbe avere un impatto negativo su operazioni organizzative e beni, individui, altre organizzazioni o nazione attraverso un sistema di informazione tramite accesso non autorizzato, distruzione, divulgazione o modifica di informazioni e/o negazione del servizio»*

Tratto da: «Computer Technology Research Corp. – Enterprisewide Network Security – Effective Implementation and International Standard - ed. 1994»



Un malintenzionato può ***attaccare qualsiasi dispositivo*** *collegato ad una rete e, indirettamente, anche un dispositivo non connesso (tramite USB, ecc.)*

Gli attacchi avvengono ai ***Dispositivi fisici****: computer, cellulari, processi produttivi, autovetture, apparati rete, domestici, POS, ATM, ecc.*

E alle loro

Applicazioni*: finanziarie (certificati TLS, ATM, POS, CC, ecc.), produzione, posta, cloud, social, ecc.*

COME*?*

Agendo sui Dati o sul Sw residenti nella ***Memoria Centrale*** *del dispositivo e nella* ***Storage (Memoria Periferica)*** *ad esso collegato*

IDENTIFICAZIONE DELLE MINACCE E CALCOLO DEI RISCHI

[Rif.: 1) WP 248 rev.01" ai fini del regolamento (UE) 2016/679; 2) ISO/IEC 27005:2018]

Obiettivo: identificare le minacce sia per i soggetti interessati sia per le risorse fisiche e logiche derivanti dal programma, dal sistema informatico o da un processo.

Risultato atteso: identificazione delle minacce e calcolo dei rischi per la privacy, per i dati non personali, per le risorse fisiche (HW, SO, varie componenti dell'infrastruttura).

Guida Implementazione

- *Le minacce per la privacy includono, ma non sono limitati a:*
  - ✓ *accesso non autorizzato al PII (perdita di riservatezza);*
  - ✓ *modifica non autorizzata del PII (perdita di integrità);*
  - ✓ *smarrimento, il furto o la rimozione non autorizzata del PII (perdita di disponibilità).*
- *È possibile prendere in considerazione altri aspetti come i seguenti.*
  - ✓ *eccessiva raccolta di PII (perdita del controllo operativo);*
  - ✓ *collegamento non autorizzato o improprio del PII;*
  - ✓ *informazioni insufficienti per quanto riguarda lo scopo per l'elaborazione del PII (Jack di trasparenza);*
  - ✓ *mancata considerazione i diritti dei principali PII (ad esempio la perdita del diritto di accesso);*
  - ✓ *trattamento dei PII senza la conoscenza o il consenso dei principali PII (a meno che tale trattamento sia previsto dalla pertinente normativa o regolamento);*
  - ✓ *condivisione o riproposizione PII con terze parti senza il consenso del principale PII; e inutilmente prolungata ritenzione del PII.*
- *Gli scenari che coinvolgono l'uso improprio e/o abuso, così come disturbi tecnici o ambientali, devono essere considerati come potenziali minacce.*
- *Ovunque giustificabile, il responsabile per lo svolgimento di una VdI dovrebbe fare uno sforzo per ottenere dalle parti interessate il sostegno per l'identificazione dei rischi.*

Minacce generiche

Le attività di supporto (su cui il PII fanno affidamento) sono in genere le seguenti:

1. *Utente fornito di hardware e software, come smartphone, tablet, software del browser Internet sul computer di casa, Internet TV, ecc.;*
2. *Hardware: computer, relè di comunicazione, drive USB, hard disk, ecc.;*
3. *Software: sistemi operativi, la messaggistica, database, applicazioni aziendali, ecc.; canali informatici: via cavo, wireless, fibra ottica, ecc.;*
4. *Individui: gli utenti, amministratori, top management, ecc.; documenti cartacei: stampa, fotocopia, ecc.;*
5. *Canali di trasmissione della carta: mail, flusso di lavoro, etc.*

Le azioni su tali attività di supporto (che le fonti di rischio possono fare, volontaria o meno) sono in genere il seguente:

1. USO ANOMALO/FUNZIONE DI SCORRIMENTO*: le attività di supporto vengono deviate dal loro contesto destinazione d'uso senza essere alterati o danneggiati;*
2. DANNI*: sostenere le attività sono parzialmente o completamente danneggiato; spionaggio: sostenere le attività sono osservati senza subire danni;*
3. PERDITA*: le attività di supporto vengono persi, rubati, venduti o ceduti, quindi è più possibile esercitare i diritti adeguati;*

4. MODIFICA/CAMBIAMENTO*: le attività di sostegno si trasformano;*

5. SOVRACCARICO/LIMITI DI FUNZIONAMENTO SUPERATO*: le attività di supporto sono sovraccarichi, eccessivamente sfruttati o utilizzati in condizioni di non permettere loro di funzionare correttamente.*

TIPI DI MINACCE

[Rif.: ISO/IEC 27005:2018]

Le minacce possono essere:

1. ***D** (deliberata o intenzionale);*
2. ***A** (accidentale);*
3. ***E** (ambientale o naturale).*

ESEMPI DI MINACCE

[Rif.: ISO/IEC 27005:2018 International Standard, Information Technology - Security techniques - Information Security Management]

Particolare attenzione dovrebbe essere prestata alle origini di minaccia umana (D, Deliberata).

ORIGIN OF THREAT	MOTIVATION	POSSIBLE CONSEQUENCES
Hacker, cracker	Challenge Ego Rebellion Status Money	– Hacking – Social engineering – System intrusion, break-ins – Unauthorized system access
Computer criminal	Destruction of information Illegal information disclosure Monetary gain Unauthorized data alteration	– Computer crime (e.g. cyber stalking) – Fraudulent act (e.g. replay, impersonation, interception) – Information bribery – Spoofing – System intrusion
Terrorist	Blackmail Destruction Exploitation Revenge Political gain Media coverage	– Bomb/terrorism – Information warfare – System attack (e.g. distributed denial of service) – System penetration – System tampering
Industrial espionage (Intelligence, companies, foreigngovernments, othergovernmentinterests)	Competitive advantage Economic espionage	– Defence advantage – Political advantage – Economic exploitation – Information theft – Intrusion on personal privacy – Social engineering – System penetration – Unauthorized system access (access to classified, proprietary, and/or technology-related information)
Insiders (poorly trained, disgruntled, malicious, negligent, dishonest, orterminatedemployees)	Curiosity Ego Intelligence Monetary gain Revenge Unintentional errors and omissions (e.g. data entry error, programming error)	– Assault on an employee – Blackmail – Browsing of proprietary information – Computer abuse – Fraud and theft – Information bribery – Input of falsified, corrupted data – Interception – Malicious code (e.g. virus, logic bomb, Trojan horse) – Sale of personal information – System bugs – System intrusion – System sabotage – Unauthorized system access

TABELLA «MINACCE GENERALI SUL PERSONALLY IDENTIFIABLE INFORMATION (PII)»

[Rif.: ISO/IEC 29134]

Minaccia	Descrizione Minaccia
Sparizioni di PII	*1. Conservazione dei file personali; uso personale, ecc.*
	2. Inondazioni, incendi, atti di vandalismo, danni da usura naturale, stoccaggio malfunzionamento del dispositivo, ecc.
	3. Furto di un computer portatile o un cellulare; disposizione di un dispositivo o hardware, etc.
	4. Aggiunta di hardware incompatibile con conseguente malfunzionamento; rimozione di componenti essenziali per il buon funzionamento del sistema, etc.
	5. Mobile contenitore pieno; interruzione di corrente; capacità di trasformazione Sovraccarico; surriscaldamento; temperature eccessive, etc.
	6. Cancellazione dei dati; utilizzo di software contraffatto o copiato; errori dell'operatore che cancellano i dati, etc.
	7. Cancellazione di codici eseguibili in esecuzione o di sorgenti; bomba logica, etc.

	8. Mancato rinnovo della licenza per il software utilizzato per accedere ai dati, etc.
	9. Errori durante gli aggiornamenti, configurazione o manutenzione; infezione da malware; sostituzione di componenti, etc.
	10. Superamento della dimensione del database; iniezione di dati al di fuori del normale intervallo di valori, etc.
	11. Taglio cablaggio, scarsa ricezione WiFi, etc.
	12. Furto di cavi in rame, etc.
	13. Uso improprio della larghezza di banda; scaricamento non autorizzato; perdita di connessione a Internet, etc.
	14. Infortunio sul lavoro; malattia professionale; altre lesioni o malattie; morte; disturbo neurologico, psicologico o psichiatrico, etc.
	15. Riassegnazione; risoluzione del contratto o il licenziamento; acquisizione di tutta o parte dell'organizzazione, etc.
	16. Elevato carico di lavoro, stress o variazioni negative delle condizioni di lavoro; assegnazione a dipendenti di attività al di fuori delle loro capacità; cattivo utilizzo di competenze, etc.
	17. Invecchiamento di documenti archiviati; file bruciati durante un incendio, etc.
	18. Furto di documenti; Perdita di file durante un trasferimento o una copia; disposizione, etc.
	19. Cancellazione graduale nel tempo; cancellazione volontaria di porzioni di un documento, etc.
	20. Fine flusso di lavoro a seguito di una riorganizzazione; mancata consegna della posta per uno sciopero, etc.
	21. Eliminazione di un processo a seguito di una riorganizzazione; perdita di un documento da società di trasporto, etc.
	22. Cambiamento delle modalità di spedizione della posta. Riorganizzazione dei Canali di trasmissione della carta; cambiamento della lingua di lavoro, etc.
	23. Sovraccarico di mail; processo di convalida oberato, etc.

TABELLA «RELAZIONE ASSET – AZIONI – MINACCE»

[Rif.: ISO/IEC 29134]

ASSET	AZIONI	MINACCIA	DESCRIZIONE MINACCIA
HW	*Uso anomalo*	*Sparizioni di PII*	*Conservazione dei file personali; uso personale, ecc.*
	Uso anomalo	*Accesso illegittimo al PII*	*Utilizzo di unità flash USB o dischi che sono mal si adatta alla sensibilità delle informazioni; l'uso o il trasporto di hardware sensibile per fini personali, ecc.*
	Danno	*Sparizioni di PII*	*Inondazioni, incendi, atti di vandalismo, danni da usura naturale, stoccaggio malfunzionamento del dispositivo, ecc.*
	Spionaggio	*Accesso illegittimo al PII*	*Guardando la schermata di una persona a loro insaputa mentre sul treno; scattare una foto di uno schermo; geolocalizzazione di hardware; telerilevamento di segnali elettromagnetici, etc.*
	Perdita	*Sparizioni di PII*	*Furto di un computer portatile o un cellulare; disposizione di un dispositivo o hardware, etc.*
		Accesso illegittimo al PII	*Furto di un computer portatile da una camera d'albergo; furto di un cellulare professionale un borseggiatore; recupero di un dispositivo di memorizzazione scartato o hardware; perdita di un dispositivo di memorizzazione elettronica, etc.*
	Modifica	*Sparizioni di PII*	*Aggiunta di hardware incompatibile con conseguente malfunzionamento; rimozione di componenti essenziali per il buon funzionamento del sistema, etc.*
		Accesso illegittimo al PII	*Monitoraggio da un keylogger basato su hardware; rimozione di componenti hardware; collegamento di dispositivi (come unità flash USB) per lanciare un sistema operativo o di recuperare dati, etc.*
		Cambiamenti indesiderati nel PII	*Aggiunta di hardware incompatibile con conseguente malfunzionamento; rimozione di componenti essenziali per il corretto funzionamento di un'applicazione, etc.*

	Sovraccarico	*Sparizioni di PII*	*Mobile contenitore pieno; interruzione di corrente; capacità di trasformazione Sovraccarico; surriscaldamento; temperature eccessive, etc.*
	Perdita del disco rigido	*Accesso illegittimo al PII*	*Errati accordi di smaltimento o di manutenzione può causare accessi non autorizzati PII.*
SW	*Uso anomalo*	*Sparizioni di PII*	*Cancellazione dei dati; utilizzo di software contraffatto o copiato; errori dell'operatore che cancellano i dati, etc.*
		Accesso illegittimo al PII	*Scansione dei contenuti; illegittimo controllo incrociato dei dati; innalzamento dei privilegi, cancellazione delle tracce d'uso; l'invio dello spam attraverso un programma di posta elettronica; abuso di funzioni di rete, etc.*
		Cambiamenti indesiderati nel PII	*Modifica indesiderata ai dati nei database; la cancellazione di file necessari per il software per funzionare correttamente; errori dell'operatore che modificano i dati, etc.*
	Danno	*Sparizioni di PII*	*Cancellazione di codici eseguibili in esecuzione o di sorgenti; bomba logica, etc.*
	Spionaggio	*Accesso illegittimo al PII*	*Scansione di indirizzi di rete e porte; raccolta dati di configurazione; analisi dei codici sorgente al fine di individuare i difetti sfruttabili; test di come database rispondono alle query dannosi, etc.*
		Accesso illegittimo al PII	*Scansione di indirizzi di rete e porte, attaccando vulnerabilità in ascolto, analisi, reporting o porte dei broker e servizi.*
	Perdita	*Sparizioni di PII*	*Mancato rinnovo della licenza per il software utilizzato per accedere ai dati, etc.*

TIPOLOGIE DI SOFTWARE MALEVOLO (MALWARE - MALICIOUS SOFTWARE)

[Rif. https://it.wikipedia.org/wiki/Malware#Classificazione]

***MALWARE** (significa letteralmente software malintenzionato, ma di solito tradotto come software dannoso), nella sicurezza informatica, indica un qualsiasi programma informatico usato per disturbare le operazioni svolte da un utente di un computer.*

Termine coniato nel 1990 da Yisrael Radai, precedentemente veniva chiamato virus per computer; in italiano viene anche comunemente chiamato codice maligno.

- *Virus: sono parti di codice che si diffondono copiandosi all'interno di altri programmi, o in una particolare sezione del disco fisso, in modo da essere eseguiti ogni volta che il file infetto viene aperto. Si trasmettono da un computer a un altro tramite lo spostamento di file infetti ad opera degli utenti.*
- *Worm: questi malware non hanno bisogno di infettare altri file per diffondersi, perché modificano il sistema operativo della macchina ospite in modo da essere eseguiti automaticamente e tentare di replicarsi sfruttando per lo più Internet. Per indurre gli utenti ad eseguirli utilizzano tecniche di ingegneria sociale, oppure sfruttano dei difetti (Bug) di alcuni programmi per diffondersi automaticamente. Il loro scopo è rallentare il sistema con operazioni inutili o dannose.*
- *Trojan horse: software che oltre ad avere delle funzionalità "lecite", utili per indurre l'utente ad utilizzarli, contengono istruzioni dannose che vengono eseguite all'insaputa dell'utilizzatore. Non possiedono funzioni di auto-replicazione, quindi per diffondersi devono essere consapevolmente inviati alla vittima. Il nome deriva dal famoso cavallo di Troia.*
- *Backdoor: letteralmente "porta sul retro" o secondaria/alternativa. Sono dei programmi che consentono un accesso non autorizzato al sistema su cui sono in esecuzione. Tipicamente si diffondono in abbinamento ad un trojan o ad un worm, oppure costituiscono una forma di accesso lecita di emergenza ad un sistema, inserita per permettere ad esempio il recupero di una password dimenticata.*
- *Spyware: software che vengono usati per raccogliere informazioni dal sistema su cui sono installati e per trasmetterle ad un destinatario interessato.*
- *Dialer: questi programmi si occupano di gestire la connessione ad Internet tramite la normale linea telefonica. Sono malware quando vengono utilizzati in modo illecito, modificando il numero telefonico*

chiamato dalla connessione predefinita con uno a tariffazione speciale, allo scopo di trarne illecito profitto all'insaputa dell'utente.

- *Hijacker: questi programmi si appropriano di applicazioni di navigazione in rete (soprattutto browser) e causano l'apertura automatica di pagine web indesiderate.*
- *Rootkit: i rootkit solitamente sono composti da un driver e a volte, da copie modificate di programmi normalmente presenti nel sistema. I rootkit non sono dannosi in sé, ma hanno la funzione di nascondere, sia all'utente che a programmi tipo antivirus, la presenza di particolari file o impostazioni del sistema. Vengono quindi utilizzati per mascherare spyware e trojan.*
- *Scareware: non sono altro che porte di accesso che si nascondono sui manifesti pubblicitari e installano altri malware e spesso c'è il pericolo che facciano installare malware che si fingono antivirus tipo il famoso "rogue antispyware".*
- *Rabbit: programmi che esauriscono le risorse del computer creando copie di sé stessi (in memoria o su disco) a grande velocità.*
- *Adware: programmi che presentano all'utente messaggi pubblicitari durante l'uso, a fronte di un prezzo ridotto o nullo. Possono causare danni quali rallentamenti del PC e rischi per la privacy in quanto comunicano le abitudini di navigazione ad un server remoto.*
- *Malvertising: Malicious Advertising, sono degli attacchi che originano dalle pubblicità delle pagine web.*
- *File batch: hanno estensione ".bat". I file batch non sono veri e propri malware, ma solo semplici File di testo interpretati da Prompt dei comandi di Microsoft Windows. In base ai comandi imposti dall'utente, il sistema li interpreta come "azioni da eseguire", e se per caso viene imposto di formattare il computer, il file esegue l'operazione imposta, perché eseguire i file inoltrati al processore è un'operazione di routine. Questo rende i file batch pericolosi. I file batch sono spesso utilizzati nel ciberbullismo.*
- *Rogue Antispyware: malware che si finge un programma per la sicurezza del PC, spingendo gli utenti ad acquistare una licenza del programma.*
- *Ransomware Virus che cripta tutti i dati presenti su un disco, secondo una chiave di cifratura complessa; poi, per ottenerla e decrittografare il computer, bisogna pagare il cracker che ha infettato il pc e quindi ottenere la chiave di cifratura per "tradurre" i dati.*
- *Keylogger: programmi in grado di registrare tutto ciò che un utente digita su una tastiera o che copia e incolla rendendo così possibile il furto di password o di dati che potrebbero interessare qualcun altro. Generalmente i keylogger vengono installati sul computer dai trojan o dai worm oppure viene installato nel pc attraverso l'accesso remoto. Esistono anche Keylogger hw che possono essere installati dalla rete Internet inviano informazioni al malintenzionato quali password, email, ecc.*
- *"A comando": cioè vengono attivati secondo le volontà del cracker nel momento che ritiene opportuno.*
- *"Automatici": che si dividono in altre due sottocategorie:*
  - *"Da esecuzione", cioè vengono eseguiti e quindi si attivano quando l'utente li avvia;*
  - *"Da avvio", cioè si attivano quando si spegne/accende il device.*
- *Bomba logica: è un tipo di malware che "esplode" ovvero fa sentire i suoi effetti maligni al verificarsi di determinate condizioni o stati del PC fissati dal cracker stesso.*
- *Bomba a decompressione: è un file che si presenta come un file compresso. Deve essere l'utente ad eseguirlo. All'apparenza sembra un innocuo file da pochi Kilobyte ma, appena aperto, si espande fino a diventare un file di circa quattro Petabyte, occupando quindi tutto lo spazio su disco rigido.*
- *Packers: è l'abbreviazione di «runtime packer» o «archivi autoestraenti». Sw che si decomprime in memoria quando viene eseguito il «file compresso». Questa tecnica è anche chiamata «compressione eseguibile».*
- *Crypters: tecnica di offuscamento. L'offuscamento viene spesso utilizzato anche negli script, come Javascript e Vbscripts. La maggior parte dei Crypters non solo crittografa il file ma il sw Crypters offre all'utente molte altre opzioni per rendere l'eseguibile nascosto il più difficile da rilevare. Obiettivo finale per gli autori di malware è FUD (Fully Undetectable), cioè essere in grado di passare inosservato.*

***DATA BREACH**, è la violazione dei dati personali oppure un disservizio (Resilienza=BC o DR) ovvero la violazione della sicurezza.*

Questa violazione, accidentale o dolosa e illecita, se comporta uno dei seguenti casi:

1. *la perdita definitiva del dato personale;*
2. *la distruzione (con possibilità di recupero) del dato personale;*
3. *la modifica o alterazione del dato personale;*
4. *la divulgazione non autorizzata o l'accesso (leaking) ai dati personali trasmessi e conservati;*

in tali casi è necessaria la comunicazione al Garante per effetto degli art. 33 e 34 del Reg. UE 2016/679.

5. *Nel caso di un disservizio o interruzione della erogazione delle funzionalità di un sistema di elaborazioni dati aziendali si trattano procedure per la gestione della Business Continuity (BC) se parziale o circoscritto, di Disaster Recovery (DR) se disastroso.*

CALCOLO DEL RISCHIO (RISK ASSESSMENT)

[Rif.: 1) NIST SP 800-30; NIST SP 800-82

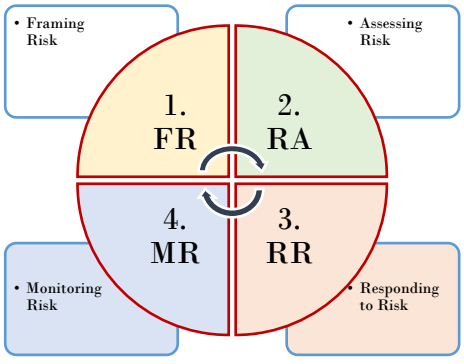
ASSIOMI

(A): *«Sono i rischi che contano, non le vulnerabilità»*

(B): *«La probabilità e l'impatto possono essere ridotti, il rischio non può essere eliminato»*

RISK MANAGEMENT PROCESS

- *Il Risk Assessment (RA) è una componente chiave di un'organizzazione olistica*
- *I processi di Risk Management (RM) includono:*
  1. *framing risk (focalizzarsi sui rischi);*
  2. *assessing risk (valutare il peso del rischio);*
  3. *responding to risk (adottare contromisure);*
  4. *monitoring risk (controllo continuo).*



INTERRELAZIONE DEI PROCESSI

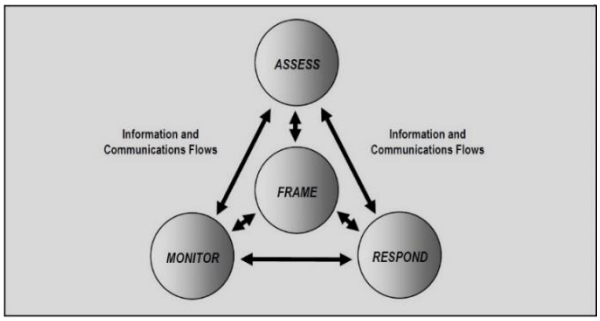
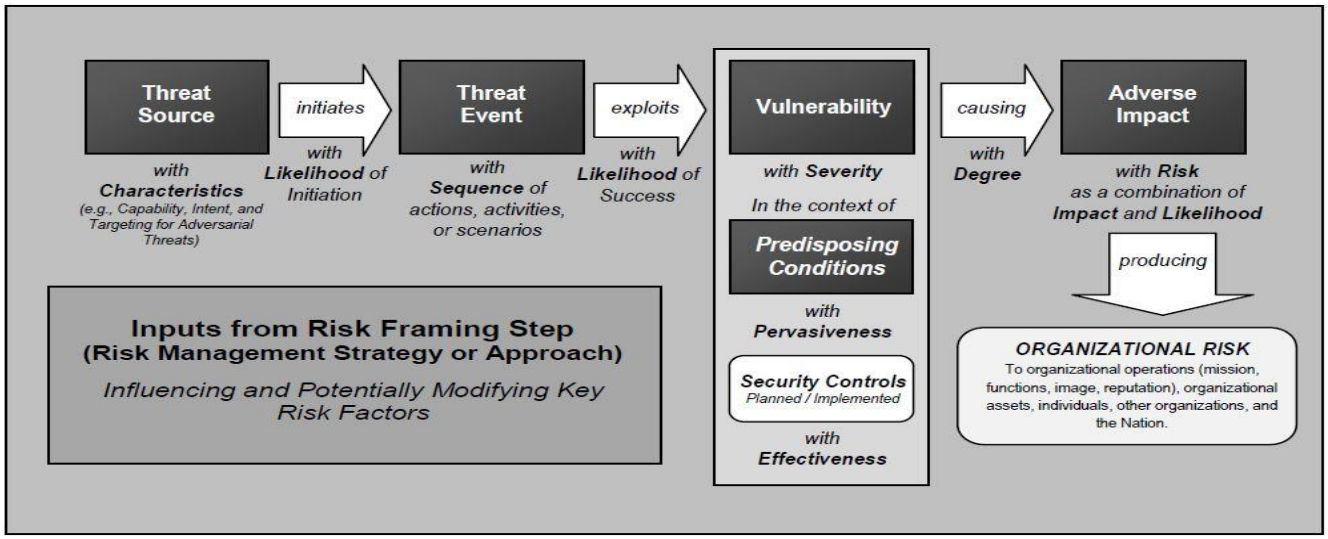


Table 2: Security Control Class, Family, and Identifier

RISK MANAGEMENT MODEL

La Fig.3 illustra un esempio un modello di gestione del rischio includendo la chiave dei fattori di rischio e la relazione tra i fattori. Ogni fattore di rischio è usato nel processo di Risk Assessment.

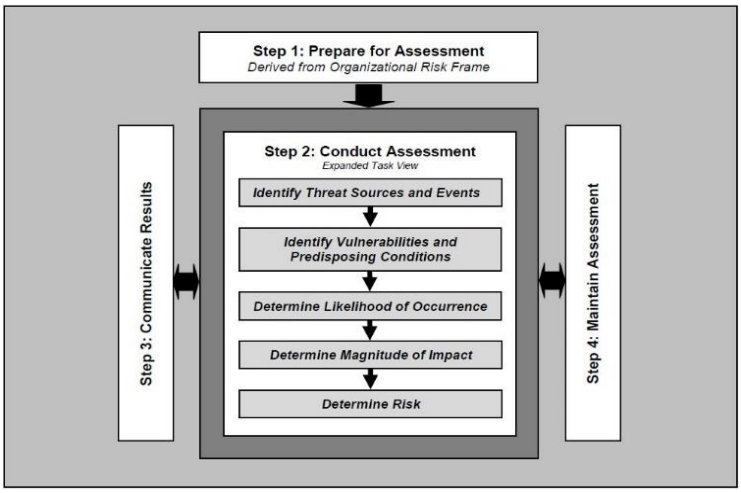
Figure 3: Generic Risk Model with Key Risk Factors



BASIC STEP OF RISK ASSESSMENT (RA) PROCESS

La Fig.5 illustra i passaggi di base del processo di valutazione del rischio e mette in evidenza i compiti specifici per condurre la valutazione.

Figure 5: Risk Assessment Process



COME STIMARE LA **GRAVITÀ** DELL'IMPATTO

Il livello di impatto delle conseguenze identificate dovrebbe essere stimato tenendo conto di queste conseguenze e dei controlli previsti o implementati.

1. TRASCURABILE (LOW)*: i principali PII o interessati non saranno influenzati oppure possono incontrare piccoli inconvenienti che potranno superare senza alcun problema (tempo è trascorso per le reimmerse informazioni, fastidi, irritazioni, etc.).*

2. LIMITATA (MEDIUM)*: i PII o interessati possono incontrare inconvenienti significativi o disagi che saranno in grado di superare nonostante qualche difficoltà (costi aggiuntivi, diniego di accesso ai servizi alle imprese, la paura, la mancanza di comprensione, stress, disturbi fisici minori, etc.).*

3. SIGNIFICATIVA (HIGH)*: i PII o interessati possono incontrare conseguenze significative che dovrebbero essere in grado di superare anche con gravi difficoltà (appropriazione indebita di fondi, liste nere dalle banche, danni materiali, perdita di posti di lavoro, invito a comparire, peggioramento delle condizioni di salute, ecc.).*

4. MASSIMA (VERY HIGH)*: i PII o interessati possono incontrare conseguenze significative o addirittura irreversibili tali da non poter essere superate (difficoltà finanziarie, come il debito inutilizzabili o incapacità di lavorare, disturbi psicologici o fisici a lungo termine, la morte, ecc.).*

COME STIMARE LA **PROBABILITÀ** DI UN EVENTO

Deve essere valutata la probabilità che ogni minaccia possa essere efficace, tenendo conto delle vulnerabilità delle attività di sostegno e della capacità della minaccia sfruttare le fonti di rischio: competenze, tempo a disposizione, le risorse finanziarie, la vicinanza al sistema di informazione, motivazione, senso di impunità, ecc.

1. TRASCURABILE (LOW)*: Effettuare una minaccia sfruttando le proprietà delle attività di supporto non sembra possibile per le fonti di rischio selezionati (per esempio il furto di documenti cartacei conservati in una stanza protetta da un lettore di badge e codice di accesso).*

2. LIMITATA (MEDIUM)*: Eseguire una minaccia sfruttando le proprietà di attività di supporto risulta difficile per le fonti di rischio selezionati (ad esempio furto di documenti cartacei memorizzati in una camera protetta da un lettore di badge).*

3. SIGNIFICATIVA (HIGH): Realizzare una minaccia sfruttando le proprietà delle attività di supporto sembra essere possibile per le fonti di rischio selezionati (per esempio il furto di documenti cartacei archiviati negli uffici che non è possibile accedere senza prima del check–in alla reception).

4. MASSIMA (VERY HIGH)*: Effettuare una minaccia sfruttando le proprietà delle attività di supporto sembra essere estremamente facile per le fonti di rischio selezionati (per esempio il furto di documenti cartacei archiviati in una hall).*

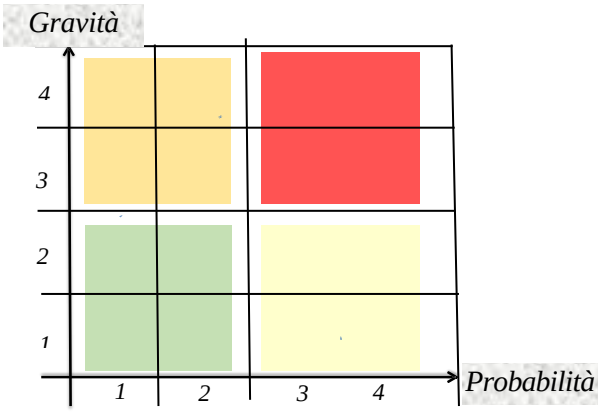
Mappa situazione del rischio

Esempio degli indicatori dell'impatto e della probabilità e della posizione del risultato all'interno di un quadrante.

Calcolo del rischio

Rischio = Gravità x Probabilità

LIVELLO DI IDENTIFICAZIONE	VALORE GRAVITÀ O IMPATTO
< 5	1. Trascurabile (Low)
= 5	2. Limitata (Medium)
= 6	3. Significativa (High)
> 6	4. Massima (Very high)
GESTIONE VULNERABILITÀ RISORSA	**VALORE PROBABILITÀ**
< 5	1. Trascurabile (Low)
= 5	2. Limitata (Medium)
= 6	3. Significativa (High)
> 6	4. Massima (Very high)



CLASSIFICAZIONE DEI RISCHI

Dopo aver identificato e valutato i rischi, il TdT deve specificare il modo in cui saranno gestiti questi rischi.

Il Titolare del sistema dovrebbe anche descrivere il modo in cui gli obiettivi di privacy sono state attuati o fornire una giustificazione se non lo sono stati.

Di seguito, sono proposte le possibili opzioni che possono essere adottate per gestire tali rischi:

1. RISCHIO MODIFICA*: il rischio è gestito attraverso l'individuazione e l'introduzione di ulteriori controlli, riducendo così il rischio a livelli accettabili;*

2. RISCHIO RITENZIONE*: il proprietario del sistema accetta il rischio così com'è, se soddisfa i criteri di accettazione, senza alcuna ulteriore azione;*

3. RISCHIO PREVENZIONE*: il responsabile del sistema decide non mettere l'applicazione nella produzione;*

4. CONDIVISIONE DEL RISCHIO*: il rischio è condiviso con un terzo, in grado di gestire il rischio identificato in modo più efficace e quindi ridurre il rischio a livelli accettabili.*

OPZIONI PER IL TRATTAMENTO DEL RISCHIO

Ci sono 4 opzioni disponibili per il trattamento del rischio:

1. RIDUZIONE (MODIFICATION)
2. MANTENIMENTO (RETENTION)
3. PREVENZIONE (AVOIDANCE)
4. TRASFERIMENTO (SHARING)

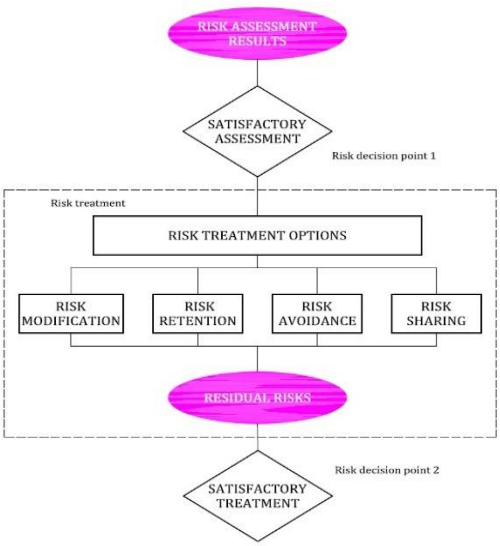


Figure 3 — The risk treatment activity

1. RIDUZIONE DEL RISCHIO

La riduzione del rischio può essere raggiunta attraverso la selezione di controlli appropriati. Dopo la selezione dei controlli potrebbe esserci qualche rischio residuo, che può essere definito inaccettabile o definito accettabile per l'organizzazione e per le parti interessate.

2. MANTENIMENTO DI RISCHIO

Se il livello di rischio soddisfa i criteri di rischio, non vi è alcuna necessità di attuare ulteriori controlli e il rischio può essere mantenuto.

3. PREVENZIONE DEI RISCHI

Quando i rischi individuati sono considerati troppo alti, può essere presa una decisione per evitare completamente il rischio, con il ritiro da un'attività pianificata o esistente o un insieme di attività, o la modifica delle condizioni in cui è gestita l'attività.

4. TRASFERIMENTO DEL RISCHIO

Il trasferimento del rischio implica:

- *la decisione di condividere determinati rischi con soggetti esterni;*
- *la creazione di nuovi rischi o modificare i rischi esistenti, pertanto, dovrà essere necessario il trattamento del rischio aggiuntivo.*

È possibile trasferire la responsabilità di gestire il rischio, ma non è normalmente possibile trasferire la responsabilità di un impatto
L'informativa sulla privacy è generalmente conosciuta come un insieme di regole che pubblicizzate specificano che i dati delle persone possono essere raccolti da un'organizzazione, come saranno utilizzati e se saranno mantenuti all'interno di tale organizzazione o condivise o vendute ad altre organizzazioni

ULTERIORI PASSI

Ci sono 4 opzioni disponibili per il trattamento del rischio:

1. A14: DETERMINARE I CONTROLLI
2. A15: CREARE I PIANI DI TRATTAMENTO DEI RISCHI
3. A16: GESTIONE DEI RISCHI RESIDUI E

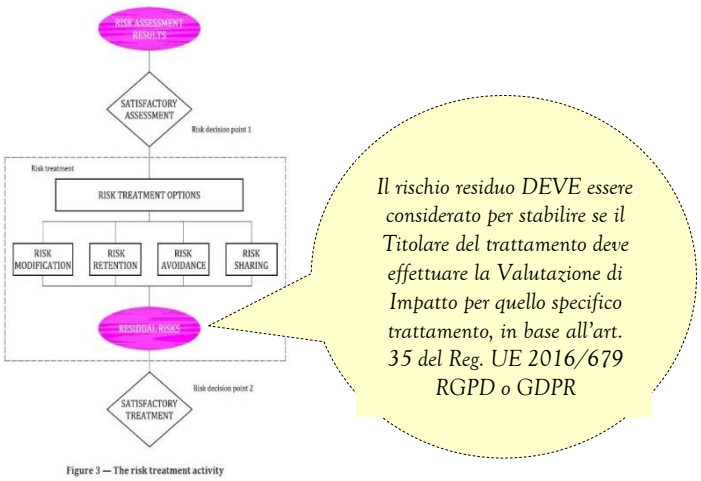


Figure 3 — The risk treatment activity

LIVELLO DI RISCHIO FINALE

Una volta che le minacce rilevanti sono state identificate, la loro quantificazione porterà a rischi connessi agli eventi temuti che devono essere considerati dal punto di vista del loro impatto/gravità e probabilità.

I rischi devono essere presentati in ordine di priorità.

L'ordine di priorità per i rischi identificati e quantificati dovrebbe portare la seguente dichiarazione.

RISCHI CON UN	ATTENZIONE SU MISURE DI
alto livello di gravità e alta probabilità	✓ *prevenzione* ✓ *protezione* ✓ *recupero*
alto livello di gravità e bassa probabilità	✓ *prevenzione*
basso livello di gravità e alta probabilità	✓ *recupero*
bassa gravità e probabilità	

In sintesi le misure di:

- **PREVENZIONE** *agiscono sulla* GRAVITÀ
- **RECUPERO** *agiscono sulla* PROBABILITÀ

In alcuni casi NON *si riesce né a* **PREVENIRE** *né a* **PROTEGGERE***: si può solo* RECUPERARE*!* **RESILIENZA**

VALUTAZIONE DELLA VULNERABILITÀ O VULNERABILITY ASSESSMENT (VA)

[Rif.: (Toward) A Secure System Engineering Methodology – Model Main and Model Appendices]

*Scopo di questa metodologia non è "***penetrare e riparare***" un sistema ma piuttosto scoprire i suoi punti deboli e le strategie di* ***progettazione*** *ragionevoli per creare sistemi più forti.*

DEFINIZIONE DI VULNERABILITY E VULNERABILITY ASSESSMENT

[Rif.: NIST SP 800-53A; NIST SP 800-160 Vol.1]

VULNERABILITY

> Weakness in an information system, system security procedures, internal controls or implementation that could be exploited or triggered by a threat source.

VULNERABILITY ASSESSMENT [COMMITTEE ON NATIONAL SECURITY SYSTEMS INSTRUCTION (CNSSI) 4009, ADAPTED]

> Systematic examination of an information system or product to:
>
> 1) **DETERMINE** the adequacy of security and privacy measures,
> 2) **IDENTIFY** security and privacy deficiencies [nota personale: ad esempio, attraverso l'uso di tecniche SAST, DAST, IAST, DAST, PT (def. par. 5.2 del NIST SP 800-115), BAS, RASP, WAF],
> 3) **PROVIDE** data from which to predict the effectiveness of proposed security and privacy measures and
> 4) **CONFIRM** the adequacy of such measures after implementation.

CARATTERIZZAZIONE DEGLI ATTACCHI E SCELTA DI CONTROMISURE RAZIONALI

Questa metodologia si basa su un modello di "albero degli attacchi".

Un albero di attacco è uno strumento di visualizzazione che enumera e soppesa diversi attacchi contro un sistema.

È composta da 5 passi.

P1. Creare alberi di attacco per il sistema.

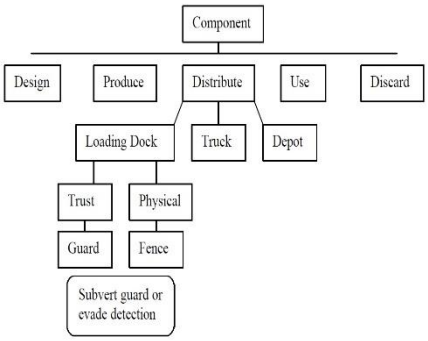
P2. Applicare pesi sulle foglie.

P3. Potare l'albero in modo che rimangano solo le foglie sfruttabili.

P4. Generare le contromisure corrispondenti.

P5. Ottimizzare le opzioni di contromisura.

Albero degli attacchi



P1. CREARE ALBERI DI ATTACCO PER IL SISTEMA

- ✓ *Creare l'albero di attacco replicando il lavoro di un avversario per trovare i punti deboli in un sistema.*
- ✓ *Il nodo radice del nostro albero è il componente che ha richiesto analisi.*
- ✓ *Per formare i nodi figlio, si decompone il nodo nel suo ciclo di vita.*
- ✓ *Ogni fase del ciclo di vita suddivisa in due categorie di accesso:*
  1) *la sicurezza fisica*
  2) *il modello di fiducia.*
- ✓ *Se appropriato, ogni nodo viene nuovamente decomposto in questo modo.*
- ✓ *L'analisi termina in una serie di foglie di vulnerabilità.*

P2. APPLICARE PESI SULLE FOGLIE

- ✓ *Per ogni foglia dell'albero di attacco, si assegna all'avversario valori qualitativi per rischio, accesso e costo.*

Esempio: un possibile nodo per i messaggi crittografati sarebbe la raccolta passiva e la decrittazione della forza bruta del testo cifrato. Il rischio di attacco è basso poiché viene eseguito in modo sicuro a distanza, l'accesso richiesto è basso e il costo dipende dalla forza dell'algoritmo crittografico.

P3. POTARE L'ALBERO IN MODO CHE RIMANGANO SOLO LE FOGLIE SFRUTTABILI

- ✓ *Si "pota" l'albero: le contromisure sono necessarie solo per quegli attacchi che soddisfano gli obiettivi di un avversario, corrispondono alle sue capacità e offrono un ritorno sufficiente.*

Esempio: se un determinato attacco richiede 2256 byte di memoria del computer, potrebbe essere eliminato in modo sicuro come al di là delle risorse di qualsiasi avversario. Se un altro attacco richiede l'accesso a un sistema di comunicazione chiuso, come una rete autonoma, potrebbe essere al di fuori della portata di alcuni avversari ma alla portata di altri.

P4. GENERARE LE CONTROMISURE CORRISPONDENTI

- ✓ *Si determinano le contromisure per i nodi più sfruttabili.*

P5. OTTIMIZZARE LE OPZIONI DI CONTROMISURA

- ✓ *Si classificano le contromisure in base ai suoi 5 attributi:*
  - *(1) costo per l'acquisto e l'esecuzione;*
  - *(2) facilità d'uso;*
  - *(3) compatibilità con la tecnologia sul posto e capacità di interoperare con altre comunità di interesse;*
  - *(4) il suo overhead sulle risorse di sistema;*
  - *(5) time to market o disponibilità.*

ESEMPI DI VULNERABILITÀ

[Rif.: ISO/IEC 27005:2018]

TYPES	EXAMPLES OF VULNERABILITIES	EXAMPLES OF THREATS
Hardware	Insufficient maintenance/faulty installation of storage media	Breach of information system maintainability
	Lack of periodic replacement schemes	Destruction of equipment or media
	Susceptibility to humidity, dust, soiling	Dust, corrosion, freezing
	Sensitivity to electromagnetic radiation	Electromagnetic radiation
	Lack of efficient configuration change control	Error in use
	Susceptibility to voltage variations	Loss of power supply
	Susceptibility to temperature variations	Meteorological phenomenon
	Unprotected storage	Theft of media or documents
	Lack of care at disposal	Theft of media or documents
	Uncontrolled copying	Theft of media or documents
Site	Inadequate or careless use of physical access control to buildings and rooms	Destruction of equipment or media
	Location in an area susceptible to flood	Flood
	Unstable power grid	Loss of power supply
	Lack of physical protection of the building, doors and windows	Theft of equipment
Network	Lack of proof of sending or receiving a message	Denial of actions
	Unprotected communication lines	Eavesdropping
	Unprotected sensitive traffic	Eavesdropping
	Poor joint cabling	Failure of telecommunication equipment
	Single point of failure	Failure of telecommunication equipment
	Lack of identification and authentication of sender and receiver	Forging of rights
	Insecure network architecture	Remote spying
	Transfer of passwords in clear	Remote spying
	Inadequate network management (resilience of routing)	Saturation of the information system
	Unprotected public network	Unauthorized use of equipment
TYPES	EXAMPLES OF VULNERABILITIES	EXAMPLES OF THREATS
Personnel	Absence of personnel	Breach of personnel availability
	Inadequate recruitment procedures	Destruction of equipment or media
	Insufficient security training	Error in use
	Incorrect use of software and hardware	Error in use
	Lack of security awareness	Error in use
	Lack of monitoring mechanisms	Illegal processing of data
	Unsupervised work by outside or cleaning staff	Theft of media or documents
	Lack of policies for the correct use of telecommunications media and messaging	Unauthorized use of equipment

DEFINIZIONE DI PENETRATION TESTING

[Rif.: NIST SP 800-160 Vol.1]

> A test methodology intended to circumvent the security function of a system.
>
> Note: Penetration testing may leverage system documentation (e.g., system design, source code, manuals) and is conducted within specific constraints. Some penetration test methods use brute force techniques.

APPLICAZIONE DELLE CONTROMISURE, VALUTAZIONE D'IMPATTO O GESTIONE DEL RISCHIO RESIDUO, CONTROLLI

Di seguito si forniscono delle sintesi delle tabelle contenenti i controlli finalizzati a verificare il livello di sicurezza del sistema.

L'elenco completo è disponibile nel capitolo «7.8. Questionari e Tabelle» del manuale indicato nel riferimento 21.

TABELLA «ELEMENTI DI SICUREZZA – DALL'ART. 2 DEL REG. DI ESECUZIONE (UE) 2018/151»

Recante modalità di applicazione della direttiva (UE) 2017/1148 per quanto riguarda l'ulteriore specificazione degli elementi che i fornitori di servizi digitali devono prendere in considerazione ai fini della gestione dei rischi collegati alla sicurezza delle reti e dei sistemi informativi e dei parametri per determinare l'eventuale impatto rilevante di un incidente.

Dal comma 1: Elementi per la sicurezza delle reti e dei sistemi informativi e del loro ambiente fisico
a) mappatura dei sistemi informativi e la definizione di una serie di politiche adeguate in materia di gestione della sicurezza informatica, comprese l'analisi dei rischi, le risorse umane, la sicurezza delle operazioni, l'architettura di sicurezza, la gestione del ciclo di vita dei dati e dei sistemi protetti e, se del caso, la crittografia e la sua gestione; *b) disponibilità di una serie di misure volte a proteggere le reti e i sistemi informativi dei fornitori di servizi digitali dai danni attraverso il ricorso a un approccio globale ai pericoli basato sui rischi, che affronti ad esempio gli errori di sistema, gli errori umani, gli atti dolosi o i fenomeni naturali;* *c) definizione e mantenimento di politiche adeguate al fine di assicurare l'accessibilità e, se del caso, la tracciabilità delle forniture critiche utilizzate nella prestazione dei servizi;*

TABELLA «ELEMENTI DI SICUREZZA – DALL'ART. 2 DEL REG. DI ESECUZIONE (UE) 2018/151»

Dal comma 1: Numero di utenti interessati da un incidente, in particolare gli utenti che dipendono dal servizio per la fornitura dei propri servizi
a) il numero di persone fisiche e giuridiche interessate con cui è stato concluso un contratto per la fornitura del servizio, oppure; *b) il numero di utenti interessati che hanno utilizzato il servizio in particolare in base ai precedenti dati sul traffico.*
Dal comma 2: Durata dell'incidente è il periodo tra la perturbazione della regolare prestazione del servizio in termini di disponibilità, autenticità, integrità o riservatezza e il momento del ripristino
Dal comma 3: Diffusione geografica relativamente all'area interessata dall'incidente, il fornitore di servizi digitali è in grado di stabilire se l'incidente influisce sulla fornitura dei suoi servizi in determinati Stati membri.
Dal comma 4: Perturbazione del funzionamento del servizio è misurata per una o più delle seguenti caratteristiche compromesse dall'incidente: disponibilità, autenticità, integrità o riservatezza dei dati o dei servizi correlati.
Dal comma 5: Portata dell'impatto sulle attività economiche e sociali, il fornitore di servizi digitali è in grado di dedurre, sulla base di indicazioni quali la natura delle sue relazioni contrattuali con il cliente o, se del caso, il numero potenziale di utenti interessati, se l'incidente ha causato importanti perdite materiali o immateriali per gli utenti, ad esempio in relazione alla salute e alla sicurezza o danni materiali.

TABELLA «IMPATTO RILEVANTE DI UN INCIDENTE – DALL'ART. 4 DEL REG. (UE) 2018/151»

- *Dal comma 1: Un incidente è considerato come avente un impatto rilevante se si verifica almeno una delle seguenti situazioni*

- ✓ *il servizio fornito da un fornitore di servizi digitali non è stato disponibile per oltre 5.000.000 di ore utente, dove per ore utente si intende il numero di utenti interessati nell'Unione per una durata di sessanta minuti;*
- ✓ *l'incidente ha provocato una perdita di integrità, autenticità o riservatezza dei dati conservati, trasmessi o trattati o dei relativi servizi offerti o accessibili tramite una rete e un sistema informativo del fornitore di servizi digitali che ha interessato oltre 100.000 utenti nell'Unione;*
- ✓ *l'incidente ha generato un rischio per la sicurezza pubblica, l'incolumità pubblica o in termini di perdite di vite umane;*
- ✓ *l'incidente ha provocato danni materiali superiori a 1.000.000 di EUR per almeno un utente nell'Unione.*

TABELLA ASSET

1. *HW - PC, Server, File; etc.*
2. *SW - Dati; Programmi di sistema o gestionali.*
3. *Computer channels - Cablaggio, Apparati di comunicazione Wi–Fi, router, switch, Hub, etc.*
4. *Risorse umane - Personale dipendente e non*
5. *Documenti cartacei – Documenti*
6. *Canali di trasmissione della carta - Mail, Corrieri, ecc.*

TABELLA AZIONI

1. *Danno*
2. *Spionaggio*
3. *Perdita*
4. *Modifica*
5. *Sovraccarico*
6. *Perdita del disco rigido*
7. *Uso anomalo*

TABELLA «ESEMPI DI LIVELLO D'IMPATTO O GRAVITÀ, IN BASE ALLA NATURA DEL PII»

[Rif.: NIST SP 800-122]

NATURA DEL PII (PERSONALLY IDENTIFIABLE INFORMATION – INFORMAZIONI PERSONALI)	LIVELLO DI IMPATTO
PII che sono accessibili al pubblico (ad esempio, negli elenchi telefonici, rubriche o elenchi di selezione)	*1*
PII che richiedono un interesse legittimo per l'accesso (ad esempio, i file di pubblico ristretto oi membri di una lista di distribuzione)	*2*
PII la cui divulgazione non autorizzata in grado di influenzare la reputazione del capitale PII (ad esempio, informazioni sul reddito, prestazioni sociali, tassa di proprietà o sanzioni)	*3*
PII la cui divulgazione non autorizzata, la modifica, la perdita o la distruzione può influenzare l'esistenza o la salute, la libertà e la vita del capitale PII (ad es. Informazioni sull'impegno ad una istituzione, una frase, recensioni del personale, dati sanitari, i debiti inutilizzabili, o se la PII principale è a rischio di diventare una vittima in un procedimento penale)	*4*

LISTA DELLE «CONTROMISURE GENERICHE» (SONO RIPORTATE LE PRIME 12 SU 39)

[Rif.: Smart Grid Task Force 2012-14 - Expert Group 2: Regulatory Recommendations for Privacy, Data Protection and Cyber-Security in the Smart Grid Environment]

#	CONTROMISURE	OBIETTIVI
1	Ridurre al minimo la quantità di dati personali	*Ridurre la gravità dei rischi limitando la quantità di dati personali a ciò che è strettamente necessario per raggiungere un obiettivo definito*
2	Gestione dei periodi di conservazione dei dati personali	*Ridurre la gravità dei rischi assicurando che i dati personali non siano conservati per più di quanto necessario*
3	Informare gli interessati	*Garantire che i soggetti siano informati*
4	Ottenere il consenso dei soggetti interessati	*Consentire agli interessati di effettuare una scelta gratuita, specifica e informata*
5	Gestione delle persone all'interno dell'organizzazione che hanno accesso legittimo	*Ridurre i rischi connessi alle persone all'interno dell'organizzazione (dipendenti, subappaltatori, insegnanti e visitatori) che hanno accesso legittimo ai dati personali*
6	Gestione dell'accesso legittimo di terzi ai dati personali	*Ridurre il rischio che l'accesso ai dati personali da parte di terzi possa compromettere le libertà civili delle persone interessate e la privacy*
7	Monitoraggio degli accessi logici	*Limitare i rischi degli accessi ai dati personali di persone non autorizzate*
8	Suddivisione dei dati personali	*Ridurre la possibilità che i dati possano essere correlati e che tale correlazione possa implicare una violazione su tutti i dati personali*
9	Cifrare i dati personali	*Rendere incomprensibili i dati personali a chiunque acceda senza autorizzazione*
10	Anonimizzare i dati personali	*Rimuovere le caratteristiche che permettano la identificazione dei dati personali*
11	Protezione degli archivi dei dati personali	*Definire tutte le procedure per la conservazione e la gestione degli archivi contenenti i dati personali*
12	Gestione delle violazioni dei dati personali	*Avere un'organizzazione in grado di rilevare e trattare incidenti che possano incidere sulle libertà civili e sulla privacy degli interessati*

CONTROLLI

IL CONTROLLO È UNA CONTROMISURA!

*Fare riferimento al Capitolo "**The Controls**" all'interno del manuale "**NIST SP 800-53**".*

Questa pubblicazione fornisce informazioni di base sul controllo della privacy e della sicurezza per il Governo federale USA.

Sono disponibili tre linee di base di controllo della sicurezza (una per ogni livello di impatto del sistema: basso impatto, impatto moderato e alto impatto), nonché una linea di base della privacy che viene applicata ai sistemi indipendentemente dal livello di impatto.

Oltre alle linee di base del controllo, questa pubblicazione fornisce indicazioni su misura e una serie di presupposti di lavoro che aiutano a guidare e informare il processo di selezione del controllo.

Infine, fornisce indicazioni sullo sviluppo di sovrapposizioni per facilitare la personalizzazione della linea di base di controllo per comunità di interesse, tecnologie e ambienti operativi specifici.

In questo manuale sono elencati i controlli necessari all'adozione delle misure di protezione dei sistemi, delle organizzazioni e della privacy; tali controlli sono progettati per facilitare la Gestione del Rischio (Risk Management) ed essere conformi alle leggi, alle policy, ecc.

*L'appendice "**C**" **Control Summary** fornisce il sommario, suddiviso per famiglia, dei controlli per la sicurezza e la privacy.*

Ulteriori integrazioni dei controlli sono disponibili nel manuale "NIST SP 800-172".

8. GESTIONE DELLE ATTIVITÀ CONTINUATIVE "ON GOING"

MONITORAGGIO

[Rif. NIST IR 8286]

Il 6° passo per la Gestione del Rischio, indicato nel NIST IR 8286, è: **il monitoraggio continuo affinché vi sia garanzia delle condizioni di rischio aziendale entro i livelli definiti di propensione al rischio.**

Inoltre, questo documento espone la tabella rappresentante un crosswalk (percorso trasversale) o mappatura dei processi per la Gestione del Rischio Aziendale (ERM) e la loro collocazione negli standard internazionali.

Questi standard, generalmente, includono tutti gli stessi approcci:

1) *identificare il contesto,*
2) *identificare i rischi,*
3) *analizzare il rischio,*
4) *stimare l'importanza del rischio,*
5) *determinare ed eseguire la risposta al rischio,*
6) *identificare e rispondere ai cambiamenti nel tempo.*

È bene utilizzare i processi indicati nel ERM Playbook (prima colonna) come guida alla gestione dei rischi della cybersecurity.

Table 1: Notional Crosswalk Among Selected ERM and Risk Management Frameworks

ERM Playbook	ISO 31000:2009		OMB A-123	GAO Green Book	NIST Risk Management Framework		
					SP 800-30 Rev. 1	SP 800-37 Rev. 2	SP 800-39
Identify the Context	Establish External Context (5.3.2), Establish Internal Context (5.3.3)		Establish Context	Define objectives and risk tolerances (6.01)	Preparing for the Risk Assessment (3.1)	Prepare (3.1)	Framing Risk (3.1)
Identify the Risks	Risk Assessment	Risk Identification (5.4.2)	Identify Risks	Identification of Risks (7.02)	Task 2-1: Identify and characterize threat sources of concern (3.2), Task 2-2: Identify potential threat events, threat sources (3.2), Task 2-3: Identify vulnerabilities/predisposing conditions (3.2)	Prepare (3.1), Task P-14, Risk Assessment - System, Risk Assessment Report (RAR) Assess (3.5)	
Analyze the Risks		Risk Analysis (5.4.3)	Analyze and Evaluate	Analysis of Risks (7.05)	Task 2-5: Determine the adverse impacts from threat events (3.2), Task 2-4: Determine the likelihood (3.2), Task 2-6: Determine the risk to the organization (3.2) Risk Assessment Report (Appendix K)		Assessing Risk (3.2)
Assess Impact		Calculate Level of Risk		Management estimates the significance of a risk, considering the magnitude of impact, likelihood of occurrence, and nature of the risk			
Assess Likelihood							
Prioritize Risks							
Calculate Exposure							
Plan and Execute Response Strategies		Risk Evaluation (5.4.4)	Develop Alter-natives	Response to Risks (7.08)	Task 3-1: Communicate Risk Assessment Results Task 3-2: Share Risk-Related Information (3.3) Also See 800-37 Rev. 2 See 800-39	Categorize (3.2), Select (3.3), and Implement (3.4)	Responding to Risk (3.3)
	Risk Treatment (5.5)		Respond to Risks			Implement (3.4), Authorize (3.6), Residual Risk reflected in POA&M	
Monitor, Evaluate, and Adjust	Monitoring and review (5.6)		Monitor and Review	Identification of Change (9.02)	Task 4-1: Conduct ongoing monitoring of the risk factors (3.4) Task 4-2: Update Risk Assessment	Monitor (3.7)	Monitoring Risk (3.4)
				Analysis of and Response to Change (9.04)			

INVENTORY AND VALUATION OF ASSETS

Sempre più spesso, molte delle risorse da cui dipende un'organizzazione non sono sotto il suo controllo diretto.

Le risorse tecniche esterne possono includere software basato su cloud o servizi di piattaforma, circuiti di telecomunicazione e monitoraggio video.

Il personale può includere la forza lavoro interna, fornitori di servizi esterni e partner di terze parti.

PLAN AND EXECUTE RISK RESPONSE STRATEGIES

La pianificazione e l'esecuzione delle risposte ai rischi è un'attività iterativa. La risposta selezionata per ogni rischio sarà informata dalla guida dei dirigenti in merito alla propensione al rischio e alla tolleranza al rischio; poiché le autorità di supervisione del rischio monitorano il successo di tali risposte, forniranno indicazioni finanziarie e di missione ai leader operativi per informare le future attività di gestione del rischio. In alcuni casi, la valutazione del rischio può portare alla decisione di intraprendere ulteriori analisi per confermare le stime o monitorare più da vicino i risultati.

APPLYING SECURITY CONTROLS TO REDUCE RISK EXPOSURE

Si consideri un'organizzazione che identifichi diversi rischi per la sicurezza informatica negativi ad alta esposizione, tra cui che pratiche di autenticazione inadeguate (ad esempio password deboli o riutilizzate) potrebbero consentire la divulgazione di informazioni finanziarie sensibili dei clienti e che i dipendenti del fornitore di software potrebbero ottenere un accesso non autorizzato e manomettere il dati finanziari.

L'organizzazione può applicare diversi controlli deterrenti (documentando gli identificatori di controllo applicati e qualsiasi nota applicabile nella colonna dei commenti del registro dei rischi), inclusi i banner di avvertimento e la minaccia di azione penale per tutti gli attori della minaccia che tentano intenzionalmente di ottenere un accesso non autorizzato.

I controlli preventivi includono l'applicazione di forti criteri di gestione delle identità e l'utilizzo di token di autenticazione a più fattori che aiutano a ridurre le vulnerabilità di autenticazione.

Il fornitore di software ha installato controlli di rilevamento che monitorano i log di accesso e avvisano il centro operativo per la sicurezza dell'organizzazione se il personale interno si connette al database del cliente senza necessità di accesso. Inoltre, il database finanziario è crittografato in modo da proteggere i suoi dati se il file system viene esfiltrato.

Per quanto riguarda la risposta positiva al rischio, si consideri l'esempio di un'organizzazione che abbia identificato il rischio positivo di significativi risparmi sui costi spostando un importante sistema di business finanziario in una soluzione cloud Software-as-a-Service (SaaS).

L'analisi del rischio ha determinato che l'opportunità sarebbe estremamente vantaggiosa per l'impresa.

Con questi controlli e metodi in atto e dopo averli valutati come efficaci, i rischi rimanenti possono essere analizzati per determinare l'impatto residuo, la probabilità e l'esposizione.

Se l'esposizione residua rientra nei livelli di tolleranza al rischio, le parti interessate possono procedere per ottenere i benefici dell'opportunità.

MONITOR, EVALUATE, AND ADJUST

Dalla prima comprensione del contesto interno/esterno alla discussione e autorizzazione della risposta al rischio, è necessario un dialogo continuo tra tutti gli stakeholder rilevanti.

Sebbene tali discussioni avvengano spesso all'interno di una determinata unità aziendale o organizzazione subordinata, l'impresa trarrà vantaggio da una comunicazione frequente e trasparente in merito alle opzioni di rischio, alle decisioni, ai cambiamenti e agli aggiustamenti.

I registri ei profili dei rischi per la sicurezza informatica in evoluzione forniscono un metodo formale per comunicare le conoscenze e le decisioni istituzionali riguardanti i rischi per la sicurezza informatica e il loro contributo all'ERM.

CONTINUOUS RISK MONITORING

Poiché i rischi per la sicurezza informatica e il loro impatto intrinseco su altri rischi cambiano frequentemente, le condizioni di rischio aziendale dovrebbero essere costantemente monitorate per garantire che rimangano entro livelli accettabili.

Ad esempio, tale monitoraggio potrebbe determinare quando i rischi di sicurezza informatica negativi per un sistema si stanno avvicinando al livello di tolleranza al rischio, innescando una revisione del rischio che potrebbe comportare una priorità più alta per il rischio e l'implementazione di ulteriori risposte al rischio.

Il monitoraggio del rischio trae vantaggio da una cultura positiva del rischio all'interno dell'azienda.

Una tale cultura porta a un approccio coeso e basato sul team al monitoraggio e alla gestione dei rischi.

Il sostegno a tale cultura include attività proattive, come evidenziato nella tabella seguente.

Ulteriori dettagli sono descritti nei seguenti manuali:

- *nel "Task S-5 Continuous Monitoring Strategy -System", all'interno del capitolo "3.3 Select", del manuale "NIST SP 800-37":*

  Task S-5 Continuous Monitoring Strategy - System*: Develop and implement a system-level strategy for monitoring control effectiveness that is consistent with and supplements the organizational continuous monitoring strategy. A continuous monitoring strategy for the system that reflects the organizational risk management strategy is developed.[Cybersecurity Framework: ID.GV; DE.CM]*

- *Capitolo "3.4 Monitoring Risk" del manuale "NIST SP 800-39".*

Table 5: Examples of Proactive Activities

Activity Example	Description
Cultural Risk Awareness	Encourage employees to look for cybersecurity risk issues before they become significant.
Risk Response Training	Train employees and partners on enterprise strategy, risk appetite, and selected risk responses.
Risk Management Performance	Discuss the impact of cybersecurity risk on every employee and partner, and why effective management of risks is an important part of everyone's job.
Risk Response Preparedness	Conduct exercises to provide practical and meaningful experience in recognizing, reporting, and responding to cybersecurity risk scenarios.
Risk Management Governance	Remind staff of organizational policies and procedures that are established to help improve risk awareness and response.
Risk Transparency	Enable an environment where employees and partners may openly and proactively report potential risk situations without fear of reprisals.

Le politiche e i processi dovrebbero specificare la frequenza e i metodi approvati per il monitoraggio, la valutazione dell'efficacia e l'adeguamento delle risposte al rischio.

Un elemento del monitoraggio del rischio è determinare e pubblicare ruoli di gestione del rischio responsabili in tutta l'azienda, inclusi quelli nelle organizzazioni.

Le relazioni tra queste entità dovrebbero essere comunicate chiaramente, ad esempio il modo in cui un comitato di rischio aziendale formale può essere informato da consigli di rischio o gruppi di lavoro subordinati.

Possono aiutare a garantire la comunicazione incrociata tra altri gruppi che supportano la gestione del rischio, come la gestione delle risorse umane, legale, di controllo e di conformità.

La Fase 6 RMF Monitor, tratta dal capitolo 2.4.3 del NIST SP 800-30, dice:

> *Le organizzazioni possono aggiornare le valutazioni del rischio su base continuativa utilizzando le informazioni relative alla sicurezza dai processi di monitoraggio continuo dell'organizzazione.*
>
> *Processi di monitoraggio continuo valutano:*
>
> *(i) l'efficacia dei controlli di sicurezza;*
>
> *(ii) modifiche ai sistemi informativi e agli ambienti operativi;*
>
> *(iii) conformità a legislazione, regolamenti, direttive, politiche, standard e linee guida federali.*
>
> *Man, mano che le valutazioni del rischio vengono aggiornate e perfezionate, le organizzazioni utilizzano i risultati per aggiornare la strategia di gestione del rischio, incorporando così le lezioni apprese nei processi di gestione del rischio, migliorando le risposte al rischio e costruendo una solida base di informazioni su minacce e vulnerabilità su misura per le missioni organizzative/funzioni aziendali.*

CIBERRESILIENZA

*Fare riferimento al Capitolo "**The Controls**" all'interno del manuale "**NIST SP 800-160 Vol.2 Developing Cyber Resilient Systems: A SSE Approach**".*

Vedi Parte Seconda, capitolo "Developing Cyber Resilient Systems".

POTENZIALI EFFETTI (QUATTORDICI) SUGLI EVENTI DELLA MINACCIA

PRINCIPIO DELLA RESILIENZA

Le soluzioni di resilienza informatica sono rilevanti solo se hanno qualche effetto sul rischio, in particolare riducendo la probabilità che si verifichino eventi di minaccia, la capacità degli eventi di minaccia di causare danni e l'estensione di tale danno.

Dal punto di vista della protezione di un sistema dalle minacce avversarie, si possono identificare 5 effetti desiderati di alto livello sull'avversario:

1. *Reindirizzare [Redirect (1)]*
2. *Precludere [Preclude (5)],*
3. *Impedire [Impede (9)],*
4. *Limitare [Limit (14)] ed*
5. *Esporre [Expose (17)].*

Questi effetti spesso sono troppo generici per facilitare la definizione di specifiche misure di efficacia; pertanto, vengono definite le seguenti classi di effetti più specifiche:

6. *impedire o scoraggiare [Deter (1), (2)], deviare [Divert (1), (3)] e ingannare [Deceive (1), (4)] o raggirare a supporto del reindirizzamento [Redirect (1)];*
7. *prevenire [Prevent], contrastare [Preempt (5), (7)] e rimuovere [Expunge (5), (6)] a sostegno di precludere [Preclude (5)];*
8. *contenere [Contain (9), (10)]), Degradare [Degrade (9), (11)], ritardare [Delay (9), (12)] ed esercitare [Exert (9), (13)] a sostegno di impedire [Impede (9)];*
9. *accorciare [Shorten (14), (15)] e recuperare [Recover] a supporto del limitare; e*
10. *rilevare [Detect (17), (18)], rivelare [Reveal (17), (20)] e verificare [Scrutinize (17), (19)] a supporto dell'esposizione [Expose (17)].*

PROPRIETÀ 1 DELLA RESILIENZA

1 - Quando si considera la ciberresilienza per il processo operativo, l'ingegneria della sicurezza dei sistemi garantisce che la strategia operativa includa aspetti della ciberresilienza.

2 - Gli aspetti della resilienza informatica della strategia operativa garantiscono che gli obiettivi aziendali o di missione possano essere raggiunti utilizzando le capacità di resilienza informatica del sistema in congiunzione con le capacità di altri sistemi con cui il sistema di interesse interagisce o da cui dipende e che i servizi di sicurezza del sistema sono resilienti.

PROPRIETÀ 2 DELLA RESILIENZA

Un modello di resilienza informatica è comportamentale e strutturale.

Un modello comportamentale di resilienza informatica rappresenta:

- ✓ *il comportamento di un sistema (a un dato livello architetturale o intervallo di livelli) per facilitare l'analisi degli effetti cibernetici di eventi avversi sui sistemi e sul comportamento del sistema;*
- ✓ *il comportamento del sistema rispetto ai requisiti di prestazione delle attività o della missione, comprese le prestazioni di sicurezza in una varietà di condizioni avverse;*
- ✓ *gli effetti delle soluzioni di resilienza informatica o delle linee d'azione.*

Un modello strutturale di ciberresilienza identifica dove e come all'interno di un'architettura di sistema sono implementate tecniche e approcci di ciberresilienza selezionati o sono applicati i principi di progettazione di ciberresilienza.

PARTE II: PROGETTAZIONE DELLA CYBERSECURITY

9. CONSIDERATIONS FOR A MULTIDISCIPLINARY APPROACH IN THE ENGINEERING OF TRUSTWORTHY SECURE SYSTEMS

[Rif. NIST SP 800-160 Vol.1]

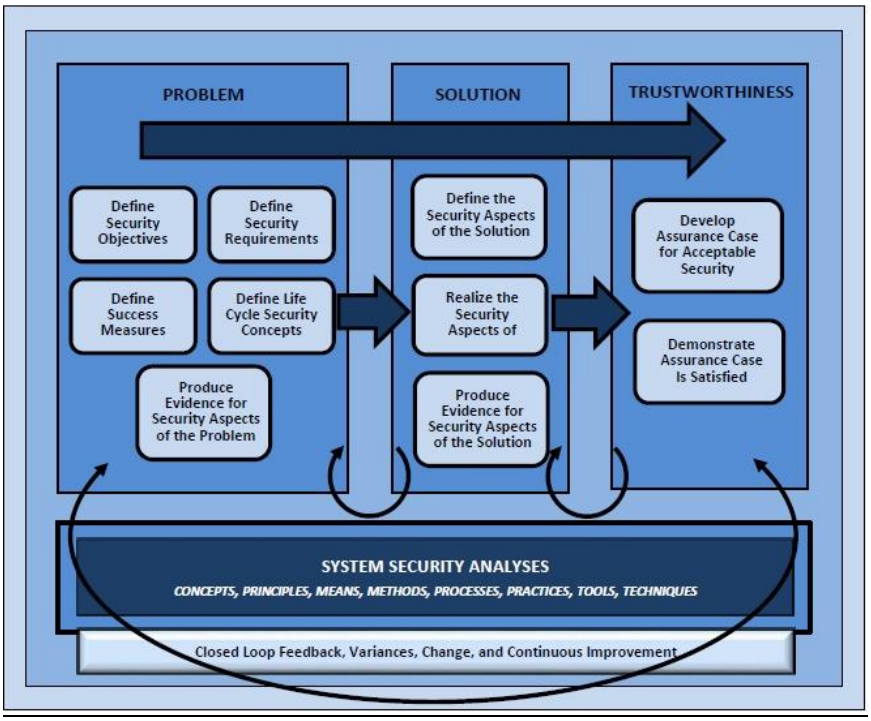


Figure 3: Systems Security Engineering Framework

Il framework definisce 3 contesti all'interno dei quali vengono condotte le attività di ingegneria della sicurezza dei sistemi.

Questi sono:

1st. ***PROBLEM***

2nd. ***SOLUTION***

3rd. ***TRUSTWORTHINESS***

Stabilire i tre contesti aiuta a garantire che l'ingegneria di un sistema sia guidata da una comprensione sufficientemente completa del problema articolata in una serie di obiettivi di sicurezza delle parti interessate che riflettono le esigenze di protezione e le preoccupazioni di sicurezza.

Inoltre, vi è un focus esplicito e una serie di attività per dimostrare la validità della soluzione nel fornire una sicurezza adeguata attraverso vincoli concorrenti e spesso contrastanti.

SYSTEMS SECURITY ENGINEERING FRAMEWORK – WHY IT MATTERS

*Stabilire i contesti di **PROBLEM, SOLUTION** e **TRUSTWORTHINESS** come componenti chiave di un framework di ingegneria della sicurezza dei sistemi garantisce che la sicurezza di un sistema si basi sul raggiungimento di una comprensione sufficientemente completa del problema come definito da una serie di obiettivi di sicurezza delle parti interessate, preoccupazioni di sicurezza, esigenze di protezione e requisiti di sicurezza.*

Questa comprensione è essenziale per sviluppare soluzioni di sicurezza efficaci, ovvero un sistema sufficientemente affidabile e adeguatamente sicuro per proteggere le risorse delle parti interessate in termini di perdite e conseguenze associate.

THE PROBLEM CONTEXT

*Il **CONTESTO DEL PROBLEMA** definisce la base per un sistema sufficientemente sicuro e accettabile, data la missione, le capacità, le esigenze di prestazione e le preoccupazioni degli stakeholder; i vincoli imposti dalle preoccupazioni degli stakeholder relativi a costi, tempistiche, tolleranza al rischio e alle perdite; e altri vincoli associati ai concetti del ciclo di vita del sistema.*

Il contesto del problema include:

*1°. Determinazione dei **CONCETTI** di sicurezza del ciclo di vita;*

*2°. Definizione degli **OBIETTIVI** di sicurezza;*

*3°. Definizione dei **REQUISITI** di sicurezza; e*

*4°. Determinazione delle **MISURE** di successo.*

*Gli **OBIETTIVI** di sicurezza stabiliscono e definiscono cosa significa essere adeguatamente protetti in termini di protezione contro la perdita di asset e le conseguenze di tale perdita di asset.*

Agli obiettivi di sicurezza sono associate misure di successo.

*Le **MISURE** di successo costituiscono criteri specifici e misurabili relativi alle misure di performance operativa e alle preoccupazioni degli stakeholder.*

Le misure di successo includono sia la forza della protezione che il livello di garanzia, o fiducia, nella capacità di protezione che è stata progettata.

*Queste misure influenzano lo sviluppo dei **REQUISITI** di sicurezza e lo sviluppo delle dichiarazioni di garanzia.*

*I **CONCETTI** di sicurezza del ciclo di vita sono i processi, i metodi e le procedure associati al sistema durante il suo ciclo di vita e forniscono contesti distinti per l'interpretazione della sicurezza del sistema.*

Questi concetti servono anche per la portata e l'attenzione limitata nell'affrontare le esigenze di protezione e per considerazioni e vincoli più ampi che informano sulla sicurezza.

Le esigenze di protezione sono determinate in base agli obiettivi di sicurezza, ai concetti del ciclo di vita e alle preoccupazioni delle parti interessate.

*Le **ESIGENZE** di protezione sono successivamente trasformate in **REQUISITI** di sicurezza delle parti interessate e vincoli associati ai requisiti di sistema e le misure necessarie per convalidare che tutti i requisiti siano stati soddisfatti.*

THE SOLUTION CONTEXT

*Il **CONTESTO DELLA SOLUZIONE** trasforma i requisiti di sicurezza delle parti interessate in requisiti di progettazione per il sistema; affronta tutte le architetture di sicurezza, il design e gli aspetti correlati necessari per realizzare un sistema che soddisfi tali requisiti; e produce prove sufficienti per dimostrare che tali requisiti sono stati soddisfatti.*

Il contesto della soluzione si basa su una strategia di protezione della sicurezza del sistema proattiva e reattiva equilibrata che esercita il controllo su eventi, condizioni, perdita di risorse e conseguenze della perdita di risorse nella misura possibile, praticabile e accettabile per le parti interessate.

Il contesto della soluzione include:

*1°. **DEFINIZIONE** degli aspetti di sicurezza della soluzione;*

*2°. **REALIZZAZIONE** degli aspetti di sicurezza della soluzione; e*

*3°. **PRODUZIONE** delle prove per gli aspetti di sicurezza della soluzione.*

Gli aspetti di sicurezza della soluzione includono lo sviluppo della strategia di protezione del sistema; i requisiti di progettazione della sicurezza del sistema; le viste e i punti di vista dell'architettura di sicurezza; il design della sicurezza; gli aspetti, le capacità e le limitazioni della sicurezza nelle procedure del ciclo di vita del sistema e le misure di verifica delle prestazioni di sicurezza associate.

*Gli **ASPETTI** di sicurezza della soluzione vengono realizzati durante l'implementazione del progetto di sicurezza del sistema in accordo con l'architettura di sicurezza e in soddisfazione dei requisiti di sicurezza.*

L'evidenza associata agli aspetti di sicurezza della soluzione è ottenuta con un livello di fedeltà e grado di rigore che è influenzato dal livello di garanzia mirato dagli obiettivi di sicurezza.

Le prove di garanzia sono ottenute da metodi standard di verifica dell'ingegneria dei sistemi (ad esempio, analisi, dimostrazione, ispezione e test) e da metodi di convalida complementari applicati rispetto ai requisiti delle parti interessate.

THE TRUSTWORTHINESS CONTEXT

Il contesto di affidabilità è un contesto decisionale che fornisce una dimostrazione basata su prove, attraverso il ragionamento, che il sistema di interesse è ritenuto affidabile sulla base di una serie di affermazioni derivate dagli obiettivi di sicurezza. Il contesto di affidabilità è costituito da:

*1°. **SVILUPPARE** e **MANTENERE** il caso di garanzia; e*

*2°. **DIMOSTRARE** che il caso di garanzia è soddisfatto.*

Il contesto di affidabilità è fondato sul concetto di un caso di garanzia.

Un caso di garanzia è un insieme ben definito e strutturato di argomenti e un corpo di prove che dimostrano che un sistema soddisfa affermazioni specifiche rispetto a un dato attributo di qualità.

I casi di garanzia forniscono anche artefatti motivati e verificabili che supportano l'affermazione che un'affermazione o una serie di affermazioni è soddisfatta, comprese le argomentazioni sistematiche e le relative prove sottostanti e le ipotesi esplicite a sostegno delle affermazioni [ISO/IEC 15026-2].

Un caso di garanzia viene utilizzato per dimostrare che un sistema presenta alcune proprietà emergenti complesse come sicurezza, protezione, resilienza, affidabilità o sopravvivenza.

Il risultato fornisce una dichiarazione convincente che una sicurezza adeguata è stata raggiunta e guidata dalle esigenze e dalle aspettative delle parti interessate.

I casi di garanzia in genere includono informazioni di supporto come ipotesi, vincoli e qualsiasi inferenza che possa influenzare il processo di ragionamento.

Successivamente allo sviluppo del caso di garanzia, le analisi condotte da esperti in materia determinano che tutte le richieste di garanzia sono giustificate dalle prove prodotte e dagli argomenti che collegano le prove alle richieste.

Il caso di garanzia comprende il livello di garanzia target (desiderato), la natura delle conseguenze per le quali si richiede l'assurance e la dimensione e la complessità delle dimensioni che influiscono nella determinazione dell'affidabilità.

SYSTEMS SECURITY IN SYSTEM LIFE CYCLE PROCESSES

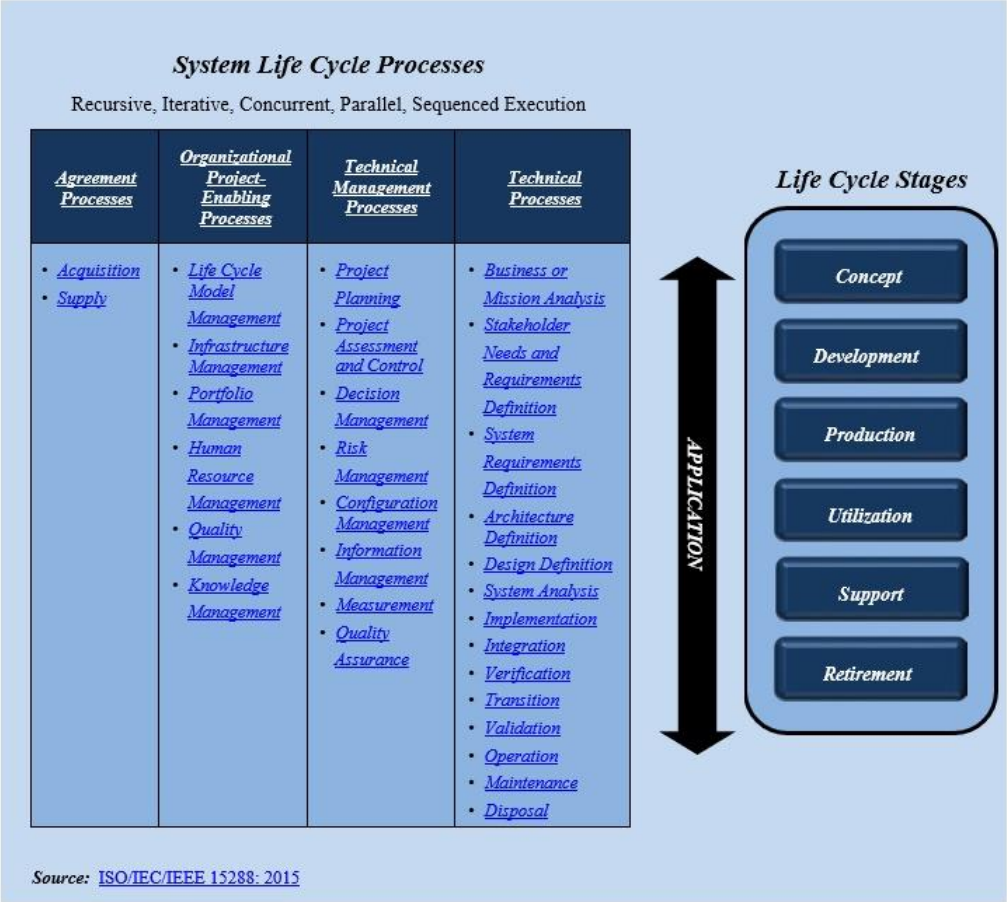


FIGURE 4: SYSTEM LIFE CYCLE PROCESSES AND LIFE CYCLE STAGES

I compiti e le attività di ingegneria della sicurezza dei sistemi sono basate su principi e concetti di sicurezza e fiducia (trust) e sfruttano i principi, i concetti, i termini e le pratiche dell'ingegneria dei sistemi per facilitare la coerenza nella loro applicazione come parte di uno sforzo di ingegneria dei sistemi.

Il raggiungimento dell'effettiva integrazione dell'ingegneria della sicurezza dei sistemi nell'ingegneria dei sistemi richiede che tutte le attività di ingegneria dei sistemi contengano esplicitamente le attività e le attività di sicurezza del sistema identificate da questa pubblicazione.

Pertanto, ***tutti i riferimenti ai processi del ciclo di vita del sistema includono esplicitamente i compiti o task e le attività di ingegneria della sicurezza dei sistemi****.*

Inoltre, ***qualsiasi riferimento a uno specifico processo del ciclo di vita del sistema include esplicitamente tutte le attività e le attività di ingegneria della sicurezza dei sistemi definite per quel processo.***

I processi del ciclo di vita del sistema vengono condotti secondo necessità per raggiungere specifici obiettivi di ingegneria dei sistemi.

In base alla progettazione, i processi possono essere applicati simultaneamente, iterativamente o ricorsivamente a qualsiasi livello nella gerarchia strutturale di un sistema, con la fedeltà e il rigore appropriati, e in qualsiasi fase del ciclo di vita del sistema, in conformità con l'acquisizione, l'ingegneria dei sistemi, o altri modelli di processo imposti.

La personalizzazione può essere motivata dalla fase del ciclo di vita del sistema; la dimensione, l'ambito e la complessità del sistema; requisiti specializzati; o la necessità di essere in grado di accogliere metodi, tecniche o tecnologie specifiche utilizzate per sviluppare il sistema.

La seguente convenzione di denominazione viene stabilita per i processi del ciclo di vita del sistema.

Ogni processo è identificato da una designazione a due caratteri (ad esempio, BA è la designazione ufficiale per il processo di Business o Mission Analysis).

La tabella 2 fornisce un elenco dei processi del ciclo di vita del sistema e dei loro designatori a due caratteri associati.

TABLE 2: PROCESS NAMES AND DESIGNATORS

ID	PROCESS	ID	PROCESS
AQ	*Acquisition*	*MS*	*Measurement*
AR	*Architecture Definition*	*OP*	*Operation*
BA	*Business or Mission Analysis*	*PA*	*Project Assessment and Control*
CM	*Configuration Management*	*PL*	*Project Planning*
DE	*Design Definition*	*PM*	*Portfolio Management*
DM	*Decision Management*	*QA*	*Quality Assurance*
DS	*Disposal*	*QM*	*Quality Management*
HR	*Human Resource Management*	*RM*	*Risk Management*
IF	*Infrastructure Management*	*SA*	*System Analysis*
IM	*Information Management*	*SN*	*Stakeholder Needs and Requirements Definition*
IN	*Integration*	*SP*	*Supply*
IP	*Implementation*	*SR*	*System Requirements Definition*
KM	*Knowledge Management*	*TR*	*Transition*
LM	*Life Cycle Model Management*	*VA*	*Validation*
MA	*Maintenance*	*VE*	*Verification*

Le attività e i task di sicurezza in ogni processo del ciclo di vita del sistema sono identificati in modo univoco utilizzando una designazione a due caratteri più una designazione numerica.

Ogni descrizione del task all'interno di un'attività di sicurezza è supportata da una sezione di discussione che fornisce informazioni aggiuntive su considerazioni rilevanti per la corretta esecuzione di tale attività.

Nel capitolo 3 "System Life Cycle Processes" del "NIST SP 800-160 Vol.1 SSE A multidisciplinary Approach in the Engineering of Trustworthy Secure Systems" sono descritti in dettaglio i contributi, le considerazioni e i risultati sulla sicurezza per i 30 processi del ciclo di vita del sistema definiti nella ISO/IEC/IEEE 15288.

Tali descrizioni sono raggruppate in 4 famiglie di processi:

1. **AGREEMENT**
2. **ORGANIZATIONAL PROJECT-ENABLING**
3. **TECHNICAL MANAGEMENT**
4. **TECHNICAL**

Nell'appendice D "SSE Activities and Task for each Systems Engineering Process" del "NIST SP 800-160 Vol.1 SSE A multidisciplinary Approach in the Engineering of Trustworthy Secure Systems" sono riportate le seguenti tabelle:

- ✓ *La Tabella D-1 riassume le attività e i compiti dei processi di* **AGREEMENT***;*
- ✓ *La Tabella D-2 riassume le attività e i compiti dai processi di* **ORGANIZATIONAL PROJECT-ENABLING***;*
- ✓ *La tabella D-3 riassume le attività e i compiti dei processi di* **TECHNICAL MANAGEMENT***; e*
- ✓ *La Tabella D-4 riassume le attività e i compiti dei processi* **TECHNICAL**.

Queste tabelle forniscono un riepilogo delle attività e delle attività di ingegneria della sicurezza dei sistemi associate ai processi del ciclo di vita del sistema in ISO/IEC/IEEE 15288.

ROLES, RESPONSIBILITIES AND SKILLS

Nell'appendice E del "NIST SP 800-160 Vol.1 SSE A multidisciplinary Approach in the Engineering of Trustworthy Secure Systems" sono descritte in dettaglio le responsabilità e le caratteristiche professionali dell'ingegnere della sicurezza.

Le responsabilità dell'ingegnere della sicurezza dei sistemi includono:

- ✓ *Mantenere una visione completa e olistica del sistema affrontando al contempo la sicurezza delle parti interessate e le preoccupazioni relative ai rischi;*
- ✓ *Garantire l'efficacia e l'idoneità degli elementi di sicurezza del sistema come fattore abilitante per il successo della missione aziendale;*
- ✓ *Garantire che i dati rilevanti su minacce e vulnerabilità siano considerati a sostegno delle decisioni rilevanti per la sicurezza;*
- ✓ *Fornire input all'analisi delle alternative e alle analisi dei requisiti, dell'ingegneria e del compromesso del rischio per ottenere una progettazione architettonica di sicurezza conveniente per le protezioni che consentono il successo della missione aziendale;*
- ✓ *Fornire le prove necessarie per supportare le affermazioni di garanzia e per dimostrare che il sistema è sufficientemente affidabile;*
- ✓ *Conduzione di attività di gestione dei rischi per la sicurezza, produzione di informazioni relative alla gestione dei rischi per la sicurezza e consulenza al team di ingegneri e alle principali parti interessate sull'impatto di minacce e vulnerabilità rilevanti per la sicurezza per la missione/attività supportata dal sistema.*

DESIGN PRINCIPLES FOR SECURITY

Nell'appendice F del "NIST SP 800-160 Vol.1 SSE A multidisciplinary Approach in the Engineering of Trustworthy Secure Systems" sono descritti in dettaglio i principi per la progettazione della sicurezza dei sistemi.

Di seguito, la tabella F-1 riassume i principi di progettazione della sicurezza.

TABLE F-1: TAXONOMY OF SECURITY DESIGN PRINCIPLES

SECURITY DESIGN PRINCIPLES	
SECURITY ARCHITECTURE AND DESIGN	
Clear Abstractions	*Hierarchical Trust*
Least Common Mechanism	*Inverse Modification Threshold*
Modularity and Layering	*Hierarchical Protection*
Partially Ordered Dependencies	*Minimized Security Elements*
Efficiently Mediated Access	*Least Privilege*
Minimized Sharing	*Predicate Permission*
Reduced Complexity	*Self-Reliant Trustworthiness*
Secure Evolvability	*Secure Distributed Composition*
Trusted Components	*Trusted Communication Channels*
SECURITY CAPABILITY AND INTRINSIC BEHAVIORS	
Continuous Protection	*Secure Failure and Recovery*
Secure Metadata Management	*Economic Security*
Self-Analysis	*Performance Security*
Accountability and Traceability	*Human Factored Security*
Secure Defaults	*Acceptable Security*
LIFE CYCLE SECURITY	
Repeatable and Documented Procedures	*Secure System Modification*
Procedural Rigor	*Sufficient Documentation*

ENGINEERING AND SECURITY FUNDAMENTALS

Nell'appendice G del "NIST SP 800-160 Vol.1 SSE A multidisciplinary Approach in the Engineering of Trustworthy Secure Systems" sono descritti in dettaglio i fondamentali o razionali per la progettazione della sicurezza dei sistemi.

Gli argomenti chiave affrontati in questa sezione includono:

1. *PROTECTION NEEDS;*
2. *SECURITY REQUIREMENTS;*
3. *SECURITY POLICY;*
4. *DISTINGUISHING REQUIREMENTS, POLICY AND MECHANISMS;*
5. *SYSTEM SECURITY ARCHITECTURE, VIEWS AND VIEWPOINTS*
6. *SECURITY RELEVANCE*
7. *SECURITY FUNCTION PROTECTION CRITICALITY*
8. *TRUSTWORTHINESS AND ASSURANCE*
9. *SYSTEM SECURITY COST, PERFORMANCE, AND EFFECTIVENESS*

TRANSFORMATION OF PROTECTION NEEDS INTO SECURITY REQUIREMENTS AND POLICY

Le esigenze di protezione delle parti interessate sono espresse e formalizzate in due forme nettamente diverse ma correlate:

1st. **REQUISITI** *di sicurezza e*

2nd. **POLITICA** *di sicurezza.*

*I **REQUISITI** di sicurezza specificano la capacità della sicurezza, le prestazioni, l'efficacia e le misure di verifica e convalida associate ed esprimono anche i vincoli sui requisiti di sistema.*

*La **POLITICA** di sicurezza consiste in un insieme ben definito di regole che governano tutti gli aspetti del comportamento rilevante per la sicurezza degli elementi del sistema.*

La figura G-1 illustra le principali fonti di input utilizzate per definire le esigenze di protezione e gli output derivati dalla specifica di tali esigenze.

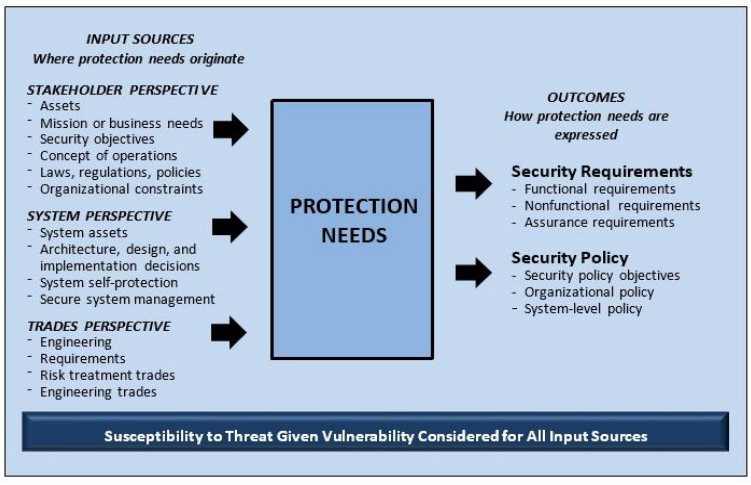


FIGURE G-1: DEFINING PROTECTION NEEDS

SECURITY REQUIREMENTS

La figura G-4 illustra la moltitudine di fattori considerati nell'analisi dei requisiti di sicurezza condotta come parte dell'ingegneria dei requisiti.

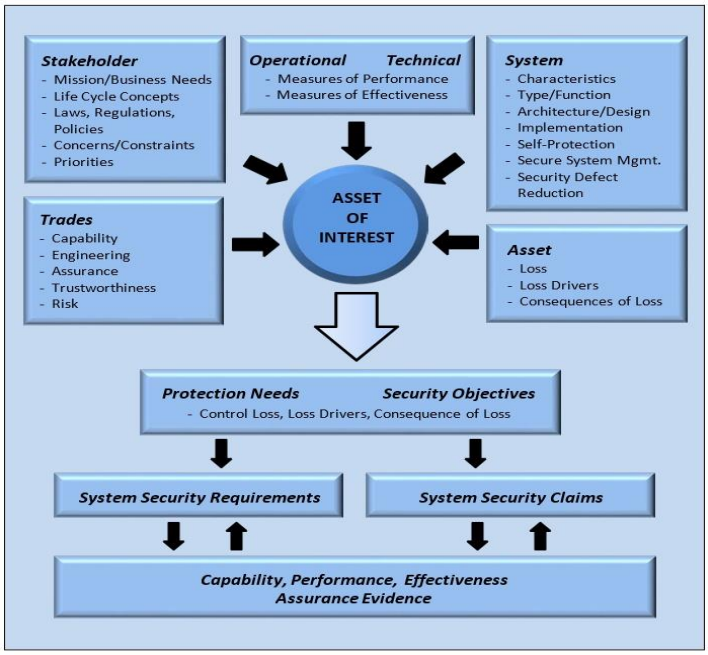


FIGURE G-4: FACTORS IN SECURITY REQUIREMENTS ANALYSIS

SECURITY POLICY

La politica di sicurezza è un concetto fondamentale.

La politica di sicurezza fornisce una serie di regole ben definite che determinano aspetti del comportamento, delle interazioni e dei risultati degli elementi di sistema ritenuti sicuri.

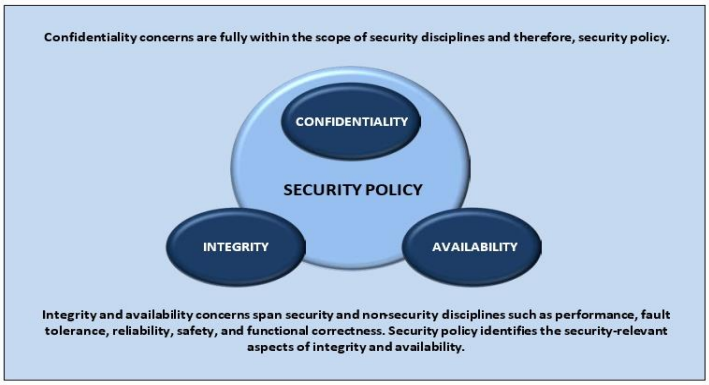


FIGURE G-5: SCOPE OF SECURITY POLICY PROPERTIES

DISTINGUISHING REQUIREMENTS, POLICY AND MECHANISMS

I termini **REQUISITI, POLITICA E MECCANISMI** *sono spesso usati in modo astratto che consentono di considerarli come sinonimi. Tuttavia, se utilizzati nel contesto dell'ingegneria di sistemi sicuri affidabili, questi termini sono nettamente diversi nel loro significato e nella loro importanza per specificare, realizzare, utilizzare e sostenere i sistemi in modo affidabile e sicuro.*

Un **REQUISITO** *è una condizione o capacità che deve essere soddisfatta o posseduta da un sistema o da un elemento del sistema per soddisfare un contratto, standard, specifica o altro documento imposto formalmente [IEEE 610.12].*

- ✓ *Una* **POLITICA** *di sicurezza è un insieme di affermazioni rispetto a ciò che è e ciò che non è consentito.*
- ✓ *Un* **MECCANISMO** *di sicurezza è un'entità o procedura che applica una parte della politica di sicurezza [Bishop05].*

- ✓ *La* **POLITICA** *di sicurezza stabilisce il comportamento necessario per ottenere una condizione di sicurezza, mentre un meccanismo di sicurezza è il mezzo con cui si ottiene il comportamento necessario.*
- ✓ *La distinzione tra* **POLITICA** *di sicurezza e* **MECCANISMO** *di sicurezza si estende anche per differenziare i* **REQUISITI** *di sicurezza (che specificano la capacità, il comportamento e gli attributi di qualità esibiti e posseduti dai meccanismi di sicurezza) dalla* **POLITICA** *di sicurezza (che specifica come i* **MECCANISMI** *di sicurezza devono comportarsi in qualche contesto operativo).*

Si noti che dal punto di vista del sistema, l'essere umano può fungere da **MECCANISMO** *di sicurezza, è soggetto a comportamenti sicuri come stabilito dalla* **POLITICA** *di sicurezza pertinente e deve avere la capacità di comportarsi in modo di qualità rispetto ai requisiti di sicurezza pertinenti.*

Si possono trarre le seguenti conclusioni:

- ✓ *i* **REQUISITI** *di sicurezza determinano la capacità dei meccanismi di sicurezza di comportarsi in qualche modo;*
- ✓ *la* **POLITICA** *di sicurezza determina il comportamento considerato "sicuro"; e*
- ✓ *affinché un* **MECCANISMO** *sia considerato sicuro, i* **REQUISITI** *per la* **CAPACITÀ** *del meccanismo devono essere coerenti con le regole di applicazione della* **POLITICA** *di sicurezza; il* **MECCANISMO** *deve soddisfare i* **REQUISITI** *di sicurezza e deve essere configurato per comportarsi nel modo definito dalla* **POLITICA** *di sicurezza.*

SYSTEM SECURITY ARCHITECTURE, VIEWS AND VIEWPOINTS

L'architettura del sistema, in generale, è concetti o proprietà fondamentali di un sistema nel suo ambiente incorporati nei suoi elementi, nelle relazioni e nei principi della sua progettazione ed evoluzione [ISO/IEC/IEEE 42010].

L'architettura del sistema trasmette informazioni sia sul sistema e sui suoi elementi sia sulle interconnessioni, le relazioni e il comportamento degli elementi a diversi livelli di astrazione, ambiti diversi, comprendendo più viste del sistema.

Una vista dell'architettura è un prodotto di lavoro che esprime l'architettura di un sistema dal punto di vista di specifici problemi di sistema [ISO/IEC IEEE 42010].

Un punto di vista dell'architettura è un prodotto di lavoro che stabilisce le convenzioni per la costruzione, l'interpretazione e l'uso delle viste dell'architettura per inquadrare problemi di sistema specifici [ISO/IEC/IEEE 42010].

SECURITY RELEVANCE

Rilevanza della sicurezza significa semplicemente che c'è qualche aspetto guidato dalla sicurezza o informato sulla sicurezza di una preoccupazione, problema, necessità o risultato.

La rilevanza della sicurezza è un attributo di molte entità legate all'ingegneria tra cui, ad esempio: requisiti; architettura; design; funzioni; personale, ruoli e responsabilità; configurazione; e politiche, procedure e documentazione.

La rilevanza della sicurezza è caratterizzata e analizzata utilizzando le seguenti designazioni:

- ✓ FUNZIONI DI APPLICAZIONE DELLA SICUREZZA*: le funzioni di applicazione della sicurezza sono direttamente responsabili della fornitura di capacità di protezione della sicurezza, incluso il farlo in conformità con l'adozione o l'applicazione delle decisioni relative alle politiche di sicurezza.*
  Un esempio di una funzione di applicazione della sicurezza è quella che prende la decisione di concedere o negare l'accesso a una risorsa.
- ✓ FUNZIONI DI SUPPORTO DELLA SICUREZZA*: le funzioni di supporto della sicurezza contribuiscono alla capacità delle funzioni di applicazione della sicurezza di fornire la capacità specificata.*
  Queste funzioni forniscono dati, servizi o eseguono operazioni da cui dipendono le funzioni di applicazione della sicurezza. Generalmente, la dipendenza è a livello funzionale.
  La gestione della memoria è un esempio di una funzione di supporto della sicurezza.

- ✓ FUNZIONI DI SICUREZZA NON INTERFERENTI*: le funzioni di sicurezza non interferenti non sono né per l'applicazione della sicurezza né per il supporto della sicurezza, ma hanno il potenziale di influenzare negativamente (cioè, interferire o corrompere) il corretto funzionamento delle funzioni di applicazione della sicurezza e di supporto della sicurezza.*
  La non interferenza della sicurezza dovrebbe essere interpretata come un obiettivo di garanzia della progettazione, il che significa che, per impostazione predefinita, queste funzioni non hanno la capacità di interferire con o alterare il comportamento delle funzioni di applicazione della sicurezza e di supporto della sicurezza.
  L'obiettivo di non interferire viene raggiunto attraverso vincoli basati sulla sicurezza sui requisiti, l'architettura, il design e l'uso di queste funzioni.

SECURITY FUNCTION PROTECTION CRITICALLY

La criticità della protezione della funzione di sicurezza riflette il grado in cui il fallimento delle funzioni di applicazione della sicurezza e di supporto della sicurezza influisce sulla capacità del sistema di fornire capacità di protezione in relazione alle conseguenze che ne derivano e il livello di garanzia associato alla fornitura della capacità di protezione .

Il fallimento, sia in forma intenzionale che non intenzionale, è determinato in relazione al rispetto dei requisiti di sicurezza e al raggiungimento solo di comportamenti, interazioni e risultati specifici.

Il guasto viene valutato, come richiesto, attraverso lo spettro dalla degradazione funzionale limitata alla completa incapacità di funzionare.

TRUSTWORTHINESS AND ASSURANCE

I concetti di sicurezza, sicurezza del sistema e sicurezza adeguata stabiliscono una natura intrinsecamente sensibile al contesto e soggettiva a qualsiasi affermazione che gli obiettivi di sicurezza del sistema siano raggiunti.

Nessuno stakeholder parla unilateralmente per tutti gli stakeholder del sistema in merito alla valutazione degli asset del sistema o alla necessità e sufficienza delle funzioni di sicurezza.

A ciò si aggiunge la natura emergente della sicurezza del sistema, ovvero un risultato determinato dal modo in cui si compongono gli elementi del sistema e le funzioni di sicurezza costituenti.

La sicurezza del sistema non è determinata esclusivamente sulla base di un singolo elemento del sistema o funzione di sicurezza in isolamento, pertanto, i requisiti e i metodi di verifica e convalida associati sono necessari da soli, ma non sono sufficienti come base per ritenere un sistema sicuro.

Sono necessari ulteriori mezzi per aiutare ad affrontare la proprietà emergente della sicurezza attraverso le preoccupazioni e le esigenze soggettive e spesso contraddittorie, concorrenti e contrastanti delle parti interessate.

Questi mezzi devono anche fornire un livello di fiducia commisurato alle conseguenze delle perdite associate alla valutazione delle attività.

SYSTEM SECURITY COST, PERFORMANCE AND EFFECTIVENESS

I costi associati alle funzioni di sicurezza includono, ad esempio, il costo per acquisire, sviluppare, integrare, far funzionare e sostenere le funzioni durante il ciclo di vita del sistema; il costo delle funzioni di sicurezza in termini di impatto sulle prestazioni del sistema; il costo dello sviluppo e della gestione della documentazione e della formazione del ciclo di vita; e il costo per ottenere e mantenere il livello di garanzia obiettivo.

Il costo della garanzia include il costo per ottenere le prove; il costo per condurre le analisi con la fedeltà e il rigore definiti dai requisiti di assurance; e il costo per fornire il ragionamento/razionale che sostenga l'affermazione che è stata raggiunta un'affidabilità sufficiente.

SUMMARY OF SYSTEMS SECURITY ACTIVITIES AND TASKS

L'elenco completo del sommario dei task e delle attività per ogni processo di ingegneria dei sistemi è nell'Appendix D del NIST SP 800-160 Vol. 1.

10. DEVELOPING CYBER RESILIENT SYSTEMS

VEDI MANUALE: NIST SP 800-160 VOL.2 DEVELOPING CYBER RESILIENT SYSTEMS: A SSE APPROACH

APPENDICE F – ELENCO DEI 18 PRINCIPI DI PROGETTAZIONE

I principi di progettazione strutturale forniscono indicazioni per le decisioni di progettazione intese a ridurre il rischio.

I principi di progettazione della sicurezza sono organizzati in una tassonomia che comprende:

- ***Architettura** e **Progettazione** della sicurezza (ovvero organizzazione, struttura, interconnessioni e interfacce)*
- ***Funzionalità** di sicurezza e comportamenti intrinseci (ovvero, quali sono le protezioni e come vengono fornite); e*
- ***Life Cycle Security** (ad es. definizione, condotta e gestione del processo di sicurezza).*

*L'applicazione di questi principi ha lo scopo di consentire una dimostrazione dell'**Affidabilità** del sistema attraverso la garanzia basata sul ragionamento su prove rilevanti e credibili.*

Applicando i principi a diversi livelli di astrazione (ad es. progettazione e composizione dei componenti), è possibile sviluppare una solida architettura di sicurezza basata su elementi di fiducia e un approccio costruttivo.

1. *F.1.1 CLEAR ABSTRACTIONS*
2. *F.1.2 LEAST COMMON MECHANISM*
3. *F.1.3 MODULARITY AND LAYERING*
4. *F.1.4 PARTIALLY ORDERED DEPENDENCIES*
5. *F.1.5 EFFICIENTLY MEDIATED ACCESS*
6. *F.1.6 MINIMIZED SHARING*
7. *F.1.7 REDUCED COMPLEXITY*
8. *F.1.8 SECURE EVOLVABILITY*
9. *F.1.9 TRUSTED COMPONENTS*
10. *F.1.10 HIERARCHICAL TRUST*
11. *F.1.11 INVERSE MODIFICATION THRESHOLD*
12. *F.1.12 HIERARCHICAL PROTECTION*
13. *F.1.13 MINIMIZED SECURITY ELEMENTS*
14. *F.1.14 LEAST PRIVILEGE*
15. *F.1.15 PREDICATE PERMISSION*
16. *F.1.16 SELF-RELIANT TRUSTWORTHINESS*
17. *F.1.17 SECURE DISTRIBUTED COMPOSITION*
18. *F.1.18 TRUSTED COMMUNICATION CHANNELS*

ASSIOMA DELL'AFFIDABILITÀ

> «La progettazione di sistemi affidabili, compresi i loro sottosistemi e i loro componenti costituenti, hanno come prerequisito i principi e i concetti di progettazione della sicurezza»

I principi e i concetti sono destinati ad essere universalmente applicabili a sistemi operativi affidabili, ai componenti, ambienti e sistemi di elaborazione completamente collegati in rete, distribuiti, mobili e virtuali.

I principi di progettazione della sicurezza sono organizzati in una tassonomia che comprende:

- *Architettura e Progettazione della sicurezza (ovvero organizzazione, struttura, interconnessioni e interfacce);*
- *Funzionalità di sicurezza e comportamenti intrinseci (ovvero, quali sono le protezioni e come vengono fornite);*
- *Life Cycle Security (ad es. definizione, condotta e gestione del processo di sicurezza).*

L'applicazione di questi principi ha lo scopo di consentire una dimostrazione dell'Affidabilità del sistema attraverso la garanzia basata sul ragionamento su prove rilevanti e credibili.

I principi e i concetti di progettazione della sicurezza dovrebbero essere parte integrante della soluzione di Sistema Totale.

TABELLA F1: TASSONOMIA DEI PRINCIPI DI PROGETTAZIONE DELLA SICUREZZA

Security Architecture and Design	
Clear Abstractions	*Hierarchical Trust*
Least Common Mechanism	*Inverse Modification Threshold*
Modularity and Layering	*Hierarchical Protection*
Partially Ordered Dependencies	*Minimized Security Elements*
Efficiently Mediated Access	*Least Privilege*
Minimized Sharing	*Predicate Permission*
Reduced Complexity	*Self-Reliant Trustworthiness*
Secure Evolvability	*Secure Distributed Composition*
Trusted Components	*Trusted Communication Channels*
Security Capability and Intrinsic Behaviors	
Continuous Protection	*Secure Failure and Recovery*
Secure Metadata Management	*Economic Security*
Self-Analysis	*Performance Security*
Accountability and Traceability	*Human Factored Security*
Secure Defaults	*Acceptable Security*
Life Cycle Security	
Repeatable and Documented Procedures	*Secure System Modification*
Procedural Rigor	*Sufficient Documentation*

ELEMENTI BASILARI DELLA SICUREZZA

Il seguente elenco indica gli elementi fondamentali della Cibersicurezza.

Tali componenti determinano anche l'ordine dei passi necessari per ottenere la sicurezza dei sistemi.

Questi passi sono il prerequisito della fase di implementazione e realizzazione della sicurezza.

Nelle diapositive successive sono descritti le singole caratteristiche dei passi attraverso le definizioni.

1°. *PRINCIPIO;*

2°. *REQUISITO;*

3°. *POLITICA;*

4°. *MECCANISMO;*

5°. *PROPRIETÀ;*

6th. *MODELLO.*

PRINCIPIO

SICUREZZA DEL SISTEMA COME PROBLEMA DI PROGETTAZIONE

«Per una sicurezza completa è necessaria una combinazione di hardware, software, comunicazioni, protezione fisica, personale e amministrativo-procedurale. In particolare, le garanzie di software da sole non sono sufficienti»

-- *The Ware Report: Defense Science Board Task Force on Computer Security, 1970:*

Ware W (1970) Security Controls for Computer Systems: Report of the Defense Science Board Task Force on Computer Security. (The Rand Corporation, Santa Monica, CA). Available at https://csrc.nist.gov/csrc/media/publications/conference-paper/1998/10/08/proceedings-of-the-21st-nissc-1998/documents/early-cs-papers/ware70.pdf

PRINCIPIO DELLA SICUREZZA

«LA RESILIENZA INFORMATICA È PARTE INTEGRANTE DELLA SICUREZZA»

REQUISITO

*I Requisiti del sistema **specificano la capacità e il comportamento** che un Meccanismo deve essere in grado di fornire.*

DEFINIZIONE 1 DI REQUISITO DELLA SICUREZZA

«I requisiti di sicurezza:

- ✓ specificano la capacità di sicurezza, le prestazioni, l'efficacia e le misure di verifica e convalida associate;
- ✓ esprimono anche vincoli ai requisiti di sistema e sono sviluppati in forme indipendenti dalla progettazione (ovvero, requisiti delle parti interessate) e dipendenti dalla progettazione (ovvero, requisiti di sistema)»

DEFINIZIONE 2 DI REQUISITO DELLA SICUREZZA

«Un requisito è una condizione o capacità che deve essere soddisfatta o posseduta da un sistema o elemento di sistema per soddisfare un contratto, uno standard, una specifica o un altro documento imposto formalmente [IEEE 610.12]»

DEFINIZIONE 3 DI REQUISITO DELLA SICUREZZA

«Il requisito della sicurezza descritto in SP 800-160 v1 (vedi Appendice N) è un "requisito che specifica le caratteristiche funzionali, di garanzia e di resistenza di un meccanismo, di un sistema o di un elemento di sistema"»

POLITICA

La Politica specifica gli aspetti particolari della stessa affinché il Meccanismo sia applicato per raggiungere gli obiettivi organizzativi.

DEFINIZIONE 1 DI POLITICA DELLA SICUREZZA

«La politica della sicurezza consiste in un insieme ben definito di regole che disciplinano tutti gli aspetti del comportamento rilevante per la sicurezza degli elementi del sistema»

DEFINIZIONE 2 DI POLITICA DELLA SICUREZZA

«Una politica di sicurezza è una serie di dichiarazioni relative a ciò che è e ciò che non è consentito, mentre un meccanismo di sicurezza è un'entità o una procedura che impone una parte della politica di sicurezza [Bishop05]. La politica di sicurezza stabilisce il comportamento necessario a raggiungere una condizione sicura»

MECCANISMO

DEFINIZIONE DI MECCANISMO DELLA SICUREZZA

«È il mezzo attraverso il quale la Politica della Sicurezza stabilisce la condotta necessaria a raggiungere una condizione sicura»

PROPRIETÀ

PROPRIETÀ 1 DELLA SICUREZZA

«I meccanismi di sicurezza informatica comprendono il controllo dell'accesso adattivo al rischio (Risk Adaptive Access Control [RAAC]) per i sistemi "servizi di sicurezza informatica" altamente adattivi (Highly Adaptive Cibersicurezza Service [HACS])»

PROPRIETÀ 2 DELLA SICUREZZA

«Quando si considera la ciberresilienza come parte del processo di Business o Mission Analysis, l'ingegneria della sicurezza dei sistemi analizza i problemi o le opportunità di business o di missione dell'organizzazione dal punto di vista degli obiettivi, degli obiettivi e dei vincoli di ciberresilienza sullo spazio della soluzione»

PROPRIETÀ 3 DELLA SICUREZZA

«Quando si considera la ciberresilienza come parte del processo di definizione delle esigenze e dei requisiti delle parti interessate, l'ingegneria della sicurezza dei sistemi scatena le esigenze delle parti interessate, in termini di resilienza informatica, e quindi traduce tali esigenze in requisiti di resilienza informatica»

PROPRIETÀ 4 DELLA SICUREZZA DEI SISTEMI

«Quando si considera la resilienza informatica come parte del processo di definizione dei requisiti di sistema, l'ingegneria della sicurezza dei sistemi identifica i requisiti di sistema per la resilienza informatica affinché riflettano i requisiti delle parti interessate identificati per la resilienza informatica»

PROPRIETÀ 5 DELLA SICUREZZA

«Quando si considera la resilienza informatica come parte del processo di definizione dell'architettura, l'ingegneria della sicurezza dei sistemi genera viste sulla resilienza informatica delle alternative dell'architettura di sistema, al fine di guidare la selezione di una o più alternative.

Inoltre, l'ingegneria della sicurezza dei sistemi accerta che i processi analitici di resilienza informatica siano stati applicati in tutte le viste rappresentative dell'architettura, al fine di identificare le dipendenze funzionali e di sicurezza, nonché le potenziali conseguenze dello sfruttamento delle vulnerabilità e delle vulnerabilità identificate dall'analisi dell'ingegneria della sicurezza»

PROPRIETÀ 6 DELLA SICUREZZA

«Quando si considera la ciberresilienza come parte del processo di definizione del progetto, l'ingegneria della sicurezza dei sistemi considera le caratteristiche del progetto di ciberresilienza, nonché in stretta relazione con le caratteristiche del progetto di sicurezza.

Il concetto di funzione sicura comprende principi e concetti di progettazione della sicurezza»

PROPRIETÀ 7 DELLA SICUREZZA

«Come parte del processo di analisi del sistema, l'ingegneria della sicurezza dei sistemi affronta gli aspetti di analisi della resilienza informatica»

PROPRIETÀ 8 DELLA SICUREZZA

«Quando si considera la ciberresilienza come parte del processo di implementazione, l'ingegneria della sicurezza dei sistemi si concentra sugli aspetti di sicurezza degli elementi di sistema e della strategia di implementazione in modo che la ciberresilienza non sia una considerazione diretta»

PROPRIETÀ 9 DELLA SICUREZZA

«Quando si considera la ciberresilienza come parte del processo di verifica, l'ingegneria dei sistemi di sicurezza produce prove del fatto che il sistema soddisfa i requisiti di sistema rilevanti per la ciberresilienza e presenta le caratteristiche richieste di ciberresilienza alla luce del presunto ambiente di minaccia»

MODELLO

DEFINIZIONE DI MODELLO DELLA SICUREZZA

«È una rappresentazione di un'architettura, un progetto o un sistema che identifichi entità e relazioni (ad es. soggetti, oggetti e un monitor di riferimento; enclavi, confini e flussi di informazioni; fonti di informazioni, destinazioni e percorsi di comunicazione)»

Un modo per analizzare facilmente la conformità ai requisiti di sicurezza e l'applicazione delle politiche di sicurezza.

Un modello di sicurezza utilizza o si basa su un framework di architettura e può essere un modello fisico, logico o informativo.

RELAZIONE TRA POLITICA E MECCANISMO

Il Meccanismo stabilisce i Requisiti: capacità, comportamento e attributi di qualità esibiti e posseduti dai meccanismi di sicurezza

La Politica specifica come i Meccanismi debbano comportarsi in alcuni contesti operativi

Si possono trarre le seguenti conclusioni:

1. *i Requisiti determinano la capacità dei Meccanismi di manifestarsi;*
2. *la Politica determina il comportamento considerato "**sicuro**";*
3. *il Meccanismo deve soddisfare i Requisiti e deve comportarsi in un modo stabilito dalla Politica.*

AFFIDABILITÀ

ASSIOMA DELL'AFFIDABILITÀ

«La progettazione di sistemi affidabili, quindi sicuri, compresi i loro sottosistemi e i loro componenti costituenti, hanno come prerequisito i principi e i concetti di progettazione della sicurezza.
Questi principi e concetti rappresentano la ricerca, lo sviluppo e l'esperienza applicativa a partire dalla prima incorporazione di meccanismi di sicurezza per sistemi operativi affidabili, fino alla vasta gamma odierna di componenti, ambienti e sistemi di elaborazione completamente collegati in rete, distribuiti, mobili e virtuali»

TREDICI PASSI PER L'IMPLEMENTAZIONE DELLA SICUREZZA

Il seguente elenco indica i passi fondamentali per la realizzazione della Cibersicurezza.

1. *identificare e classificare le infrastrutture critiche da proteggere*
2. *stabilire trattati, leggi e regole di condotta nazionali e/o internazionali ad hoc*
3. *sviluppare i rapporti diplomatici e rafforzare le partnership internazionali*
4. *focus sulla protezione dei diritti fondamentali, sulla privacy e/o sulla libertà di espressione*
5. *focus sul cyber-crime*
6. *trattare il cyber-spazio come dominio di warfare*
7. *creare apposite strutture politiche e decisionali per far fronte alla minaccia*
8. *sviluppare deterrenza per la prevenzione dei conflitti nel cyber-spazio*
9. *incrementare i livelli di sicurezza, affidabilità e resilienza delle reti e dei sistemi informatici*
10. *rafforzare la condivisione delle informazioni, l'early warning e le capacità di incident response*
11. *aumentare la consapevolezza pubblica della minaccia e l'importanza della cybersecurity*
12. *creare e/o incrementare il numero delle figure professionali ad hoc*
13. *incoraggiare l'innovazione, la ricerca e lo sviluppo*

REGOLE BASILARI

1. *Configurazione sicura tutto hardware e software*
2. *Efficace ed effettiva politica di correzione delle vulnerabilità*
3. *Account con privilegi minimi*
4. *Autenticazione attraverso password complesse (non meno di 10 caratteri, alfanumeriche, con l'inserimento di almeno una lettera maiuscola e un carattere speciale)*
5. *Efficace difesa del perimetro della rete aziendale*
6. *Sistemi di analisi, di identificazione e di protezione in tempo reale accessi degli utenti, dello stato dei sistemi informatici, dei programmi in esecuzione e del loro utilizzo delle risorse (antivirus, workstation firewall e host-based intrusion detection/prevention system)*
7. *Specifici sistemi di protezione e conformi alle politiche di sicurezza per l'uso delle e-mail e dei file allegati, per ridurre il rischio d'infezione attraverso malware*
8. *Sistemi automatizzati di analisi e filtro dei contenuti web, al fine di impedire la visualizzazione e la navigazione di siti Internet inappropriati e/o potenzialmente pericolosi per la sicurezza dei sistemi*

9. *Sistema centralizzato di raccolta, archiviazione e analisi in tempo reale dei file di log (file da conservare per almeno 6 mesi)*
10. *Prevenire l'uso non autorizzato e la trasmissione di informazioni aziendali riservate attraverso specifiche politiche di data loss prevention*
11. *Politica di utilizzo e controllo all'uso supporti di memoria rimovibili (chiavette USB, hard disk esterni, CD-ROM, memory card, ecc.).*
12. *Politica di Business Continuity (BC) e di Disaster Recovery (DR) per la resilienza dei sistemi*
13. *Programmi di formazione del personale sull'uso degli strumenti informatici, sulla sicurezza informatica e delle informazioni (protezione dei dati personali)*

MISURE MINIME DI SICUREZZA

1. *Autenticazione informatica*
2. *Adozione di procedure per l'autenticazione*
3. *Utilizzazione di un sistema di autorizzazione*
4. *Aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici*
5. *Protezione sia degli strumenti elettronici sia dei dati*
6. *Adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi*
7. *Adozione di tecniche di cifratura o di codici identificativi per determinati trattamenti di dati*

DATA SECURITY (DS)

[File: DATA SECURITY.DOCX]

La DS è composta da tre parti:

1°. *DATA INTEGRITY*
2°. *DATA CONFIDENTIALITY*
3°. *DATA AVAILABILITY*

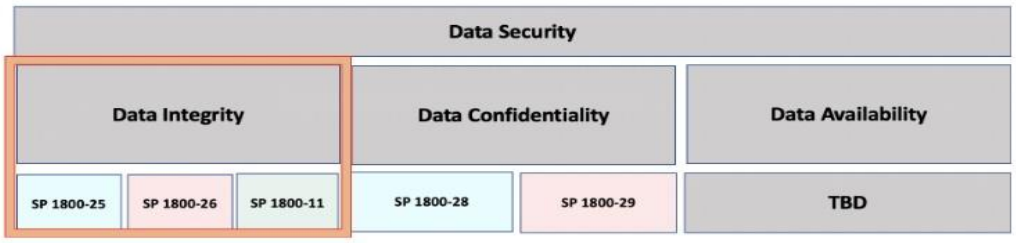


Figure 1-1 Data Security Projects

DATA INTEGRITY (DI)

I dati delle organizzazioni (database, file di sistema, configurazioni, file utente, applicazioni e dati dei clienti) sono tutti potenziali obiettivi di danneggiamento, modifica e distruzione dei dati.

Esistono tre progetti di integrità dei dati che sono allineati con le funzioni del NIST Cybersecurity Framework con l'obiettivo di formulare una difesa contro le sfide dell'integrità dei dati.

NIST ha pubblicato la versione 1.1 del Cybersecurity Framework (CSF) nell'aprile 2018 per fornire indicazioni sulla protezione e lo sviluppo della resilienza per le infrastrutture critiche e altri settori.

Il nucleo del framework contiene 5 funzioni base:

1. *IDENTIFY*
2. *PROTECT*
3. *DETECT*
4. *RESPOND*
5. *RECOVER*

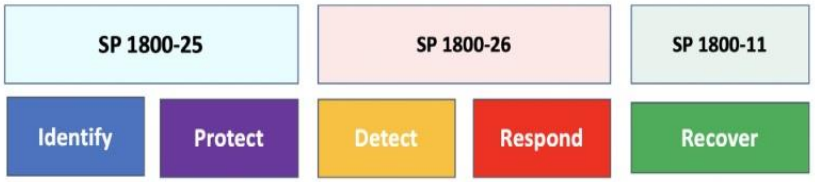


Figure 1-3 Division of CSF Functions Across Data Integrity Projects

FRAMEWORK PER L'ARCHITETTURA DELLA PRIVACY

[Rif. ISO/IEC 29101]

Definire un framework che:

1. *specifichi le peculiarità dei sistemi ICT che elaborano le PII;*
2. *elenchi i componenti per l'implementazione di tali sistemi;*
3. *fornisca viste architettoniche contestualizzando questi componenti;*

Questo framework deve essere applicabile alle entità coinvolte nella specifica, nell'acquisizione, nell'architettura, nella progettazione, nel test, nella manutenzione, nell'amministrazione e nella gestione dei sistemi ICT che elaborano le PII.

PIANO DELLA SICUREZZA (SECURITY PLAN)

[Rif. ISO/IEC 29101]

17 PASSI PER LO SVILUPPO DEL PIANO

1. *System Name and Identifier*
2. *System Categorization*
3. *Each system identified in the agency's system inventory must be categorized using FIPS 199. NIST Special Publication 800-60, Guide for Mapping Types of Information and Information Systems to Security Categories, provides implementation guidance in completing this activity. See Table 1 for a summary of FIPS 199 categories*
4. *System Owner*
5. *Authorizing Official*
6. *Other Designated Contacts*
7. *Assignment of Security Responsibility*
8. *System Operational Status*
9. *Information System Type*
10. *General Description/Purpose*
11. *System Environment*
12. *System Interconnection/Information Sharing*
13. *Laws, Regulations, and Policies Affecting the System*
14. *Security Control Selection*
15. *Minimum Security Controls*
16. *Completion and Approval Dates*
17. *Ongoing System Security Plan Maintenance*

DEFINIZIONE DEGLI OBIETTIVI E DEGLI IMPATTI

[Rif. ISO/IEC 29101]

Table 1: FIPS 199 Categorization

	POTENTIAL IMPACT		
Security Objective	**LOW**	**MODERATE**	**HIGH**
Confidentiality Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [44 U.S.C., SEC. 3542]	The unauthorized disclosure of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Integrity Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. [44 U.S.C., SEC. 3542]	The unauthorized modification or destruction of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Availability Ensuring timely and reliable access to and use of information. [44 U.S.C., SEC. 3542]	The disruption of access to or use of information or an information system could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.

RIEPILOGO CLASSI E FAMIGLIE CONTROLLO DI SICUREZZA (ISO E NIST)

[Rif. ISO/IEC 29101]

Table 2: Security Control Class, Family, and Identifier

Nella "Appendix H international Information Security Standard" del manuale "NISP SP 800-53", sono presenti le tabelle che mappano i controlli del NIST con quelli dell'ISO/IEC sia 27001 sia 15408.

CLASS	FAMILY	IDENTIFIER
Management	Risk Assessment	RA
Management	Planning	PL
Management	System and Services Acquisition	SA
Management	Certification, Accreditation, and Security Assessments	CA
Operational	Personnel Security	PS
Operational	Physical and Environmental Protection	PE
Operational	Contingency Planning	CP
Operational	Configuration Management	CM
Operational	Maintenance	MA
Operational	System and Information Integrity	SI
Operational	Media Protection	MP
Operational	Incident Response	IR
Operational	Awareness and Training	AT
Technical	Identification and Authentication	IA
Technical	Access Control	AC
Technical	Audit and Accountability	AU
Technical	System and Communications Protection	SC

DETTAGLIO 18 PRINCIPI PROGETTAZIONE - APPROACHES FOR TAKING ADVERSARIAL ACTIVITIES INTO CONSIDERATION

[Rif. Appendix H Adversary Oriented Analysis del NIST SP 800-160, Vol. 2]

Come illustrato nella Tabella H2, NTCTF (NSA/CSS Technical Cyber Threat Framework) consente alle campagne o operazioni informatiche dell'APT (Advanced Persistent Threat) di essere descritte in termini di fasi: Attacco, Obiettivi [Avversario] e Azioni [Avversario].

Le azioni identificate in NTCTF sono orientate verso l'architettura IT aziendale o un'architettura per un sistema o sistema di sistemi di comando, controllo e comunicazione.

Le 6 fasi sono:

1. *Amministrazione [**Administration**],*
2. *Preparazione [**Preparation**],*
3. *Coinvolgimento [**Engagement**],*
4. *Presenza [**Presence**],*
5. *Effetto [**Effect**] e*
6. *Processi in Corso [**Ongoing Processes**].*

Ciascuna delle fasi consiste in una serie di Obiettivi avversari e ogni Obiettivo avversario è raggiunto da una o più Azioni.

N.1 - ARCHITETTURA E PROGETTAZIONE DELLA SICUREZZA

I seguenti principi di progettazione strutturale influenzano l'architettura fondamentale del sistema, ciò include il modo in cui il sistema viene scomposto nei suoi elementi costitutivi, come gli elementi del sistema si relazionano tra loro e la natura delle interfacce tra gli elementi.

PRINCIPIO DI "CONCETTI CHIARI"

«Un sistema dovrebbe avere interfacce e funzioni semplici e ben definite che forniscano una visione coerente e intuitiva dei dati e di come essi sono gestiti»

Lo stile (ad es. chiarezza, semplicità, necessità, sufficienza) delle interfacce del sistema, combinato con una definizione precisa del loro comportamento funzionale, facilita l'analisi, l'ispezione e il collaudo, nonché l'uso corretto e sicuro del sistema.

DEFINIZIONE

«Nascondere le informazioni, chiamato anche **Programmazione indipendente dalla rappresentazione**, è una disciplina di progettazione per garantire che la rappresentazione interna delle informazioni, in un componente di sistema, **non sia visibile** a un altro componente di sistema che invoca o chiama il primo gestito internamente»

N.1.2 - LEAST COMMON MECHANISM [LCM]

PRINCIPIO DI LCM

«La quantità di meccanismi comuni a più di un utente, e da cui dipendono tutti gli utenti, dovrebbe essere ridotta al minimo [Popek74]»

Implica che componenti diversi di un sistema dovrebbero astenersi dall'utilizzare lo stesso meccanismo per accedere a una risorsa di sistema.

Secondo Saltzer75: "Ogni meccanismo condiviso (in particolare uno che coinvolge variabili condivise) rappresenta un potenziale percorso informativo tra gli utenti e deve essere progettato con grande cura per essere sicuro che non comprometta involontariamente la sicurezza."

L'implementazione del principio del LCM aiuta ridurre le conseguenze negative della condivisione dello stato del sistema tra diversi programmi.

Un singolo programma che corrompe uno stato condiviso (comprese le variabili condivise) ha il potenziale per corrompere altri programmi che dipendono dallo stato.

Il principio del meccanismo meno comune supporta anche la semplicità di progettazione e affronta il problema dei canali di archiviazione nascosti [Lampson73].

N.1.3 - MODULARITÀ E STRATIFICAZIONE

La modularità serve a isolare le funzioni e le relative strutture dati in unità logiche ben definite.

La stratificazione consente di comprendere meglio le relazioni di queste unità, in modo che le dipendenze siano chiare e la complessità indesiderata possa essere evitata.

Il principio di modularità della progettazione della sicurezza estende la modularità funzionale per includere considerazioni basate sulla fiducia, affidabilità, privilegio e politica di sicurezza.

La scomposizione modulare informata sulla sicurezza include quanto segue:

1. *assegnazione di politiche ai sistemi in una rete;*
2. *assegnazione delle politiche di sistema ai livelli; separazione delle applicazioni di sistema in processi con spazi di indirizzamento distinti; e*
3. *separazione dei processi in soggetti con privilegi distinti basati su domini di privilegi supportati dall'hardware.*

I principi di modularità e stratificazione della sicurezza non sono gli stessi del concetto di difesa in profondità, che è discusso nella sezione N.1.4.

N.1.4 - DIPENDENZE PARZIALMENTE ORDINATE

PRINCIPIO DELLE DIPENDENZE PARZIALMENTE ORDINATE

«La chiamata, la sincronizzazione e altre dipendenze nel sistema dovrebbero essere parzialmente ordinate.»

DEFINIZIONE DI STRATIFICAZIONE

«Un concetto fondamentale nella progettazione del sistema è la stratificazione, in base alla quale il sistema è organizzato in moduli o componenti ben definiti e funzionalmente correlati.»

Gli strati sono ordinati in modo lineare rispetto alle dipendenze inter-strato, in modo tale che gli strati superiori dipendono dagli strati inferiori.

Dipendenze parzialmente ordinate e stratificazione del sistema contribuiscono in modo significativo alla semplicità e alla coerenza della progettazione del sistema.

Le dipendenze parzialmente ordinate facilitano anche test e analisi del sistema.

N.1.5 - EFFICIENTLY ACCESS MEDIA [EAM]

PRINCIPIO DI EAM

«Accesso mediato in modo efficiente [EAM] stabilisce che i meccanismi di attuazione delle politiche dovrebbero utilizzare il meccanismo meno comune disponibile, soddisfacendo al contempo i requisiti delle parti interessate entro i limiti espressi.»

La mediazione (Riduzione o impedimento – nd autore) dell'accesso alle risorse di sistema (ad es. CPU, memoria, dispositivi, porte di comunicazione, servizi, infrastruttura, dati e informazioni) è spesso la funzione di sicurezza predominante dei sistemi sicuri.

Consente inoltre la realizzazione di protezioni degli stakeholder.

Una volta ottenuto l'accesso ad una risorsa di basso livello come la memoria, i meccanismi di protezione dell'hardware possono garantire che non si verifichi un accesso fuori limite.

N.1.6 - CONDIVISIONE MINIMIZZATA

PRINCIPIO DELLA CONDIVISIONE MINIMIZZATA

«Nessuna risorsa informatica dovrebbe essere condivisa tra i componenti del sistema (ad es. soggetti, processi, funzioni) a meno che non sia assolutamente necessario farlo.»

La condivisione minimizzata aiuta a semplificare la progettazione e l'implementazione, per proteggere le risorse del dominio utente da entità attive arbitrarie, in tal modo nessuna risorsa deve essere condivisa a meno che tale condivisione non sia stata esplicitamente richiesta e concessa.

La condivisione tramite un meccanismo unico può aumentare la predisposizione di dati e informazioni all'accesso, alla divulgazione, all'uso o alla modifica non autorizzati e può influire negativamente sulla capacità intrinseca fornita dal sistema.

N.1.7 - COMPLESSITÀ RIDOTTA

PRINCIPIO DELLA COMPLESSITÀ RIDOTTA

«La progettazione del sistema dovrebbe essere il più semplice e piccola possibile. Un design piccolo e semplice sarà più comprensibile, più analizzabile e meno soggetto a errori.»

Questo principio si applica a qualsiasi aspetto di un sistema, ma ha particolare importanza per la sicurezza a causa delle varie analisi eseguite per ottenere prove della proprietà di sicurezza emergente del sistema. Perché tali analisi abbiano successo, è essenziale un design piccolo e semplice.

L'applicazione del principio di complessità ridotta o contenuta contribuisce alla capacità degli sviluppatori di sistemi di comprendere la correttezza e la completezza delle funzioni di sicurezza del sistema.

N.1.8 - EVOLVIBILITÀ SICURA

PRINCIPIO DELLA EVOLVIBILITÀ SICURA

«Un sistema dovrebbe essere sviluppato per facilitare il mantenimento delle sue proprietà di sicurezza in caso di modifiche alla sua struttura funzionale, alle interfacce ed alle interconnessioni (o alla sua configurazione delle funzionalità (ad es. applicazione di politiche di sicurezza)»

Queste modifiche possono includere ad esempio: funzionalità di sistema nuove, migliorate e aggiornate; attività di manutenzione e assistenza; riconfigurazione.

Non è realistico aspettarsi che sistemi complessi rimangano sicuri in contesti non previsti durante lo sviluppo, indipendentemente dal fatto che tali contesti siano collegati all'ambiente operativo o all'utilizzo.

Un sistema può essere sicuro in alcuni nuovi contesti, ma non vi è alcuna garanzia che il suo comportamento emergente sia sempre sicuro.

Fin dall'inizio è più facile costruire l'affidabilità in un sistema e ne consegue che il mantenimento dell'affidabilità del sistema richieda la pianificazione del cambiamento anziché l'adattamento in modo ad-hoc o non metodico.

I vantaggi di questo principio includono costi ridotti per il ciclo di vita del fornitore; costi di gestione ridotti; miglioramento della sicurezza del sistema; più efficace del rischio per la sicurezza; meno incertezza del rischio.

N.1.9 - COMPONENTI AFFIDABILI

PRINCIPIO DEI COMPONENTI AFFIDABILI

«Un componente deve essere affidabile per almeno un livello commisurato alle dipendenze di sicurezza che supporta (ovvero, quanto è attendibile per eseguire le sue funzioni di sicurezza da altri componenti).»

Questo principio consente la composizione di componenti in modo tale che l'affidabilità non venga inavvertitamente diminuita e, di conseguenza, la fiducia non sia mal riposta.

In definitiva questo principio richiede una metrica in base alla quale la fiducia in un componente e l'affidabilità di un componente possano essere misurate sulla stessa scala astratta.

Il principio si applica anche a un componente composto costituito da diversi sotto componenti (ad esempio un sottosistema), che può avere livelli variabili di affidabilità.

L'ipotesi prudente è che l'affidabilità globale di un componente composto sia quella del suo sotto componente meno affidabile.

N.1.10 - TRUST GERARCHICO

PRINCIPIO DEL TRUST GERARCHICO

«Si basa sul principio dei componenti attendibili. Afferma che le dipendenze di sicurezza in un sistema formeranno un ordinamento parziale se mantengono il principio dei componenti affidabili (Trust).»

L'ordinamento parziale fornisce la base per il ragionamento di affidabilità quando si compone un sistema sicuro da componenti eterogenei e affidabili.

Per poter analizzare un sistema composto da componenti eterogenei e affidabili per la sua affidabilità complessiva, è essenziale eliminare le dipendenze circolari in termini di affidabilità.

*Se un componente più affidabile situato in uno strato inferiore del sistema dovesse dipendere da un componente meno affidabile in uno strato superiore, ciò renderebbe effettivamente i componenti nella stessa classe di equivalenza "**meno affidabile**" in base al principio dei componenti affidabili.*

N.1.11 - SOGLIA DI MODIFICA INVERSA

PRINCIPIO DELLA SOGLIA DI MODIFICA INVERSA

«Si basa sul principio dei Componenti Affidabili e sul principio del Trust Gerarchico. Afferma che il grado di protezione fornito a un componente deve essere commisurato alla sua affidabilità. All'aumentare della fiducia riposta in un componente, anche la protezione da modifiche non autorizzate del componente dovrebbe aumentare allo stesso livello.»

Questa protezione può presentarsi sotto forma di autoprotezione e affidabilità innata del componente o da protezioni fornite al componente da altri elementi o attributi dell'architettura (per includere protezioni nell'ambiente operativo).

N.1.12 - PROTEZIONE GERARCHICA

PRINCIPIO DELLA PROTEZIONE GERARCHICA

«Un componente non deve essere protetto da componenti più affidabili.»

Il componente più affidabile, deve proteggersi da tutti gli altri componenti. Ad esempio, se un kernel del sistema operativo è considerato il componente più affidabile in un sistema, allora deve proteggersi da tutte le applicazioni non attendibili che supporta, ma le applicazioni, al contrario, non devono proteggersi dal kernel.

L'affidabilità degli utenti è una considerazione per l'applicazione del principio di protezione gerarchica.

Un sistema informatico affidabile non deve proteggersi da un utente altrettanto affidabile (TRUST ZERO!).

N.1.13 - ELEMENTI DI SICUREZZA RIDOTTI AL MINIMO

PRINCIPIO DEGLI ELEMENTI DI SICUREZZA MINIMIZZATI

«Il sistema non dovrebbe avere componenti affidabili estranei.»

Questo principio ha due aspetti:

1° costo complessivo dell'analisi della sicurezza;

2° complessità dell'analisi della sicurezza.

I componenti affidabili sono generalmente più costosi da costruire, a causa del maggiore rigore dei processi di sviluppo.

Richiedono inoltre una maggiore analisi della sicurezza per qualificare la loro affidabilità.

L'analisi dell'interazione di componenti affidabili con altri componenti del sistema è uno degli aspetti più importanti della verifica della sicurezza del sistema. Se queste interazioni sono inutilmente complesse, la sicurezza del sistema sarà anche più difficile da accertare di quella le cui relazioni di fiducia interna sono semplici ed elegantemente costruite.

In generale, un minor numero di componenti attendibili comporterà un minor numero di relazioni di fiducia interne e un sistema più semplice.

N.1.14 - MINIMO PRIVILEGIO

PRINCIPIO DEL MINIMO PRIVILEGIO

«A ciascun componente dovrebbero essere assegnati privilegi sufficienti per svolgere le sue funzioni specificate, ma non di più. Ciò limita la portata delle azioni del componente, che ha due effetti desiderabili:

1) l'impatto sulla sicurezza di un guasto;
2) corruzione o uso improprio del componente avrà un impatto sulla sicurezza ridotto al minimo;
3) l'analisi della sicurezza del componente sarà semplificata.»

Il minimo privilegio è un principio pervasivo che si riflette in tutti gli aspetti della progettazione del sistema sicuro.

Le interfacce utilizzate per invocare la capacità dei componenti dovrebbero essere disponibili solo per determinati sottoinsiemi della popolazione di utenti e la progettazione dei componenti dovrebbe supportare una granularità sufficientemente per la decomposizione dei privilegi.

Può essere usato come principio guida per la struttura interna del sistema stesso.

Costruire moduli in modo che solo gli elementi incapsulati dal modulo siano gestiti direttamente dalle funzioni all'interno del modulo.

Un determinato modulo o componente dovrebbe includere solo quegli elementi di sistema necessari alla sua funzionalità e anche le modalità (ad es. lettura, scrittura) dovrebbero essere minime.

N.1.15 - AUTORIZZAZIONE DICHIARATA

PRINCIPIO DELLA AUTORIZZAZIONE DICHIARATA

«I progettisti di sistemi dovrebbero prendere in considerazione la necessità di richiedere, a più entità autorizzate, di fornire il consenso prima che un'operazione autorizzata oppure l'accesso ai dati, a informazioni, a risorse altamente sensibili possa procedere.»

La divisione dei privilegi tra più parti riduce la probabilità di abusi e garantisce che nessun singolo incidente, inganno o violazione della fiducia sia sufficiente a consentire un'azione irrecuperabile che può portare a conseguenze significativamente dannose.

N.1.16 - AFFIDABILITÀ AUTOSUFFICIENTE

PRINCIPIO DELL'AFFIDABILITÀ AUTOSUFFICIENTE

«I sistemi dovrebbero ridurre al minimo la dipendenza da altri sistemi per la propria affidabilità.»

Un sistema (risorse hw e sw e processi) dovrebbe essere affidabile per impostazione predefinita (in stretta correlazione con l'articolo 25 del Reg. UE 2016/679) con qualsiasi connessione a un'entità esterna utilizzata per integrare la sua funzione.

Se un sistema fosse tenuto a mantenere una connessione con un'altra entità esterna al fine di mantenerne l'affidabilità, quel sistema sarebbe vulnerabile alle minacce che potrebbero causare la perdita o il degrado di tale connessione.

Il vantaggio di questo principio è che l'isolamento di un sistema lo renderà meno vulnerabile agli attacchi.

Un corollario di questo principio riguarda la capacità del sistema (o dell'elemento di sistema) di operare in modo isolato e quindi risincronizzarsi con altri componenti quando si ricongiunge con essi.

N.1.17 - STRUTTURA DISTRIBUITA SICURA

PRINCIPIO DELLA STRUTTURA DISTRIBUITA SICURA

«L'insieme dei componenti distribuiti, che applicano la stessa politica di sicurezza, dovrebbe costituire un sistema che impone tale politica, così come i suoi singoli componenti.»

Molti dei principi di progettazione per sistemi sicuri riguardano il modo in cui i componenti possono o devono interagire.

La traduzione della politica di sicurezza da un sistema autonomo a un sistema distribuito o un sistema di sistemi può avere risultati imprevisti o emergenti.

I protocolli di comunicazione e i meccanismi di coerenza dei dati distribuiti aiutano a garantire che un'applicazione sia coerente alle politiche all'interno di un sistema distribuito.

Per confermare un livello di garanzia della corretta applicazione delle politiche, a livello di sistema, è necessario analizzare a fondo l'architettura di sicurezza di un sistema distribuito.

N.1.18 - CANALI DI COMUNICAZIONE AFFIDABILI

PRINCIPIO DEI CANALI DI COMUNICAZIONE AFFIDABILI

«Quando si compone un sistema, in cui esiste una potenziale minaccia alle comunicazioni tra i componenti, ciascun canale di comunicazione deve essere affidabile al livello commisurato alle dipendenze di sicurezza che supporta (ad es. quanto sia affidabile per gli altri componenti nell'eseguire le sue funzioni di sicurezza).»

Sono raggiunti da una combinazione di limitazioni dell'accesso al canale di comunicazione (per contribuire a garantire una corrispondenza accettabile nell'affidabilità degli endpoint coinvolti nella comunicazione) ed attraverso l'impiego di protezioni end-to-end per i dati trasmessi sul canale stesso (contribuire a proteggere dalle intercettazioni, modifiche ed aumentare ulteriormente la garanzia generale di una corretta comunicazione end-to-end).

Tabella H2: Struttura del quadro tecnico della ciber minaccia della NSA

STAGE	OBJECTIVE	ACTION
Administration	Planning Resource Development Research	*Examples of Research Actions* Gather information Identify capability gaps Identify information gaps
Preparation	Reconnaissance Staging	*Examples of Reconnaissance Actions* Conduct social engineering Scan devices Scrape websites
Engagement	Delivery Exploitation	*Examples of Delivery Actions* Alter communications path Send malicious email Use legitimate remote access
Presence	Execution Internal Recon Privilege Escalation Credential Access Lateral Movement Persistence	*Examples of Execution Actions* Create scheduled task Replace existing binary Write to disk
Effect	Monitor Exfiltrate Modify Deny Destroy	*Examples of Monitor Actions* Activate recording Log keystrokes
Ongoing Processes	Analysis, Evaluation, and Feedback Command and Control Evasion	*Examples of Evasion Actions* Block indicators on host Obfuscate data Remove toolkit

THE SECURE SOFTWARE DEVELOPMENT FRAMEWORK

[Rif. NIST SP 800-218]

Questo documento descrive una serie di pratiche fondamentali e valide per lo sviluppo di software sicuro chiamato SECURE SOFTWARE DEVELOPMENT FRAMEWORK (SSDF).

Le organizzazioni dovrebbero integrare la SSDF in tutte le loro pratiche di sviluppo software esistenti, esprimere i propri requisiti di sviluppo software sicuro a fornitori di terze parti utilizzando le convenzioni SSDF e acquisire software che soddisfi le pratiche descritte nella SSDF. L'utilizzo di SSDF aiuta le organizzazioni a soddisfare i seguenti consigli per lo sviluppo di software sicuro:

- ✓ *Le organizzazioni devono garantire che il personale, i processi e la tecnologia siano preparati per eseguire lo sviluppo di software sicuro.*
- ✓ *Le organizzazioni dovrebbero proteggere tutti i componenti del loro software da manomissioni e accessi non autorizzati.*
- ✓ *Le organizzazioni dovrebbero produrre software ben protetto con vulnerabilità di sicurezza minime nelle sue versioni.*
- ✓ *Le organizzazioni dovrebbero identificare le vulnerabilità residue nelle loro versioni software e rispondere in modo appropriato per affrontare tali vulnerabilità e prevenire che si verifichino simili in futuro.*

La SSDF non prescrive esattamente come implementare ciascuna pratica. L'attenzione si concentra sui risultati delle pratiche piuttosto che sugli strumenti, sulle tecniche e sui meccanismi per farlo.

Ciò significa che SSDF può essere utilizzato da organizzazioni di qualsiasi settore o comunità, indipendentemente dalle dimensioni o dalla complessità della sicurezza informatica. Può essere utilizzato per qualsiasi tipo di sviluppo software, indipendentemente dalla tecnologia, piattaforma, linguaggio di programmazione o ambiente operativo.

L'SSDF definisce solo un sottoinsieme di alto livello di ciò che le organizzazioni potrebbero dover fare, quindi le organizzazioni dovrebbero consultare i riferimenti e altre risorse per ulteriori informazioni sull'implementazione delle pratiche. Non tutte le pratiche sono applicabili a tutti i casi d'uso; le organizzazioni dovrebbero adottare un approccio basato sul rischio per determinare quali pratiche sono rilevanti, appropriate ed efficaci per mitigare le minacce alle loro pratiche di sviluppo software.

Un SOFTWARE DEVELOPMENT LIFE CYCLE (SDLC) *è una metodologia formale o informale per la progettazione, la creazione e la manutenzione del software (incluso il codice integrato nell'hardware).*

Esistono molti modelli per SDLC, tra cui a cascata, a spirale, agili e, in particolare, agili combinati con le pratiche di sviluppo software e operazioni IT (DevOps). Pochi modelli SDLC affrontano esplicitamente la sicurezza del software in dettaglio, quindi le pratiche di sviluppo del software sicuro di solito devono essere aggiunte e integrate in ogni modello SDLC.

Indipendentemente dal modello SDLC utilizzato, le pratiche di sviluppo software sicuro dovrebbero essere integrate in esso per tre motivi:

1°. *ridurre il numero di vulnerabilità nel software rilasciato,*

2°. *mitigare il potenziale impatto dello sfruttamento di vulnerabilità non rilevate o non indirizzate e*

3°. *affrontare alla radice le cause di vulnerabilità per prevenire le recidive.*

La maggior parte degli aspetti della sicurezza può essere affrontata più volte all'interno di un SDLC, ma in generale, ***prima nell'SDLC viene affrontata la sicurezza, minore è lo sforzo e il costo necessari per raggiungere lo stesso livello di sicurezza (prevenzione)****.*

*Questo principio, noto anche come "*SHIFTING LEFT*", è di fondamentale importanza indipendentemente dal modello SDLC. Lo spostamento a sinistra riduce al minimo qualsiasi debito tecnico che richiederebbe la correzione dei primi difetti di sicurezza in fase avanzata di sviluppo o dopo che il software è in produzione.*

Esistono molti documenti esistenti sulle pratiche di sviluppo software sicuro, inclusi quelli elencati nella sezione **Riferimenti**.

Questo documento non introduce nuove pratiche né definisce nuova terminologia; descrive invece una serie di pratiche consigliate di alto livello basate su standard stabiliti, linee guida e documenti sulle pratiche di sviluppo software sicuro.

Queste pratiche, denominate collettivamente SECURE SOFTWARE DEVELOPMENT FRAMEWORK (SSDF)*, hanno lo scopo di aiutare il pubblico di destinazione a raggiungere gli obiettivi di sviluppo del software sicuro.*

Inoltre, sono considerate fondamentali, valide e sicure basate su documenti di pratiche di sviluppo software sicuro stabilite.

Le pratiche sono organizzate in quattro gruppi:

1) PREPARE THE ORGANIZATION (PO): *le organizzazioni devono garantire che il personale, i processi e la tecnologia siano preparati per eseguire lo sviluppo di software sicuro a livello di organizzazione. Molte organizzazioni troveranno alcune pratiche PO applicabili anche a sottoinsiemi del loro sviluppo software sicuro, come singoli gruppi o progetti di sviluppo.*
2) PROTECT THE SOFTWARE (PS): *le organizzazioni devono proteggere tutti i componenti del software da manomissioni e accessi non autorizzati.*
3) PRODUCE WELL-SECURED SOFTWARE (PW): *le organizzazioni dovrebbero produrre software ben protetto con vulnerabilità di sicurezza minime nelle sue versioni.*
4) RESPOND TO VULNERABILITIES (RV): *le organizzazioni dovrebbero identificare le vulnerabilità residue nelle versioni del software e rispondere in modo appropriato per affrontare tali vulnerabilità e impedire che si verifichino simili in futuro.*

Ogni definizione di pratica include i seguenti elementi:

- ✓ **Practice***: il nome della pratica e un identificatore univoco, seguito da una breve spiegazione di cos'è la pratica e perché è vantaggiosa;*
- ✓ **Tasks***: una o più azioni necessarie per portare a termine una pratica;*
- ✓ **Implementation Examples***: uno o più esempi di tipi di strumenti, processi o altri metodi che potrebbero essere utilizzati per aiutare a implementare un'attività; non intende implicare che sia richiesto un esempio o una combinazione di esempi o che solo gli esempi indicati siano opzioni fattibili;*
- ✓ **Reference***: puntatori a uno o più documenti di pratiche di sviluppo sicuro stabilite e le loro mappature a un compito particolare; non tutti i riferimenti si applicano a tutte le istanze di sviluppo software.*

Le pratiche sono definite nella tabella 1 del NIST SP 800-218.

Esse sono solo un sottoinsieme di ciò che un'organizzazione potrebbe dover fare con le pratiche incentrate sull'aiutare le organizzazioni a raggiungere obiettivi di sviluppo software sicuro.

Le informazioni nella tabella sono limitate dallo spazio e molte più informazioni su ciascuna pratica possono essere trovate nei riferimenti.

Nota*: l'ordine delle pratiche e dei compiti nella tabella non intende implicare la sequenza di attuazione o l'importanza relativa di qualsiasi pratica o compito.*

CONFRONTO TRA SOLUZIONI TECNICHE DI TEST DELLA SICUREZZA

TRA RASP E WAF – 5 VANTAGGI RASP RISPETTO WAF

1 – TRASCURABILI I FALSI POSITIVI (FP)

RASP non produce molti falsi positivi, dal momento che non si basa su irregolarità del traffico di rete per produrre i suoi risultati.

A differenza di WAF, questa soluzione di sicurezza rimane in silenzio fino a quando la vulnerabilità è effettivamente sfruttato in tempo reale.

RASP riesce a distinguere con precisione tra le imprese e gli ingressi legittimi, qualcosa WAF non può fare.

Questo elimina la necessità di assumere personale dedicato per ordinare i risultati prima di essere trasmessi agli sviluppatori per la mitigazione. Il processo di bonifica è così notevolmente ridotta.

2 – SCARSI REQUISITI DI MANUTENZIONE

Implementare strumenti WAF è un processo complicato che richiede una configurazione accurata per coprire l'applicazione.

Per fornire risultati ottimali, la soluzione WAF deve essere "addestrato" con ogni nuova versione dell'applicazione web.

Spesso le organizzazioni hanno difficoltà nel tenere il passo con i cambiamenti e WAF rimanere non aggiornato. Questo porta a risultati non accurati e problemi di prestazioni.

Al contrario, RASP è una soluzione out–of–the–box che richiede poca o nessuna configurazione perché produce i risultati per il monitoraggio del flusso di dati all'interno dell'applicazione.

3 – UNA COPERTURA SUPERIORE E COMPATIBILITÀ

La sicurezza RASP può essere implementata all'interno di qualsiasi applicazione e può facilmente gestire una vasta gamma di protocolli di rete – HTTP, HTTPS, AJAX, SQL e SOAP.

D'altra parte, gli strumenti WAF sono limitati alle applicazioni Web che lavorano dal traffico rete di monitoraggio.

Inoltre, sono necessari parser specifici, i lettori di protocollo e simili add–on per rendere lo strumento WAF corrispondente al protocollo di rete specifico utilizzato dall'applicazione.

In molti casi, questo può causare una vasta gamma di problemi di compatibilità e prestazioni.

4 – PROTEZIONE PIÙ COMPLETA

I firewall di applicazioni Web (WAFs) sono efficaci per l'analisi ed il filtraggio dell'input dell'utente rilevando i modelli dannosi, ma non hanno la capacità di esaminare l'uscita dall'applicazione.

Runtime Application Self–Protection (RASP) non controlla solo l'ingresso, ma anche i modelli in uscita dai componenti dell'applicazione.

Questo dà a RASP il sopravvento nel rilevare una vasta gamma di problemi.

Le soluzioni RASP sono in grado di individuare gravi problemi che WAF di solito non riesce a rilevare: eccezioni non gestite, dirottamento di sessione, Privilege Escalation e sensibile diffusione dei dati.

5 – PUÒ ESSERE COMPLETAMENTE INTEGRATO CON SAST SOLUTIONS

RASP offre una perfetta integrazione con le soluzioni di SAST come Analisi Statica del Codice (SCA).

Questo consente alle organizzazioni di coprire l'intero spettro del ciclo di vita del prodotto, a partire dai primi anni di sviluppo fino alla post–produzione e alla distribuzione.

Gli strumenti WAF non possono competere con questa funzionalità, né possono fornire eventuali approfondimenti di bonifica.

UTILIZZO DI RASP CON SAST SI HANNO 2 VANTAGGI PRINCIPALI

I. VIRTUAL PATCHING

In molte occasioni le vulnerabilità presenti nel processo di sviluppo non vengono eliminati prima del rilascio a causa di vincoli di tempo e risorse.

Ma le organizzazioni possono ancora rilasciare questi prodotti, salvaguardando le potenziali lacune con RASP. L'applicazione è quindi sicuro da usare e può essere patchato / aggiornato in seguito secondo le esigenze.

II. MITIGAZIONE RAPIDA

Nel secondo scenario, le vulnerabilità rilevate dalla soluzione RASP possono essere situate in modo rapido sulla base delle scansioni precedentemente condotti da SAST.

Utilizzando RASP e SAST in tandem è estremamente utile in grandi e complesse applicazioni, dove i tempi di bonifica sono di grande importanza.

Questa funzionalità non è disponibile con WAF.

WAF è ancora uno strumento di sicurezza di tutto rispetto di post–produzione, ma i suoi difetti ereditari stanno portando le organizzazioni a prendere in considerazione altre alternative.

In ultima analisi il tramite di soluzioni RASP aumenta il sistema auto–immunitario dell'applicazione, le consente di reagire ad una vasta gamma di exploit, anche se i modelli dannosi riescono a infiltrarsi nelle difese.

Con le tecniche di hacking sempre più sofisticate, la sicurezza delle applicazioni deve anche evolversi e migliorare.

Utilizzando RASP insieme ad una soluzione SAST è senza dubbio la migliore combinazione 1–2 AppSec oggi.

TRA SAST E DAST

La sicurezza delle applicazioni usata per essere un ripensamento fino a pochi anni fa, ma l'aumento esponenziale della criminalità informatica e le attività dannose ha obbligato le organizzazioni a prestare maggiore attenzione a questo aspetto cruciale.

Questa presa di coscienza ha portato anche una discussione diffusa circa i pro ed i contro delle varie soluzioni AppSec che sono in offerta sul mercato.

Mentre Penetration (Pen) Testing, Interactive Application Security Testing (IAST) e Firewall di applicazioni Web (WAF) sono ampiamente riconosciute metodologie di sicurezza, tipicamente utilizzate come processi complementari con le due soluzioni in uso più comuni: Static Test Application Security (SAST) e Dynamic Application Security Testing (DAST).

SAST e DAST saranno confrontati sui 5 parametri di seguito elencati.

1. *Software Development Life Cycle (SDLC) Integrazione.*
2. *Continuous Integration distribuzione continua (CICD) Attuazione.*
3. *Vulnerabilità copertura e l'efficacia.*
4. *Mitigazione / Remediation Performance.*
5. *Ritorno dell'investimento (ROI).*

È SAST (White Box test) veramente efficace nel rilevare le vulnerabilità che si trovano comunemente di oggi? O è DAST (Black Box di prova) l'opzione migliore?

SVILUPPO SOFTWARE DEL CICLO DI VITA (SDLC)

La creazione di un ciclo di vita di sviluppo sicuro del software (SDLC) sta cominciando a diventare uno dei modi più completi a garantire Web sicuro e sviluppo di applicazioni mobile.

Ma i tre fondamentalmente diversi modelli realizzati in organizzazioni di sviluppo delle applicazioni principali di oggi sono in una grande sfida sul fronte della sicurezza.

a. *Cascata (Process Design sequenziale)*
b. *Agile / DevOps (Sviluppo iterativo)*
c. *Continuous Integration Development (CICD)*

Le grandi organizzazioni utilizzano spesso più di uno di questi, secondo le esigenze dei diversi team di sviluppo che lavorano al progetto.

SAST come SCA, hanno la flessibilità necessaria per eseguire in tutti i tipi di metodologie SDLC.

Inoltre, possono essere integrate direttamente nell'ambiente di sviluppo; questo permette agli sviluppatori di monitorare il loro codice costantemente.

Scrum Master e proprietari di prodotto in grado anche di regolare gli standard di sicurezza all'interno delle loro squadre e organizzazioni di sviluppo. Questo porta a rapida attenuazione di vulnerabilità e l'integrità del codice avanzato.

DAST, collaudo Black Box, è ideale per gli ambienti di Cascata, ma è inferiore nei metodi di sviluppo più avanzati per le sue limitazioni ereditate.

Gli strumenti DAST non possono essere utilizzati sul codice sorgente o codici applicativi uncomplied, ritardando l'utilizzo dei controlli della sicurezza nelle ultime fasi di sviluppo.

IMPLEMENTAZIONE CONTINUA SAST VS DAST QUANDO IMPLEMENTATA IN AMBIENTI (AGILE, DEVOPS)

La sicurezza del Continuous Integration inizia con la corretta applicazione della metodologia.

Continuous Integration (CI) di sicurezza sicuro e completo prevede le seguenti fasi: Scrums, repository del codice centralizzata, Build Automation, Revisione funzionalità di controllo, Automated Quality Assurance (QA) e il Code Consolation.

Static Application Security Testing (SAST) – Queste soluzioni, come ad esempio l'analisi del codice sorgente (SCA), sono pienamente in grado di coprire tutte le fasi del processo di CI.

Dall'analisi della sicurezza nelle riunioni giornaliere Scrum, attraverso la scansione automatica di codice repository fino al test dell'applicazione costruita. Ciò consente la diagnosi precoce e la mitigazione della vulnerabilità.

Nella metodologia CICD, il prodotto è in un stato di rilascio continuo.SAST è in grado di essere una soluzione per il test automatizzato, qualcosa che va di pari passo con CICD. Una volta che vengono rilevate le vulnerabilità, i team possono facilmente implementare le correzioni e, infine, la produzione di applicazioni robuste.

Dynamic Application Security Testing (DAST) – DAST è ancora una volta inferiore per le sue caratteristiche ereditarie, che gli consentono di iniziare a lavorare solo dopo il completamento della costruzione. Questo non è l'ideale per gli scenari di integrazione continua, in cui il codice è modificato con una certa frequenza e dove l'automazione è la chiave in quasi tutte le fasi di sviluppo.

VULNERABILITÀ E COPERTURA

Con l'evoluzione della criminalità informatica, le aziende hanno bisogno di soluzioni di sicurezza complete che può dare loro la massima copertura.

Le vulnerabilità più comuni, vale a dire SQLI, Cross–Site Scripting (XSS) e Cross–Site Request Forgery (CSRF) sono presenti in liste di riferimento migliori di oggi come gli errori OWASP Top–10 e SANS Top 25 Software.

La pirateria tradizionale ha comportato l'uso di Phishing o di tecniche semplici, ma la scena del crimine informatico è cambiato drasticamente negli ultimi anni. I pirati informatici oggi implementare tecniche più diverse e complesse che ingrandiscono l'importanza del codice dell'applicazione robusto con minime vulnerabilità prima del rilascio.

Static Application Security Testing (SAST) – Test White Box può aiutare ad analizzare sia sul lato server e le vulnerabilità lato client con alti tassi di successo. Inoltre il codice web / applicazione mobile solito, soluzioni SAST possono essere applicate a codificare anche in sistemi embedded e altre posizioni.

La maggior parte delle soluzioni di SAST sono pienamente compatibili con gli standard leader del settore quali:

Le suddette norme OWASP Top–10 e SANS Top 25 di sicurezza.

Payment Card Industry Data Security Standard (PCI DSS)

Health Insurance Portability e Accountability Act (HIPAA)

Motor Industry Software Reliability Association (MISRA)

Dynamic Application Security Testing (DAST) – gli strumenti di sicurezza DAST analizzano solo le richieste e le risposte. Ciò significa che le vulnerabilità nascoste come problemi di progettazione non sono rilevate. Inoltre, DAST individua numerose vulnerabilità non riflettenti (i.e – Cross–Site Scripting) che non generano un feedback in caso di attivazione.

MITIGAZIONE / BONIFICA

La scansione ed il collaudo dei progetti di piccole dimensioni sono in genere semplici e non richiedono troppa flessibilità della soluzione di sicurezza. Ma la realtà di oggi comporta grandi progetti con migliaia di LOC (linee di codice). Queste organizzazioni hanno decine o addirittura centinaia di team di sviluppatori che lavorano sulla costruzione l'applicazione.

Il problema con i grandi progetti è l'enorme numero di falsi positivi (FP). Le organizzazioni che implementano strumenti di sicurezza inefficaci devono assumere personale per prendersi cura del problema, prima che i processi di bonifica siano iniziati. Questo può causare enormi ritardi nei rilasci del prodotto ed essere molto pesante il rapporto costo / risorsa.

Static Application Security Testing (SAST) – Le grandi aziende di software in tutto il mondo stanno gravitando verso le configurazioni CICD, Agile e DevOps. Le soluzioni SAST hanno tutte le caratteristiche per fondersi in questi cicli di vita del software. Il codice può essere sottoposto a scansione veloce, le vulnerabilità sono individuate in modo accurato e il codice intatto non deve essere oggetto di ulteriori scansioni.

Dynamic Application Security Testing (DAST) – Mentre gli strumenti DAST forniscono le analisi dei rischi e assistono negli sforzi di bonifica, gli sviluppatori non sanno dove si trovano esattamente le vulnerabilità, non sapendo spesso quali contromisure implementare. Le segnalazioni della metodologia DAST sono meno soddisfacenti in numerosi casi.

Un altro svantaggio di fissare problemi di sicurezza dopo aver attivato l'applicazione è la sfida affrontata dagli sviluppatori. Le squadre responsabili per il codice devono rivisitare e si rifamiliarizzare con il codice prima di installarlo. Questo è un processo che richiede tempo, che può diventare ancora più complicato quando i nuovi lavoratori sono stati appena assunti.

RETURN OF INVESTMENT (ROI) CONFRONTANDO IL FATTORE "VALUE FOR MONEY" DELLE DUE METODOLOGIE.

Un altro aspetto importante è l'investimento richiesto dall'organizzazione.

Lo sviluppo di applicazioni Web e Mobile può rivelarsi un costo pesante, causando spesso una riduzione di investimenti sul fronte della sicurezza. Questo non è consigliato, come evidenziato nel infografica qui sotto.

Static Application Security Testing (SAST) – Test White Box considera bug di sicurezza fisse come bug generici, anche prima che il codice dell'applicazione venga compilato. Questo, insieme con il linguaggio di programmazione e la copertura ampia, facendo SAST una soluzione di sicurezza in grado di ridurre i tempi e i costi in modo significativo.

Dynamic Application Security Testing (DAST) – Oltre alle limitazioni del DAST quando si tratta di individuare le vulnerabilità nelle prime fasi del SDLC, ogni cambiamento del codice richiede anche una nuova scansione, qualcosa che può diventare un processo ingombrante, mentre lo sviluppo di grandi progetti (molti KLOCs), ostacolando in modo significativo il processo di bonifica.

TRA SAST E IAST

Con il Cybercrime crescente in tutto il mondo, la sicurezza delle applicazioni è diventata una grande sfida per le organizzazioni e governi.

Penetrazione (Pen) Testing e Dynamic Application Security Testing (DAST) sono soluzioni valide, ma hanno delle carenze.

Interactive Application Security Testing (IAST), una metodologia di sicurezza recente, è sempre più confrontata con la Static Application Security Testing (SAST).

SAST: GARANTIRE LA CREAZIONE DELL'APPLICAZIONE

Con l'aumento degli hacker con l'obiettivo di rilevare le vulnerabilità delle applicazioni, la crescente esigenza della sicurezza dovrebbe concentrarsi sull'origine: il codice sorgente.

Questo è dove Static Application Security Testing (SAST) entra in scena, consentendo la scansione rapida ed efficace del codice sorgente e rilevare i problemi prima ancora che si raggiunge la fase di costruzione dello sviluppo.

La Source Code Analysis (SCA), appartenente alla famiglia Static Application Security Testing (SAST), ha numerosi vantaggi.

È una soluzione out–of–the–box che è facile da installare e richiede poca o nessuna manutenzione.

L'attuazione è facile con i plugin di peso leggero che risiedono direttamente all'interno delle IDE, i repository di origine, per predisporre i server di gestione e gli strumenti di tracciamento dei bug.

Optando per SCA, le organizzazioni possono avviare il processo di sicurezza già in fase di sviluppo.

La scansione del codice sorgente permette la rapida identificazione di SQL Injections, Cross–Site Scripting (XSS) e altre vulnerabilità comuni che appaiono nelle principali liste di riferimento di sicurezza di oggi, come la OWASP Top–10 e SANS 25.

È anche facile da adattarsi alle norme specifiche di settore (PCI DSS, HIPAA, ecc).

INTERACTIVE APPLICATION SECURITY TESTING (IAST) SOURCE: ELSANE/GIMP

In poche parole, IAST è una combinazione tra SAST e Dynamic Application Security Testing (DAST).

Ma questa soluzione di sicurezza non è ancora matura al punto tale da poter essere confrontata con precisione con le soluzioni rivali.

Per come stanno le cose in questo momento, IAST può essere meglio definita come una "innovativa soluzione di sicurezza ibrida".

La natura di funzionamento è la simulazione di vari attacchi informatici con l'invio di diversi tipi di richieste.

L'innovazione consiste nel fatto che questa è una soluzione che in tempo reale ascolta dall'interno dell'applicazione con la capacità di rilevare attacchi non riflettenti (per esempio: XSS) a differenza DAST.

Mentre questa soluzione è unica nella sua capacità di fornire analisi in tempo reale degli attacchi, la sua efficacia varia in funzione della qualità della strumentazione.

Gli agent non sono facili da implementare in modo accurato ed in genere possono causare problemi con la stabilità, le prestazioni e la gestione.

Questi problemi tecnici sono ulteriormente complicati nelle grandi infrastrutture.

TRA SAST E IAST: 5 MOTIVI PER OPTARE PER SAST

UNA COPERTURA PIÙ AMPIA

Le simulazioni di attacco in tempo reale con le soluzioni IAST forniscono informazioni accurate, assumendo tutte le possibili combinazioni che sono state configurate ed eseguite, le quali sono difficili da raggiungere.

Anche nei miliori soluzioni, essi non possono eguagliare le prestazioni delle soluzioni di SAST, dove vi è pieno accesso sia al codice dell'applicazione sia a tutti i flussi di dati, i quali sono mappati per un efficace rilevamento delle vulnerabilità.

OVERHEAD LESSER

L'implementazione di una soluzione IAST è molto più complicata della funzionalità out–of–the–box offerta da SAST.

IAST richiede l'installazione di un agente nei nodi strategici per monitorare i dati e le istruzioni.

SAST non richiede strumentazione di sorta. Testare il codice dell'applicazione è semplice come il caricamento dei file, scegliendo la query desiderata e premendo il pulsante di scansione.

MIGLIORE COMPATIBILITÀ

L'organizzazione moderna consiste spesso di strutture di sviluppo complesse, con diverse piattaforme e framework.

Questo può complicare l'implementazione di soluzioni IAST, che richiede l'assunzione di personale dedicato per supervisionare l'installazione / manutenzione e apportare le modifiche di configurazione necessarie in caso di necessità. Con il Static Code Analysis (SCA) non vi è alcun problema del genere.

FORMAZIONE E SENSIBILIZZAZIONE

SAST ha il sopravvento in questa categoria in quanto consente il coinvolgimento di tutti gli sviluppatori nel processo di bonifica.

La soluzione è integrata nell'ambiente di sviluppo e permette l'esportazione dei risultati per il controllo e l'analisi esterni ai processi, migliorando le competenze degli sviluppatori nella codifica. Interactive Application Security Testing offre tale valore aggiunto.

DOPPIO COME UN (QA) SOLUZIONE DI QUALITY ASSURANCE

Grazie all'accesso diretto al codice dell'applicazione, le soluzioni SAST hanno la capacità di individuare difetti di codifica ed errori.

Questi problemi possono includere i casi di codice inutilizzato e altri errori logici che possono eventualmente portare a molti problemi di prestazioni (bug).

Questa funzionalità non solo aiuta il reparto QA, ma consente l'implementazione e manutenibilità dell'applicazione in modo uniforme.

TRA STATIC ANALYSIS E PEN TESTING

Penetration Testing (Pen Test) è stato a lungo lo strumento iniziale per le organizzazioni che cercavano di salvaguardare i loro applicazioni. Ma le tecniche di hacking in continua evoluzione stanno esponendo questa soluzione invecchiamento precoce.

Il Pen Testing è una metodologia che combina approcci manuali e automatici. Come suggerisce il nome, questa tecnica di test comporta fondamentalmente esperti di sicurezza software cercando di sfruttare il codice di applicazione con strumenti di hacking dedicati. I risultati vengono poi inviati alla sicurezza dell'organizzazione.

Questo metodo di prova basato sul rischio, di solito fornisce risultati accurati e report, ma è ben lungi dall'essere completo.

L'efficacia reale dipende dalla capacità del tester di pensare "fuori dagli schemi", come gli stessi test sono tipicamente basati su un elenco predeterminato di exploit noti. Spesso, questi database sono obsoleti e la creazione di un piano di test personalizzato richiede troppe risorse. Queste limitazioni danneggiano l'efficacia del test e spesso sono necessari ulteriori test.

TRA STATIC ANALYSIS E PEN TESTING: 7 MOTIVI PER SCEGLIERE SAST/SCA

RETURN OF INVESTMENT (ROI)

Pen Testing è un processo che deve essere eseguito in più cicli per essere veramente efficace come soluzione di sicurezza. Ulteriori problemi con questa metodologia: il costo elevato; il test può iniziare soltanto dopo che l'applicazione è stata sviluppata e funzionante. Questo significa che se si trovano delle vulnerabilità, per il rilascio devono essere affrontati ritardi e problemi.

Nonostante che il Pen Testing è richiesto come un regolamento in molti settori, le organizzazioni che desiderano implementarlo come loro principale linea di difesa, devono prendere in considerazione le ripercussioni finanziarie ed i problemi tecnici (i.e – Versione rollback) che possono sorgere.

SAST offre una migliore ROI dal momento che entra in gioco all'inizio della fase di sviluppo e cattura le vulnerabilità in anticipo con rapida rimozione.

SAST deve essere acquistato e implementato solo una volta.

Pen Testing deve essere pagato prima di ogni ciclo di test e la rende una costosa proposta.

POCA O NESSUNA MANODOPERA NECESSARIA

Pen Testing viene in genere per dipendenti dedicati.

BONIFICA PIÙ VELOCE

Le soluzioni SAST sono spesso raccomandate per le organizzazioni che cercano una rapida bonifica della vulnerabilità. Il motivo principale alla base di questo è la capacità di individuare la posizione della vulnerabilità (pin–point) raccomandando le Best Fix Locations, che permettono l'eliminazione di difetti multipli con una correzione. Pen Testing non offre nessuno di questi benefici.

Pen Testing può richiedere giorni e addirittura settimane, quando sono in fase di sperimentazione grandi progetti. Ad esempio, il Pen Testing di 20 pagine Web richiede in genere circa 3 settimane di lavoro in media. E i problemi non finiscono qui. Gli sviluppatori hanno spesso reimparare il codice, un processo che può richiedere molto più tempo quando nuovi sviluppatori sono assunti dall'organizzazione.

Con SAST i risultati dei test sono disponibili quasi in tempo reale, con i risultati accessibili anche prima della scansione. Questo può essere estremamente importante durante la prova di progetti di grandi dimensioni con diversi KLOCs.

MIGLIORE PRECISIONE

Come spiegato in precedenza, il Pen Testing è solo efficace come il tester e gli strumenti che ha a sua disposizione.

Spesso la conoscenza di base della vulnerabilità che usa il tester è obsoleta e incompleta, ciò comporta falsi negativi (FN), rendendo il test inefficace.

Il Pen Testing inoltre non ha accesso al codice dell'applicazione, ostacolando la visibilità della vulnerabilità.

SAST è uno strumento di sicurezza in grado di eseguire la scansione del codice dell'applicazione senza sforzo e fornire i risultati ancor prima che la scansione sia completata.

Alcune soluzioni offrono anche una funzionalità open–query per personalizzare ulteriormente il test con specifiche esigenze delle aziende e ridurre al minimo la comparsa di falsi positivi (FP).

VALORE EDUCATIVO PER GLI SVILUPPATORI

SAST ha consente il coinvolgimento di tutti gli sviluppatori nel processo di bonifica. La soluzione è integrata nell'ambiente sviluppo e permette l'esportazione del ritrovamento degli errori attraverso controllo / analisi offline, migliorando le competenze dello sviluppatore nelle pratiche di codifica sicure. Pen Testing non offre tale valore aggiunto.

POSSONO ESSERE INTEGRATI NEL PROCESSO DI SVILUPPO

Le soluzioni SAST sono considerate le migliori quando si tratta di integrarle nel processo di sviluppo del software. Oltre ai vantaggi di ROI questo permette di ridurre sensibilmente il carico di lavoro del personale della sicurezza e gli sviluppatori.

D'altra parte, Pen Testing entra in funzione solo quando l'applicazione è in esecuzione, uno svantaggio questo importante che può comportare ritardi nel rilascio del prodotto.

QA FUNZIONALITÀ

SAST ha la possibilità di svolgere le diverse attività correlate QA con le sue caratteristiche di analisi approfondite rilevando errori di codifica, di logica inutilizzati, funzioni che aiutano a eliminare i bug di prestazioni e problemi di stabilità. Questa funzionalità aggiuntiva è sostanzialmente esclusiva di SAST.

Implementando SAST in fase di sviluppo, l'organizzazione può semplicemente evitare di essere trascinato in più cicli di Pen Testing e rischiare ritardi nella consegna. La stragrande maggioranza delle vulnerabilità sono già eliminate nel momento in cui viene raggiunta la realizzazione, permettendo un agevole rilascio sul mercato.

TRA SAST E WAF – 5 MOTIVI PER OPTARE PER SAST

Con l'industrializzazione della criminalità informatica e aumento di hacking di gravità, il valore delle tecniche di sicurezza delle applicazioni tradizionali sta implodendo. Il Web Application Firewall (WAF), considerato come un go–to di sicurezza soluzione fino a non molto tempo fa, sta vivendo una costante erosione nella sua efficacia. D'altra parte, Static Application Security Testing (SAST) soluzioni stanno guadagnando slancio.

Come suggerisce il nome, il **Web Application Firewall (WAF)** *è fondamentalmente una barriera di sicurezza (plug–in server o basato su cloud) che si trova di fronte alla richiesta di ispezione in tempo reale delle richieste degli utenti. Ciò comporta il monitoraggio del traffico sito web con la possibilità di bloccare quando dannoso attività è rilevata, come richiesto dalla specifica organizzazione.*

Se correttamente configurato, WAF è in grado di localizzare le iniezioni di codice (iniezioni SQL / LDAP, XSS, ecc) e altre vulnerabilità. Supponendo che i parametri dello strumento sono state configurate in modo accurato, gli attacchi possono essere rilevati o bloccati. Tutto il traffico di rete dal livello OSI fino al livello di applicazione può essere monitorato con WAF.

WAF può essere implementata in due modi – modalità blocco e la modalità Detect.

1. *Modalità Blocco: le minacce vengono bloccate in "tempo reale", le patch temporanee vengono applicate e le successive richieste provenienti dalla stessa fonte sono tutte contrassegnate come dannoso.*
2. *Modalità Detect: è una modalità di "monitoraggio", dove il personale di sicurezza viene avvisato ogni volta che viene rilevato attività dannose.*

STATIC APPLICATION SECURITY TESTING (SAST)

SAST ha un approccio più diretto perché si concentra sul codice sorgente.

Questa soluzione di sicurezza comporta fondamentalmente l'integrazione della scansione dei codici statico in tutte le fasi del ciclo di vita di sviluppo del software (SDLC).

Acquisendo anche parti di codice sorgente, il processo di bonifica diventa veloce ed efficace.

Tra SAST e Secure SDLC in genere comporta 6 tappe: analisi, progettazione, codifica, test, implementazione e manutenzione.

Questo tipo di scenario è idealmente creato da abbracciare Continuous Integration (CICD) o comunemente attuate metodologie di sviluppo iterativo, come Agile o DevOps. Test SAST si mescola perfettamente con questi ambienti, grazie al suo peso leggero plugin per IDE.

Un grande vantaggio SAST ha oltre WAF è la capacità di pin–point vulnerabili junctions nel codice dell'applicazione. Ad esempio, analisi del codice sorgente (SCA), dalla metodologia SAST, permette agli sviluppatori di accelerare in modo significativo gli sforzi di risanamento di fissaggio diverse vulnerabilità con un numero minimo di correzioni. SAST, inoltre, non ri–scansione del codice invariato, con conseguente tempi di test più veloci.

TRA SAST E WAF – PERCHÉ SAST È L'OPZIONE MIGLIORE

TOTAL COST OF OWNERSHIP

Le soluzioni SAST possono essere installati rapidamente e richiedono poca o nessuna manutenzione. Il codice viene analizzato automaticamente dopo ogni commit come parte del SDLC e risultati sono generati secondo le esigenze. Non è il caso di WAF, dove personale dedicato deve configurare costantemente ed ottimizzare lo strumento per assicurarsi che sta producendo ottimi risultati.

L'implementazione WAF richiede anche del personale per risolvere il FPs e trasmettere le vulnerabilità agli sviluppatori. I problemi di bonifica possono anche sorgere quando gli sviluppatori non hanno familiarità con la struttura del codice di applicazione.

MIGLIORARE IL ROI

SAST è l'opzione migliore quando si tratta di bonifica nello sviluppo e nella costruzione di fase. Ciò consente di far risparmiare all'organizzazione tempo, denaro e risorse, riducendo al minimo la necessità di patch post–release e aggiornamenti di sicurezza. WAF può iniziare a lavorare solo dopo che l'applicazione è stata installata e funzionante. Il risparmio per difetto con SAST possono ammontare a migliaia di dollari.

I FALSI POSITIVI NON INCIDONO SULLE PRESTAZIONI

Mentre si può affermare quale dei due produce più falsi positivi, SAST ha di nuovo il vantaggio.

L'occasionale falso positivo tilevati nella scansione del codice nel ciclo di sviluppo è un problema che può essere affrontato con facilità, ma tale situazione con WAF non è fattibile perché se WAF produce un FP in "tempo reale", l'utente sarà bloccato e non potrà utilizzare l'applicazione.

VATAGGI DELLA FORMAZIONE E MIGLIORAMENTO DEGLI STANDARD DI CODIFICA

Nell'attuare SAST i team di sviluppo e i team di test possono far parte del processo di convalida della protezione. Questo migliora le capacità di codifica dello sviluppatore e promuove la consapevolezza AppSec.

Con WAF le uniche persone coinvolte nel processo sono il team della sicurezza. Gli sviluppatori sono tenuti fuori dal giro e non vi è nessuna tendenza di miglioramento effettivo negli standard di codifica per la sicurezza.

NON SI LIMITA SOLO ALLE APPLICAZIONI WEB

A differenza di WAF, ke soluzioni SAST sono in grado di testare applicazioni web complesse.

L'analisi statica del codice è ugualmente efficace nella scansione di sistemi in tempo reale, applicazioni mobili e software su dispositivi embedded.

SAST può essere utilizzato anche in un processo sequenziale di progettazione (cascata) in cui pezzi di codice devono essere testati.

STANDARD PCI DSS, OWASP E CWE SANS A CONFRONTO

PCI DSS	*OWASP*	*CWE SANS*
***A** – Card–not–present merchants (e–commerce or mail/telephone–order), that have fully outsourced all cardholder data functions to PCI DSS compliant third–party service providers, with no electronic storage, processing, or transmission of any cardholder data on the merchant's systems or premises.*	***A1** – Injection*	***CWE–89 –** Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')*
***A–EP** – E–commerce merchants who outsource all payment processing to PCI DSS validated third parties, and who have a website(s) that doesn't directly receive cardholder data but that can impact the security of the payment transaction. No storage, processing, or transmission of cardholder data on merch systems or premises.*	***A2** – Broken Authentication and Session Management*	***CWE–78 –** Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')*
***B** – Merchants using only:* ➢ *Imprint machines with no electronic cardholder data storage, and/or* ➢ *Standalone, dial–out terminals with no electronic cardholder data storage.*	***A3** – Cross–Site Scripting (XSS)*	***CWE–120 –** Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')*
***B–IP** – Merchants using only standalone, PTS–approved payment terminals with an IP connection to the payment processor with no electronic cardholder data storage.*	***A4** – Insecure Direct Object References*	***CWE–79 –** Improper Neutralization of Input During Web Page Generation ('Cross–site Scripting')*
***C–VT** – Merchants who manually enter a single transaction at a time via a keyboard into an Internet–based, virtual payment terminal solution that is provided and hosted by a PCI DSS validated third party service provider. No electronic cardholder data storage.*	***A5** – Security Misconfiguration*	***CWE–306 –** Missing Authentication for Critical Function*
***C** – Merchants with payment application systems connected to the Internet, no electronic cardholder data storage.*	***A6** – Sensitive Data Exposure*	***CWE–862 –** Missing Authorization*
***P2PE** – Merchants using only hardware payment terminals included in and managed via a validated, PCI SSC–listed P2PE solution, with no electronic cardholder data storage.*	***A7** – Missing Function Level Access Control*	***CWE–798 –** Use of Hard–coded Credentials*

PCI DSS	OWASP	CWE SANS
***D* – SAQ D for Merchants:** *All merchants not included in descriptions for the above SAQ types.*	***A8** – Cross–Site Request Forgery (CSRF)*	***CWE–311 –** Missing Encryption of Sensitive Data*
***D* – SAQ D for Service Providers:** *All service providers defined by a payment brand as eligible to complete an SAQ.*	***A9** – Using Components with Known Vulnerabilities*	***CWE–434 –** Unrestricted Upload of File with Dangerous Type*
	***A10** –Unvalidated Redirects and Forwards*	***CWE–807 –** Reliance on Untrusted Inputs in a Security Decision*
	Clickjacking	***CWE–250 –** Execution with Unnecessary Privileges*
	Concurrency Flaws	***CWE–352 –** Cross–Site Request Forgery (CSRF)*
	Denial of Service	***CWE–22 –** Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')*
	Expression Language Injection (CWE–917)	***CWE–494 –** Download of Code Without Integrity Check*
	Information Leakage and Improper Error Handling	***CWE–863 –** Incorrect Authorization*
	Insufficient Anti–automation (CWE–799)	***CWE–829 –** Inclusion of Functionality from Untrusted Control Sphere*
	Insufficient Logging and Accountability	***CWE–732 –** Incorrect Permission Assignment for Critical Resource*
	Lack of Intrusion Detection and Response	***CWE–676 –** Use of Potentially Dangerous Function*
	Malicious File Execution	***CWE–327 –** Use of a Broken or Risky Cryptographic Algorithm*
	Mass Assignment (CWE–915)	***CWE–131 –** Incorrect Calculation of Buffer Size*
	User Privacy	***CWE–307 –** Improper Restriction of Excessive Authentication Attempts*
		***CWE–601 –** URL Redirection to Untrusted Site ('Open Redirect')*
		***CWE–134 –** Uncontrolled Format String*
		***CWE–190 –** Integer Overflow or Wraparound*
		***CWE–759 –** Use of a One–Way Hash without a Salt*

L'UE E LA CYBERSECURITY

3 – LA MODALITÀ D'INTERVENTO – LEGGE / TECNOLOGIA

LEGGE

ART. 25 - PROTEZIONE DEI DATI FIN DALLA PROGETTAZIONE E PROTEZIONE PER IMPOSTAZIONE PREDEFINITA

§1 dice: ... sia al momento di determinare i mezzi del trattamento (**software di «qualità»**) sia all'atto del trattamento stesso (**procedure online o batch**) il titolare del trattamento mette in atto misure tecniche e organizzative adeguate, quali la pseudonimizzazione, volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione (**storicizzazione -vedi considerando 156**) ..

§2 dice: Il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità (**profili**) del trattamento ....

§3 dice: Un meccanismo di certificazione approvato ai sensi dell'articolo 42 può essere utilizzato come elemento per dimostrare la conformità ai requisiti di cui ai paragrafi 1 e 2 del presente articolo

ART. 32 - SICUREZZA DEL TRATTAMENTO (USO DI SISTEMI SOFTWARE + HARDWARE)

*§1 dice: Tenendo conto dello stato dell'arte .... come anche del rischio (**art. 35 - PIA**) di varia probabilità e gravità .... il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio (**misure di attenuazione del danno e riduzione della probabilità**), ... se del caso...*

a) la pseudonimizzazione e la cifratura dei dati personale

SISTEMA

1. Mezzi del trattamento (**software di «qualità»**) - procedure per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche (software) e organizzative sia nel ciclo di vita del software in ambiente di Sviluppo sia in Esercizio al fine di garantire la sicurezza del trattamento:
   a. la riduzione o l'annullamento della vulnerabilità ***(es.: istruzioni del sorgente)*** con strumenti di:
      - *Change Management Ciclo di vita del sw*:
        - analisi STATICA (STATIC APPLICATION SECURITY TESTING)
        - test DINAMICO (DYNAMIC APPLICATION SECURITY TESTING)
        - test PT (PENETRATION TESTING)
        - test INTERATTIVO (INTERACTIVE APPLICATION SECURITY TESTING)
   b. strumenti di Controllo Qualità Sicurezza (fisica e logica): simulazione degli attacchi e delle violazioni BAS (BREACH AND ATTACK SIMULATION)
      - *Sicurezza perimetrale dall' esterno e dall' interno*:
        - protezione RUNTIME (RUNTIME APPLICATION SELF PROTECTION)
        - protezione del WEB (WEB APPLICATION FIREWALL)
   c. controllo accessi e profili utenze con strumenti di:
      - *Solo dati necessari e controllo anomalie o errori*:
        - identificazione e di controllo degli accessi
        - raccolta e di classificazione dei dati (impostazione predefinita)
        - analisi dei log e di monitoraggio
2. *Protezione dei dati*: Strumenti per la: Pseudonimizzazione, Minimizzazione, Cifratura

Pedico Aldo © - Teleion S.r.l via Ferrero 31 - 10098 Rivoli (TO) - Tel. 3482244924 – email: a.pedico@teleion.it 20

3 – La modalità d'intervento – Legge / Tecnologia

LEGGE

…… continua l'art. 32 ……

*b) la capacità di assicurare su base permanente la riservatezza (**controllo degli accessi 1° e 2° liv.…**), l'integrità (**alterazione**), la disponibilità (**Backup e Restore; sistemi di continuità**) e la resilienza dei sistemi (**SW + HW → BC o DR**) e dei servizi di trattamento (**BC e DR**)*

*c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico (**BC e DR**)*

*d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche (**SW + HW**) e organizzative (**ciclo di vita del SW -sviluppo e esercizio-: SW, processi e ruoli**) al fine di garantire la sicurezza del trattamento*

*§2 dice: … si tiene conto in special modo dei rischi presentati dal trattamento che derivano in particolare dalla distruzione (**loss**), dalla perdita (**loss**), dalla modifica (**loss**), dalla divulgazione (**leak; estrusione**) non autorizzata o dall'accesso (**leak; intrusione**), in modo accidentale o illegale, a dati personali trasmessi (**in movimento**), conservati (**a riposo**) o comunque trattati (**in uso**)* ***→ ATTENZIONE! → Introduzione dei processi per la gestione del DLP***

TECNOLOGIA

3. Disponibilità del dato: procedure e programmi di **Backup e Restore;** strumenti di **analisi dei log** e di **monitoraggio**
4. Resilienza dei sistemi SW, HD e servizi di trattamento: procedure e programmi di **Backup e Restore**, **strumenti di analisi dei log e di monitoraggio**
5. Incidente fisico o tecnico: procedure tecniche ed organizzative per la gestione della **Business Continuity** ed il **Disaster Recovery**
6. Distruzione (**loss**), Perdita (**loss**), Modifica (**loss**), Divulgazione (**leak; estrusione**) non autorizzata o Accesso (**leak; intrusione**), di dati personali
7. Trasmessi (**in movimento**), Conservati (**a riposo**), Trattati (**in uso**)

Pedico Aldo © - Teleion S.r.l via Ferrero 31 - 10098 Rivoli (TO) - Tel. 3482244924 – email: a.pedico@teleion.it 4

ELENCO ARGOMENTI

1) *LEGGI EUROPEE*
2) *METODOLOGIA EDPB 1/2018 – NOTE OPERATIVE E SPECIFICHE TECNICHE PER LA PREDISPOSIZIONE ALLA CERTIFICAZIONE*
3) *MODELLO CMMC ART 25 E 32 DEL 2016/679*
4) *CONFORMITÀ E SUCCESSIVA CERTIFICAZIONE*

LEGGI EUROPEE

1. *Regolamento Generale Europeo per la Protezione dei Dati [Reg. (UE) 2016/679] RGPD o GDPR*
2. *Dir. (UE) 2016/1148: recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione.*
3. *Reg. (UE) 2017/745 [MDR] Relativo ai dispositivi medici*
4. *Reg. (UE) 2017/746 [IVDR] Relativo ai dispositivi medico-diagnostici in vitro*
5. *Reg. (UE) 2018/151: per quanto riguarda l'ulteriore specificazione degli elementi che i fornitori di servizi digitali devono prendere in considerazione ai fini della gestione dei rischi posti alla sicurezza delle reti e dei sistemi informativi e dei parametri per determinare l'eventuale impatto rilevante di un incidente.*
6. *Reg (UE) 2018/1807 Relativo alla libera circolazione dei dati non personali nell'UE*
7. *Reg. (UE) 2019/881 Cibersicurezza (Cybersecurity Act)*

   Relativo all'ENISA, l'Agenzia dell'Unione europea per la cibersicurezza, e alla certificazione della cibersicurezza per le tecnologie dell'informazione e della comunicazione, e che abroga il regolamento (UE) n. 526/2013 («regolamento sulla cibersicurezza»).

   Gli articoli 58, 60, 61, 63, 64 e 65 si applicano dal 28 giugno 2021.

   In particolare Articolo 65 – Sanzioni: "Gli Stati membri stabiliscono le norme relative alle sanzioni applicabili in caso di violazione del presente titolo e di violazione dei sistemi europei di certificazione della cibersicurezza e adottano tutte le misure necessarie per assicurarne l'applicazione. Le sanzioni previste devono essere effettive, proporzionate e dissuasive. Gli Stati membri notificano senza indugio tali norme e misure alla Commissione e provvedono poi a dare notifica delle eventuali modifiche successive."

REGOLAMENTO GENERALE EUROPEO PER LA PROTEZIONE DEI DATI [REG. (UE) 2016/679]

CONSIDERANDO 77

«Gli orientamenti per la messa in atto di opportune misure e per dimostrare la conformità da parte del titolare del trattamento o dal responsabile del trattamento in particolare per quanto riguarda ***l'individuazione del rischio connesso al trattamento****, .., potrebbero essere forniti in particolare mediante codici di condotta approvati,* ***certificazioni approvate****, ……»*

CONSIDERANDO 81

«.. L'applicazione da parte del responsabile del trattamento di un codice di condotta approvato ***o di un meccanismo di certificazione approvato*** *può essere utilizzata come elemento per dimostrare il rispetto degli obblighi da parte del titolare del trattamento...»*

ARTICOLO 24 - RESPONSABILITÀ DEL TITOLARE DEL TRATTAMENTO

3. ***L'adesione*** *ai codici di condotta di cui all'articolo 40* ***o a un meccanismo di certificazione*** *di cui all'articolo 42* ***può essere utilizzata come elemento per dimostrare il rispetto degli obblighi del titolare del trattamento.***

ARTICOLO 42 – CERTIFICAZIONE

1. Gli Stati membri, le autorità di controllo, il comitato e la Commissione incoraggiano, in particolare a livello di Unione, l'istituzione di meccanismi di certificazione della protezione …….

3. La ***certificazione è volontaria*** *e accessibile tramite una procedura trasparente.*

*5. La **certificazione** ai sensi del presente articolo **è rilasciata dagli organismi di certificazione** ……..*

ARTICOLO 43 - ORGANISMI DI CERTIFICAZIONE

*1. ….., gli organismi di certificazione in possesso del livello adeguato di competenze riguardo alla protezione dei dati, **rilasciano e rinnovano la certificazione**, … Gli Stati membri garantiscono che tali organismi di certificazione siano accreditati da uno o entrambi dei seguenti organismi:*

2. Gli organismi di certificazione di cui al paragrafo 1 sono accreditati in conformità di tale paragrafo solo se:

*c) **hanno istituito procedure per il rilascio**, il riesame periodico e la revoca delle certificazioni, dei sigilli e dei marchi di protezione dei dati;*

ARTICOLO 48 - POTERI

3. Ogni autorità di controllo ha tutti i poteri autorizzativi e consultivi seguenti:

*f) **rilasciare certificazioni e approvare i criteri di certificazione** conformemente all'articolo 42, paragrafo 5;*

REGOLAMENTO UE 2019/881 CIBERSICUREZZA (CYBERSECURITY ACT)

ARTICOLO 53 - AUTOVALUTAZIONE DELLA CONFORMITÀ

1. *Un sistema europeo di certificazione della cibersicurezza può **consentire un'autovalutazione della conformità sotto la sola responsabilità del fabbricante o del fornitore di prodotti** TIC, **servizi** TIC o **processi** TIC. Tale autovalutazione della conformità è consentita unicamente in relazione ai prodotti TIC, servizi TIC e processi TIC **che presentano un basso rischio corrispondenti al livello di affidabilità «di base».***
2. *Il fabbricante o fornitore di prodotti TIC, servizi TIC o processi TIC può rilasciare una dichiarazione UE di conformità in cui afferma che è stato dimostrato il rispetto dei requisiti previsti nel sistema. Rilasciando tale dichiarazione, il fabbricante o fornitore di prodotti TIC, servizi TIC o processi TIC **si assume la responsabilità della conformità** del prodotto TIC, servizio TIC o processo TIC ai requisiti previsti in tale sistema.*
4. *Il rilascio di una dichiarazione **UE di conformità è volontario**, salvo diversamente specificato nel diritto dell'Unione o degli Stati membri.*
5. *Le dichiarazioni UE di conformità sono riconosciute in tutti gli Stati membri.*

ARTICOLO 56 - CERTIFICAZIONE DELLA CIBERSICUREZZA

1. ***I prodotti TIC, i servizi TIC e i processi TIC certificati ricorrendo a un sistema europeo di certificazione della cibersicurezza adottato a norma dell'articolo 49 sono considerati conformi ai requisiti di tale sistema.***
2. *La certificazione della cibersicurezza è volontaria, salvo diversamente specificato dal diritto dell'Unione o degli Stati membri.*

ARTICOLO 83 - CONDIZIONI GENERALI PER INFLIGGERE **SANZIONI** AMMINISTRATIVE PECUNIARIE

2. *Le sanzioni amministrative pecuniarie sono inflitte, in funzione delle circostanze di ogni singolo caso, … **Al momento di decidere se infliggere una sanzione amministrativa pecuniaria e di fissare l'ammontare della stessa in ogni singolo caso si tiene debito conto dei seguenti elementi:***
   *j) l'adesione ai codici di condotta approvati ai sensi dell'articolo 40 **o ai meccanismi di certificazione** approvati ai sensi dell'articolo 42;*

METODOLOGIA EDPB 1/2018 – NOTE OPERATIVE E SPECIFICHE TECNICHE PER LA PREDISPOSIZIONE ALLA CERTIFICAZIONE

1

È composta dai seguenti 5 passi:

1. *REQUISITI DI CONFORMITÀ E ATTRIBUTI DELL'OGGETTO O OBIETTIVO DA PREDISPORRE ALLA CERTIFICAZIONE*
2. *STABILIRE CHE COSA PUÒ ESSERE PREDISPOSTO ALLA CERTIFICAZIONE*
3. *DETERMINARE L'OGGETTO O OBIETTIVO (TOE) DELLA PREDISPOSIZIONE ALLA CERTIFICAZIONE*
4. *METODI DI VALUTAZIONE DELL'OGGETTO O OBIETTIVO DA PREDISPORRE ALLA CERTIFICAZIONE*
5. *DOCUMENTAZIONE DELLA VALUTAZIONE*

P1 – REQUISITI DI CONFORMITÀ E ATTRIBUTI DELL'OGGETTO O OBIETTIVO DA PREDISPORRE ALLA CERTIFICAZIONE

A) REQUISITI DI CONFORMITÀ*: di seguito sono riportati gli articoli che definiscono i principi ai quali si devono far sottostare gli adempimenti legali, le misure organizzative e tecniche.*

Dall'art. 5 – Principi applicabili al trattamento di dati personali

Principi oggetto della verifica: liceità; correttezza; trasparenza; limitazione della finalità; adeguati; pertinenti e limitati («minimizzazione dei dati»); le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati («esattezza»); misure tecniche e organizzative adeguate («limitazione della conservazione»); protezione; mediante misure tecniche e organizzative adeguate; da trattamenti non autorizzati o illeciti e dalla perdita; dalla distruzione o dal danno accidentali («integrità e riservatezza»).

Dall'art. 6 – Liceità del trattamento, verificare:

1. *il rispetto dei requisiti indicati nella "Sez. 6 – WP259 Linee guida sul Consenso" del presente manuale, nel caso specifico se l'interessato ha espresso il consenso;*
2. *se il trattamento è necessario **all'esecuzione di un contratto** di cui **l'interessato è parte o all'esecuzione di misure precontrattuali** adottate su richiesta dello stesso;*
3. *se il trattamento è necessario per **adempiere un obbligo legale**;*
4. *se il trattamento è necessario per la **salvaguardia degli interessi vitali dell'interessato**;*
5. *se il trattamento è necessario per **l'esecuzione di un compito si interesse pubblico o connesso all'esercizio di pubblici poteri** di cui è investito il titolare del trattamento;*
6. *se il trattamento è necessario per il **perseguimento del legittimo interesse del titolare del trattamento o di terzi**; Artt. dal 12 al 23 tutto il CAPO III – Diritti dell'interessato.*

Dall'art. 25 – Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita: inserire specifiche dei controlli del Calcolo del Rischio.

*Dall'art. 32 – Sicurezza del trattamento: **inserire specifiche dei controlli del Calcolo del Rischio**.*

Dall'art. 33 – Notifica di una violazione dei dati personali all'autorità di controllo:

1. *in caso di violazione dei dati personali, il titolare del trattamento notifica la violazione all'autorità di controllo competente a norma dell'articolo 55 senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza;*
2. *il Responsabile del trattamento informa il titolare del trattamento senza ingiustificato ritardo dopo essere venuto a conoscenza della violazione;*
3. *la notifica deve almeno:*
   a) *descrivere la natura della violazione dei dati personali compresi, ove possibile;*
   b) *le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;*

c) comunicare il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;

d) descrivere le probabili conseguenze della violazione;

e) descrivere le misure adottate o di cui si propone l'adozione per porre rimedio alla violazione e per attenuarne i possibili effetti negativi;

f) fornire le informazioni in fasi successive senza ulteriore ingiustificato ritardo;

g) documentare qualsiasi violazione, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio.

Dall'art. 35 – Valutazione d'impatto sulla protezione dei dati: inserire specifiche dei controlli del Calcolo del Rischio.

Dall'art. 42 – Certificazione

In particolare il comma 2 evidenzia ***il vincolo di applicare le garanzie adeguate mediante strumenti contrattuali o di altro tipo****: "….****i meccanismi, i sigilli o i marchi possono essere istituiti al fine di dimostrare la previsione di garanzie appropriate*** *da parte dei titolari del trattamento o responsabili del trattamento non soggetti al presente regolamento ai sensi dell'art. 3, nel quadro dei trasferimenti di dati personali verso paesi terzi o organizzazioni internazionali alle condizioni di cui all'art. 46 §2 f) (****un meccanismo di certificazione approvato a norma dell'art. 42, unitamente all'impegno vincolante ed esigibile da parte del titolare del trattamento o del responsabile del trattamento nel paese terzo ad applicare le garanzie adeguate****,…).*

Detti titolari del trattamento o responsabili del trattamento ***assumono l'impegno vincolante azionabile****, mediante strumenti contrattuali o di altro tipo giuridicamente vincolanti,* ***di applicare le stesse adeguate garanzie****".*

B) ATTRIBUTI DA PRENDERE ULTERIORMENTE IN CONSIDERAZIONE

1. *VERIFICABILITÀ;*
2. *IMPORTANZA;*
3. *IDONEITÀ.*

P2 – STABILIRE CHE COSA PUÒ ESSERE PREDISPOSTO ALLA CERTIFICAZIONE

A) QUANDO SI VALUTA UN'OPERAZIONE DI ELABORAZIONE, DEVONO ESSERE CONSIDERATE LE SEGUENTI TRE COMPONENTI PRINCIPALI:

1. *Elencare i processi e le procedure relative alle operazioni di trattamento;*
2. *Elencare i dati personali (ambito materiale del RGPD);*
3. *Definire i sistemi tecnici: l'infrastruttura, come l'hardware e il software, utilizzata per elaborare i dati personali;*

B) PER OGNUNA DELLE COMPONENTI INDICATE PRECEDENTEMENTE, ED UTILIZZATE NELLE OPERAZIONI DI TRATTAMENTO, DEVONO ESSERE VALUTATI ALMENO I SEGUENTI QUATTRO DIVERSI FATTORI CHE POTREBBERO ESSERE INFLUENZATI.

1. *L'organizzazione e la struttura legale del Titolare del Trattamento o del Responsabile del Trattamento;*
2. *Il dipartimento, l'ambiente e le persone coinvolte nelle operazioni di trattamento;*
3. *La descrizione tecnica degli elementi da valutare;*

4. *L'infrastruttura IT che supporta l'operazione di elaborazione, inclusi sistemi operativi, sistemi virtuali, database, sistemi di autenticazione e autorizzazione, router e firewall, sistemi di archiviazione, infrastruttura di comunicazione o accesso ad Internet e misure tecniche associate.*

[Esempi]

- *La conformità all'uso di un'infrastruttura tecnica distribuita in un'operazione di elaborazione dipende dalle categorie di dati che è stato progettato per elaborare. Le misure organizzative dipendono dalle categorie e dalla quantità di dati e dall'infrastruttura tecnica utilizzata per l'elaborazione, tenendo conto della natura, della portata, del contenuto e delle finalità del trattamento, nonché dei rischi per i diritti e le libertà delle persone interessate.*
- *L'elaborazione dei dati dei dipendenti ai fini della retribuzione o gestione delle ferie è un insieme di operazioni ai sensi del RGPD e può comportare un prodotto, un processo o un servizio nella terminologia ISO.*

Il processo di governance stabilito per la gestione dei reclami come parte del trattamento dei dati dei dipendenti ai fini del pagamento degli stipendi.

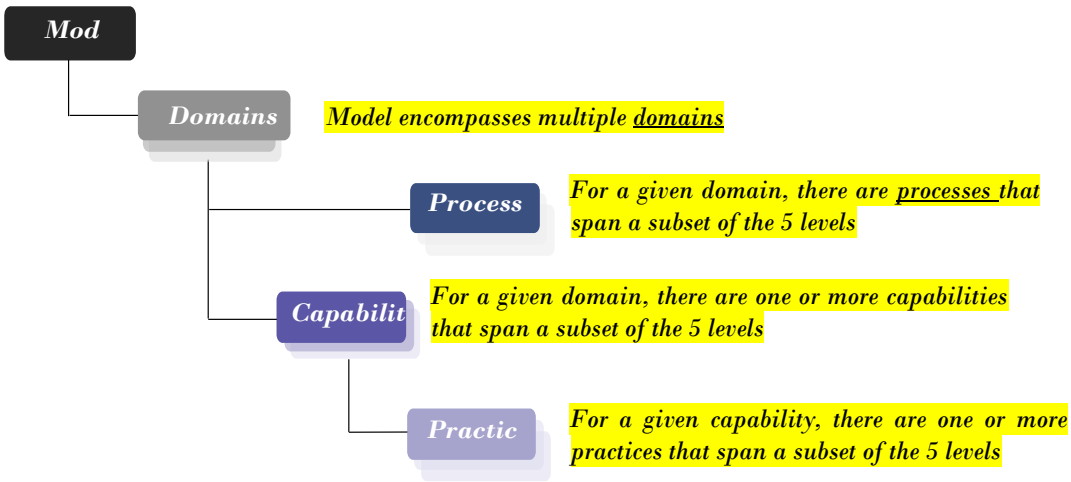
MODELLO CMMC PER LA CERTIFICAZIONE

[Rif. CMMC – Cybersecurity Maturity Model Certification - Modello per la certificazione o autocertificazione del sistema di cibersicurezza]

Il framework CMMC (Cybersecurity Maturity Model Certification) è costituito da processi di maturità e migliori pratiche di cybersecurity da più standard di cybersecurity, framework e altri riferimenti, nonché input dagli stakeholder della Defense Industrial Base (DIB) e del Dipartimento della Difesa (DoD).

La struttura del modello (Fig.1) organizza questi processi e pratiche in un insieme di domini e li mappa su cinque livelli.

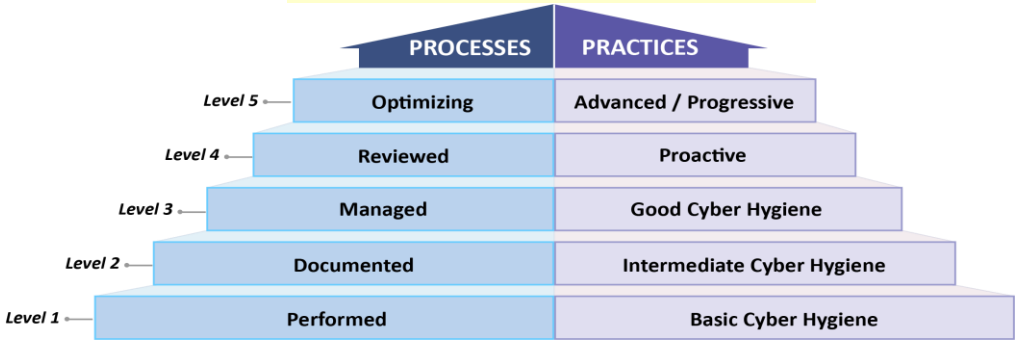
Al fine di fornire una struttura aggiuntiva, il framework allinea anche le pratiche a una serie di funzionalità all'interno di ciascun dominio. Le sottosezioni che seguono forniscono ulteriori informazioni su ciascun elemento del modello.



l modello CMMC misura la maturità della sicurezza informatica con cinque livelli. Ognuno di questi livelli, a sua volta, consiste in una serie di processi e pratiche.

- *I Processi vanno da «**Eseguito**» (Performed) a livello 1 a «**Ottimizzazione**» (Optimizing) a livello 5*
- *Le Pratiche vanno da «**Basic Cyber Hygiene**» a livello 1 a «**Avanzato/Progressivo**» (Advanced/Progressive) a livello 5.*

FIGURE 2. CMMC LEVELS AND DESCRIPTIONS



LEVEL 1

- *Processi:* ***Eseguiti (Performed)***

Il livello 1 richiede che un'organizzazione esegua le pratiche specificate. Poiché l'organizzazione può essere in grado di eseguire queste pratiche solo in modo ad hoc e può fare affidamento sulla documentazione o meno, la maturità del processo non viene valutata per il Livello 1.

- *Pratiche:* ***Cyber Hygiene di base***

Il livello 1 si concentra sulla protezione della FCI e consiste solo in pratiche che corrispondono ai requisiti di protezione di base specificati in CFR 52.204-21 («Salvaguardia di base dei sistemi di informazione degli appaltatori coperti»).

LIVELLO 2

- *Processi:* ***Documentati (Documented)***

Il livello 2 richiede che un'organizzazione stabilisca e documenti pratiche e politiche per guidare l'implementazione dei loro sforzi CMMC.

- *Pratiche:* ***Intermediate Cyber Hygiene***

Il livello 2 è costituito da un sottoinsieme dei requisiti di sicurezza specificati in NIST SP 800-171, nonché da pratiche di altri standard e riferimenti.

LEVEL 3

- *Processi:* ***Gestiti (Managed)***

Il livello 3 richiede che un'organizzazione stabilisca, mantenga e risorse un piano che dimostri la gestione delle attività per l'implementazione pratica. Il piano può includere informazioni su missioni, obiettivi, piani di progetto, risorse, formazione richiesta e coinvolgimento delle parti interessate.

- *Pratiche:* ***Good Cyber Hygiene***

Il livello 3 si concentra sulla protezione di CUI e comprende tutti i requisiti di sicurezza specificati in NIST SP 800-171, nonché pratiche aggiuntive da altri standard e riferimenti per mitigare le minacce.

LIVELLO 4

- *Processi:* ***Rivisti (Reviewed)***

Il livello 4 richiede che un'organizzazione riveda e misuri le pratiche per l'efficacia. Oltre a misurare le pratiche per l'efficacia, le organizzazioni di questo livello sono in grado di intraprendere azioni correttive quando necessario e informare la gestione di livello superiore dello stato o delle questioni su base ricorrente.

- *Pratiche:* ***Proattivi (Proactive)***

Il livello 4 si concentra sulla protezione di CUI dagli APT e comprende un sottoinsieme dei requisiti di sicurezza avanzati di NIST SP 800-171B, nonché altre migliori pratiche di sicurezza informatica. Queste pratiche migliorano le capacità di rilevamento e risposta di un'organizzazione per affrontare e adattarsi alle mutevoli tattiche, tecniche e procedure (TTP) utilizzate dagli APT.

LEVEL 5

- *Processi:* ***Ottimizzazione (Optimizing)***

Il livello 5 richiede un'organizzazione per standardizzare e ottimizzare l'implementazione dei processi all'interno dell'organizzazione.

- *Pratiche:* ***Avanzate/Progressive (Advanced/Progressive)***

Il livello 5 si concentra sulla protezione della CUI dagli APT. Le pratiche aggiuntive aumentano la profondità e la sofisticazione delle capacità di sicurezza informatica.

DOMINI

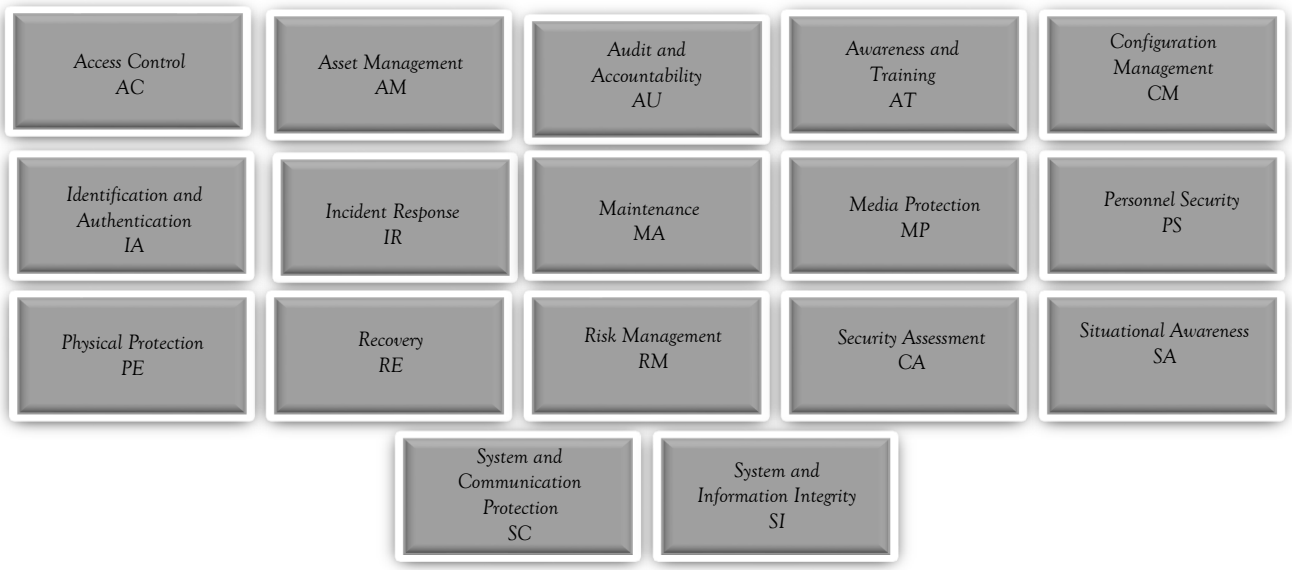
Il modello CMMC è composto da 17 domini.

La maggior parte di questi domini proviene dalle aree relative alla sicurezza della pubblicazione 200 degli Standard federali di elaborazione delle informazioni (FIPS) e dalle relative famiglie dei requisiti di sicurezza dal NIST SP 800-17.

Il modello CMMC include anche i 3 domini:

1. ASSET MANAGEMENT (AM)
2. RECOVERY (RE)
3. SITUATIONAL AWARENESS (SA)

FIGURE 4. CMMC DOMAINS



CAPABILITIES

Ciascun dominio è costituito da un insieme di processi e capabilities (e, a sua volta, pratiche) attraverso i 5 livelli.

Di seguito, la tabella 1 elenca le 43 funzionalità associate ai 17 domini nel modello CMMC.

Table 1. CMMC Capabilities

DOMAIN	CAPABILITY
Access Control (AC)	*Establish system access requirements* *Control internal system access* *Control remote system access* *Limit data access to authorized users and processes*
Asset Management (AM)	*Identify and document assets*
Audit and Accountability (AU)	*Define audit requirements* *Perform auditing* *Identify and protect audit information* *Review and manage audit logs*
Awareness and Training (AT)	*Conduct security awareness activities* *Conduct training*
Configuration Management (CM)	*Establish configuration baselines* *Perform configuration and change management*
Identification and Authentication (IA)	*Grant access to authenticated entities*
Incident Response (IR)	*Plan incident response* *Detect and report events* *Develop and implement a response to a declared incident* *Perform post incident reviews* *Test incident response*
Maintenance (MA)	*Manage maintenance*
Media Protection (MP)	*Identify and mark media* *Protect and control media* *Sanitize media* *Protect media during transport*
Personnel Security (PS)	*Screen personnel* *Protect CUI during personnel actions*
Physical Protection (PE)	*Limit physical access*
Recovery (RE)	*Manage back-ups*
Risk Management (RM)	*Identify and evaluate risk* *Manage risk*
Security Assessment (CA)	*Develop and manage a system security plan* *Define and manage controls* *Perform code reviews*
Situational Awareness (SA)	*Implement threat monitoring*
Systems and Communications Protection (SC)	*Define security requirements for systems and communications* *Control communications at system boundaries*
System and Information Integrity (SI)	*Identify and manage information system flaws* *Identify malicious content* *Perform network and system monitoring* *Implement advanced email protections*

PROCESSES

Nel contesto del modello CMMC, l'istituzionalizzazione dei processi fornisce ulteriori garanzie che le pratiche associate a ciascun livello siano implementate in modo efficace.

Il modello CMMC è costituito da 5 processi di maturità che vanno dai livelli di maturità (ML) 2-5 e si applicano a tutti i domini (Tabella 2).

Le organizzazioni eseguono pratiche a livello 1 ma la maturità del processo non viene valutata per ML 1.

Table 2. CMMC Processes

MATURITY LEVEL	DESCRIPTION	PROCESSES
ML 1	*Performed*	*There are no maturity processes assessed at Maturity Level 1.* *An organization performs Level 1 practices but does not have process institutionalization requirements.*
ML 2	*Documented*	*Establish a policy that includes [DOMAIN NAME].*
		Document the CMMC practices to implement the [DOMAIN NAME] policy.
ML 3	*Managed*	*Establish, maintain, and resource a plan that includes [DOMAIN NAME].*
ML 4	*Reviewed*	*Review and measure [DOMAIN NAME] activities for effectiveness.*
ML 5	*Optimizing*	*Standardize and optimize a documented approach for [DOMAIN NAME] across all applicable organization units.*

Elenco delle pratiche per ciascun dominio e per ogni livello.

Ogni pratica è specificata usando la convenzione di: [Dominio].[Livello].[Numero Pratica] dove:

- *Dominio è l'abbreviazione del dominio di due lettere;*
- *Livello è il numero del livello;*

Numero Pratica è l'identificatore assegnato a quella pratica.

List of practices

DOMINIO: ACCESS CONTROL (AC)	
LEVEL 1	
AC.1.001	*Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).*
LEVEL 2	
AC.2.005	Provide privacy and security notices consistent with applicable CUI rules.
DOMINIO: RISK MANAGEMENT (RM)	
LEVEL 2	
RM.2.141	*Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of CUI.*
LEVEL 3	
RM.3.144	Periodically perform risk assessments to identify and prioritize risks according to the defined risk categories, risk sources, and risk measurement criteria.

NISTIR 8183 REV. 1 - CYBERSECURITY FRAMEWORK VER. 1.1 MANUFACTURING PROFILE

AND

NISTIR 8183A VOL.1 - CYBERSECURITY FRAMEWORK MANUFACTURING PROFILE LOW IMPACT LEVEL EXAMPLE IMPLEMENTATIONS GUIDE: Vol. 1 – General Implementation Guidance

10A. ABSTRACT

Questa guida fornisce una guida all'implementazione generale (Vol.1) ed esempi di soluzioni proof-of-concept che dimostrano come i prodotti disponibili open source e commerciali off-the-shelf (COTS) potrebbero essere implementati negli ambienti di produzione per soddisfare i requisiti del Cybersecurity Framework (CSF) Profilo di produzione a basso livello di impatto.

Nella guida sono inclusi esempi di soluzioni proof-of-concept con reti misurate, dispositivi e impatti sulle prestazioni operative per un ambiente di produzione basato sui processi (Vol.2) e un ambiente di produzione discreto (Vol.3).

I produttori dovrebbero prendere le proprie decisioni in merito all'ampiezza delle soluzioni proof-of-concept che implementano volontariamente.

Alcuni fattori importanti da considerare includono: dimensioni dell'azienda, competenze in materia di sicurezza informatica, tolleranza al rischio e panorama delle minacce.

Il Profilo di Produzione CSF può essere utilizzato come tabella di marcia per la gestione del rischio di sicurezza informatica per i produttori ed è in linea con gli obiettivi del settore manifatturiero e le migliori pratiche del settore.

Il Profilo di Produzione fornisce un approccio volontario basato sul rischio per la gestione delle attività di sicurezza informatica e del rischio informatico per i sistemi di produzione ed ha lo scopo di integrare ma non sostituire gli attuali standard di sicurezza informatica e le linee guida del settore che il produttore sta adottando.

10B. EXECUTIVE SUMMARY

Questa sezione fornisce sia i dettagli di implementazione del Cybersecurity Framework (CSF) sviluppati per l'ambiente di produzione sia una guida all'implementazione generale (Vol.1) ed esempi di soluzioni proof-of-concept che dimostrano come i prodotti disponibili open source e commerciali off-the-shelf (COTS) potrebbero essere implementati negli ambienti di produzione per soddisfare i requisiti del Cybersecurity Framework (CSF) Profilo di produzione a basso livello di impatto.

Nel caso del "Manufacturing Profile" del Cybersecurity Framework *può essere utilizzato come roadmap per ridurre il rischio di cybersecurity per i produttori in linea con gli obiettivi del settore manifatturiero e le migliori pratiche del settore.*

Il profilo offre ai produttori:

- ✓ *un metodo per identificare le opportunità per migliorare l'attuale posizione di sicurezza informatica del sistema di produzione*
- ✓ *una valutazione della loro capacità di far funzionare l'ambiente di controllo al loro livello di rischio accettabile*
- ✓ *un approccio standardizzato alla preparazione del piano di sicurezza informatica per la garanzia continua della sicurezza del sistema di produzione.*

Il profilo è costruito attorno alle aree funzionali primarie del Cybersecurity Framework che enumerano le funzioni di base delle attività di sicurezza informatica.

Le cinque aree funzionali principali sono: ***IDENTIFICA****,* ***PROTEGGI, RILEVA, RISPONDI*** *e* ***RIPRISTINA****.*

Queste aree funzionali primarie costituiscono un punto di partenza da cui sviluppare un profilo specifico del produttore o del settore ai livelli di rischio definiti di ***BASSO, MODERATO E ALTO****.*

Questo profilo "Target" di produzione si concentra sui risultati desiderati in materia di sicurezza informatica e può essere utilizzato come tabella di marcia per identificare le opportunità per migliorare l'attuale posizione di sicurezza informatica del sistema di produzione.

Il Profilo di Produzione fornisce una priorità delle attività di sicurezza per soddisfare specifici obiettivi aziendali/mission.

Sono quindi identificate le pratiche di sicurezza pertinenti e attuabili che possono essere implementate per supportare gli obiettivi chiave della missione.

Inoltre, questo profilo di produzione fornisce un approccio volontario e basato sul rischio per la gestione delle attività di sicurezza informatica e la riduzione del rischio informatico per i sistemi di produzione ed ha lo scopo di migliorare ma non sostituire gli attuali standard di sicurezza informatica e le linee guida del settore che il produttore sta adottando.

Un sistema di produzione potrebbe essere classificato come Basso impatto potenziale se ci si può aspettare che la perdita di integrità, disponibilità o riservatezza abbia un effetto negativo limitato sulle operazioni di produzione, sui prodotti fabbricati, sulle risorse, sull'immagine del marchio, sulle finanze, sul personale, sul pubblico in generale o l'ambiente. Un effetto negativo limitato significa che, ad esempio, la perdita di integrità, disponibilità o riservatezza potrebbe:

- ✓ *provocare un degrado della capacità di missione in una misura e durata tale che il sistema possa svolgere le sue funzioni primarie, ma l'efficacia delle funzioni è notevolmente ridotta*
- ✓ *comportare danni minori agli asset operativi,*
- ✓ *comportare una perdita finanziaria minore, o*
- ✓ *causare danni minori alle persone.*

Nella guida sono inclusi esempi di soluzioni proof-of-concept con impatti misurati sulla rete, sui dispositivi e sulle prestazioni operative per un ambiente di produzione basato sui processi (Vol.2) e un ambiente di produzione discreto (Vol.3).

I produttori dovrebbero prendere le proprie decisioni in merito all'ampiezza delle soluzioni proof-of-concept che implementano volontariamente. Alcuni fattori importanti da considerare includono: dimensioni dell'azienda, competenze in materia di sicurezza informatica, tolleranza al rischio e panorama delle minacce.

Sebbene le soluzioni proof-of-concept in questa guida utilizzino una suite di prodotti commerciali, questa guida non approva questi prodotti, né garantisce la conformità con alcuna iniziativa normativa.

11. INTRODUCTION

L'Executive Order 13636, "Improving Critical Infrastructure Cybersecurity", ha diretto lo sviluppo del Cybersecurity Framework volontario che fornisce un approccio ***prioritario***, ***flessibile***, ***ripetibile***, *basato sulle prestazioni e conveniente per gestire il rischio di cybersecurity per tali processi, informazioni e sistemi direttamente coinvolto nella fornitura di servizi di infrastrutture critiche.*

Il Cybersecurity Framework è un assemblaggio volontario basato sul rischio di standard di settore e best practice progettati per aiutare le organizzazioni a gestire i rischi per la sicurezza informatica.

Il Framework, creato attraverso la collaborazione tra governo e settore privato, utilizza un linguaggio comune per affrontare e gestire il rischio di sicurezza informatica in modo conveniente in base alle esigenze aziendali senza imporre requisiti normativi aggiuntivi.

Per rispondere alle esigenze dei produttori, è stato sviluppato un profilo di produzione del Cybersecurity Framework, attraverso la collaborazione tra il governo e il settore privato, per essere un approccio attuabile per l'implementazione dei controlli di sicurezza informatica in un sistema di produzione e nel suo ambiente.

Il profilo definisce attività e risultati di sicurezza informatica specifici per la protezione del sistema di produzione, dei suoi componenti, della struttura e dell'ambiente. Attraverso l'uso del profilo, il produttore può allineare le attività di sicurezza informatica con i requisiti aziendali, la tolleranza al rischio e le risorse. Il profilo fornisce un approccio specifico del settore manifatturiero alla sicurezza informatica da standard, linee guida e best practice del settore.

PURPOSE AND SCOPE

Molti produttori di piccole e medie dimensioni hanno espresso difficoltà nell'attuazione di un programma di sicurezza informatica basato su standard.

Questa guida fornisce una guida all'implementazione generale (Vol.1) ed esempi di soluzioni proof-of-concept che dimostrano come i prodotti disponibili open source e Commerciali Off-The-Shelf (COTS) potrebbero essere implementati negli ambienti di produzione per soddisfare i requisiti del Cybersecurity Framework (CSF) Profilo di produzione a basso livello di impatto.

Un sistema di produzione potrebbe essere classificato come Basso impatto potenziale se ci si può aspettare che la perdita di integrità, disponibilità o riservatezza abbia un effetto negativo limitato sulle operazioni di produzione, sui prodotti fabbricati, sulle risorse, sull'immagine del marchio, sulle finanze, sul personale, sul pubblico in generale o l'ambiente.

Un effetto ***negativo limitato*** *significa che, ad esempio, la perdita di integrità, disponibilità o riservatezza potrebbe:*

- ✓ *provocare un degrado della capacità di missione in una misura e durata tale che il sistema possa svolgere le sue funzioni primarie, ma l'efficacia delle funzioni è notevolmente ridotta*
- ✓ *comportare danni minori agli asset operativi,*
- ✓ *comportare una perdita finanziaria minore o*
- ✓ *provocare un danno minore alle persone.*

Nella guida sono inclusi esempi di soluzioni proof-of-concept con rete misurata, dispositivi e impatti sulle prestazioni operative per un ambiente di produzione basato sui processi (Vol.2) e un ambiente di produzione basato su discreti (Vol.3).

I produttori dovrebbero prendere le proprie decisioni in merito all'ampiezza delle soluzioni proof-of-concept che implementano volontariamente.

Alcuni fattori importanti da considerare includono: dimensioni dell'azienda, competenze in materia di sicurezza informatica, tolleranza al rischio e panorama delle minacce.

Il profilo di produzione CSF può essere utilizzato come tabella di marcia per la gestione del rischio di sicurezza informatica per i produttori ed è in linea con gli obiettivi del settore manifatturiero e le migliori pratiche del settore.

Il profilo di produzione fornisce un approccio volontario basato sul rischio per la gestione delle attività di sicurezza informatica e del rischio informatico per i sistemi di produzione.

Il profilo di produzione ha lo scopo di migliorare ma non sostituire gli attuali standard di sicurezza informatica e le linee guida del settore che il produttore sta adottando.

Sebbene le soluzioni proof-of-concept in questa guida utilizzino una suite di prodotti commerciali, questa guida non approva questi prodotti, né garantisce la conformità con alcuna iniziativa normativa.

Gli esperti di sicurezza delle informazioni di ciascuna organizzazione dovrebbero identificare i prodotti che si integreranno al meglio con i loro strumenti esistenti e l'infrastruttura del sistema di produzione.

Le organizzazioni possono adottare volontariamente queste soluzioni o una che aderisca completamente a queste linee guida o possono utilizzare questa guida come punto di partenza per personalizzare e implementare parti di una soluzione.

Questa guida non descrive regolamenti o pratiche obbligatorie, né ha alcuna autorità legale.

Questo progetto è guidato dai seguenti presupposti:

- ✓ *le soluzioni sono state sviluppate in un ambiente di laboratorio,*
- ✓ *l'ambiente è basato sull'ambiente di un piccolo produttore tipico,*
- ✓ *l'ambiente non riflette la complessità di un ambiente di produzione e*
- ✓ *un'organizzazione può accedere alle competenze e alle risorse necessarie per implementare una soluzione di sicurezza informatica di produzione.*

12. OVERVIEW OF MANUFACTURING SYSTEMS

Manufacturing is a large and diverse industrial sector.

***Manufacturing industries can be categorized as either process-based, discrete-based or a combination of both**.*

***Process-based** manufacturing industries typically utilize 2 main process types:*

4. ***Continuous Manufacturing Processes.** These processes run continuously, often with phases to make different grades of a product. Typical continuous manufacturing processes include fuel or steam flow in a power plant, petroleum in a refinery, and distillation in a chemical plant.*
5. ***Batch Manufacturing Processes.** These processes have distinct processing steps, conducted on a quantity of material. There is a distinct start and end to a batch process with the possibility of brief steady state operations during intermediate steps. Typical batch manufacturing processes include food, beverage, and biotech manufacturing.*

***Discrete-based** manufacturing industries typically conduct a series of operations to create a distinct product. Electronic and mechanical parts assembly and parts machining are typical examples of this type of industry.*

Both process-based and discrete-based industries utilize similar types of control systems, sensors, and networks. Additionally, some facilities are a hybrid of discrete and process-based manufacturing.

Manufacturing systems are usually located within a confined factory or plant-centric area.

Communications in manufacturing industries are typically performed using fieldbus and local area network (LAN) technologies that are reliable and high speed. Wireless networking technologies are also gaining popularity in manufacturing industries.

Fieldbus includes, for example, DeviceNet, Modbus, and Controller Area Network (CAN) bus.

The manufacturing sector of the critical infrastructure community includes public and private owners and operators, along with other entities.

Members of the distinct critical infrastructure sector perform functions that are supported by industrial control systems (ICS) and by information technology (IT).

This reliance on technology, communication, and the interconnectivity of ICS and IT has changed and expanded the potential vulnerabilities and increased potential risk to manufacturing system operations.

13. THE CYBERSECURITY FRAMEWORK

See chapter Overview of the Cybersecurity Framework into Part I.

14. CSF MANUFACTURING PROFILE OVERVIEW

The Manufacturing Profile was developed to be an actionable approach for implementing cybersecurity controls into a manufacturing system and its environment.

The specific statements in the Subcategories in Section 7 of the Manufacturing Profile were derived from the security controls of the NIST SP 800-53 and are customized to the manufacturing domain using relevant informative references.

The general informative references of ISA/IEC 62443 from the Cybersecurity Framework are also listed in the References column. COBIT 5 is sourced for Subcategories that have no corresponding 800-53 references.

Additional input came from NIST SP 800-82, Rev.2, Section 6.2 (Guidance on the Application of Security Controls to ICS) and Appendix G (ICS Overlay). For informative references to an entire control family or set of controls (such as Subcategory ID.GV-1's informative reference to all "policy and procedures" controls), the approach took a holistic view of the controls comprising the family/set.

The Manufacturing Profile expresses tailored values for cybersecurity controls for the manufacturing system environment. These represent the application of the Categories and Subcategories from the Cybersecurity Framework based on domain-specific relevance, business drivers, risk assessment, and the manufacturer's priorities. Users of the Profile can also add Categories and Subcategories as needed to address unique and specific risks.

15. CSF MANUFACTURING PROFILE IMPLEMENTATION APPROACH

Meeting the Manufacturing Profile Subcategory requirements can be accomplished by developing and implementing policies and procedures and/or implementing technical solutions, depending on the particular Subcategory language.

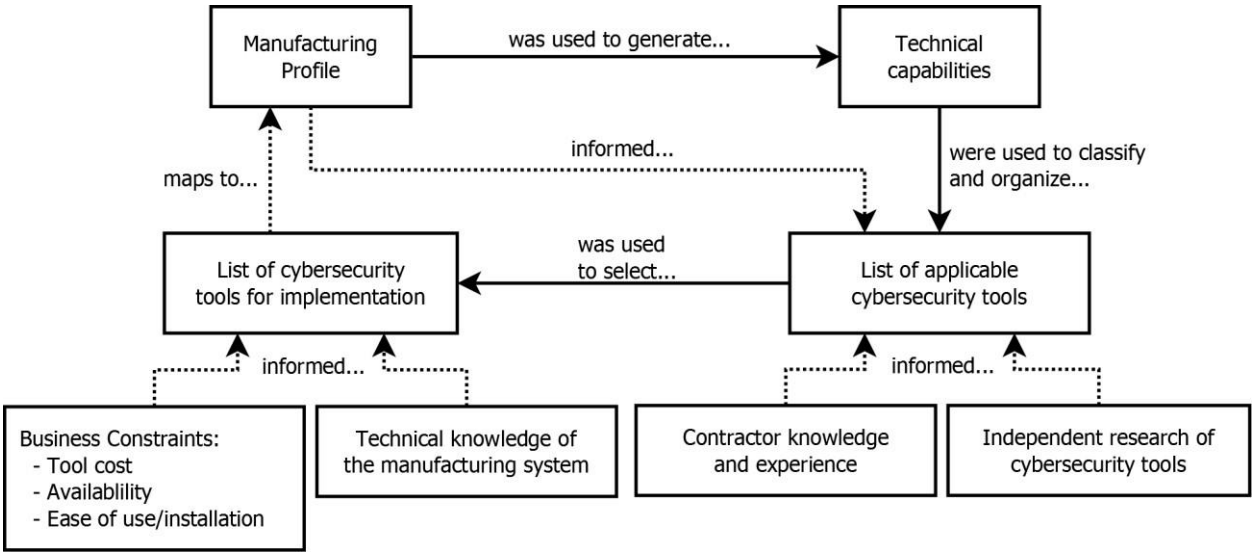


Figure 4-1. Approach used for identifying, planning and implementing technical cybersecurity capabilities

Figure 4-1 provides a visual representation of the approach used for identifying, planning and implementing technical cybersecurity capabilities as well as identifying the complementary cybersecurity processes and procedures.

The Cybersecurity Framework Manufacturing Profile (CFMP) was the principal resource describing the cybersecurity outcomes desired in both of NIST's manufacturing testbed scenarios. The outcomes described in the Manufacturing Profile are grounded by and cross referenced with prescriptive cybersecurity controls from standards relevant to Industrial Control Systems (ICS) owners and operators.

The initial step of this planning process was focused on researching what cybersecurity related tools, configurations, and best practices are required to achieve the specific outcomes or Profile Subcategories. The Profile Subcategories and specific language provided by mapped cybersecurity controls provided insight into classifications of technical capabilities needed to be implemented in the testbed environments. From these high-level classifications of capabilities, NIST researchers identified and built a list of commercial products and open source tools that fit into each of these classifications. The list of solutions was then used to inform implementation planning and select specific solutions, tools, and products for implementation in the testbed environment. The selection of these technologies for implementation was informed by: technical knowledge of the testbed; solution cost; availability; maturity; level of expertise required for implementation and management; and the lab IT administrator's expertise.

The mapping of technical solutions to Profile Subcategories in most cases did not provide exact one-to-one coverage. In most scenarios, during the planning process there was a realization that implementing one technical capability might only satisfy portions of multiple Subcategories and in some scenarios implementation of multiple technical capabilities were required in order to achieve the outcome described by a Profile Subcategory. Some Profile Subcategories (e.g., PR.DS-3) required the implementation of a technical capability complemented by the addition of a cybersecurity policy or procedure. While this mapping adds complexity to the planning process it enables system owners to gain an understanding of what technical solutions will enable them to achieve the most Subcategory outcomes. Priorities can be assigned based the specific mission and business objectives of the organization.

Section 5 provides an overview of the six policy and procedure documents needed to meet the requirements specified in the CSF Manufacturing Profile Low Impact Level.

Section 6 provides the technical capabilities needed to meet the requirements specified in the CSF Manufacturing Profile Low Impact Level.

Section 7 examines potential solutions that can address the requirements specified in the CSF Manufacturing Profile Low Impact Level.

16. POLICY/PROCEDURAL CAPABILITIES OVERVIEW

For the implementation of the two use cases, six policy and procedural documents were produced for each:

CYBERSECURITY PROGRAM DOCUMENT

The Cybersecurity Program document establishes guidelines and principles for initiating, implementing, maintaining, and improving information security management of the organization. It is a documented set of the organization's security policies, procedures, guidelines and standards. The program is intended to protect the confidentiality, integrity and availability of information resources.

CYBERSECURITY POLICY DOCUMENT

The Cybersecurity Policy document defines the cybersecurity requirements for the proper and secure use of the Information Technology services in the organization. Its goal is to protect the organization and its users to the maximum extent possible against cybersecurity threats that could jeopardize their integrity, privacy, reputation, and business outcomes.

CYBERSECURITY OPERATIONS DOCUMENT

The Cybersecurity Operations document defines the operational steps management and employees will follow ensuring consistency with response to events occurring within the manufacturing system. This document contains

content which should be referred to often to help ensure all employees and individuals performing work within the manufacturing system are familiar with cybersecurity operations.

RISK MANAGEMENT DOCUMENT

The Risk Management Strategy document defines how risks associated with the organization will be identified, analyzed, and managed. It outlines the risk management strategy for the organization. In addition, it provides standard terminology, clear roles and responsibilities and details of the risk management process. This document can be used by the management to understand risks, estimate impacts, and define responses to issues. It is designed to guide the project team and stakeholders.

INCIDENT RESPONSE PLAN DOCUMENT

The Incident Response Plan document describes the plan for responding to information security incidents within an organization. It defines the roles and responsibilities of participants, characterization of incidents, relationships to other policies and procedures, and reporting requirements. The purpose of this plan is to detect and react to cybersecurity incidents, determine their scope and risk, respond appropriately to the incident, communicate the results and risk to all stakeholders, and reduce the likelihood of the incident from reoccurring.

SYSTEM RECOVERY PLAN DOCUMENT

The System Recovery Plan is designed to ensure the continuation of vital manufacturing/business processes in the event a cybersecurity incident occurs. Its purpose is to provide a structured approach for responding to cybersecurity incidents by leveraging the infrastructure inventory and configuration information relevant to the organization's IT and OT environments to restore operational capabilities.

This plan has been developed to accomplish the following objectives:

- ✓ *limit the magnitude of any loss by minimizing the duration of a manufacturing interruption,*
- ✓ *assess damage, repair the damage, and restore manufacturing system,*
- ✓ *manage the recovery operation in an organized and effective manner, and*
- ✓ *prepare personnel to respond effectively in system recovery situations.*

17. TECHNICAL CAPABILITIES OVERVIEW

This section discusses the technical capabilities identified by the team necessary to meet the CSF Manufacturing Profile language. For each technical capability, an overview of the capability is provided, the security benefits of implementing the capability is listed, any potential system impacts the capability could have on the manufacturing system are discussed, and the CSF Manufacturing Profile Subcategories that are addressed when the capability is implemented are listed.

HARDWARE INVENTORY MANAGEMENT

C - MANUFACTURING PROFILE SUBCATEGORIES

ID.AM-1, PR.DS-3, DE.CM-7

SOFTWARE AND FIRMWARE INVENTORY MANAGEMENT

C - MANUFACTURING PROFILE SUBCATEGORIES

ID.AM-2, PR.DS-3, DE.CM-7

SYSTEMS DEVELOPMENT LIFECYCLE MANAGEMENT

C - MANUFACTURING PROFILE SUBCATEGORIES

PR.DS-3, PR.IP-1, PR.IP-2, PR.IP-6, DE.CM-7

NETWORK ARCHITECTURE DOCUMENTATION

C - MANUFACTURING PROFILE SUBCATEGORIES

ID.AM-3, ID.AM-4

CONFIGURATION MANAGEMENT

C - MANUFACTURING PROFILE SUBCATEGORIES

ID.AM-3, ID.AM-4, PR.IP-1, PR.IP-4, PR.MA-1

BASELINE ESTABLISHMENT

C - MANUFACTURING PROFILE SUBCATEGORIES

ID.AM-3, PR.IP-1, DE.AE-1, DE-CM-7

CHANGE CONTROL

C - MANUFACTURING PROFILE SUBCATEGORIES

PR.IP-1, PR.IP-3, PR.MA-1, DE.CM-7

CONFIGURATION BACKUPS

C - MANUFACTURING PROFILE SUBCATEGORIES

PR.IP-1, PR.IP-4

DATA BACKUP

C - MANUFACTURING PROFILE SUBCATEGORIES

PR.IP-4

DATA REPLICATION

C - MANUFACTURING PROFILE SUBCATEGORIES

PR.IP-4

NETWORK SEGMENTATION AND SEGREGATION

C - MANUFACTURING PROFILE SUBCATEGORIES

PR.AC-5

NETWORK BOUNDARY PROTECTION

A - SECURITY BENEFIT

Firewalls allow organizations to segment their networks, restricting access to only authorized connections. These devices monitor and log traffic accessing or attempting to access the network. This functionality provides forensic data that can be critical for response and recovery activities. More advanced firewalls, commonly called Next Generation Firewalls (NGFW), include antivirus and malware protection with datasets continuously upgraded to detect new threats. These NGFWs can provide other advanced security protections such as intrusion detection, deep packet inspection, virtual private network (VPN) services, and denial of service protection. The physical and logical isolation characteristics of a DMZ are important because they enable access only to designated servers and information stored within the isolated DMZ with no visibility directly into the sensitive manufacturing network. Having a DMZ network reduces and controls access to those internal systems from outside of the organization. Intrusion detection and prevention systems can monitor, detect, analyze, and prevent unauthorized network or system access.

B - POTENTIAL SYSTEM IMPACTS

Network boundary protections can potentially impact the manufacturing system. Care must be taken when planning and deploying network boundary protections. Increased network latency may be caused by in-line boundary protection devices (e.g., firewalls), especially if the capabilities of the device and network do not match (e.g., a 100 Mbps Ethernet device on a 1 Gbps network).

C - MANUFACTURING PROFILE SUBCATEGORIES

PR.AC-5, PR.PT-4, DE.CM-1

SECURE REMOTE ACCESS

C - MANUFACTURING PROFILE SUBCATEGORIES

PR.AC-5, PR.MA-2

MANAGED NETWORK INTERFACES

C - MANUFACTURING PROFILE SUBCATEGORIES

PR.AC-5

MAP DATA FLOWS

C - MANUFACTURING PROFILE SUBCATEGORIES

ID.AM-3, ID.AM-4, PR.AC-5, DE.AE-1

TIME SYNCHRONIZATION

C - MANUFACTURING PROFILE SUBCATEGORIES

PR.PT-1

CREDENTIAL MANAGEMENT

C - MANUFACTURING PROFILE SUBCATEGORIES

PR.AC-1, PR.MA-1, PR.MA-2

AUTHENTICATION AND AUTHORIZATION

C - MANUFACTURING PROFILE SUBCATEGORIES

PR.AC-1, PR.MA-1, PR.MA-2, PR-PT-3, PR.PT-4, DE.CM-3

ANTI-VIRUS/MALWARE

C - MANUFACTURING PROFILE SUBCATEGORIES

DE.CM-4

RISK ASSESSMENT

A - SECURITY BENEFIT

A risk assessment will evaluate an organization's security posture by considering external and internal threats. In doing so, a risk assessment will identify current security vulnerabilities, control gaps, and noncompliance with standards. It is performed either via audits consisting of surveys, discussions, and/or questionnaires. Risk assessments are part of an overall risk management process, providing senior leaders/executives with the information needed to determine appropriate courses of action in response to identified risks. The results of these

assessments can be leveraged to create awareness amongst employees and be used as a training tool as well. Performing regular risk assessments can reduce incidents in the workplace.

B - POTENTIAL SYSTEM IMPACTS

Risk assessment tools should not impact the manufacturing system, as they are typically operated and accessed outside of the manufacturing system.

C - MANUFACTURING PROFILE SUBCATEGORIES

ID.RA-1

VULNERABILITY SCANNING

A - SECURITY BENEFIT

Identification of known security vulnerabilities present in the manufacturing network can be used to help inform patch management activities.

B - POTENTIAL SYSTEM IMPACTS

Vulnerability scanning tools can impact an operational system. Vulnerability scanning tools may require a software agent to be installed on the device or may perform authenticated scanning via the network. Vulnerability scanning tools may generate excessive network traffic or, in extreme cases, cause device failures due to the intrusive methods used during scanning. These tools should be configured to use the minimum amount of network bandwidth required for proper operation. It is recommended that scans be planned around scheduled downtime and not be performed while the manufacturing system is operational.

C - MANUFACTURING PROFILE SUBCATEGORIES

ID.RA-1, DE.CM-8

VULNERABILITY MANAGEMENT

A - SECURITY BENEFIT

Vulnerability management tools allow a manufacturer to apply security updates to its systems and identify where compensating controls are needed to protect equipment that cannot be updated.

B - POTENTIAL SYSTEM IMPACTS

Vulnerability management can potentially impact the manufacturing system. A patch may remove a vulnerability, but it can also introduce a risk from a production or safety perspective.

Patching a vulnerability may also change the way the operating system or application functions. It is recommended to consult with the product vendor to see if they have a list of approved patches and a vulnerability management process. It is recommended that vulnerability management be planned around scheduled downtime and integrated with the system development lifecycle, configuration management, and change management processes.

C - MANUFACTURING PROFILE SUBCATEGORIES

ID.RA-1, DE.CM-4, RS.MI-3

INCIDENT MANAGEMENT

A - SECURITY BENEFIT

Incident management tools enable manufacturers to minimize downtimes due to incidents and increase the efficiency and productivity of the manufacturing system. Information gained during incident handling can be used to better prepare for handling any future incident.

Incident response plans enable organizations to act proactively before an incident or immediately after an incident is noticed to limit the impact from incidents.

B - POTENTIAL SYSTEM IMPACTS

Incident management tools should not impact the manufacturing system, as they are typically operated and accessed outside of the manufacturing system.

C - MANUFACTURING PROFILE SUBCATEGORIES

RS.MI-2, RS.MI-3

NETWORK MONITORING

A - SECURITY BENEFIT

Network monitoring tools can identify suspicious traffic and other threat vectors, allowing manufacturers to respond fast to an incident. They can help to reduce incidents caused by human error, configuration issues and other environmental factors. Effective network monitoring helps to detect, diagnose, and resolve network performance issues, reducing incidents by proactively identifying threats and bottlenecks.

B - POTENTIAL SYSTEM IMPACTS

Network monitoring tools should not impact the manufacturing system, as they are typically operated and accessed outside of the manufacturing system. However, certain methods of capturing network traffic (e.g., in-line network probes, mirror ports) can increase processing load on network devices and can increase network latency.

C - MANUFACTURING PROFILE SUBCATEGORIES

PR.DS-5, PR.MA-2, PR.PT-4, DE.CM-1, DE.CM-6, DE.CM-7

SYSTEM USE MONITORING

C - MANUFACTURING PROFILE SUBCATEGORIES

PR.AC-1, PR.DS-5, PR.MA-2, DE.CM-3

MAINTENANCE TRACKING

C - MANUFACTURING PROFILE SUBCATEGORIES

PR.MA-1, PR.MA-2

PHYSICAL ACCESS CONTROL

C - MANUFACTURING PROFILE SUBCATEGORIES

PR.AC-2, PR.DS-5, PR.MA-1

PHYSICAL ACCESS MONITORING

C - MANUFACTURING PROFILE SUBCATEGORIES

PR.AC-2, PR.PT-1, DE.CM-2, DE.CM-3

PORTS AND SERVICES LOCKDOWN

C - MANUFACTURING PROFILE SUBCATEGORIES

PR.IP-1, PR.PT-3

MEDIA PROTECTION

A - SECURITY BENEFIT

Media protection solutions reduce the threat of unknown and potentially malicious devices from being connected to the manufacturing system equipment.

B- POTENTIAL SYSTEM IMPACTS

Media protection solutions can potentially impact the manufacturing system. Media protection for privileged users may be impactful to the manufacturing system by limiting their ability to respond to a manufacturing system event or incident. Care must be taken to verify privileged users have the access required to perform their roles and functions.

C - MANUFACTURING PROFILE SUBCATEGORIES

PR.PT-2

ENCRYPTION

A - SECURITY BENEFIT

Encryption provides data confidentiality when data is in use, in transit or at rest by converting plaintext into ciphertext that can only be viewed by recipients having the correct keys. If data is compromised or leaked, the likelihood of sensitive information being exposed would be minimized.

B - POTENTIAL SYSTEM IMPACTS

Tools that perform methods of encryption can potentially impact the manufacturing system.

Computational operations to encrypt and decrypt data require processing power and memory. These effects can be exacerbated when they are executed on embedded devices. Depending on the encryption and decryption methods used, time-sensitive data communications may also be impacted. Additionally, physical network hardware used to encrypt traffic between multiple devices may increase network latency. While encryption is an effective data confidentiality and integrity tool, the implementation must be carefully planned to minimize any potential disruption to the manufacturing processes.

C - MANUFACTURING PROFILE SUBCATEGORIES

PR.DS-5

DATA LOSS PREVENTION

A - SECURITY BENEFIT

Detects and prevents exposure of sensitive information across network devices.

B - POTENTIAL SYSTEM IMPACTS

Network-based data loss prevention tools that monitor and detect data loss should not typically impact the manufacturing system. Endpoint-based data loss prevention tools can potentially impact the manufacturing system, as they utilize processing power and/or network bandwidth. If possible, these tools should be configured to use the minimum amount of processing power required for proper operation.

C - MANUFACTURING PROFILE SUBCATEGORIES

PR.DS-5

MEDIA SANITIZATION

A - SECURITY BENEFIT

Media sanitization solutions ensure confidential information is removed or destroyed from any device containing storage media (e.g., USB flash drives, internal or external hard drives, memory cards). Devices not sanitized appropriately can become a security concern when decommissioned items are no longer in the company's possession.

B - POTENTIAL SYSTEM IMPACTS

Media sanitization tools should not impact the manufacturing system, as they are typically operated outside of the manufacturing system. These processes should be integrated with the configuration and change management processes to ensure accountability and tracking of the components.

C - MANUFACTURING PROFILE SUBCATEGORIES

PR.DS-3, PR-IP-6

EVENT LOGGING

A - SECURITY BENEFIT

Event logging provides important information regarding operations of the system. This information can aid in improving reporting, log collection, analysis, and can help prevent security breaches. Robust logging capabilities help meet any compliance requirements as well as reduce the impact of security incidents.

B - POTENTIAL SYSTEM IMPACTS

Event logging solutions can potentially impact the manufacturing system. For the event logger to operate properly, devices within the manufacturing system must generate messages destined for the logger. Network bandwidth will be consumed to send these messages, and the amount of traffic is highly dependent on the number of hosts and the configured logging level (e.g., critical errors, warnings, debug). A risk-based decision must be made between the amount of consumed network bandwidth and the desired logging level. Processing load may increase on devices that send a large number of messages to the event logger.

C - MANUFACTURING PROFILE SUBCATEGORIES

PR.PT-1, DE.AE-3, DE.CM-1, DE.CM-6, DE.DP-3, RS.AN-3

FORENSICS

A - SECURITY BENEFIT

Collection of forensics-related data within a network environment provides the ability to examine network data for additional evidence needed to determine malicious activities and identify potential actors. Collections of device and network logs can help identify threat actors for prosecution. Forensics-related data are also useful if the incident requires help from an outside incident response company.

B - POTENTIAL SYSTEM IMPACTS

Forensic tools should not impact the manufacturing system, as they are typically operated outside of the manufacturing system.

C - MANUFACTURING PROFILE SUBCATEGORIES

DE.AE-2, RS.AN-3

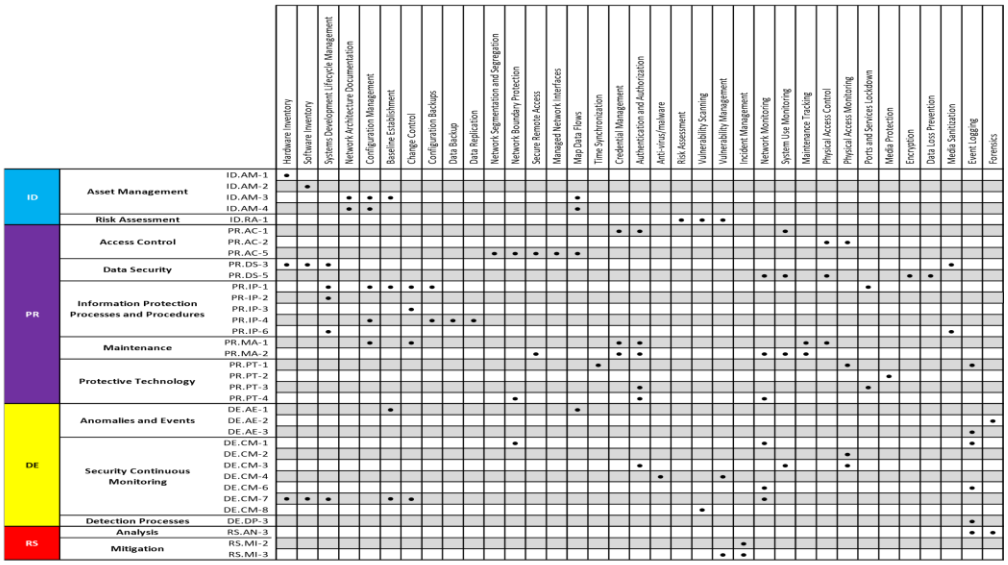


Table 6-1. Mapping of CSF Manufacturing Profile Subcategories to Technical Capabilities

Table 6-1 summarizes the information discussed in this Section and shows the coverage of CSF Manufacturing Profile Subcategories addressed when the technical capabilities are implemented as part of a cybersecurity program.

18. CAPABILITIES MAPPING TO MANUFACTURING PROFILE

This section examines the policies and procedures, described in Section 5, and/or technical solutions, described in Section 6, required to meet the language specified in each particular Subcategory, and lists potential solutions that fulfil the requirements that are accessible by small manufacturers. Accessibility criteria included cost, ease of use, and level of effort to implement. The list of potential solutions is not intended to be all inclusive, but to provide examples. Specific solutions that were implemented in the lab environment for each use case are included in Volume 2 and Volume 3.

FUNCTION	CATEGORY	SUBCATEGORY	MANUFACTURING PROFILE	IMPLEMENTATION OVERVIEW
IDENTIFY	Asset Management (ID.AM)	ID.AM-1	**Low** Document an inventory of manufacturing system components that reflects the current system. Manufacturing system components include for example PLCs, sensors, actuators, robots, machine tools, firmware, network switches, routers, power supplies, and other networked components or devices. System component inventory is reviewed and updated as defined by the organization. Information deemed necessary for effective accountability of manufacturing system components includes, for example, hardware inventory specifications, component owners, networked components or devices, machine names and network addresses. Inventory specifications include, for example, manufacturer, device type, model, serial number, and physical location.	These Subcategory requirements can be met by implementing solutions that provide the **Hardware Inventory** technical capability. Potential solutions for meeting these Subcategory requirements include: Open-AudIT, Nmap, LANSweeper, Spiceworks, OCSinventory-ng, Excel (manual entry) Solutions that were implemented in use cases: Open-AudIT
		ID.AM-2	**Low** Document an inventory of manufacturing system software components that reflects the current system. Manufacturing system software components include for example software license information, software version numbers, HMI and other ICS component applications, software, operating systems. System software inventory is reviewed and updated as defined by the organization.	These Subcategory requirements can be met by implementing solutions that provide the **Software Inventory** technical capability. Potential solutions for meeting these Subcategory requirements include: Open-AudIT, Nmap, LANSweeper, Spiceworks, OCSinventory-ng, Excel (manual entry) Solutions that were implemented in use cases: Open-AudIT
		ID.AM-3	**Low** Document all connections within the manufacturing system, and between the manufacturing system and other systems. All connections are documented, authorized, and reviewed. Connection information includes, for example, the interface characteristics, data characteristics, ports, protocols, addresses, description of the data, security requirements, and the nature of the connection.	These Subcategory requirements can be met by implementing solutions that provide the **Network Architecture Documentation, Configuration Management, Baseline Establishment, and Map Data Flows** technical capabilities. Potential solutions for meeting these Subcategory requirements include: GRASSMARLIN, Microsoft Visio, Wireshark, Nmap, Open-AudIT, Tenable Nessus, Ntopng Solutions that were implemented in use cases GRASSMARLIN Microsoft Visio Wireshark Open AudIT
		ID.AM-4	**Low** Identify and document all external connections for the manufacturing system. Examples of external systems include engineering design services, and those that are controlled under separate authority, personal devices, and other hosted services.	These Subcategory requirements can be met by implementing solutions that provide the **Network Architecture Documentation, Configuration Management, and Map Data Flows** technical capabilities. Potential solutions for meeting these Subcategory requirements include: GRASSMARLIN, Microsoft Visio, Wireshark, Nmap, Open-AudIT, Tenable Nessus, Ntopng Solutions that were implemented in use cases

FUNCTION	CATEGORY	SUBCATEGORY	MANUFACTURING PROFILE	IMPLEMENTATION OVERVIEW
				GRASSMARLIN Microsoft Visio Wireshark Open-AudIT
		ID.AM-5	**Low** Identify and prioritize manufacturing system components and functions based on their classification, criticality, and business value. Identify the types of information in possession, custody, or control for which security safeguards are needed (e.g. sensitive or protected information).	These Subcategory requirements can be met by developing policies and procedures in the **Asset Criticality Matrix** section of the **Risk Management** document
		ID.AM-6	**Low** Establish and maintain personnel cybersecurity roles and responsibilities for the manufacturing system. Include cybersecurity roles and responsibilities for third-party providers. Third-party providers are required to notify the organization of any personnel transition (including transfers or terminations) involving personnel with physical or logical access to the manufacturing system components. Third-party providers include, for example, service providers, contractors, and other organizations providing manufacturing system development, technology services, outsourced applications, or network and security management.	These Subcategory requirements can be met by developing policies and procedures in the **Role-based Security Responsibilities** section of the cybersecurity policy document
	Business Environment (ID.BE)	ID.BE-1	**Low** Define and communicate the organization's role in the supply chain. Identify the upstream and downstream supply channels that are outside of the organization's operations. Identify the overall mission supported by the manufacturing system.	These Subcategory requirements can be met by developing policies and procedures in the **Organization Overview** section of the **Cybersecurity Program** document.
		ID.BE-2	**Low** Define and communicate the manufacturer's place in critical infrastructure and its industry sector. Define and communicate critical infrastructure and key resources relevant to the manufacturing system. Develop, document, and maintain a critical infrastructure and key resources protection plan.	These Subcategory requirements can be met by developing policies and procedures in the **Organization Overview** section of the **Cybersecurity Program** document.
		ID.BE-3	**Low** Establish and communicate priorities for manufacturing missions, objectives, and activities with consideration for security and the resulting risk to manufacturing operations, components, and individuals. Identify critical manufacturing system components and functions by performing a criticality analysis.	These Subcategory requirements can be met by developing policies and procedures in the **Organization Overview** section of the **Cybersecurity Program** document.
		ID.BE-4	**Low** Identify and prioritize supporting services for critical manufacturing system processes and components. Provide an uninterruptable power supply for identified critical manufacturing system components to facilitate the transition of the manufacturing system to long-term alternate power in the event of a primary power source loss.	These Subcategory requirements can be met by developing policies and procedures in the **Organization Overview** and **Emergency Power** sections of the **Cybersecurity Program** document.
		ID.BE-5	**Low** Establish resilience requirements for the manufacturing system to support delivery of critical services.	These Subcategory requirements can be met by developing policies and procedures in the **System Recovery** document.

FUNCTION	CATEGORY	SUBCATEGORY	MANUFACTURING PROFILE	IMPLEMENTATION OVERVIEW
	Governance (ID.GV)	ID.GV-1	**Low** Develop and disseminate a security policy that provides an overview of the security requirements for the manufacturing system. The policy includes, for example, the identification and assignment of roles, responsibilities, management commitment, coordination among organizational entities, and compliance. It also reflects coordination among organizational entities responsible for the different aspects of security (i.e., technical, physical, personnel, cyber-physical, access control, media protection, vulnerability management, maintenance, monitoring), and covers the full life cycle of the manufacturing system. Review and update the security policy as determined necessary. Ensure the security policy is approved by a senior official with responsibility and accountability for the risk being incurred by manufacturing operations.	These Subcategory requirements can be met by developing policies and procedures in the **Cybersecurity Policy** document.
	Governance (ID.GV)	ID.GV-2	**Low**	These Subcategory requirements can be met by developing policies and procedures in the **Cybersecurity Program** document.
	Governance (ID.GV)	ID.GV-2 ID.GV-3	Develop and disseminate a security program for the manufacturing system that includes, for example, the identification of personnel security roles and assignment of responsibilities, management commitment, coordination among organizational entities, and compliance. This includes security requirements, roles and responsibilities for third-party providers. Review and update the security program as determined necessary.	These Subcategory requirements can be met by developing policies and procedures in the **Cybersecurity Program** document. These Subcategory requirements can be met by developing policies and procedures in the **Applicable Laws and Regulations** section of the **Cybersecurity Program** document.
		ID.GV-3 ID.GV-4	**Low** Ensure that legal and regulatory requirements affecting the manufacturing operations regarding cybersecurity are understood and managed.	These Subcategory requirements can be met by developing policies and procedures in the **Applicable Laws and Regulations** section of the **Cybersecurity Program** document. These Subcategory requirements can be met by developing policies and procedures in the **Risk Management** document.
		ID.GV-4	**Low** Develop a comprehensive strategy to manage risk to manufacturing operations. Include cybersecurity considerations in the risk management strategy. Review and update the risk management strategy as determined necessary. Determine and allocate required resources to protect the manufacturing system.	These Subcategory requirements can be met by developing policies and procedures in the **Risk Management** document.
	Risk Assessment (ID.RA)	ID.RA-1	**Low** Develop a plan to identify, document, and report vulnerabilities that exist on the manufacturing system. Include the use of vulnerability scanning where safe and feasible on the manufacturing system, its components, or a representative system.	Some of these Subcategory requirements can be met by implementing solutions that provide the **Risk Assessment, Vulnerability Scanning and Vulnerability Management** technical capabilities. Potential solutions for meeting these Subcategory requirements include: DHS Cybersecurity Evaluation Tool (CSET), NamicSoft, OpenVAS, Tenable Nessus, AlienVault OSSIM, Microsoft Excel (Manual) Solutions that were implemented in use cases: CSET NamicSoft Tenable Nessus Some of these Subcategory requirements can be met by developing policies and procedures in the **Vulnerability Management** section of the **Cybersecurity Operations** document.
		ID.RA-2	**Low**	These Subcategory requirements can be met by developing policies and procedures in the

FUNCTION	CATEGORY	SUBCATEGORY	MANUFACTURING PROFILE	IMPLEMENTATION OVERVIEW
			Establish and maintain ongoing contact with security groups and associations, and receive security alerts and advisories. Security groups and associations include, for example, special interest groups, forums, professional associations, news groups, and/or peer groups of security professionals in similar organizations. Implement a threat awareness program that includes a cross-organization information-sharing capability. Organizations should consider having both an unclassified and classified information sharing capability. Collaborate and share information about potential vulnerabilities and incidents on a timely basis. The DHS National Cybersecurity & Communications Integration Center (NCCIC) serves as a centralized location where operational elements involved in cybersecurity and communications reliance are coordinated and integrated. The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) collaborates with international and private sector Computer Emergency Response Teams (CERTs) to share control systems-related security incidents and mitigation measures.	**Information Sharing Plan** and **Security Awareness Training** sections of the **Cybersecurity Program** document, **Risk Identification** section of the **Risk Management** document, and **Information Sharing Policy** section of the **Incident Response Plan** document.
	Risk Assessment (ID.RA)	ID.RA-3	**Low** Conduct and document periodic assessment of risk to the manufacturing system that takes into account threats and likelihood of impact to manufacturing operations and assets. The risk assessment includes threats from insiders and external parties.	These Subcategory requirements can be met by developing policies and procedures in the **Risk, Monitor and Control** section of the **Risk Management** document.
		ID.RA-4	**Low** Conduct criticality reviews of the manufacturing system that define the potential adverse impacts to manufacturing operations, assets, and individuals if compromised or disabled.	These Subcategory requirements can be met by developing policies and procedures in the **Periodic Reviews** section of the **Risk Management** document.
		ID.RA-5	**Low** Conduct risk assessments of the manufacturing system incorporating threats, vulnerabilities, likelihood, and impact to manufacturing operations, assets, and individuals. Disseminate risk assessment results to relevant stakeholders.	These Subcategory requirements can be met by developing policies and procedures in the **Risk Monitor and Control** and **Risk Reporting** sections of the **Risk Management** document.
		ID.RA-6	**Low** Develop and implement a comprehensive strategy to manage risk to the manufacturing system that includes the identification and prioritization of risk responses.	These Subcategory requirements can be met by developing policies and procedures in the **Risk Management** document.
	Risk Management Strategy (ID.RM)	ID.RM-1	**Low** Establish a risk management process for the manufacturing system that effectively identifies, communicates, and facilitates addressing risk-related issues and information among key stakeholders internally and externally.	These Subcategory requirements can be met by developing policies and procedures in the **Risk Notification Process** section of the **Risk Management** document.
		ID.RM-2	**Low** Define the risk tolerance for the manufacturing system.	These Subcategory requirements can be met by developing policies and procedures in the **Risk Tolerance** section of the **Risk Management** document.
		ID.RM-3	**Low** Ensure the risk tolerance for the manufacturing system is informed by the organization's role in critical infrastructure and sector-specific risk analysis.	These Subcategory requirements can be met by developing policies and procedures in the **Risk Tolerance** section of the **Risk Management** document.
PROTECT	Access Control (PR.AC)	PR.AC-1	**Low** Establish and manage identification mechanisms and credentials for users and of the manufacturing system.	These Subcategory requirements can be met by implementing solutions that provide the **Credential Management, Authentication and Authorization, and System Use Monitoring** technical capabilities. Potential solutions for meeting these Subcategory requirements include: Microsoft Active Directory, FreeIPA, Open LDAP, native operating system/device capabilities. Solutions that were implemented in use cases:

FUNCTION	CATEGORY	SUBCATEGORY	MANUFACTURING PROFILE	IMPLEMENTATION OVERVIEW
				Microsoft Active Directory *Native operating system/device capabilities*
		PR.AC-2	**Low** *Protect physical access to the manufacturing facility. Determine access requirements during emergency situations.* *Maintain and review visitor access records to the facility where the manufacturing system resides.* *Physical access controls may include, for example, lists of authorized individuals, identity credentials, escort requirements, guards, fences, turnstiles, locks, monitoring of facility access.*	*These Subcategory requirements can be met by implementing solutions that provide the **Physical Access Control and Physical Access Monitoring** technical capabilities.* *Potential solutions for meeting these Subcategory requirements include: lists of authorized individuals, sign in/out sheets, identity credentials, escort requirements, guards, fences, turnstiles, locks, electronic access control systems, cameras, monitoring of facility access.* *Solutions that were implemented in use cases:* *Locks* *Fences* *Electronic Access Control System* *Sign in/out sheet*
		PR.AC-3	**Low** *Establish usage restrictions, connection requirements, implementation guidance, and authorizations for remote access to the manufacturing system.* *Provide an explicit indication of active remote access connections to users physically present at the devices.* *Remote access methods include, for example, wireless, dial-up, broadband, VPN connections, mobile device connections, and communications through external networks.*	*These Subcategory requirements can be met by developing policies and procedures in the **Remote Access** section of the cybersecurity policy document.*
	Access Control (PR.AC)	PR.AC-4	**Low** *Define and manage access permissions for users of the manufacturing system. Identify and document user actions that can be performed on the manufacturing system without identification or authentication (e.g. during emergencies).*	*These Subcategory requirements can be met by developing policies and procedures in the **Personnel Actions** section of the **Cybersecurity Operations** document.*
		PR.AC-5	**Low** *Protect network integrity of the manufacturing system, incorporating network segmentation and segregation where appropriate. Identify and control connections between system components. Monitor and control connections and communications at the external boundary and at key internal boundaries within the manufacturing system.* *Employ boundary protection devices.* *Boundary protection mechanisms include, for example, routers, gateways, unidirectional gateways, data diodes, and firewalls separating system components into logically separate networks or subnetworks.*	*These Subcategory requirements can be met by implementing solutions that provide the **Network Segmentation and Segregation, Network Boundary Protection, Secure Remote Access, Managed Network Interfaces, Map Data Flows** technical capabilities.* *Potential solutions for meeting these Subcategory requirements include: routers, gateways, unidirectional gateways, data diodes, firewalls, DMZ, switches, SNORT, BRO, VPNs, remote desktops, Native operating system/device capabilities, GRASSMARLIN, Microsoft Visio, Wireshark, Ntopng* *Solutions that were implemented in use cases:* *Routers* *Firewalls* *DMZ* *Switches* *VPNs* *TeamViewer* *Native operating system/device capabilities* *GRASSMARLIN* *Microsoft Visio* *Wireshark*
	Awareness and Training (PR.AT)	PR.AT-1	**Low** *Provide security awareness training for all manufacturing system users and managers.*	*These Subcategory requirements can be met by developing policies and procedures in the **Security Awareness Training** section of the **Cybersecurity Program** document.*

FUNCTION	CATEGORY	SUBCATEGORY	MANUFACTURING PROFILE	IMPLEMENTATION OVERVIEW
			Training could include, for example, a basic understanding of the protections and user actions needed to maintain security of the system, responding to suspected cybersecurity incidents, and awareness of operational security.	
	Awareness and Training (PR.AT)	PR.AT-2	**Low** *Ensure that users with privileged access to the manufacturing system understand the requirements and responsibilities of their assignments.* *Establish standards for measuring, building, and validating individual qualifications for privileged users.*	*These Subcategory requirements can be met by developing policies and procedures in the **Security Awareness Training** section of the **Cybersecurity Program** document.*
		PR.AT-3	**Low** *Establish and enforce security requirements for third-party providers and users. Ensure that third-party providers understand their responsibilities regarding the security of the manufacturing system and the responsibilities of their assignments. Require notifications be given for any personnel transfers, termination, or transition involving personnel with physical or logical access to the manufacturing system components.* *Ensure that providers of external system services comply with defined security requirements. Monitor and audit external service providers for security compliance.*	*These Subcategory requirements can be met by developing policies and procedures in the **Security Awareness Training and Third party responsibilities and requirements** section of the **Cybersecurity Program** document.*
		PR.AT-4	**Low** *Ensure that senior executives understand the requirements for the security and protection of the manufacturing system, and their responsibilities for achieving them.*	*These Subcategory requirements can be met by developing policies and procedures in the **Commitment from Management** section of the **Cybersecurity Program** document.*
		PR.AT-5	**Low** *Ensure that personnel responsible for the physical protection and security of the manufacturing system and facility are trained for, and understand their responsibilities.* *Establish standards for measuring, building, and validating individual qualifications for physical security personnel.*	*These Subcategory requirements can be met by developing policies and procedures in the **Employee Requirements** section of the cybersecurity policy document.*
	Data Security (PR.DS)	PR.DS-1	**Low** *None*	*NA*
		PR.DS-2	**Low** *None*	*NA*
	Data Security (PR.DS)	PR.DS-3	**Low** *Enforce accountability for all manufacturing system components throughout the system lifecycle, including removal, transfers, and disposition.* *Sanitize portable media prior to disposal, release, or reuse. All system components entering and exiting the facility are authorized, monitored, and controlled, and records are maintained of those items.*	*Some of these Subcategory requirements can be met by implementing solutions that provide the **Hardware Inventory, Software Inventory, Systems Development Lifecycle Management, and Media Sanitization** technical capabilities.* *Potential solutions for meeting these Subcategory requirements include: Open-AudIT, LANSweeper, Spiceworks, OCSinventory-ng, AlienVault OSSIM, MS Excel (Manual), media sanitization tools.* *Solutions that were implemented in use cases:* *Open-AudIT* *DBAN* *Some of these Subcategory requirements can be met by developing policies and procedures in the **Lifecycle Accountability of Devices** section of the **Cybersecurity Policy** document and **Media Sanitization** section of the **Cybersecurity Operations** document.*

FUNCTION	CATEGORY	SUBCATEGORY	MANUFACTURING PROFILE	IMPLEMENTATION OVERVIEW
		PR.DS-4	**Low** Ensure that adequate resources are maintained for manufacturing system information processing, networking, telecommunications, and data storage. Off-load audit records from the manufacturing system for processing to an alternate system.	These Subcategory requirements can be met by developing policies and procedures in the **Monitoring the Manufacturing System** and **Resources are Maintained** sections of the **Cybersecurity Operations** document.
	Data Security (PR.DS)	PR.DS-5	**Low** Protect the manufacturing system against data leaks. Monitor the manufacturing system at the external boundary and at key internal points to detect unauthorized access and use. Develop and document access agreements for all users of the manufacturing system.	Some of these Subcategory requirements can be met by implementing solutions that provide the **Network Monitoring, System Use Monitoring, Physical Access Control, Encryption, and Data Loss Prevention** technical capabilities. Potential solutions for meeting these Subcategory requirements include: Security Onion, SNORT, Suricata, Zeek Network Security Monitor, Native operating system/device capabilities, lists of authorized individuals, sign in/out sheets, identity credentials, escort requirements, guards, fences, turnstiles, locks, electronic access control systems, cameras, monitoring of facility access, Microsoft EFS, Microsoft BitLocker, AxCrypt, VeraCrypt, GTB Inspector, Comodo DOME Solutions that were implemented in use cases: Security Onion Microsoft EFS Locks Fences Electronic Access Control System Sign in/out sheets GTB Inspector VeraCrypt Some of these Subcategory requirements can be met by developing policies and procedures in the **User Access Agreement** section of the **Cybersecurity Policy** document.
		PR.DS-6	**Low** None	N/A
		PR.DS-7	**Low** None	N/A
	Information Protection Processes and Procedures (PR.IP)	PR.IP-1	**Low** Develop, document, and maintain a baseline configuration for the manufacturing system. Baseline configurations include for example, information about manufacturing system components (e.g. software license information, software version numbers, HMI and other ICS component applications, software, operating systems), current version numbers and patch information on operating systems and applications; and configuration settings/parameters), network topology, and the logical placement of those components within the system architecture. Configure the manufacturing system to provide only essential capabilities.	These Subcategory requirements can be met by implementing solutions that provide the **Systems Development Lifecycle Management, Configuration Management, Baseline Establishment, Change Control, Configuration Backups, and Ports and Services Lockdown** technical capabilities. Potential solutions for meeting these Subcategory requirements include: OpenAudIT, LANSweeper, Spiceworks, OCSinventory-ng, Microsoft Excel (Manual), I-doit, Salt, Puppet, Ansible, GRASSMARLIN, Wireshark, Nmap and Native operating system/device capabilities Solutions that were implemented in use cases: Open-AudIT Microsoft Excel

FUNCTION	CATEGORY	SUBCATEGORY	MANUFACTURING PROFILE	IMPLEMENTATION OVERVIEW
			Review the baseline configuration and disable unnecessary capabilities.	GRASSMARLIN Wireshark Native operating system/device capabilities
		PR.IP-2	**Low** Manage the manufacturing system using a system development life cycle that includes security considerations. Include security requirements into the acquisition process of the manufacturing system and its components.	These Subcategory requirements can be met by implementing solutions that provide the **Systems Development Lifecycle Management** technical capability. Potential solutions for meeting these Subcategory requirements include: Open-AudIT, LANSweeper, Spiceworks, OCSinventory-ng, MS Excel (Manual) Solutions that were implemented in use cases: Open -AudIT
	Information Protection Processes and Procedures (PR.IP)	PR.IP-3	**Low** Employ configuration change control for the manufacturing system and its components. Conduct security impact analyses in connection with change control reviews.	Some of these Subcategory requirements can be met by implementing solutions that provide the **Change Control** technical capability. Potential solutions for meeting these Subcategory requirements include: Open-AudIT, GRASSMARLIN, Wireshark, I-doit, Salt, Puppet, Ansible. Solutions that were implemented in use cases: Open-AudIT GRASSMARLIN Wireshark Some of these Subcategory requirements can be met by developing policies and Procedures in the **Change Control** section of the **Cybersecurity Operations** document.
		PR.IP-4	**Low** Conduct and maintain backups for manufacturing system data. Manufacturing system data includes for example software, configurations and settings, documentation, system configuration data including computer configuration backups, application configuration backups, operational control limits, control bands and set points for pre-incident operation for all ICS programmable equipment	These Subcategory requirements can be met by implementing solutions that provide the **Configuration Management, Change Control, Configuration Backups, Data Backup, and Data Replication** technical capabilities. Potential solutions for meeting these Subcategory requirements include: OpenAudIT, I-doit, Salt, Puppet, Ansible, Veeam Backup and Replication, Bacula Systems, Clonezilla, Commvault Backup & Recovery, Redo backup, and Native operating system/device capabilities. Solutions that were implemented in use cases: Open-AudIT Veeam Backup and Replication Native operating system/device capabilities.
	Information Protection Processes and Procedures (PR.IP)	PR.IP-5	**Low** Define, implement, and enforce policy and regulations regarding emergency and safety systems, fire protection systems, and environment controls for the manufacturing system. Fire suppression mechanisms should take the manufacturing environment into account (e.g., water sprinkler systems could be hazardous in specific environments).	These Subcategory requirements can be met by developing policies and procedures in the **Fire and Safety Regulations** section of the **Cybersecurity Program** document.
		PR.IP-6	**Low** Ensure that manufacturing system data is destroyed according to policy	These Subcategory requirements can be met by implementing solutions that provide the **Systems Development Lifecycle Management and Media Sanitization** technical capabilities Potential solutions for meeting these Subcategory requirements include: Open-

FUNCTION	CATEGORY	SUBCATEGORY	MANUFACTURING PROFILE	IMPLEMENTATION OVERVIEW
				AudIT, LANSweeper, Spiceworks, OCSinventory-ng, AlienVault OSSIM, MS Excel (Manual), media sanitization tools. *Solutions that were implemented in use cases:* *Open-AudIT* *DBAN*
		PR.IP-7	***Low*** *Incorporate improvements derived from the monitoring, measurements, assessments, and lessons learned into protection process revisions.* *Ensure that the security plan for the manufacturing system facilitates the review, testing, and continual improvement of the security protection processes.*	*These Subcategory requirements can be met by developing policies and procedures in the* ***Periodic Reevaluation of the Program*** *section of the* ***Cybersecurity Program*** *document.*
		PR.IP-8	***Low*** *Collaborate and share information about manufacturing system related security incidents and mitigation measures with designated sharing partners.* *Employ automated mechanisms where feasible to assist in information collaboration.*	*These Subcategory requirements can be met by developing policies and procedures in the* ***Information Sharing Policy*** *section of the* ***Incident Response Plan*** *document.*
	Information Protection Processes and Procedures (PR.IP)	***PR.IP-9***	***Low*** *Develop and maintain response and recovery plans that identify essential functions and associated contingency requirements, as well as providing a roadmap for implementing incident response. Plans should incorporate recovery objectives, restoration priorities, metrics, contingency roles, personnel assignments and contact information. Address maintaining essential functions despite system disruption, and the eventual restoration of the manufacturing system. Define incident types, resources and management support needed to effectively maintain and mature the incident response and contingency capabilities.*	*These Subcategory requirements can be met by developing policies and procedures in the* ***Incident Response Plan*** *and* ***System Recovery Plan*** *documents.*
		PR.IP-10	***Low*** *Review response and recovery plans to determine the effectiveness of the plans, and the readiness to execute the plans.*	*These Subcategory requirements can be met by developing policies and procedures in the* ***Incident Management*** *section of the* ***Cybersecurity Program*** *document.*
		PR.IP-11	***Low*** *Develop and maintain a personnel security program for the manufacturing system. Personnel security program should include policy, position risk designations, personnel screening, terminations and transfers, access agreements, third-party roles and responsibilities, and personnel sanctions.*	*These Subcategory requirements can be met by developing policies and procedures in the* ***Cybersecurity Program*** *document*
		PR.IP-12	***Low*** *Establish and maintain a process that allows continuous review of vulnerabilities, and defines strategies to mitigate them.*	*These Subcategory requirements can be met by developing policies and procedures in the* ***Vulnerability Management*** *section of the* ***Cybersecurity Operations*** *document.*
	Maintenance (PR.MA)	***PR.MA-1***	***Low*** *Schedule, perform, document and review records of maintenance and repairs on manufacturing system components.*	*Some of these Subcategory requirements can be met by implementing solutions that provide the* ***Configuration Management, Change Control, Credential Management, Authentication and Authorization, Maintenance Tracking, and Physical Access Control*** *technical capabilities.*

FUNCTION	CATEGORY	SUBCATEGORY	MANUFACTURING PROFILE	IMPLEMENTATION OVERVIEW
			Establish a process for maintenance personnel authorization, and escort non-authorized maintenance personnel. *Verify impacted security controls following maintenance or repair*	*Potential solutions for meeting these Subcategory requirements include: Open-AudIT, I-doit, Salt, Puppet, Ansible, GRASSMARLIN, Wireshark, Microsoft Active Directory, FreeIPA, OCSinventory-ng, Fixx, Freshservice, and Microsoft Excel.* *Solutions that were implemented in use cases:* *Open-AudIT* *Microsoft Excel* *GRASSMARLIN* *Wireshark* *Microsoft Active Directory* *Some of these Subcategory requirements can be met by developing policies and procedures in the* ***Physical Security*** *and* ***System Maintenance*** *section of the* ***Cybersecurity Policy*** *document.*
	Maintenance (PR.MA)	***PR.MA-2***	***Low*** *Enforce approval requirements, control, and monitoring, of remote maintenance activities.* *Employ strong authenticators, record keeping, and session termination for remote maintenance.*	*Some of these Subcategory requirements can be met by implementing solutions that provide the* ***Secure Remote Access, Credential Management, Authentication and Authorization, Network Monitoring, System Use Monitoring, and Maintenance Tracking*** *capabilities.* *Potential solutions for meeting these Subcategory requirements include: VPN, Remote desktop, Microsoft Active Directory, FreeIPA, OCSinventory-ng, Fixx, Freshservice, Microsoft Excel, and Native operating system/device capabilities.* *Solutions that were implemented in use cases:* *Cisco AnyConnect VPN* *TeamViewer* *Microsoft Active Directory* *Microsoft Excel* *Native operating system/device capabilities.* *Some of these Subcategory requirements can be met by developing policies and procedures in the* ***Remote Maintenance*** *and* ***System Maintenance*** *section of the* ***Cybersecurity Policy*** *document.*
	Protective Technology (PR.PT)	***PR.PT-1***	***Low*** *Generate audit records containing information that establishes what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or manufacturing components associated with the event.* *Generate time stamps from an internal system clock that is mapped to Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT).*	*These Subcategory requirements can be met by implementing solutions that provide the* ***Time Synchronization, Physical Access Monitoring and Event Logging*** *technical capabilities.* *Potential solutions for meeting these Subcategory requirements include: Native operating system/device capabilities, Electronic Access Control System, Sign in/out sheets, cameras, Graylog, Alienvault – OSSIM, SIEMonster.* *Solutions that were implemented in use cases:* *Native operating system/device capabilities* *Electronic Access Control System* *Sign in/out sheets* *Graylog*
		PR.PT-2	***Low***	

FUNCTION	CATEGORY	SUBCATEGORY	MANUFACTURING PROFILE	IMPLEMENTATION OVERVIEW
	Protective Technology (PR.PT)		Employ safeguards to restrict the use of portable storage devices.	These Subcategory requirements can be met by implementing solutions that provide the **Media Protection** technical capability. Potential solutions for meeting these Subcategory requirements include: USB Port Locks, Native operating system/device capabilities. Solutions that were implemented in use cases: USB Port Locks
		PR.PT-3	**Low** Configure the manufacturing system to provide only essential capabilities	These Subcategory requirements can be met by implementing solutions that provide the **Authentication and Authorization, and Ports and Services Lockdown** technical capabilities. Potential solutions for meeting these Subcategory requirements include: Microsoft Active Directory, FreeIPA, Nmap, Native operating system/device capabilities Solutions that were implemented in use cases: Microsoft Active Directory Native operating system/device capabilities
		PR.PT-4	**Low** Monitor and control communications at the external boundary and at key internal boundaries within the manufacturing system.	These Subcategory requirements can be met by implementing solutions that provide the **Network Boundary Protection, Authentication and Authorization, and Network Monitoring** technical capabilities. Potential solutions for meeting these Subcategory requirements include: firewalls, Security Onion, SNORT, Suricata, Zeek Network Security Monitor, Microsoft Active Directory, FreeIPA Solutions that were implemented in use cases: Microsoft Active Directory Security Onion Firewalls
DETECT	Anomalies and Events (DE.AE)	DE.AE-1	**Low** Ensure that a baseline of network operations and expected data flows for the manufacturing system is developed, documented, and maintained to detect events.	These Subcategory requirements can be met by implementing solutions that provide the **Baseline Establishment and Map Data Flows** technical capabilities. Potential solutions for meeting these Subcategory requirements include: Open-AudIT, GRASSMARLIN, Wireshark, I-doit, Salt, Puppet, Ansible, Microsoft Visio, and Ntopng Solutions that were implemented in use cases: Open-AudIT GRASSMARLIN Wireshark Microsoft Visio
		DE.AE-2	**Low** Review and analyze detected events within the manufacturing system to understand attack targets and methods.	These Subcategory requirements can be met by implementing solutions that provide the **Forensics** technical capability. Potential solutions for meeting these Subcategory requirements include: Graylog, Wireshark, Security Onion, Zeek Network Security Monitor, CAINE (Computer Aided Investigative Environment)

FUNCTION	CATEGORY	SUBCATEGORY	MANUFACTURING PROFILE	IMPLEMENTATION OVERVIEW
				Solutions that were implemented in use cases: Graylog Wireshark Security Onion
		DE.AE-3	**Low** Ensure that event data is compiled across the manufacturing system using various sources such as event reports, audit monitoring, network monitoring, physical access monitoring, and user/administrator reports	These Subcategory requirements can be met by implementing solutions that provide the **Event Logging** technical capability. Potential solutions for meeting these Subcategory requirements include: Graylog, Alienvault – OSSIM, SIEMonster. Solutions that were implemented in use cases: Graylog
	Anomalies and Events (DE.AE)	DE.AE-4	**Low** Determine negative impacts to manufacturing operations, assets, and individuals resulting from detected events, and correlate with risk assessment outcomes.	These Subcategory requirements can be met by developing policies and procedures in the **Monitoring the Manufacturing System** section of the **Cybersecurity Operations** document.
		DE.AE-5	**Low** Define incident alert thresholds for the manufacturing system.	Some of these Subcategory requirements can be met by developing policies and procedures in the **Incident Response Plan** document.
	Security Continuous Monitoring (DE.CM)	DE.CM-1	**Low** Conduct ongoing security status monitoring of the manufacturing system network to detect defined cybersecurity events and indicators of potential cybersecurity events. Detect unauthorized local, network, and remote connections, and identify unauthorized use of the manufacturing system. Generate audit records for defined cybersecurity events. Monitor network communications at the external boundary of the system and at key internal boundaries within the system. Heighten system monitoring activity whenever there is an indication of increased risk.	Some of these Subcategory requirements can be met by implementing solutions that provide the **Network Boundary Protection, Network Monitoring, and Event Logging** technical capabilities. Potential solutions for meeting these Subcategory requirements include: firewalls, Security Onion, SNORT, Suricata, Zeek Network Security Monitor Graylog, Alienvault – OSSIM, SIEMonster. Solutions that were implemented in use cases: Firewalls Security Onion Graylog Some of these Subcategory requirements can be met by developing policies and procedures in the **Continuous Monitoring** section of the **Cybersecurity Policy** document
		DE.CM-2	**Low** Conduct ongoing security status monitoring of the manufacturing system facility to detect physical security incidents.	These Subcategory requirements can be met by implementing solutions that provide the **Physical Access Monitoring** technical capability. Potential solutions for meeting these Subcategory requirements include: electronic access control systems, cameras, Sign in/out sheets Solutions that were implemented in use cases: Electronic access control system Sign in/out sheet
	Security Continuous Monitoring (DE.CM)	DE.CM-3	**Low** Conduct security status monitoring of personnel activity associated with the manufacturing system. Enforce software usage and installation restrictions.	These Subcategory requirements can be met by implementing solutions that provide the **Authentication and Authorization, System Use Monitoring, and Physical Access Monitoring** technical capabilities. Potential solutions for meeting these Subcategory requirements include: Microsoft Active Directory, FreeIPA, Symantec Endpoint Protection, Native operating system/device capabilities, electronic access control systems, cameras, Sign in/out sheets

FUNCTION	CATEGORY	SUBCATEGORY	MANUFACTURING PROFILE	IMPLEMENTATION OVERVIEW
				Solutions that were implemented in use cases: *Active Directory* *Symantec Endpoint Protection* *Native operating system/device capabilities* *Electronic access control system* *Sign in/out sheet*
		DE.CM-4	***Low*** *Deploy malicious code protection mechanisms throughout the manufacturing system where safe and feasible to detect and eradicate malicious code.* *Update malicious code protection mechanisms whenever new releases are available in accordance with the configuration management policy and procedures for the manufacturing system.*	*These Subcategory requirements can be met by implementing solutions that provide the **Anti-virus/malware and Vulnerability Management** technical capabilities.* *Potential solutions for meeting these Subcategory requirements include: Symantec Endpoint Protection, ClamAV, NamicSoft, OpenVAS, Tenable Nessus* *Solutions that were implemented in use cases:* *Symantec Endpoint Protection* *NamicSoft*
		DE.CM-5	***Low*** *None*	*NA*
	Security Continuous Monitoring (DE.CM)	**DE.CM-6**	***Low*** *Conduct ongoing security status monitoring of external service provider activity on the manufacturing system.* *Detect defined cybersecurity events and indicators of potential cybersecurity events from external service providers.* *Monitor compliance of external providers with personnel security policies and procedures, and contract security requirements.*	*These Subcategory requirements can be met by implementing solutions that provide the **Network Monitoring and Event Logging** technical capabilities.* *Potential solutions for meeting these Subcategory requirements include: Security Onion, SNORT, Suricata, Zeek Network Security Monitor, Graylog, Alienvault – OSSIM, SIEMonster.* *Solutions that were implemented in use cases:* *Security Onion* *Graylog*
		DE.CM-7	***Low*** *Conduct ongoing security status monitoring on the manufacturing system for unauthorized personnel, connections, devices, access points, and software.* *Monitor for system inventory discrepancies.*	*These Subcategory requirements can be met by implementing solutions that provide the **Hardware Inventory, Software Inventory, Systems Development Lifecycle Management, Baseline Establishment, Change Control, and Network Monitoring** technical capabilities.* *Potential solutions for meeting these Subcategory requirements include: Open-AudIT, LANSweeper, Spiceworks, OCSinventory-ng, AlienVault OSSIM, Microsoft Excel (Manual), I-doit, Salt, Puppet, Ansible, GRASSMARLIN, Wireshark, Security Onion, SNORT, Suricata, Zeek Network Security Monitor* *Solutions that were implemented in use cases:* *Open-AudIT* *GRASSMARLIN* *Wireshark* *Microsoft Excel* *Security Onion*
	Security	**DE.CM-8**	***Low***	

FUNCTION	CATEGORY	SUBCATEGORY	MANUFACTURING PROFILE	IMPLEMENTATION OVERVIEW
	Continuous Monitoring (DE.CM)		*Conduct vulnerability scans on the manufacturing system where safe and feasible. Include analysis, remediation, and information sharing in the vulnerability scanning process.* *Employ control system-specific vulnerability scanning tools and techniques where safe and feasible.* *Active vulnerability scanning, which introduces network traffic, is used with care on manufacturing systems to ensure that system functions are not adversely impacted by the scanning process.*	*Some of these Subcategory requirements can be met by implementing solutions that provide the **Vulnerability Scanning** capability.* *Potential solutions for meeting these Subcategory requirements include: Tenable Nessus, OpenVAS, AlienVault OSSIM* *Solutions that were implemented in use cases:* *Tenable Nessus* *Some Subcategory requirements can be met by developing policies and procedures in the **Vulnerability Management** section of the **Cybersecurity Operations** document.*
	Detection Processes (DE.DP)	**DE.DP-1**	***Low*** *Define roles and responsibilities for detection activities on the manufacturing system and ensure accountability.*	*These Subcategory requirements can be met by developing policies and procedures in the **Role-based Security Responsibilities** section of the **Cybersecurity Policy** document.*
		DE.DP-2	***Low*** *Conduct detection activities in accordance with applicable federal and state laws, industry regulations and standards, policies, and other applicable requirements.*	*These Subcategory requirements can be met by developing policies and procedures in the **Continuous Monitoring** section of the **Cybersecurity Policy** document.*
		DE.DP-3	***Low, Moderate and High*** *Validate that event detection processes are operating as intended.*	*These Subcategory requirements can be met by implementing solutions that provide the **Event Logging** technical capability.* *Potential solutions for meeting these Subcategory requirements include: Graylog, Alienvault – OSSIM, SIEMonster.* *Solutions that were implemented in use cases:* *Graylog*
	Detection Processes (DE.DP)	**DE.DP-4**	***Low*** *Communicate event detection information to defined personnel.* *Event detection information includes for example, alerts on atypical account usage, unauthorized remote access, wireless connectivity, mobile device connection, altered configuration settings, contrasting system component inventory, use of maintenance tools and nonlocal maintenance, physical access, temperature and humidity, equipment delivery and removal, communications at the information system boundaries, use of mobile code, use of VoIP, and malware disclosure.*	*These Subcategory requirements can be met by developing policies and procedures in the **Continuous Monitoring** section of the **Cybersecurity Policy** document.*
		DE.DP-5	***Low*** *Incorporate improvements derived from the monitoring, measurements, assessments, and lessons learned into detection process revisions.* *Ensure the security plan for the manufacturing system provides for the review, testing, and continual improvement of the security detection processes.*	*These Subcategory requirements can be met by developing policies and procedures in the **Incident Management** and **Periodic Reevaluation of the Program** section of the **Cybersecurity Program** document.*
RESPOND	***Response Planning (RS.RP)***	**RS.RP-1**	***Low*** *Execute the response plan during or after a cybersecurity event on the manufacturing system.*	*These Subcategory requirements can be met by developing policies and procedures in the **Purpose and Scope** section of the **Incident Response Plan** document.*
	Communications (RS.CO)	**RS.CO-1**	***Low*** *Ensure personnel understand objectives, restoration priorities, task sequences and assignment responsibilities for event response.*	*These Subcategory requirements can be met by developing policies and procedures in the **Policy** section of the **Incident Response Plan** document*

FUNCTION	CATEGORY	SUBCATEGORY	MANUFACTURING PROFILE	IMPLEMENTATION OVERVIEW
	Communications (RS.CO)	RS.CO-2	**Low** Employ prompt reporting to appropriate stakeholders for cybersecurity events on the manufacturing system. Ensure that cybersecurity events on the manufacturing system are reported consistent with the response plan.	These Subcategory requirements can be met by developing policies and procedures in the **Internal and External Communications** section of the **Incident Response Plan** document
		RS.CO-3	**Low** Share cybersecurity incident information with relevant stakeholders per the response plan.	These Subcategory requirements can be met by developing policies and procedures in the **Internal and External Communications Policy** section of the **Incident Response Plan** document.
		RS.CO-4	**Low** Coordinate cybersecurity incident response actions with all relevant stakeholders. Stakeholders for incident response include for example, mission/business owners, manufacturing system owners, integrators, vendors, human resources offices, physical and personnel security offices, legal departments, operations personnel, and procurement offices.	These Subcategory requirements can be met by developing policies and procedures in the **Internal and External Communications** section of the **Incident Response Plan** document
		RS.CO-5	**Low** Share cybersecurity event information voluntarily, as appropriate, with industry security groups to achieve broader cybersecurity situational awareness. For example, the DHS National Cybersecurity & Communications Integration Center (NCCIC) serves as a centralized location where operational elements involved in cybersecurity and communications reliance are coordinated and integrated. The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) collaborates with international and private sector Computer Emergency Response Teams (CERTs) to share control systems-related cybersecurity incidents and mitigation measures.	These Subcategory requirements can be met by developing policies and procedures in the **Continuous Monitoring** section of the **Cybersecurity Policy** document.
	Analysis (RS.AN)	RS.AN-1	**Low** Investigate cybersecurity-related notifications generated from detection systems.	These Subcategory requirements can be met by developing policies and procedures in the **Monitoring the Manufacturing System** section of the **Cybersecurity Operations** document.
		RS.AN-2	**Low** Understand the full implication of the cybersecurity incident based on thorough investigation and analysis results. Correlate detected event information and incident responses with risk assessment outcomes to achieve perspective on incident impact across the organization.	These Subcategory requirements can be met by developing policies and procedures in the **Policy** section of the **Incident Response Plan** document
		RS.AN-3	**Low** Conduct forensic analysis on collected cybersecurity event information to determine root cause.	These Subcategory requirements can be met by implementing solutions that provide the **Event Logging and Forensics** technical capabilities. Potential solutions for meeting these Subcategory requirements include: Graylog, Wireshark, Zeek Network Security Monitor, CAINE (Computer Aided Investigative Environment), Alienvault – OSSIM, SIEMonster, Security Onion Solutions that were implemented in use cases: Graylog Wireshark Security Onion

FUNCTION	CATEGORY	SUBCATEGORY	MANUFACTURING PROFILE	IMPLEMENTATION OVERVIEW
		RS.AN-4	**Low** Categorize cybersecurity incidents according to level of severity and impact consistent with the response plan.	These Subcategory requirements can be met by developing policies and procedures in the **Incident Severity Classification** section of the **Incident Response Plan** document.
	Mitigation (RS.MI)	RS.MI-1	**Low** Contain cybersecurity incidents to minimize impact on the manufacturing system.	These Subcategory requirements can be met by developing policies and procedures in the **Incident Response Workflow** section of the **Incident Response Plan** document.
		RS.MI-2	**Low** Mitigate cybersecurity incidents occurring on the manufacturing system.	These Subcategory requirements can be met by implementing solutions that provide the **Incident Management** technical capability. Potential solutions for meeting these Subcategory requirements include: Sandia Cyber Omni Tracker (SCOT), The Hive Project, Request Tracker Incident Response (RTIR) Solutions that were implemented in use cases: The Hive Project
		RS.MI-3	**Low** Ensure that vulnerabilities identified while responding to a cybersecurity incident are mitigated or documented as accepted risks.	These Subcategory requirements can be met by implementing solutions that provide the **Vulnerability Management and Incident Management** technical capabilities. Potential solutions for meeting these Subcategory requirements include: NamicSoft, OpenVAS, Tenable Nessus, AlienVault OSSIM, Sandia Cyber Omni Tracker (SCOT), The Hive Project, Request Tracker Incident Response (RTIR) Solutions that were implemented in use cases: NamicSoft The Hive Project
	Improvements (RS.IM)	RS.IM-1	**Low** Incorporate lessons learned from ongoing incident handling activities into incident response procedures, training, and testing, and implement the resulting changes accordingly.	These Subcategory requirements can be met by developing policies and procedures in the **Policy** section of the **Incident Response Plan** document
		RS.IM-2	**Low** Update the response plans to address changes to the organization, manufacturing system, attack vectors, or environment of operation and problems encountered during plan implementation, execution, or testing. Updates may include, for example, responses to disruptions or failures, and predetermined procedures Enable a process for the response plan to evolve to reflect new threats, improved technology, and lessons learned.	These Subcategory requirements can be met by developing policies and procedures in the **Policy** section of the **Incident Response Plan** document
RECOVER	Recovery Planning (RC.RP)	RC.RP-1	**Low** Execute the recovery plan during or after a cybersecurity incident on the manufacturing system. Restore the manufacturing system within a predefined time-period from configuration-controlled and integrity-protected information representing a known, operational state for the components.	These Subcategory requirements can be met by developing policies and procedures in the **Objectives** section of the **System Recovery Plan** document.
	Improvements (RC.IM)	RC.IM-1	**Low** Incorporate lessons learned from ongoing recovery activities into system recovery procedures, training, and testing, and implement the resulting changes accordingly.	These Subcategory requirements can be met by developing policies and procedures in the **Plan Testing** and **Plan Maintenance** sections of the **System Recovery Plan** document.
		RC.IM-2	**Low**	

FUNCTION	CATEGORY	SUBCATEGORY	MANUFACTURING PROFILE	IMPLEMENTATION OVERVIEW
	Improvements (RC.IM)		Update the recovery plan to address changes to the organization, manufacturing system, or environment of operation and problems encountered during plan implementation, execution, or testing. Ensure that updates are integrated into the recovery plans.	These Subcategory requirements can be met by developing policies and procedures in the **Plan Testing** and **Plan Maintenance** sections of the **System Recovery Plan** document.
	Communications (RC.CO)	RC.CO-1	**Low** Centralize and coordinate information distribution, and manage the public facing representation of the organization. Public relations management may include, for example, managing media interactions, coordinating and logging all requests for interviews, handling and 'triaging' phone calls and e-mail requests, matching media requests with appropriate and available internal experts who are ready to be interviewed, screening all of information provided to the media, ensuring personnel are familiar with public relations and privacy policies.	These Subcategory requirements can be met by developing policies and procedures in the **Internal and External Communications** section of the **System Recovery Plan** document.
		RC.CO-2	**Low** Employ a crisis response strategy to protect against negative impact and repair organizational reputation. Crisis response strategies include, for example, actions to shape attributions of the crisis, change perceptions of the organization in crisis, and reduce the negative effect generated by the crisis.	These Subcategory requirements can be met by developing policies and procedures in the **Internal and External Communications** section of the **System Recovery Plan** document
		RC.CO-3	**Low** Communicate recovery activities to all relevant stakeholders, and executive and management teams.	These Subcategory requirements can be met by developing policies and procedures in the **Internal and External Communications** section of the **System Recovery Plan** document.

19. MANUFACTURING BUSINESS/MISSION OBJECTIVES

Lo sviluppo del Profilo ha incluso l'identificazione dei comuni obiettivi aziendali e della missione nel settore manifatturiero.

Questi obiettivi forniscono il contesto necessario per identificare e gestire le attività di mitigazione del rischio di sicurezza informatica.

Sono stati individuati cinque obiettivi comuni:

1. *Mantenere la sicurezza ambientale*
2. *Mantenere la sicurezza umana*
3. *Mantenere gli obiettivi di produzione*
4. *Mantenere la qualità del prodotto*
5. *Mantenere le informazioni sensibili*

IMPLEMENTAZIONE DEL CYBERSECURITY FRAMEWORK (CSF) NELLA PRODUZIONE MANIFATTURIERA

Il «Profilo di Produzione» del CSF può essere utilizzato come piano delle attività per ridurre il rischio di sicurezza informatica per i produttori in linea con gli obiettivi del settore manifatturiero.

Questo Profilo di Produzione fornisce un approccio basato sul rischio per la gestione delle attività di sicurezza informatica e la riduzione del rischio informatico per i sistemi di produzione.

I Sistemi di Controllo Industriale (Industrial Control Systems - ICS), che includono i sistemi di produzione, rappresentano diversi tipi di sistemi di controllo tra cui Sistemi di Controllo di Supervisione e Acquisizione Dati (Supervisory Control And Data Acquisitions - SCADA), Sistemi di Controllo Distribuito (distributed control systems - DCS) e altre configurazioni di sistemi di controllo come Controllori Logici Programmabili (Programmable Logic Controllers - PLC) spesso presenti nei settori industriali e delle infrastrutture critiche. Un ICS è costituito da combinazioni di componenti di controllo (ad esempio, elettrici, meccanici, idraulici e pneumatici) che agiscono insieme per raggiungere un obiettivo industriale (ad esempio, produzione, trasporto di materia o energia).

ICS supporta il vasto e diversificato settore industriale manifatturiero e può essere classificato come basato su processo, basato su componenti discreti o una combinazione di entrambi.

Il Profilo di Produzione può essere caratterizzato come l'allineamento di standard, linee guida e pratiche al Framework Core in uno scenario di implementazione pratica.

Le industrie manifatturiere basate sui processi utilizzano in genere due tipi di processi principali:

1. PROCESSI DI PRODUZIONE CONTINUI. *Questi processi vengono eseguiti continuamente, spesso con fasi per realizzare diversi gradi di un prodotto. I tipici processi di produzione continua includono il flusso di carburante o vapore in una centrale elettrica, petrolio in una raffineria e distillazione in un impianto chimico.*
2. PROCESSI DI PRODUZIONE IN BATCH. *Questi processi hanno fasi di lavorazione distinte, condotte su una quantità di materiale. C'è un inizio e una fine distinti di un processo batch con la possibilità di brevi operazioni stazionarie durante le fasi intermedie. I tipici processi di produzione in batch includono la produzione di alimenti, bevande e biotecnologie.*

Allo scopo di mantenere:

1. SICUREZZA AMBIENTALE*: gestire i rischi di sicurezza informatica che potrebbero influire negativamente sull'ambiente, compresi i danni accidentali e intenzionali; il rischio di cibersicurezza sul sistema di produzione potrebbe potenzialmente influire negativamente sulla sicurezza ambientale; il personale dovrebbe comprendere le interdipendenze di sicurezza informatica e sicurezza ambientale.*
2. SICUREZZA UMANA*: gestire i rischi per la sicurezza informatica che potrebbero avere un potenziale impatto sulla sicurezza umana; il rischio per la sicurezza informatica sul sistema di produzione potrebbe potenzialmente influire negativamente sulla sicurezza umana; il personale dovrebbe comprendere la sicurezza informatica e le interdipendenze in materia di sicurezza.*
3. OBIETTIVI DI PRODUZIONE*: gestire i rischi di sicurezza informatica che potrebbero influire negativamente sugli obiettivi di produzione; il rischio di sicurezza informatica sul sistema di produzione, compreso il danneggiamento degli asset, potrebbe potenzialmente influire negativamente sugli obiettivi di produzione; il personale dovrebbe comprendere la sicurezza informatica e le interdipendenze degli obiettivi di produzione.*
4. QUALITÀ DEL PRODOTTO*: gestire i rischi di sicurezza informatica che potrebbero influire negativamente sulla qualità del prodotto; protezione contro la compromissione dell'integrità del processo di produzione e dei dati associati.*
5. INFORMAZIONI SENSIBILI*: gestire i rischi per la sicurezza informatica che potrebbero portare alla perdita o alla compromissione della proprietà intellettuale dell'organizzazione e dei dati aziendali sensibili, comprese le informazioni di identificazione personale (PII).*

ESEMPI APPLICAZIONE TABELLA FUNZIONI

Table 2 *IDENTIFY Business Mission Objectives*

		Maintain Human Safety	Maintain Environmental Safety	Maintain Quality of Product	Maintain Production Goals	Maintain Trade Secrets
Category		Subcategories				
ID	Asset Management	ID.AM-1	ID.AM-1	ID.AM-1	ID.AM-1	ID.AM-1
		ID.AM-2	ID.AM-2	ID.AM-2	ID.AM-2	ID.AM-2
		ID.AM-3	ID.AM-3	ID.AM-3	ID.AM-3	ID.AM-3
		ID.AM-4	ID.AM-4	ID.AM-4	ID.AM-4	ID.AM-4
		ID.AM-5	ID.AM-5	ID.AM-5	ID.AM-5	ID.AM-5
		ID.AM-6	ID.AM-6	ID.AM-6	ID.AM-6	ID.AM-6
	Business Environment	ID.BE-1	ID.BE-1	ID.BE-1	ID.BE-1	ID.BE-1
		ID.BE-2	ID.BE-2	ID.BE-2	ID.BE-2	ID.BE-2
		ID.BE-3	ID.BE-3	ID.BE-3	ID.BE-3	ID.BE-3
		ID.BE-4	ID.BE-4	ID.BE-4	ID.BE-4	ID.BE-4
		ID.BE-5	ID.BE-5	ID.BE-5	ID.BE-5	ID.BE-5
	Governance	ID.GV-1	ID.GV-1	ID.GV-1	ID.GV-1	ID.GV-1
		ID.GV-2	ID.GV-2	ID.GV-2	ID.GV-2	ID.GV-2
		ID.GV-3	ID.GV-3	ID.GV-3	ID.GV-3	ID.GV-3
		ID.GV-4	ID.GV-4	ID.GV-4	ID.GV-4	ID.GV-4
	Risk Assessment	ID.RA-1	ID.RA-1	ID.RA-1	ID.RA-1	ID.RA-1
		ID.RA-2	ID.RA-2	ID.RA-2	ID.RA-2	ID.RA-2
		ID.RA-3	ID.RA-3	ID.RA-3	ID.RA-3	ID.RA-3
		ID.RA-4	ID.RA-4	ID.RA-4	ID.RA-4	ID.RA-4
		ID.RA-5	ID.RA-5	ID.RA-5	ID.RA-5	ID.RA-5
		ID.RA-6	ID.RA-6	ID.RA-6	ID.RA-6	ID.RA-6
	Risk Management Strategy	ID.RM-1	ID.RM-1	ID.RM-1	ID.RM-1	ID.RM-1
		ID.RM-2	ID.RM-2	ID.RM-2	ID.RM-2	ID.RM-2
		ID.RM-3	ID.RM-3	ID.RM-3	ID.RM-3	ID.RM-3
	Supply Chain Management	ID.SC-1	ID.SC-1	ID.SC-1	ID.SC-1	ID.SC-1
		ID.SC-2	ID.SC-2	ID.SC-2	ID.SC-2	ID.SC-2
		ID.SC-3	ID.SC-3	ID.SC-3	ID.SC-3	ID.SC-3
		ID.SC-4	ID.SC-4	ID.SC-4	ID.SC-4	ID.SC-4
		ID.SC-5	ID.SC-5	ID.SC-5	ID.SC-5	ID.SC-5

Table 3 *PROTECT Business Mission Objectives*

		Maintain Human Safety	Maintain Environmental Safety	Maintain Quality of Product	Maintain Production Goals	Maintain Trade Secrets
Category		Subcategories				
PR	Identity Management, Authentication and Access Control	PR.AC-1	PR.AC-1	PR.AC-1	PR.AC-1	PR.AC-1
		PR.AC-2	PR.AC-2	PR.AC-2	PR.AC-2	PR.AC-2
		PR.AC-3	PR.AC-3	PR.AC-3	PR.AC-3	PR.AC-3
		PR.AC-4	PR.AC-4	PR.AC-4	PR.AC-4	PR.AC-4
		PR.AC-5	PR.AC-5	PR.AC-5	PR.AC-5	PR.AC-5
		PR.AC-6	PR.AC-6	PR.AC-6	PR.AC-6	PR.AC-6
		PR.AC-7	PR.AC-7	PR.AC-7	PR.AC-7	PR.AC-7
	Awareness and Training	PR.AT-1	PR.AT-1	PR.AT-1	PR.AT-1	PR.AT-1
		PR.AT-2	PR.AT-2	PR.AT-2	PR.AT-2	PR.AT-2
		PR.AT-3	PR.AT-3	PR.AT-3	PR.AT-3	PR.AT-3
		PR.AT-4	PR.AT-4	PR.AT-4	PR.AT-4	PR.AT-4
		PR.AT-5	PR.AT-5	PR.AT-5	PR.AT-5	PR.AT-5
	Data Security	PR.DS-1	PR.DS-1	PR.DS-1	PR.DS-1	PR.DS-1
		PR.DS-2	PR.DS-2	PR.DS-2	PR.DS-2	PR.DS-2
		PR.DS-3	PR.DS-3	PR.DS-3	PR.DS-3	PR.DS-3
		PR.DS-4	PR.DS-4	PR.DS-4	PR.DS-4	PR.DS-4
		PR.DS-5	PR.DS-5	PR.DS-5	PR.DS-5	PR.DS-5
		PR.DS-6	PR.DS-6	PR.DS-6	PR.DS-6	PR.DS-6
		PR.DS-7	PR.DS-7	PR.DS-7	PR.DS-7	PR.DS-7
		PR.DS-8	PR.DS-8	PR.DS-8	PR.DS-8	PR.DS-8
	Information Protection Processes and Procedures	PR.IP-1	PR.IP-1	PR.IP-1	PR.IP-1	PR.IP-1
		PR.IP-2	PR.IP-2	PR.IP-2	PR.IP-2	PR.IP-2
		PR.IP-3	PR.IP-3	PR.IP-3	PR.IP-3	PR.IP-3
		PR.IP-4	PR.IP-4	PR.IP-4	PR.IP-4	PR.IP-4
		PR.IP-5	PR.IP-5	PR.IP-5	PR.IP-5	PR.IP-5
		PR.IP-6	PR.IP-6	PR.IP-6	PR.IP-6	PR.IP-6
		PR.IP-7	PR.IP-7	PR.IP-7	PR.IP-7	PR.IP-7
		PR.IP-8	PR.IP-8	PR.IP-8	PR.IP-8	PR.IP-8
		PR.IP-9	PR.IP-9	PR.IP-9	PR.IP-9	PR.IP-9
		PR.IP-10	PR.IP-10	PR.IP-10	PR.IP-10	PR.IP-10
		PR.IP-11	PR.IP-11	PR.IP-11	PR.IP-11	PR.IP-11
		PR.IP-12	PR.IP-12	PR.IP-12	PR.IP-12	PR.IP-12
	Maintenance	PR.MA-1	PR.MA-1	PR.MA-1	PR.MA-1	PR.MA-1
		PR.MA-2	PR.MA-2	PR.MA-2	PR.MA-2	PR.MA-2
	Protective Technology	PR.PT-1	PR.PT-1	PR.PT-1	PR.PT-1	PR.PT-1
		PR.PT-2	PR.PT-2	PR.PT-2	PR.PT-2	PR.PT-2
		PR.PT-3	PR.PT-3	PR.PT-3	PR.PT-3	PR.PT-3
		PR.PT-4	PR.PT-4	PR.PT-4	PR.PT-4	PR.PT-4
		PR.PT-5	PR.PT-5	PR.PT-5	PR.PT-5	PR.PT-5

Table 4 *DETECT Business Mission Objectives*

		Maintain Human Safety	Maintain Environmental Safety	Maintain Quality of Product	Maintain Production Goals	Maintain Trade Secrets
Category		Subcategories				
DE	Anomalies and Events	DE.AE-1	DE.AE-1	DE.AE-1	DE.AE-1	DE.AE-1
		DE.AE-2	DE.AE-2	DE.AE-2	DE.AE-2	DE.AE-2
		DE.AE-3	DE.AE-3	DE.AE-3	DE.AE-3	DE.AE-3
		DE.AE-4	DE.AE-4	DE.AE-4	DE.AE-4	DE.AE-4
		DE.AE-5	DE.AE-5	DE.AE-5	DE.AE-5	DE.AE-5
	Security Continuous Monitoring	DE.CM-1	DE.CM-1	DE.CM-1	DE.CM-1	DE.CM-1
		DE.CM-2	DE.CM-2	DE.CM-2	DE.CM-2	DE.CM-2
		DE.CM-3	DE.CM-3	DE.CM-3	DE.CM-3	DE.CM-3
		DE.CM-4	DE.CM-4	DE.CM-4	DE.CM-4	DE.CM-4
		DE.CM-5	DE.CM-5	DE.CM-5	DE.CM-5	DE.CM-5
		DE.CM-6	DE.CM-6	DE.CM-6	DE.CM-6	DE.CM-6
		DE.CM-7	DE.CM-7	DE.CM-7	DE.CM-7	DE.CM-7
		DE.CM-8	DE.CM-8	DE.CM-8	DE.CM-8	DE.CM-8
	Detection Processes	DE.DP-1	DE.DP-1	DE.DP-1	DE.DP-1	DE.DP-1
		DE.DP-2	DE.DP-2	DE.DP-2	DE.DP-2	DE.DP-2
		DE.DP-3	DE.DP-3	DE.DP-3	DE.DP-3	DE.DP-3
		DE.DP-4	DE.DP-4	DE.DP-4	DE.DP-4	DE.DP-4
		DE.DP-5	DE.DP-5	DE.DP-5	DE.DP-5	DE.DP-5

Table 5 *RESPOND Business Mission Objectives*

		Maintain Human Safety	Maintain Environmental Safety	Maintain Quality of Product	Maintain Production Goals	Maintain Trade Secrets
Category		Subcategories				
RS	Response Planning	RS.RP-1	RS.RP-1	RS.RP-1	RS.RP-1	RS.RP-1
	Communications	RS.CO-1	RS.CO-1	RS.CO-1	RS.CO-1	RS.CO-1
		RS.CO-2	RS.CO-2	RS.CO-2	RS.CO-2	RS.CO-2
		RS.CO-3	RS.CO-3	RS.CO-3	RS.CO-3	RS.CO-3
		RS.CO-4	RS.CO-4	RS.CO-4	RS.CO-4	RS.CO-4
		RS.CO-5	RS.CO-5	RS.CO-5	RS.CO-5	RS.CO-5
	Analysis	RS.AN-1	RS.AN-1	RS.AN-1	RS.AN-1	RS.AN-1
		RS.AN-2	RS.AN-2	RS.AN-2	RS.AN-2	RS.AN-2
		RS.AN-3	RS.AN-3	RS.AN-3	RS.AN-3	RS.AN-3
		RS.AN-4	RS.AN-4	RS.AN-4	RS.AN-4	RS.AN-4
		RS.AN-5	RS.AN-5	RS.AN-5	RS.AN-5	RS.AN-5
	Mitigation	RS.MI-1	RS.MI-1	RS.MI-1	RS.MI-1	RS.MI-1
		RS.MI-2	RS.MI-2	RS.MI-2	RS.MI-2	RS.MI-2
		RS.MI-3	RS.MI-3	RS.MI-3	RS.MI-3	RS.MI-3
	Improvements	RS.IM-1	RS.IM-1	RS.IM-1	RS.IM-1	RS.IM-1
		RS.IM-2	RS.IM-2	RS.IM-2	RS.IM-2	RS.IM-2

Table 6 *RECOVER Business Mission Objectives*

		Maintain Human Safety	Maintain Environmental Safety	Maintain Quality of Product	Maintain Production Goals	Maintain Trade Secrets
Category		Subcategories				
RC	Recovery Planning	RC.RP-1	RC.RP-1	RC.RP-1	RC.RP-1	RC.RP-1
	Improvements	RC.IM-1	RC.IM-1	RC.IM-1	RC.IM-1	RC.IM-1
		RC.IM-2	RC.IM-2	RC.IM-2	RC.IM-2	RC.IM-2
	Communications	RC.CO-1	RC.CO-1	RC.CO-1	RC.CO-1	RC.CO-1
		RC.CO-2	RC.CO-2	RC.CO-2	RC.CO-2	RC.CO-2
		RC.CO-3	RC.CO-3	RC.CO-3	RC.CO-3	RC.CO-3

LIVELLI D'IMPATTO

Oltre agli obiettivi per l'allineamento di un insieme di controlli di sicurezza a supporto degli obiettivi aziendali critici, il Profilo di Produzione è anche strutturato in 3 livelli d'impatto basati sulla categorizzazione delle informazioni e dei processi all'interno del sistema di produzione.

Questo capitolo è composto da 3 passi:

1. CATEGORIZATION PROCESS
2. PROFILE'S HIERARCHICAL SUPPORTING STRUCTURE
3. RISK MANAGEMENT

CATEGORIZATION PROCESS

È il primo passo del NIST Risk Management Framework (RMF) e fornisce alle organizzazioni informazioni per supportare la personalizzazione dell'implementazione del controllo della sicurezza informatica. Come definito dal NIST Federal Information Processing Standard (FIPS) 199, il processo di categorizzazione si basa su 3 livelli d'impatto: **BASSO**, **MODERATO** *o* **ALTO**.

1. BASSO*: se ci si può aspettare che la perdita di integrità, disponibilità o riservatezza abbia un effetto negativo limitato sulle operazioni di produzione, sui prodotti fabbricati, sulle risorse, sull'immagine del marchio, sulle finanze, sul personale, sul pubblico in generale o sull'ambiente.*
2. MODERATO*: se ci si può aspettare che la perdita di integrità, disponibilità o riservatezza abbia un grave effetto negativo sulle operazioni di produzione, sui prodotti fabbricati, sulle risorse, sull'immagine del marchio, sulle finanze, sul personale, sul pubblico in generale o sull'ambiente.*
3. ALTO*: se ci si può aspettare che la perdita di integrità, disponibilità o riservatezza abbia un effetto negativo grave o catastrofico sulle operazioni di produzione, sui prodotti fabbricati, sulle risorse, sull'immagine del marchio, sulle finanze, sul personale, sul pubblico in generale o sull'ambiente*

Le tabelle seguenti forniscono esempi di motivazioni basate sulla missione per la selezione della categorizzazione di sicurezza del sistema di produzione

Table 7 Manufacturing System Impact Levels [3]

Impact Category	Low Impact	Moderate Impact	High Impact
Injury	Cuts, bruises requiring first aid	Requires hospitalization	Loss of life or limb
Financial Loss ($)	Tens of thousands	Hundreds of thousands	Millions
Environmental Release	Temporary damage	Lasting damage	Permanent damage, off-site damage
Interruption of Production	Temporary reductions without impacting quarterly production	Temporary reductions requiring additional shifts or overtime to meet quarterly production	Significant reduction and impact to meet quarterly production
Public Image	Temporary damage	Lasting damage	Permanent damage

Table 8 Manufacturing System Impact Levels Based on Product Produced and Industry Concerns [3]

Category	Low Impact	Moderate Impact	High Impact
Product Produced	Non-hazardous materials or products Non-ingested consumer products	Some hazardous products or steps during production High amount of proprietary information	Critical infrastructure Hazardous materials Ingested products
Industry Examples	Plastic injection molding Warehousing	Automotive metal stamping Pulp and paper Semiconductors Automotive production	Utilities Petrochemical Food and beverage Pharmaceutical

Un **LIMITATO** *effetto negativo significa che, ad esempio, la perdita di integrità, disponibilità o riservatezza potrebbe:*

- *causare un degrado della capacità di missione in una misura e durata tale che il sistema possa svolgere le sue funzioni primarie, ma l'efficacia delle funzioni è notevolmente ridotta;*
- *comportare danni minori alle attività operative riparabili senza ulteriori interruzioni delle operazioni;*
- *comportare minori perdite finanziarie;*
- *provocare danni minori a persone che richiedono solo il primo soccorso di base.*

Un **GRAVE** *effetto significa che, ad esempio, la perdita di integrità, disponibilità o riservatezza potrebbe:*

- *causare un significativo degrado della capacità di missione in una misura e durata tale che il sistema può svolgere le sue funzioni primarie, ma l'efficacia delle funzioni è significativamente ridotta;*
- *provocare danni significativi alle risorse operative riparabili (o sostituibili) con un impatto limitato sulle capacità operative;*
- *comportare una perdita finanziaria significativa;*
- *provocare danni significativi a persone che necessitano di ricovero in ospedale, ma non comportano la morte o lesioni gravi potenzialmente letali.*

Un **CATASTROFICO** *effetto significa che, ad esempio, la perdita di integrità, disponibilità o riservatezza potrebbe:*

- *causare un grave degrado o perdita della capacità della missione in una misura e durata tale che il sistema non è in grado di svolgere una o più delle sue funzioni primarie;*
- *provocare gravi danni alle risorse operative che richiedono molto tempo per la riparazione o la sostituzione, con conseguente prolungamento dei tempi di fermo;*
- *comportare gravi perdite finanziarie;*
- *provocare danni gravi o catastrofici a persone che comportano la morte o lesioni gravi potenzialmente letali.*

PROFILE'S HIERARCHICAL SUPPORTING STRUCTURE

La guida al profilo è scalabile e supporta l'intensificazione delle protezioni di sicurezza dove necessario, mantenendo una linea di base convenzionale.

Ogni livello di impatto superiore si basa sulla linea di base a partire dalla designazione Basso.

Salvo diversa indicazione, i livelli Moderato e Alto ciascuno migliorano tutte le disposizioni dei livelli sottostanti.

- ✓ *Una classificazione* ***moderata*** *include tutte le implementazioni di protezione moderata e bassa*

✓ *Una classificazione **alta** include tutte le implementazioni di sicurezza **alta, moderata e bassa***

Ciascun livello di impatto è posizionato come piattaforma per supportare l'implementazione o categorizzazione del livello di impatto superiore successivo.

La sezione 7 fornisce il linguaggio della sottocategoria CSF per ogni livello di impatto personalizzato per il dominio di produzione.

7. Manufacturing Profile Subcategory Guidance

Function	Category	Subcategory	Manufacturing Profile Guidance	Reference
IDENTIFY	Asset Management (ID.AM)	ID.AM-1	**Low Impact**	ISA/IEC 62443-2-1:2009 4.2.3.4 ISA/IEC 62443-3-3:2013 SR 7.8 CM-8
			Document an inventory of manufacturing system components that reflects the current system. Manufacturing system components include for example PLCs, sensors, actuators, robots, machine tools, firmware, network switches, routers, power supplies, and other networked components or devices. System component inventory is reviewed and updated as defined by the organization. Information deemed necessary for effective accountability of manufacturing system components includes, for example, hardware inventory specifications, component owners, networked components or devices, machine names and network addresses. Inventory specifications include, for example, manufacturer, device type, model, serial number, and physical location.	
			Moderate Impact	
			Identify individuals who are both responsible and accountable for administering manufacturing system components.	CM-8 (1)(3)(5)
			High Impact	
			Identify mechanisms for detecting the presence of unauthorized hardware and firmware components within the manufacturing system. Where safe and feasible, these mechanisms should be automated.	CM-8 (2)(4)
		ID.AM-2	**Low Impact**	ISA/IEC 62443-2-1:2009 4.2.3.4 ISA/IEC 62443-3-3:2013 SR 7.8 CM-8
			Document an inventory of manufacturing system software and firmware components that reflects the current system. Manufacturing system software components include for example software license information, software version numbers, Human Machine Interface (HMI) and other ICS component applications, software, operating systems. System software inventory is reviewed and updated as defined by the organization.	
			Moderate Impact	
			Identify individuals who are both responsible and accountable for administering manufacturing system software.	CM-8 (1)(3)(5)
			High Impact	
			Identify mechanisms for detecting the presence of unauthorized software within the manufacturing system. Where safe and feasible, these mechanisms should be automated.	CM-8 (2)(4)

19A. RESPONDING **TO** & RECOVERING **FROM** A CYBER ATTACK

[Rif.: NIST - Resp. TO & Recov. FROM Cyber Attack ICS]

CYBERSEC CAPABILITIES

Una volta rilevato un evento di sicurezza informatica, in genere vengono eseguite le seguenti attività prima che l'evento sia risolto in modo soddisfacente.

1. EVENT REPORTING
2. LOG REVIEW
3. EVENT ANALISYS
4. INCIDENT HANDLING AND RESPONSE
5. ERADICATION AND RECOVERY

Sfruttare queste capacità di sicurezza informatica facilita una risoluzione soddisfacente di un evento di attacco informatico.

Di seguito sono riepilogate brevemente queste capacità e della sottocategoria NIST Cybersecurity Framework che corrisponde a queste capacità.

Queste attività sono descritte in dettaglio in ISA/IEC 62443-2-1, *Requisiti del programma di sicurezza per i proprietari di risorse* IACS.

ISA/IEC 62443 *è una raccolta di standard internazionali per la sicurezza informatica ICS pubblicata dalla* INTERNATIONAL SOCIETY OF AUTOMATION *(http://www.isa.org)*

1 - EVENT REPORTING

Una volta rilevato, un evento deve essere segnalato al personale appropriato e gli viene assegnata la priorità appropriata per la gestione per garantire che venga generata consapevolezza dei rischi per la sicurezza in modo che le azioni necessarie possano essere prese in modo tempestivo.

CSF Category	CSF Subcategory ID	CSF Subcategory Requirements
Detection Processes	DE.DP-4	Event detection information is communicated
Communications	RS.CO-2	Incidents are reported consistent with established criteria
	RS.CO-3	Information is shared consistent with response plans
	RS.CO-4	Coordination with stakeholders occurs consistent with response plans

Gli eventi dovrebbero essere valutati per determinare chi dovrebbe riceverli e stabilirne la priorità.

Una volta effettuata la determinazione, il sistema dovrebbe essere configurato per avere gli eventi segnalati in modo appropriato.

2 - LOG REVIEW

Gli eventi devono essere scritti in uno o più registri di controllo/eventi protetti e conservati per un periodo di tempo adeguato.

CSF Category	CSF Subcategory ID	CSF Subcategory Requirements
Protective Technology	PR.PT-1	Audit/log records are determined, documented, implemented, and reviewed in accordance with policy

La registrazione degli eventi è un mezzo principale per la revisione e l'analisi degli eventi.

La conservazione dei registri di eventi/audit fornisce supporto per l'analisi forense, che consente l'identificazione delle cause principali e delle vulnerabilità tecniche e comportamentali.

Esaminare gli eventi per rilevare e identificare le attività sospette e le violazioni della sicurezza al fine di dare loro la priorità.

Avendo un'appropriata cronologia degli eventi, l'analisi degli eventi può essere utilizzata per correlare gli eventi e per comprendere meglio le circostanze che circondano il verificarsi degli eventi.

Tutte queste attività supportano la risposta agli eventi, inclusa la determinazione delle cause principali e le azioni intraprese per ridurre al minimo gli impatti e proteggere meglio il sistema da attività sospette e violazioni della sicurezza in futuro.

3 - EVENT ANALYSIS

Gli eventi relativi alla sicurezza devono essere analizzati per identificare e caratterizzare attacchi, compromissioni della sicurezza e incidenti di sicurezza.

CSF Category	CSF Subcategory ID	CSF Subcategory Requirements
Anomalies and Events	DE.AE-2	Detected events are analyzed to understand attack targets and methods
	DE.AE-3	Event data are collected and correlated from multiple sources and sensors
	DE.AE-4	Impact of events is determined
Analysis	RS.AN-1	Notifications from detection systems are investigated
	RS.AN-2	The impact of the incident is understood
	RS.AN-3	Forensics are performed
	RS.AN-4	Incidents are categorized consistent with response plans

Due motivi principali per cui gli eventi sono analizzati:

1) Identificare le compromissioni e le condizioni sospette, che sono spesso raggiunte dalla correlazione di eventi connessi.

   Ciò include l'identificazione delle condizioni che circondano il verificarsi di eventi con tentativi di scoprire le cause principali, come gestirle e proteggersi dalle ricorrenze.

2) Dare priorità e classificarli rispetto al rischio che rappresentano

4 - INCIDENT HANDLING AND RESPONSE

Un processo di risposta agli incidenti dovrebbe essere impiegato e mantenuto aggiornato per valutare e rispondere agli incidenti di sicurezza dei SISTEMI DI CONTROLLO E AUTOMAZIONE INDUSTRIALE *(*INDUSTRIAL AUTOMATION AND CONTROL SYSTEMS [IACS]*).*

Dovrebbe essere utilizzato un processo per la valutazione degli incidenti di sicurezza che identifichi i potenziali impatti, le minacce e le vulnerabilità che hanno permesso il verificarsi dell'incidente.

La valutazione degli incidenti di sicurezza IACS *consente ai produttori di determinarne l'impatto in modo da poter sviluppare e implementare una risposta adeguata.*

*Una risposta adeguata dovrebbe includere il contenimento, la riduzione degli impatti, l'applicazione di contromisure per chiudere le vulnerabilità e la protezione dell'*IACS *da minacce future.*

CSF Category	CSF Subcategory ID	CSF Subcategory Requirements
Information Protection Processes and Procedures	PR.IP-09	Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed
	PR.IP-10	Response and recovery plans are tested
Communications	RS.CO-1	Personnel know their roles and order of operations when a response is needed
Mitigation	RS.MI-1	Incidents are contained
Response Planning	RS.RP-1	Response plan is executed during or after an incident

5 - ERADICATION AND RECOVERY

L'obiettivo di questa fase è consentire il ripristino delle normali operazioni eliminando gli artefatti dell'incidente (ad esempio, rimuovere il codice dannoso, ricreare l'immagine dei sistemi infetti) e mitigare le vulnerabilità o altre condizioni che sono state sfruttate.

CSF Category	CSF Subcategory ID	CSF Subcategory Requirements
Recovery Planning	RC.RP-1	Recovery plan is executed during or after a cybersecurity incident

Una volta contenuto l'incidente, assicurarsi che tutti i mezzi di accesso persistente alla rete siano stati sradicati, che l'attività dell'avversario sia sufficientemente contenuta e che tutte le prove siano state raccolte.

Può anche comportare il rafforzamento o la modifica dell'ambiente per proteggere i sistemi mirati e riparare i sistemi infetti.

Questo è spesso un processo iterativo.

Quindi ripristinare il funzionamento dei sistemi interessati e verificare che funzioni come previsto. (Sicurezza informatica e sicurezza delle infrastrutture Agenzia, Playbook sugli incidenti di sicurezza informatica e sulla risposta alle vulnerabilità, novembre 2021, pag. 15-16.

Disponibile: https://www.cisa.gov/sites/default/files/publications/Federal_Government_Cybersecurity_Incid253

ent_and_Vulnerability_Response_Playbooks_508C.pdf)

5.1 - ERADICATION - *Attività da svolgere:*

1. *Riparare tutti i sistemi infetti negli ambienti* OT*;*
2. *Ricreare l'immagine dei sistemi interessati (spesso da fonti "gold") o ricostruire i sistemi da zero;*
3. *Ricostruire l'hw (necessario quando l'incidente riguarda i rootkit);*
4. *Installare le patch;*
5. *Reimpostare le password sugli account compromessi;*
6. *Sostituire i file compromessi con versioni pulite:*
   a) *Scaricare il programma* PLC *(*PROGRAMMING LOGIC CONTROLLER*);*
   b) *Scaricare il programma* HMI *(*HUMAN-MACHINE INTERFACE*)*
   c) *Recuperare il backup dei dati storici;*

7. *Monitorare eventuali segnali di risposta dell'avversario alle attività di contenimento.*

5.2 - RECOVERY - *Attività da svolgere:*

1. *Rafforzare la sicurezza perimetrale (ad es. set di regole firewall, elenchi di controllo accessi router di confine);*
2. *Ricollegare i sistemi ricostruiti alla rete;*
3. *Testare accuratamente i sistemi, compresi i controlli di sicurezza;*
4. *Ripristinare le normali operazioni dei sistemi e verificare che funzionino normalmente;*
5. *Monitorare le operazioni per comportamenti anomali;*
6. *Eseguire una revisione indipendente delle attività relative al compromesso e alla risposta.*

CYBER ATTACK SCENARIOS

Saranno dimostrate le funzioni di risposta e ripristino del quadro di sicurezza informatica del NIST per i seguenti IMPATTI SUL FUNZIONAMENTO DELL'IMPIANTO.

1. LOSS OF VIEW
2. MANIPULATION OF VIEW
3. LOSS OF CONTROL
4. MANIPULATION OF CONTROL
5. CORRUPTED PROGRAM FILES OR DATA
6. THEFT OF OPERATIONAL INFORMATION

SCENARIO 1 – UNAUTHORIZED COMMAND MESSAGE

Vedi Capitolo 3 del "NIST - Resp. TO & Recov. FROM Cyber Attack ICS]"

Source: Unauthorized Command Message - attackics (mitre.org)

SCENARIO 2 – MODIFICATION OF PROCESS OR CONTROLLER PARAMETERS

Vedi Capitolo 3 del "NIST - Resp. TO & Recov. FROM Cyber Attack ICS]"

Source: Modify Parameter - attackics (mitre.org)

SCENARIO 3 – DISABLING OR ENCRYPTING HMI OR OPERATOR CONSOLE

Vedi Capitolo 3 del "NIST - Resp. TO & Recov. FROM Cyber Attack ICS]"

Source: Denial of Control - attackics (mitre.org)
Denial of View - attackics (mitre.org)

SCENARIO 4 – DATA HISTORIAN COMPROMISE

Vedi Capitolo 3 del "NIST - Resp. TO & Recov. FROM Cyber Attack ICS]"

Source: Data Historian Compromise - attackics (mitre.org)

SCENARIO 5 – UNAUTHORIZED CONNECTION IS DETECTED

Vedi Capitolo 3 del "NIST - Resp. TO & Recov. FROM Cyber Attack ICS]"

Source: Wireless Compromise - attackics (mitre.org)

SCENARIO 6 – UNAUTHORIZED DEVICE IS DETECTED

Vedi Capitolo 3 del "NIST - Resp. TO & Recov. FROM Cyber Attack ICS]"

Source: Rogue Master - attackics (mitre.org)

SECURITY CONTROL MAP

Questa tabella mappa le caratteristiche dei prodotti commerciali che l'NCCoE applicherà a questa sfida alla sicurezza informatica agli standard applicabili e alle migliori pratiche descritte nel quadro per il miglioramento della sicurezza informatica delle infrastrutture critiche e ad altre attività del NIST.

Questo esercizio ha lo scopo di dimostrare l'applicabilità nel mondo reale degli standard e delle migliori pratiche, ma non implica che i prodotti con queste caratteristiche soddisfino i requisiti di un settore per l'approvazione o l'accreditamento normativo.

Security Capability	CSF Category	CSF Subcategory ID	CSF Subcategory Requirements
Event Reporting	Detection Processes	DE.DP-4	Event detection information is communicated
	Communications	RS.CO-2	Incidents are reported consistent with established criteria
		RS.CO-3	Information is shared consistent with response plans
		RS.CO-4	Coordination with stakeholders occurs consistent with response plans
Log Review	Protective Technology	PR.PT-1	Audit/log records are determined, documented, implemented, and **reviewed** in accordance with policy
Event Analysis	Anomalies and Events	DE.AE-2	Detected events are analyzed to understand attack targets and methods
		DE.AE-3	Event data are collected and correlated from multiple sources and sensors
		DE.AE-4	Impact of events is determined
	Analysis	RS.AN-1	Notifications from detection systems are investigated
		RS.AN-2	The impact of the incident is understood
		RS.AN-3	Forensics are performed
		RS.AN-4	Incidents are categorized consistent with response plans
Incident handling response	Information Protection Processes and Procedures	PR.IP-09	Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed
		PR.IP-10	Response and recovery plans are tested
	Communications	RS.CO-1	Personnel know their roles and order of operations when a response is needed
	Mitigation	RS.MI-1	Incidents are contained
	Response Planning	RS.RP-1	Response plan is executed during or after an incident
Eradication, Recovery	Recovery Planning	RC.RP-1	Recovery plan is executed during or after a cybersecurity incident

PARTE IV: SUPERFICIE DI ATTACCO DEI DISPOSITIVI MOBILE

[MOBILE DEVICE & INFRASTRUCTURE ATTACK SURFACE]

[Rif.: NIST IR 8144; NIST SP 1800-13]

20. STORIA

La funzionalità fornita dai dispositivi mobili si è notevolmente evoluta negli ultimi due decenni e continua a progredire rapidamente.

Una volta introdotti i moderni sistemi operativi mobili oltre un decennio più tardi, il panorama delle minacce è cambiato drasticamente quando gli utenti hanno iniziato a fidarsi di questi dispositivi con grandi quantità di informazioni personali sensibili e aziendali.

Poco dopo l'adozione su larga scala dei moderni smartphone, si è verificato un grande aumento nell'uso e nella distribuzione dei servizi cloud.

I componenti principali della superficie di attacco mobile sono:

1) la tecnologia per i dispositivi mobili (Mobile Technology Stack);

2) i protocolli di rete mobile e locale;

3) la catena di fornitura.

21. MOBILE TECHNOLOGY STACK

Dispositivi mobili includono:

1) funzionalità cellulare;

2) sensori ambientali;

3) processori crittografici;

4) metodi di comunicazione wireless e cablata;

5) touchscreen;

6) interfaccia audio;

7) videocamere;

8) capacità come videoproiezione.

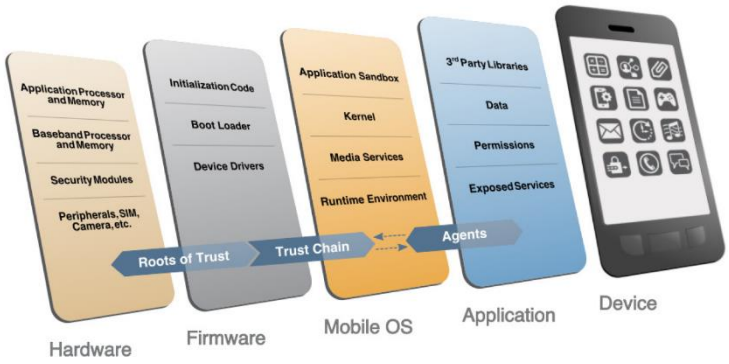


Figure 1 - Mobile Device Technology Stack

La Figura 1 illustra lo stack tecnologico del dispositivo mobile.

Per smartphone e tablet con funzionalità cellulare, esiste una separazione tra l'hardware e il firmware utilizzati per accedere alle reti cellulari, e l'hw e il fw utilizzati per il funzionamento del sistema operativo mobile per uso generale.

L'hw e il fw utilizzati per accedere alla rete cellulare, spesso indicato come sottosistema di telefonia, in genere esegue un sistema operativo in tempo reale (Real Time Operating System - RTOS). Questo sottosistema di telefonia è chiamato colloquialmente il processore in banda base e può essere implementato su un sistema dedicato su un chip (System on Chip - SoC) o incluso come parte del SoC contenente il processore dell'applicazione che esegue anche il sistema operativo mobile per uso generale.

Il firmware necessario per avviare il sistema operativo mobile (ad esempio, bootloader) può verificare il codice di inizializzazione del dispositivo aggiuntivo, i driver di dispositivo utilizzati per le periferiche e parti del sistema operativo mobile, il tutto prima che un utente possa utilizzare il dispositivo.

Se il codice di inizializzazione viene modificato o manomesso in qualche modo, il dispositivo potrebbe non funzionare correttamente.

Molti dispositivi mobili moderni contengono un ambiente di esecuzione isolato, utilizzato specificamente per le funzioni critiche per la sicurezza.

Le applicazioni mobili possono essere scritte in codice nativo in esecuzione vicino all'hardware, in lingue interpretate o in lingue Web di alto livello.

Il grado di funzionalità delle applicazioni mobili dipende fortemente dalle interfacce di programmazione delle applicazioni (Application Programming Interfaces - API) esposte dal sistema operativo mobile.

Mentre alcuni dei meccanismi di comunicazione sono wireless (ad es. Cellulare, WiFi, Bluetooth, GPS, NFC), altri richiedono una connessione fisica (ad es. cavo di alimentazione e sincronizzazione, SIM, memoria esterna).

Come mostrato nella Figura 2, ciascuno di questi diversi meccanismi di comunicazione di dispositivi wireless e cablati espone il

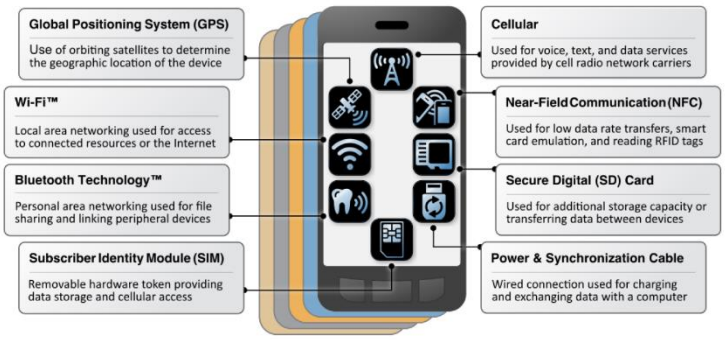


Figure 2 - Mobile Device Communication Mechanisms

dispositivo a una serie distinta di minacce e deve essere protetto o la sicurezza generale del dispositivo potrebbe essere compromessa.

Il nome standard della SIM è Universal Integrated Circuit Card (UICC).

Questo System on a Chip (SoC) ospita l'identità dell'interessato (ovvero International Mobile Subscriber Identity), le chiavi crittografiche pre-condivise e le informazioni di configurazione necessarie per ottenere l'accesso alle reti cellulari.

L'UICC è essenzialmente una smart card che esegue un'applicazione Java nota come Universal Subscriber Identity Module (USIM), che viene utilizzata per eseguire una serie di applicazioni che controllano l'accesso e l'autenticazione del telefono con le reti cellulari e i partner di roaming del MNO (Mobile Network Operator).

La tecnologia chiamata Embedded SIM (eSIM) è stata integrata in alcuni dispositivi mobili.

Gli eSIM consentiranno agli MNO (di fornire in remoto le informazioni sugli abbonati durante la configurazione iniziale del dispositivo e consentiranno la modifica remota dell'abbonamento da un MNO a un altro.

Sebbene questa tecnologia possa cambiare radicalmente il modo in cui i dispositivi mobili vengono sottoposti a provisioning sulla rete dell'operatore e pertanto introduce una nuova serie di minacce.

22. CELLULAR AIR INTERFACE (CAI)

Il CAI è probabilmente l'interfaccia di rete che definisce i moderni dispositivi mobili.

I sistemi cellulari iniziali, come il Sistema globale per le comunicazioni mobili (GSM) di seconda generazione (2G) e il Sistema universale di telecomunicazioni mobili di terza generazione (3G), sono stati modellati sul tradizionale sistema telefonico a commutazione di circuito.

Le nuove reti di quarta generazione (4G) Long Term Evolution (LTE) sono state progettate per utilizzare un modello a commutazione di pacchetto sia per i dati che per la voce.

Una rete LTE fornisce una connettività IP coerente tra il dispositivo mobile di un utente finale e i servizi basati su IP sulla rete di dati a pacchetto (PDN).

CAI è il termine tecnico per la connessione radio tra un dispositivo mobile e la torre cellulare.

I servizi gestiti da MNO possono includere chiamate a commutazione di circuito, VoLTE (Voice over LTE), dati di servizio supplementare non strutturato (USSD), posta vocale integrata con notifiche e messaggistica (ad es. Short Messaging Service (SMS)).

I servizi di messaggistica di livello carrier sono comunemente chiamati messaggi di testo, ma includono SMS, l'estensione di SMS nota come Multimedia Messaging Service (MMS) e il nuovo Rich Communication Services (RCS).

USSD è un metodo obsoleto per stabilire una sessione in tempo reale con un servizio o un'applicazione per condividere rapidamente brevi messaggi.

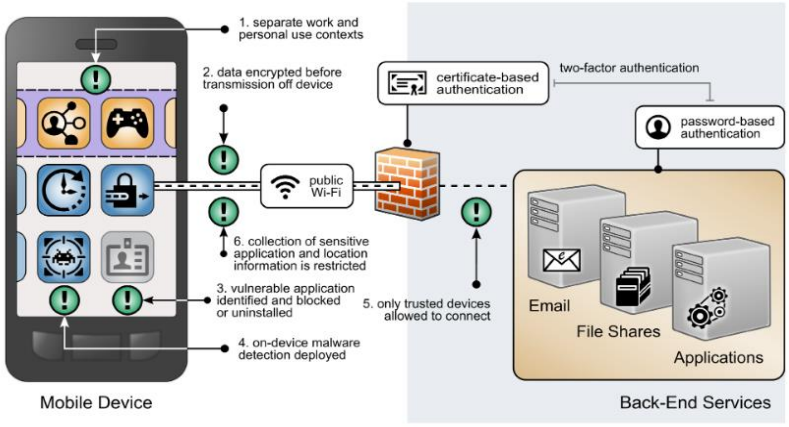
Sebbene non comune negli Stati Uniti, USSD viene utilizzato nei mercati emergenti per una serie di servizi, incluso il mobile banking.

Per ulteriori discussioni sull'architettura di sicurezza LTE, consultare NISTIR 8071 - Panoramica sull'architettura LTE e analisi della sicurezza.

22A. SECURITY AND PRIVACY GOALS

[Rif.: capitolo "4.1.3 Security and Privacy Goals" del NIST SP 1800-22]

Figure 4-1 Security and Privacy Goals



I seguenti obiettivi sono stati evidenziati sopra nella Figura 4-1 Obiettivi di sicurezza e privacy, con un punto esclamativo verde:

1. SEPARATE ORGANIZATION AND PERSONAL INFORMATION.

Le implementazioni BYOD possono mettere a rischio i dati dell'organizzazione consentendo loro di viaggiare all'esterno di reti e sistemi interni quando vi si accede su un dispositivo personale.

Le implementazioni BYOD possono anche mettere a rischio i dati personali acquisendo informazioni dai dispositivi dei dipendenti.

Per aiutare a mitigare questo problema, le informazioni organizzative e personali possono essere separate limitando il flusso di dati tra le applicazioni gestite dall'organizzazione e quelle non gestite.

Gli obiettivi includono aiutare a prevenire l'incrocio di dati sensibili tra contesti lavorativi e personali.

2. ENCRYPT DATA IN TRANSIT.

I dispositivi distribuiti in scenari BYOD possono sfruttare reti non sicure, mettendo i dati a rischio di intercettazione.

Per aiutare a mitigare questo problema, i dispositivi mobili possono connettersi all'organizzazione tramite una VPN o una soluzione simile per crittografare tutti i dati prima che vengano trasmessi dal dispositivo, proteggendo dall'intercettazione i dati altrimenti non crittografati.

Un utente non sarebbe in grado di accedere alle risorse dell'organizzazione senza una connessione VPN attiva e i certificati richiesti.

3. IDENTIFY VULNERABLE APPLICATIONS.

I dipendenti possono installare un'ampia gamma di applicazioni sui dispositivi di proprietà personale, alcune delle quali potrebbero presentare punti deboli di sicurezza.

Quando vengono identificate applicazioni personali vulnerabili, un'organizzazione può rimuovere il profilo di lavoro del dipendente o il file di configurazione dal dispositivo invece di disinstallare le applicazioni personali del dipendente.

4. DETECT MALWARE.

Sui dispositivi di proprietà personale senza criteri di restrizione in atto, gli utenti possono ottenere applicazioni al di fuori degli archivi di applicazioni ufficiali, aumentando il rischio di installare malware sotto mentite spoglie.

Per proteggere da questo rischio, un'organizzazione potrebbe distribuire il rilevamento del malware ai dispositivi per identificare le applicazioni dannose e facilitare la correzione.

5. TRUSTED DEVICE ACCESS.

Poiché i dispositivi mobili possono connettersi da posizioni sconosciute, un'organizzazione può fornire ai dispositivi mobili un certificato di sicurezza che consente di identificarli e autenticarli nel punto di connessione, che si combina con le credenziali dell'utente per creare l'autenticazione a due fattori dai dispositivi mobili.

Un dipendente non sarebbe in grado di accedere alle risorse dell'organizzazione senza i certificati richiesti.

6. RESTRICT INFORMATION COLLECTION.

Gli strumenti di gestione dei dispositivi mobili possono tenere traccia delle applicazioni e delle informazioni sulla posizione, inclusi indirizzo fisico, coordinate geografiche, cronologia delle posizioni, indirizzo IP *(*INTERNET PROTOCOL*) e identificatore di set sicuro (*SECURE SET IDENTIFIER [SSID]*).*

Queste funzionalità possono rivelare informazioni sensibili sui dipendenti, come luoghi o abitudini visitati di frequente.

Gli strumenti di gestione dei dispositivi possono essere configurati per escludere le informazioni sull'applicazione e sulla posizione.

L'esclusione della raccolta di informazioni protegge ulteriormente la privacy dei dipendenti quando i dati del dispositivo e dell'applicazione sono condivisi all'esterno dell'organizzazione per il monitoraggio e l'analisi.

22B. MOBILE ECOSYSTEM THREATS

[Rif.: capitolo "3.5.2 Mobile Ecosystem Threats" del NIST SP 1800-13]

Qualsiasi discussione sui rischi e le vulnerabilità è incompleta senza considerare le minacce coinvolte.

*NIST SP 800-150, Guide to Cyber Threat Information Sharing, afferma che una minaccia informatica è "*qualsiasi circostanza o evento con il potenziale di avere un impatto negativo sulle operazioni organizzative (inclusi missione, funzioni, immagine o reputazione), risorse organizzative, individui, altri organizzazioni o la Nazione attraverso un sistema informativo tramite accesso non autorizzato, distruzione, divulgazione o modifica delle informazioni e/o negazione del servizio*".*

Per semplificare questo concetto, una minaccia è tutto ciò che può sfruttare una vulnerabilità per danneggiare una risorsa.

Trovare l'intersezione di questi tre comporterà un rischio.

Comprendere le minacce applicabili a un sistema è il primo passo per determinarne i rischi.

*Per maggiori approfondimenti vedere il catalogo delle minacce mobili (*MOBILE THREAT CATALOG - MTC*) del NIST, insieme al relativo rapporto IR 8144 del NIST, Valutazione delle minacce ai dispositivi mobili e all'infrastruttura.*

*Ogni voce dell'MTC (vedi capitolo "*32. Metodologia per individuare le minacce – Mobile Threat Catalogue [MTC]*") contiene diverse informazioni: un identificatore, una categoria, una descrizione di alto livello, dettagli sulla sua origine, esempi di exploit, esempi di vulnerabilità ed esposizioni comuni, possibili contromisure e riferimenti accademici.*

Ai fini di questa guida pratica, siamo principalmente interessati a identificatori di minacce, categorie, descrizioni e contromisure.

A grandi linee, l'MTC copre 32 categorie di minacce raggruppate in 12 classi distinte, come mostrato nella Tabella 3-1.

Di queste categorie, tre in particolare, evidenziate in verde nella tabella, sono coperte dalla guida in questa guida pratica.

Se implementata correttamente, questa guida aiuterà a mitigare tali minacce.

Le altre categorie, sebbene siano ancora elementi importanti dell'ecosistema mobile e critici per la salute di un'architettura di mobilità complessiva, non rientrano nell'ambito di questo documento.

L'intero ecosistema mobile dovrebbe essere considerato quando si analizzano le minacce all'architettura; questo ecosistema è rappresentato nella Figura 3-1, tratta da NIST IR 8144.

Ciascun attore nell'ecosistema (l'utente del dispositivo mobile, l'azienda, l'operatore di rete, lo sviluppatore dell'applicazione e il produttore di apparecchiature originali (OEM)) può trovare suggerimenti per scoraggiare altre minacce esaminando l'MTC e il NIST IR 8144, di seguito rappresentata nel capitolo "30. Mobile Ecosystem".

Molti di questi condividono soluzioni comuni, come l'utilizzo del software EMM per monitorare l'integrità del dispositivo e l'installazione di applicazioni solo da fonti autorizzate.

TABLE 3-1 THREAT CLASSES AND CATEGORIES

Threat Class	Threat Category
Application	Malicious or Privacy-Invasive Applications
	Vulnerable Applications
Authentication	Authentication: User or Device to Network
	Authentication: User or Device to Remote Service
	Authentication: User to Device
Cellular	Carrier Infrastructure
	Carrier Interoperability
	Cellular Air Interface
	Consumer-Grade Femtocell
	Short Message Service (SMS)/Multimedia Messaging Service (MMS)/Rich Communication Services (RCS)
	Unstructured Supplementary Service Data (USSD)
	Voice over Long-Term Evolution (VoLTE)
Ecosystem	Mobile Application Store
	Mobile OS & Vendor Infrastructure
EMM	EMM
Global Positioning System (GPS)	GPS
Local Area Network and Personal Area Network	Network Threats: Bluetooth
	Network Threats: Near Field Communication (NFC)
	Network Threats: Wi-Fi
Payment	Application-Based
	In-Application Purchases
	NFC-Based
Physical Access	Physical Access
Privacy	Behavior Tracking
Supply Chain	Supply Chain
Stack	Baseband Subsystem
	Boot Firmware
	Device Drivers
	Isolated Execution Environments
	Mobile Operating System
	Secure Digital (SD) Card
	Universal Subscriber Identity Module (USIM)/Subscriber Identity Module (SIM)/Universal Integrated Circuit Card (UICC) Security

12 ENTERPRISE MOBILE THREATS

[Rif.: NIST - 12 Enterprise Mobile Threats]

Esistono molti tipi di minacce mobili e provengono da una varietà di fonti. Dalle minacce basate sull'applicazione a un avversario nel mezzo, le possibilità possono essere schiaccianti.

In risposta, l'NCCoE ha compilato un elenco delle minacce più comuni per i dispositivi mobili per aiutare le organizzazioni a dare priorità alle loro soluzioni in base alla probabilità di un attacco.

1 - PRIVACY INTRUSIVE APPLICATION *Unauthorized access to sensitive information via a malicious or privacy intrusive application.*	1 – VIOLAZIONE DELLA PRIVACY *Accesso non autorizzato a informazioni sensibili tramite un'applicazione dannosa o intrusiva per la privacy*

2 - ACCOUNT CREDENTIAL THEFT THROUGH PHISHING *Theft of credentials through a short message service SMS or email phishing campaign.*	2 - FURTO DI CREDENZIALI DELL'ACCOUNT TRAMITE PHISHING *Furto di credenziali attraverso un servizio di messaggistica breve (SMS) o campagna di phishing via email.*
3 - MALICIOUS APPLICATION *Unauthorized applications installed via URLs in SMS or email messages.*	3 - APPLICAZIONE DANNOSA *Applicazioni non autorizzate installate tramite URL in SMS o messaggi di posta elettronica*
4 - OUTDATED PHONE *Confidentiality and Integrity loss due to exploitation of known vulnerability in the operating system or firmware.*	4 - TELEFONO OBSOLETO *Perdita della Riservatezza e dell'Integrità dovute allo sfruttamento di vulnerabilità note nel sistema operativo o firmware.*
5 - CAMERAS AND MICROPHONES REMOTE ACCESS *Cameras, microphones , or other device sensors are misused without the device owner's knowledge.*	5 - TELECAMERE E MICROFONI ACCESSO REMOTO *Fotocamere, microfoni o altri sensori del dispositivo vengono utilizzati in modo improprio all'insaputa del proprietario del dispositivo.*
6 - SENSITIVE DATA TRANSMISSION *Data in transit is eavesdropped on.*	6 - TRASMISSIONE DI DATI SENSIBILI *I dati in transito vengono intercettati.*
7 - BRUTE-FORCE ATTACKS TO UNLOCK A PHONE *Compromise of device integrity via brute-forced device unlock code.*	7 - ATTACCHI PER SBLOCCO FORZATO DEL TELEFONO *Compromissione dell'integrità del dispositivo tramite sblocco forzato del dispositivo.*
8 - WEAK PASSWORD PRACTICES PROTECTION *Unauthorized access to remote services via authentication or credential storage vulnerabilities.*	8 - PROTEZIONE DELLE PASSWORD DEBOLI *Accesso non autorizzato a servizi remoti tramite autenticazione o vulnerabilità di archiviazione delle credenziali.*
9 - UNMANAGED DEVICE PROTECTION *Unauthorized access of enterprise resources from an unmanaged and potentially compromised device.*	9 - PROTEZIONE DISPOSITIVO NON GESTITO *Accesso non autorizzato alle risorse aziendali da un dispositivo non gestito e potenzialmente compromesso.*
10 - LOST OR STOLEN DATA PROTECTION *Loss of organizational data due to a lost or stolen device.*	10 - PROTEZIONE DEI DATI PERSI O RUBATI *Perdita di dati aziendali a causa di un dispositivo smarrito o rubato.*
11 - PROTECTING DATA FROM BEING INADVERTENTLY BACKED UP TO A CLOUD SERVICE *Loss of confidentiality of organizational data due to its unauthorized storage in non-organizationally managed cloud services.*	11 - PROTEZIONE DEI DATI DAL BACKUP INVOLONTARIO SU UN SERVIZIO CLOUD *Perdita di riservatezza dei dati organizzativi a causa della loro archiviazione non autorizzata in servizi cloud non gestiti dall'organizzazione.*
12 - PERSONAL IDENTIFICATION NUMBER (PIN) OR PASSWORD-SHARING PROTECTION *Unauthorized access to work applications via bypassed lock screen.*	12 - PROTEZIONE NUMERO IDENTIFICAZIONE PERSONALE (PIN) O PASSWORD CONDIVISA *Accesso non autorizzato alle applicazioni di lavoro tramite bypass della schermata di blocco.*

23. WIRELESS FIDELITY (WIFI)

Il WiFi è una tecnologia di rete locale wireless (WLAN) basata sulla serie di standard IEEE 802.11.

Le distribuzioni nei campus o nelle aziende hanno maggiori probabilità di implementare funzionalità di sicurezza come la crittografia WPA2.

Smartphone, laptop e altri dispositivi che utilizzano il WiFi spesso devono riconnettersi a un punto di accesso wireless centrale (AP).

Ulteriori indicazioni per l'installazione, la configurazione, la distribuzione e la sicurezza del WiFi possono vedere NIST SP 800-153 - Linee guida per la protezione di reti wireless locali o SP 800-97 - Creazione di reti di sicurezza wireless robuste: una guida a IEEE 802.

24. GLOBAL NAVIGATION SATELLITE SYSTEM (GNSS)

GNSS fornisce il posizionamento geo-spaziale in tutto il mondo tramite il sistema di posizionamento globale (Global Positioning System - GPS), che utilizza la comunicazione della linea con una rete satellitare per permettere al telefono a determinare la sua posizione.

Questi sistemi funzionano indipendentemente dalle reti cellulari.

Il governo federale degli Stati Uniti gestisce una rete GPS; i dispositivi mobili possano utilizzare altri sistemi (ad es. GLONASS, Galileo).

Altre tecniche includono il posizionamento assistito Wi-Fi, che sfrutta database di identificatori di set di servizi noti (SSID) e geolocalizzazione di indirizzi IP.

25. BLUETOOTH

Bluetooth è una tecnologia di comunicazione wireless a corto raggio.

È utilizzata principalmente per stabilire reti personali senza fili (Personal Area Networks - PAN).

Per ulteriori informazioni sulla sicurezza Bluetooth, vedere NIST SP 800-121 Rev.1 - Guida alla sicurezza Bluetooth.

26. NEAR FIELD COMMUNICATION (NFC)

NFC utilizza le emissioni in radiofrequenza per stabilire comunicazioni a bassa portata tra dispositivi abilitati NFC (esempio: lettura QR code).

Utilizzato per distanze inferiori a 4 pollici, ma può potenzialmente operare e costituire una minaccia a distanze molto maggiori.

NFC si basa sul set di standard di identificazione a radiofrequenza (Radio Frequency IDentification - RFID).

La tecnologia di pagamento mobile si basa su NFC poiché le nuove tecnologie di portafoglio mobile vengono implementate su larga scala.

L'uso di NFC per le transazioni finanziarie lo rende attraente agli autori di attacchi criminali.

Per ulteriori informazioni sulle problematiche di sicurezza associate all'RFID, consultare NIST SP 800-98 - Linee guida per la protezione dei sistemi di identificazione a radiofrequenza (RFID).

27. SECURE DIGITAL (SD) CARD

Le schede SD vengono in genere utilizzate per espandere la capacità di archiviazione dei dispositivi mobili per archiviare dati come foto, video, musica e dati delle applicazioni.

Le schede SD non sono integrate in tutti i dispositivi mobili, anche se l'uso di schede SD è particolarmente popolare nei paesi in via di sviluppo in cui l'archiviazione integrata potrebbe non essere comune.

28. POWER & SYNCHRONIZATION PORT

La porta di alimentazione e sincronizzazione su un dispositivo mobile viene spesso utilizzata per caricare un dispositivo mobile e può assumere la forma di Universal Serial Bus (USB) Type-C, Micro-USB, Apple Lightning o Apple 30 pin.

Il cavo viene anche utilizzato per trasportare dati o accedere al dispositivo da un altro sistema informativo.

I casi d'uso includono la sincronizzazione o il backup dei dati su un PC o il provisioning in un sistema di gestione della mobilità aziendale.

Questo cavo può anche essere utilizzato per caricare un altro dispositivo in alcune circostanze. A causa di questo duplice uso di potenza e dati, questa interfaccia viene utilizzata come vettore per numerosi attacchi.

29. SUPPLY CHAIN PORT

Le minacce alla catena di approvvigionamento sono particolarmente difficili da mitigare perché i componenti dei dispositivi mobili sono in costante sviluppo e provengono da decine di migliaia di produttori di apparecchiature originali (OEM).

Alcuni sottocomponenti di dispositivi mobili (ad es. processori in banda base) richiedono un firmware abbinato sviluppato dall'OEM.

Questo firmware può a sua volta contenere vulnerabilità del software e può aumentare la superficie di attacco complessiva del dispositivo mobile.

Nel caso dei dispositivi iOS integrati verticalmente, Apple sviluppa il sistema operativo mobile, hardware e firmware specializzati.

L'intero processo di progettazione e produzione ha il potenziale per influenzare notevolmente l'architettura di sicurezza del dispositivo mobile risultante.

[NIST propone un metodo (strumento, questionario e calcolo) per l'analisi d'impatto dei rischi nella catena di approvvigionamento - vedi rif. 10]

30. MOBILE ECOSYSTEM

I negozi di applicazioni rappresentano un ulteriore vettore di minaccia per gli aggressori di distribuire malware o altri software dannosi agli utenti finali.

È particolarmente vero per i negozi di applicazioni di terze parti non supervisionati direttamente dai fornitori di sistemi operativi mobili.

Questo ecosistema mobile è rappresentato nella figura accanto.

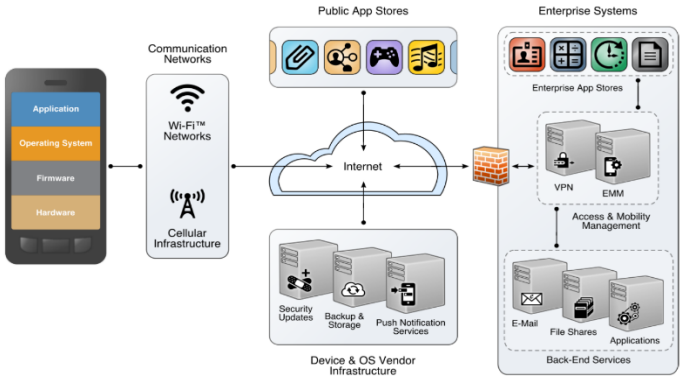


Figure 3 - Mobile Ecosystem

31. PAGAMENTI TRAMITE L'USO DEL MOBILE

[Rif.: PCI Mobile Payment Acceptance Security Guidelines for Merchants as End-Users]

Applicazioni di accettazione del pagamento che funzionano su qualsiasi dispositivo portatile elettronico di consumo (ad es. smartphone, tablet o PDA) non dedicato esclusivamente all'elaborazione delle transazioni di accettazione del pagamento, in cui il dispositivo elettronico portatile ha accesso a dati in chiaro.

Questa sottocategoria è denominata "Categoria 3, Scenario 2".

Gli standard PCI separati e la documentazione disponibile sul sito Web PCI SSC riguardano tutte le altre categorie e scenari:

- *Domande di accettazione dei pagamenti mobili e domande frequenti su PA-DSS*
- *Requisiti di sicurezza modulari POI PCI PTS (categoria 1)*

- *Standard di sicurezza dei dati delle applicazioni di pagamento PCI (PA-DSS) (categoria 2)*
- *Accettare pagamenti mobili con uno smartphone o un tablet (categoria 3, scenario 1)*

PERCHÉ IL CELLULARE È DIVERSO

Grazie al design, quasi tutte le applicazioni mobili potrebbero accedere ai dati dell'account archiviati o passati attraverso il dispositivo mobile; ciò rappresenta una sfida per i commercianti per dimostrare aderenza allo Standard PCI Data Security.

L'affidabilità è più significativa per i pagamenti mobili poiché tale ambiente è frammentato tra produttori di dispositivi, sviluppatori di sistemi operativi, progettisti di applicazioni, operatori di rete e l'uso di vari protocolli per connettere queste diverse entità.

PCI Mobile Payment Acceptance Security Guidelines discutono di tali sfide insieme alle opportunità di sfruttare i controlli di sicurezza emergenti.

Payment Card Industry Security Standards Council (PCI SSC) riconosce che i commercianti possano utilizzare dispositivi portatili elettronici di consumo (ad es. Smartphone, tablet, PDA o collettivamente "dispositivi mobili") che non siano dedicati esclusivamente all'accettazione del pagamento per l'elaborazione delle transazioni. (I POS sono dispositivi esclusivamente dedicati ai pagamenti)

Laddove l'implementazione hw e sw dei dispositivi mobili dei commercianti non è attualmente in grado di soddisfare le linee guida, possono scegliere di implementare una soluzione di crittografia Point-to-Point (PCI P2PE) convalidata da PCI.

L'implementazione di tale soluzione includerebbe l'aggiunta di un dispositivo POI (Point of Interaction) approvato da PCI.

Attraverso l'uso di una soluzione convalidata, i dati dell'account sono crittografati dal POI ed il dispositivo mobile funge da canale attraverso il quale è trasmessa la transazione di pagamento crittografata.

RISCHI PER LA SICUREZZA DEI DISPOSITIVI MOBILI

I dispositivi mobili possono includere anche più tecnologie cellulari (ad esempio LTE, CDMA e GSM), GPS, Bluetooth, infrarossi (IR) e funzionalità di Comunicazione Near-Field (NFC).

Il rischio è ulteriormente aumentato dai supporti rimovibili (ad esempio, scheda SIM e scheda SD), l'elettronica interna utilizzata per i test da parte del produttore, i sensori incorporati (ad esempio, sensori di inclinazione o di movimento, sensori termici, sensori di pressione e sensori di luce) e biometrici lettori.

Le configurazioni di registrazione e debug a livello di operatore e di rete comportano rischi aggiuntivi.

Un dispositivo mobile con connettività wireless consente di rimuoverlo dalla posizione di un commerciante, che di solito è considerato sicuro, e portato in una posizione che è conveniente per il cliente, ciò può offrire vantaggi al commerciante, ma comporta anche numerosi rischi per la sicurezza:

1. *facilità per un criminale di rubare il terminale, modificarlo e restituirlo senza che nessuno si accorga che è scomparso e, di conseguenza,*
2. *il dispositivo mobile non avendo una posizione fissa, risulta più impegnativo per il commerciante tenerne traccia.*

OBIETTIVI PER LA SECURITY OF A PAYMENT TRANSACTION

Obiettivo 1: impedire l'intercettazione dei dati dell'account quando inseriti in un dispositivo mobile.

Obiettivo 2: impedire la compromissione dei dati dell'account durante l'elaborazione o l'archiviazione nel dispositivo mobile.

Obiettivo 3: impedire l'intercettazione dei dati dell'account dopo la trasmissione dal dispositivo mobile.

I 3 principali rischi associati alle transazioni di pagamento mobili sono:

1. *dati dell'account che entrano nel dispositivo;*
2. *dati dell'account che risiedono nel dispositivo;*
3. *dati dell'account in uscita dal dispositivo.*

Guida associata per affrontare ciascuno dei tre rischi:

1. *Impedire l'accesso al dispositivo fisico non autorizzato*
2. *Impedire l'accesso al dispositivo logico non autorizzato*
3. *Proteggere il dispositivo mobile dal malware*
4. *Assicurare che il dispositivo mobile sia in uno stato sicuro*
5. *Disabilitare le funzioni del dispositivo non necessarie*
6. *Rilevare smarrimento o furto*
7. *Garantire lo smaltimento sicuro dei vecchi dispositivi*

PRACTICES AND RESPONSIBILITIES

Appendice B: migliori pratiche e responsabilità

La tabella accanto delinea ogni best practice e chi dovrebbe essere responsabile della sua implementazione.

Includono:

- *Merchant as an End User (M): qualsiasi entità che utilizza la soluzione di accettazione del pagamento mobile per accettare pagamenti;*
- *Mobile Payment-Acceptance Solution Provider (SP): l'entità che integra tutti i pezzi nella soluzione di accettazione dei pagamenti mobili ed è responsabile dell'amministrazione back-end della soluzione. Ciò include il commerciante come fornitore di soluzioni.*

BEST PRACTICE	M	SP
1. Prevent account data from being intercepted when entered into a mobile device.	X	X
2. Prevent account data from compromise while processed or stored within the mobile device.	X	X
3. Prevent account data from interception upon transmission out of the mobile device.		X
4. Prevent unauthorized physical device access.	X	
5. Protect mobile device from malware.	X	X
6. Ensure the device is in a secure state.		X
7. Disable unnecessary device functions.	X	X
8. Detect loss or theft.	X	X
9. Ensure the secure disposal of the device.	X	
10. Implement secure solutions.	X	X
11. Ensure the secure use of the payment-acceptance solution.	X	
12. Prefer online transactions.		X
13. Prevent unauthorized use.	X	
14. Inspect system logs and reports.	X	X
15. Ensure that customers can validate the merchant/transaction.		X
16. Issue secure receipts.		X

La tabella seguente delinea ogni best practice insieme a chi dovrebbe essere responsabile della sua implementazione.

Includono:

- Device Manufacturer (DM): *include produttori di dispositivi mobili, integratori, sviluppatori di firmware e qualsiasi produttore responsabile dello sviluppo di hardware OEM.*
- Sviluppatore OS (OD): *include l'entità che crea e mantiene il sistema operativo, incluso ma non limitato all'entità responsabile dell'architettura del sistema operativo, dei driver di dispositivo e dello sviluppo di patch.*
- Sviluppatore di applicazioni (AD): *include qualsiasi sviluppatore di software che crea e mantiene un'applicazione utilizzata come parte della soluzione di accettazione del pagamento. Ciò include il commerciante come sviluppatore di applicazioni.*

- Commerciante come utente finale (M): *qualsiasi entità che utilizza la soluzione di accettazione del pagamento mobile per accettare pagamenti.*
- Provider di soluzioni di accettazione dei pagamenti mobili (SP): *l'entità che integra tutti i pezzi nella soluzione di accettazione dei pagamenti mobili ed è responsabile dell'amministrazione back-end della soluzione, ciò include il commerciante come fornitore di soluzioni.*

BEST PRACTICE	DM	OD	AD	M	SP
1. Prevent account data from being intercepted when entered into a mobile device.	x	x	x		x
2. Prevent account data from compromise while processed or stored within the mobile device.	x	x	x		x
3. Prevent account data from interception upon transmission out of the mobile device.	x	x	x		x
4. Prevent unauthorized logical device access.		x	x	x	x
5. Create server-side controls and report unauthorized access.		x	x	x	x
6. Prevent escalation of privileges.	x	x	x		x
7. Create the ability to remotely disable payment application.		x	x		x
8. Detect loss or theft.	x	x	x	x	x
9. Harden supporting systems.			x		x
10. Prefer online transactions.			x		x
11. Conform to secure coding, engineering, and testing.		x	x		x
12. Protect against known vulnerabilities.		x	x		x
13. Protect the mobile device from unauthorized applications.	x	x	x		
14. Protect the mobile device from malware.		x	x	x	x
15. Protect the mobile device from unauthorized attachments.	x	x			
16. Create instructional materials for implementation and use.	x	x	x		x
17. Support secure merchant receipts.		x	x		x
18. Provide an indication of a secure state.	x	x	x		x

Appendice D: Ulteriori Rischi Associati ai dispositivi Mobile

1. DEVICE VALIDATION
2. REGIONAL JURISDICTION
3. TECHNOLOGICAL LIMITATIONS
4. INDETERMINABLE RISKS
5. EVOLUTION OF TECHNOLOGY AND UNFORESEEN ATTACK VECTORS
6. VULNERABILITIES MARKETS
7. INTENTIONALLY INSERTED BACKDOORS
8. NETWORK CONNECTIONS
9. MEMORY MANAGEMENT
10. ANTI-MALWARE
11. VARIATION OF DEVICES
12. ACCESS CONTROL

32. METODOLOGIA PER INDIVIDUARE LE MINACCE – MOBILE THREAT CATALOGUE [MTC]

[Rif.: NIST SP 1800-13144]

Le minacce sono state identificate utilizzando il processo di valutazione del rischio NIST SP 800-30.

PASSI

1) IDENTIFICARE *le minacce nei meccanismi di comunicazione, nella catena di fornitura mobile e ad ogni livello dello stack tecnologico dei dispositivi mobili.*

2) SUDDIVIDERE *le minacce in categorie unendole alle informazioni relative a istanze specifiche di tali minacce.*

3) IDENTIFICARE *quali sistemi associati sono inclusi e le capacità di mitigazione applicabili.*

STRUTTURA DEL CATALOGO

Le minacce sono presentate in categorie e sottocategorie all'interno del catalogo.

Per ogni minaccia identificata, vengono fornite le seguenti informazioni:

1) THREAT CATEGORY*: la principale area tematica relativa a questa minaccia.*
   1. *Mobile Device Technology Stack;*
   2. *Network Protocols, Technologies, and Infrastructure;*
   3. *Authentication Mechanisms;*
   4. *Supply Chain;*
   5. *Physical Access;*
   6. *Ecosystem;*
   7. *Enterprise Mobility;*
   8. *Pagamenti*

2) THREAT IDENTIFIER (ID)*: è un identificatore univoco per fare riferimento a una specifica minaccia. Le categorie di identificatori generali utilizzate all'interno del MTC sono*
   1. *APP: Application;*
   2. *STA: Stack;*
   3. *CEL: Cellular;*
   4. *GPS: Global Positioning System;*
   5. *LPN: Local Area Network & Personal Area Network;*
   6. *AUT: Authentication;*
   7. *SPC: Supply Chain;*
   8. *PHY: Physical;*
   9. *ECO: Ecosystem;*
   10. *EMM: Enterprise Mobility Management;*
   11. *PAY: Payment.*

3) THREAT ORIGIN*: riferimento al materiale di origine utilizzato per identificare inizialmente la minaccia.*

4) EXPLOIT EXAMPLE*: esempio dell'origine della vulnerabilità o di una istanza di questa minaccia.*

5) COMMON VULNERABILITY AND EXPOSURE (CVE) REFERENCE*: una vulnerabilità specifica situata nel National Vulnerability Database (NVD). Un'origine di vulnerabilità può descrivere una vulnerabilità specifica, che può o meno essere associata a un CVF.*

6) POSSIBLE COUNTERMEASURE*: controlli di sicurezza o mitigazioni che potrebbero ridurre l'impatto di una particolare minaccia. Se non è presente una contromisura, potrebbe essere un'area per ricerche future.*

DESCRIZIONE DELLE CATEGORIE

Ci sono 12 schede all'interno del MTC (Mobile Threat Catalog), ognuna delle quali funge da categorie di minacce generali con sottocategorie definite come necessarie.

1) MOBILE DEVICE TECHNOLOGY STACK

Lo stack tecnologico del dispositivo mobile è costituito:

a) *dall'hardware;*

b) *dal firmware;*

c) *dal software utilizzati per ospitare e far funzionare il dispositivo mobile.*

1. Applicazioni mobile: *la scheda Applicazioni contiene minacce correlate all'applicazione software sviluppata per un dispositivo mobile o, più specificamente, un sistema operativo mobile.*

   Applicazioni vulnerabili: questa sottocategoria contiene minacce relative a vulnerabilità software discrete che risiedono all'interno di applicazioni mobili in esecuzione sul sistema operativo mobile.

   Nota: *alcune vulnerabilità possono essere specifiche di un determinato sistema operativo mobile, mentre altre possono essere generalmente applicabili.*

   - ✓ *Applicazioni dannose o invasive per la privacy: questa sottocategoria identifica le minacce basate sul malware mobile, in parte sulla tassonomia della classificazione mobile di Google. Non ci sono vulnerabilità specifiche del software in questa sottocategoria e di conseguenza non vengono citati nel CVE. Ulteriori categorie di malware sono incluse nella sottocategoria per aumentare la tassonomia di classificazione di Google.*

2. Sistema operativo mobile*: sistema operativo progettato specificamente per un dispositivo mobile e per l'esecuzione di applicazioni mobili.*
3. Driver di dispositivo*: plug-in utilizzati per interagire con l'hardware del dispositivo e altre periferiche (ad es. Fotocamera, accelerometro).*
4. Ambienti di esecuzione isolati*: ambiente basato su hardware o firmware integrato nel dispositivo mobile che può fornire molte funzionalità come archiviazione chiavi attendibile, verifica del codice, integrità del codice ed esecuzione affidabile per i processi rilevanti per la sicurezza.*
5. Scheda SD*: le schede SD sono memoria rimovibile utilizzata per espandere la capacità di archiviazione dei dispositivi mobili per archiviare dati come foto, video, musica e dati delle applicazioni.*
6. Firmware di avvio*: il firmware necessario per avviare il sistema operativo mobile (ad es. Bootloader). Il firmware può verificare il codice di inizializzazione del dispositivo aggiuntivo, i driver di dispositivo utilizzati per le periferiche e parti del sistema operativo mobile, il tutto prima che un utente possa utilizzare il dispositivo.*
7. Sottosistema banda base*: raccolta di hardware e firmware utilizzati per comunicare con la rete cellulare tramite la radio cellulare.*
8. Scheda SIM*: questo token hardware rimovibile è un SoC che ospita l'IMSI, chiavi crittografiche pre-condivise e informazioni di configurazione necessarie per ottenere l'accesso alle reti cellulari.*

2) NETWORK PROTOCOLS, TECHNOLOGIES, AND INFRASTRUCTURE

Questa categoria include i protocolli e le tecnologie wireless utilizzati dai dispositivi mobili.

1. Cellulare*: esistono minacce a numerosi sistemi cellulari, suddivise nelle seguenti sottocategorie:*

   - ✓ *Interfaccia aerea: è la connessione radio tra un ricevitore e una stazione base.*

     Nota: mentre sono elencate una serie di minacce generali all'interfaccia aerea cellulare, sono incluse anche minacce specifiche a determinati protocolli cellulari (ad es. GSM, CDMA, LTE).

- ✓ *USSD: un metodo per stabilire sessioni in tempo reale con un servizio o un'applicazione per condividere rapidamente brevi messaggi. Sebbene i messaggi USSD possano viaggiare su SMS, il protocollo stesso è distinto.*
- ✓ *Infrastruttura di trasporto: questa categoria comprende le minacce alle stazioni base, backhaul e core di rete cellulare.*

  Nel campo delle telecomunicazioni, una rete di backhaul (carico di ritorno) o rete di ritorno è la porzione (sottoinsieme) di una rete gerarchica che comprende i collegamenti intermedi tra la rete centrale (o nucleo o dorsale) e le piccole sottoreti ai «margini» della stessa rete gerarchica.
- ✓ *Interoperabilità del vettore: questa sottocategoria è principalmente riservata alla segnalazione di minacce associate alla rete di segnalazione.*
- ✓ *VoLTE: l'applicazione di rete a commutazione di pacchetto utilizzata per effettuare chiamate vocali all'interno di LTE. Sebbene non sia supportato in tutte le reti MNO, sono in corso implementazioni su larga scala in tutto il mondo.*

2. LAN e PAN*: questa categoria di minacce è costituita dalle tecnologie di rete wireless locali e personali.*
   - ✓ *WiFi: è una tecnologia WLAN basata sulla serie di standard IEEE 802.11.*
   - ✓ *Bluetooth: è una tecnologia di comunicazione (con un suo protocollo) wireless a medio raggio e a bassa potenza.*
   - ✓ *NFC: è una tecnologia di comunicazione wireless a corto raggio comunemente utilizzata per le tecnologie di portafoglio mobile e la configurazione periferica, sebbene esistano numerose altre applicazioni.*
3. GPS*: una rete di satelliti in orbita utilizzata per aiutare un dispositivo a determinare la sua posizione.*

3) AUTHENTICATION MECHANISMS

I meccanismi di autenticazione sono raggruppati nelle 3 sottocategorie elencate di seguito. I tipi di credenziali e token individuali non sono suddivisi nelle proprie categorie e sono invece inclusi in una di queste tre grandi categorie.

1. Utente o dispositivo*: meccanismi utilizzati per l'autenticazione con un dispositivo mobile, come password, impronte digitali o riconoscimento vocale.*
2. Utente o dispositivo al servizio remoto*: meccanismi che un utente o un'entità non persona distinta (Non-Person Entity NPE) utilizza per autenticarsi in remoto.*
3. Utente o dispositivo alla rete*: meccanismi che un utente, dispositivo mobile o periferica utilizza per autenticarsi su una rete (ad es. Wi-Fi, cellulare). Ciò include comunemente la dimostrazione del possesso di un token crittografico.*

4) SUPPLY CHAIN

Questa categoria include le minacce relative alla catena di fornitura dei dispositivi e dei componenti. Nella misura in cui sono inclusi, le minacce relative alla catena di approvvigionamento del software sono rilevate come Sfruttamento delle Vulnerabilità nella categoria Applicazioni.

5) PHYSICAL ACCESS

Questa categoria include minacce generali provenienti dall'esterno del dispositivo, come perdita del dispositivo e stazioni di ricarica dannose.

6) ECOSYSTEM

Questa categoria comprende le minacce relative all'ecosistema mobile il quale include una serie di elementi, tra cui EMM (Enterprise Mobility Management), infrastruttura del fornitore del sistema operativo mobile e servizi aziendali mobili come e-mail, contatti e calendario.

- ✓ Infrastruttura del fornitore del S.O. mobile*: aggiornamenti, servizi ausiliari come il cloud storage.*

- ✓ Native Public and Enterprise Stores*: negozi di applicazioni mobili, musica, film, giochi, ecc.*

7) ENTERPRISE MOBILITY

Questa categoria di minacce comprende i sistemi di gestione della mobilità aziendale e le minacce ai servizi aziendali.

8) PAGAMENTI

Le minacce relative ai pagamenti mobili sono incluse in questa categoria, inclusa una varietà di tecnologie di pagamento mobili come USSD (Unstructured Supplementary Service Data), pagamenti basati su NFC e «tokenizzazione» con carta di credito.

32A. BIOMETRIA

[Rif.: NIST IR 8334]

INTRODUZIONE

Molte organizzazioni di pubblica sicurezza (Public Security Organization - PSO) stanno adottando dispositivi mobili, come smartphone e tablet, per consentire l'accesso sul campo a informazioni sensibili per i primi soccorritori.

I dispositivi mobili più recenti supportano una o più forme di biometria per l'autenticazione degli utenti.

L'accesso su richiesta ai dati sulla sicurezza pubblica è fondamentale per garantire che i primi soccorritori possano fornire le cure e il supporto necessari durante un'emergenza.

I requisiti di autenticazione destinati a salvaguardare tali informazioni, come l'immissione di una password complessa o il recupero di un token crittografico e la lettura di una password monouso, possono ostacolare l'accesso.

I PSO sono incaricati di implementare meccanismi di autenticazione efficienti e sicuri per proteggere l'accesso alle informazioni sensibili soddisfacendo al contempo le esigenze dei loro ambienti operativi.

La biometria può aiutare a identificare gli individui in base alle loro caratteristiche fisiche.

Le funzionalità biometriche sono diventate onnipresenti su smartphone e tablet commerciali, tra cui l'impronta digitale di Apple e la scansione del viso, l'impronta digitale di Samsung, la scansione del viso e dell'iride e molti altri.

L'utilizzo della biometria con i dispositivi mobili potrebbe potenzialmente aiutare a rendere l'autenticazione più rapida e semplice, ma ci sono sfide con la biometria dei dispositivi mobili in generale e anche specificamente per i primi soccorritori.

BIOMETRICS AND BIOMETRIC AUTHENTICATION BASICS

DEFINIZIONE*: le linee guida sull'identità digitale del NIST definiscono la biometria come "**riconoscimento automatizzato di individui in base alle loro caratteristiche biologiche e comportamentali**".*

È importante garantire che solo le persone autorizzate possano accedere alle informazioni sensibili.

L'autenticazione di un utente implica la verifica dell'evidenza di uno o più fattori di autenticazione, come descritto nella Tabella 1.

Table 1: Authentication Factors

Authentication Factor	Description	Examples
Something you know	A *secret*—non-public information shared between an end user and a digital service.	Password Personal identification number (PIN)
Something you have	A physical device that stores a secret and is possessed by the end user and only the end user.	Cryptographic token
Something you are	A biometric. As Section 2.2 discusses, biometrics are *private*, not secret, so there are limitations on using "something you are" authentication factors.	Fingerprint Facial image Iris pattern

MULTI-FACTOR AUTHENTICATION (MFA) - *autenticazione che utilizza una combinazione di due o più tipi di fattori di autenticazione: fornisce un'autenticazione più forte rispetto all'autenticazione a un fattore. Inoltre, le politiche di sicurezza come la CJIS Security Policy richiedono MFA per l'accesso alle informazioni sensibili.*

*Un'opzione per l'MFA consiste nel richiedere all'utente finale di autenticarsi con "***qualcosa che hai***" attivato da "***qualcosa che conosci***", in modo che il servizio abbia la prova del possesso del dispositivo fisico.*

Sfortunatamente, questo è spesso difficile per i primi soccorritori, che dovrebbero memorizzare i segreti e inserire rapidamente il segreto corretto durante un'emergenza per ottenere l'accesso a informazioni vitali.

*Un'altra opzione per l'MFA è utilizzare "***qualcosa che sei***" invece di "***qualcosa che conosci***" per attivare "***qualcosa che hai***".*

Ad esempio, un primo soccorritore potrebbe utilizzare un'impronta biometrica anziché un PIN o una password per attivare un dispositivo mobile contenente una chiave crittografica segreta ben protetta.

BIOMETRIC MATCHING AND VERIFICATION MODE

La Figura 2 mostra i passaggi di un modello di corrispondenza biometrica semplificato per la verifica dell'identità di una persona.

Durante la registrazione, i dati biometrici di un nuovo utente vengono raccolti e archiviati per un uso futuro nella verifica dell'identità durante i tentativi di autenticazione.

La metà superiore della Figura 2 illustra i seguenti passaggi.

1. *Un campione biometrico viene raccolto catturando un'immagine (o qualche altra somiglianza) del tratto biometrico (noto anche come presentazione) dal nuovo utente.*
2. *Il campione biometrico viene elaborato in un set di caratteristiche contenente le caratteristiche utilizzate per caratterizzare la gamma di somiglianze e differenze tra i campioni.*
3. *Il set di funzionalità viene convertito, per mezzo di in una rappresentazione matematica, in una forma compatta denominata modello. Il modello di iscrizione (enrollment template) è un campione conforme ai requisiti di qualità del sistema biometrico.*
4. *Il modello di registrazione viene archiviato come riferimento per i confronti nelle richieste di identità future.*

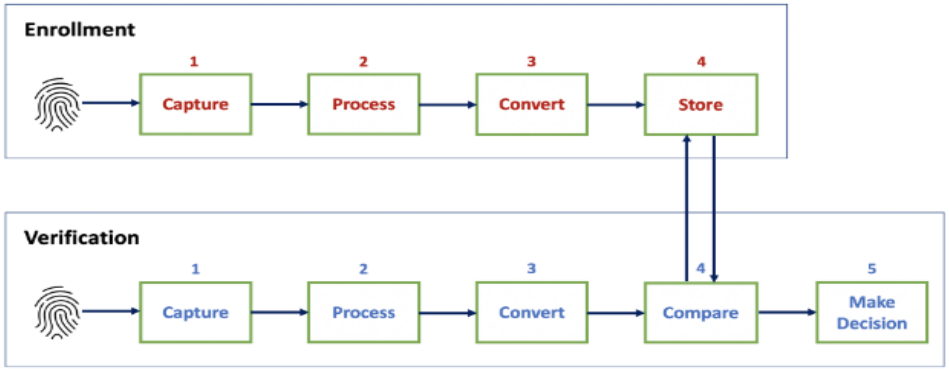


Figure 2: Simplified Biometric Matching Model

La metà inferiore della Figura 2 illustra i passaggi per verificare un'identità dichiarata:

1. *L'utente che rivendica l'identità dell'iscritto presenta un nuovo campione del biometrico precedentemente registrato (ad esempio, impronta digitale) per generare un campione di autenticazione (chiamato anche sonda/*probe*).*
2. *Il campione di autenticazione viene elaborato in un set di funzioni.*
3. *Il set di funzionalità viene convertito in un modello.*
4. *Il modello viene quindi confrontato con il modello di registrazione per l'identità rivendicata mediante un algoritmo di corrispondenza per generare un punteggio di somiglianza.*
5. *Il punteggio di somiglianza viene confrontato con un punteggio soglia per decidere se i due campioni provenissero dalla stessa persona e dallo stesso dito.*

Gli ultimi due passaggi, la generazione di un punteggio di somiglianza e il confronto con un punteggio di soglia, indicano ciò che rende la biometria significativamente diversa dagli altri tipi di fattori di autenticazione.

*I fattori di autenticazione "***Qualcosa che sai***" e "***qualcosa che hai***" utilizzano confronti deterministici per verificare l'identità.*

In altre parole, quando un utente fornisce una password per l'autenticazione, tale password deve corrispondere esattamente alla password memorizzata con cui viene confrontata.

Quando una chiave crittografica viene utilizzata in un protocollo di autenticazione, la chiave deve essere esattamente la chiave necessaria.

TIP*: i passaggi nella Figura 2 possono essere utilizzati anche per identificare una persona sconosciuta. Il modello da verificare può essere confrontato con tutti i modelli di iscrizione, non solo con uno. Tuttavia, è importante notare che le immagini utilizzate per la verifica possono funzionare diversamente se utilizzate a scopo di identificazione.*

Quando la biometria è utilizzata nell'autenticazione, una misurazione corrente di una caratteristica o di un tratto è confrontata con misurazioni memorizzate.

Le misurazioni nuove e memorizzate non sono esattamente le stesse, quindi il confronto delle misurazioni determina una valutazione della probabilità che siano misurazioni della stessa persona.

Un'autenticazione che utilizza la biometria è probabilistica, non deterministica.

L'impostazione corretta del punteggio soglia per un sistema biometrico è di fondamentale importanza per le prestazioni complessive del sistema.

Le prestazioni di alcuni dati biometrici non sono uniformi tra i diversi gruppi demografici, quindi è importante incorporare un campione rappresentativo di individui nel testare le prestazioni di un'implementazione biometrica.

BIOMETRIC SYSTEM COMPONENT

Il modello di corrispondenza biometrica è implementato da un sistema biometrico.

Un tipico sistema biometrico ha diversi componenti di base, inclusi i seguenti.

- ✓ *Un* **SENSOR** *raccoglie un campione; esempi includono lettori di impronte digitali e fotocamere. I sensori vengono utilizzati sia per la registrazione che per la verifica.*
- ✓ *Un* **EXTRACTOR** *converte il campione in un modello.*
- ✓ *Un* **DATABASE** *di* **REFERENCE** *memorizza i modelli di iscrizione.*
- ✓ *Un* **COMPARATOR** *genera un punteggio confrontando i modelli da verificare con i riferimenti memorizzati.*
- ✓ *Un* **MATCHER** *genera un risultato di corrispondenza controllando il punteggio di somiglianza con il punteggio di soglia.*

Questi componenti non sono necessariamente tutti in un unico posto.

Alcuni sistemi biometrici per dispositivi mobili hanno tutti i componenti all'interno dei dispositivi mobili stessi, mentre altri sistemi biometrici hanno alcuni componenti all'interno dei dispositivi mobili e alcuni componenti su server remoti.

Ad esempio, il **COMPARATOR** *potrebbe trovarsi all'interno di un dispositivo mobile, consentendo il confronto locale.*

Oppure potrebbe essere su un server remoto, in modo che i dati biometrici acquisiti dal dispositivo mobile locale possano essere trasferiti a quel server per il confronto con i riferimenti archiviati.

SCREEN UNLOCKING

La registrazione e la verifica avvengono localmente sul dispositivo e possono verificarsi quando il dispositivo è offline.

Lo sblocco dello schermo non autentica intrinsecamente l'utente su alcun sistema o applicazione remota, né fornisce alcuna affermazione dell'identità dell'utente oltre al fatto che la biometria presentata corrisponda a un modello precedentemente registrato su quel dispositivo specifico.

Una volta sbloccato, tuttavia, il dispositivo può concedere all'utente l'accesso a sistemi e applicazioni remoti tramite credenziali memorizzate o sessioni e token attivi.

Lo sblocco dello schermo è un importante controllo di sicurezza, ma le Linee guida sull'identità digitale rilevano che lo sblocco di un dispositivo tramite corrispondenza biometrica non può essere considerato un fattore di autenticazione.

In genere non è possibile per il verificatore ottenere alcuna informazione su come o se il dispositivo è stato sbloccato.

CAUTION: *le Linee guida sull'identità digitale rilevano che lo sblocco di un dispositivo tramite corrispondenza biometrica non può essere considerato un fattore di autenticazione.*

LOCAL AND REMOTE BIOMETRIC VERIFICATION

Le Digital Identity Guidelines descrivono diversi tipi di MFA che potrebbero incorporare dati biometrici, inclusi dispositivi OTP (One Time Password) e dispositivi crittografici in forme hardware e software.

Questi autenticatori in genere richiedono la verifica dell'utente con un segreto biometrico (o un segreto memorizzato) per attivare l'autenticatore.

Una volta attivato, l'autenticatore svolge la sua funzione crittografica (ad esempio, genera una password monouso o firma crittograficamente una richiesta di autenticazione).

Quando la biometria è utilizzata per attivare un autenticatore a più fattori in questo modo, la convalida biometrica è locale (sul dispositivo dell'utente o su un autenticatore hardware stesso).

Il servizio remoto o l'applicazione a cui l'utente si sta autenticando non ha un'interazione diretta con il biometrico, ma poiché è noto che l'autenticatore richieda l'attivazione biometrica, il processo di autenticazione crittografica garantisce che l'autenticazione a più fattori sia stata eseguita.

In alternativa alla verifica locale, la misurazione biometrica può essere inviata (tipicamente in forma astratta) a un server remoto per la verifica.

BIOMETRICS AND PRIVACY

La raccolta e l'uso di campioni biometrici sollevano problemi di privacy.

I dati biometrici sono intrinsecamente personali e alcuni tipi di dati biometrici possono essere abusati per identificare e tracciare le persone.

Alcuni dati biometrici, come le immagini facciali, possono essere acquisiti a distanza senza la cooperazione o la conoscenza del soggetto.

Identificatori come nomi utente o indirizzi e-mail possono essere modificati se sono esposti a individui non autorizzati, ma i dati biometrici sono legati alle caratteristiche innate del soggetto e in genere non possono essere modificati.

I dati biometrici costituiscono informazioni sensibili di identificazione personale (PII), che comportano l'obbligo di proteggerli dall'accesso o dalla divulgazione non autorizzati.

Ai sensi dell'Health Insurance Portability and Accountability Act del 1996 (HIPAA), anche i dati biometrici sono considerati informazioni sanitarie protette (PHI).

L'utilizzo dell'impronta digitale o del riconoscimento facciale per sbloccare un dispositivo mobile è un esempio di verifica locale.

La compromissione dei dati biometrici registrati richiede in genere l'ottenimento del dispositivo fisico e l'annullamento dei meccanismi di sicurezza del software e del firmware.

Quando viene utilizzata la verifica remota, i modelli biometrici sono generalmente archiviati in un database centrale e l'immagine biometrica (o una rappresentazione astratta da essa derivata) è inviata in rete.

Ciò introduce il rischio di intercettazione dei dati biometrici in transito; inoltre, se il database di verifica è compromesso, ciò potrebbe consentire la compromissione di massa dei dati biometrici di tutti gli individui iscritti al sistema.

Per mitigare questi rischi, NIST SP 800-63B richiede che i dati biometrici siano inviati su un canale protetto autenticato e che siano implementate le protezioni dei modelli biometrici specificate nell'International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 24745. ISO/IEC 24745 fornisce requisiti di sicurezza e privacy e linee guida per la gestione dei dati biometrici, incluso un meccanismo per revocare un biometrico registrato.

CHALLENGES IN BIOMETRIC EFFICACY

Per utilizzare la biometria nell'autenticazione, è necessaria una ragionevole fiducia che il sistema biometrico verifichi correttamente le persone autorizzate e non verifichi le persone non autorizzate.

ERRORS AND METRICS

Ogni componente in un sistema biometrico introduce una probabilità di errore per l'intero sistema:

1. *Un* **ERRORE DI ACQUISIZIONE (FAILURE OF CAPTURE - FTC)** *si verifica quando un sensore non riesce a rilevare correttamente un campione a causa di alcune limitazioni (ad esempio, cattive condizioni di illuminazione).*

2. *Un* **ERRORE DI ESTRAZIONE (FAILURE OF EXTRACT - FTX)** *si verifica quando la qualità del campione non è sufficientemente buona per generare un modello valido.*
3. *Una* **MANCATA REGISTRAZIONE (FAILURE TO ENROLL - FTE)** *si verifica quando un modello non soddisfa i criteri di registrazione (ad esempio, il modello non è un identificatore di riferimento distinguibile in modo univoco).*
4. *Gli errori di* **FALSA CORRISPONDENZA (FALSE MATCH - FM)** *si verificano quando il matcher decide erroneamente che un modello appena raccolto corrisponde al riferimento memorizzato e gli errori di falsa corrispondenza* **(FALSE NON MATCH - FNM)** *si verificano quando decide erroneamente che un modello appena raccolto non corrisponde al riferimento memorizzato.*

La combinazione di questi errori definisce l'accuratezza complessiva del sistema biometrico.

Varie metriche sono utilizzate per descrivere l'accuratezza dei sistemi biometrici:

1. *Il* **FALSE ACCEPT RATE (FAR)** *è la frequenza della falsa corrispondenza. Ciò si verifica quando il campione di un individuo viene confrontato con il riferimento di un altro individuo e il punteggio di confronto supera la soglia, quindi viene effettuata una corrispondenza errata.*
2. *Il* **TASSO DI FALSO RIFIUTO (FALSE REJECT RATE - FRR)** *è la frequenza dei falsi non corrispondenti (frequenza dei falsi negativi – nota di Aldo Pedico). Ciò si verifica quando il campione di un individuo viene confrontato con il riferimento dello stesso individuo e il punteggio di confronto è inferiore alla soglia, quindi erroneamente non viene effettuata una corrispondenza.*
3. *Lo* **SPOOF ACCEPT RATE (SAR)** *è la frequenza con cui un sistema biometrico accetta un campione noto precedentemente registrato (ad esempio, una fotografia o una registrazione della voce di qualcuno) per il confronto invece di un campione effettivo. SAR non è un termine standard del settore, ma viene utilizzato nella documentazione di Google.*

CAUTION*: a volte viene utilizzato il termine False Match Rate (FMR) al posto di FAR, ma questi termini hanno in realtà significati leggermente diversi e non dovrebbero essere scambiati. L'FMR include tutti i campioni, indipendentemente dai problemi di qualità dell'immagine, mentre il FAR include solo i campioni che possono essere elaborati correttamente in modelli. La stessa distinzione vale per il tasso di falsa corrispondenza (FNMR) e l'FRR*

BIOMETRIC UNLOCKING PERFORMANCE

Google ha documentato le soglie di prestazione per lo sblocco biometrico dei dispositivi mobili con Android.

Le implementazioni biometriche di Android sono designate come Classe 1, 2 o 3 in base a numerosi requisiti, incluso il rispetto delle metriche SAR, FAR e FRR presentate nella Tabella 2.

La colonna Biometric Pipeline è una valutazione dell'impatto di una compromissione del sistema operativo sulla sicurezza dei dati biometrici.

La pipeline è considerata sicura se tale compromissione non consente la lettura di dati biometrici o l'inserimento di dati che possono influenzare una decisione di autenticazione.

Sebbene i produttori di dispositivi mobili Android debbano testare i propri dispositivi in base ai requisiti e soddisfare anche i requisiti di compatibilità, non devono pubblicare i risultati.

TIP*: vedere https://source.android.com/security/biometric/measure per informazioni dettagliate sui processi di valutazione di Android per la misurazione dell'autenticazione del viso, dell'iride e delle impronte digitali*

Table 2: Google Standards for Biometric Unlocking of Android Mobile Devices

Biometric Tier	Metrics			Biometric Pipeline
	SAR	FAR	FRR	
Class 3 (formerly Strong)	0 - 7%	< 0.002%	10%	Secure
Class 2 (formerly Weak) for new devices	7 - 20%	< 0.002%	10%	Secure
Class 2 (formerly Weak) for upgrading devices	7 - 20%	< 0.002%	10%	Insecure/Secure
Class 1 (formerly Convenience) for new devices	> 20%	< 0.002%	10%	Insecure/Secure
Class 1 (formerly Convenience) for upgrading devices	> 20%	< 0.002%	10%	Insecure/Secure

THE FUTURE OF BIOMETRICS

La biometria è un'area di ricerca e sviluppo attivi, con capacità nuove e migliorate che appaiono regolarmente.

THREE DIMENSIONAL MEASUREMENTS

I sensori di impronte digitali di oggi funzionano catturando una misurazione bidimensionale di un'impronta digitale.

Questi sensori sono soggetti a diverse sfide, come le dita bagnate che interferiscono con la cattura.

Alcuni fornitori commerciali hanno sviluppato sensori a ultrasuoni che catturano misurazioni tridimensionali di un'impronta digitale.

Ciò include le misurazioni delle creste e delle valli delle impronte digitali, fornendo dati aggiuntivi che potrebbero potenzialmente creare un modello altamente accurato.

Inoltre, questa tecnologia può essere in grado di misurare con precisione le impronte digitali in condizioni avverse come umidità o contaminazione.

È importante notare che questi vantaggi teorici dei sensori di impronte digitali a ultrasuoni non sono stati ancora confermati dalla ricerca.

Sebbene non sia attualmente implementato, potrebbe essere possibile leggere le impronte digitali attraverso rivestimenti come i guanti in lattice.

Mentre i dati aggiuntivi forniti dalla misurazione tridimensionale potrebbero potenzialmente migliorare l'accuratezza e l'usabilità della biometria delle impronte digitali, in almeno un caso l'introduzione di nuove tecniche di misurazione ha avuto conseguenze indesiderate.

Quando Samsung ha introdotto un nuovo lettore di impronte digitali a ultrasuoni sullo smartphone Galaxy S10 nell'ottobre 2019, alcuni utenti hanno segnalato che i loro telefoni potevano essere sbloccati dalle impronte digitali di altri utenti (non registrati).

Samsung ha scoperto che con tipi specifici di protezioni dello schermo installate sul dispositivo, il lettore a ultrasuoni rilevava modelli tridimensionali nelle protezioni dello schermo come parte dell'impronta digitale dell'utente durante la registrazione.

Poiché questi modelli erano presenti indipendentemente dall'effettivo dito posizionato sul lettore, creavano un'alta probabilità di falsi errori di accettazione.

Samsung ha risolto il problema con una patch software e ha consigliato a tutti gli utenti di eliminare le impronte digitali registrate e di registrarsi nuovamente.

Questo episodio dimostra perché le nuove tecnologie biometriche dovrebbero essere generalmente considerate con cautela.

Allo stesso modo, sono in fase di sviluppo sensori in grado di fornire misurazioni tridimensionali delle caratteristiche del viso con la promessa di misurazioni più accurate.

WEARABLE SENSORS

Gli smartwatch contengono già sensori in grado di misurare l'andatura e la frequenza cardiaca e i più recenti hanno sensori in grado di catturare i ritmi cardiaci e i livelli di saturazione di ossigeno. Questi sensori hanno lo scopo di fornire dati di monitoraggio della salute per aiutare a rilevare problemi medici.

Tuttavia, sono dati biometrici che possono essere utili per altri scopi.

Ad esempio, supponiamo che un dispositivo indossabile utilizzi il riconoscimento delle impronte digitali per autenticare una persona.

Quando una persona viene autenticata tramite un'impronta digitale, l'indossabile potrebbe associare l'identità a una misurazione dell'elettrocardiogramma.

Attraverso il monitoraggio continuo dell'elettrocardiogramma, l'indossabile potrebbe autenticare continuamente chi lo indossa.

La combinazione dell'elettrocardiogramma e della scansione delle impronte digitali potrebbe fornire una forma di PAD, rendendo più difficile per un utente malintenzionato utilizzare un'impronta digitale fabbricata o altri dati biometrici senza falsificare anche l'autenticazione indossabile.

*Oltre ai tipi di sensori aggiuntivi, i dispositivi indossabili collegati a un dispositivo mobile tramite Bluetooth o Near Field Communication (NFC) offrono la possibilità di aggiungere un fattore "***qualcosa che hai***" al processo di autenticazione senza creare l'onere di trasportare un altro dispositivo, questi offrono anche potenziali vantaggi funzionali.*

BEHAVIORAL BIOMETRIC QUALITY

I sistemi biometrici possono distinguere i soggetti in base a caratteristiche fisiche (o biologiche) e comportamentali.

Alcune delle modalità fisiche includono viso, impronte digitali, iride, schema vascolare/venoso, geometria della mano e retina.

Le modalità comportamentali includono voce, firma, scrittura a mano, battitura e dinamica dell'andatura.

Molte tecnologie biometriche comportamentali incorporano strategie di apprendimento automatico (Machine Learning - ML) che utilizzano un periodo di formazione iniziale per creare un profilo modello dell'utente registrato.

Una volta stabilito, il profilo può essere costantemente confrontato con gli input del sensore per produrre una probabilità che il comportamento attualmente osservato corrisponda al profilo stabilito.

*Poiché la biometria comportamentale generalmente implica la raccolta di informazioni per un periodo di tempo, è più comunemente utilizzata come parte di una strategia di "***autenticazione continua***" per valutare la fiducia durante una sessione piuttosto che come metodo di autenticazione iniziale all'inizio di una sessione.*

Questo approccio si basa sul presupposto che le misurazioni effettuate durante la fase di apprendimento siano affidabili (cioè che non includano misurazioni di individui diversi).

*Alcuni dati biometrici comportamentali possono essere soggetti a "***deriva***" ("***drift***"), in cui il comportamento dell'utente registrato cambia nel tempo o cambiamenti drammatici improvvisi come gli effetti di un infortunio o di un intervento chirurgico sull'andatura di un utente.*

La biometria comportamentale in genere coinvolge algoritmi proprietari per l'interpretazione dei dati dei sensori, la creazione di profili e il confronto continuo, rendendo difficile misurarne l'efficacia in modo standard e uniforme.

La biometria comportamentale viene generalmente utilizzata insieme agli autenticatori convenzionali e ha il potenziale per aumentare la sicurezza fornendo segnali di rischio aggiuntivi.

BIOMETRIC FUSION

Un approccio consiste nell'utilizzare la biometria fusa: raccogliere e utilizzare più dati biometrici.

Molti schemi di fusione biometrica sono stati e continuano ad essere sviluppati e testati.

La sfida per la biometria fusa è imparare quali tratti fondere, quando fondere i tratti e come fondere i tratti per ottenere i migliori risultati complessivi.

La fusione può avvenire all'interno o attraverso uno qualsiasi dei componenti di un sistema biometrico.

Le misurazioni biometriche possono anche essere fuse con segnali resi disponibili da altri sensori su un dispositivo client, inclusi dati biometrici comportamentali e altri dati contestuali come la posizione.

Biometrica Fusion si riferisce a questo ampio concetto di fusione in cui la biometria fisica, la biometria comportamentale e altri dati contestuali o segnali di rischio possono essere considerati in un calcolo complessivo della fiducia.

I dispositivi mobili in genere includono una vasta gamma di sensori, comprese le fotocamere rivolte all'utente; radio cellulari, Bluetooth e Wi-Fi; Ricevitori GPS (Global Positioning System); e accelerometri.

Le modalità biometriche fisiche e comportamentali come il volto, la voce, l'andatura e le dinamiche delle interazioni del dispositivo (incluso l'angolo con cui l'utente tiene il dispositivo) possono essere misurate utilizzando una combinazione di input del sensore.

Oltre alla biometria, è possibile misurare e analizzare gli attributi contestuali.

Gli attributi contestuali potrebbero includere dispositivi connessi (inclusi dispositivi indossabili e altri dispositivi Bluetooth), reti disponibili e connesse (ad es. Wi-Fi) e posizione GPS.

Qualsiasi combinazione di questi attributi biometrici e contestuali può essere misurata, analizzata e utilizzata per creare e aggiornare continuamente un "punteggio di affidabilità" composito che indica la sicurezza che il dispositivo viene utilizzato dall'utente autorizzato.

Come con la biometria comportamentale, questa valutazione continua della fiducia sfrutta spesso il machine learning e la valutazione rispetto a un modello addestrato di comportamenti e input previsti.

In una revisione del 2019 dei documenti di ricerca disponibili sulla biometria fusa, il NIST ha concluso che la biometria fusa aveva potenziali vantaggi, tra cui la **COMPENSAZIONE DELLE DISPARITÀ** *in termini di universalità, unicità e permanenza di diverse modalità biometriche e rendendo più difficili gli attacchi di presentazione.*

Sebbene molti dei documenti esaminati sostengano una maggiore precisione quando sono stati fusi più dati biometrici, la maggior parte non ha fornito prove sufficienti per valutare appieno tali affermazioni.

Sebbene sia difficile determinarne la precisione e l'efficacia, la biometria fusa presenta potenziali vantaggi se utilizzata insieme agli autenticatori convenzionali.

Il punteggio di affidabilità composito generato dalla biometria fusa potrebbe essere utilizzato per ridurre i requisiti di autenticazione per le risorse meno sensibili, ad esempio consentendo l'accesso senza richiedere MFA quando un punteggio di affidabilità è alto.

Come con la biometria comportamentale, un punteggio di affidabilità composito potrebbe essere utilizzato per richiedere un'autenticazione aggiuntiva o graduale quando il punteggio è inferiore a una certa soglia o attivare un blocco del dispositivo mobile e richiedere una riautenticazione completa.

Note*: Poiché i dati biometrici sono autenticatori probabilistici, anche quando sono fusi più dati biometrici, non soddisfano i requisiti SP 800-63B per Authenticator Assurance Level (AAL)2. Tuttavia, i dati biometrici possono supportare AAL2 se utilizzati come parte di uno schema MFA che include un autenticatore che fornisce un fattore di possesso.*

PARTE V: AMBIENTE CLOUD

[Rif.: Threat Modeling for Cloud Data Center Infrastructures; NIST IR 8320]

33. MODELLO DI MINACCE

CLOUD O OUTSOURCING: *termini diversi per identificare la dislocazione remota dei dati digitali e dei processi automatici presso terzi.*

I problemi di sicurezza ci sono e ci saranno sempre: cambiano le tecnologie e i termini (public cloud, private cloud, soluzioni hybrid e chi più ne ha più ne metta) ma le preoccupazioni rimangono.

Modelli di minaccia e le metriche di sicurezza, tra cui superficie di attacco, albero di attacco, grafico di attacco, metrica basata su albero di attacco (ATM) e metrica basata su rete Bayesian (BN).

SUPERFICIE DI ATTACCO: *originariamente proposta come metrica per la sicurezza del software, la superficie di attacco cattura i componenti software che possono causare potenziali vulnerabilità.*

- ✓ *Questi possono includere punti di entrata e uscita (ad es. Metodi in un programma software che accettano input dell'utente o generano output), canali di comunicazione (ad es. TCP o UDP) ed elementi di dati non attendibili (ad es. File di configurazione o chiavi di registro letti dal Software).*
- ✓ *A causa della complessità dell'esame del codice sorgente, la maggior parte dei lavori esistenti applica il concetto in modo meno formale. Ad esempio, tra un utente finale, il provider cloud e i servizi cloud, è possibile comporre sei superfici di attacco*

ALBERO DI ATTACCO: *mentre la superficie di attacco si concentra su ciò che può fornire agli attaccanti privilegi iniziali o accessi a un sistema, gli alberi d'attacco dimostrano i possibili percorsi di attacco che possono essere seguiti dall'attaccante per infiltrarsi ulteriormente nel sistema.*

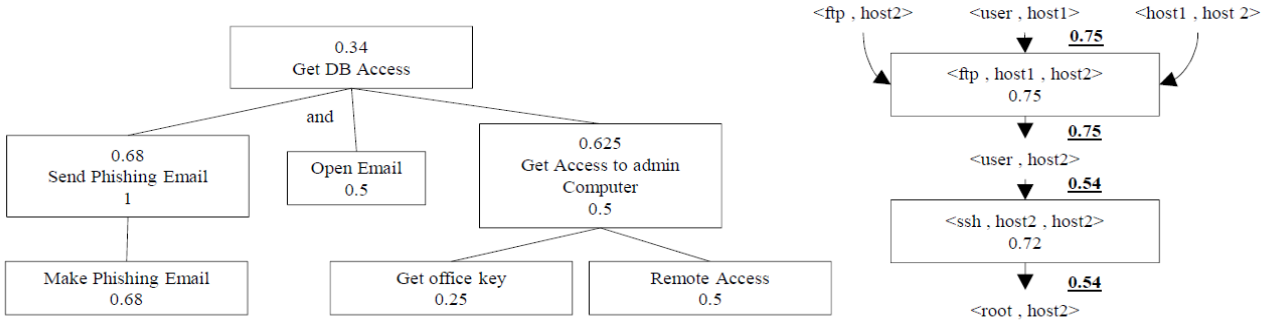


Fig. 1: Attack Tree (Left) and Attack Graph (Right)

Il lato sinistro della Fig.1 mostra un esempio di albero di attacco in cui l'obiettivo dell'attaccante è ottenere l'accesso al database. Nell'esempio, ci sono 2 modi per raggiungere il nodo radice (l'obiettivo). Innanzitutto, l'attaccante può seguire i percorsi sinistro e medio contemporaneamente (a causa dell'etichetta «AND»), oppure l'attaccante può seguire il percorso giusto per raggiungere il nodo principale.

La probabilità all'interno di un rettangolo è il punteggio CVSS diviso 10, e ogni numero sottolineato rappresenta la probabilità di eseguire con successo quell'exploit. L'obiettivo di attacco ha una probabilità di 0,54 e se cambiamo il servizio FTP su host2 e supponiamo che la nuova probabilità diventi 0,4, la nuova probabilità di attacco per l'obiettivo diventerà 0,228, indicando una maggiore sicurezza.

Nella parte destra della Figura 1, ogni tripletta all'interno di un rettangolo indica un exploit <vulnerabilità del servizio, host di origine, host di destinazione> e ogni coppia in testo normale indica una <condizione, host> pre o post condizione degli exploit.

Le relazioni logiche tra i nodi sono rappresentato in base al presupposto che qualsiasi exploit può essere eseguito se e solo se tutte le sue pre-condizioni sono già soddisfatte (ad esempio, nella Fig.1, il primo exploit richiede che

tutte e tre le pre-condizioni siano soddisfatte), mentre qualsiasi condizione può essere soddisfatta da un exploit per il quale il primo è una post-condizione.

I modelli di minaccia di cui sopra sono tutti di natura qualitativa.

La metrica basata sull'albero di attacco (ATM) quantifica la minaccia in un albero di attacco usando il concetto di probabilità di successo.

La probabilità di ciascun nodo nella struttura di attacco è generalmente determinata sulla base di dati storici, opinioni di esperti o entrambi.

Nella Fig.1, il numero sopra l'etichetta rappresenta la probabilità complessiva di successo e il numero sotto l'etichetta rappresenta la probabilità di ciascun nodo da solo.

La probabilità sul nodo radice indica il percorso più rischioso, che dovrebbe essere prioritario nel rafforzamento della sicurezza.

La metrica basata su BN [24, 9] può essere applicata ai grafici di attacco per calcolare la probabilità per un attaccante medio di compromettere un asset critico.

Le probabilità condizionali che un exploit possa essere eseguito alla luce delle sue condizioni preliminari sono tutte soddisfatte, possono generalmente essere stimate sulla base di punteggi di vulnerabilità standard (ad esempio, i punteggi CVSS).

Nella Fig.1, la probabilità all'interno di un rettangolo è il punteggio CVSS diviso per 10, e ogni numero sottolineato rappresenta la probabilità di eseguire con successo quell'exploit.

In questo esempio, l'obiettivo di attacco ha una probabilità di 0,54 e se cambiamo il servizio FTP su host2 e supponiamo che la nuova probabilità diventi 0,4, la nuova probabilità di attacco per l'obiettivo diventerà 0,228, indicando una maggiore sicurezza.

34. SUPERFICIE D'ATTACCO

Applichiamo il concetto di superficie di attacco a livello di risorsa.

Consideriamo la classe di servizio come lo strato intermedio tra gli utenti e il fornitore di servizi cloud, nel senso che, se un utente desidera attaccare un fornitore di servizi cloud, deve passare attraverso una superficie di attacco costituita da servizi.

Concentriamo sui punti di entrata e di uscita che indicano rispettivamente i mezzi attraverso i quali inizia l'attacco e quelli attraverso i quali i dati vengono divulgati.

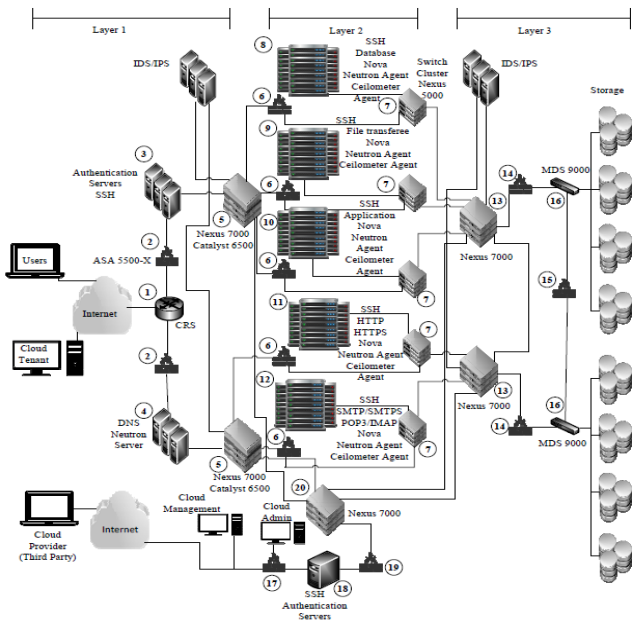


Fig. 2: Cloud Data Center Infrastructure 1

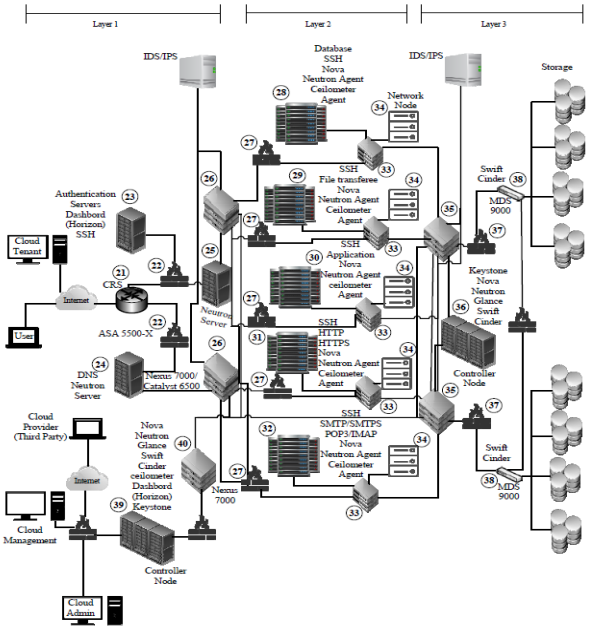


Fig. 3: Cloud Data Center Infrastructure 2

Nelle figure 2 e 3 si può osservare che ci sono 3 tipi di superfici di attacco in un data center cloud.

1) *Superfici di attacco correlate alla rete fisica, che coinvolgono componenti hardware e software, quali switch, router, server, applicazioni e sistemi operativi.*
2) *Superfici di attacco correlate alla virtualizzazione, come hypervisor e switch virtuali.*
3) *Sistemi operativi cloud, come i componenti Open-Stack (Glance, Neutron, Nova, Ceilometer e Keystone).*

Il primo tipo di superficie di attacco è simile a quello delle reti tradizionali, ma devono essere considerati anche i componenti relativi al cloud in esecuzione sulla rete fisica.

ATTACK SURFACE W.R.T. USERS

Consideriamo due tipi di utenti.

1) **L'UTENTE NORMALE** *che utilizza il servizio cloud può mirare ad attaccare il titolare del cloud proprietario di quel servizio, un altro titolare del cloud o i suoi utenti che utilizzano lo stesso cloud o il fornitore del cloud.*
2) **L'INQUILINO** *del cloud può mirare ad attaccare un altro inquilino del cloud e i suoi utenti o il fornitore del cloud. (Diverse superfici possono essere utilizzate dagli utenti per attaccare il cloud, tra cui hypervisor, VM, API e servizi Web e componenti OpenStack - ad es. Horizon, Keystone, Neutron, Glance e Nova).*

Esempio 1

Un utente normale desidera attaccare un hypervisor sul server VM del database (host 8) per rubare informazioni su tutte le VM in esecuzione su quella macchina. Innanzitutto, il punto di ingresso per iniziare questo attacco è la VM del database sull'hypervisor. Dopo aver ottenuto gli accessi iniziali alla VM del database, quella VM diventa un punto di uscita per attaccare l'hypervisor.

Infine, con l'accesso all'hypervisor, ad esempio attraverso lo sfruttamento di CVE-2013-4344, l'attaccante può ottenere i dati relativi a tutte le VM in esecuzione su questo hypervisor e l'hypervisor diventa quindi un punto di uscita.

Quindi prendere in considerazione un inquilino cloud che vuole attaccare un altro inquilino ospitato sulla stessa macchina fisica. Innanzitutto, l'attaccante può utilizzare la propria VM come punto di ingresso per ottenere un privilegio per l'hypervisor, ad esempio applicando CVE-2012-3515, quindi l'attaccante utilizzerà l'hypervisor come punto di ingresso per ottenere gli accessi alla VM di destinazione.

ATTACK SURFACE W.R.T. CLOUD PROVIDER

Il provider cloud si riferisce a un operatore che ha i privilegi di accedere a determinati componenti (ad es. Switch, firewall e SAN) per scopi di manutenzione e gestione.

Questo tipo di utenti malintenzionati può utilizzare i suoi accessi alle risorse per attaccare il centro dati cloud. Tutti e tre i tipi di superfici di attacco spiegati in precedenza possono essere utilizzati da tale attaccante.

Esempio 2

Un operatore che ha accesso a Nexus 7000 (nodo 13) per la gestione desidera ottenere l'accesso a dati sensibili relativi ad un inquilino.

Innanzitutto, può utilizzare Nexus 7000 come punto di ingresso per ottenere un privilegio di root su Nexus 7000, quindi utilizzare questa macchina come punto di uscita per avviare un altro attacco per ottenere dati dal dispositivo di archiviazione (nodo 16].

Altri riferimenti per la gestione della sicurezza in altri ambienti - Information Supplement: PCI DSS Cloud Computing Guidelines.

34A. MINACCE, CONTROMISURE E MONITORAGGIO

MINACCE

Dal NIST IR 8320 - Hw Enabled Security: Enabled Layered Approach Platform Security Cloud and Edge Computing Cases, prendere cap. 2, 3, 4

CONTROMISURE

Dal NIST IR 8320 - Hw Enabled Security: Enabled Layered Approach Platform Security Cloud and Edge Computing Cases, prendere cap. 5

MONITORAGGIO

Dal NIST IR 8320 - Hw Enabled Security: Enabled Layered Approach Platform Security Cloud and Edge Computing Cases, prendere cap. 6, 7

PARTE VI: ICT SUPPLY CHAIN RISK MANAGEMENT - SCRM

[Rif.: NIST SP 800-161; NIST SP 1800-34B]

34B. ABSTRACT

[Rif.: NIST SP 1800-34B]

Organizations are increasingly at risk of cyber supply chain compromise, whether intentional or unintentional.

Cyber supply chain risks include counterfeiting (contraffazione), unauthorized production, tampering (manomissione), theft, and insertion of unexpected software and hardware.

Managing these risks requires ensuring the integrity of the cyber supply chain and its products and services.

This project will demonstrate how organizations can verify that the internal components of the computing devices they acquire, whether laptops or servers, are genuine and have not been tampered with.

This solution relies on device vendors storing information within each device, and organizations using a combination of commercial off-the-shelf and open-source tools that work together to validate the stored information.

This NIST Cybersecurity Practice Guide provides a preliminary draft describing the work performed so far to build and test the full solution.

34C. CHALLENGE

[Rif.: NIST SP 1800-34B]

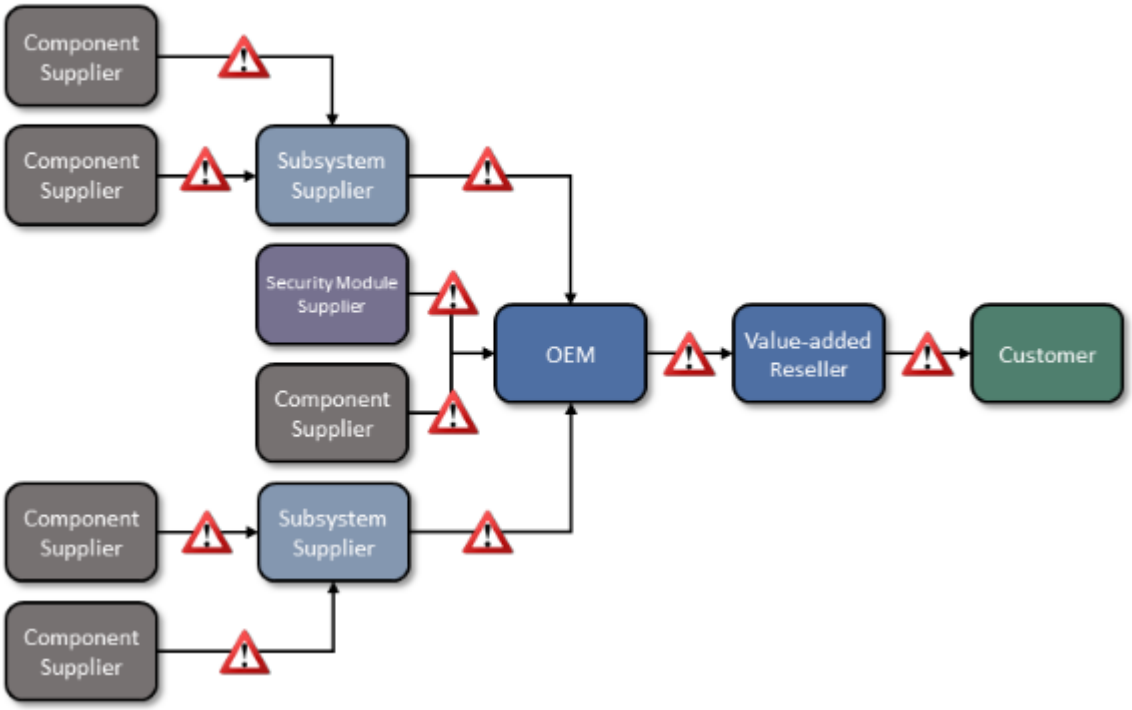
Technologies today rely on complex, globally distributed and interconnected supply chain ecosystems to provide highly refined, cost-effective, and reusable solutions.

The provenance and integrity of a delivered device and its components are typically accepted without validating through technology that there have been no unexpected modifications.

Assuming that all acquired computing devices are genuine and unmodified INCREASES THE RISK OF A COMPROMISE AFFECTING PRODUCTS IN AN ORGANIZATION'S SUPPLY CHAIN*, which in turn increases risks to customers and end users, as illustrated in Figure 1-1.*

Mitigating this risk is not addressed at all in many cases.

Figure 1-1 Supply Chain Risk



34D. RISK ASSESSMENT

[Rif.: NIST SP 1800-34B]

NIST SPECIAL PUBLICATION (SP) 800-30 R1, GUIDE FOR CONDUCTING RISK ASSESSMENTS, *states that risk is "a measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of:*

(i) the adverse impacts that would arise if the circumstance or event occurs; and

(ii) the likelihood of occurrence.

The guide further defines risk assessment as "the process of identifying, estimating, and prioritizing risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of an information system. Part of risk management incorporates threat and vulnerability analyses, and considers mitigations provided by security controls planned or in place."

The NCCoE recommends that any discussion of supply chain risk management should begin with a comprehensive review of NIST SP 800-161, Supply Chain Risk Management Practices.

NIST SP 800-161 defines an ICT supply chain compromise as an occurrence within the ICT supply chain whereby an adversary jeopardizes the confidentiality, integrity, or availability of a system or the information the system processes, stores, or transmits. An ICT supply chain compromise can occur anywhere within the system development life cycle of the product or service.

In addition, NIST SP 800-37 R2, Risk Management Framework for Information Systems and Organizations provides Risk Management Framework *guidance that gives a baseline to assess risks to information system assets, including threats to the IT system supply chain.*

THREATS

Prototype implementation does not defend against all ICT threats, but Table 3-1 captures threats from NIST SP 800-161 that are relevant to this project.

TABLE 3-1 NIST SP 800-161 THREAT EVENTS

Threat Events	Description
Craft attacks specifically based on deployed IT environment.	Adversary develops attacks (e.g., crafts targeted malware) that take advantage of knowledge of the organizational IT environment.
Create counterfeit/spoof website.	Adversary creates duplicates of legitimate websites; when users visit a counterfeit site, the site can gather information or download malware.
Craft counterfeit certificates.	Adversary counterfeits or compromises a certificate authority so that malware or connections will appear legitimate.
Create and operate false front organizations to inject malicious components into the supply chain.	Adversary creates false front organizations with the appearance of legitimate suppliers in the critical life cycle path that then inject corrupted/malicious information system components into the organizational supply chain.
Insert counterfeit or tampered hardware into the supply chain.	Adversary intercepts hardware from legitimate suppliers. Adversary modifies the hardware or replaces it with faulty or otherwise modified hardware.
Insert tampered critical components into organizational systems.	Adversary replaces, through supply chain, subverted insider, or some combination thereof, critical information system components with modified or corrupted components.
Compromise design, manufacture, and/or distribution of information system components (including hardware, software, and firmware).	Adversary compromises the design, manufacture, and/or distribution of critical information system components at selected suppliers.
Conduct supply chain attacks targeting and exploiting critical hardware, software, or firmware.	Adversary targets and compromises the operation of software (e.g., through malware injections), firmware, and hardware that perform critical functions for organizations. This is largely accomplished as supply chain attacks on both commercial off-the-shelf and custom information systems and components.
Obtain unauthorized access.	Adversary with authorized access to organizational information systems gains access to resources that exceeds authorization.
Inadvertently introduce vulnerabilities into software products.	Due to inherent weaknesses in programming languages and software development environments, errors and vulnerabilities are introduced into commonly used software products.

VULNERABILITIES

This document is guided by NIST SP 800-161, which describes an ICT supply chain vulnerability as the following:

"A vulnerability is a weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source [FIPS 200], [NIST SP 800-34 R1], [NIST SP 800-53 R4], [NIST SP 800-53A R4], [NIST SP 800-115].

Within the ICT SCRM context, it is any weakness in the system/component design, development, manufacturing, production, shipping and receiving, delivery, operation, and component end-of life that can be exploited by a threat agent. This definition applies to both the systems/components being developed and integrated (i.e., within the SDLC) and to the ICT supply chain infrastructure, including any security mitigations and techniques, such as identity management or access control systems. ICT supply chain vulnerabilities may be found in:

- ✓ The systems/components within the SDLC (i.e., being developed and integrated);
- ✓ The development and operational environment directly impacting the SDLC; and
- ✓ The logistics/delivery environment that transports ICT systems and components (logically or physically)."

RISK

Vedi capitolo ".3.4.3 Risk" del NIST SP 1800-34B

34E. SECURITY CONTROL MAP

[Rif.: NIST SP 1800-34B]

The following tables map the security characteristics defined in our project description (Table 3-3) to the applicable NIST Cybersecurity Framework Functions, Categories, and Subcategories (Table 3-4) to assist organizations better manage and reduce C-SCRM risk. We have also included a mapping to specific SP 800-53 r4 security controls and indicated (in bold) if the control is part of the SP 800-161 baseline security controls to assist organizations interested in alignment with NIST C-SCRM best practices.

Table 3-3 Security Characteristics

Identifier	Security Characteristic
1	Establish a strong device identity to support binding artifacts to a specific device.
2	Cryptographically bind platform attributes and other manufacturing information to a given computer system.
3	Establish assurance for multi-supplier production in which components are embedded at various stages.
4	Provide an acceptance test capability that validates source and integrity of assembled components for the recipient organization of the computer system.
5	Detect unexpected component (firmware) swaps or tampering during the life cycle of the computing device in an operational environment.

Table 3-4 Security Characteristics and Controls Mapping

Cybersecurity Framework v1.1			SP 800-53 R4	Security Characteristics Addressed
Function	**Category**	**Subcategory**		
Identify (ID)	Supply Chain Risk Management (ID.SC)	ID.SC-4: Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations.	**AU-2**	5
			AU-6	5
			SA-19	1,3
	Asset Management (ID.AM)	ID.AM-1: Physical devices and systems within the organization are inventoried.	**CM-8**	4
			AU-10	4
Protect (PR)	Identity Management, Authentication and Access Control (PR.AC)	PR.AC-6: Identities are proofed and bound to credentials and asserted in interactions.	**IA-4**	1
	Data Security (PR.DS)	PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity.	SI-7	4,5
		PR.DS-8: Integrity checking mechanisms are used to verify hardware integrity.	**SA-10**	4,5
			SA-18	1
Detect (DE)	Security Continuous Monitoring (DE.CM)	DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed.	**PE-20**	5

34F. TECHNOLOGIES

[Rif.: NIST SP 1800-34B]

Table 3-5 lists all of the technologies used in this project, and provides a mapping among the generic component term, the specific product or technology used, the function or capability it provides, and the Cybersecurity Framework Subcategories that the product helps support.

Refer to Table 3-4 for an explanation of the NIST Cybersecurity Framework Subcategory codes.

TABLE 3-5 PRODUCTS AND TECHNOLOGIES

Component	Product/Technology	Function/Capability	Cybersecurity Framework Subcategories
Component or Subsystem Manufacturer	Intel Transparent Supply Chain	Tools and processes to ensure supply chain security from the manufacturer to the purchasing organization	ID.SC-4, PR.DS-6
	Seagate EXOS X18 18 Terabyte Hard Drive	Secure device authentication, firmware attestation	ID.SC-4, PR.AC-6, PR.DS-6, PR.DS-8
OEM or VAR	Dell Technologies	Manufactures computing devices and binds them to verifiable artifacts	ID.SC-4
	Hewlett Packard Enterprise		
	HP Inc.		
	Lenovo		
Computing Device	Dell PowerEdge R640 Server	A client device (laptop) or server purchased by an organization to execute tasks by end users	ID.SC-4, PR.AC-6
	Dell Precision 3530		
	HPE ProLiant DL360		
	HP Inc. Elitebook 360 830 G5		
	HP Inc. 840 G7		
	Intel Server Board S2600WTT		
	Lenovo ThinkPad T480		
Asset Discovery and Management System	RSA Archer	Ensures computing devices and associated components are tracked and uniquely identified	ID.AM-1
Configuration Management System	Microsoft Configuration Manager	Enforces corporate governance and policies through actions such as applying software patches and updates, removing denylisted software, and automatically updating configurations	DE.CM-7
Security Information and Event Management Tool	RSA Archer	Real-time analysis of alerts and notifications generated by organizational information systems	DE.CM-7
Certificate Authority	HIRS ACA	Issues an Attestation Identity Credential in accordance with TCG specifications	PR.AC-6, PR.DS-8
Platform Integrity Validation System	Eclypsium Analytic Platform	Validates the integrity of firmware installed on computing devices	PR.DS-6
	HIRS ACA	Validates platform components in accordance with TCG specifications	PR.DS-8
	Platform Manifest Correlation System	Ingests platform manifest data from participating manufacturers	ID.AM-1

34G. CONSIDERAZIONI

Le soluzioni Commercial Off-The-Shelf (COTS) possono essere proprietarie o open source e possono soddisfare le esigenze di una base globale di clienti del settore pubblico e privato.

La stessa globalizzazione e altri fattori che consentono benefici aumentano anche il rischio di un evento di minaccia che può influenzare direttamente o indirettamente la catena di fornitura delle TIC, spesso non rilevata, e in un modo che può comportare rischi per l'utente finale.

Questi rischi della catena di approvvigionamento delle TIC possono includere l'inserimento di contraffazioni, la produzione non autorizzata, la manomissione, il furto, l'inserimento di software e hardware dannosi, nonché le cattive pratiche di produzione e sviluppo nella catena di approvvigionamento delle TIC.

ICT SCRM comprende attività nel ciclo di vita dello sviluppo del sistema, tra cui ricerca e sviluppo (R&S), progettazione, produzione, acquisizione, consegna, integrazione, operazioni e smaltimento/ritiro dei prodotti TIC di un'organizzazione (ovvero hardware e software) e servizi.

ICT SCRM si trova all'intersezione di Sicurezza, Integrità, Resilienza e Qualità.

- ✓ La sicurezza fornisce la riservatezza, l'integrità e la disponibilità *delle informazioni che descrivono la catena di fornitura ICT (ad esempio, informazioni sui percorsi dei prodotti e servizi ICT, sia logici che fisici); oppure attraversa la catena di fornitura delle TIC (ad esempio proprietà intellettuale contenuta in prodotti e servizi TIC), nonché informazioni sulle parti che partecipano alla catena di fornitura TIC (chiunque tocchi un prodotto o servizio TIC durante il suo ciclo di vita);*
- ✓ L'integrità si concentra sul garantire *che i prodotti o servizi ICT nella catena di fornitura ICT siano autentici, inalterati e che i prodotti e servizi ICT funzionino secondo le specifiche dell'acquirente e senza funzionalità indesiderate aggiuntive.*
- ✓ La resilienza si concentra sul garantire *che la catena di approvvigionamento delle TIC fornirà i prodotti e i servizi TIC richiesti sotto stress o fallimento;*
- ✓ La qualità si concentra sulla riduzione *delle vulnerabilità che possono limitare la funzione prevista di un componente, causare guasti ai componenti o offrire opportunità di sfruttamento.*

PARTE VII: LA CIBERSICUREZZA E L'ORGANIZZAZIONE AZIENDALE (ERM)

[Rif.: 1) NIST IR 8286; 2) NIST IR 8183; 3) NIST IR 8286A]

La gestione del rischio d'impresa richiede la comprensione di tutti i rischi NEGATIVI *(minacce) e* POSITIVI *(opportunità) per un'azienda, determinando il modo migliore per affrontare tali rischi e assicurando che vengano intraprese le azioni necessarie.*

Nell'ambito di un programma ERM, le imprese gestiscono l'insieme combinato di rischi in modo olistico.

Tutte le organizzazioni e le imprese, indipendentemente dalle dimensioni o dal tipo, dovrebbero garantire che il rischio per la cibersicurezza riceva la dovuta attenzione mentre svolgono le loro funzioni ERM.

Il documento sui rischi critici utilizzato per tracciare e comunicare le informazioni sui rischi per tutti questi passaggi all'interno dell'azienda è chiamato registro dei rischi.

35. APPROCCIO ALL'ENTERPRISE RISK MANAGEMENT

La Figura 2 del ERM Playbook mostra un esempio di un framework ERM.

La riga superiore nella Figura 2 mostra 6 passi con le frecce che ne indicano la sequenza.

La riga inferiore di caselle spiega l'output di ogni passaggio.

L'elemento nella parte inferiore della figura indica che la comunicazione e la consultazione avvengono in tutte le fasi.

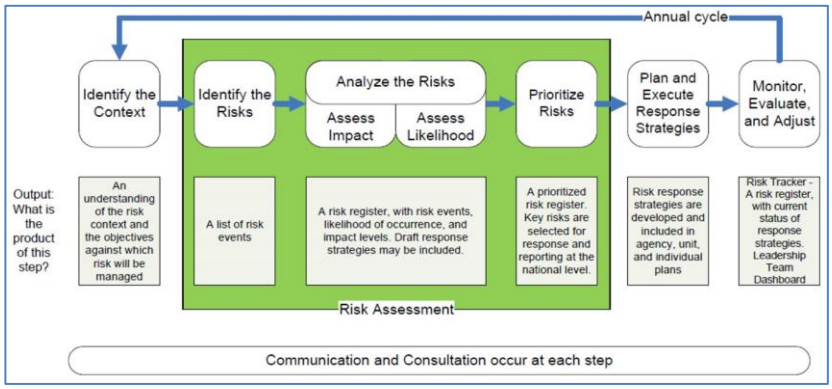


Figure 2: ERM Framework Example

SEI PASSI PER LA GESTIONE DEL RISCHIO

1) IDENTIFICARE IL CONTESTO. *Il contesto è l'ambiente in cui l'impresa opera ed è influenzato dai rischi connessi.*
2) IDENTIFICARE I RISCHI. *Significa: identificare l'insieme completo di rischi positivi (**opportunità**) e negativi (**minacce**); determinare quali eventi potrebbero migliorare o ostacolare gli obiettivi, compresi i rischi derivanti dal mancato perseguimento di un'opportunità.*
3) ANALIZZARE I RISCHI. *Stima della probabilità che si verifichi un evento di rischio e il potenziale impatto delle conseguenze descritte.*
4) PRIORIZZARE I RISCHI. *Esposizione calcolata per ciascun rischio in base alla probabilità e all'impatto potenziale, quindi i rischi sono classificati in base alla loro esposizione.*
5) PIANIFICARE ED ESEGUIRE STRATEGIE DI RISPOSTA AL RISCHIO. *La risposta appropriata è determinata per ciascun rischio, con le decisioni descritte nella guida al rischio da parte della leadership.*
6) MONITORARE, VALUTARE E REGOLARE. *Il monitoraggio continuo garantisce che le condizioni di rischio aziendale rimangano entro i livelli definiti di propensione al rischio.*

DIVARIO TRA GESTIONE DEL RISCHIO DI SICUREZZA INFORMATICA E ERM

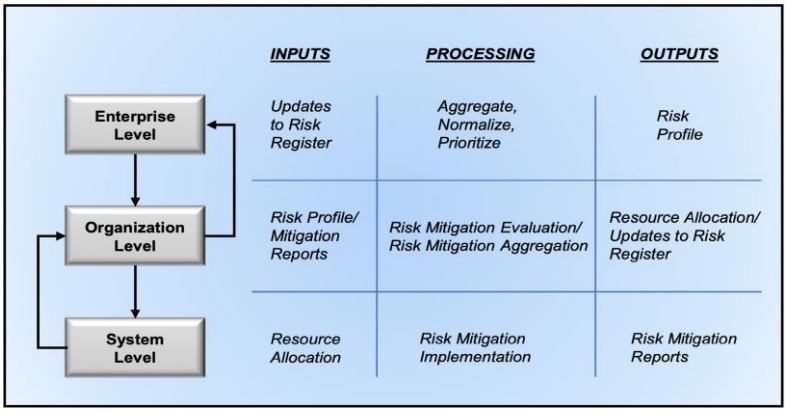
Per allineare il rischio della cibersicurezza con il rischio aziendale

Disporre di un registro dei rischi per la cibersicurezza, che sarebbe principalmente informato dagli obiettivi di cibersicurezza dell'impresa al fine di consentire un facile trasferimento delle conoscenze sul rischio di cibersicurezza dalla Gestione del Rischio di Cibersicurezza all'ERM.

Le organizzazioni dovrebbero utilizzare un registro dei rischi di sicurezza informatica per queste attività di gestione del rischio:

1. AGGREGAZIONE DEI RISCHI *derivanti da minacce avverse e guasti del sistema che provocano informazioni compromesse o segnali di controllo. L'aggregazione è il consolidamento di informazioni simili o correlate.*
2. NORMALIZZAZIONE DELLE INFORMAZIONI *tra le unità organizzative per fornire ai dirigenti aziendali le informazioni necessarie per misurare la missione, le finanze e l'esposizione della reputazione. La normalizzazione è la conversione di informazioni in rappresentazioni e categorizzazioni coerenti.*
3. PRIORIZZARE LE ATTIVITÀ *di mitigazione del rischio operativo combinando le informazioni sui rischi con la missione aziendale e gli orientamenti di bilancio per attuare le risposte appropriate*

Fig.3: Information Flow Between System, Organization, and Enterprise Levels



IMPLEMENTAZIONE DEL CYBERSECURITY FRAMEWORK (CSF)

Il «Profilo di Produzione» del CSF può essere utilizzato come piano delle attività per ridurre il rischio di sicurezza informatica per i produttori in linea con gli obiettivi del settore manifatturiero.

Questo Profilo di Produzione fornisce un approccio basato sul rischio per la gestione delle attività di sicurezza informatica e la riduzione del rischio informatico per i sistemi di produzione.

I Sistemi di Controllo Industriale (Industrial Control Systems - ICS), che includono i sistemi di produzione, rappresentano diversi tipi di sistemi di controllo tra cui Sistemi di Controllo di Supervisione e Acquisizione Dati (Supervisory Control And Data Acquisitions - SCADA), Sistemi di Controllo Distribuito (distributed control systems - DCS) e altre configurazioni di sistemi di controllo come Controllori Logici Programmabili (Programmable Logic Controllers - PLC) spesso presenti nei settori industriali e delle infrastrutture critiche. Un ICS è costituito da combinazioni di componenti di controllo (ad esempio, elettrici, meccanici, idraulici e pneumatici) che agiscono insieme per raggiungere un obiettivo industriale (ad esempio, produzione, trasporto di materia o energia).

ICS supporta il vasto e diversificato settore industriale manifatturiero e può essere classificato come basato su processo, basato su componenti discreti o una combinazione di entrambi.

Il Profilo di Produzione può essere caratterizzato come l'allineamento di standard, linee guida e pratiche al Framework Core in uno scenario di implementazione pratica.

Le industrie manifatturiere basate sui processi utilizzano in genere due tipi di processi principali:

1. PROCESSI DI PRODUZIONE CONTINUI. *Questi processi vengono eseguiti continuamente, spesso con fasi per realizzare diversi gradi di un prodotto. I tipici processi di produzione continua includono il flusso di carburante o vapore in una centrale elettrica, petrolio in una raffineria e distillazione in un impianto chimico.*

2. PROCESSI DI PRODUZIONE IN BATCH. *Questi processi hanno fasi di lavorazione distinte, condotte su una quantità di materiale. C'è un inizio e una fine distinti di un processo batch con la possibilità di brevi operazioni stazionarie durante le fasi intermedie. I tipici processi di produzione in batch includono la produzione di alimenti, bevande e biotecnologie.*

CINQUE OBIETTIVI AZIENDALI E DI MISSIONE DELLA PRODUZIONE

Lo sviluppo del Profilo ha incluso l'identificazione dei comuni obiettivi aziendali e della missione nel settore manifatturiero.

Questi obiettivi forniscono il contesto necessario per identificare e gestire le attività di mitigazione del rischio di sicurezza informatica.

Sono stati individuati cinque obiettivi comuni:

1. MANTENERE LA SICUREZZA AMBIENTALE: *gestire i rischi di sicurezza informatica che potrebbero influire negativamente sull'ambiente, compresi i danni accidentali e intenzionali; il rischio di cibersicurezza sul*

sistema di produzione potrebbe potenzialmente influire negativamente sulla sicurezza ambientale; il personale dovrebbe comprendere le interdipendenze di sicurezza informatica e sicurezza ambientale.

2. MANTENERE LA SICUREZZA UMANA*: gestire i rischi per la sicurezza informatica che potrebbero avere un potenziale impatto sulla sicurezza umana; il rischio per la sicurezza informatica sul sistema di produzione potrebbe potenzialmente influire negativamente sulla sicurezza umana; il personale dovrebbe comprendere la sicurezza informatica e le interdipendenze in materia di sicurezza.*
3. MANTENERE GLI OBIETTIVI DI PRODUZIONE*: gestire i rischi di sicurezza informatica che potrebbero influire negativamente sugli obiettivi di produzione; il rischio di sicurezza informatica sul sistema di produzione, compreso il danneggiamento degli asset, potrebbe potenzialmente influire negativamente sugli obiettivi di produzione; il personale dovrebbe comprendere la sicurezza informatica e le interdipendenze degli obiettivi di produzione.*
4. MANTENERE LA QUALITÀ DEL PRODOTTO*: gestire i rischi di sicurezza informatica che potrebbero influire negativamente sulla qualità del prodotto; protezione contro la compromissione dell'integrità del processo di produzione e dei dati associati.*
5. MANTENERE LE INFORMAZIONI SENSIBILI*: gestire i rischi per la sicurezza informatica che potrebbero portare alla perdita o alla compromissione della proprietà intellettuale dell'organizzazione e dei dati aziendali sensibili, comprese le informazioni di identificazione personale (PII).*

ESEMPI APPLICAZIONE TABELLA FUNZIONI

Table 2 *IDENTIFY Business Mission Objectives*

		Maintain Human Safety	Maintain Environmental Safety	Maintain Quality of Product	Maintain Production Goals	Maintain Trade Secrets
	Category	Subcategories				
ID	Asset Management	ID.AM-1	ID.AM-1	ID.AM-1	ID.AM-1	ID.AM-1
		ID.AM-2	ID.AM-2	ID.AM-2	ID.AM-2	ID.AM-2
		ID.AM-3	ID.AM-3	ID.AM-3	ID.AM-3	ID.AM-3
		ID.AM-4	ID.AM-4	ID.AM-4	ID.AM-4	ID.AM-4
		ID.AM-5	ID.AM-5	ID.AM-5	ID.AM-5	ID.AM-5
		ID.AM-6	ID.AM-6	ID.AM-6	ID.AM-6	ID.AM-6
	Business Environment	ID.BE-1	ID.BE-1	ID.BE-1	ID.BE-1	ID.BE-1
		ID.BE-2	ID.BE-2	ID.BE-2	ID.BE-2	ID.BE-2
		ID.BE-3	ID.BE-3	ID.BE-3	ID.BE-3	ID.BE-3
		ID.BE-4	ID.BE-4	ID.BE-4	ID.BE-4	ID.BE-4
		ID.BE-5	ID.BE-5	ID.BE-5	ID.BE-5	ID.BE-5
	Governance	ID.GV-1	ID.GV-1	ID.GV-1	ID.GV-1	ID.GV-1
		ID.GV-2	ID.GV-2	ID.GV-2	ID.GV-2	ID.GV-2
		ID.GV-3	ID.GV-3	ID.GV-3	ID.GV-3	ID.GV-3
		ID.GV-4	ID.GV-4	ID.GV-4	ID.GV-4	ID.GV-4
	Risk Assessment	ID.RA-1	ID.RA-1	ID.RA-1	ID.RA-1	ID.RA-1
		ID.RA-2	ID.RA-2	ID.RA-2	ID.RA-2	ID.RA-2
		ID.RA-3	ID.RA-3	ID.RA-3	ID.RA-3	ID.RA-3
		ID.RA-4	ID.RA-4	ID.RA-4	ID.RA-4	ID.RA-4
		ID.RA-5	ID.RA-5	ID.RA-5	ID.RA-5	ID.RA-5
		ID.RA-6	ID.RA-6	ID.RA-6	ID.RA-6	ID.RA-6
	Risk Management Strategy	ID.RM-1	ID.RM-1	ID.RM-1	ID.RM-1	ID.RM-1
		ID.RM-2	ID.RM-2	ID.RM-2	ID.RM-2	ID.RM-2
		ID.RM-3	ID.RM-3	ID.RM-3	ID.RM-3	ID.RM-3
	Supply Chain Management	ID.SC-1	ID.SC-1	ID.SC-1	ID.SC-1	ID.SC-1
		ID.SC-2	ID.SC-2	ID.SC-2	ID.SC-2	ID.SC-2
		ID.SC-3	ID.SC-3	ID.SC-3	ID.SC-3	ID.SC-3
		ID.SC-4	ID.SC-4	ID.SC-4	ID.SC-4	ID.SC-4
		ID.SC-5	ID.SC-5	ID.SC-5	ID.SC-5	ID.SC-5

Table 3 *PROTECT Business Mission Objectives*

		Maintain Human Safety	Maintain Environmental Safety	Maintain Quality of Product	Maintain Production Goals	Maintain Trade Secrets
	Category	Subcategories				
PR	Identity Management, Authentication and Access Control	PR.AC-1	PR.AC-1	PR.AC-1	PR.AC-1	PR.AC-1
		PR.AC-2	PR.AC-2	PR.AC-2	PR.AC-2	PR.AC-2
		PR.AC-3	PR.AC-3	PR.AC-3	PR.AC-3	PR.AC-3
		PR.AC-4	PR.AC-4	PR.AC-4	PR.AC-4	PR.AC-4
		PR.AC-5	PR.AC-5	PR.AC-5	PR.AC-5	PR.AC-5
		PR.AC-6	PR.AC-6	PR.AC-6	PR.AC-6	PR.AC-6
		PR.AC-7	PR.AC-7	PR.AC-7	PR.AC-7	PR.AC-7
	Awareness and Training	PR.AT-1	PR.AT-1	PR.AT-1	PR.AT-1	PR.AT-1
		PR.AT-2	PR.AT-2	PR.AT-2	PR.AT-2	PR.AT-2
		PR.AT-3	PR.AT-3	PR.AT-3	PR.AT-3	PR.AT-3
		PR.AT-4	PR.AT-4	PR.AT-4	PR.AT-4	PR.AT-4
		PR.AT-5	PR.AT-5	PR.AT-5	PR.AT-5	PR.AT-5
	Data Security	PR.DS-1	PR.DS-1	PR.DS-1	PR.DS-1	PR.DS-1
		PR.DS-2	PR.DS-2	PR.DS-2	PR.DS-2	PR.DS-2
		PR.DS-3	PR.DS-3	PR.DS-3	PR.DS-3	PR.DS-3
		PR.DS-4	PR.DS-4	PR.DS-4	PR.DS-4	PR.DS-4
		PR.DS-5	PR.DS-5	PR.DS-5	PR.DS-5	PR.DS-5
		PR.DS-6	PR.DS-6	PR.DS-6	PR.DS-6	PR.DS-6
		PR.DS-7	PR.DS-7	PR.DS-7	PR.DS-7	PR.DS-7
		PR.DS-8	PR.DS-8	PR.DS-8	PR.DS-8	PR.DS-8
	Information Protection Processes and Procedures	PR.IP-1	PR.IP-1	PR.IP-1	PR.IP-1	PR.IP-1
		PR.IP-2	PR.IP-2	PR.IP-2	PR.IP-2	PR.IP-2
		PR.IP-3	PR.IP-3	PR.IP-3	PR.IP-3	PR.IP-3
		PR.IP-4	PR.IP-4	PR.IP-4	PR.IP-4	PR.IP-4
		PR.IP-5	PR.IP-5	PR.IP-5	PR.IP-5	PR.IP-5
		PR.IP-6	PR.IP-6	PR.IP-6	PR.IP-6	PR.IP-6
		PR.IP-7	PR.IP-7	PR.IP-7	PR.IP-7	PR.IP-7
		PR.IP-8	PR.IP-8	PR.IP-8	PR.IP-8	PR.IP-8
		PR.IP-9	PR.IP-9	PR.IP-9	PR.IP-9	PR.IP-9
		PR.IP-10	PR.IP-10	PR.IP-10	PR.IP-10	PR.IP-10
		PR.IP-11	PR.IP-11	PR.IP-11	PR.IP-11	PR.IP-11
		PR.IP-12	PR.IP-12	PR.IP-12	PR.IP-12	PR.IP-12
	Maintenance	PR.MA-1	PR.MA-1	PR.MA-1	PR.MA-1	PR.MA-1
		PR.MA-2	PR.MA-2	PR.MA-2	PR.MA-2	PR.MA-2
	Protective Technology	PR.PT-1	PR.PT-1	PR.PT-1	PR.PT-1	PR.PT-1
		PR.PT-2	PR.PT-2	PR.PT-2	PR.PT-2	PR.PT-2
		PR.PT-3	PR.PT-3	PR.PT-3	PR.PT-3	PR.PT-3
		PR.PT-4	PR.PT-4	PR.PT-4	PR.PT-4	PR.PT-4
		PR.PT-5	PR.PT-5	PR.PT-5	PR.PT-5	PR.PT-5

Table 4 *DETECT Business Mission Objectives*

		Maintain Human Safety	Maintain Environmental Safety	Maintain Quality of Product	Maintain Production Goals	Maintain Trade Secrets
Category		Subcategories				
DE	Anomalies and Events	DE.AE-1	DE.AE-1	DE.AE-1	DE.AE-1	DE.AE-1
		DE.AE-2	DE.AE-2	DE.AE-2	DE.AE-2	DE.AE-2
		DE.AE-3	DE.AE-3	DE.AE-3	DE.AE-3	DE.AE-3
		DE.AE-4	DE.AE-4	DE.AE-4	DE.AE-4	DE.AE-4
		DE.AE-5	DE.AE-5	DE.AE-5	DE.AE-5	DE.AE-5
	Security Continuous Monitoring	DE.CM-1	DE.CM-1	DE.CM-1	DE.CM-1	DE.CM-1
		DE.CM-2	DE.CM-2	DE.CM-2	DE.CM-2	DE.CM-2
		DE.CM-3	DE.CM-3	DE.CM-3	DE.CM-3	DE.CM-3
		DE.CM-4	DE.CM-4	DE.CM-4	DE.CM-4	DE.CM-4
		DE.CM-5	DE.CM-5	DE.CM-5	DE.CM-5	DE.CM-5
		DE.CM-6	DE.CM-6	DE.CM-6	DE.CM-6	DE.CM-6
		DE.CM-7	DE.CM-7	DE.CM-7	DE.CM-7	DE.CM-7
		DE.CM-8	DE.CM-8	DE.CM-8	DE.CM-8	DE.CM-8
	Detection Processes	DE.DP-1	DE.DP-1	DE.DP-1	DE.DP-1	DE.DP-1
		DE.DP-2	DE.DP-2	DE.DP-2	DE.DP-2	DE.DP-2
		DE.DP-3	DE.DP-3	DE.DP-3	DE.DP-3	DE.DP-3
		DE.DP-4	DE.DP-4	DE.DP-4	DE.DP-4	DE.DP-4
		DE.DP-5	DE.DP-5	DE.DP-5	DE.DP-5	DE.DP-5

Table 5 *RESPOND Business Mission Objectives*

		Maintain Human Safety	Maintain Environmental Safety	Maintain Quality of Product	Maintain Production Goals	Maintain Trade Secrets
Category		Subcategories				
RS	Response Planning	RS.RP-1	RS.RP-1	RS.RP-1	RS.RP-1	RS.RP-1
	Communications	RS.CO-1	RS.CO-1	RS.CO-1	RS.CO-1	RS.CO-1
		RS.CO-2	RS.CO-2	RS.CO-2	RS.CO-2	RS.CO-2
		RS.CO-3	RS.CO-3	RS.CO-3	RS.CO-3	RS.CO-3
		RS.CO-4	RS.CO-4	RS.CO-4	RS.CO-4	RS.CO-4
		RS.CO-5	RS.CO-5	RS.CO-5	RS.CO-5	RS.CO-5
	Analysis	RS.AN-1	RS.AN-1	RS.AN-1	RS.AN-1	RS.AN-1
		RS.AN-2	RS.AN-2	RS.AN-2	RS.AN-2	RS.AN-2
		RS.AN-3	RS.AN-3	RS.AN-3	RS.AN-3	RS.AN-3
		RS.AN-4	RS.AN-4	RS.AN-4	RS.AN-4	RS.AN-4
		RS.AN-5	RS.AN-5	RS.AN-5	RS.AN-5	RS.AN-5
	Mitigation	RS.MI-1	RS.MI-1	RS.MI-1	RS.MI-1	RS.MI-1
		RS.MI-2	RS.MI-2	RS.MI-2	RS.MI-2	RS.MI-2
		RS.MI-3	RS.MI-3	RS.MI-3	RS.MI-3	RS.MI-3
	Improvements	RS.IM-1	RS.IM-1	RS.IM-1	RS.IM-1	RS.IM-1
		RS.IM-2	RS.IM-2	RS.IM-2	RS.IM-2	RS.IM-2

Function and Category Unique Identifiers

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
PR	Protect	PR.AC	Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

Table 6 *RECOVER Business Mission Objectives*

		Maintain Human Safety	Maintain Environmental Safety	Maintain Quality of Product	Maintain Production Goals	Maintain Trade Secrets
Category		Subcategories				
RC	Recovery Planning	RC.RP-1	RC.RP-1	RC.RP-1	RC.RP-1	RC.RP-1
	Improvements	RC.IM-1	RC.IM-1	RC.IM-1	RC.IM-1	RC.IM-1
		RC.IM-2	RC.IM-2	RC.IM-2	RC.IM-2	RC.IM-2
	Communications	RC.CO-1	RC.CO-1	RC.CO-1	RC.CO-1	RC.CO-1
		RC.CO-2	RC.CO-2	RC.CO-2	RC.CO-2	RC.CO-2
		RC.CO-3	RC.CO-3	RC.CO-3	RC.CO-3	RC.CO-3

MANUFACTURING SYSTEM CATEGORIZATION AND RISK MANAGEMENT

Oltre agli obiettivi per l'allineamento di un insieme di controlli di sicurezza a supporto degli obiettivi aziendali critici, il Profilo di Produzione è anche strutturato in 3 livelli d'impatto basati sulla categorizzazione delle informazioni e dei processi all'interno del sistema di produzione.

Questo capitolo è composto da 3 passi:

1. CATEGORIZATION PROCESS
2. PROFILE'S HIERARCHICAL SUPPORTING STRUCTURE
3. RISK MANAGEMENT

CATEGORIZATION PROCESS

*È il primo passo del NIST Risk Management Framework (RMF) e fornisce alle organizzazioni informazioni per supportare la personalizzazione dell'implementazione del controllo della sicurezza informatica. Come definito dal NIST Federal Information Processing Standard (FIPS) 199, il processo di categorizzazione si basa su 3 livelli d'impatto: **BASSO**, **MODERATO** o **ALTO**.*

1. BASSO: *se ci si può aspettare che la perdita di integrità, disponibilità o riservatezza abbia un effetto negativo limitato sulle operazioni di produzione, sui prodotti fabbricati, sulle risorse, sull'immagine del marchio, sulle finanze, sul personale, sul pubblico in generale o sull'ambiente.*

2. **MODERATO:** *se ci si può aspettare che la perdita di integrità, disponibilità o riservatezza abbia un grave effetto negativo sulle operazioni di produzione, sui prodotti fabbricati, sulle risorse, sull'immagine del marchio, sulle finanze, sul personale, sul pubblico in generale o sull'ambiente.*

3. **ALTO:** *se ci si può aspettare che la perdita di integrità, disponibilità o riservatezza abbia un effetto negativo grave o catastrofico sulle operazioni di produzione, sui prodotti fabbricati, sulle risorse, sull'immagine del marchio, sulle finanze, sul personale, sul pubblico in generale o sull'ambiente*

Le tabelle seguenti forniscono esempi di motivazioni basate sulla missione per la selezione della categorizzazione di sicurezza del sistema di produzione

Table 7 Manufacturing System Impact Levels [3]

Impact Category	Low Impact	Moderate Impact	High Impact
Injury	Cuts, bruises requiring first aid	Requires hospitalization	Loss of life or limb
Financial Loss ($)	Tens of thousands	Hundreds of thousands	Millions
Environmental Release	Temporary damage	Lasting damage	Permanent damage, off-site damage
Interruption of Production	Temporary reductions without impacting quarterly production	Temporary reductions requiring additional shifts or overtime to meet quarterly production	Significant reduction and impact to meet quarterly production
Public Image	Temporary damage	Lasting damage	Permanent damage

Table 8 Manufacturing System Impact Levels Based on Product Produced and Industry Concerns [3]

Category	Low Impact	Moderate Impact	High Impact
Product Produced	Non-hazardous materials or products Non-ingested consumer products	Some hazardous products or steps during production High amount of proprietary information	Critical infrastructure Hazardous materials Ingested products
Industry Examples	Plastic injection molding Warehousing	Automotive metal stamping Pulp and paper Semiconductors Automotive production	Utilities Petrochemical Food and beverage Pharmaceutical

Un **LIMITATO** *effetto negativo significa che, ad esempio, la perdita di integrità, disponibilità o riservatezza potrebbe:*

- *causare un degrado della capacità di missione in una misura e durata tale che il sistema possa svolgere le sue funzioni primarie, ma l'efficacia delle funzioni è notevolmente ridotta;*
- *comportare danni minori alle attività operative riparabili senza ulteriori interruzioni delle operazioni;*
- *comportare minori perdite finanziarie;*
- *provocare danni minori a persone che richiedono solo il primo soccorso di base.*

Un **GRAVE** *effetto significa che, ad esempio, la perdita di integrità, disponibilità o riservatezza potrebbe:*

- *causare un significativo degrado della capacità di missione in una misura e durata tale che il sistema può svolgere le sue funzioni primarie, ma l'efficacia delle funzioni è significativamente ridotta;*
- *provocare danni significativi alle risorse operative riparabili (o sostituibili) con un impatto limitato sulle capacità operative;*
- *comportare una perdita finanziaria significativa;*
- *provocare danni significativi a persone che necessitano di ricovero in ospedale, ma non comportano la morte o lesioni gravi potenzialmente letali.*

Un **CATASTROFICO** *effetto significa che, ad esempio, la perdita di integrità, disponibilità o riservatezza potrebbe:*

- *causare un grave degrado o perdita della capacità della missione in una misura e durata tale che il sistema non è in grado di svolgere una o più delle sue funzioni primarie;*

- *provocare gravi danni alle risorse operative che richiedono molto tempo per la riparazione o la sostituzione, con conseguente prolungamento dei tempi di fermo;*
- *comportare gravi perdite finanziarie;*
- *provocare danni gravi o catastrofici a persone che comportano la morte o lesioni gravi potenzialmente letali.*

PROFILE'S HIERARCHICAL SUPPORTING STRUCTURE

La guida al profilo è scalabile e supporta l'intensificazione delle protezioni di sicurezza dove necessario, mantenendo una linea di base convenzionale.

Ogni livello di impatto superiore si basa sulla linea di base a partire dalla designazione Basso.

Salvo diversa indicazione, i livelli Moderato e Alto ciascuno migliorano tutte le disposizioni dei livelli sottostanti.

- ✓ *Una classificazione **moderata** include tutte le implementazioni di protezione moderata e bassa*
- ✓ *Una classificazione **alta** include tutte le implementazioni di sicurezza **alta, moderata e bassa***

Ciascun livello di impatto è posizionato come piattaforma per supportare l'implementazione o categorizzazione del livello di impatto superiore successivo.

La sezione 7 fornisce il linguaggio della sottocategoria CSF per ogni livello di impatto personalizzato per il dominio di produzione.

7. Manufacturing Profile Subcategory Guidance

Function	Category	Subcategory	Manufacturing Profile Guidance	Reference
IDENTIFY	Asset Management (ID.AM)	ID.AM-1	**Low Impact**	
			Document an inventory of manufacturing system components that reflects the current system. Manufacturing system components include for example PLCs, sensors, actuators, robots, machine tools, firmware, network switches, routers, power supplies, and other networked components or devices. System component inventory is reviewed and updated as defined by the organization. Information deemed necessary for effective accountability of manufacturing system components includes, for example, hardware inventory specifications, component owners, networked components or devices, machine names and network addresses. Inventory specifications include, for example, manufacturer, device type, model, serial number, and physical location.	ISA/IEC 62443-2-1:2009 4.2.3.4 ISA/IEC 62443-3-3:2013 SR 7.8 CM-8
			Moderate Impact	
			Identify individuals who are both responsible and accountable for administering manufacturing system components.	CM-8 (1)(3)(5)
			High Impact	
			Identify mechanisms for detecting the presence of unauthorized hardware and firmware components within the manufacturing system. Where safe and feasible, these mechanisms should be automated.	CM-8 (2)(4)
		ID.AM-2	**Low Impact**	
			Document an inventory of manufacturing system software and firmware components that reflects the current system. Manufacturing system software components include for example software license information, software version numbers, Human Machine Interface (HMI) and other ICS component applications, software, operating systems. System software inventory is reviewed and updated as defined by the organization.	ISA/IEC 62443-2-1:2009 4.2.3.4 ISA/IEC 62443-3-3:2013 SR 7.8 CM-8
			Moderate Impact	
			Identify individuals who are both responsible and accountable for administering manufacturing system software.	CM-8 (1)(3)(5)
			High Impact	
			Identify mechanisms for detecting the presence of unauthorized software within the manufacturing system. Where safe and feasible, these mechanisms should be automated.	CM-8 (2)(4)

PARTE VIII: IOT: CIBERSICUREZZA E RISCHI PER LA PRIVACY

[Rif.: 1) NIST IR 8228; 2) CSDE - The C2 Consensus on IoT Device Security Baseline Capabilities (Council to Secure the Digital Economy); 3) NIST IR 8259]

36. FUNZIONALITÀ DEI DISPOSITIVI IOT

Ogni dispositivo IoT offre funzionalità o funzioni che può essere usato da solo o in combinazione con altri dispositivi IoT e non IoT per raggiungere uno o più obiettivi.

Le capacità del trasduttore interagiscono con il mondo fisico e fungono da vantaggio tra ambienti digitali e fisici. Le funzionalità del trasduttore consentono ai dispositivi di elaborazione di interagire direttamente con le entità fisiche di interesse.

Ogni dispositivo IoT ha almeno una capacità di trasduttore.

I due tipi di capacità del trasduttore sono:

1) RILEVAMENTO*: la capacità di fornire un'osservazione di un aspetto del mondo fisico sotto forma di dati di misurazione.*

   Alcuni esempi sono la misurazione della temperatura, l'imaging radiografico, il rilevamento ottico e il rilevamento audio;

2) ATTUANTE*: la capacità di cambiare qualcosa nel mondo fisico.*

   Esempi di capacità di azionamento includono bobine di riscaldamento, erogazione di scosse elettriche cardiache, serrature elettroniche delle porte, funzionamento di veicoli aerei senza equipaggio, servomotori e bracci robotici.

La funzionalità dell'interfaccia è abilitare le interazioni del dispositivo (ad esempio, le comunicazioni da dispositivo a dispositivo, comunicazioni da uomo a dispositivo). I tipi di funzionalità dell'interfaccia sono:

1) **INTERFACCIA APPLICATIVA***: la possibilità per altri dispositivi di elaborazione di comunicare con un dispositivo IoT tramite un'applicazione per dispositivi IoT. Un esempio di funzionalità dell'interfaccia dell'applicazione è l'API (Application Programming Interface);*

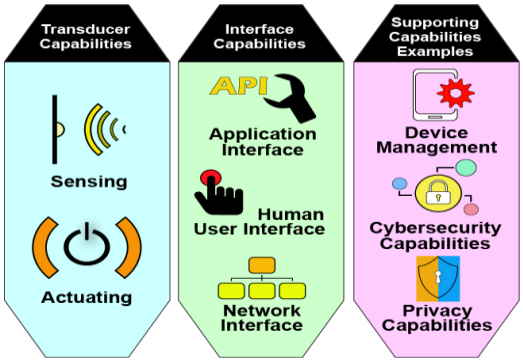
2) **INTERFACCIA UTENTE UMANA***: la possibilità di comunicare direttamente tra un dispositivo IoT e le persone. Esempi di funzionalità dell'interfaccia utente includono touch screen, dispositivi tattili, microfoni, fotocamere e altoparlanti;*

3) **INTERFACCIA DI RETE***: la possibilità d'interfacciarsi con una rete di comunicazione allo scopo di comunicare dati da o verso un dispositivo IoT, in altre parole, di utilizzare una rete di comunicazione. Una funzionalità di interfaccia di rete include sia ha che sw (ad esempio, una scheda o chip di interfaccia di rete e l'implementazione sw del protocollo di rete che utilizza la scheda o il chip). Esempi di funzionalità dell'interfaccia di rete includono Ethernet, Wi-Fi, Bluetooth, Long-Term Evolution (LTE) ed ogni dispositivo IoT ha almeno una funzionalità d'interfaccia di rete abilitata e può avere più di un dispositivo.*

Le funzionalità di supporto forniscono funzionalità che supportano le altre funzionalità IoT.

Esempi sono la gestione dei dispositivi, la sicurezza informatica e le funzionalità di privacy.

Questa figura riepiloga queste funzionalità del dispositivo IoT



37. CONSIDERAZIONI SULLA SICUREZZA E SUI RISCHI

Il rischio di sicurezza informatica e il rischio per la privacy sono correlati ma concetti distinti.

*Il Rischio è definito dal NIST SP 800-37 come "*una misura in cui un'entità è minacciata da una circostanza o evento potenziale, e in genere è una funzione di:

1. l'impatto negativo, o l'entità del danno, che si presenterebbe se si verifica la circostanza o l'evento;
2. la probabilità di insorgenza."

La sicurezza informatica, il rischio riguarda le minacce: *lo sfruttamento delle vulnerabilità da parte degli attori delle minacce per compromettere la riservatezza, l'integrità o la disponibilità di dispositivi o dati.*

La privacy, il rischio riguarda azioni sui dati: *operazioni che elaborano informazioni personali (PII) durante il ciclo di vita delle informazioni per soddisfare le esigenze di missione o di business di un'organizzazione o di un'elaborazione di informazioni personali "autorizzate" e, come effetto collaterale, causano agli individui di sperimentare alcuni tipi di problemi.*

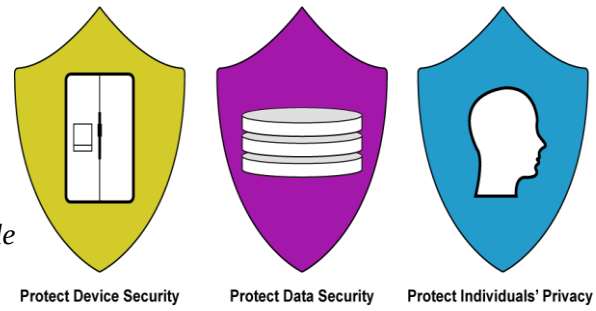
I rischi per la privacy e la sicurezza informatica si sovrappongono alle preoccupazioni relative alla sicurezza informatica delle informazioni personali, ma esistono anche problemi di privacy senza implicazioni per la sicurezza informatica e problemi di sicurezza informatica senza implicazioni per la privacy.

TRE OBIETTIVI DI ATTENUAZIONE DEI RISCHI DI ALTO LIVELLO

La sicurezza informatica e i rischi per la privacy per i dispositivi IoT possono essere considerati in termini di tre obiettivi di attenuazione dei rischi di alto livello:

1) **Proteggere la sicurezza del dispositivo**. *Impedire che un dispositivo venga utilizzato per condurre attacchi, inclusa la partecipazione a DDoS (Distributed Denial of Service) contro altre organizzazioni, intercettare il traffico di rete o compromettere altri dispositivi sullo stesso segmento di rete.*
2) **Proteggere la sicurezza dei dati.** *Proteggere la riservatezza, l'integrità e/o la disponibilità dei dati (comprese le informazioni personali) raccolti, archiviati, elaborati o trasmessi da o verso il dispositivo IoT.*
3) **Proteggere la privacy delle persone.** *Proteggere la privacy degli individui influenzata dall'elaborazione delle informazioni personali oltre i rischi gestiti attraverso la protezione della sicurezza dei dispositivi e dei dati.*

Obiettivi di mitigazione del rischio



PROTEGGERE LA SICUREZZA DEL DISPOSITIVO

Aree di mitigazione dei rischi per l'obiettivo 1, proteggere la sicurezza del dispositivo:

1. **Gestione delle risorse:** *mantenere un inventario aggiornato di tutti i dispositivi IoT e delle relative caratteristiche durante il ciclo di vita dei dispositivi al fine di utilizzare tali informazioni per scopi di sicurezza informatica e gestione dei rischi per la privacy;*

2. **Gestione delle vulnerabilità:** *identificare ed eliminare le vulnerabilità note nel software e nel firmware dei dispositivi IoT al fine di ridurre la probabilità e la facilità di sfruttamento e compromissione;*

3. **Gestione degli accessi**: *impedisce l'accesso fisico e logico non autorizzato e improprio, l'utilizzo e l'amministrazione dei dispositivi IoT da parte di persone, processi e altri dispositivi informatici;*

4. **Rilevamento degli incidenti di sicurezza del dispositivo**: *monitorare e analizzare l'attività del dispositivo IoT per individuare eventuali tracce di incidenti relative alla sicurezza del dispositivo.*

PROTEGGERE LA SICUREZZA DEI DATI

Aree di mitigazione dei rischi per l'obiettivo 2, proteggere la sicurezza dei dati:

1. **Protezione dei dati:** *impedisce l'accesso e la manomissione ai dati inattivi o in transito che potrebbero esporre informazioni riservate o consentire la manipolazione e l'interruzione delle operazioni dei dispositivi IoT;*

2. **Rilevamento degli incidenti di sicurezza dei dati**: *monitorare e analizzare l'attività del dispositivo IoT per individuare eventuali tracce di incidenti relativi alla sicurezza dei dati.*

PROTEGGERE LA PRIVACY DEGLI INDIVIDUI

Aree di mitigazione dei rischi per l'obiettivo 3, proteggere la privacy degli individui:

1. **Information Flow Management** (Gestione del flusso di informazioni): *mantenere una mappatura aggiornata e accurata del ciclo di vita delle informazioni, inclusi il tipo di azione dei dati, gli elementi di PII elaborati dall'azione sui dati, la parte che esegue l'elaborazione ed eventuali ulteriori fattori contestuali pertinenti l'elaborazione da utilizzare per scopi di gestione del rischio.*

2. **Gestione autorizzazioni di elaborazione PII**: *Gestire le autorizzazioni delle PII per impedire elaborazioni non autorizzate.*

3. **Processo decisionale informato**: *consente agli utenti di: 1) partecipare al processo decisionale; 2) comprendere gli effetti dell'elaborazione delle PII e delle interazioni con il dispositivo; 3) risolvere i problemi.*

4. **Gestione dei dati dissociati**: *identificare l'elaborazione delle PII autorizzate e determinare come le PII possano essere ridotte al minimo o dissociate da individui e dispositivi IoT.*

5. **Rilevamento violazione della privacy:** *monitorare e analizzare l'attività del dispositivo IoT per individuare tracce di violazioni che coinvolgano la privacy.*

Nota: NIST (IR 8228) propone 49 controlli raggruppati in 25 aspettative

AREE DI MITIGAZIONE DEL RISCHIO SUPPORTATE DA OGNI DISPOSITIVO

Aree di mitigazione del rischio supportate da ogni dispositivo di base capacità di sicurezza informatica:

1. **Asset Management**: *mantenere un inventario attuale e accurato di tutti i dispositivi IoT e delle loro caratteristiche pertinenti durante i cicli di vita dei dispositivi al fine di utilizzare tali informazioni per la Gestione del rischio. Essere in grado di distinguere ogni dispositivo IoT da tutti gli altri è necessario per le altre aree comuni di mitigazione del rischio: Gestione delle vulnerabilità, Gestione degli accessi, Protezione dei dati e Rilevamento degli incidenti.*

2. **Vulnerability Management**: *identificare e mitigare le vulnerabilità note nel software del dispositivo IoT durante i cicli di vita dei dispositivi, al fine di ridurre la probabilità e la facilità di sfruttamento e compromissione. Le vulnerabilità possono essere eliminate installando aggiornamenti (ad es. Patch) e modificando le impostazioni di configurazione, inoltre possono anche correggere i problemi operativi del dispositivo IoT.*

3. **Access Management**: *impedisce l'accesso fisico e logico non autorizzato e improprio a processi e altri dispositivi informatici. Limitare l'accesso alle interfacce riduce la superficie di attacco del dispositivo, offrendo agli aggressori meno opportunità di comprometterlo.*

4. **Data Protection:** *impedire l'accesso e la manomissione dei dati inattivi o in transito che potrebbero sia esporre informazioni riservate sia consentire la manipolazione o l'interruzione delle operazioni dei dispositivi IoT durante il loro ciclo di vita;*

5. **Incident Detection:** *monitora e analizza l'attività del dispositivo IoT per rilevare eventuali incidenti che coinvolgano la sicurezza dei dispositivi e dei dati durante l'intero ciclo di vita dei dispositivi. Queste tracce possono essere utili per studiare compromessi e risolvere alcuni problemi operativi.*

Aree di mitigazione rischio supportate da ogni dispositivo

38. IDENTIFICATORI

Un dispositivo IoT può avere un identificatore o un numero di identificatori diversi che possono essere stabiliti dal produttore o aggiunti prima della distribuzione.

Gli identificatori possono essere utilizzati come parte del processo di onboarding del dispositivo o come parte della gestione in corso del dispositivo/dell'applicazione.

Ogni identificatore deve essere univoco in uno spazio dei nomi per consentirne il riferimento senza ambiguità.

Esempi:

- ***Identificatori integrati specifici** del dispositivo associati all'hardware fisico di un dispositivo, come gli indirizzi MAC di livello 2 utilizzati per identificare il dispositivo in una rete di accesso o l'identità internazionale delle apparecchiature mobili (IMEI – International Mobile Equipment Identity) o l'identificatore delle apparecchiature mobili (MEID – Mobile Equipment Identifier) di un cellulare dispositivo.*
- ***Identificatori basati su abbonamento** che possono essere utilizzati per consentire l'accesso del dispositivo ai servizi di rete basati su WAN. Questi includono l'identità mobile internazionale dell'interessato mobile o l'IMSI (International Mobile Subscriber Identity) utilizzati per l'accesso alla rete cellulare.*
- ***Identificatori di applicazioni IoT** che consentono a un'applicazione IoT di identificare e accedere ai dispositivi per l'uso. Ogni applicazione IoT che utilizza un dispositivo IoT specifico può avere il proprio identificativo applicazione univoco.*
- ***Identificatori del sistema di gestione dei dispositivi IoT**, identificatori univoci separati per l'accesso di gestione ai dispositivi sotto il controllo o l'ambito del sistema di gestione.*
- ***Identificatori di tracciamento** delle risorse come codici di prodotto elettronici (EPC – Electronic Product Codes) e identificatori di tag (TID – Tag IDentifiers); questi sono utilizzati per ottenere informazioni di tracciabilità*
- ***Certificati attendibili**, che possono avere un "Nome univoco" diverso da tutto quanto sopra ma che dovrebbe essere correlato a un'identità nota.*

L'identificatore utilizza:

- ✓ *L'identità è la base per l'affidabilità.*
- ✓ *Ogni dispositivo dovrebbe essere in grado di generare e/o archiviare almeno un identificatore legato all'identità.*
- ✓ *L'identità del dispositivo è l'elemento fondamentale da cui dipende un'ampia gamma di controlli di sicurezza e gestibilità del dispositivo per la corretta funzionalità.*
- ✓ *La memorizzazione e l'utilizzo di ciascuno degli identificativi del dispositivo devono essere protetti in modo appropriato per tale identificatore.*

Esempio di come gli identificatori sono usati in Root of Trust

- ✓ *Root of Trust (RoT) è un componente che esegue una o più funzioni specifiche di sicurezza, quali misurazione, archiviazione, reportistica, verifica e/o aggiornamento.*

PARTE IX: RISCHI DEI CERTIFICATI TLS

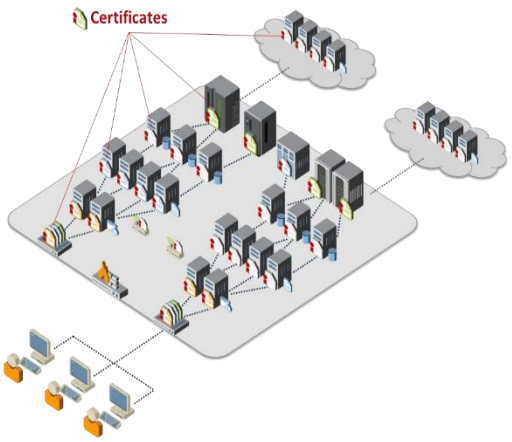
[Rif.: NIST SP 1800-16]

39. CERTIFICATI TLS

TLS è il protocollo di sicurezza utilizzato per autenticare e proteggere le comunicazioni Internet e delle reti interne per un ampio numero di altri protocolli, incluso Hypertext Transfer Protocol (http) per i server Web; LDAP (Lightweight Directory Access Protocol) per server di directory; e Simple Mail Transfer Protocol, Post Office Protocol e Internet Message Access Protocol per e-mail.

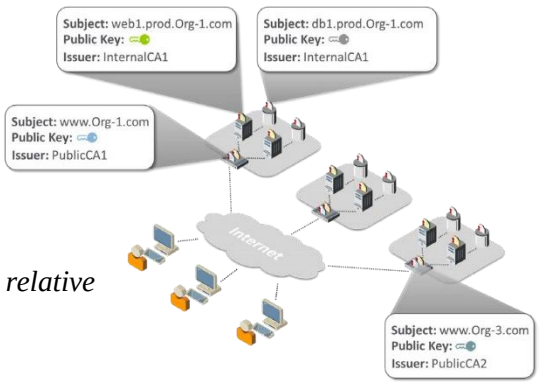
I certificati server TLS servono come identità di macchine che consentono ai client di autenticare i server tramite mezzi crittografici. Ad esempio, quando un cliente bancario si connette attraverso Internet a un sito Web di banking online, il browser del cliente (ovvero il client TLS) presenterà un messaggio di errore se il server non fornisce un certificato valido che corrisponde all'indirizzo inserito dall'utente browser.

Uso di certificati all'interno delle organizzazioni



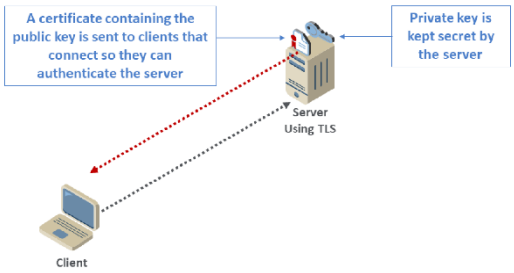
La maggior parte delle grandi aziende ha migliaia di certificati, ognuno dei quali identifica un server specifico nel proprio ambiente. (Nota: i browser Web svolgono il ruolo dei client sui server Web. In quanto tali, contengono funzionalità per stabilire automaticamente connessioni TLS per conto degli utenti, valutare i certificati ricevuti durante il processo di handshake TLS e presentare errori quando si verificano problemi di certificati imprevisti.)

Ogni certificato del server TLS contiene l'indirizzo del server che identifica (ad es. www.organization1.com) e una chiave crittografica, chiamata chiave pubblica, unica per il server e utilizzata dai client per l'autenticazione sicura del server.



Indirizzo del server, chiave pubblica e informazioni sull'emittente relative a quattro dei certificati server TLS dell'organizzazione

Come mostrato nella figura, ogni server possiede una chiave privata che corrisponde alla chiave pubblica nel certificato in modo che ciascun server possa dimostrare di essere il titolare del certificato.



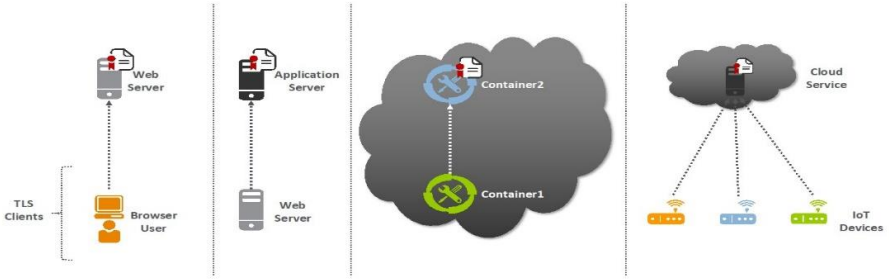
Mentre il certificato è condiviso con qualsiasi client che si connette al server, è fondamentale che la chiave privata sia protetta e segreta, quindi non può essere ottenuta da un utente malintenzionato e utilizzata per impersonare il server

Molte chiavi private utilizzate con TLS sono archiviate in file di testo normale sui server TLS. In alternativa, le chiavi private possono essere archiviate in file crittografati con una password; le password sono generalmente archiviate in file di configurazione in chiaro, quindi sono accessibili dal software del server TLS all'avvio.

Le chiavi private possono essere visualizzate e copiate dagli amministratori di sistema o attori malintenzionati.

Oltre agli utenti con browser che si collegano a server che dispongono di certificati server TLS, i processi automatizzati si collegano anche come client ai server TLS e devono fidarsi dei certificati server TLS. Esempi di processi automatizzati che fungono da client TLS includono un server Web che effettua richieste a un server delle applicazioni, un contenitore cloud che si collega a un altro o un dispositivo Internet of Things (IoT) che si collega a un servizio cloud.

La figura mostra il Browser e vari processi automatizzati (server Web, contenitori e dispositivi IoT) connettersi come client ai server TLS



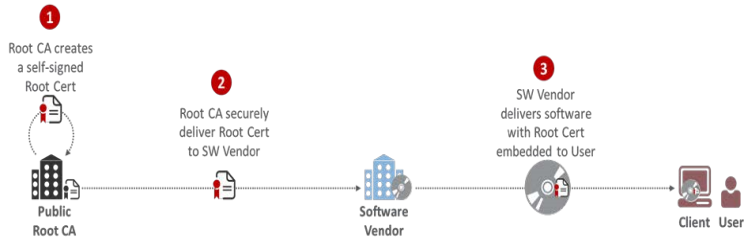
40. CERTIFICATION AUTHORITIES

I certificati del server TLS sono emessi da entità chiamate autorità di certificazione (CA).

Le autorità di certificazione firmano digitalmente i certificati in modo da poterne convalidare l'autenticità, per impedire agli aggressori di impersonare facilmente i server. I client (ad es. Browser, dispositivi, applicazioni, servizi) convalidano i certificati utilizzando un certificato della CA per verificare la firma. I client, come i browser, sono configurati per fidarsi di specifiche CA. Questo viene fatto installando sul client un certificato CA, comunemente chiamato ***Certificato Radice*** *(****Root Certificate****).*

Alcune CA prevedono che il loro certificato di root venga installato dai produttori di software nel loro software (ad es. Browser, applicazione o sistema operativo) in modo che i certificati emessi dalle CA siano ampiamente considerati affidabili. Queste CA siano comunemente chiamate "Root CA" pubbliche.

"Root CA" di CA pubblica come viene consegnato all'utente e installato



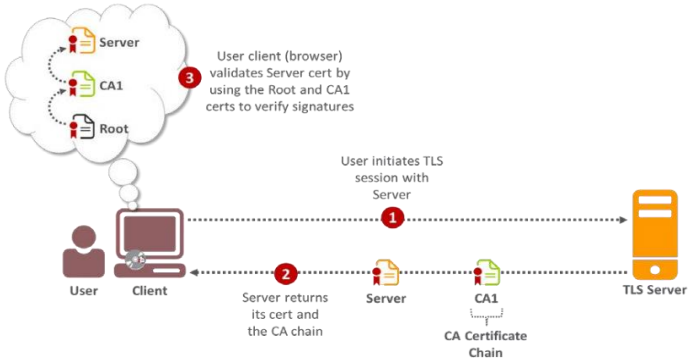
Per proteggerli dagli attacchi, le CA principali non sono generalmente connesse a Internet e non emettono direttamente i certificati del server TLS.

Le CA principali certificano altre CA, generalmente chiamate CA intermedie o emittenti, che rilasciano certificati server TLS.

La figura mostra una CA principale emettere un certificato a una CA intermedia/emittente, che rilascia certificati server TLS.

Come mostrato nella figura, quando un client, come un browser, si connette a un server TLS, il server restituirà il proprio certificato e il certificato per la CA che ha emesso il proprio certificato (chiamato catena di Certificati della CA).

*La figura mostra il momento della connessione al server, il client riceve sia il certificato TLS del server sia la sua catena di certificati CA (**CA Certificate Chain**).*



Esistono tre diversi tipi di certificati emessi da CA pubbliche (come specificato da CA/Browser Forum, che definisce gli standard per le CA pubbliche), ciascuno con un diverso livello di convalida richiesto dalla CA per confermare l'identità del richiedente e la sua autorità a ricevere un certificato per il dominio in questione:

1. **Domain Validated (DV)***: la CA convalida che il richiedente :*
   a. *sia il proprietario del dominio, verificando che il richiedente possa rispondere a un indirizzo e-mail associato al dominio;*
   b. *abbia il controllo operativo del sito Web all'indirizzo del dominio o sia in grado per apportare modifiche al record Domain Name System (DNS) per il dominio.*

2. **Organization Validated (OV)***: oltre ai controlli per i certificati DV, la CA effettua un'ulteriore verifica dell'organizzazione del richiedente.*

3. **Extended Validation (EV)***: i certificati EV sono sottoposti ai controlli più rigorosi, compresa la verifica dell'identità e dell'esistenza legale, fisica e operativa dell'entità che richiede il certificato, utilizzando registri ufficiali.*

41. PROCESSO DI RILASCIO DEL CERTIFICATO

RUOLI

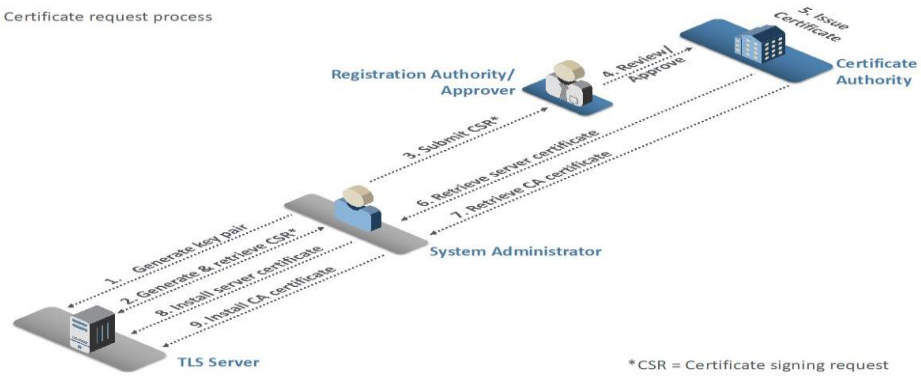
1) *AS (Amministratore di Sistema) per il server TLS utilizza le utilità sul server per generare una coppia di chiavi crittografiche (chiave pubblica e chiave privata).*
2) *AS inserisce l'indirizzo del server (ad es. www.organization1.com). Le utility creano una richiesta per un certificato, chiamata Richiesta di Firma del Certificato (Certificate Signing Request - CSR), che contiene l'indirizzo del server e la chiave pubblica. AS recupera una copia del CSR (che è contenuta in un file) dal server.*
3) *AS invia il CSR all'Autorità di Registrazione (Registration Authority - RA), che funge da revisore e approvatore della richiesta di certificato.*
4) *RA/Responsabile dell'approvazione esamina il CSR, esegue i controlli necessari per confermare la validità della richiesta e l'autorità del richiedente, quindi invia un'approvazione alla CA.*
5) *CA emette il certificato.*
6) *CA notifica all'AS che il certificato è pronto, tramite e-mail una copia del certificato o fornendo un collegamento dal quale può essere scaricato. AS recupera il certificato del server.*
7) *AS recupera la CA Certificate Chain dalla CA.*
8) *AS installa il certificato del server sul server.*
9) *AS installa la catena di certificati CA (Certificate Chain) sul server.*

La catena di certificati CA viene utilizzata dai client TLS per convalidare la firma sul certificato del server.

Quando un client si connette a un server TLS, il server restituisce il suo certificato e la catena di certificati CA, che può contenere uno o più certificati CA.

Il client inizia con uno dei certificati CA radice attendibili localmente e convalida successivamente le firme sui certificati nella catena di certificati CA fino a quando non raggiunge il certificato server.

AS deve annotare la data di scadenza nel certificato per assicurarsi che un nuovo certificato sia richiesto e installato prima della scadenza del certificato esistente.



42. RISCHI RELATIVI AL CERTIFICATO DEL SERVER TLS

Quando i certificati del server TLS non sono gestiti correttamente, le organizzazioni rischiano impatti negativi su entrate, clienti e reputazione.

Esistono quattro tipi principali di incidenti negativi derivanti dalla cattiva gestione dei certificati:

1) **INTERRUZIONI** *a importanti applicazioni aziendali, causate da certificati scaduti;*
2) **VIOLAZIONI** *della sicurezza derivanti dalla rappresentazione del server;*
3) **INTERRUZIONI O VIOLAZIONI** *della sicurezza risultanti da una mancanza di cripto-agilità;*
4) **MAGGIORE VULNERABILITÀ** *agli attacchi tramite minacce crittografate.*

NOTA*: mentre i certificati del server TLS consentono la riservatezza per le comunicazioni legittime, possono anche consentire agli aggressori di nascondere le loro attività dannose all'interno di connessioni TLS crittografate. Quando un certificato del server TLS è installato e abilitato su un server, tutti gli utenti che si connettono (inclusi gli aggressori) possono stabilire una connessione crittografata con il server.*

RISCHIO: OUTAGES CAUSED BY EXPIRED CERTIFICATES

Vari scenari che comportano la scadenza di un certificato mentre è ancora in uso, causando un'interruzione, tra cui:

- *AS (amministratore di sistema) dimentica il certificato;*
- *AS ignora le notifiche che il certificato scadrà presto;*
- *Non installa o aggiorna correttamente la catena di certificati CA;*
- *AS viene riassegnato e nessun altro riceve notifiche di scadenza;*
- *AS registra un nuovo certificato ma non lo installa nei server in tempo o lo installa in modo errato;*
- *L'applicazione si basa su più server con bilanciamento del carico e il certificato non viene aggiornato su tutti;*

Il certificato è installato su un sistema di backup, ma il certificato è scaduto prima che il sistema di backup fosse ripristinato.

La risoluzione dei problemi relativi a un incidente in cui un'applicazione non è disponibile a causa di un certificato scaduto può essere complessa e spesso richiede ore per scoprire l'origine del problema.

Se le persone che utilizzano il browser accedono al server su cui è distribuito un certificato scaduto, ciascuna di queste persone riceverà un messaggio di errore, chiarendo che la causa del problema è un certificato scaduto.

Se, d'altra parte, i client che si connettono al server con il certificato scaduto sono sistemi automatizzati (ad esempio, i client sono server Web e il server con il certificato scaduto è un server delle applicazioni), i server Web che agiscono come client interromperanno le operazioni quando incontrano il certificato scaduto.

Possono registrare un messaggio di errore, ma tale messaggio potrebbe non essere immediatamente scoperto nel file di registro, aumentando il tempo necessario per identificare la causa principale dell'interruzione e risolverlo.

Se i certificati distribuiti sui sistemi di backup non vengono aggiornati quando scadono, può verificarsi un'interruzione se le operazioni vengono spostate sui sistemi di backup.

RISCHIO: SERVER IMPERSONATION

Se le persone che utilizzano il browser accedono al server su cui è distribuito un certificato scaduto, ciascuna di queste persone riceverà un messaggio di errore, chiarendo che la causa del problema è un certificato scaduto.

Un utente malintenzionato può essere in grado di impersonare un server TLS legittimo (ad esempio un sito Web bancario) se l'attaccante è in grado di ottenere un certificato fraudolento contenente l'indirizzo del server e la chiave pubblica dell'autore dell'attacco ingannando un'autorità di certificazione attendibile nell'emettere il certificato a l'attaccante o compromettendo la CA e rilasciando il certificato.

Un client che si connette al server dell'attaccante accetterà il certificato perché il certificato contiene l'indirizzo al quale il client intendeva connettersi e perché il certificato è stato emesso da un'autorità di certificazione attendibile.

Poiché il certificato contiene la chiave pubblica dell'attaccante (e l'attaccante detiene anche la chiave privata corrispondente a questa chiave pubblica), l'attaccante può decrittografare le comunicazioni dal client (comprese le password destinate all'accesso al server legittimo).

In alternativa, se l'utente malintenzionato può accedere a una copia della chiave privata del server legittimo, l'utente malintenzionato può intercettare o impersonare quel server utilizzando il certificato del server legittimo.

Per eseguire correttamente questi attacchi, l'autore dell'attacco deve reindirizzare il traffico destinato al server legittimo verso un sistema su cui opera l'attaccante (ad esempio, utilizzando il Border Gate Protocol - BGP) o il compromesso DNS.

NOTA*: BGP viene utilizzato per comunicare percorsi ottimali tra i fornitori di servizi Internet su Internet. È possibile che un utente malintenzionato dirottino il traffico pubblicizzando falsamente che il percorso più veloce verso uno o più indirizzi di protocollo Internet [IP] avviene tramite sistemi l'attaccante sta funzionando, causando così il reindirizzamento del traffico attraverso i sistemi dell'attaccante. Il DNS fornisce la traduzione tra indirizzi leggibili dall'uomo [ad esempio www.company123.com] e indirizzi IP. Se un attaccante può compromettere l'account DNS di un'organizzazione, allora l'utente malintenzionato può modificare l'indirizzo IP a cui verrà inviato il traffico destinato a tale organizzazione.*

La maggior parte delle chiavi private utilizzate sui server TLS sono archiviate in file.

Le chiavi private sono gestite e gestite direttamente dagli amministratori di sistema, che possono effettuare copie delle chiavi private.

Molti server TLS sono raggruppati (per il bilanciamento del carico); in molti casi, lo stesso certificato del server TLS e la chiave privata saranno copiati su ciascun server nel cluster.

La gestione manuale e la copia delle chiavi private aumentano significativamente la possibilità di un compromesso della chiave e le conseguenze di riservatezza e integrità dei dati del compromesso della chiave (incluso ma non limitato alla rappresentazione del server).

RISCHIO: LACK OF CRYPTO-AGILITY (VELOCITÀ DI AGGIORNAMENTO)

Esistono diversi tipi di incidenti che hanno richiesto alle organizzazioni di sostituire un gran numero di certificati TLS e chiavi private, tra cui:

1) COMPROMISSIONE DELLA CA*: se una CA viene violata da un utente malintenzionato, l'utente malintenzionato può far sì che la CA emetta certificati fraudolenti.*
2) ALGORITMO VULNERABILE*: gli algoritmi crittografici sono costantemente valutati per le vulnerabilità, dalle parti con intenti sia positivi che negativi. Quando viene trovato un algoritmo vulnerabile (ad es. Secure Hash Algorithm 1 (SHA-1) per la generazione della firma), i certificati del server TLS che dipendono dall'algoritmo devono essere sostituiti.*
3) BUG DELLA LIBRERIA CRITTOGRAFICA*: poiché le operazioni crittografiche sono piuttosto complesse, alcuni gruppi si sono specializzati nello sviluppo di librerie crittografiche utilizzate dai server TLS e da altri sistemi. Se viene rilevato un bug con le funzioni di generazione delle chiavi di una libreria crittografica, è necessario sostituire tutte le chiavi generate dall'introduzione del bug.*

RISCHIO: ENCRYPTED THREATS

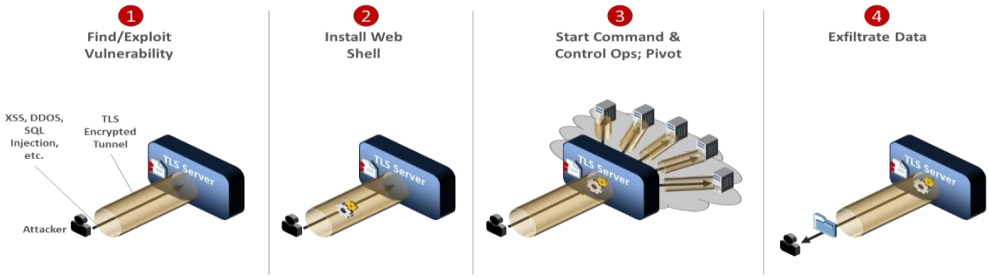
I certificati del server TLS consentono la riservatezza per le comunicazioni legittime, possono anche consentire agli aggressori di nascondere le loro attività dannose all'interno di connessioni TLS crittografate.

Quando un certificato del server TLS è installato e abilitato su un server, tutti gli utenti che si connettono (inclusi gli aggressori) possono stabilire una connessione crittografata al server.

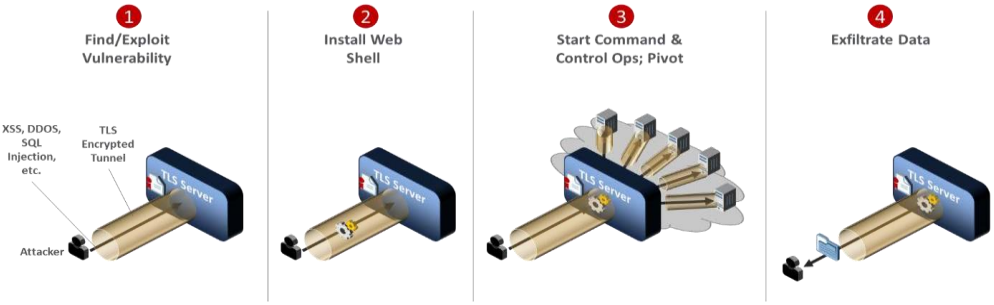
Un utente malintenzionato che stabilisce una connessione crittografata può quindi iniziare a sondare il server alla ricerca di vulnerabilità all'interno di tale connessione crittografata.

I passaggi, mostrati nella figura e dettagliati di seguito, descrivono come un attaccante può sfruttare le connessioni crittografate nei suoi attacchi.

La figura mostra come un attaccante sfrutta le connessioni crittografate per nascondere gli attacchi



1) *L'attaccante inizia connettendosi a un server e stabilisce una sessione TLS crittografata. All'interno di quella sessione crittografata, il malintenzionato può rilevare le vulnerabilità presenti sul server e sul suo software.*
2) *Se l'attaccante scopre una vulnerabilità e aumenta sufficientemente i propri privilegi, l'attaccante può caricare sul server malware, generalmente chiamato "Web shell".*
3) *Con questo "Web shell" caricato, il malintenzionato può inviare comandi tramite connessioni TLS (ovvero connessioni crittografate facilitate dal certificato del server). L'aggressore può quindi lavorare per ruotare su altri sistemi sondando le vulnerabilità nei server accessibili dal sistema compromesso. Il maggiore utilizzo della crittografia consente a un utente malintenzionato di non essere rilevato.*
4) *Una volta che l'attaccante ha raggiunto con successo i dati desiderati è in grado di utilizzare il "Web shell" per estrarli. Poiché l'attaccante sta stabilendo connessioni TLS utilizzando il certificato del server per connettersi al Web shell, tutti i dati estratti vengono crittografati durante il trasporto.*



Le organizzazioni che si preoccupano di questi rischi vogliono l'opzione di decrittografare il traffico TLS interno in modo che possa essere ispezionato.

L'ispezione del traffico TLS interno può essere utilizzata non solo per il rilevamento di intrusioni e malware ma anche per la risoluzione dei problemi, il rilevamento di frodi, la medicina legale e il monitoraggio delle prestazioni.

Eseguire l'ispezione comporta importanti compromessi tra la sicurezza del traffico e la visibilità del traffico stesso

Alcuni esempi per ottenere visibilità nelle comunicazioni crittografate:

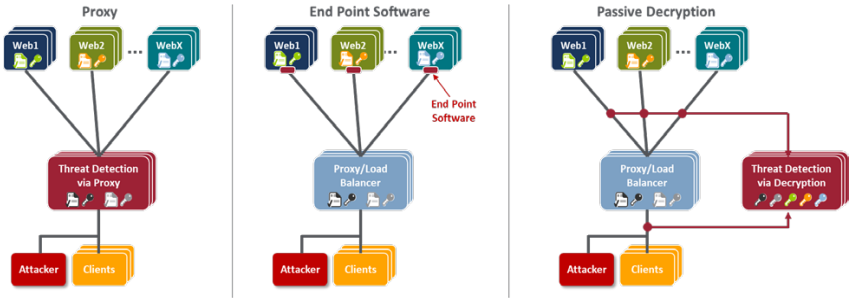
- *collocare un sistema di rilevamento delle minacce che funge da proxy inverso di fronte ai server;*
- *installare software end point su ciascun server per monitorare le comunicazioni.*

L'uso di proxy di rilevamento delle minacce è l'ideale a livello di organizzazioni per monitorare le comunicazioni Internet in entrata per gli attacchi.

Il proxy di rilevamento delle minacce:

- *è connesso in linea;*
- *richiede che tutto il traffico in entrata lo attraversi prima di passare al dispositivo successivo;*
- *termina la connessione TLS;*
- *decodifica ed esamina il traffico in entrata; se si ritiene che il traffico sia dannoso, il proxy lo rilascia.*

Metodi per ottenere la visibilità nelle comunicazioni crittografate



Ulteriori considerazioni sul proxy:

- *sta alla fine di tutte le connessioni TLS, per cui deve disporre di un certificato per ciascun server a cui i client stanno tentando di connettersi;*
- *decodifica ed esamina il traffico; stabilisce una sessione TLS con il server appropriato; invia il traffico a quel server in una sessione TLS crittografata;*
- *molte applicazioni aziendali includono più livelli di server e servizi (ad esempio, bilanciamento del carico, server Web, server applicazioni, database, servizi di identità) che comunicano tra loro internamente tramite sessioni TLS crittografate, rendendo poco pratico il posizionamento di proxy di rilevamento delle minacce tra tutti i sistemi su reti interne;*
- *il software dell'end point può essere installato su ciascun server per monitorare le comunicazioni;*
- *la decrittazione passiva e fuori banda e l'analisi delle minacce sono eseguite utilizzando dispositivi che decodificano le comunicazioni crittografate con TLS ma che non sono alla fine delle connessioni TLS;*
- *la connessione TLS viene stabilita tra il client e il server; il dispositivo di decrittografia passiva ascolta il traffico TLS senza influenzarlo e lo decodifica;*
- *l'analisi delle minacce viene eseguita dal dispositivo di decrittografia passiva o tramite altri sistemi a cui viene inoltrato il traffico decrittografato;*
- *i dispositivi di decodifica passiva incentrati sulla sicurezza possono rilevare il traffico dannoso che è stato inviato su connessioni TLS, ma questi dispositivi non reagiscono in tempo reale per bloccare questo traffico;*
- *la decrittazione passiva non richiede un cambiamento nell'architettura di rete o il caricamento di software aggiuntivo sui server TLS;*
- *la decrittografia passiva rappresenta una sfida per la gestione dei certificati del server TLS, poiché le chiavi private devono essere copiate nei dispositivi di decrittografia da ciascun server TLS le cui comunicazioni saranno monitorate;*
- *il trasferimento delle chiavi private deve essere effettuato in modo sicuro per evitare un compromesso delle chiavi e rapidamente per evitare punti ciechi nel monitoraggio degli attacchi; l'automazione può essere di grande aiuto nel trasferimento sicuro delle chiavi private dai server TLS al dispositivo di decrittografia e nel mantenere le chiavi aggiornate quando i certificati vengono sostituiti.*

NOTA:

1. *per maggiori dettagli sulle caratteristiche delle chiavi si consiglia il documento n° 39*
2. *per approfondimenti sui controlli di sicurezza si consiglia la "Table 1 Mapping the Recommended Best Practices for TLS Server Certificate Management to the Cybersecurity Framework" nella "Appendix C - Mapping to the Cybersecurity Framework" nel documento n° 38*

PARTE X: RISCHI DELLA INFRASTRUTTURA DELLA MEMORIA/STORAGE

[Rif.: NIST SP 800-209]

ARCHIVIAZIONE, ELABORAZIONE E RETI COSTITUISCONO I 3 ELEMENTI FONDAMENTALI DELL'INFRASTRUTTURA INFORMATICA

43. ELENCO DELLE AREE DI ATTENZIONE ALLA SICUREZZA

1. *SICUREZZA FISICA;*
2. *AUTENTICAZIONE E AUTORIZZAZIONE;*
3. *GESTIONE DELLE MODIFICHE;*
4. *CONTROLLO DELLA CONFIGURAZIONE;*
5. *RISPOSTA AGLI INCIDENTI E RIPRISTINO.*

All'interno di queste aree, sono coperti anche i controlli di sicurezza specifici per le tecnologie di archiviazione, come NAS (Network-Attached Storage) e Storage Area Network (SAN).

44. ELENCO PARTICOLARI SPECIFICHE DI SICUREZZA

1. *DATA PROTECTION;*
2. *ISOLATION;*
3. *RESTORATION ASSURANCE;*
4. *ENCRYPTION.*

45 TIPOLOGIE DI ARCHIVIAZIONE

STORIA DELL'ARCHITETTURA DEL SISTEMA DI ARCHIVIAZIONE

La prima forma di infrastruttura di archiviazione digitale è l'archiviazione diretta (DAS) in cui l'elemento di archiviazione o il dispositivo (ad esempio nastro, disco rigido) è direttamente collegato al server host senza alcuna rete interposta;

La seconda è quella in cui le risorse sono raggruppate in modo intelligente, situate attraverso la rete, accessibili tramite protocolli di rete e accessibili da più host o server. Quest'ultimo tipo è l'unico modo per supportare le esigenze di accesso ai dati dei sistemi distribuiti, poiché i componenti dell'applicazione che devono condividere i dati si trovano in nodi diversi di una rete. In questa fase dell'evoluzione, ***l'infrastruttura di archiviazione ha assunto 2 forme, a seconda del tipo di protocollo di rete:***

1) *la risorsa è semplicemente un* ***nodo in una rete*** *che utilizza la comune tecnologia di rete (ad esempio LAN, WAN); esempio l'archiviazione di rete (NAS), che fornisce l'accesso file level a client eterogenei attraverso una rete utilizzando protocolli di livello superiore, come NFS o SMB/CIFS.*
2) *tutte le risorse di archiviazione (ad esempio Fibre Channel)* ***comunicano con una rete dedicata****; esempio la rete di archiviazione (SAN) che utilizza una rete specializzata ad alta velocità (ad esempio Fibre-Channel) che fornisce accesso a livello di blocco allo storage.*

L'infrastruttura di archiviazione si è evoluta nel corso degli anni per diventare ricca di funzionalità in settori quali prestazioni ed efficienza grazie agli sviluppi su due aree:

- ✓ AREA 1: *supporti di memorizzazione, che presenta unità a stato solido (SSD) con capacità elevata e funzionalità di efficienza della memoria (ad es. deduplicazione, compressione, ecc.) rispetto alle unità a disco rigido (HDD);*
- ✓ AREA 2: *architettura del sistema di archiviazione utilizzando concetti come la virtualizzazione dello storage (complessità gestionale e fornitura garanzie di sicurezza).*

HCI

Un HCI combina: (1) storage, (2) computing e (3) networking in una singola unità hardware o chassis e ha incorporato uno strato di astrazione per la gestione di tutti e tre i componenti. Include:

a) console software comune o strumento di gestione per la gestione di tutti e tre i componenti;

b) hypervisor per il calcolo virtualizzato;

c) archiviazione definita dal software;

d) reti virtualizzate raggruppate insieme per funzionare su standard;

e) hardware standard.

I sistemi di archiviazione, host e switch di rete integrati sono progettati per essere gestiti come un unico sistema in tutte le istanze di un'infrastruttura iperconvergente. Ogni unità hardware può essere configurata come nodo di un cluster per creare pool di risorse di archiviazione condivise, fornendo così il vantaggio di ponenti di calcolo, archiviazione e un'infrastruttura di archiviazione aziendale centralizzata.

SERVIZI CLOUD

I servizi di archiviazione Cloud spesso includono:

1) Servizi di archiviazione a blocchi, che espongono dispositivi a blocchi definiti dal software che possono essere presentati agli host virtuali in esecuzione nel cloud

2) Servizi di archiviazione oggetti, che possono essere mappati su host, applicazioni o persino altri servizi cloud

3) File system condivisi scalabili, che possono consentire a un set scalabile di host di accedere allo stesso file system ad alta velocità

4) Una varietà di servizi di replica, memorizzazione nella cache, archiviazione, mirroring e copia temporizzata su tutto quanto sopra

Vengono inoltre offerti servizi cloud aggiuntivi, come servizi di database gestiti, data lake, cache di memoria e code di messaggi, tutti in grado di memorizzare dati con stato e transitori.

ALTRE TIPOLOGIE

*Un altro tipo di infrastruttura di archiviazione è quella che contiene interfacce per supportare le esigenze di archiviazione dei dati delle applicazioni «**stateful**» emergenti progettate utilizzando l'architettura basata su microservizi e distribuite utilizzando container organizzati in cluster con piattaforme di orchestrazione dei container.*

Queste piattaforme dispongono di un meccanismo plug-in standard tramite un'interfaccia di archiviazione contenitore (Container Storage Interface - CSI) che collega i cluster configurati da essi a diversi tipi di implementazioni di archiviazione persistenti.

46. TASSONOMIE

Questa tecnologia può essere considerata dalle seguenti 2 tassonomie:

1) POSIZIONE DELLA RISORSA*: il dispositivo di archiviazione è direttamente collegato al client di archiviazione o al computer host; è chiamato memoria ad accesso diretto (DAS) oppure è presente una rete che separa il computer host e il dispositivo di archiviazione (archiviazione di rete);*

2) TIPO DI ARCHIVIAZIONE (TIPO DI ACCESSO)*: questa classificazione si basa sull'interfaccia di servizio offerta dal sistema di archiviazione utilizzato dal software client. (Archiviazione collegata alla rete: NAS; accesso a livello di file attraverso la rete e la rete di archiviazione SAN i cui protocolli forniscono l'accesso a livello di blocco attraverso la rete).*

47. MINACCE

ELENCO DELLE MINACCE

1) CREDENTIAL THEFT

2) CRACKING ENCRYPTION

3) INFECTION OF MALWARE AND RANSOMWARE [IL RANSOMWARE È UN TIPO DI MALWARE]

4) BACKDOORS AND UNPATCHED VULNERABILITIES

5) PRIVILEGE ESCALATION

6) HUMAN ERROR AND DELIBERATE MISCONFIGURATION

CRACKING ENCRYPTION

Gli algoritmi di crittografia utilizzano la casualità per creare chiavi o altri componenti chiave.

Le crittografie possono presentare una serie di punti deboli, da algoritmi di crittografia e generatori di chiavi deboli a vulnerabilità sul lato server, chiavi trapelate, difetti di progettazione fondamentali di bug e backdoor componenti chiave.

Usare crittografia avanzata; Proteggere le chiavi di crittografia.

Quando si tratta di generare chiavi, la stessa chiave non dovrebbe essere creata due volte. Alcuni attacchi mirano a interrompere il generatore di numeri casuali in modo che emetta lo stesso numero casuale per la generazione di chiavi due volte di seguito.;

INFECTION OF MALWARE AND RANSOMWARE

Il Ransomware è un tipo di Malware.

Può essere trasmesso tramite condivisione di file, download di software gratuito, allegati e-mail, utilizzo di dispositivi di archiviazione portatili compromessi e visita di siti Web infetti.

Può essere erroneamente installato su un host di gestione dello storage e di conseguenza causare danni come furto di credenziali, escalation di privilegi, corruzione/perdita/alterazione dei dati, compromettere backup futuri e altro. In generale, il malware utilizzerà le vulnerabilità del sistema operativo per installarsi ed eseguire varie azioni, il che significa che i sistemi operativi più comuni verranno probabilmente attaccati.

Per questo motivo, sarebbe più facile attaccare il sistema di gestione della memoria rispetto al dispositivo di memorizzazione.

BACKDOORS AND UNPATCHED VULNERABILITIES

Le backdoor sono meccanismi software creati intenzionalmente da venditori o singoli collaboratori per motivi spesso considerati legittimi dall'autore (ad esempio, per migliorare il supporto, il debug, la sicurezza nazionale, ecc.).

Dato il loro potenziale pericoloso, le backdoor non sono ufficialmente documentate e devono essere conosciute da un gruppo ristretto di individui. Quindi possono trapelare ….

PRIVILEGE ESCALATION

È l'atto di sfruttare un bug, un difetto di progettazione o una supervisione della configurazione per ottenere un accesso elevato alle risorse che sono normalmente protette da un'applicazione o da un utente. Si presenta in due forme:

I. **VERTICALE**: *un utente o un'applicazione con privilegi inferiori accede a funzioni o contenuti riservati a utenti o applicazioni con privilegi più elevati, e*

II. **ORIZZONTALE**: *un utente normale accede a funzioni o contenuti riservati ad altri utenti normali. Nei sistemi di archiviazione, questo tipo di minaccia può comportare una vasta gamma di rischi, tra cui: a) corruzione dei dati, b) alterazione dei dati, c) perdita dei dati e altro ancora.*

Ad esempio: un utente malintenzionato può utilizzare privilegi elevati per ottenere l'accesso a un sistema di archiviazione, eliminare i volumi di archiviazione e modificare la configurazione dell'accesso. ***L'attacco può anche compromettere le copie di backup*** *dei dati (ad es. copie sincrone/asincrone, istantanee) o* ***la generazione di backup futuri****.*

L'escalation può verificarsi a vari livelli, come i componenti di archiviazione (ad esempio array di archiviazione, host/client), i dispositivi di rete (ad esempio lo switch) o i sistemi di gestione (ad esempio i sistemi di gestione dello storage).

HUMAN ERROR AND DELIBERATE MISCONFIGURATION

Anche con l'esistenza di controlli di sicurezza, gli utenti possono realizzare una configurazione di archiviazione tecnicamente consentita che presenti comunque un'esposizione inaccettabile (ad esempio, arrestare la replica o il backup per manutenzione senza riattivarlo in seguito). Tale omissione potrebbe essere involontaria (ovvero un errore) o intenzionale (ovvero un sabotaggio).

Gli errori umani assumono forme diverse e alcuni sono significativamente più difficili da identificare o prevenire rispetto ad altri:

- *Errori di battitura*
- *Mancanza di conoscenza o familiarità con le basi di sicurezza interne e le migliori pratiche del fornitore*
- *Errata comunicazione tra individui o squadre*
- *Errori relativi all'orchestrazione o all'automazione dell'infrastruttura di archiviazione:*
  - ✓ *Diretto, come bug negli script e nei manifesti oppure*
  - ✓ *Indiretto, come dipendenze software non realizzate.*

48. RISCHI

Definizione di Rischio per la Sicurezza [Rif. NIST SP 800-53A; NIST SP 800-53]

«è la misura in cui un'entità è minacciata da una potenziale circostanza o evento.

Il rischio è in genere una funzione di:

(i) **IMPATTI NEGATIVI** *(entità del danno) che potrebbero verificarsi in caso di circostanze o eventi;*

(ii) **PROBABILITÀ** *che si verifichi.*

I rischi per la sicurezza relativi al sistema di informazione derivano dalla perdita di riservatezza, integrità o disponibilità di informazioni o sistemi di informazione.

Questi rischi riflettono i potenziali impatti negativi sulle operazioni organizzative (inclusi missione, funzioni, immagine o reputazione), beni organizzativi, individui, altre organizzazioni e la nazione»

ELENCO DEI RISCHI DELLA MEMORIA E DELLO STORAGE

1. DATA BREACH
2. DATA EXPOSURE
3. UNAUTHORIZED DATA ALTERATION
4. DATA CORRUPTION
5. COMPROMISING BACKUPS
6. DATA OBFUSCATION AND ENCRYPTION
7. TAMPERING OF STORAGE-RELATED LOG AND AUDIT DATA
8. DATA AVAILABILITY AND DENIAL OF SERVICE

DATA BREACH

Incidente che coinvolge tutte le informazioni: copiate, trasmesse, visualizzate, rubate o utilizzate

Le violazioni dei dati possono provenire da una fonte esterna o da una fonte interna, da un malintenzionato o un dipendente scontento e possono essere eseguite con tracce nascoste o completamente rimosse

DATA EXPOSURE

Esposizione involontaria di informazioni altrimenti riservate

L'esposizione sensibile dei dati si verifica a causa della non protezione adeguata di una risorsa di dati

Esempi: trasmissione al destinatario errato, messa a disposizione su un motore di ricerca, configurazione errata del controllo di accesso per consentire l'autorizzazione alla lettura di informazioni a utenti/gruppi, dati in oggetti disponibili al pubblico con chiavi crittografiche deboli, che non implementano pratiche con password con hash e salted (che è una forma di crittografia simile alla crittografia) e altre pratiche di archiviazione dei dati non sicure.

UNAUTHORIZED DATA ALTERATION AND ADDITION

L'attaccante ottiene l'accesso all'infrastruttura di archiviazione dei dati e modifica i dati in modo tale da costringere le transazioni future a utilizzare informazioni imprecise.

In alcuni casi, questo tipo di rischio viene realizzato utilizzando il metodo del «salami attack», in cui l'attaccante ruba un po' alla volta per un lungo periodo di tempo da un gran numero di transazioni (ad esempio, arrotondando per eccesso piccole somme).

DATA CORRUPTION

La corruzione dei dati si riferisce ad errori nei dati che si verificano durante la scrittura, la lettura, l'archiviazione, la trasmissione o l'elaborazione e che introducono modifiche involontarie ai dati originali.

Quando si verifica il danneggiamento dei dati, un file contenente tali dati produrrà risultati imprevisti quando vi si accede dal sistema o dall'applicazione correlata.

Alcuni tipi di malware possono danneggiare intenzionalmente i file come parte dei loro payload, di solito sovrascrivendoli con codice non operativo o spazzatura, mentre un virus non dannoso può anche danneggiare i file involontariamente quando li accede.

COMPROMISING BACKUPS

Il backup è sensibile a più errori:

- *configurazione errata: potrebbe comportare un backup del database eseguito senza applicare tecniche per garantire coerenza o fedeltà dell'ordine di scrittura;*
- *conservazione insufficiente: potrebbe significare che almeno una parte dei dati, passati o nuovi, sarà irrecuperabile;*
- *malintenzionato attacca un asset «primario», le sue copie e interferisce con il processo di backup «**avvelenando**» gradualmente le copie future;*
- *altra strategia di «avvelenamento»: infettare copie di backup di immagini del s.o. e di sw; in questo modo, quando un singolo componente o persino un intero ambiente viene ricostruito nel tentativo di combattere un'infezione, alcune parti del malware saranno incluse nell'ambiente ripristinato*

DATA OBFUSCATION AND ENCRYPTION

Offuscamento reversibile e la crittografia dei dati rendono i dati non disponibili per l'utente

Questo tipo di rischio è comunemente usato negli attacchi ransomware.

È reversibile e comunemente pensato per essere identificato al fine di riscatto.

TAMPERING OF STORAGE-RELATED LOG AND AUDIT DATA

La manomissione dei dati di registro e di controllo relativi all'archiviazione è il punto in cui un malintenzionato elimina o modifica i dati di registro per impedire la traccia di controllo nel tentativo di nascondere l'attacco o di indurre in errore le persone che indagano sugli attacchi con informazioni false.

I registri possono essere parzialmente modificati, ad esempio modificando il timestamp.

L'impatto di questo rischio è che l'attaccante o l'attacco può rimanere inosservato dai sistemi di sicurezza che si basano sui dati di registro.

Durante questo periodo, l'attaccante può eseguire ulteriori movimenti che possono compromettere i dati e il servizio. Ad esempio, un attacco di forza bruta per accedere a un sistema sensibile può essere nascosto eliminando i tentativi di accesso dai registri.

Un'altra forma di questo rischio comporta la manomissione del meccanismo stesso di registrazione (ad esempio, disabilitazione, riempimento di tutto lo spazio libero con messaggi sintetici, convincere i clienti a inviare i dati di registro ai server di registro, ecc.).

DATA AVAILABILITY AND DENIAL OF SERVICE [DOS]

Interruzione della disponibilità dei dati può verificarsi a causa di danni intenzionali o non intenzionali.

Il danno può essere fisico, come una disconnessione lungo il percorso di comunicazione o logico, come la configurazione errata di un endpoint dei componenti di rete. Ad esempio: a) un malintenzionato può eliminare le impostazioni di mascheramento SAN di un dispositivo di archiviazione a blocchi o sospendere le impostazioni di esportazione in NFS in modo che i client non possano accedere ai propri dati

Interrompe la disponibilità dei dati inondando la risorsa di destinazione con richieste per sovraccaricare i sistemi e impedire che alcune o tutte le richieste legittime siano soddisfatte.

49. MAPPATURA DELLE MINACCE CON I RISCHI

THREATS – INSECURE STATES AND ADVERSARY CAPABILITIES	OCCURRENCE – RISK OUTCOMES
Privilege escalation	*Application system – Data breach, data exposure, unauthorized data alteration, data corruption* *Administrative system – Compromise of existing and future backups, ransomware attack, DoS attack, tamper storage-related log and audit data, unsafe storage configuration parameters*
Credential theft	*Depending on whether user credentials or administrator credentials are compromised, all risk outcomes for privilege escalation apply to this threat.*
Cracking encryption	*Data breach and exposure of (a) data at rest, (b) data in transit, and (c) user/administrator session data*
Infection of malware and ransomware	*Malware can enable other threats – Privilege escalation, credential theft* *Malware, depending on where it is present – application systems or administrative systems can impact all risk outcomes in Section 3.2*
Backdoors and unpatched vulnerabilities	*Depends on the nature of the vulnerability, but in many cases, all risk outcomes for privilege escalation apply to this threat*
Human error and deliberate misconfiguration	*Depending on its type and scope, misconfiguration can impact all risk outcomes in Section 3.2*

50. SUPERFICI D'ATTACCO

1. PHYSICAL ACCESS
2. ACCESS TO STORAGE OS
3. ACCESS TO MANAGEMENT HOSTS
4. STORAGE CLIENTS
5. MANAGEMENT APIS, MANAGEMENT SOFTWARE, IN-BAND MANAGEMENT
6. STORAGE NETWORK (TAP INTO, ALTER TO GAIN ACCESS)
7. COMPUTE ENVIRONMENT OF KEY INDIVIDUALS – STORAGE ADMINS
8. ELECTRICITY NETWORK

PHYSICAL ACCESS

Due tipi di accesso:

a) «OVERT ACCESS» in cui l'attaccante si maschera da persona appartenente alla situazione (ad esempio, recitando la parte di un addetto alle pulizie, un tecnico o il personale di manutenzione dell'edificio);

b) «TAILGATING» accede ad aree riservate nel data center.

Sono vulnerabili:

a) i cavi di comunicazione (attingere alla comunicazione di archiviazione accedendo fisicamente ai cavi);

b) le componenti periferiche, come tastiera e mouse, sostituite con componenti infette (ad es. infiltrarsi in una tastiera infetta che include un componente «keylogger» che trasmette dati sensibili o infetta il sistema con malware);

c) l'accesso ai supporti rimovibili trasportati tra siti di archiviazione.

ACCESS TO STORAGE OS

Intrusione in un dispositivo di archiviazione sfruttando le vulnerabilità del s.o. stesso, ad esempio: array di archiviazione, switch, dispositivi di protezione dei dati e dispositivi di virtualizzazione dello storage.

ACCESS TO MANAGEMENT HOSTS

Accesso al s.o. di gestione del sistema di archiviazione e della memoria: l'attaccante infiltrandosi con malware o attraverso una vulnerabilità del s.o. può, hackerare un eseguibile, leggere i dati memorizzati nella cache, installare un «tap» di memoria per leggerne i dati, ottenere l'accesso al relativo array di archiviazione e sua configurazione.

STORAGE CLIENTS

Se l'accesso in banda all'archiviazione è abilitato, il malintenzionato che impersona il client di archiviazione può inviare comandi di gestione

Se il client è compromesso, il malintenzionato può anche danneggiare i backup futuri, in tal caso, può attendere un po', danneggiando la capacità dell'organizzazione perché non sarà in grado di utilizzare i backup compromessi.

MANAGEMENT APIS, MANAGEMENT SOFTWARE, IN-BAND MANAGEMENT

Un malintenzionato può accedere a un dispositivo di archiviazione rappresentando l'host o il software di gestione tramite l'API di gestione; in questo caso, il malintenzionato non deve infiltrarsi nel software di gestione per accedere alle funzionalità di gestione. Alcune apparecchiature consentono l'accesso in banda tramite i collegamenti dati (ad es. Percorsi Fibre Channel). Il dispositivo di archiviazione consente l'accesso alla gestione in banda attraverso lo stesso sistema di connessione utilizzato per il servizio di archiviazione, in questo modo, apre un'altra superficie di attacco, che può essere sfruttata dagli aggressori che possono impersonare un client di archiviazione durante l'invio di comandi di gestione.

STORAGE NETWORK (TAP INTO, ALTER TO GAIN ACCESS)

I dati sono trasferiti attraverso componenti della rete, come switch di archiviazione, cavi ed estensori. Se tali componenti sono compromessi, il malintenzionato può attingere al percorso dei dati e copiare, visualizzare, reindirizzare o rubare i dati e può leggere i dati di configurazione.

Un'altra forma di attacco è «Man In The Middle» (MITM), in particolare gli attacchi MITM Fibre Channel. Lo scopo del MITM è di sniffare i dati, alterarli o aggirare i meccanismi di crittografia e autenticazione.

Esempio: un'entità che utilizza IP, come uno switch o un sistema operativo, invierà richieste ARP (Address Resolution Protocol) quando comunica con altre entità. Il problema con ARP è che qualsiasi entità dannosa potrebbe inviare una risposta ARP invece del server effettivo. Poiché non esiste autenticazione con ARP, analogamente a come non esiste autenticazione con PLOGI nei Fabric Fibre Channel, un'entità che riceve una risposta ARP da un utente malintenzionato aggiornerebbe la tabella di routing con le informazioni errate. Inoltre, anche se un nodo non ha inviato una richiesta ARP, che richiederebbe l'indirizzo MAC di un indirizzo IP specifico, potrebbe potenzialmente ricevere una risposta ARP e aggiornare la propria tabella di routing. Ad esempio, un utente malintenzionato potrebbe inviare risposte ARP all'intero segmento di rete, comunicando a ciascuna entità che l'indirizzo MAC del router, ovvero 172.16.1.1, è in realtà l'indirizzo MAC dell'entità dannosa. Quando un nodo tenta di comunicare con qualsiasi altro nodo passando attraverso il router predefinito, in realtà andrà prima all'entità dannosa poiché utilizza l'indirizzo MAC dell'entità dannosa per il routing di livello 2.

COMPUTE ENVIRONMENT OF KEY INDIVIDUALS – STORAGE ADMINS

Accesso remoto all'infrastruttura di archiviazione. Un malintenzionato può installare malware in questo ambiente remoto che a sua volta installerà un registratore di chiavi che consente l'intercettazione delle credenziali di accesso.

ELECTRICITY NETWORK

Un enorme picco di corrente elettrica, come il tipo causato da un fulmine, può danneggiare e cancellare i dati memorizzati nei dischi elettromagnetici.

Le fluttuazioni di tensione creano rumore nella linea di terra. Il rumore della linea di terra può essere intercettato da un hacker collegato a una presa di corrente nelle vicinanze.

Un altro metodo si basa su un malware chiamato **Power Hammer**, *che può sottrarre furtivamente i dati da computer utilizzando linee elettriche. Questo malware filtra i dati da una macchina compromessa regolandone il consumo energetico, che può essere controllato attraverso il carico di lavoro della CPU.*

Informazioni sensibili, quali password e chiavi di crittografia, ***possono essere rubati un bit alla volta modulando le modifiche nel flusso corrente****. Nella variante a livello di linea di questo attacco, il malintenzionato intercetta i bit di dati estratti dal malware toccando il cavo di alimentazione del computer infetto. Nell'attacco a livello di fase, l'attaccante raccoglie i dati dal pannello di servizio elettrico principale.*

*I dati possono essere raccolti utilizzando un «****Tap****» (rubinetto) non invasivo che misura le emissioni sui cavi di alimentazione e quindi convertiti in una forma binaria tramite demodulazione e decodifica.*

51. LINEE GUIDA DELLA SICUREZZA

1. PHYSICAL STORAGE SECURITY
2. DATA PROTECTION
3. AUTHENTICATION AND DATA ACCESS CONTROL
4. AUDIT AND LOGGING
5. PREPARATION FOR DATA INCIDENT RESPONSE AND CYBER RECOVERY
6. GUIDELINES FOR NETWORK CONFIGURATION
7. ISOLATION
8. RESTORATION ASSURANCE
9. ENCRYPTION
10. ADMINISTRATIVE ACCESS
11. CONFIGURATION MANAGEMENT

PHYSICAL STORAGE SECURITY

I dettagli sono indicati nel NIST 800-171 e ISO 27040.

DATA PROTECTION

In base alla gamma di obiettivi e ai controlli primari dal punto di vista dell'archiviazione, ci sono questi contesti in cui orientare i controlli:

a. Backup e ripristino dei dati,

b. Tecnologie di replica,

c. *Protezione continua dei dati e copie,*

d. *Copie istantanee temporizzate (snapshots).*

ISOLATION

In caso di incidente, per fornire un ampio supporto per il ripristino da vari scenari, è necessario garantire un isolamento sufficiente tra asset di dati, classi e sistemi di archiviazione che contengono dati di ripristino, in particolare. In questo contesto, le organizzazioni dovrebbero conservare almeno due tipi separati di copie di protezione dei loro dati:

a. *Non malicious recovery copies (da utilizzare in caso di disastro naturale, guasto hardware, errore umano, ecc.), per DR, backup, ecc.*

b. *Cyber attack recovery copies (per l'evento di un attacco), ambiente isolato.*

ENCRYPTION

Nei sistemi di archiviazione, la crittografia delle informazioni sensibili dovrebbe essere implementata end-to-end, tra cui:

a. *Data at rest (dati a riposo);*

b. *Data in transit;*

c. *Administrative access (connessione tramite protocolli, API, reti di archiviazione).*

ADMINISTRATIVE ACCESS

Controllare e gestire un ampio spettro di elementi di archiviazione, inclusi array, rete, strumenti di gestione, backup, replica e archiviazione nel cloud.

CONFIGURATION MANAGEMENT

Fornire visibilità e controllo su impostazioni, comportamento e attributi fisici e logici delle risorse di archiviazione durante il loro ciclo di vita.

Nel contesto della sicurezza dello storage, ciò comporta:

a. *Mantenimento dell'inventario completo e attuale,*

b. *Gestione del cambiamento e*

c. *Garantire che la configurazione soddisfi continuamente le basi di sicurezza dell'organizzazione e le migliori pratiche del settore e che sia priva di rischi noti.*

*L'elenco dettagliato delle 11 precedenti raccomandazioni è nel capitolo «**4 - Security Guidelines for Storage Deployments nel NIST 800-209 Security Guidelines for Storage Infrastructure**»*

PARTE XI: ZERO TRUST (ZT)

[Rif.: NIST SP 800-207; NIST Planning for a ZT Arch.: A Starting Guide for Administrators]

52. PERCHÉ ZERO TRUST?

L'infrastruttura di un'azienda è diventata più complessa.

Una singola azienda può gestire diverse reti interne, uffici remoti con la propria infrastruttura locale, individui remoti e/o mobili e servizi cloud.

Questa complessità ha superato i metodi tradizionali di sicurezza della rete basata sul perimetro poiché non esiste un perimetro unico e facilmente identificabile.

La sicurezza della rete basata sul perimetro si è dimostrata insufficiente poiché una volta che gli aggressori ne violano il perimetro, non subiscono ostacoli per ulteriori movimenti trasversali.

PER CUI

1°. *Questa complessità porta allo sviluppo di un nuovo modello dei principi della sicurezza noto come "zero trust" (ZT).*

2°. *ZT si concentra principalmente sulla protezione dei dati, dispositivi e utenti.*

3°. *Si presume che un malintenzionato sia sempre presente nella rete (e … NON "se arriverà!") e che la rete non sia più affidabile.*

53. STORIA

La Defense Information Systems Agency (DISA) e il Dipartimento della difesa americano hanno pubblicato il loro lavoro su una strategia aziendale più sicura denominata "Black Core" [BCORE] (Nucleo Nero).

Il Black Core implicava il passaggio da un modello di ***sicurezza basato sul perimetro a uno incentrato sulla sicurezza delle singole transazioni****.*

Jericho Forum nel 1994 ha pubblicizzato l'idea della deperimetrizzazione, limitando la fiducia implicita in base alla posizione della rete e le limitazioni del fare affidamento su difese singole e statiche su un ampio segmento di rete [JERICHO].

I concetti di deperimetrizzazione si sono evoluti e migliorati nel più ampio concetto di ZT, che è stato successivamente coniato da John Kindervag mentre era a Forrester.

ZT è il termine che descrivere varie soluzioni di sicurezza informatica che hanno ***spostato la sicurezza dalla fiducia implicita in base alla posizione della rete alla valutazione della fiducia sulle transazioni****.*

NIST a febbraio 2020 pubblica il draft SP 800-207 e, ad agosto c.a., il documento finale, disponibile gratuitamente a chiunque

54. DEFINIZIONI

1) **ZT**: È L'INSIEME DEI PRINCIPI SUI QUALI SONO PIANIFICATE, IMPLEMENTATE E GESTITE LE ARCHITETTURE INFORMATICHE.

   ZT UTILIZZA UNA VISIONE OLISTICA CHE CONSIDERA TUTTI I POTENZIALI RISCHI PER UNA DETERMINATA MISSIONE O PROCESSO AZIENDALE E COME VENGONO MITIGATI.

   IN QUANTO TALE, NON ESISTE UN'UNICA IMPLEMENTAZIONE O ARCHITETTURA SPECIFICA DELL'INFRASTRUTTURA, MA DIPENDE DAL FLUSSO DI LAVORO (CIOÈ PARTE DELLA MISSIONE AZIENDALE) ANALIZZATO E DALLE RISORSE UTILIZZATE NELL'ESECUZIONE DI TALE FLUSSO DI LAVORO.

2) **ZTA***: piano di sicurezza che utilizza concetti ZT e comprende relazioni tra i componenti, pianificazione del flusso di lavoro e policy di accesso.*
   - ✓ *Un'impresa ZT è l'infrastruttura di rete (fisica e virtuale) e le politiche operative in atto per un'azienda come piano di ZTA.*
   - ✓ *Utilizza i principi ZT per pianificare l'infrastruttura e i flussi di lavoro aziendali.*
   - ✓ *È un insieme di principi guida nell'infrastruttura di rete e nella progettazione e nel funzionamento del sistema.*

55. PRINCIPI ZT

1. *Termine per un set di paradigmi di sicurezza informatica che* **SPOSTANO LE DIFESE DI RETE DA PERIMETRI STATICI BASATI SULLA RETE PER CONCENTRARSI SU UTENTI, ASSET E RISORSE.**
2. *Presuppone che* **NON VI SIA ALCUNA FIDUCIA IMPLICITA CONCESSA ALLE RISORSE O AGLI ACCOUNT UTENTE** *in base esclusivamente alla loro posizione fisica o di rete (ad esempio, reti locali rispetto a Internet).*
3. *L'autenticazione e l'autorizzazione (sia utente sia dispositivo) sono funzioni discrete eseguite prima che sia stabilita una sessione a una risorsa aziendale.*
4. *La fiducia zero è una risposta alle tendenze della rete aziendale che includono utenti remoti e risorse basate su cloud non presenti all'interno di un confine di rete di proprietà aziendale.*
5. *Zero focus sulla protezione delle risorse,* **NON SUI SEGMENTI DI RETE**, *poiché* **LA POSIZIONE DELLA RETE NON È PIÙ VISTA COME IL COMPONENTE PRINCIPALE DELLA POSIZIONE DI SICUREZZA DELLA RISORSA**.

1 - TENETS THAT DEAL WITH NETWORK IDENTITY GOVERNANCE

I. TUTTA L'AUTENTICAZIONE E L'AUTORIZZAZIONE DELLE RISORSE SONO DINAMICHE E APPLICATE RIGOROSAMENTE PRIMA CHE L'ACCESSO SIA CONSENTITO.

2 - TENETS THAT DEAL WITH END DEVICES

I. TUTTE LE FONTI DI DATI E I SERVIZI INFORMATICI SONO CONSIDERATI RISORSE.

II L'AZIENDA MONITORA E MISURA L'INTEGRITÀ E LA POSIZIONE DI SICUREZZA DI TUTTE LE RISORSE DI PROPRIETÀ E ASSOCIATE.

Questo principio si occupa degli aspetti dell'igiene informatica:

- ✓ *configurazione,*
- ✓ *applicazione di patch,*
- ✓ *caricamento delle applicazioni, ecc.*

3 - TENETS THAT APPLY TO DATA FLOWS

I. TUTTE LE COMUNICAZIONI SONO PROTETTE INDIPENDENTEMENTE DALLA POSIZIONE DELLA RETE.

In ZT, la rete è sempre considerata contestata.
Si dovrebbe presumere che un utente malintenzionato sia presente sulla rete e possa osservare/modificare le comunicazioni.

II. L'ACCESSO ALLE SINGOLE RISORSE AZIENDALI È CONCESSO PER SESSIONE.

In un'architettura ZT ideale, ogni operazione univoca sarebbe sottoposta ad autenticazione e autorizzata prima di essere eseguita.

III. *L'ACCESSO ALLE RISORSE È DETERMINATO DA POLICY DINAMICHE, COMPRESO LO STATO OSSERVABILE DELL'IDENTITÀ DEL CLIENT, DELL'APPLICAZIONE/SERVIZIO E DELL'ASSET RICHIEDENTE, E PUÒ INCLUDERE ALTRI ATTRIBUTI COMPORTAMENTALI E AMBIENTALI.*

In ZT, il comportamento predefinito per tutte le risorse consiste nel negare tutte le connessioni con un elenco di autorizzazioni.

IV. *L'AZIENDA RACCOGLIE QUANTE PIÙ INFORMAZIONI POSSIBILI SULLO STATO ATTUALE DELLE RISORSE, DELL'INFRASTRUTTURA DI RETE E DELLE COMUNICAZIONI E LE UTILIZZA PER MIGLIORARE LA PROPRIA POSIZIONE DI SICUREZZA.*

ZT aggiunge un fattore di risposta dinamica che mancava (o non era possibile) nelle precedenti architetture perimetrali.

56. FONDAMENTALI DELLA ZT

1. *Tutte le fonti di dati e i servizi di elaborazione sono considerati risorse.*
2. *Tutte le comunicazioni sono protette indipendentemente dal percorso di rete.*
   - ✓ *La posizione all'interno della rete non implica fiducia: i requisiti di sicurezza devono essere sempre soddisfatti a prescindere dalla provenienza della richiesta.*
3. *L'accesso alle singole risorse aziendali viene concesso per sessione.*
   - ✓ *La fiducia nel richiedente è valutata prima che sia concesso l'accesso. Ovvero, prima di avviare una sessione o eseguire una transazione con una risorsa.*
4. *L'accesso alle risorse è determinato da una politica dinamica, incluso lo stato osservabile dell'identità del cliente, dell'applicazione/servizio e della risorsa richiedente, e può includere altri attributi comportamentali e ambientali.*
   - ✓ *Gli attributi ambientali possono includere fattori come la posizione del richiedente nella rete, l'ora, gli attacchi attivi segnalati, ecc.*
5. *L'azienda monitora e misura l'integrità e la sicurezza di tutte le risorse di proprietà e associate.* **NESSUNA RISORSA È INTRINSECAMENTE AFFIDABILE.**
6. *Tutte le autenticazioni e autorizzazioni delle risorse sono dinamiche e applicate rigorosamente prima che l'accesso sia consentito.*
   - ✓ *Ciclo costante di accesso, scansione e valutazione delle minacce, adattamento e rivalutazione continua della fiducia.*
7. *L'azienda raccoglie quante più informazioni possibili sullo stato attuale delle risorse, dell'infrastruttura di rete e delle comunicazioni e le utilizza per migliorare il proprio stato di sicurezza.*
   - ✓ *Le informazioni acquisite per migliorare la creazione e l'applicazione delle politiche.*

57. PRESUPPOSTI PER LO SVILUPPO DELLA RETE ZTA

1. L'INTERA RETE PRIVATA AZIENDALE NON È CONSIDERATA UNA ZONA DI FIDUCIA IMPLICITA.
   - ✓ *Le risorse dovrebbero sempre comportarsi come se un utente malintenzionato fosse presente sulla rete .*
2. I DISPOSITIVI SULLA RETE POTREBBERO NON ESSERE DI PROPRIETÀ O CONFIGURABILI DALL'AZIENDA.
3. NESSUNA RISORSA È INTRINSECAMENTE ATTENDIBILE
   - ✓ *Questa valutazione deve essere continua per tutta la durata della sessione.*
4. NON TUTTE LE RISORSE AZIENDALI SI TROVANO SU UN'INFRASTRUTTURA DI PROPRIETÀ DELL'AZIENDA
   - ✓ *Le risorse includono soggetti aziendali remoti e servizi cloud.*
5. I SOGGETTI E LE RISORSE AZIENDALI REMOTE NON POSSONO FIDARSI DELLA LORO CONNESSIONE DI RETE LOCALE.
   - ✓ *I soggetti remoti dovrebbero presumere che la rete locale (cioè non di proprietà dell'azienda) sia ostile.*
   - ✓ *Gli asset dovrebbero presumere che tutto il traffico sia monitorato e potenzialmente modificato.*
   - ✓ *Tutte le richieste di connessione devono essere autenticate e autorizzate.*
6. ASSET E FLUSSI DI LAVORO CHE SI SPOSTANO TRA L'INFRASTRUTTURA AZIENDALE E NON AZIENDALE DEVONO AVERE UNA POLITICA E UNA POSIZIONE DI SICUREZZA COERENTI.
   - ✓ *Asset e carichi di lavoro dovrebbero mantenere la loro posizione di sicurezza quando si spostano da o verso l'infrastruttura di proprietà aziendale.*
   - ✓ *Include i dispositivi che si spostano da reti aziendali a reti non aziendali (ovvero utenti remoti) ed anche la migrazione dei carichi di lavoro da data center locali a istanze cloud non aziendali.*

58. OBIETTIVI ZT

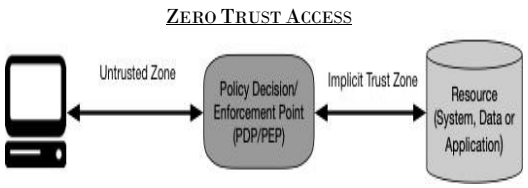
1. **IMPEDIRE** *l'accesso non autorizzato rendendo il controllo degli accessi il più granulare possibile.*
2. **RIDURRE** *le incertezze ponendo attenzione all'Authentication, all'Authorization e alla Shrinking (riduzione) delle zone di fiducia implicite, costringendo al minimo i ritardi temporali nei meccanismi di autenticazione.*
3. **LIMITARE** *al minimo privilegio e* ***rendere*** *il più granulari possibile le regole di accesso .*

59. MODELLO ZT

Nel modello astratto di accesso mostrato nella Figura 1, un utente o una macchina deve accedere a una risorsa aziendale. L'accesso è concesso tramite le Policy Decision Point (PDP) e l'applicazione della Policy Enforcement Point (PEP).

1. *Il sistema deve garantire che l'utente sia autentico e la richiesta sia valida.*
2. *Il PDP/PEP passa la corretta valutazione per consentire al soggetto di accedere alla risorsa. Ciò implica che zero trust si applica a due aree fondamentali: autenticazione e autorizzazione.*

- ✓ *Qual è il livello di fiducia sull'identità dell'utente per questa richiesta univoca?*
- ✓ *L'accesso alla risorsa è consentito dato il livello di fiducia nell'identità dell'utente?*
- ✓ *Il dispositivo utilizzato per la richiesta ha la corretta posizione di sicurezza?*



- ✓ *Ci sono altri fattori che dovrebbero essere considerati e che cambiano il livello di fiducia (ad esempio, ora, posizione del soggetto, posizione di sicurezza del soggetto)?*

59A. ZT PROCESS

NIST SP 800-37, Revisione 2 descrive la metodologia del RISK MANAGEMENT FRAMEWORK *e le sue sette fasi:*

1. *Organizational and system preparation (PREPARE step)*
2. *System categorization (CATEGORIZE step)*
3. *Control selection (SELECT step)*
4. *Control implementation (IMPLEMENT step)*
5. *Control assessment (ASSESS step)*
6. *System authorization (AUTHORIZE step)*
7. *Control monitoring (MONITOR step)*

Sebbene i passaggi siano descritti in ordine, dopo l'implementazione iniziale, possono essere eseguiti o rivisitati in qualsiasi sequenza.

I singoli compiti che compongono i sette passaggi potrebbero essere condotti e rivisitati secondo necessità, e possibilmente in parallelo con altri passaggi/compiti.

Le transizioni tra i passaggi possono essere fluide (vedi figura 2).

Questo è vero quando si sviluppa e si implementa una ZTA, poiché la natura dinamica di ZT può richiedere una reiterazione o transizioni rapide nelle fasi RMF per rispondere a nuove informazioni o cambiamenti tecnologici.

I dettagli dei singoli passaggi sono documentati in NIST SP 800-37r2 e nella Guida rapida di accompagnamento.

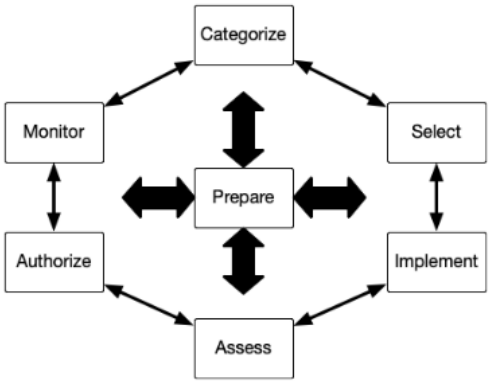


Figure 2: RMF State Machine

Per una migrazione iniziale, i passaggi sono generalmente seguiti in ordine (ma non è necessario).

I passaggi RMF sono molto simili ai passaggi di alto livello sviluppati per ZT da John Kindervag e sono parzialmente mappati di seguito.

Questo processo presuppone che il limite di autorizzazione sia stato creato e che i componenti di sistema utilizzati nel flusso di lavoro siano noti (ovvero che la fase **PREPARE** *sia stata eseguita e che i dati siano stati raccolti).*

Il passaggio **CATEGORIZE** *non è esplicito poiché questa descrizione di alto livello non è stata sviluppata pensando alle agenzie federali.*

1. *Mappare la superficie di attacco della risorsa e identificare le parti chiave che verrebbero prese di mira da un malintenzionato. Questi saranno coperti dalle attività nel passaggio* **SELECT**.

2. *Dalla fase* **PREPARE** *(attività P-12 e P-13), i flussi di dati dovrebbero essere identificati e mappati.*

3. *La fase* **IMPLEMENT***: concentrarsi sull'implementazione dei controlli della fase* **SELECT** *sulla risorsa e sulla relativa* PEP (POLICY ENFORCEMENT POINT).

Il PEP *può essere un componente software separato dalla risorsa stessa e viene utilizzato per soddisfare i controlli relativi all'autenticazione/autorizzazione.*

La rete sottostante non deve essere considerata attendibile, quindi i collegamenti tra le singole risorse devono passare attraverso un PEP (POLICY ENFORCEMENT POINT).

4. *La fase di* **ASSESS***: assicurarsi che tutte le politiche di accesso sviluppate e messe in atto durante la fase di* **IMPLEMENT** *siano implementate e funzionino come previsto. Ciò si concluderebbe con il passaggio* **AUTHORIZE***, in cui il sistema e il flusso di lavoro sono considerati in uno stato per iniziare l'operazione effettiva.*

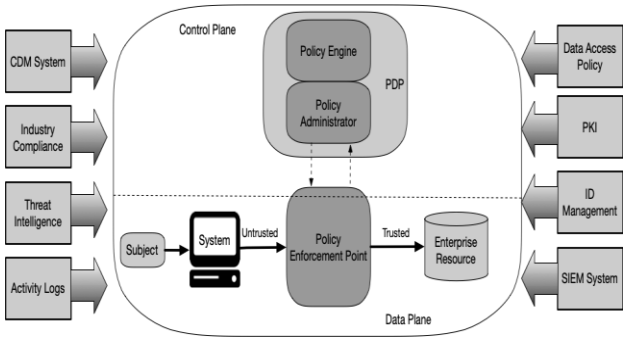
PER I DETTAGLI DEI SINGOLI PROCESSI VEDI PARAGRAFO "2.1 THE PROCESS" DEL MANUALE "NIST – PLANNING FOR A ZT ARCHITECTURE: A STARTING GUIDE FOR ADMINISTRATORS".

60. COMPONENTI DELLA ZTA

Il PDP è diviso in 2 componenti logiche:

1. IL MOTORE DELLA POLITICA
2. L'AMMINISTRATORE DELLA POLITICA (DEFINITI DI SEGUITO).

CORE ZERO TRUST LOGICAL COMPONENTS



I componenti logici ZTA utilizzano un piano di controllo separato per comunicare, mentre i dati dell'applicazione vengono comunicati su un piano dati.

Descrizione dei componenti

1. POLICY ENGINE (PE)
2. POLICY ADMINISTRATOR (PA)
3. POLICY ENFORCEMENT POINT (PEP)
4. CONTINUOUS DIAGNOSTICS AND MITIGATION (CDM) SYSTEM
5. INDUSTRY COMPLIANCE SYSTEM
6. THREAT INTELLIGENCE FEED(S)
7. NETWORK AND SYSTEM ACTIVITY LOGS
8. DATA ACCESS POLICIES
9. ENTERPRISE PUBLIC KEY INFRASTRUCTURE (PKI)
10. ID MANAGEMENT SYSTEM
11. SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM) SYSTEM

POLICY ENGINE (PE)

È responsabile della decisione finale di concedere l'accesso a una risorsa per un determinato argomento.

Utilizza la politica aziendale e input da fonti esterne (ad esempio, sistemi CDM, servizi di intelligence sulle minacce descritti di seguito) come input per un algoritmo di attendibilità per concedere, negare o revocare l'accesso alla risorsa.

È abbinato al componente dell'amministratore dei criteri.

Acquisisce e registra la decisione (come approvata o negata) e l'amministratore della politica esegue la decisione.

POLICY ADMINISTRATOR (PA)

È responsabile di stabilire e/o interrompere il percorso di comunicazione tra un soggetto e una risorsa (tramite i comandi ai PEP pertinenti).

Genera qualsiasi autenticazione e token di autenticazione della sessione o credenziali utilizzate da un client per accedere a una risorsa.

Autorizza o nega una sessione.

Se la sessione è autorizzata, configura il PEP per consentire l'avvio della sessione.

Se la sessione è negata, segnala al PEP di interrompere la connessione.

POLICY ENFORCEMENT POINT (PEP)

Abilita, monitora e chiude le connessioni tra un soggetto e una risorsa aziendale.

Comunica con la PA per inoltrare richieste e/o ricevere aggiornamenti delle politiche dalla PA.

Il PEP può essere suddiviso in due diversi componenti: 1) il client (ad esempio, agente su un laptop); 2) lato risorsa (ad esempio, componente gateway di fronte alla risorsa che controlla l'accesso) o un singolo componente del portale che agisce come gatekeeper per i percorsi di comunicazione.

CONTINUOUS DIAGNOSTICS AND MITIGATION (CDM) SYSTEM

Raccoglie informazioni sullo stato corrente dell'asset aziendale e applica gli aggiornamenti alla configurazione e ai componenti software.

Fornisce al PE le informazioni sull'asset che effettua una richiesta di accesso, ad esempio se sta eseguendo il sistema operativo con patch appropriato (OS), l'integrità dei componenti software approvati dall'azienda o la presenza di componenti non approvati e se l'asset presenta vulnerabilità note.

INDUSTRY COMPLIANCE SYSTEM

Garantisce che l'impresa rimanga conforme a qualsiasi regime normativo a cui potrebbe rientrare (ad esempio, FISMA, requisiti di sicurezza delle informazioni del settore sanitario o finanziario).

Include tutte le regole dei criteri che un'impresa sviluppa per garantire la conformità.

THREAT INTELLIGENCE FEED(S)

Fornisce informazioni da fonti interne o esterne che aiutino il PE a prendere decisioni di accesso.

Include anche difetti scoperti di recente nel software, malware identificato di recente e attacchi segnalati ad altre risorse a cui il motore dei criteri vorrà negare l'accesso dalle risorse aziendali.

NETWORK AND SYSTEM ACTIVITY LOGS

Aggrega registri delle risorse, traffico di rete, azioni di accesso alle risorse e altri eventi che forniscono feedback in tempo reale (o quasi) sull'atteggiamento di sicurezza dei sistemi informativi aziendali.

Le scansioni del monitor, il traffico di rete e i metadati sono archiviati per la creazione di criteri contestuali, analisi forensi o analisi successive, tali dati diventano un obiettivo per gli aggressori.

DATA ACCESS POLICIES

Sono gli attributi, le regole e le politiche sull'accesso alle risorse aziendali.

È codificato (tramite l'interfaccia di gestione) o generato dinamicamente dal motore dei criteri.

Sono il punto di partenza per autorizzare l'accesso a una risorsa in quanto forniscono i privilegi di accesso di base per account e applicazioni / servizi nell'azienda.

Devono essere basate sui ruoli e sui bisogni definiti della missione dell'organizzazione (ERM).

ENTERPRISE PUBLIC KEY INFRASTRUCTURE (PKI)

È responsabile della generazione e della registrazione dei certificati rilasciati dall'azienda a risorse, soggetti, servizi e applicazioni.

Include anche l'ecosistema dell'autorità di certificazione globale e la PKI.

ID MANAGEMENT SYSTEM

Crea, archivia e gestisce gli account e i record di identità (ad esempio, server LDAP (Light Directory Access Protocol)).

Contiene le informazioni necessarie sull'oggetto (ad es. Nome, indirizzo e-mail, certificati) e altre caratteristiche aziendali come ruolo, attributi di accesso e risorse assegnate.

SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM) SYSTEM

Raccoglie informazioni incentrate sulla sicurezza per un'analisi successiva.

Questi dati vengono quindi utilizzati per perfezionare le policy e avvisare di possibili attacchi contro le risorse aziendali.

61. MODELLI DI DISTRIBUZIONE ZTA

A seconda di come è configurata una rete aziendale, più modelli di distribuzione ZTA possono essere utilizzati per diversi processi aziendali in un'azienda

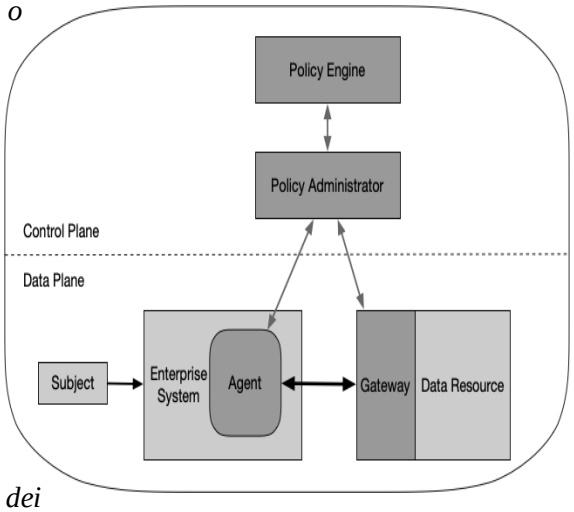
1. DEVICE AGENT/GATEWAY-BASED DEPLOYMENT
2. ENCLAVE-BASED DEPLOYMENT
3. RESOURCE PORTAL-BASED DEPLOYMENT
4. DEVICE APPLICATION SANDBOXING

A seconda di come è configurata una rete aziendale, più modelli di distribuzione ZTA possono essere utilizzati per diversi processi aziendali in un'azienda.

DEVICE AGENT/GATEWAY-BASED DEPLOYMENT

Il PEP è diviso in due componenti che risiedono sulla risorsa o come un componente direttamente davanti a una risorsa.

Ad esempio, ogni risorsa emessa dall'azienda ha un agente del dispositivo installato che coordina le connessioni e ogni risorsa ha un componente (cioè il gateway) che viene posizionato direttamente davanti in modo che la risorsa comunichi solo con il gateway, fungendo essenzialmente da proxy per la risorsa.



L'agent è un componente software che indirizza una parte (o tutto) il traffico al PEP appropriato per consentire la valutazione delle richieste.

Il gateway è responsabile della comunicazione con l'amministratore dei criteri e consente solo i percorsi di comunicazione approvati configurati dall'amministratore dei criteri.

In uno scenario tipico, un soggetto con un laptop fornito dall'azienda desidera connettersi a una risorsa aziendale (ad esempio, applicazione/database delle risorse umane).

PROTOCOLLO DI COLLOQUIO

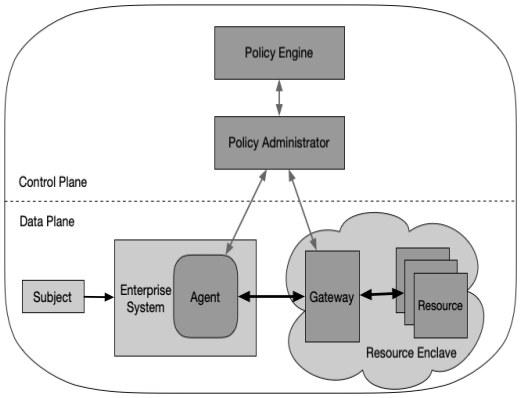
1) *La richiesta di accesso viene presa dall'Agent e la inoltra al PA.*
2) *Il PA inoltra la richiesta al PE per la valutazione.*
3) *Se la richiesta è autorizzata, il PA configura un canale di comunicazione tra l'Agent e il Gateway della risorsa pertinente tramite il Control Plane.*
   Ciò può includere informazioni quali un indirizzo IP (Internet Protocol), informazioni sulla porta, chiave di sessione o simili elementi di sicurezza.
4) *L'Agent e il Gateway si connettono e iniziano i flussi di dati di applicazioni/servizi crittografati.*
5) *La connessione tra l'Agent e il Gateway è interrotta quando il flusso di lavoro è completato o quando è attivato dal PA a causa di un evento di sicurezza (ad es. timeout della sessione, errore di riautenticazione).*

Questo modello è utilizzato al meglio per le aziende che dispongono di un robusto programma di gestione dei dispositivi e di risorse discrete in grado di comunicare con il gateway.

ENCLAVE-BASED DEPLOYMENT

I componenti del gateway potrebbero non risiedere su asset ma risiedere invece al confine di un'enclave di risorse (ad esempio, data center in loco) come mostrato nella Figura 4.

ENCLAVE GATEWAY MODEL



Queste risorse servono un singolo funzione aziendale o potrebbe non essere in grado di comunicare direttamente con un gateway (ad esempio, un sistema di database legacy che non dispone di un'interfaccia di programmazione dell'applicazione [API] che può essere utilizzata per comunicare con un gateway).

Può essere utile anche per le aziende che utilizzano micro-servizi basati su cloud per un singolo processo aziendale (ad esempio, notifica agli utenti, ricerca nel database, esborso di stipendio).

Il cloud privato si trova dietro un gateway.

Lo svantaggio è che il gateway protegge una raccolta di risorse e potrebbe non essere in grado di proteggere ogni risorsa individualmente.

RESOURCE PORTAL-BASED DEPLOYMENT

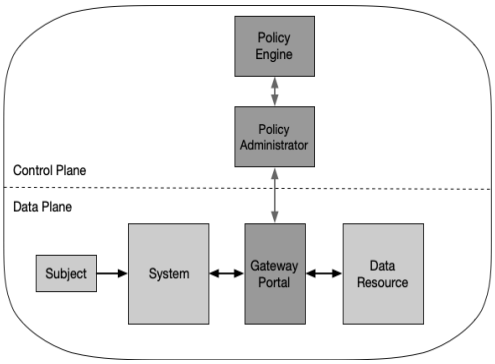
Il PEP è un singolo componente che funge da gateway per le richieste del soggetto.

Il gateway può essere per una singola risorsa o un'enclave per una raccolta di risorse utilizzate per una singola funzione aziendale.

Un esempio potrebbe essere un portale gateway in un cloud privato o in un data center contenente applicazioni legacy, come mostrato nella Figura 5.

Vantaggio principale: non è necessario installare un componente software su tutti i dispositivi client; è più flessibile per le politiche BYOD.

RESOURCE PORTAL MODEL



Gli amministratori aziendali non devono assicurarsi che ogni dispositivo abbia l'agent prima dell'uso.

Può scansionare e analizzare risorse e dispositivi solo una volta connessi al PEP e può non essere in grado di monitorarli continuamente per rilevare malware, vulnerabilità prive di patch e configurazione appropriata.

Differenza principale: non esiste un agente locale che gestisca le richieste, QUINDI L'AZIENDA POTREBBE NON AVERE PIENA VISIBILITÀ O CONTROLLO ARBITRARIO SULLE RISORSE IN QUANTO PUÒ VEDERLE SCANSIONARLE SOLO QUANDO SI CONNETTONO A UN PORTALE.

QUESTE RISORSE POTREBBERO ESSERE INVISIBILI ALL'AZIENDA TRA QUESTE SESSIONI.

CONSENTE INOLTRE AGLI AGGRESSORI DI SCOPRIRE E TENTARE DI ACCEDERE AL PORTALE O TENTARE UN ATTACCO DOS (DENIAL OF SERVICE) CONTRO IL PORTALE.

DEVICE APPLICATION SANDBOXING

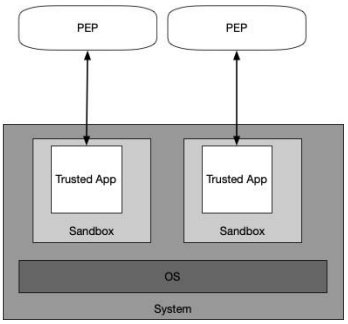
Un'altra variante consiste in applicazioni o processi controllati sono eseguiti in compartimenti stagni sulle risorse.

Questi compartimenti potrebbero essere macchine virtuali, contenitori o qualche altra implementazione.

Il dispositivo in oggetto esegue applicazioni approvate e controllate in una sandbox.

Le applicazioni possono comunicare con il PEP per richiedere l'accesso alle risorse, ma il PEP rifiuterà le richieste da altre applicazioni sull'asset.

APPLICATION SANDBOXES



VANTAGGIO: PRINCIPALE VANTAGGIO CONSISTE NELLE SINGOLE APPLICAZIONI SEGMENTATE DAL RESTO DELL'ASSET.

Se l'asset non può essere sottoposto a scansione per rilevare eventuali vulnerabilità, queste singole applicazioni in modalità Sandbox potrebbero essere protette da una potenziale infezione da malware sull'asset host.

SVANTAGGIO: MANTENERE QUESTE APPLICAZIONI IN MODALITÀ SANDBOX PER TUTTE LE RISORSE E POTREBBERO NON AVERE PIENA VISIBILITÀ SULLE RISORSE DEI CLIENTI.

Assicurarsi che ogni applicazione in modalità sandbox sia sicura, il che potrebbe richiedere uno sforzo maggiore rispetto al semplice monitoraggio dei dispositivi.

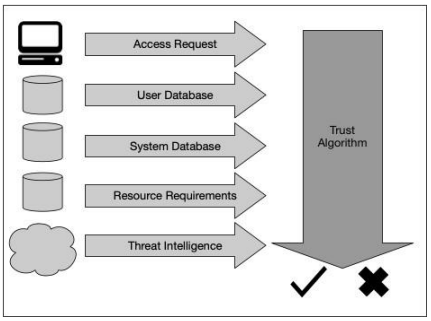
62. ALGORITMO DI FIDUCIA

Il PE può essere pensato come il cervello e l'algoritmo di fiducia come il suo processo di pensiero principale.

L'algoritmo di fiducia (TA - Trust Algorithm) è il processo utilizzato dal motore delle politiche per concedere o negare l'accesso a una risorsa.

Il PE riceve input da più fonti: il database delle politiche con informazioni osservabili su soggetti, attributi e ruoli dei soggetti, modelli storici di comportamento dei soggetti, fonti di intelligence sulle minacce e altre fonti di metadati.

TRUST ALGORITHM INPUT



Categorie degli input dell'algoritmo:

1. ACCESS REQUEST
2. SUBJECT DATABASE
3. ASSET DATABASE AND OBSERVABLE STATUS
4. RESOURCE ACCESS REQUIREMENTS
5. THREAT INTELLIGENCE

ACCESS REQUEST

Questa è la richiesta effettiva del soggetto.

La risorsa richiesta è l'informazione principale utilizzata, ma vengono utilizzate anche le informazioni sul richiedente.

Include la versione del sistema operativo, il software utilizzato e il livello di patch.

A seconda di questi fattori e della posizione di sicurezza delle risorse, l'accesso alle risorse potrebbe essere limitato o negato.

ASSET DATABASE AND OBSERVABLE STATUS

È il database che contiene lo stato noto di ogni risorsa di proprietà dell'azienda (e possibilmente nota non aziendale/BYOD) fisica e virtuale.

Questo viene confrontato con lo stato della risorsa che effettua la richiesta e può includere la versione del sistema operativo, il software presente e la sua integrità, posizione (posizione di rete e geolocalizzazione) e livello di patch.

A seconda dello stato della risorsa rispetto a questo database, l'accesso alle risorse potrebbe essere limitato o negato.

RESOURCE ACCESS REQUIREMENTS

Questa serie di criteri completa l'ID utente e il database degli attributi [SP800-63] e definisce i requisiti minimi per l'accesso alla risorsa.

I requisiti possono includere livelli di garanzia dell'autenticatore, come la posizione di rete MFA [MultiFactor Authentication] (ad esempio, negare l'accesso da indirizzi IP esteri), la sensibilità dei dati e le richieste di configurazione delle risorse.

Questi requisiti dovrebbero essere sviluppati sia dai responsabili dei dati sia dai responsabili dei processi aziendali che utilizzano i dati (cioè i responsabili della missione).

THREAT INTELLIGENCE

È un feed di informazioni o su minacce generali e malware attivo che opera su Internet.

Può includere informazioni specifiche sulla comunicazione che potrebbero essere sospette (come le query per possibili nodi di comando e controllo del malware).

Questi feed possono essere servizi esterni o scansioni interne e scoperte e possono includere firme di attacco e mitigazioni.

È l'unico componente che molto probabilmente sarà sotto il controllo di un servizio piuttosto che dell'impresa.

La determinazione finale viene quindi passata al PA (Policy Administrator) per l'esecuzione.

Il PA configura i PEP per abilitare la comunicazione autorizzata e possono anche sospendere una sessione di comunicazione per riautenticare e autorizzare nuovamente la connessione ed è anche responsabile dell'emissione del comando per terminare la connessione (ad es.: dopo un timeout, al termine del flusso di lavoro, a causa di un avviso di sicurezza).

63. REQUISITI DELLA RETE A SUPPORTO DELLA ZTA

ELENCO DEI REQUISITI

1. ENTERPRISE ASSETS HAVE BASIC NETWORK CONNECTIVITY.
2. THE ENTERPRISE MUST BE ABLE TO DISTINGUISH BETWEEN WHAT ASSETS ARE OWNED OR MANAGED BY THE ENTERPRISE AND THEIR CURRENT SECURITY POSTURE.
3. THE ENTERPRISE CAN CAPTURE ALL NETWORK TRAFFIC.
4. ENTERPRISE RESOURCES SHOULD NOT BE REACHABLE WITHOUT ACCESSING A PEP.
5. THE DATA PLANE AND CONTROL PLANE ARE LOGICALLY SEPARATE.
6. ENTERPRISE ASSETS CAN REACH THE PEP COMPONENT.
7. THE PEP IS THE ONLY COMPONENT THAT ACCESSES THE POLICY ADMINISTRATOR AS PART OF A BUSINESS FLOW.
8. REMOTE ENTERPRISE ASSETS SHOULD BE ABLE TO ACCESS ENTERPRISE RESOURCES WITHOUT NEEDING TO TRAVERSE ENTERPRISE NETWORK INFRASTRUCTURE FIRST.
9. THE INFRASTRUCTURE USED TO SUPPORT THE ZTA ACCESS DECISION PROCESS SHOULD BE MADE SCALABLE TO ACCOUNT FOR CHANGES IN PROCESS LOAD.
10. ENTERPRISE ASSETS MAY NOT BE ABLE TO REACH CERTAIN PEPS DUE TO OBSERVABLE FACTORS.

DESCRIZIONE DEI REQUISITI

1. LE RISORSE AZIENDALI HANNO UNA CONNETTIVITÀ DI RETE DI BASE.

   La rete locale (LAN), controllata o meno dall'azienda, fornisce il routing e l'infrastruttura di base (ad esempio, DNS).

   L'asset aziendale remoto potrebbe non utilizzare necessariamente tutti i servizi di infrastruttura.

2. L'AZIENDA DEVE ESSERE IN GRADO DI DISTINGUERE TRA QUALI RISORSE SONO DI PROPRIETÀ O GESTITE DALL'AZIENDA E IL LORO ATTUALE STATO DI SICUREZZA.

   Ciò è determinato dalle credenziali rilasciate dall'azienda e dal mancato utilizzo di informazioni che non possono essere autenticate (ad es. indirizzi MAC di rete che possono essere falsificati).

3. L'AZIENDA PUÒ ACQUISIRE TUTTO IL TRAFFICO DI RETE.

L'azienda registra i pacchetti visti sul piano dati, anche se non è in grado di eseguire l'ispezione a livello di applicazione (ovvero, OSI livello 7) su tutti i pacchetti.

L'azienda filtra i metadati sulla connessione (ad esempio, destinazione, ora, identità del dispositivo) per aggiornare dinamicamente le politiche e informare il PE mentre valuta le richieste di accesso.

4. LE RISORSE AZIENDALI NON DOVREBBERO ESSERE RAGGIUNGIBILI SENZA ACCEDERE A UN PEP.

   Le risorse aziendali non accettano connessioni in entrata arbitrarie da Internet.

   Le risorse accettano connessioni configurate in modo personalizzato solo dopo che un client è stato autenticato e autorizzato.

   Questi percorsi di comunicazione sono impostati dal PEP.

   Le risorse potrebbero essere rilevabili solo se accedono al PEP; ciò impedisce agli aggressori di identificare i bersagli tramite la scansione o il lancio di attacchi DoS contro le risorse situate dietro i PEP.

NOTA*: alcuni componenti dell'infrastruttura di rete (ad esempio, server DNS) devono essere accessibili.*

5. IL PIANO DATI E IL PIANO DI CONTROLLO SONO LOGICAMENTE SEPARATI.

   Il PE, il PA e i PEP comunicano su una rete che è logicamente separata e non direttamente accessibile da risorse e risorse aziendali.

   Il piano dati viene utilizzato per il traffico dati delle applicazioni/servizi.

   Il PE, il PA e i PEP utilizzano il piano di controllo per comunicare e gestire i percorsi di comunicazione tra le risorse.

   I PEP devono essere in grado di inviare e ricevere messaggi sia dai dati che dai piani di controllo.

6. LE RISORSE AZIENDALI POSSONO RAGGIUNGERE LA COMPONENTE PEP.

   I soggetti aziendali devono poter accedere alla componente PEP per avere accesso alle risorse; ciò potrebbe assumere la forma di un portale Web, un dispositivo di rete o un agente software sull'asset aziendale che abilita la connessione.

7. IL PEP È L'UNICO COMPONENTE CHE ACCEDE ALLA PA COME PARTE DI UN FLUSSO AZIENDALE.

   Ogni PEP che opera sulla rete aziendale dispone di una connessione all'amministratore dei criteri per stabilire percorsi di comunicazione dai client alle risorse.

   Tutto il traffico dei processi aziendali passa attraverso uno o più PEP.

8. LE RISORSE AZIENDALI POTREBBERO NON ESSERE IN GRADO DI RAGGIUNGERE DETERMINATI PEP A CAUSA DI FATTORI OSSERVABILI.

   Ad un soggetto remoto non dovrebbe essere richiesto di utilizzare un collegamento alla rete aziendale (ad esempio, rete privata virtuale [VPN]) per accedere ai servizi utilizzati dall'azienda e ospitati da un provider di cloud pubblico (ad esempio, e-mail).

9. L'INFRASTRUTTURA UTILIZZATA PER SUPPORTARE IL PROCESSO DECISIONALE DI ACCESSO ZTA DOVREBBE ESSERE SCALABILE PER TENERE CONTO DELLE MODIFICHE NEL CARICO DEL PROCESSO.

   I PE, PA e PEP utilizzati in a ZTA diventano i componenti chiave in qualsiasi processo aziendale.

   Il ritardo o l'incapacità di raggiungere un PEP (o l'incapacità dei PEP di raggiungere il PA/PE) influisce negativamente sulla capacità di eseguire il flusso di lavoro.

   Un'azienda che implementa una ZTA deve fornire i componenti per il carico di lavoro previsto o essere in grado di scalare rapidamente l'infrastruttura per gestire un maggiore utilizzo quando necessario.

10. LE RISORSE AZIENDALI REMOTE DOVREBBERO ESSERE IN GRADO DI ACCEDERE ALLE RISORSE AZIENDALI SENZA DOVER PRIMA ATTRAVERSARE L'INFRASTRUTTURA DI RETE AZIENDALE.

Potrebbe esserci una norma che stabilisce che le risorse mobili possano non essere in grado di raggiungere determinate risorse se la risorsa richiedente si trova al di fuori del paese di origine dell'azienda.

Questi fattori potrebbero essere basati sulla posizione (geolocalizzazione o posizione di rete), tipo di dispositivo o altri criteri.

64. DEPLOYMENT SCENARIOS/USE CASES (ORGANIZZAZIONE)

Qualsiasi ambiente aziendale può essere progettato tenendo a mente i principi di ZT.

La maggior parte delle organizzazioni ha già alcuni elementi di zero fiducia nella propria infrastruttura aziendale o è in procinto di implementare policy e best practice per la sicurezza delle informazioni e la resilienza.

Diversi scenari di implementazione e casi d'uso si prestano facilmente a una ZTA.

Ad esempio, ZTA ha le sue radici in organizzazioni che sono distribuite geograficamente e/o hanno una forza lavoro altamente mobile.

Detto questo, qualsiasi organizzazione può beneficiare di un'architettura ZT.

Nei casi d'uso seguenti, ZTA non è esplicitamente indicato poiché l'impresa ha probabilmente sia infrastrutture perimetrali che possibilmente ZTA. Come discusso nella sezione 7.2, è probabile che ci sarà un periodo in cui i componenti ZTA e l'infrastruttura di rete perimetrale saranno contemporaneamente operativi in un'azienda.

ESEMPI

VEDI CAPITOLO 4 DEL NIST SP 800-207

65. THREATS ASSOCIATED WITH ZTA

1. SUBVERSION OF ZTA DECISION PROCESS
2. DENIAL-OF-SERVICE OR NETWORK DISRUPTION
3. STOLEN CREDENTIALS/INSIDER THREAT
4. VISIBILITY ON THE NETWORK
5. STORAGE OF NETWORK INFORMATION
6. RELIANCE ON PROPRIETARY DATA FORMATS
7. USE OF NON-PERSON ENTITIES (NPE) IN ZTA ADMINISTRATION

In ZTA, il PE e il PA sono i componenti chiave dell'intera azienda.

Non si verifica alcuna comunicazione tra le risorse aziendali a meno che non sia approvata e possibilmente configurata da PE e PA.

Qualsiasi amministratore aziendale, con accesso alla configurazione delle regole del PE, potrebbe eseguire modifiche non approvate o commettere errori che possano interrompere le operazioni aziendali.

Una PA compromessa potrebbe consentire l'accesso a risorse che non sarebbero state approvate (es., a un dispositivo sovvertito di proprietà personale).

La mitigazione dei rischi significa che i componenti PE e PA devono essere correttamente configurati e monitorati e qualsiasi modifica alla configurazione deve essere registrata e soggetta a verifica.

1. SUBVERSION OF ZTA DECISION PROCESS

In ZTA, il PE e il PA sono i componenti chiave dell'intera azienda.

Non si verifica alcuna comunicazione tra le risorse aziendali A MENO CHE NON SIA APPROVATA E POSSIBILMENTE CONFIGURATA DA PE E PA*; ciò significa che questi componenti* DEVONO ESSERE CONFIGURATI E MANTENUTI CORRETTAMENTE.

Qualsiasi amministratore aziendale, con accesso alla configurazione delle regole del PE, POTREBBE ESSERE IN GRADO DI ESEGUIRE MODIFICHE NON APPROVATE O COMMETTERE ERRORI CHE POSSONO INTERROMPERE LE OPERAZIONI AZIENDALI.

UN PA COMPROMESSO POTREBBE CONSENTIRE L'ACCESSO *a risorse che altrimenti non sarebbero state approvate (ad esempio, a un dispositivo sovvertito di proprietà personale).*

LA MITIGAZIONE DEI RISCHI ASSOCIATI SIGNIFICA CHE I COMPONENTI PE E PA DEVONO ESSERE CORRETTAMENTE CONFIGURATI E MONITORATI E QUALSIASI MODIFICA ALLA CONFIGURAZIONE DEVE ESSERE REGISTRATA E SOGGETTA A VERIFICA.

2. DENIAL-OF-SERVICE OR NETWORK DISRUPTION

In ZTA, la PA è il componente chiave per l'accesso alle risorse.

Le risorse aziendali non possono connettersi tra loro senza l'autorizzazione della PA e l'azione di configurazione.

Le aziende possono mitigare questa minaccia facendo in modo che l'applicazione delle policy risieda in un ambiente cloud adeguatamente protetto o venga replicata in diverse posizioni seguendo le indicazioni sulla resilienza informatica [SP 800-160v2].

È possibile che un malintenzionato possa intercettare e bloccare il traffico verso un PEP o PA da una parte o tutti gli account utente all'interno di un'azienda (ad esempio, una filiale o anche un singolo dipendente remoto); in tali casi, solo una parte dei soggetti aziendali è interessata; questo è possibile anche nelle VPN di accesso remoto legacy e non è esclusivo di ZTA.

Un provider di hosting può anche portare accidentalmente offline un PE o PA basato su cloud.

3. STOLEN CREDENTIALS / INSIDER THREAT

ZT correttamente implementate, policy di sicurezza delle informazioni e resilienza e best practice RIDUCONO IL RISCHIO *che un malintenzionato ottenga un ampio accesso tramite credenziali rubate o attacchi interni.*

Il principio ZT di "NESSUNA FIDUCIA" IMPLICITA, BASATA SULLA POSIZIONE DI RETE*, significa che* GLI AGGRESSORI DEVONO COMPROMETTERE UN ACCOUNT O UN DISPOSITIVO ESISTENTE PER OTTENERE UN PUNTO D'APPOGGIO IN UN'AZIENDA.

UNA ZTA ADEGUATAMENTE SVILUPPATA E IMPLEMENTATA DOVREBBE IMPEDIRE*, a un account o una risorsa compromessa,* DI ACCEDERE A RISORSE AL DI FUORI DELLA SUA NORMALE COMPETENZA O DEI SUOI SCHEMI DI ACCESSO*; ciò significa che* GLI ACCOUNT CON CRITERI DI ACCESSO ALLE RISORSE A CUI È INTERESSATO UN MALINTENZIONATO SAREBBERO GLI OBIETTIVI PRINCIPALI DEGLI AGGRESSORI.

Gli aggressori possono utilizzare phishing, ingegneria sociale o una combinazione di attacchi per ottenere credenziali di account importanti.

4. VISIBILITY ON THE NETWORK

Il traffico è ispezionato e registrato sulla rete e analizzato per identificare e reagire a potenziali attacchi contro l'azienda; tuttavia, una parte (forse la maggior parte) del traffico sulla rete aziendale potrebbe essere opaco agli strumenti di analisi della rete di livello 3.

Questo traffico può provenire da risorse non di proprietà aziendale (ad es. servizi appaltati che utilizzano l'infrastruttura aziendale per accedere a Internet) o applicazioni/servizi resistenti al monitoraggio passivo.

L'azienda può raccogliere metadati (ad es. indirizzi di origine e di destinazione, ecc.) sul traffico crittografato e utilizzarli per rilevare un aggressore attivo o un possibile malware che comunica sulla rete.

Le tecniche di apprendimento automatico [Anderson] possono essere utilizzate per analizzare il traffico che non può essere decrittografato ed esaminato; L'IMPIEGO DI QUESTO TIPO DI APPRENDIMENTO AUTOMATICO CONSENTIREBBE ALL'AZIENDA DI CLASSIFICARE IL TRAFFICO COME VALIDO O POTENZIALMENTE DANNOSO E SOGGETTO A RIMEDIO.

5. STORAGE OF NETWORK INFORMATION

Una minaccia correlata al monitoraggio e all'analisi del traffico di rete aziendale è il componente di analisi stesso.

Le scansioni del monitor, il traffico di rete e i metadati vengono archiviati per la creazione di criteri contestuali, analisi forensi o analisi successive, TALI DATI DIVENTANO UN OBIETTIVO PER GLI AGGRESSORI.

Se un malintenzionato riesce ad accedere con successo a queste informazioni, potrebbe essere in grado di ottenere informazioni dettagliate sull'architettura aziendale e identificare le risorse per ulteriori ricognizioni e attacchi.

Un'altra fonte di informazioni di ricognizione per un malintenzionato in un'azienda ZT È LO STRUMENTO DI GESTIONE UTILIZZATO PER CODIFICARE LE POLITICHE DI ACCESSO*; come il traffico memorizzato,* QUESTO COMPONENTE CONTIENE CRITERI DI ACCESSO ALLE RISORSE E PUÒ FORNIRE A UN MALINTENZIONATO INFORMAZIONI SU QUALI ACCOUNT È PIÙ UTILE COMPROMETTERE *(ad esempio, quelli che hanno accesso alle risorse di dati desiderate).*

6. RELIANCE ON PROPRIETARY DATA FORMATS

ZTA si basa su diverse fonti di dati per prendere decisioni di accesso, comprese le informazioni sull'oggetto richiedente, sulla risorsa utilizzata, sull'intelligence aziendale ed esterna e sull'analisi delle minacce.

Spesso, le risorse utilizzate per archiviare ed elaborare queste informazioni non hanno uno standard comune e aperto su come interagire e scambiare informazioni; QUESTO PUÒ PORTARE A CASI IN CUI UN'AZIENDA È BLOCCATA IN UN SOTTOINSIEME DI PROVIDER A CAUSA DI PROBLEMI DI INTEROPERABILITÀ.

SE UN FORNITORE AVESSE UN PROBLEMA DI SICUREZZA O UN'INTERRUZIONE, UN'IMPRESA POTREBBE NON ESSERE IN GRADO DI MIGRARE A UN NUOVO FORNITORE SENZA COSTI ESTREMI *(ad esempio, la sostituzione di più risorse) o passando attraverso un lungo programma di transizione (ad esempio, traducendo le regole della politica da un formato proprietario a un altro).*

Per mitigare i rischi associati, LE AZIENDE DOVREBBERO VALUTARE I FORNITORI DI SERVIZI SU BASE OLISTICA CONSIDERANDO FATTORI COME I CONTROLLI DI SICUREZZA DEI FORNITORI, I COSTI DI CAMBIO AZIENDALE E LA GESTIONE DEI RISCHI DELLA CATENA DI FORNITURA OLTRE A FATTORI PIÙ TIPICI COME PRESTAZIONI, STABILITÀ, *ecc.*

7. USE OF NON-PERSON ENTITIES (NPE) IN ZTA ADMINISTRATION

L'I.A. e altri agenti basati su software vengono implementati per gestire i problemi di sicurezza sulle reti aziendali; questi componenti devono interagire con i componenti di gestione di ZTA (ad esempio, il PE, il PA), a volte al posto di un amministratore umano.

Si presume che la maggior parte dei sistemi tecnologici automatizzati utilizzerà alcuni mezzi per l'autenticazione quando si utilizza un'API per i componenti delle risorse; IL RISCHIO MAGGIORE QUANDO SI UTILIZZA LA TECNOLOGIA AUTOMATIZZATA PER LA CONFIGURAZIONE E L'APPLICAZIONE DELLE POLICY È LA POSSIBILITÀ CHE FALSI POSITIVI (AZIONI INNOCUE SCAMBIATE PER ATTACCHI) E FALSI NEGATIVI (ATTACCHI SCAMBIATI PER ATTIVITÀ NORMALE) INFLUISCANO SULLA POSIZIONE DI SICUREZZA DELL'AZIENDA*; questo può essere ridotto con un'analisi di ritaratura regolare per correggere le decisioni sbagliate e migliorare il processo decisionale.*

IL RISCHIO ASSOCIATO È CHE UN MALINTENZIONATO SARÀ IN GRADO DI INDURRE O COSTRINGERE UN NPE A ESEGUIRE ALCUNE ATTIVITÀ.

L'agente software può avere UN LIVELLO INFERIORE PER L'AUTENTICAZIONE *(ad esempio, chiave API rispetto a MFA)* PER ATTIVITÀ AMMINISTRATIVE O RELATIVE ALLA SICUREZZA RISPETTO A UN UTENTE UMANO.

SE UN MALINTENZIONATO PUÒ INTERAGIRE CON L'AGENTE, POTREBBE TEORICAMENTE INDURRE L'AGENTE A CONSENTIRE ALL'AGGRESSORE UN ACCESSO PIÙ AMPIO O A ESEGUIRE ALCUNE ATTIVITÀ PER CONTO DELL'AGGRESSORE.

ESISTE IL RISCHIO CHE UN MALINTENZIONATO POSSA ACCEDERE ALLE CREDENZIALI DI UN AGENTE SOFTWARE E IMPERSONARE L'AGENTE DURANTE L'ESECUZIONE DELLE ATTIVITÀ.

65A. DATA CLASSIFICATION AND PRACTICES

Nell'ambito di un approccio Zero Trust, la gestione della sicurezza incentrata sui dati mira a migliorare la protezione delle informazioni indipendentemente da dove risiedano o con chi siano condivisi.

1) *Definire l'architettura nozionale che:*
   a. *indichi persone, sistemi, applicazioni e servizi e dispositivi degli utenti finali direttamente coinvolti o interessati dalle attività di classificazione dei dati. Questi saranno rappresentativi per lo scenario, non esaustivi.*
   b. *denoti attività del ciclo di vita dei dati come creazione/acquisizione, elaborazione, archiviazione, trasmissione/trasporto/condivisione, conservazione e distruzione dei dati. Queste attività saranno rappresentative dello scenario, non esaustive.*
   c. *evidenzi come la classificazione dei dati sia fondamentale per mitigare le preoccupazioni relative alla protezione dei dati, come la fuga di dati, in un mondo in cui i dati vengono distribuiti tra applicazioni ospitate in numerosi luoghi, elaborati su molti dispositivi e accessibili da diversi gruppi di utenti in qualsiasi momento e da qualsiasi luogo.*
   d. *non includi necessariamente l'implementazione di controlli di sicurezza per l'applicazione dei dati o per la protezione del sistema. L'intento degli scenari e delle architetture è esplorare le sfide specifiche per la classificazione dei dati e l'espressione di tali classificazioni, piuttosto che su come le classificazioni espresse possono essere tradotte dalle singole organizzazioni in controlli di sicurezza implementati.*

2) *Definire le classificazioni dei dati che saranno applicate ai set di dati specificati nello scenario.*

   Le classificazioni devono tenere conto dei regolamenti, delle leggi e delle politiche organizzative applicabili.

3) *Creare una serie di regole di gestione dei dati per specificare i requisiti di applicazione per i dati nello scenario in base alle relative classificazioni dei dati.*

   Questa serie di regole di gestione dei dati deve essere completamente compatibile con le classificazioni dei dati, per includere l'applicazione dei requisiti di protezione dei dati, requisiti di condivisione sicura dei dati, conservazione dei dati requisiti, ecc.

1. HIGH-LEVEL ARCHITECTURE

COMPONENT LIST

L'architettura di alto livello includerà, ma non si limiterà solo ad includerli, i seguenti componenti:

- ✓ **ENDPOINT***:*
  - **Dispositivi client***: vari PC (desktop o laptop) e dispositivi mobili saranno coinvolti nella creazione, archiviazione, trasmissione, conservazione e distruzione dei dati, nonché nella gestione della sicurezza incentrata sui dati. Alcuni dispositivi client saranno gestiti dall'organizzazione. Alcuni verranno utilizzati dai dipendenti dell'organizzazione, mentre altri verranno utilizzati da persone di altre organizzazioni.*

- **App per dispositivi client***: i dispositivi client avranno app COTS (Commercial Off The Shelf) utilizzate per attività del ciclo di vita dei dati, come software di elaborazione testi e software client di posta elettronica.*
- **Dispositivi aggiuntivi***: esempi di tipi di dispositivi aggiuntivi che potrebbero essere utilizzati sono le stampanti in rete e i dispositivi Internet of Things (IoT).*

✓ **DISPOSITIVI DI RETE/INFRASTRUTTURA***: l'architettura includerà dispositivi come firewall, router o switch necessari per la funzionalità di rete e la limitazione del traffico di rete, nonché il software per la gestione di tali dispositivi.*

✓ **SERVIZI E APPLICAZIONI***: l'architettura includerà diversi tipi di servizi e applicazioni coinvolti nelle attività del ciclo di vita dei dati per uno o più scenari. Di seguito sono riportati esempi di possibili tipi di servizi e applicazioni:*

- **SERVIZI / APPLICAZIONI AZIENDALI***: posta elettronica, collaborazione, condivisione di file, conferenze web, backup di file/dati, archivi di codice, sistemi di gestione dei contenuti Servizi/Applicazioni dati: elaborazione dei dati, analisi dei dati, intelligenza artificiale/servizi di apprendimento automatico.*
- **SERVIZI / APPLICAZIONI AZIENDALI***: una varietà di applicazioni aziendali da sistema a sistema e da uomo a sistema, sia COTS che scritte su misura, comprese quelle che producono e/o consumano dati.*

✓ **SOLUZIONI DI CLASSIFICAZIONE DEI DATI***: l'architettura includerà diversi tipi di componenti utilizzati per eseguire responsabilità di classificazione dei dati, come la scoperta dei dati, l'inventario, l'analisi, la classificazione e l'etichettatura.*

DESIRED SECURITY CAPABILITIES

Sviluppare un disegno di riferimento e implementazione utilizzando la tecnologia disponibile in commercio che soddisfi le seguenti caratteristiche:

✓ Tutti i dati sono rilevati e analizzati per determinare come dovrebbero essere classificati.

✓ La creazione, la modifica e l'eliminazione di tutte le regole di classificazione e gestione dei dati è riservata esclusivamente al personale autorizzato, con tutte le azioni registrate e verificabili e con tutte le comunicazioni protette.

✓ Per tutte le classificazioni dei dati e le serie di regole per la gestione dei dati, esiste un meccanismo per verificare l'integrità della politica o della serie di regole.

✓ Etichette o tag di classificazione dei dati sono assegnati a tutti i dati.

✓ Per tutte le etichette o tag di classificazione dei dati assegnati ai dati, esiste un meccanismo per verificare l'integrità dell'etichetta o del tag.

PARTE XII: TELEMEDICINA O TELEHEALTH [RPM]

[Rif.: NIST SP 1800-30; NIST – Mitigating Cybersecurity Risk in Telehealth Smart Home Integration]

66. INTRODUZIONE

Sempre più spesso, le organizzazioni di assistenza sanitaria (Healthcare Delivery Organizations - HDO) si affidano alle capacità di telemedicina e monitoraggio remoto dei pazienti (Remote Patient Monitoring - RPM) per curare i pazienti a casa. RPM è conveniente ed economico e il suo tasso di adozione è aumentato. Tuttavia, senza adeguate misure di privacy e sicurezza informatica, persone non autorizzate possono esporre dati sensibili o interrompere i servizi di monitoraggio dei pazienti.

Le soluzioni RPM coinvolgono più attori come partecipanti all'assistenza clinica di un paziente. Questi attori includono HDO, fornitori di piattaforme di telemedicina e i pazienti stessi. Ogni partecipante utilizza, gestisce e mantiene diversi componenti tecnologici all'interno di un ecosistema interconnesso e ciascuno è responsabile della salvaguardia del proprio componente contro minacce e rischi unici associati alle tecnologie RPM 60.

Questa guida pratica presuppone che l'HDO si impegni con un fornitore di piattaforma di telemedicina che è un'entità separata dall'HDO e dal paziente. Il fornitore della piattaforma di telemedicina gestisce un'infrastruttura, applicazioni e una serie di servizi distinti. Il fornitore della piattaforma di telemedicina si coordina con l'HDO per fornire, configurare e distribuire i componenti RPM a casa del paziente e garantisce una comunicazione sicura tra il paziente e il medico.

66A. SCOPE

[Rif.: NIST – Mitigating Cybersecurity Risk in Telehealth Smart Home Integration]

This project's objective is to identify and mitigate cybersecurity and privacy risks based on patient use of smart home devices interfacing with patient information systems.

While a key project focal point provides guidance for safeguarding the use of smart home devices, safeguards will be limited to the use of the devices, and will not address device manufacture, hardware, operating systems, or software development techniques that may be used to enable clinical access functionality.

66B. SCENARIOS

SCENARIO 1: PROGRAMMAZIONE DELLA VISITA DEL PAZIENTE

La pianificazione delle visite del paziente indagherà quando un paziente esprime il desiderio di programmare una visita con il proprio fornitore di cure.

Il dispositivo Smart Home può avere funzionalità codificate che riconoscono il comando vocale e attivano la logica dell'applicazione.

La logica dell'applicazione può aprire una sessione in rete con un sistema di informazioni sul paziente.

Il sistema di informazione del paziente fornisce il feedback del paziente consigliando le date e gli orari disponibili per una visita.

La logica dell'applicazione fornisce una risposta audio che consente al paziente di selezionare e prenotare un orario con un operatore sanitario.

Dopo che il paziente ha selezionato una data e una fascia oraria con comandi verbali, la logica applicativa si interfaccia con un sistema di schedulazione.

Le interazioni avverranno su Internet pubblico.

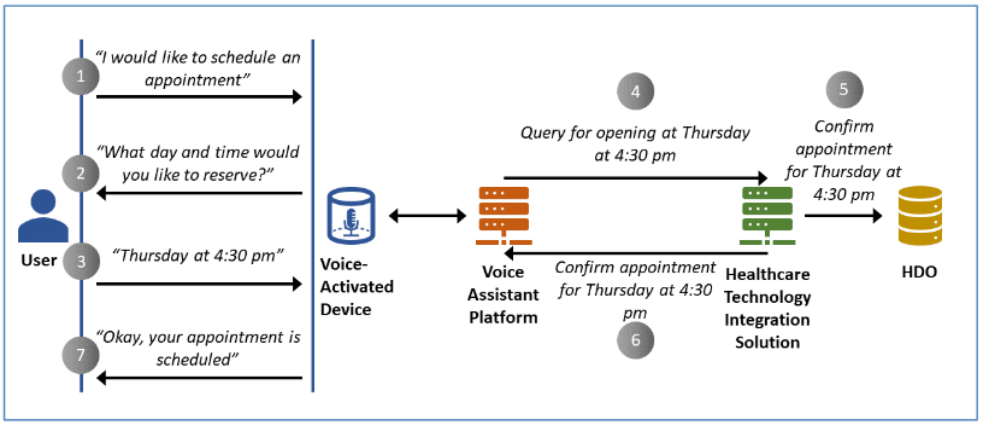
La Figura 2-1 mostra un'interazione ipotetica che consente ai pazienti di interagire con il dispositivo smart home per programmare una visita di persona.

Il potenziale flusso di dati ritiene che i comandi vocali possano offrire un'interfaccia utente a un'applicazione ospitata da una piattaforma di terze parti.

L'applicazione può interrogare i sistemi di calendario, fornire feedback al paziente e programmare la visita nei sistemi HDO.

Risultati e feedback vengono trasmessi in audio sul dispositivo smart home del paziente.

Figure 2-1 Patient Visitation Scheduling



SCENARIO 2: NUOVA PRESCRIZIONE PER IL PAZIENTE

Il dispositivo smart home applica funzionalità codificate per ricevere il comando vocale e attiva la logica dell'applicazione che stabilisce una sessione di rete con un sistema di informazione del paziente.

Il sistema informativo del paziente identificherà le prescrizioni del paziente.

Il paziente identificherà la prescrizione che vorrebbe avere nuovamente.

Il sistema di informazione del paziente avrà un'interfaccia per consentire al medico di approvare o rifiutare una richiesta.

La conferma include lo stato di approvazione o rifiuto e i farmaci sono inoltrati al paziente.

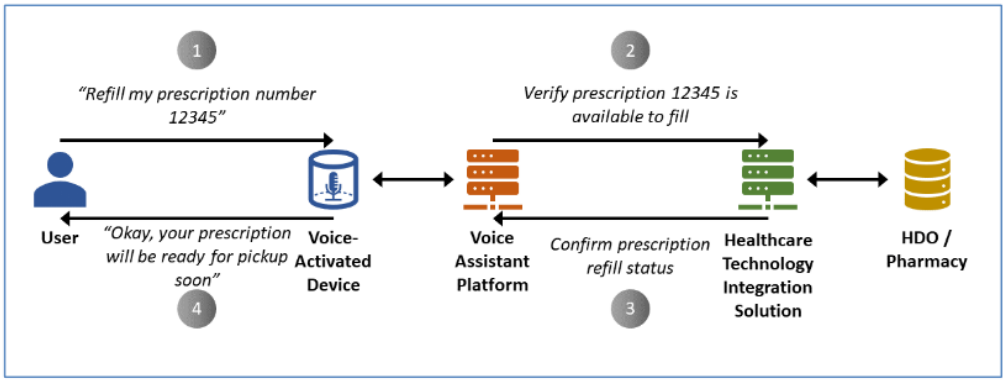
I risultati possono essere presentati tramite audio.

La Figura 2-2 descrive uno scenario ipotetico in cui un paziente può utilizzare un dispositivo smart home per una nuova prescrizione.

Il potenziale flusso di dati considera che i comandi vocali possano offrire un'interfaccia utente a un'applicazione ospitata da una piattaforma di terze parti.

L'applicazione può interagire con i sistemi della farmacia per determinare se una prescrizione può essere reinserita fornendo un feedback al paziente come audio sul dispositivo.

Figure 2-2 Patient Prescription Refill



SCENARIO 3: CHECK-IN DEL PAZIENTE

Il check-in del paziente presuppone che esso possa avere una prescrizione che richieda un'azione regolare e un feedback fornito dal paziente. Un esempio della prescrizione potrebbe essere il monitoraggio dei livelli di dolore.

Un paziente vocalizza che risponde alla richiesta prescritta.

Il dispositivo smart home applica funzionalità codificate per ricevere il comando vocale e attiva la logica dell'applicazione che stabilisce una sessione con un sistema di informazione del paziente.

Il sistema di informazione del paziente consente a un medico di fornire, ad esempio, un questionario.

Il sistema informativo del paziente accede al questionario. L'interrogazione sarà programmatica, con domande fornite al paziente via audio.

Le risposte del paziente sono registrate dal sistema.

Le interazioni avverranno su Internet pubblico.

La Figura 2-3 descrive uno scenario ipotetico in cui un paziente può partecipare a una prescrizione.

La prescrizione può includere la risposta a domande che misurano i livelli di dolore percepito dal paziente su base giornaliera.

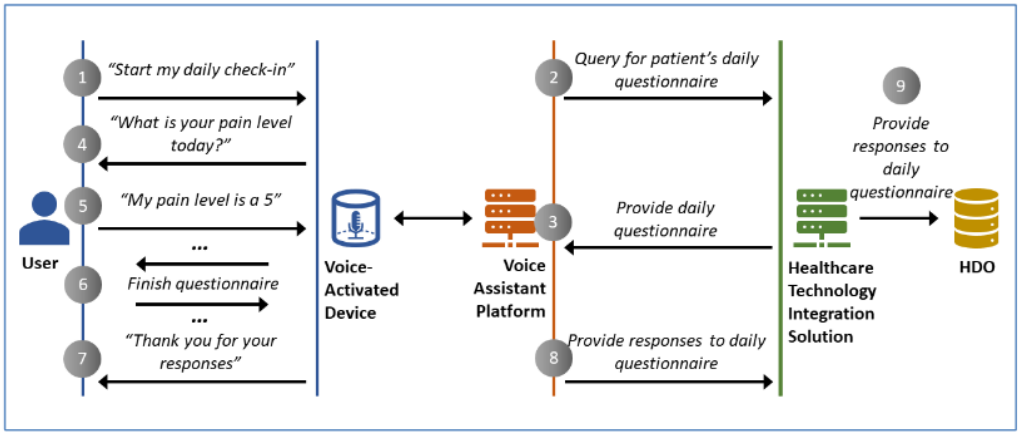
I pazienti possono iniziare il regime quotidiano utilizzando i comandi vocali sul proprio dispositivo smart home.

È possibile avviare un'applicazione che fornisca un questionario come una serie di domande audio.

I pazienti possono rispondere alle domande utilizzando l'interazione vocale.

L'applicazione registra le informazioni sui sistemi clinici gestiti da HDO utilizzati per gestire il regime del paziente.

Figure 2-3 Patient Regimen Check-In



66C. HIGH LEVEL ARCHITECTURE

Figure 3-1 describes high-level architecture posits for four domains where components operate to enable telehealth smart home integration.

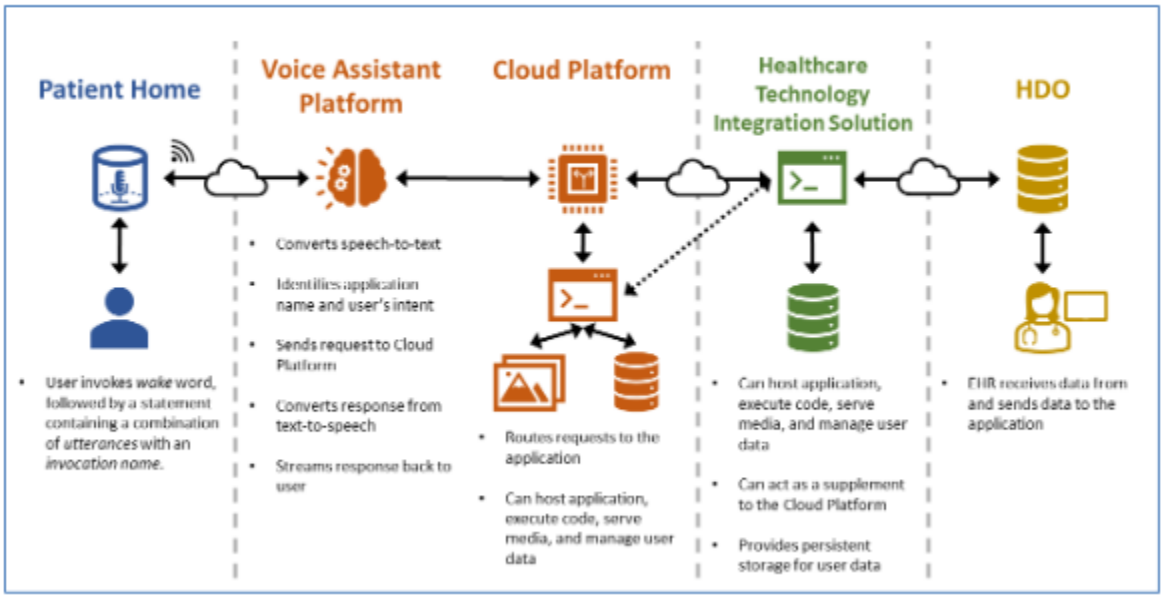
1st. THE FIRST DOMAIN *is the patient home.*

2nd. THE SECOND DOMAIN *operates as a cloud service provider. The cloud service provider has a voice assistant platform that receives voice input from smart home devices and uses natural language processing technology to use voice input as a user interface to application logic. Application logic may be hosted in a cloud platform.*

3rd. THE THIRD DOMAIN *is a healthcare technology integration solution. There may exist application logic that does not require implementing the third domain. For example, application logic may exist that allows patients to query generic data stores that provide publicly available information. Examples of this may be medical databases that implement decision trees allowing the patient to understand symptoms associated with ailments, identifying the address of healthcare facilities, or receiving medical condition awareness that is not specific to the patient.*

4th. THE FOURTH DOMAIN *is the HDO. HDOs may host patient information and clinical systems, patient portals, electronic record systems, or other systems.*

Figure 3-1 High-Level Architecture



COMPONENT LIST

Per maggiori dettagli delle COMPONENT LIST *dei singoli* DOMINI, *vedere capitolo 3 del manuale NIST – Mitigating Cybersecurity Risk in Telehealth Smart Home Integration*

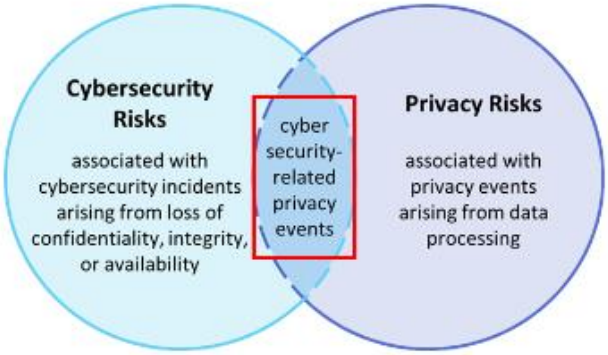
DESIRED REQUIREMENTS

The NCCoE applies two frameworks to identify potential cybersecurity and privacy outcomes for this project: the NIST Cybersecurity Framework and the NIST Privacy Framework.

For this project, the NCCoE selects privacy-relevant outcomes based on the intersection of the two frameworks.

Figure 3-2 depicts the overlap between the NIST CYBERSECURITY AND PRIVACY FRAMEWORKS. GRAPHICALLY, *the diagram uses a red box that highlights the common concepts between the two Frameworks as explored in the scope of this build.*

Figure 3-2 Cybersecurity and Privacy Risk Relationship



Note: Vedi anche il capitolo "2. Quali differenze e punti in comune con la Privacy" nel presente manuale.

Le attività necessarie per lo sviluppo del RISK MANAGEMENT *sono indicate nel capitolo* DESIRED REQUIREMENTS *del manuale NIST – Mitigating Cybersecurity Risk in Telehealth Smart Home Integration.*

66D. SECURITY MAP CONTROL

Table 5-1 maps the characteristics of the commercial products that the NCCoE will apply to this cybersecurity challenge to the applicable standards and best practices described in the Framework for Improving Critical Infrastructure Cybersecurity, and to other NIST activities.

TABLE 5-1 SECURITY CONTROL MAP

*Nel capitolo "*5 SECURITY CONTROL MAP*" è indicato l'elenco completo dei controlli per ogni singola funzione stabiliti dagli standard internazionali.*

NIST Cybersecurity Framework v1.1				Sector-Specific Standards and Best Practices		
Function	Category	Subcategory	NIST SP 800-53 Revision 5	IEC TR 80001-2-2	HIPAA Security Rule	ISO/IEC 27001
IDENTIFY (ID)	Risk Assessment (ID.RA)	ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk	CA-2 CA-7 PM-16 PM-28 RA-2 RA-3	SGUD	45 C.F.R. §§ 164.308(a)(1)(ii)(A) 164.308(a)(1)(ii)(B) 164.308(a)(1)(ii)(D) 164.308(a)(7)(ii)(D) 164.308(a)(7)(ii)(E) 164.316(a)	A.12.6.1

67. RISK ASSESSMENT

THREATS

*Vedi Capitolo "*3.4.1 THREATS" DEL NIST SP 1800-30

Le tabelle seguenti descrivono gli eventi e considerano la probabilità di variazione in base a questo contesto. Notare che i valori assegnati sono fittizi.

La probabilità è classificata utilizzando un intervallo che va da molto basso a molto alto, coerente con un modello descritto nell'Appendice G del NIST 800-30. Di seguito è riportato un abstract della tabella. I valori qualitativi dalla descrizione della probabilità di minaccia.

Vedi TABLE C-2 ASSESSMENT SCALE: LIKELIHOOD OF THREAT EVENT INITIATION NELLA APPENDICE C.

La Tabella 3-1 di seguito è un esempio di tassonomia delle minacce applicata all'intero ecosistema RPM. La tassonomia delle minacce utilizza una classificazione di RISERVATEZZA (C - CONFIDENTIALITY), INTEGRITÀ (I - INTEGRITY) E DISPONIBILITÀ (A - AVAILABILITY), *l'evento di minaccia considerato e una descrizione dell'evento di minaccia. Sebbene la tassonomia delle minacce fornisca una vista panoramica delle minacce, le organizzazioni potrebbero voler eseguire la modellazione delle minacce per determinare l'applicazione contestuale delle minacce. Minacce e rischi nell'Appendice C descrive i concetti su come esaminare le minacce contestualizzate.*

Table 3-1 Threat Taxonomy

C, I, A	THREATS	DESCRIPTION
C	*Phishing*	*Phishing attacks are a form of social engineering, where the attacker presents themselves as a trusted party to gain the confidence of the victim*
I, A	*Malware*	*Malware is unauthorized code that may be introduced to a system. It performs unintended actions that may disrupt normal system function. Malware may masquerade as desirable apps or applications.*
I, A	*Commad and Control*	*Command and control attacks may begin with deployment of malware. Malware may allow a system to be operated remotely by unauthorized entities. Should a system fall victim to a command and control attack, that system may then be used as a pivot point to attack other components, either within the organization's infrastructure or as a point where attacks may be launched against other organizations*
A	*Ransomware*	*Ransomware is a form of malware that disrupts access to system resources. A typical form of ransomware involves the malware employing encryption that disables a legitimate system user from accessing files. Ransomware attacks generally involve a demand for payment to restore files. Payment does not ensure that the attacker will decrypt files, however.*
C	*Credential escalation*	*Credential escalation attacks seek to take user account capabilities and extend those to a privileged level of capability*
I, A	*Operating system or application disruption*	*The operating system or application may be adversely affected by malicious actors that successfully implement malware on the target device. Data may be altered, or the device or application may not function properly.*

C	*Data exfiltration*	*Malicious actors may be able to retrieve sensitive information from vulnerable devices. Malware may be used for this purpose.*
A	*DoS Attack*	*Flooding network connections with high-volume traffic to disrupt communication in patient home, between home and telehealth platform, or between telehealth platform provider and HDO. Such type of attack could also be used to damage a device, e.g., though accelerated battery depletion*
I	*Transmitted data manipulation*	*Unauthorized individuals may intercept and alter data transmissions.*

Vedi tabelle C-4, 6, 7, 9, 10, 11, 12, 13, 14 del cap. C-7.1 del NIST SP 1800-30

BUSINESS PROCESSES

Diverse funzioni sono eseguite con il sistema RPM *eseguite nei rispettivi ambiti.*

I dati dei pazienti sono raccolti e archiviati e i pazienti interagiscono dalla propria abitazione; le comunicazioni tra pazienti e team di assistenza sono instradate attraverso il fornitore della piattaforma di telemedicina, che è ospitata nel cloud; i medici ricevono e interagiscono con i dati dei pazienti dall'HDO.

La Tabella C-7 identifica questi e altri processi aziendali che supportano le funzioni RPM.

VULNERABILITIES

La tabella nella sezione C-6 dell'Appendice C, Minacce e rischi, *elenca tali vulnerabilità utilizzando un approccio olistico e rappresenta le vulnerabilità che questo progetto ha identificato e per le quali offre una guida.*

La tabella 3-2 di seguito mostra la tassonomia problematica delle azioni sui dati identificata per l'intero ecosistema RPM. Questa tassonomia problematica dell'azione dei dati utilizza una designazione di:

- PREVEDIBILITÀ (P - PREDICTABILITY): *consentire ipotesi affidabili da parte di individui, proprietari e operatori sui dati e sulla loro elaborazione da parte di un sistema, prodotto o servizio;*
- GESTIBILITÀ (M - MANAGEABILITY): *fornire la capacità di amministrazione granulare dei dati, inclusa l'alterazione, la cancellazione e la divulgazione selettiva*;
- DISASSOCIABILITÀ (D - DISASSOCIABILITY): *consentire il trattamento di dati o eventi senza associazione a persone o dispositivi al di fuori delle esigenze funzionali del sistema;*

l'azione problematica sui dati considerata; e la descrizione dell'azione sui dati problematici. Sebbene la tassonomia dell'azione problematica sui dati fornisca una visione panoramica dell'azione sui dati problematici, un'organizzazione potrebbe voler eseguire una valutazione del rischio per determinare l'applicazione contestuale dell'azione sui dati problematici.

La discussione su Rischi e azioni sui dati problematici nell'Appendice *D introduce la PRAM e fornisce un'analisi più dettagliata*

Table 3-2 Problematic Data Action Taxonomy

P, M, D	PROBLEMATIC DATA ACTION	DESCRIPTION
P, M	*Distortion*	*Inaccurate or misleadingly incomplete data are used or disseminated. Distortion can present users in an inaccurate, unflattering, or disparaging manner, opening the door for stigmatization, discrimination, or loss of liberty. RPM context: Incorrect or unintended use of biometric devices may introduce data quality issues into the RPM environment, resulting in inaccurate or incomplete data being used to make decisions regarding patient care*
M	*Insecurity*	*Lapses in data security can result in various problems, including loss of trust, exposure to economic loss and other identity theft-related harms, and dignity losses.* *RPM context: Biometric data and patient health information flows through various entities in the RPM solution, each of which plays a role in protecting the information.*
D, M	*Reidentication*	*De-identified data, or data otherwise disassociated from specific individuals, becomes identifiable or associated with specific individuals again. It can lead to problems such as discrimination, loss of trust, or dignity losses. RPM context: Disassociated processing is intentionally used during some dataflows within the RPM solution to mitigate the risk of exposing identifiable patient information to vendors, administrators, and other practitioners that are outside of the patient's care team.*
P, M	*Unanticipated revelation*	*Data reveals or exposes an individual or facets of an individual in unexpected ways. Unanticipated revelation can arise from aggregation and analysis of large and/or diverse data sets. Unanticipated revelation can give rise to dignity losses, discrimination, and loss of trust and autonomy.* *RPM context: Using one or more biometric devices can indicate potential health problems for which a patient is being monitored to others beyond the patient's healthcare provide.*

Table C-8 Vulnerability Taxonomy

VULNERABILITY DESCRIPTION	VULNERABILITY SEVERITY	PREDISPOSING CONDITION	PERVASIVENESS OF PREDISPOSING CONDITION
Out of Date software	*High*	*Systems may not have patches deployed in a timely fashion, or software may not be validated to assure that applications may operate appropriately should the underlying operation system receive new updates.*	*High*
Permissive configuration settings	*High*	*Underlying operating systems or security components (e.g., firewall) may have configuration settings that allow actions that exceed the minimum necessary to operate the application.*	*High*
Unmanaged or improperly managed credentials	*High*	*Applications may use service or other privileged accounts to operate, or operating systems may have privileged accounts that have expansive access to the host system(s). These access privileges may exceed the minimum necessary to operate applications.*	*High*
Unprotected data	*High*	*Data on systems may lack restrictions that limit accessibility*	*High*
Failing or missing integrity or authenticity verification	*High*	*Data path may lack end-to-end data integrity or authenticity verification.*	*High*

CYBERSECURITY RISK AND PRIVACY RISK

La Tabella 3-3, Tassonomia dei rischi di sicurezza informatica descrive i rischi di sicurezza informatica di alto livello che influiscono sull'ambiente RPM.

La tabella della tassonomia dei rischi cattura i rischi chiave, assegnando dove il rischio può avere un impatto sull'organizzazione attraverso una dimensione di Riservatezza, Integrità e Disponibilità (CIA - Confidentiality, Integrity and Availability).

TABLE 3-3 CYBERSECURITY RISK TAXONOMY

C, I, A	RISK	DESCRIPTION	RISK LEVEL
C	*Fraudulent use of health-related information*	*Health-related information may be used for several different fraudulent means, such as identity theft, insurance fraud, or extortion.*	*Medium*
I	*Patient diagnoses disrupted based on timeliness disruption, leading to patient safety concerns*	*Unavailability or significant delay in delivering biometric data may negate the benefits of remote patient monitoring. Clinicians may not be able to provide appropriate care should biometric data transmission be disrupted.*	*Medium*
I	*Incorrect patient diagnosis due to change of data*	*A critical patient event is missed due to changes in the data stream between device and HDO.*	*High*
A	*Process disruption due to ransomware*	*Ransomware may prevent normal device operations. Data may be irretrievable and therefore, may prevent clinical care.*	*High*
I, A	*Systemic disruption due to component compromise*	*Disruptions to the system that affect its availability or integrity may compromise the benefits derived from remote patient monitoring.*	*High*
I	*Clinician misdiagnosis*	*If data are altered inappropriately, clinicians may make inaccurate diagnoses, resulting in patient safety issues.*	*High*

La Tabella 3-4, Tassonomia dei rischi per la privacy, descrive i rischi per la privacy di alto livello che influiscono sull'ambiente RPM, inoltre, cattura i rischi chiave, assegnando dove il rischio può avere un impatto sugli individui, nelle aree di prevedibilità, gestibilità e dissociabilità.

I livelli di rischio per la privacy per gli individui dipendono dal contesto della distribuzione della soluzione RPM specifica e non sono inclusi.

TABLE 3-4 PRIVACY RISK TAXONOMY

P, M, D	RISK	PROBLEMATIC DATA ACTION
M	*Unauthorized individuals may access data on devices*	*Insecurity: Data not protected at rest or in transit*
P, M	*Biometric device types can indicate patient health problems that individuals would prefer not to disclose beyond their healthcare provider*	*Unanticipated revelation: Biometric device types can indicate patient health problems individuals would prefer not to disclose beyond their healthcare provider.*
P, M	*Incorrect data capture of readings by devices may impact quality of patient care*	*Distortion: Device misuse may cause failure to monitor patients in accordance with their healthcare plan.*
D, M	*Aggregated data may expose patient information*	*Re-identification: Associating biometric data with patient identifiers can expose health conditions.*
P, M	*Exposure of patient information through multiple providers of system components*	*Unanticipated Revelation: Data sharing across parties can increase the risk of exposure due to confidentiality-related incidents, which can reveal patient health information in ways or to parties that the individual may not expect.*

SECURITY CONTROL MAP

La mappatura ha stabilito un set iniziale di funzioni, categorie e sottocategorie di controllo appropriate, dimostrando come le sottocategorie del Cybersecurity Framework selezionate si mappano ai controlli in NIST SP 800-53, nonché al NIST NICE Framework, NIST SP 800-513.

La tabella elenca anche gli standard specifici del settore e le migliori pratiche di altri organismi di normazione (ad esempio, la INTERNATIONAL ELECTROTECHNICAL COMMISSION [IEC] TECHNICAL REPORTS [TR], L'INTERNATIONAL ORGANIZATION FOR STANDARDIZATION [ISO]*), nonché* L'HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT [HIPAA].

La mappa dei controlli di sicurezza, mostrata nella Tabella 3-5, identifica un set di controlli, inclusi quelli implementati in modo specifico nella build del laboratorio, così come il set pervasivo di controlli come descritto nella Sezione 5.2, Controlli pervasivi, che gli HDO dovrebbero distribuire.

I professionisti dovrebbero fare riferimento a NIST SP 1800-24, Securing Picture Archiving and Communication System (PACS), Appendice C per un'ulteriore descrizione dei controlli pervasivi.

Vedi CAPITOLO 3.5 SECURITY CONTROL MAP DEL NIST SP 1800-30

TECHNOLOGIES

La Tabella 3-7 elenca tutte le tecnologie utilizzate in questo progetto e fornisce una mappatura tra il termine dell'applicazione generica, il prodotto specifico utilizzato e i controlli di sicurezza forniti dal prodotto.

Fare riferimento alla Tabella 3-5 per una spiegazione dei codici della sottocategoria NIST Cybersecurity Framework e fare riferimento alla Tabella 3-6 per la spiegazione dei codici della sottocategoria NIST Privacy Framework.

Sebbene questa guida pratica rilevi che la soluzione RPM viene distribuita in tre domini, gli HDO devono riconoscere che la responsabilità della gestione del rischio rimane con l'HDO.

La mitigazione del rischio può essere ottenuta mediante strumenti o pratiche, in cui le misure di privacy e sicurezza vengono applicate come appropriato in ciascuno dei domini.

Per questa guida pratica, il fornitore della piattaforma di telemedicina è un'entità di terze parti, distinta dal paziente e dall'HDO.

I fornitori di piattaforme di telemedicina dovrebbero implementare un ambiente di controllo adeguato che consenta al fornitore di piattaforme di telemedicina di collaborare con gli HDO nella fornitura di soluzioni RPM. L'ambito di questa guida pratica si concentra sui controlli che vengono distribuiti nell'HDO.

Il fornitore della piattaforma di telemedicina è un'entità separata e dovrebbe garantire che siano implementati controlli adeguati nel proprio ambiente.

Inoltre, i fornitori di piattaforme di telemedicina devono garantire che le apparecchiature distribuite a casa del paziente includano misure di salvaguardia adeguate.

Vedi TABLE 3-7 PRODUCTS AND TECHNOLOGIES DEL NIST SP 1800-30

PERVASIVE CONTROLS

Vedi NIST SP 1800-24.

TELEHEALTH PLATFORM PROVIDERS

Attività dei TELEHEALTH PLATFORM PROVIDERS*:*

1) *configurano, mantengono e gestiscono i dispositivi distribuiti nel dominio della casa del paziente;*
2) *forniscono dispositivi ai pazienti che sono stati iscritti a un programma RPM dal loro HDO;*
3) *eseguono la gestione delle risorse per i dispositivi forniti e quindi indirizzano ID.AM-1, ID.AM-2, ID.AM-4, ID.AM-5, ID.IM-P1, ID.IM-P2 e ID.IM-P7. I fornitori di piattaforme di telemedicina sono responsabili di rivolgersi a ID.RA-1;*
4) *autenticano le sessioni in base all'identificatore del dispositivo.*

Quando i pazienti inviano o trasferiscono dati da dispositivi biometrici, i dati vengono instradati al fornitore della piattaforma di telemedicina.

Il TELEHEALTH PLATFORM PROVIDER *riceve i dati e li mette a disposizione dei medici e degli utenti del sistema tramite un portale.*

I portali utilizzano identificatori univoci per le credenziali (ad esempio, nome utente/password) e garantiscono che le connessioni al portale siano protette utilizzando Transport Layer Security (TLS) 1.2.

Per questa guida pratica, i TELEHEALTH PLATFORM PROVIDERS *hanno fornito dispositivi biometrici e tablet che utilizzavano comunicazioni di dati cellulari; i dispositivi non erano esplicitamente autorizzati ad accedere alle reti Wi-Fi.*

La rimozione della funzionalità Wi-Fi ha separato la comunicazione RPM dal traffico di rete che potrebbe essere stato presente nel dominio di casa del paziente.

Questa guida pratica ha utilizzato dispositivi che erano equipaggiati per comunicare su 4G Long-Term Evolution (LTE), che utilizza la crittografia asimmetrica tra il dispositivo e la torre cellulare.

Ulteriori indagini sulla protezione dei dati in transito non sono state determinate in questa guida pratica.

Il TELEHEALTH PLATFORM PROVIDER *si rivolge a PR.AC-1, PR.AC-4, PR.DS-1, PR.DS-2, PR.DS -4, PR.DS-6, PR.PT-1, PR.PT-3, PR.PT-4, PR.AC-P1, PR.AC-P4, PR.DS-P1, PR.DS-P2 , PR.DS-P4, PR.DS-P6, CT.DM-P8, PR.PT-P2 e PR.PT-P3.*

Questa guida pratica ha implementato i servizi di provider di piattaforme di telemedicina con Accuhealth e Vivify Health.

RISK ASSESSMENT (ID.RA AND ID.RA-P)

Questa guida pratica ha implementato strumenti che affrontano elementi di ID.RA-5 (threats, vulnerabilities, likelihoods and impacts sono usati per determinare il rischio) e ID.RA-P4.

Questa guida pratica ha implementato Tenable.sc per affrontare la gestione delle vulnerabilità.

Tenable include la scansione delle vulnerabilità e il dashboard che visualizzano le vulnerabilità identificate con punteggi e altre metriche che consentono ai tecnici della sicurezza di stabilire le priorità.

I TELEHEALTH PLATFORM PROVIDERS:

1) *dispongono di infrastrutture e strutture organizzative separate che richiedono approcci simili;*
2) *ospitano i propri servizi con varie implementazioni;*
3) *implementano soluzioni simili per i loro ambienti.*

IDENTITY MANAGEMENT, AUTHENTICATION AND ACCESS CONTROL (PR.AC AND PR.AC-P) PROTECTIVE TECHNOLOGY (PR.PT-P)

Questa guida pratica ha considerato molte delle sottocategorie di gestione delle identità come parte di una serie di controlli pervasivi discussi in NIST SP 1800-24, Securing Picture Archiving and Communication System (PACS).

Gli HDO e i TELEHEALTH PLATFORM PROVIDERS *dovrebbero applicare soluzioni simili per affrontare la gestione delle identità umane, dei dispositivi e dei sistemi. Le soluzioni campione sono fornite in NIST SP 1800-24.*

Estendendo i concetti di zona della rete descritti in NIST SP 1800-8, Securing Wireless Infusion Pumps nelle Healthcare Delivery Organizations, questa guida pratica ha implementato le VLAN con set di funzionalità firewall utilizzando Cisco Firepower Threat Defense.

Questa guida pratica si rivolge a PR.AC-5 implementando VLAN che rappresentano le zone di rete trovate all'interno di un HDO.

Il NIST Cybersecurity Framework implementa la gestione dell'identità, l'autenticazione e il controllo degli accessi sotto la funzione Protect utilizzando la categoria PR.AC.

All'interno dell'HDO, questa guida pratica implementa PR.AC-5 utilizzando Cisco Firepower per stabilire zone di rete come un insieme di VLAN.

Le zone di rete assicurano che i componenti di ciascuna zona non abbiano fiducia implicita, e quindi i compromessi sugli endpoint trovati in una zona sono limitati nella loro capacità di influenzare i dispositivi che operano in altre zone.

Questa guida pratica ha implementato tre strumenti Cisco principali per l'ambiente HDO: Cisco Firepower, Cisco Umbrella e Cisco Stealthwatch. Come notato, questa guida pratica ha utilizzato Firepower per creare e gestire le VLAN all'interno dell'ambiente.

Cisco Firepower include un dashboard di gestione centrale che ha consentito ai tecnici della sicurezza di configurare e gestire altre funzionalità all'interno della suite di strumenti Cisco.

Firepower include anche funzionalità di rilevamento delle intrusioni e visibilità sul traffico di rete e analisi di rete che hanno consentito agli ingegneri di rilevare e analizzare eventi, monitorare la rete e rilevare codice dannoso e quindi affrontare DE.AE-2, DE.CM-1 e DE.CM- 4. Cisco Firepower ha indirizzato PR.AC-5, PR.PT-4, PR.AC-P5 e PR.PT-P3.

Le credenziali AD hanno fornito agli ingegneri l'autenticazione per diversi componenti distribuiti in laboratorio. L'implementazione di AD del laboratorio riguarda PR.AC-1, PR.AC-4, PR.AC-P1 e PR.AC-P4.

Il fornitore della piattaforma di telemedicina assicura che PR.AC-5, PR.AC-6, PR.AC-7, PR.AC-P5 e PR.AC-P6 siano soddisfatti gestendo i componenti che vengono distribuiti a casa del paziente.

I componenti RPM forniti da Accuhealth per la casa del paziente utilizzano un percorso di comunicazione cellulare in cui persone non autorizzate non possono rimuovere o alterare le schede SIM.

Il percorso di comunicazione dati cellulare assicura che i componenti RPM siano separati dai dispositivi non attendibili che possono operare a casa del paziente e quindi implementa PR.AC-5 e PR.AC-P5.

I pazienti arruolati in RPM sono predeterminati dall'HDO e il fornitore della piattaforma di telemedicina fornisce i componenti RPM a un gruppo di pazienti noto e stabilito.

Gli HDO che arruolano pazienti nel programma RPM affrontano parzialmente PR.AC-1 e PR.AC-P1.

I medici che identificano i pazienti possono svolgere un'attività di verifica dell'identità, mentre i TELEHEALTH PLATFORM PROVIDERS *possono completare le attività PR.AC-1 e PR.AC-P1 creando account o record relativi al paziente e all'apparecchiatura RPM che il paziente riceve.*

I dispositivi biometrici forniti dal paziente (ad es. "Porta il tuo dispositivo") sono stati esclusi dall'architettura di questa guida pratica. Il TELEHEALTH PLATFORM PROVIDER *gestisce i componenti distribuiti a casa dei pazienti e garantisce quindi che PR.AC-6 e PR.AC-P6 siano indirizzati.*

Il TELEHEALTH PLATFORM PROVIDER *configura i dispositivi per includere autenticazioni che applicano l'autenticazione dei componenti.*

Per questa guida pratica, sono autenticati solo i dispositivi biometrici gestiti dai fornitori di piattaforme di telemedicina.

Questo implementa PR.AC-7 e PR.AC-P6.

Le case dei pazienti possono includere altri dispositivi, come i dispositivi di proprietà personale, che non fanno parte dell'ecosistema RPM.

I dispositivi non gestiti da TELEHEALTH PLATFORM PROVIDER *non dispongono di credenziali di autenticazione per la soluzione RPM.*

DATA SECURITY (PR.DS AND PR.DS-P)

Questa guida ha implementato PR.DS-2 e PR.DS-P2 per garantire che i dati in transito siano protetti.

Gli HDO che si collegano a console ospitate nel cloud utilizzando TLS 1.2.

Il TELEHEALTH PLATFORM PROVIDER *ha assicurato l'implementazione di PR.DS-3 e PR.DS-P3 per i dispositivi biometrici RPM distribuiti a casa del paziente.*

Accuhealth e Vivify Health utilizzano la crittografia AES Advanced Encryption Standard (AES) per i dati inattivi e l'indirizzo PR.DS-1 e PR.DS-P1.

Per maggiori dettagli, vedi CAPITOLO 5.6 E 5.7.

FUNCTIONAL EVALUATION

Questa guida utilizza il NIST Cybersecurity Framework.

Il Cybersecurity Framework include concetti di categoria e sottocategoria che consentono a questa guida pratica di sviluppare un'architettura di riferimento.

L'architettura di riferimento riflette i casi d'uso e i flussi di dati analizzati dall'NCCoE.

Questa guida allinea gli strumenti per la privacy e la sicurezza informatica alle sottocategorie del quadro di sicurezza informatica.

L'architettura di riferimento mostra dove sono stati distribuiti gli strumenti.

Per maggiori dettagli, vedi CAPITOLO 6.1.1 RPM FUNCTIONAL EVALUATION *contenente la* TABLE 6-1 FUNCTIONAL EVALUATION REQUIREMENTS ED IL RELATIVO CAPITOLO 6.1.2 TEST CASE *con I casi di prova.*

APPENDIX C THREATS AND RISKS

Le organizzazioni devono comprendere i rischi associati ai sistemi che distribuiscono.

NIST fornisce due corpi di lavoro che consentono alle organizzazioni di esaminare il rischio e determinare come i rischi possono essere mitigati.

Il National Cybersecurity Center of Excellence (NCCoE) utilizza il NIST Cybersecurity Framework come guida per la gestione dei rischi nella tecnologia sanitaria.

In armonia con il Cybersecurity Framework c'è il NIST Risk Management Framework (RMF).

Questa appendice illustra come applicare il Cybersecurity Framework e l'RMF nella gestione dei rischi per l'ambiente di monitoraggio remoto del paziente (RPM).

*I Business Processes, i rischi, le minacce per il paziente, per il provider e per HDO, le vulnerabilità, sono elencati nell'*APPENDIX C DEL NIST SP 1800-30

68. ARCHITECTURE

La soluzione ha distribuito componenti in tre domini che consistono nella casa del paziente, nel fornitore della piattaforma di telemedicina e nell'HDO.

La casa del paziente è l'ambiente in cui vive il paziente e utilizza componenti RPM che includono dispositivi di monitoraggio biometrico, dispositivi che il paziente utilizza per comunicare con il proprio team di assistenza e dispositivi che il paziente utilizza per uso personale.

Questa guida pratica incorpora i fornitori di piattaforme di telemedicina ospitate nel cloud all'interno dell'architettura.

Il fornitore della piattaforma di telemedicina mantiene componenti che includono componenti virtuali o fisici con server per gestire, mantenere e ricevere comunicazioni di dati dal domicilio del paziente o dall'HDO.

L'HDO mantiene il proprio ambiente e include componenti quali postazioni di lavoro e sistemi clinici per ricevere e interpretare i dati dei pazienti e registrare le interazioni dei pazienti in un sistema di cartelle cliniche elettroniche (EHR).

La Figura 4-1 illustra un'architettura distribuita RPM di alto livello.

L'architettura illustrata rileva due percorsi principali attraverso i quali le comunicazioni di rete percorrono.

Il Path 1 mostra i dispositivi biometrici che comunicano con il fornitore della piattaforma di telemedicina mentre il Path 2 mostra l'uso di un'app mobile.

L'App mobile funziona su un dispositivo di interfaccia (ad esempio, un tablet con provisioning).

Per il Path 2, i pazienti utilizzano il tablet per raccogliere dati dai dispositivi biometrici.

Il Path 2 non prevede il trasferimento di dati tra il dispositivo biometrico direttamente al fornitore della piattaforma di telemedicina. Piuttosto, i pazienti raccolgono dati biometrici con il tablet.

I pazienti utilizzano il tablet per le comunicazioni, con scambi di dati tra il domicilio del paziente e il fornitore della piattaforma di telemedicina.

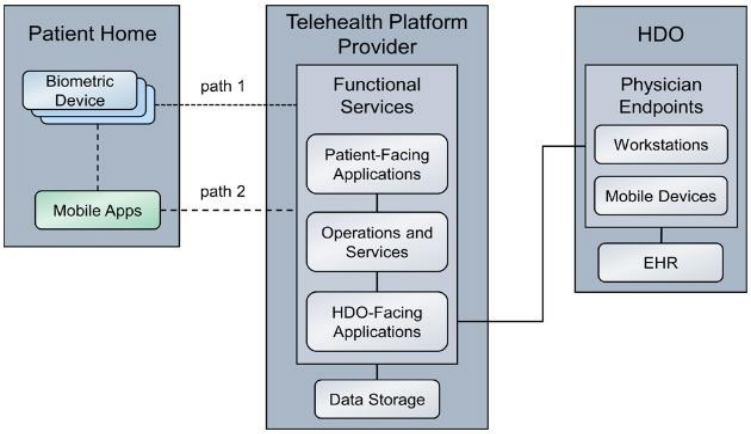


FIGURA 4-1 RPM ARCHITECTURE

LAYERING THE ARCHITECTURE

Il laboratorio sanitario NCCoE ha stratificato l'architettura distribuita con tre livelli:

1st. BUSINESS,

2nd. SICUREZZA

3rd. INFRASTRUTTURA.

Il livello BUSINESS *si concentra sulle capacità funzionali che includono letture biometriche e interazioni con i pazienti.*

Il livello SECURITY *descrive concettualmente come il laboratorio NCCoE implementa le capacità di sicurezza.*

Il livello INFRASTRUCTURE *rappresenta la rete e l'ambiente di comunicazione.*

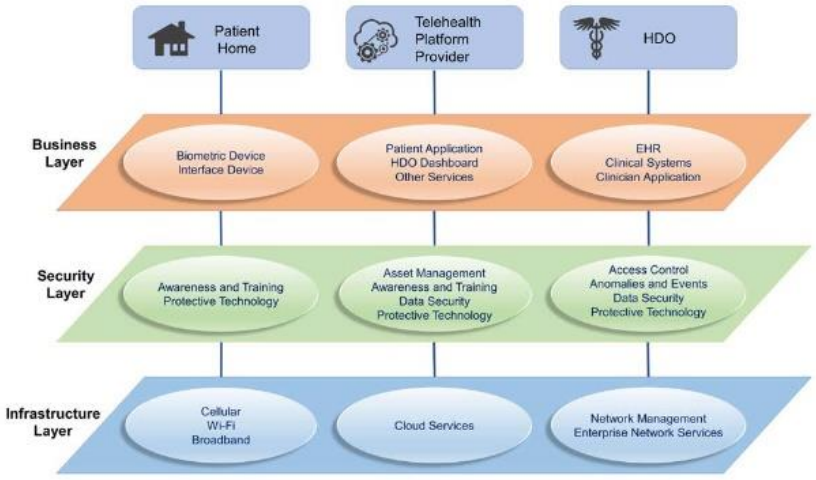


FIGURE 4-2 ARCHITECTURE LAYERS

L'NCCoE implementa anche un livello Infrastruttura che rappresenta l'ambiente di rete e di comunicazione.

Gli strati intersecano ciascuno dei tre domini.

A. *Dominio della casa del paziente (Patient Home): implementa il livello aziendale utilizzando i dispositivi biometrici e i dispositivi di interfaccia che acquisiscono e trasmettono i dati biometrici dal paziente e consentono al paziente di comunicare rispettivamente con il team di assistenza clinica. Inoltre, può includere un componente del livello di sicurezza che separa il traffico di rete tra i componenti RPM e i dispositivi di proprietà personale quando i dispositivi RPM utilizzano la stessa infrastruttura di rete (ad esempio, tramite Wi-Fi) dei dispositivi di proprietà personale. Quando i dispositivi funzionano e comunicano tramite Wi-Fi, il livello infrastruttura sarebbe costituito da punti di accesso Wi-Fi, router e switch che il paziente utilizza.*

B. *Dominio del provider (Telehealth Platform Provider) della piattaforma di telemedicina implementa tre livelli.*

1°. *Il livello Business è costituito da servizi che facilitano la gestione dei dati dei pazienti e funzionalità di web o audioconferenza.*

2°. *Il livello Sicurezza è costituito da componenti utilizzati per proteggere l'ambiente, come meccanismi di autenticazione, sistemi di gestione dei certificati o funzionalità di registrazione della sicurezza.*

3°. *Il livello Infrastruttura è costituito da componenti di rete e server che possono essere implementati come servizi cloud.*

C. *Dominio HDO: implementa il livello Business con applicazioni e sistemi clinici utilizzati per supportare il programma RPM.*

Il livello Sicurezza rappresenta l'implementazione della capacità di sicurezza, che include meccanismi di autenticazione, capacità di monitoraggio della rete e scansione delle vulnerabilità come esempi rappresentativi.

L'HDO implementa il livello Infrastruttura con servizi IT fondamentali come AD, DNS e dispositivi di rete.

La Figura 4-2 mostra una vista di alto livello dei tre livelli che intersecano ciascun dominio di questi componenti e come ci siamo avvicinati alla loro implementazione nell'ambiente di laboratorio.

Gli HDO dovrebbero valutare i fornitori di piattaforme di telemedicina per determinare l'adeguatezza del controllo.

HIGH-LEVEL ARCHITECTURE COMMUNICATIONS PATHWAYS

Vedi CAPITOLO 4.2 HIGH-LEVEL ARCHITECTURE COMMUNICATIONS PATHWAYS *per i dettagli*: CELLULAR DATA PATHWAYS; BROADBAND PATHWAYS.

Vedi CAPITOLO 4.3 DATA AND PROCESS FLOWS

Vedi CAPITOLO 4.4 SECURITY CAPABILITIES *per i dettagli*: RISK ASSESSMENT CONTROLS; IDENTITY MANAGEMENT, AUTHENTICATION AND ACCESS CONTROL; DATA SECURITY; ANOMALIES AND EVENTS AND SECURITY CONTINUOUS MONITORING

FINAL ARCHITECTURE

La guida pratica ha costruito un'architettura che ha indirizzato i percorsi di comunicazione A e B descritti nella Sezione 4.2, High Level Architecture Communications Pathways.

Questa guida pratica ha anche implementato una soluzione Layer 2 su Layer 3 fornita da Onclave Networks come prova del concetto per proteggere le sessioni di rete tra la casa del paziente e il Telehealth Platform Provider.

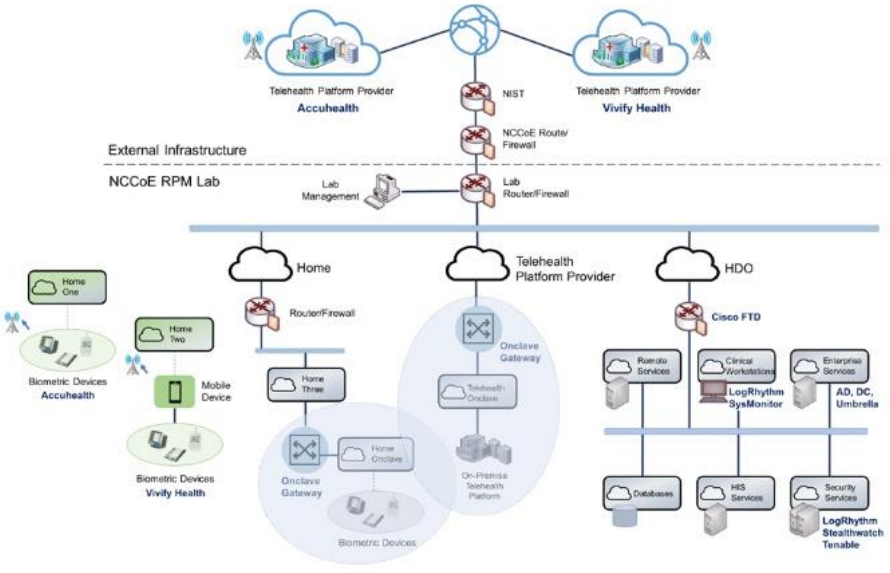


FIGURE 4-7 FINAL ARCHITECTURE

La discussione sulla soluzione Onclave appare nell'Appendice E del manuale.

La soluzione Onclave discute una considerazione di costruzione futura in cui i fornitori di piattaforme di telemedicina possono implementare approcci simili, migliorando ulteriormente le sessioni di dati in transito dal domicilio del paziente quando quei dispositivi comunicano su una connessione a banda larga.

La Figura 4-7 illustra l'architettura di riferimento finale dell'esempio Soluzione RPM.

69. PRIVACY RISK ASSESSMENT METHODOLOGY (PRAM)

Il NIST Privacy Framework fa riferimento al concetto di "azioni problematiche sui dati", che deriva dalla NIST Privacy Risk Assessment Methodology (PRAM).

Un'azione problematica sui dati si verifica quando i dati elaborati dai sistemi possono essere compromessi o portare a conseguenze indesiderate che potrebbero causare problemi alle persone.

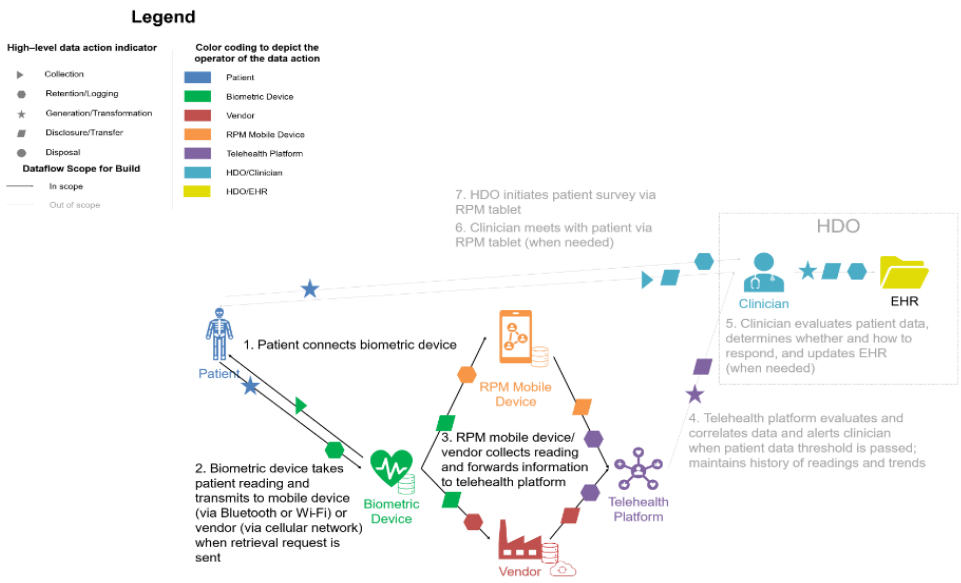
Le azioni problematiche sui dati hanno paralleli al concetto di "minacce" e "vulnerabilità" in quanto rappresentano conseguenze negative per gli individui.

La guida ha applicato la NIST Privacy Risk Assessment Methodology (PRAM) per condurre una valutazione del rischio per la privacy per l'architettura RPM.

L'elaborazione può includere raccolta, conservazione, registrazione, analisi, generazione, trasformazione o fusione, divulgazione, trasferimento e smaltimento dei dati.

La Figura D-1 mostra la vista sulla privacy del flusso di dati della soluzione RPM ed è stata utilizzata per condurre la Valutazione del Rischio per la Privacy (Privacy Risk Assessment).

Figure D-1 Privacy View of RPM Solution Dataflow



*Per i dettagli sulle "*PROBLEMATIC DATA ACTIONS*" e "*MITIGATIONS*", vedi* CAPITOLI D.2 E D.3 DELL'APPENDIX D.
*Inoltre, l'*APPENDIX E *per l'uso* DELL'IOT, *l'*APPENDIX F *per la descrizione del* MODELLO GATEWAY ENCLAVE *di* ZERO TRUST*; la descrizione delle architetture finali sono indicate nella* SEZIONE 30C

69A. ZERO TRUST E LA TELEHEALTH

L'architettura della Telemedicina può essere ricondotta nel paradigma di Zero Trust.

L'Appendice F del NIST SP 1800-30B Applicazione del modello OSI per comprendere l'architettura Zero Trust

L'ISO e l'IEC descrivono il modello OSI come composto da sette livelli denominati:

7° *livello:* APPLICAZIONE,

6° *livello:* PRESENTAZIONE,

5° *livello: SESSIONE,*

4° *livello: TRASPORTO,*

3° *livello: RETE,*

2° *livello: COLLEGAMENTO DATI,*

1° *livello: FISICO,*

in cui i livelli sono numericamente ordinati al contrario.

Cioè, il livello di applicazione è considerato come **Livello 7***, mentre il livello fisico è considerato come livello 1, una prova di concetto per proteggere le sessioni di rete tra la casa del paziente e il fornitore della piattaforma di telemedicina.*

I dispositivi che operano al **Livello 2** *hanno indirizzi* MAC (MEDIA ACCESS CONTROL) *mediante i quali i dispositivi, come i dispositivi biometrici, possono comunicare attraverso un segmento di rete locale (LAN).*

Le soluzioni **Livello 2** *e* **Livello 3** *consentono ai dispositivi che non implementano il livello di rete di avere un'interconnettività più ampia. E forniscono sicurezza limitando l'accesso ai dispositivi e proteggendo le comunicazioni in transito dei dati, ad esempio con la crittografia.*

Le organizzazioni possono prendere in considerazione soluzioni Layer 2 su Layer 3 per dispositivi che potrebbero essere soggetti a minacce Internet.

I dispositivi biometrici possono implementare l'interconnettività **Livello 2** *e* **Livello 3***; tuttavia, non dispongono di controlli robusti che impediscono l'accesso remoto non autorizzato.*

*La pubblicazione "*NIST (SP) 800-207 ZERO TRUST ARCHITECTURE*" descrive un modello di* GATEWAY ENCLAVE *che può essere applicato a un'architettura di telemedicina per il monitoraggio remoto del paziente (*Telehealth REMOTE PATIENT MONITORING – RPM - Architecture*).*

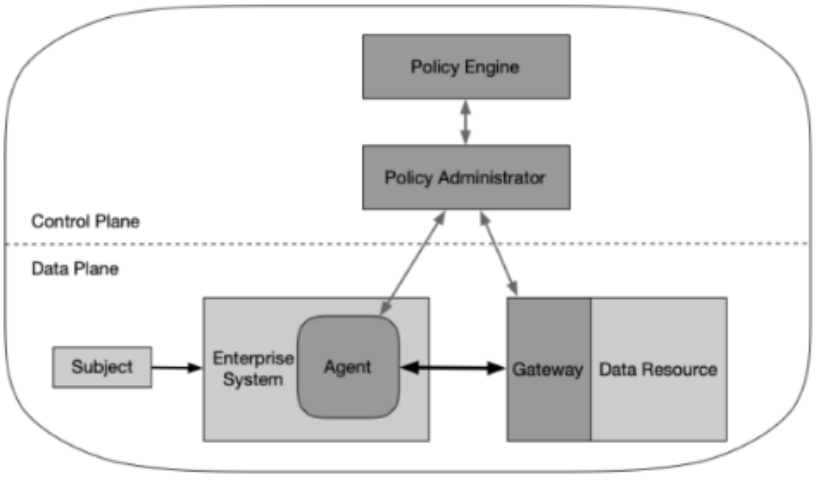
Nel modello del gateway dell'enclave, una soluzione ZERO TRUST *opera su due piani concettuali:*

1. PIANO *di* CONTROLLO (CONTROL PLANE)
2. PIANO DATI (DATA PLANE).

I dispositivi di gestione della microsegmentazione operano in un PIANO DI CONTROLLO (CONTROL PLANE). *Questi dispositivi di gestione forniscono funzionalità amministrative e di policy per supportare enclave sicure.*

I componenti operativi, come dispositivi biometrici, servizi di provider di piattaforme di telemedicina e dispositivi ospitati da organizzazioni di assistenza sanitaria, possono operare nel PIANO DATI (DATA PLANE).

Figure F-1 Enclave Gateway Model [25]



La Figura F-1 mostra il modello di gateway dell'enclave.

La soluzione **Livello** *2 e* **Livello** *3 utilizzata in questa guida pratica introduce i principi sull'architettura* ZERO TRUST (ZTA) all'RPM *di telemedicina.*

I dispositivi biometrici gestiti possono essere soggetti a minacce che possono essere presenti nella rete domestica del paziente.

L'approccio **Livello** *2 e* **Livello** *3 segmenta i componenti* RPM *di altri dispositivi che possono operare nella casa del paziente.*

I dispositivi non associati ai componenti RPM *distribuiti non dispongono di un percorso di comunicazione con i dispositivi* RPM.

ZTA consente ai dispositivi biometrici di autenticarsi nella soluzione di sicurezza **Livello 2** *e* **Livello** 3 *in modo che solo il traffico proveniente dai componenti RPM attraversi la rete* **Livello** 2 *e* **Livello** 3.

*Chi è interessato può fare riferimento al "*NIST SP 800-207 ZERO TRUST ARCHITECTURE".

PARTE XIII: BLOCKCHAIN

[Rif.: EU Blockchain Observatory and Forum – An initiative of the European Commission: Blockchain and GDPR; CNIL - Blockchain & GDPR: Solutions for a responsible use of the blockchain in the context of personal data; 2015 IEEE – Blockchain: Decentralizing Privacy: Using Blockchain to Protect Personal Data dal sito https://ieeexplore.ieee.org/document/7163223; ENISA WP2018 O.2.2.5: Reinforcing trust and security in the area of electronic communication and online services – December 2018]

70. LA TECNOLOGIA (PROTOCOLLO BLOCKCHAIN)

Le Transazioni o Trattamenti (secondo la terminologia GDPR) gestiscono basi dati che si fondano su architetture Centralizzate, Decentralizzate oppure Distribuite.

In tutte e tre le tipologie, valgono le seguenti caratteristiche generali:

1. SICUREZZA: *dati cifrati;*
2. CONSENSO: *dati modificabili solo col consenso di tutti;*
3. IMMUTABILITÀ: *garanzie di immutabilità e incorruttibilità (libro mastro distribuito, Trust e Fiducia);*
4. TRASPARENZA: *tutti i partecipanti possono vedere tutto;*

71. LISTA DI CONTROLLO SUDDIVISA IN CONTESTI

Lista degli argomenti sui quali concentrare i controlli al fine di verificare la compatibilità dei trattamenti con quanto stabilito dal GDPR e ulteriori considerazioni sull'architettura del protocollo a supporto della valutazione del rischio.

1) RACCOMANDAZIONI: *sono contenuti i prerequisiti per la contestualizzazione dell'attività, indispensabili ad un corretto svolgimento della verifica*

2) RUOLI

3) DIRITTI DELL'INTERESSATO (DALL'ARTICOLO 12 AL 23)

4) REQUISITI DI SICUREZZA GARANTITI DAL TRATTAMENTO (ARTICOLI 25 E 32)

RACCOMANDAZIONI

Regole empiriche per la progettazione

1) Raccogliere i dati personali su reti private autorizzate.

2) Liceità del trattamento.

3) *Scelta di un metodo crittografico adeguato per archiviare i dati che consenta all'interessato di avvicinarsi ad un esercizio dei suoi diritti.*
4) *In fase di progettazione del programma, concedere la restrizione del trattamento o le richieste di intervento umano.*
5) *Il GDPR stabilisce che il consenso sia granulare e non ambiguo. Avviando una transazione un utente sta assumendo un obbligo contrattuale con la piattaforma e ciò potrebbe costituire la base per il trattamento: qui abbiamo un atto passivo.*
6) *In una rete blockchain privata autorizzata, richiedere che ciascun partecipante accetti determinati termini e condizioni prima di ottenere l'accesso alla rete stessa.*
7) *Le blockchain permissioned dovrebbero essere favorite poiché consentono un miglior controllo sulla governance dei dati personali, in particolare per quanto riguarda i trasferimenti al di fuori dell'UE.*
8) *Il requisito di adeguate salvaguardie per i trasferimenti al di fuori dell'UE, come le regole aziendali vincolanti o le clausole contrattuali standard, sono interamente applicabili alle blockchain autorizzate.*
9) *Mentre le opportune salvaguardie per un trasferimento al di fuori dell'UE possono essere utilizzate in una blockchain autorizzata, come clausole contrattuali standard, regole aziendali vincolanti, codici di condotta o persino meccanismi di certificazione, CNIL osserva che queste garanzie sono più difficili da implementare in una blockchain pubblica, dato che il titolare dei dati non ha un controllo reale sulla posizione dei miner.*

RUOLI

TITOLARE DEL TRATTAMENTO

1) *Identificazione e obblighi dei responsabili e titolari del trattamento. Esistono situazioni in cui è difficile e forse impossibile identificare i titolari, ad esempio quando i singoli utenti pubblicano transazioni o definiscono contratti intelligenti decentralizzati su una blockchain pubblica.*
2) *CNIL osserva che i partecipanti, che hanno il diritto di scrivere sulla catena e che decidono di inviare i dati per la convalida da parte dei miner, possono essere considerati come titolari.*
3) *Gli sviluppatori, che creano e mantengono la tecnologia blockchain open source, non dovrebbero essere considerati titolari.*
4) *Gli attori, che eseguono il protocollo blockchain sui loro computer, al fine di fungere da nodi di convalida o nodi partecipanti pubblici, non dovrebbero essere considerati titolari (controller).*
5) *Se gli utenti inviano i dati personali al libro mastro come parte di un'attività commerciale, è più probabile che siano considerati titolari.*
6) *Le persone fisiche che immettono dati personali, che non riguardano un'attività professionale o commerciale, non sono titolari (in base all'esclusione "puramente personale o di attività familiare" di cui all'articolo 2 del GDPR).*
7) *Quando un gruppo decide di eseguire operazioni di elaborazione per uno scopo comune, CNIL raccomanda ai partecipanti di prendere una decisione comune sulle responsabilità del titolare:*
   - ✓ *creando una persona giuridica come titolare dei dati; oppure*
   - ✓ *designando il partecipante che prenda le decisioni per il gruppo come titolare;*
   - ✓ *in caso contrario, è probabile che tutti i partecipanti siano considerati contitolari.*

RESPONSABILE DEL TRATTAMENTO

1) *Gli sviluppatori di contratti intelligenti che trattano i dati personali per conto del titolare del trattamento, sono responsabili (processor).*
2) *I miner sono responsabili se convalidano la transazione contenente dati personali.*

3) *È responsabile del trattamento chi stabilisce un contratto con il partecipante, agendo in tal modo come titolare, che specifica gli obblighi di ciascuna parte e che riproduce le disposizioni dell'articolo 28 del GDPR.*
4) *È responsabile del trattamento lo sviluppatore del contratto intelligente che elabora i dati personali per conto del partecipante.*

DIRITTI DELL'INTERESSATO

DI INFORMAZIONE

1. *Le applicazioni impongono agli utenti permessi nel momento in cui avviene la registrazione e tali permessi sono concessi a tempo indeterminato; l'unico modo per modificare l'accordo è opt-out. È necessario dare la possibilità all'utente di modificare i permessi e revocare l'accesso ai dati raccolti.*
2. *Il titolare deve fornire informazioni concise che siano facilmente accessibili e formulate in termini chiari all'interessato prima di inviare i dati personali ai miner per la convalida.*

DI CANCELLAZIONE

1. *CNIL riconosce che alcune tecniche di crittografia, associate alla distruzione delle chiavi, possono essere considerate come una cancellazione anche se non è una cancellazione nel senso più stretto.*
2. *Quando i dati registrati sono generati da una funzione di hash keyed o un testo cifrato ottenuto tramite algoritmi e chiavi "state of the art", il titolare può rendere i dati praticamente inaccessibili e quindi avvicinarsi agli effetti della cancellazione dei dati.*

DI RETTIFICA E D'OPPOSIZIONE

1) *È tecnicamente impossibile concedere la richiesta di rettifica effettuata da un interessato quando il testo in chiaro o i dati con hash sono registrati.*
2) *Il titolare inserisce i dati aggiornati in un nuovo blocco. Una transazione successiva può annullare logicamente una transazione iniziale, anche se la prima transazione apparirà ancora nella catena.*
3) *Il titolare dovrebbe fornire la possibilità dell'intervento umano che consenta alla persona interessata di contestare la decisione.*
4) *L'utente deve poter modificare le autorizzazioni concesse a un servizio in qualsiasi momento emettendo una transazione con una nuova serie di autorizzazioni, incluso revocare l'accesso ai dati precedentemente memorizzati.*

DI ACCESSO

1) *Elaborazione automatizzata: gli interessati possono chiedere al titolare se i loro dati sono utilizzati o meno per il processo decisionale automatico.*
2) *Territorialità: vi sono anche obblighi in termini di luogo in cui può avvenire l'elaborazione dei dati, noti anche come "trasferimenti di dati personali verso paesi terzi".*

ALLA PORTABILITÀ

CNIL ritiene che l'esercizio di tale diritto sia compatibile con le proprietà tecniche.

REQUISITI DI SICUREZZA (ARTICOLI 25 E 32)

ANONIMIZZAZIONE DATI

1. *L'anonimizzazione dei dati personali, è la validità di varie tecniche che consentono agli utenti di registrare "prove di dati" (proofs of data) senza rivelare effettivamente i dati.*
2. *Mascheratura degli indirizzi personali*
   - ✓ *Le chiavi pubbliche o gli indirizzi sono generalmente dati personali. Su alcune reti blockchain pubbliche, gli indirizzi dei mittenti e dei destinatari delle transazioni possono essere visti da tutti, in base al GDPR tali indirizzi sarebbero spesso considerati* PSEUDONIMI.
   - ✓ *La tecnica di mascheratura degli indirizzi più comune è denominata "*SERVIZIO DI INDIVIDUAZIONE INDIRETTA DI TERZE PARTI*". Consiste nel chiedere a una terza parte di aggregare molte transazioni blockchain e di inviarle alla contabilità utilizzando la propria chiave pubblica.*
   - ✓ *Le "*FIRME AD ANELLO*" sono un'altra tecnica con la quale più parti firmano una determinata transazione in modo tale che un estraneo possa essere sicuro che una delle parti è il firmatario legittimo, ma non quale.*
3. *Crittografia dei dati personali*
   - ✓ *I dati personali crittografati in modo* REVERSIBILE *sono personali ed in quanto tali rientrano nell'ambito del GDPR.*
   - ✓ *Una crittografia forte sui dati personali, produce come risultato uno pseudonimo, non un anonimo. Questo per il semplice motivo che, finché la chiave esiste da qualche parte, i dati possono essere decifrati, portando a un* RISCHIO DI INVERSIONE.
   - ✓ *Il dato personale "*hashed*" rientra in un contesto ambiguo.*
   - ✓ *Usare tecniche di "*salting*" o "*peppering*", che implicano l'aggiunta di informazioni extra ai dati per renderlo abbastanza grande da rendere estremamente difficoltoso un attacco di inversione dei dati.*

PROTEZIONE DEI DATI FIN DALLA PROGETTAZIONE E PER IMPOSTAZIONE PREDEFINITA

Il sistema, all'atto della sua prima registrazione, genera all'utente una nuova identità condivisa (utente, servizio) e inviata, insieme alle autorizzazioni associate, alla blockchain.

MINIMIZZAZIONE DEI DATI

1) *Il principio di minimizzazione richiede che i dati raccolti siano pertinenti e limitati a quanto strettamente necessario agli scopi per i quali sono trattati. Un periodo di conservazione dei dati deve quindi essere definito in base allo scopo del loro trattamento.* SE LA CANCELLAZIONE NON È POSSIBILE ALLORA SI DETERMINA UN CONFLITTO COL DIRITTO ALL'OBLIO (VEDI RICHIESTA AL GARANTE)
2) *Ogni partecipante ha un identificatore composto da una serie di caratteri alfanumerici che appaiono casuali e che costituiscono la sua chiave pubblica. Questi identificatori sono sempre visibili, in quanto sono essenziali per il suo corretto funzionamento.* CNIL RITIENE CHE QUESTI DATI NON POSSANO ESSERE ULTERIORMENTE RIDOTTI AL MINIMO E CHE I LORO PERIODI DI CONSERVAZIONE SIANO, IN SOSTANZA, IN LINEA CON LA DURATA DELL'ESISTENZA DELLA BLOCKCHAIN.
3) *Se una valutazione impatto (art. 35) ha dimostrato che* I RISCHI RESIDUI SONO ACCETTABILI, I DATI POSSONO ESSERE CONSERVATI ANCHE IN TESTO CHIARO. *Alcuni titolari del trattamento potrebbero avere l'obbligo legale di rendere pubbliche e accessibili alcune informazioni, senza un periodo di*

conservazione: in questo caso particolare, è possibile prevedere la memorizzazione di dati personali su una blockchain pubblica.

4) *Dato che gli identificatori dei partecipanti, vale a dire le loro chiavi pubbliche, sono essenziali per il corretto funzionamento della blockchain,* **CNIL** RITIENE CHE NON SIA POSSIBILE MINIMIZZARLI ULTERIORMENTE; IL PERIODO DI CONSERVAZIONE È IN LINEA CON QUELLO DELLA BLOCKCHAIN.

72. CONSIDERAZIONI PER IL CALCOLO DEL RISCHIO

CARATTERISTICHE DELL'ARCHITETTURA*: le sue caratteristiche potrebbero essere in conflitto con quanto stabilito dal Regolamento e per ognuna di esse è necessario valutare l'impatto.*

PUBBLICA

1) *Senza richiesta di permessi o autorizzazioni a chiunque è consentito di diventare un nodo partecipante o un nodo di convalida.*
2) *Non c'è il proprietario della rete, nessuna procedura di iscrizione, nessuna registrazione e nessuna restrizione su chi può farlo.*
3) *Tutti i nodi possono vedere tutti i dati, così come gli indirizzi del mittente e del destinatario.*
4) *Chiunque può decidere di crittografare i dati prima di inviarli; si può utilizzare un servizio di reindirizzamento di terze parti per offuscare l'indirizzo del mittente o del destinatario.*

PUBBLICHE E AUTORIZZATE

Chiunque può essere un nodo partecipante e vedere tutti i dati, ma solo gli attori pre-approvati possono diventare nodi di convalida e aggiungere dati al libro mastro.

1. BLOCKCHAIN PUBBLICA, GESTITA DA MIGLIAIA DI NODI:

   1) *non privata;*
   2) *non molto veloce;*
   3) *molto decentralizzata;*
   4) *molto difficile interrompere il funzionamento (art. 32 per BC e DR) o acquisirne il controllo.*

Può essere utilizzata:

1) *per archiviare le risorse crittografiche per lunghi periodi di tempo senza scambiarle;*
2) *come bridge per spostare queste cripto risorse da una rete di trading privata a un'altra;*
3) *in progettazione, la blockchain di base rende possibile l'interoperabilità della rete privata con altre reti in tutto il mondo, ma i membri del consorzio devono essere estremamente attenti a non compromettere i dati personali quando i dati vengono scambiati tra i due livelli.*

2. QUANDO SI CONSIDERA L'USO DI TECNICHE DI MASCHERAMENTO, È NECESSARIO VALUTARE DUE RISCHI IN DETTAGLIO:

   - RISCHIO DI INVERSIONE*, nonostante la crittografia utilizzata, è possibile invertire il processo e ricostituire i dati originali attraverso la decrittazione.*
   - RISCHIO DI CORRELAZIONE*, è il rischio di collegamento di dati crittografati ad un individuo confrontandolo con altre informazioni.*

3…MASSIMA ATTENZIONE QUANDO SI COLLEGANO BLOCKCHAIN PRIVATE CON QUELLE PUBBLICHE.

4…DIMENSIONI:

generazione transazione → blocco con altre transazioni → blocchi della catena ∈ Libro Mastro distribuito in tutti i nodi → aumento continuo dello spazio necessario ad ospitare tutte le informazioni (incrementali)

PRIVATE (PERMISSIONED)

1) *Regole che definiscono chi è in grado di vedere e quali dati.*
2) *Definire procedure tecniche e organizzative per limitare l'impatto di un potenziale errore dell'algoritmo: vulnerabilità su un meccanismo crittografico.*
3) *Definire un piano di emergenza che consenta di modificare gli algoritmi quando è identificata una vulnerabilità.*
4) *Definire una governance delle modifiche al software utilizzato per creare transazioni.*
5) *Definire procedure tecniche ed organizzative per garantire un allineamento tra le autorizzazioni pianificate e l'applicazione pratica.*
6) *Il titolare deve garantire la sicurezza delle chiavi segrete utilizzate.*

PARTE XIV: HW-ENABLED SECURITY: CONTAINER PLATFORM SECURITY PROTOTYPE

[Rif.: NIST IR 8320]

73. PREMESSA

Nei data center cloud e nell'edge computing odierni, le superfici di attacco sono notevolmente aumentate, l'hacking è diventato industrializzato e la maggior parte delle implementazioni dei controlli di sicurezza non sono coerenti o coerenti.

La base di qualsiasi strategia di sicurezza per data center o edge computing dovrebbe essere la protezione della piattaforma su cui verranno eseguiti e accessibili i dati e i carichi di lavoro.

La piattaforma fisica rappresenta il primo livello per qualsiasi approccio alla sicurezza a più livelli e fornisce le protezioni iniziali per garantire che i controlli di sicurezza di livello superiore (Nord-Sud, Est-Ovest, vedi capitolo "7.3.5 Identifying Candidate Solutions" del "NIST SP 800-207 Zero Trust Architecture") possano essere considerati affidabili.

Questo report spiega un approccio basato su tecniche e tecnologie di sicurezza abilitate per hardware per salvaguardare le distribuzioni di container in ambienti cloud multi-tenant. Descrive anche un'implementazione proof-of-concept dell'approccio - un prototipo - che è inteso come un modello o un modello per la comunità di sicurezza generale.

74. INTRODUZIONE

Scopo di questa pubblicazione è descrivere un approccio per la salvaguardia delle distribuzioni di contenitori di applicazioni in ambienti cloud multi-tenant.

Questa pubblicazione spiega innanzitutto le sfide di sicurezza selezionate che coinvolgono le tecnologie di cloud computing IaaS (Infrastructure as a Service) e la geolocalizzazione sotto forma di tag di risorse.

Quindi descrive un'implementazione del proof of concept, un prototipo, progettato per affrontare queste sfide.

La pubblicazione fornisce dettagli sufficienti sull'implementazione del prototipo in modo che le organizzazioni possano riprodurlo se lo desiderano.

La pubblicazione vuole essere un modello o un modello che può essere utilizzato dalla comunità di sicurezza generale per convalidare e implementare l'implementazione descritta.

È importante notare che l'implementazione del prototipo presentato in questa pubblicazione è solo un modo possibile per risolvere le sfide alla sicurezza.

Non intende precludere l'uso di altri prodotti, servizi, tecniche, ecc. Che possono anche risolvere adeguatamente il problema, né intende precludere l'uso di prodotti o servizi cloud non espressamente menzionati in questa pubblicazione.

Questa pubblicazione si basa sulla terminologia e sui concetti descritti nella bozza del white paper del NIST,

Sicurezza abilitata per hardware per piattaforme server: abilitazione di un approccio a più livelli alla sicurezza della piattaforma per casi d'uso di cloud ed edge computing.

La lettura di questo white paper è un prerequisito per leggere questa pubblicazione perché spiega i concetti e definisce la terminologia chiave utilizzata in questa pubblicazione.

75. IMPLEMENTAZIONE DEL PROTOTIPO

Questa sezione definisce l'implementazione del prototipo.

La sezione 2.1 spiega le basi dell'obiettivo.

La sezione 2.2 fornisce maggiori dettagli, delineando tutti gli obiettivi intermedi che devono essere raggiunti per ottenere l'implementazione del prototipo desiderata.

Questi requisiti sono raggruppati in tre fasi del caso d'uso, ciascuna delle quali è esaminata più da vicino nelle sezioni da 2.2.1 a 2.2.3, rispettivamente.

FINALITÀ

Le tecnologie di cloud computing condivise sono progettate per essere altamente agili e flessibili, utilizzando in modo trasparente tutte le risorse disponibili per elaborare le distribuzioni di container per i propri clienti.

Tuttavia, ci sono problemi di sicurezza e privacy nel consentire l'orchestrazione della distribuzione di container senza restrizioni.

OGNI VOLTA CHE SONO PRESENTI PIÙ DISTRIBUZIONI DI CONTAINER SU UN SINGOLO SERVER CLOUD, È NECESSARIO SEPARARE TALI DISTRIBUZIONI L'UNA DALL'ALTRA IN MODO CHE NON INTERFERISCANO TRA LORO, OTTENGANO L'ACCESSO AI DATI SENSIBILI RECIPROCI O ALTRIMENTI COMPROMETTANO LA SICUREZZA O LA PRIVACY DEL CONTENITORI.

UN'ALTRA PREOCCUPAZIONE CON IL CLOUD COMPUTING CONDIVISO È CHE I CARICHI DI LAVORO POTREBBERO SPOSTARSI DA SERVER CLOUD SITUATI IN UN PAESE A SERVER SITUATI IN UN ALTRO PAESE.

Ogni paese ha le proprie leggi per la sicurezza dei dati, la privacy e altri aspetti della tecnologia dell'informazione (IT)

Poiché i requisiti di queste leggi possono essere in conflitto con le politiche o i mandati di un'organizzazione (ad es. Leggi, regolamenti), un'organizzazione può decidere di dover limitare i server cloud che utilizza in base alla loro posizione.

UN DESIDERIO COMUNE È QUELLO DI UTILIZZARE SOLO SERVER CLOUD FISICAMENTE SITUATI NELLO STESSO PAESE DELL'ORGANIZZAZIONE O FISICAMENTE UBICATI NELLO STESSO PAESE DI ORIGINE DELLE INFORMAZIONI.

La determinazione della posizione fisica approssimativa di un oggetto, come un server di cloud computing, è generalmente nota come geolocalizzazione.

LA GEOLOCALIZZAZIONE PUÒ ESSERE ESEGUITA IN MOLTI MODI, CON VARI GRADI DI PRECISIONE, MA I METODI DI GEOLOCALIZZAZIONE TRADIZIONALI NON SONO PROTETTI E VENGONO APPLICATI TRAMITE CONTROLLI GESTIONALI E OPERATIVI CHE NON POSSONO ESSERE AUTOMATIZZATI O RIDIMENSIONATI.

PERTANTO, I METODI DI GEOLOCALIZZAZIONE TRADIZIONALI NON POSSONO ESSERE CONSIDERATI AFFIDABILI PER SODDISFARE LE ESIGENZE DI SICUREZZA DEL CLOUD.

*La motivazione alla base di questo caso d'uso è migliorare la sicurezza e accelerare l'adozione delle tecnologie di cloud computing stabilendo un metodo di "**root of trust**" hw automatizzato per applicare e monitorare l'integrità della piattaforma e le restrizioni di geolocalizzazione per i server cloud.*

*Una radice di attendibilità hw è una combinazione intrinsecamente affidabile di hw e fw responsabile della misurazione dell'integrità della piattaforma e delle informazioni di geolocalizzazione sotto forma di **tag di asset**.*

Le misurazioni effettuate dalla radice di attendibilità hw vengono archiviate in un hw a prova di manomissione e vengono trasmesse utilizzando chiavi crittografiche uniche per quell'hardware a prova di manomissione.

A queste informazioni si accede da strumenti di gestione e sicurezza che utilizzano protocolli crittografici per affermare l'integrità della piattaforma e confermare la posizione dell'host.

*Questo caso d'uso si basa sul lavoro precedente documentato in **NIST IR 7904, Trusted Geolocation in the Cloud: Proof of Concept Implementation**.*

OBIETTIVI

L'uso di pool d'elaborazione affidabili è un approccio leader per l'aggregazione di sistemi affidabili e la loro separazione dalle risorse non attendibili, il che si traduce nella separazione dei carichi di lavoro più sensibili e di valore più elevato dalle applicazioni comuni e dai carichi di lavoro dei dati.

I principi di funzionamento sono:

1) ***CREARE** una parte del cloud per soddisfare i requisiti di sicurezza specifici e variabili degli utenti;*
2) ***CONTROLLARE** l'accesso a quella parte del cloud in modo che le giuste applicazioni (carichi di lavoro) vengano distribuite lì;*
3) ***ABILITARE** gli audit di quella parte del cloud in modo che gli utenti possano verificare la conformità.*

Questi pool di elaborazione affidabili consentono all'IT di ottenere i vantaggi dell'ambiente cloud dinamico, continuando a applicare livelli più elevati di protezione per i carichi di lavoro più critici.

*L'obiettivo finale è essere in grado di utilizzare la "**fiducia**" come limite logico per la distribuzione dei carichi di lavoro cloud su piattaforme server all'interno di un cloud.*

Questo obiettivo dipende da obiettivi prerequisiti più piccoli descritti come fasi, che possono essere pensati come requisiti che la soluzione deve soddisfare. A causa del numero di prerequisiti, sono stati raggruppati in tre fasi:

0. ***ATTESTAZIONE DELLA PIATTAFORMA E AVVIO MISURATO DEL NODO DI LAVORO**. Ciò garantisce che l'integrità della piattaforma del server cloud sia misurata e disponibile per le fasi successive.*
1. ***POSIZIONAMENTO AFFIDABILE DEL CARICO DI LAVORO**. Questa fase consente di orchestrare le distribuzioni di container per l'avvio solo su piattaforme server attendibili all'interno di un cloud.*
2. ***ASSET TAGGING E POSIZIONE ATTENDIBILE**. Questa fase consente di avviare le distribuzioni di container solo su piattaforme server affidabili all'interno di un cloud, prendendo in considerazione le limitazioni qualitative dei tag di asset (ad esempio, le informazioni sulla posizione).*

Gli obiettivi prerequisiti per ogni fase, insieme a informazioni più generali su ciascuna fase, sono spiegati di seguito.

STAGE 0: PLATFORM ATTESTATION AND MEASURED WORKER NODE LAUNCH

Un componente fondamentale di una soluzione è avere una certa garanzia che la piattaforma su cui è in esecuzione la distribuzione del contenitore possa essere considerata attendibile.

Se la piattaforma non è affidabile, non solo espone l'applicazione e i dati del tenant a un maggior rischio di compromissione, ma non vi è alcuna garanzia che il tag dell'asset rivendicato del server cloud sia accurato.

AVERE LA CERTEZZA DI BASE DELL'AFFIDABILITÀ È LA FASE INIZIALE DELLA SOLUZIONE.

La fase 0 include i seguenti prerequisiti obiettivi:

1. *Configurare una piattaforma server cloud come attendibile.*

   La "piattaforma server cloud" include la configurazione hardware (ad es. Integrità del BIOS), la configurazione del sistema operativo (OS) (caricatore di avvio e configurazione e integrità del kernel del sistema operativo) e l'integrità del runtime del contenitore.

   Ciò include anche le diverse tecnologie di protezione hardware abilitate sul server. Queste tecnologie della catena di fiducia (CoT) forniscono la verifica dell'integrità della piattaforma. Ulteriori tecnologie e dettagli possono essere trovati nella summenzionata bozza del white paper del NIST e sono discussi nella sezione 3.2.

2. *Prima del lancio di ogni nodo di lavoro del contenitore, verificare (misurare) l'affidabilità della piattaforma del server cloud.*

   Gli elementi configurati nell'obiettivo 1 (BIOS, sistema operativo, runtime del contenitore) devono avere la loro configurazione verificata prima di avviare il runtime del contenitore per garantire che il livello di attendibilità presunto sia ancora in vigore.

3. *Durante l'esecuzione del runtime del contenitore, verificare periodicamente l'affidabilità della piattaforma del server cloud.*

   Questo controllo periodico è essenzialmente lo stesso controllo eseguito come obiettivo 2, tranne per il fatto che viene eseguito frequentemente durante l'esecuzione del runtime del contenitore. Idealmente, questo controllo farebbe parte di un monitoraggio continuo.

Il raggiungimento di tutti questi obiettivi non impedirà il successo degli attacchi, ma farà sì che le modifiche non autorizzate alla piattaforma cloud siano rilevate più rapidamente di quanto non sarebbero state altrimenti. Ciò impedisce l'avvio di nuove distribuzioni di container con requisiti di affidabilità sulla piattaforma compromessa.

STAGE 1: TRUSTED WORKLOAD PLACEMENT

Una volta che la fase 0 è stata completata con successo, il prossimo obiettivo è quello di essere in grado di orchestrare il posizionamento dei carichi di lavoro da avviare solo su piattaforme affidabili.

Il posizionamento del carico di lavoro è un attributo chiave del cloud computing, che migliora la scalabilità e l'affidabilità.

Lo scopo di questa fase è garantire che qualsiasi server su cui viene avviato un carico di lavoro soddisfi il livello di garanzia di sicurezza richiesto in base alla policy di sicurezza del carico di lavoro.

La fase 1 include il seguente obiettivo prerequisito:

1. *Distribuire i carichi di lavoro solo su server cloud con piattaforme affidabili.*

   Ciò significa fondamentalmente che esegui la fase 0, obiettivo 3 (controllo dell'affidabilità della piattaforma) e distribuisci un carico di lavoro sul server cloud solo se l'audit dimostra che la piattaforma è affidabile.

Il raggiungimento di questo obiettivo garantisce che i carichi di lavoro vengano distribuiti su piattaforme affidabili, riducendo così la possibilità di compromettere il carico di lavoro.

STAGE 2: ASSET TAGGING AND TRUSTED LOCATION

La fase successiva si basa sulla fase 1 aggiungendo la possibilità di monitorare e applicare continuamente le restrizioni dei tag degli asset.

La fase 2 include i seguenti prerequisiti obiettivi:

1. *Disporre di informazioni sui tag degli asset attendibili per ogni istanza della piattaforma attendibile.*

Queste informazioni sarebbero archiviate nel modulo crittografico del server cloud (come un hash crittografico all'interno del modulo crittografico hardware) in modo che possano essere verificate e verificate prontamente.

2. *Fornire la gestione della configurazione e i meccanismi di applicazione delle policy per piattaforme affidabili che includono l'applicazione delle limitazioni dei tag di risorse.*

   Questo obiettivo si basa sulla fase 1, obiettivo 1 (distribuire carichi di lavoro solo su server cloud con piattaforme affidabili); migliora la fase 2, obiettivo 1 aggiungendo un controllo del tag dell'asset al server su cui avviare il carico di lavoro.

3. *Durante l'orchestrazione del carico di lavoro, controllare periodicamente l'etichetta dell'asset della piattaforma del server cloud rispetto alle limitazioni dei criteri dell'etichetta dell'asset.*

   Questo obiettivo si basa sulla fase 0, obiettivo 3 (affidabilità della piattaforma di controllo), ma verifica specificamente le informazioni sui tag delle risorse rispetto alle norme per i tag delle risorse per garantire che la codifica delle risorse del server non violi le norme.

Il raggiungimento di questi obiettivi garantisce che i carichi di lavoro non vengano avviati su un server in una posizione di confine non adatta.

Ciò evita problemi causati da cloud che si estendono su diversi luoghi fisici (ad esempio, regolamenti, livelli di sensibilità, paesi o stati con diverse leggi sulla sicurezza dei dati e sulla privacy).

76. PROTOTYPING STAGE 0

Questa sezione descrive la fase 0 dell'implementazione del prototipo (attestazione della piattaforma e lancio del nodo di lavoro misurato).

SOLUTION OVERVIEW

*Questa fase del caso d'uso consente la creazione di quelli che vengono chiamati "**pool di calcolo**" attendibili.*

*Conosciuti anche come "**pool attendibili**", sono raggruppamenti fisici o logici di hw di elaborazione in un data center contrassegnati da policy di sicurezza specifiche e variabili e l'accesso e l'esecuzione di app e carichi di lavoro vengono monitorati, controllati, verificati, ecc.*

In questa fase della soluzione, un avvio attestato della piattaforma viene considerato come un nodo attendibile e viene aggiunto al pool attendibile.

La figura 1 illustra il concetto di pool attendibili.

Le risorse contrassegnate in verde indicano quelle affidabili.

È possibile definire criteri critici in modo che i servizi cloud sensibili alla sicurezza possano essere avviati solo su queste risorse affidabili.

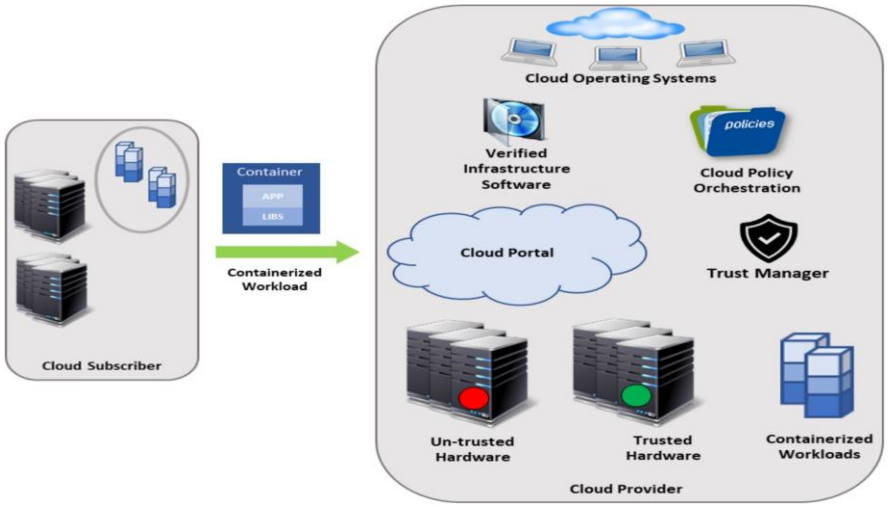


FIGURE 1: CONCEPT OF TRUSTED COMPUTE POOLS

Per avere un lancio affidabile della piattaforma, le due domande chiave a cui è necessario rispondere sono:

1) *In che modo l'entità che necessita di queste informazioni può sapere se una piattaforma specifica ha le necessarie funzionalità di sicurezza avanzate basate su hardware abilitate e se una piattaforma specifica ha un firmware della piattaforma/sistema operativo definito / conforme e un runtime del contenitore in esecuzione su di essa?*
2) *Perché l'entità che richiede queste informazioni, che in un ambiente cloud sarebbe uno scheduler/orchestrator che cerca di pianificare un carico di lavoro su un insieme di nodi/server disponibili, dovrebbe credere alla risposta della piattaforma?*

L'attestazione fornisce le risposte definitive a queste domande.

L'ATTESTAZIONE È IL PROCESSO DI FORNIRE UNA FIRMA DIGITALE DI UNA SERIE DI MISURAZIONI MEMORIZZATE IN MODO SICURO NELL'HARDWARE, QUINDI CHIEDERE AL RICHIEDENTE DI CONVALIDARE LA FIRMA E LA SERIE DI MISURAZIONI, INOLTRE, RICHIEDE RADICI DI FIDUCIA.

*La piattaforma deve avere un "**Root-of-Trust for Measurement (RTM)**" implicitamente attendibile per fornire una misurazione accurata e le funzionalità di sicurezza avanzate basate su hardware forniscono RTM.*

*La piattaforma deve anche avere un "**Root-of-Trust for Reporting (RTR)**" e un "**Root-of-Trust for Storage (RTS)**" e le stesse funzionalità di sicurezza avanzate basate su hardware forniscono questi.*

*L'entità che ha contestato la piattaforma per queste informazioni ora può determinare la fiducia della piattaforma lanciata confrontando il set di misurazioni fornito con le misurazioni "**known good/golden**".*

*Gestire il "**known good**" per diverse piattaforme e sistemi operativi e vari software BIOS e garantire che siano protetti da manomissioni e spoofing è una sfida fondamentale per le operazioni IT.*

Questa funzionalità può essere interna a un provider di servizi oppure può essere fornita come servizio da una terza parte fidata per l'utilizzo da parte di provider di servizi e aziende.

SOLUTION ARCHITECTURE

La Figura 2 fornisce una vista a più livelli dell'architettura del sistema della soluzione.

I server indicati nel pool di risorse includono un modulo hardware per la memorizzazione di chiavi e misurazioni sensibili.

Tutti i server sono configurati dal server di gestione cloud.

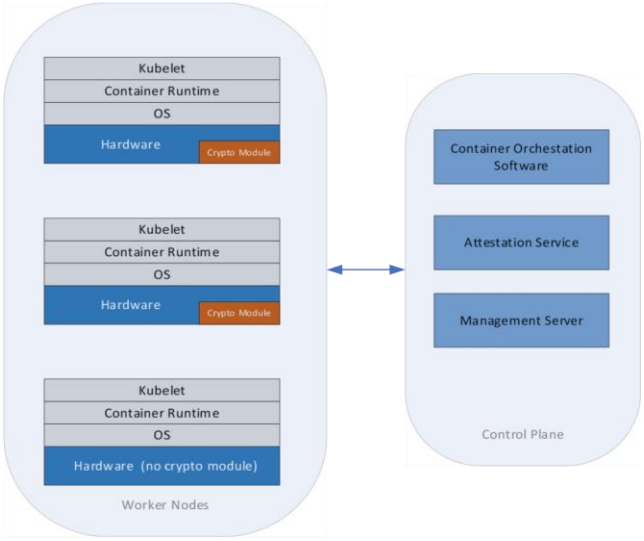


FIGURE 2: STAGE 0 SOLUTION SYSTEM ARCHITECTURE

Il passaggio iniziale nella creazione di un'istanza dell'architettura richiede il provisioning del server per funzionalità di sicurezza avanzate basate su hardware.

Ciò richiede l'accesso fisico o remoto al server per accedere al BIOS, abilitare una serie di opzioni di configurazione per utilizzare il modulo hardware (inclusa la proprietà del modulo) e attivare le funzionalità di sicurezza avanzate basate sull'hardware.

Questo processo dipende fortemente dal BIOS e dal produttore di apparecchiature originali (OEM).

Questo passaggio è obbligatorio per un avvio misurato della piattaforma.

La console di gestione fornisce il monitoraggio e la gestione remoti di tutti i server in questa architettura della soluzione.

Consente la configurazione remota del BIOS necessaria per misurare e proteggere un server.

Controlla periodicamente le misurazioni di tutti i server monitorati e le confronta con le golden measurements che sono state prese in ottime condizioni.

Quando tali misurazioni non corrispondono, indicando una compromissione della sicurezza della piattaforma, avvisa l'amministratore tramite e-mail e/o messaggio di testo.

L'amministratore può quindi utilizzare la console di gestione per intraprendere azioni correttive, che potrebbero includere lo spegnimento del server o la riconfigurazione o l'aggiornamento del firmware del server.

La piattaforma viene avviata in modo misurato e vengono misurati i componenti del BIOS e del sistema operativo (crittograficamente) e inserito nel modulo di protezione hardware del server.

Questi valori di misurazione sono accessibili tramite il server di gestione cloud tramite l'interfaccia di programmazione dell'applicazione (API).

Quando gli host vengono inizialmente configurati con il server di gestione cloud, i valori di misurazione rilevanti vengono memorizzati nella cache nel database di gestione cloud.

Oltre al lancio misurato, questa architettura della soluzione fornisce anche disposizioni per assegnare un tag di asset protetto a ciascuno dei server durante il processo di provisioning.

Il tag dell'asset viene fornito a un indice non volatile nel modulo hardware tramite un meccanismo fuori banda e su un avvio della piattaforma i contenuti dell'indice vengono inseriti/estesi nel modulo hardware.

Funzionalità di sicurezza avanzate basate su hw forniscono l'interfaccia e l'attestazione delle informazioni sull'etichetta dell'asset, inclusa la ricerca dell'etichetta dell'asset e la stringa/descrizione leggibile/presentabile dall'utente.

77. PROTOTYPING STAGE 1

Questa sezione discute lo Stage 1 dell'implementazione del prototipo (posizionamento attendibile del carico di lavoro), che si basa sul lavoro della Stage 0 e aggiunge componenti che orchestrano il posizionamento dei carichi di lavoro da avviare su piattaforme affidabili.

SOLUTION OVERVIEW

La figura 3 mostra il funzionamento della soluzione dello stadio 1. Si presuppone che il server A e il server B siano due server all'interno dello stesso cloud.

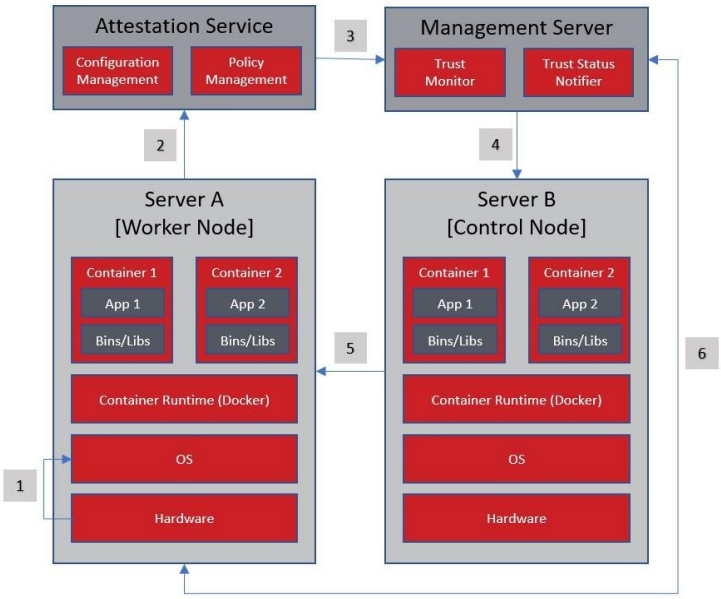


FIGURE 3: STAGE 1 SOLUTION OVERVIEW

Ci sono sei passaggi generici eseguiti nel funzionamento del prototipo dello Stage 1, come descritto di seguito e riflesso dai numeri nella Figura 3:

1) *Il server A esegue un avvio misurato, con le funzionalità di sicurezza avanzate basate su hardware che popolano le misurazioni nel modulo hardware.*
2) *Il server A invia un preventivo alla Trust Authority. Il preventivo include hash firmati di vari firmware della piattaforma e componenti del sistema operativo.*
3) *L'autorità di certificazione verifica la firma e i valori hash e invia l'attestazione dello stato di integrità della piattaforma al server di gestione.*
4) *Il server di gestione applica i requisiti dei criteri del carico di lavoro sul server B in base ai requisiti dell'utente.*
5) *Il server B avvia carichi di lavoro che richiedono un'infrastruttura affidabile solo su piattaforme server che sono state attestate come affidabili.*
6) *Ogni piattaforma server viene controllata periodicamente in base ai suoi valori di misurazione.*

SOLUTION ARCHITECTURE

L'architettura dello Stage 1 è identica all'architettura dello Stage 0 (vedere la Figura 2), con misurazioni aggiuntive correlate all'orchestrazione del posizionamento del carico di lavoro tra host attendibili.

78. PROTOTYPING STAGE 2

Questa sezione discute lo Stage 2 dell'implementazione del prototipo (posizionamento sicuro del carico di lavoro basato sull'affidabilità e sull'asset tag), che si basa sul lavoro dello Stage 1 e aggiunge componenti che tengono conto delle limitazioni delle etichette degli asset.

SOLUTION OVERVIEW

Stage 2 aggiunge il monitoraggio delle misurazioni in un dashboard di governance, rischio e conformità.

Un grafico che potrebbe apparire in tale dashboard potrebbe riflettere la dimensione relativa dei pool di server cloud affidabili e non affidabili.

Questo potrebbe essere visualizzato in percentuale e/o conteggio.

La tabella 1 è una pagina di drill-down dalla visualizzazione dashboard di alto livello. Fornisce maggiori dettagli su tutti i server all'interno del cloud.

In questo esempio, ci sono tre server.

Le informazioni elencate per ogni server includono l'indirizzo IP del server e l'Universally Unique IDentifier (UUID) e lo stato delle misurazioni (convalida dell'avvio attendibile e convalida dell'integrità del sistema- trusted boot validation and system health validation).

TABLE 1: TRUSTED BOOT COMPLIANCE VIEW

Cloud Host IP	*Hardware UUID*	*Trusted Boot Validation*	*System Health Validation*
<Host 1>	*<UUID 1>*	*Yes/No*	*Yes/No*
<Host 2>	*<UUID 2>*	*Yes/No*	*Yes/No*
<Host 3>	*<UUID 3>*	*Yes/No*	*Yes/No*

La Figura 4 mostra un'analisi dettagliata dalla Tabella 1 per un singolo server.

Include dati di misurazione dettagliati per la convalida dell'avvio affidabile, insieme allo stato della connessione e all'elenco dei tag dell'asset che possono includere il valore del tag dell'asset.

Mostra anche quando il server è stato misurato e quando scade la validità di questa misurazione.

Misurare frequentemente le caratteristiche di ogni server (ad esempio ogni cinque minuti) aiuta a ottenere una soluzione di monitoraggio continuo per i server.

General Information			
Host Info:	<IP Address or Host Name>	**UUID:**	<Unique ID>
Trust Report Created On:	<Time Stamp>	**Trust Report Expires On:**	<Time Stamp>
Asset Tag Status:	<Deployed/Not Deployed>	**Asset Tag List:**	<Name-1/Value-1> <Name-N/Value-N>
Flavor Group Name:	<Name>	**Connection Status:**	<Connected / Not connected>

Trust Information			
Overall System Trust:	<Trusted/Untrusted>		
Software Trust:	<Trusted/Untrusted>	**Platform Trust:**	<Trusted/Untrusted>
Asset Tag Trust:	<Trusted/Untrusted>	**Host Unique Trust:**	<Trusted/Untrusted>

FIGURE 4: SINGLE SERVER OVERVIEW

Nota: per ulteriori approfondimenti si rimanda alle appendice del manuale.

PARTE XV: DIGITAL TWINS [DT]

[Rif.: NIST IR 8356]

79. ABSTRACT

La tecnologia Digital Twin consente la creazione di rappresentazioni elettroniche di entità del mondo reale e la visualizzazione dello stato di tali entità.

La sua visione completa richiederà standard che non sono stati ancora sviluppati.

È relativamente nuovo sebbene utilizzi molte tecnologie di base esistenti e, in molti casi, appaia simile alle capacità di modellazione e simulazione esistenti.

Questo rapporto cerca di fornire chiarezza nella comprensione del concetto e dello scopo dei DT.

Offre una nuova definizione di DT e descrive caratteristiche, caratteristiche, funzioni e usi operativi previsti.

Il rapporto discute quindi le nuove sfide alla sicurezza informatica presentate dalle architetture dei DT.

Infine, discute le tradizionali sfide alla sicurezza informatica e considerazioni sulla fiducia nel contesto delle linee guida e dei documenti NIST esistenti.

80. DEFINITION OF DIGITAL TWINS (DT)

Attualmente, ci sono diverse "definizioni" non ufficiali per i DT: alcune create da ricercatori, alcune da comitati e consorzi per gli standard, alcune dall'industria e altre ancora che sono implicitamente suggerite da imprese commerciali che affermano che le loro applicazioni software sono "DT-compliant" nonostante l'assenza di qualsiasi definizione concordata o consenso di visione per i DT.

Nonostante la nebulosa comprensione odierna e la mancanza di una definizione formale di ciò che i DT sono realmente, o che alla fine diventeranno, la definizione di DT utilizzata in questo documento è:

"DT is the electronic representation — the digital representation — of a real-world entity, concept or notion, either physical or perceived." (DT è la rappresentazione elettronica - la rappresentazione digitale - di un'entità, un concetto o una nozione del mondo reale, fisico o percepito)

In pratica, un DT consisterà in una definizione che sarà creata e persisterà in un ambiente informatico digitale.

Le applicazioni software per computer leggeranno le definizioni dei DT per presentare a un utente umano una vista virtuale dell'oggetto del mondo reale rappresentato dal DT.

81. CYBERSECURITY CONSIDERATIONS

Le nuove tendenze nell'informatica possono sembrare poco più di un semplice rebranding della tecnologia esistente, come il cloud computing e i big data.

Tuttavia, un'analisi più attenta può rivelare che l'integrazione di componenti noti combinata con una certa maturazione nel settore ha creato nuove caratteristiche e funzionalità, e queste nuove capacità spesso comportano sfide di sicurezza informatica uniche che non necessariamente esistevano per ciascuno dei componenti.

Queste sfide potrebbero quindi richiedere nuovi approcci alla sicurezza informatica o una nuova applicazione delle tecniche tradizionali di sicurezza informatica.

Detto questo, la tradizionale sicurezza informatica necessaria per ogni singolo componente è quasi sempre ancora necessaria nella tecnologia aggregata.

La tecnologia DT non è diversa.

I componenti della tecnologia dei DT (ad esempio, dispositivi strumentali, metriche aggregate, visualizzazione e controllo remoto) non sono nuovi.

Tuttavia, nel complesso, può abilitare un nuovo e potente paradigma.

Questa sezione esplorerà le novità nella tecnologia dei DT dal punto di vista della sicurezza informatica, quali sfide presentano queste nuove funzionalità, come potrebbero essere protette e come gli approcci tradizionali di sicurezza informatica si applicano ancora ai singoli componenti e meccanismi che compongono la tecnologia dei DT.

82. NOVEL CYBERSECURITY CHALLENGES

La tecnologia dei DT ha almeno cinque nuove funzionalità che richiedono considerazioni speciali sulla sicurezza informatica:

1. *Strumentazione massiccia di oggetti (solitamente utilizzando la tecnologia IoT);*
2. *Centralizzazione delle misurazioni degli oggetti nelle definizioni dei DT;*
3. *Visualizzazione/Rappresentazione del funzionamento degli oggetti attraverso definizioni di DT;*

4. *Controllo remoto degli oggetti attraverso la manipolazione delle definizioni dei DT;*
5. *Standard per le definizioni dei DT che consentono l'accesso e il controllo universali.*

Questo elenco non è necessariamente esaustivo e con la maturazione della tecnologia dei DT sorgeranno senza dubbio ulteriori nuove sfide per la sicurezza informatica.

83. MASSIVE INSTRUMENTATION OF OBJECTS

I progressi nella tecnologia IoT hanno fornito un'ampia varietà di sensori economici e collegati in rete che possono essere utilizzati per strumentare oggetti.

Questa strumentazione può quindi alimentare le definizioni dei DT, consentendo la modellazione di oggetti del mondo reale e il monitoraggio in tempo reale (e possibilmente il controllo remoto) di molti oggetti a un livello fine di granularità.

Questo monitoraggio sarà probabilmente eseguito con sensori IoT economici e collegati in rete.

Questi sensori possono presentare vulnerabilità, capacità di elaborazione, throughput di rete, alimentazione e potenziale di aggiornamento limitati.

Ciò ha un significato per la sicurezza informatica perché il funzionamento interno dettagliato degli oggetti del mondo reale verrebbe rivelato (e possibilmente controllato) attraverso la sfera digitale.

In precedenza, tali oggetti erano protetti dalle interferenze digitali perché non erano dotati di strumentazione digitale.

Tutto ciò cambierebbe con oggetti DT strumentati (ad esempio, case "intelligenti", edifici "intelligenti" e città "intelligenti").

84. CENTRALIZATION OF OBJECT MEASUREMENTS

***Questa massiccia strumentazione di oggetti potrebbe fornire a un'entità dannosa la visibilità (e forse il controllo) sul funzionamento interno dettagliato di un oggetto attraverso la compromissione dei sensori.* RISCHIO!!**

Tuttavia, ogni sensore o controller è un dispositivo IoT separato.

Il loro numero e la loro distribuzione potrebbero impedire a un'entità maligna di assumere completamente il controllo dell'oggetto fisico strumentato.

Tuttavia, la tecnologia del DT implica la centralizzazione dei dati e il controllo dei feed dalla massiccia strumentazione di un oggetto. *Ciò crea una grande efficienza nella simulazione, modellazione e controllo,* ***ma centralizza anche i dati sensibili e le interfacce di controllo. Se la definizione del DT viene violata, l'attaccante ha accesso totale a tutti i dati sull'oggetto strumentato.***

85. VISUALIZATION/REPRESENTATION OF OBJECT OPERATION

Un utente malintenzionato con il controllo della definizione del DT e dei dati dell'oggetto strumentato potrebbe manipolare il modo in cui l'oggetto viene presentato agli utenti della definizione del DT.

C'è una forte enfasi nella tecnologia dei DT su VR e AR.

Il controllo della definizione del DT consente la manipolazione della realtà presentata all'operatore umano.

Il design di un oggetto da costruire potrebbe apparire corretto quando in realtà l'attaccante lo ha ridisegnato presentando dei difetti.

Lo stato di un oggetto monitorato potrebbe essere modificato per indurre un operatore a intraprendere un'azione che poi danneggerebbe l'oggetto o le persone e le cose intorno all'oggetto.

Un oggetto DT controllato a distanza potrebbe essere manipolato da un utente malintenzionato mentre la visualizzazione all'utente nasconde eventuali modifiche.

Poiché una definizione di DT può presentare lo stato del suo oggetto correlato attraverso più della semplice visualizzazione a un essere umano, le definizioni di DT potrebbero essere progettate per presentare rappresentazioni di oggetti ad altri sistemi digitali di consumo, comprese altre definizioni di DT.

Le definizioni dei DT possono essere costruite l'una sull'altra seguendo un modello di programmazione orientata agli oggetti (OOP).

Possono anche utilizzare una rappresentazione di un oggetto da un'altra definizione di DT per modellare oggetti che hanno un collegamento (sia fisico che virtuale).

La manipolazione di una rappresentazione di DT può quindi ingannare o corrompere le definizioni di DT correlate e altri sistemi digitali che consumano la rappresentazione dell'oggetto della definizione di DT.

86. REMOTE CONTROL OF OBJECTS

Uno degli obiettivi della tecnologia dei DT è quello di avere una simulazione dettagliata di un oggetto attraverso un'ampia strumentazione e utilizzare tale simulazione per controllare a distanza l'oggetto.

La tecnologia di controllo remoto esiste da tempo per molti tipi di oggetti; ciò che è diverso qui è l'obiettivo di costruire un facsimile digitale che sia costantemente aggiornato e di aggiungere controlli alla rappresentazione digitale pur avendo gli effetti trasmessi all'oggetto controllato.

Una definizione di DT hackerato fornirebbe quindi non solo l'accesso di un utente malintenzionato ai meccanismi di controllo remoto grezzo, ma anche a un facsimile digitale aggiornato in tempo reale con meccanismi di controllo dell'astrazione di livello forse più elevato.

Questi controlli di livello superiore sarebbero più facili da capire e da usare.

L'aggressore potrebbe manipolare questi controlli a livello di definizione del DT o a livello dei segnali grezzi del telecomando mentre inganna qualsiasi operatore umano presentando un falso facsimile digitale.

Ciò potrebbe ingannare l'utente che si affida al facsimile digitale fornito piuttosto che alle singole metriche non elaborate dell'oggetto strumentato.

87. STANDARDS FOR DT DEFINITIONS

Una spinta significativa nella comunità tecnologica dei DT è la creazione di standard per i DT che saranno adottati dagli strumenti per la creazione della definizione di DT, il monitoraggio, il collegamento agli oggetti monitorati e la manipolazione remota.

Questa spinta alla standardizzazione, in caso di successo, consentirebbe a qualsiasi strumento basato su standard di funzionare con qualsiasi definizione di DT.

Questo è un fattore significativo nell'entusiasmo per la tecnologia dei DT perché potrebbe eliminare quelli che ora sono silos proprietari di strumentazione telecomandata.

La standardizzazione, sebbene vantaggiosa in generale, potrebbe aiutare gli aggressori a sovvertire i DT.

La standardizzazione dei dispositivi IoT (e dei loro protocolli di comunicazione) utilizzati per strumentare gli oggetti potrebbe rendere più facile per gli aggressori decifrare le misurazioni e inviare comandi alla strumentazione.

La standardizzazione della rappresentazione della definizione del DT potrebbe consentire a un utente malintenzionato di sovvertire più facilmente una definizione esistente o di sostituirne una del tutto (ad esempio, con una dannosa creata dall'aggressore).

Potrebbe consentire a un utente malintenzionato di fornire più facilmente false visualizzazioni agli operatori umani.

In sintesi, la standardizzazione potrebbe ridurre notevolmente la curva di apprendimento per gli aggressori per manipolare le definizioni dei DT rimuovendo gli esclusivi meccanismi di misurazione e controllo proprietari che esistono in molti degli oggetti odierni monitorati e controllati in remoto.

Un altro possibile scenario (simile al problema attuale delle app dannose negli app store) è quello degli aggressori che creano definizioni di DT dall'aspetto utile ma dannose e le forniscono al pubblico.

Gli standard dei DT renderebbero facile per chiunque capire come scrivere una definizione di DT e quindi come crearne una falsa che potrebbe sembrare autentica.

Questo è simile ai phisher che creano messaggi di posta elettronica che sembrano legittimi ma portano gli utenti a pagine Web dannose.

Una volta pubblicate, chiunque disponga di un toolkit per DT standardizzato potrebbe quindi eseguire le definizioni dannose.

88. TRADITIONAL CYBERSECURITY CHALLENGES AND TOOLS

Sebbene le nuove sfide in materia di sicurezza informatica delle architetture dei DT siano state finora al centro dell'attenzione, ***i componenti della tecnologia dei DT hanno sfide tradizionali in materia di sicurezza informatica che devono essere affrontate****.*

Queste sfide includono le aree di riservatezza, integrità, disponibilità, manutenibilità, affidabilità e sicurezza.

Questa sezione esamina alcune di queste esigenze e gli approcci alla sicurezza informatica comunemente utilizzati per affrontarle.

Questo non vuole essere un elenco esaustivo, ma piuttosto un campione della sicurezza informatica tradizionale importante ed ovvia che dovrà essere implementata*.*

Qualsiasi sforzo serio per proteggere un sistema di DT dovrebbe seguire una guida più esauriente per la gestione del rischio.

Per i sistemi del governo degli Stati Uniti (applicabile anche a qualsiasi sistema), questo include il NIST Risk Management Framework (RMF).

Fondamentale per la sicurezza informatica di tutti i sistemi è il NIST Cybersecurity Framework; i controlli sulla privacy sono coperti dal NIST Privacy Framework.

La tecnologia Digital Twin si concentra sulla strumentazione e sul controllo di un oggetto

Sia l'implementazione del DT sia la sua strumentazione dovrebbero avere controlli di sicurezza informatica implementati e testati per proteggere dagli attacchi utilizzando un catalogo completo di controllo della sicurezza informatica (ad esempio, utilizzando il NIST Cybersecurity Framework o la pubblicazione speciale NIST 800-53, precedentemente citati.

Controlli per sistemi informativi e organizzazioni).

Per gli oggetti fisici, la sicurezza informatica dell'IoT sarà importante poiché la tecnologia dei DT si basa su una strumentazione completa.

La guida alla sicurezza informatica IoT può essere trovata nel programma NIST Cybersecurity for IoT.

Sarà importante garantire la sicurezza informatica dei dati in transito dai dispositivi IoT al repository centrale di definizione del DT.

Dovrebbero essere utilizzati algoritmi di crittografia pubblici e standardizzati poiché gli schemi di crittografia proprietari possono essere deboli e mancare di un controllo approfondito.

La definizione di DT, il suo stato attuale e i dati raccolti dovrebbero essere crittografati quando non vengono utilizzati attivamente per ottenere la sicurezza informatica dei dati a riposo.

Devono essere in atto politiche e meccanismi di governance dei dati per garantire che solo il personale corretto abbia accesso ai dati necessari all'interno di una definizione di DT.

I meccanismi di autenticazione forte devono quindi supportare questa governance per garantire che le politiche di accesso non vengano sovvertite.

Ciò può includere l'autenticazione a due o più fattori, nonché l'uso di chiavi hardware.

La sicurezza fisica del sistema DT deve essere mantenuta poiché l'accesso fisico è spesso sufficiente per aggirare molti meccanismi di sicurezza digitale. Ciò include sia la strumentazione IoT dell'oggetto monitorato sia

l'hardware che mantiene il facsimile del DT. Il software e l'hardware utilizzati per la manutenzione e la simulazione della definizione del DT dovrebbero essere progettati e testati per essere robusti e tolleranti ai guasti poiché il guasto potrebbe comportare conseguenze significative nel mondo fisico. Ciò è particolarmente vero poiché gli standard consentiranno ai programmi di DT di funzionare con un numero qualsiasi di definizioni di DT, che avranno tutte sensibilità diverse a guasti e guasti.

Infine, il sistema del DT (che copre la strumentazione, i canali di controllo/dati, la definizione del DT e i meccanismi di visualizzazione/rappresentazione) deve essere adeguatamente autorizzato dai funzionari dell'organizzazione appropriati in quanto dotato di sicurezza informatica sufficiente data la tolleranza al rischio del sistema.

Inoltre, è necessario condurre un'analisi della privacy e implementare i controlli sulla privacy sulla base di un catalogo completo di controllo della privacy se il sistema contiene dati sensibili alla privacy (ad esempio, utilizzando il NIST Privacy Framework, Privacy Framework).

Si potrebbe sostenere che, in un ambiente specializzato e sicuro, non è necessario disporre di questo livello di sicurezza informatica.

Tuttavia, anche le reti più sicure hanno solitamente delle connessioni con il mondo esterno, anche se non persistenti (es. aggiornamenti del programma tramite trasferimenti di chiavette USB o introduzione di nuovo hardware).

È meglio pianificare la sicurezza informatica sulla base di un modello "zero trust" in cui tutto fa del suo meglio per proteggersi da tutto il resto.

89. TRUST CONSIDERATION

Questa sezione analizza una serie di 14 considerazioni sulla fiducia che potrebbe essere necessario affrontare per migliorare l'utilità della tecnologia dei DT.

Non si concentra direttamente sulla valutazione del rischio e sulla mitigazione del rischio, ma piuttosto sulla fiducia.

Cioè, la tecnologia del DT fornirà la funzionalità operativa desiderata con un livello di qualità accettabile?

Rispondere a questa domanda inizia con una comprensione della fiducia.

In questo caso, la fiducia è la probabilità che il comportamento previsto e il comportamento effettivo siano equivalenti dato un contesto, un ambiente e un punto fissi nel tempo.

La fiducia è vista come un livello di fiducia.

In questa sezione, la fiducia è considerata a diversi livelli:

1) Il DT è funzionalmente equivalente all'oggetto fisico?

2) È possibile comporre un DT specifico con un altro DT?

3) Sono disponibili sufficienti informazioni sull'ambiente e sul contesto dell'oggetto fisico?

4) La tecnologia dei DT può essere standardizzata al punto in cui è possibile la certificazione dei DT?

1) **Digital Twin Creation Ordering**: il momento in cui viene creato un DT avrà un impatto sulla correttezza del DT.

Ad esempio, viene creato prima che l'oggetto fisico sia creato o è sottoposto a reverse engineering dall'entità fisica (che è destinato a rispecchiare)?

Entrambi gli approcci sono validi.

Tuttavia, la fedeltà del DT può essere ridotta se viene creato dopo che l'entità fisica esiste perché potrebbero esserci incognite interne sull'entità fisica esistente che non possono essere scoperte.

Una buona analogia qui è il software commerciale off-the-shelf (COTS). Tali prodotti sono scatole nere: il codice sorgente non è disponibile per il cliente o l'integratore e, quindi, nasconde la sintassi interna.

Per il DT, questa è una considerazione di fiducia.

2) **Temporale**: il paradigma del DT ha una componente temporale implicita, in particolare poiché si occupa di oggetti fisici e gli oggetti fisici sono vincolati dal tempo.

La teoria e la modellazione dell'affidabilità hardware afferma che gli oggetti fisici, anche quando inattivi, soffrono di livelli di decadimento nel tempo.

Ad esempio, se un'auto non è stata accesa per anni, è probabile che la batteria sia scarica e l'auto non si avvii.

Gli oggetti fisici si degradano e si affaticano nel tempo dopo l'uso.

Tuttavia, un DT non si degraderà né si affaticherà nel tempo.

Pertanto, a un certo punto i gemelli fisici e digitali saranno in conflitto a un certo livello.

Ad esempio, una parte metallica potrebbe sviluppare fratture dell'attaccatura dei capelli dopo l'uso che non sono rappresentate nel DT.

Ciò potrebbe suggerire che il DT debba essere rielaborato o mantenuto per tenerne conto.

Ad esempio, un oggetto fisico all'istante t+1 sarà probabilmente diverso dall'istante t.

Tuttavia, il DT dovrebbe essere lo stesso ai tempi t e t+1 a meno che non si aggiorni dinamicamente con i feed dall'oggetto fisico.

Avere accesso a un timestamp accurato per l'oggetto fisico e il DT è una considerazione di fiducia.

3) **Ambiente**: il paradigma del DT ha una componente ambientale implicita o esplicita che non può essere trascurata.

Per gli oggetti fisici, è necessaria una descrizione delle tolleranze ambientali o dei profili di utilizzo previsti per molte delle "anomalie", in particolare l'interoperabilità.

Ad esempio, i mattoni utilizzati per costruire edifici sono realizzati con una varietà di materiali; alcuni mattoni si rompono più facilmente sotto stress rispetto ad altri e alcuni mattoni sono più adatti a determinate temperature e climi.

Queste informazioni aggiuntive sull'utilizzo operativo previsto devono essere archiviate con un DT.

Senza questo, sarà difficile determinare se l'oggetto fisico è "adatto allo scopo" poiché lo scopo implica l'ambiente e il contesto.

Influenze ambientali sconosciute hanno afflitto sistemi e software critici per la sicurezza.

Considera l'esecuzione di PowerPoint durante una presentazione.

Di solito, il presentatore fa poco più che toccare i tasti Pagina su o Pagina giù.

Si potrebbe sostenere che il profilo operativo per l'esecuzione di PowerPoint durante una presentazione è duplice:

1) la presentazione caricata e
2) gli input dei pulsanti dal presentatore.

Tuttavia, se la presentazione procede senza intoppi (ad esempio, in modo affidabile e tempestivo) è anche una funzione di tutti gli input che PowerPoint riceve dal disco, dalla memoria e dal sistema operativo in tempo reale.

Se, ad esempio, la presentazione si blocca passando dalla diapositiva x alla diapositiva x+1, è probabile che sia coinvolto qualcosa relativo a influenze ambientali "sconosciute (ad esempio, un altro processo in esecuzione sulla macchina allo stesso tempo e che ruba risorse e cicli di calcolo).

Definire con precisione quanti più fattori ambientali possibile è una considerazione di fiducia.

4) **Difetti di produzione**: il paradigma del DT ha una relazione interessante con la produzione di massa.

Un DT può essere utilizzato per guidare un processo di produzione.

Ad esempio, una fabbrica che produce lampadine avrà una certa percentuale di difetti per mille lampadine.

Non tutte le lampadine prodotte saranno utilizzabili e per quelle utilizzabili ci saranno ancora piccole (possibilmente microscopiche) distinzioni tra le singole lampadine.

Queste piccole differenze possono influire sulla durata di una lampadina specifica.

L'imballaggio su un set di lampadine offrirà un'approssimazione per quanto tempo una lampadina funzionerà prima del burnout.

Ciò evidenzia che un DT potrebbe non solo descrivere i componenti sottostanti di una lampadina media, ma anche suggerire come dovrebbe essere prodotto se la rappresentazione dettaglia anche una metrica, come il tempo per esaurirsi.

Garantire che un processo di produzione produca un prodotto con la corretta aspettativa di vita in base alle informazioni in un DT è una considerazione di fiducia.

5) **Equivalenza funzionale**: il paradigma del DT necessita di un mezzo per determinare l'equivalenza funzionale tra il DT e l'oggetto fisico.

Senza questo, la fiducia è sospetta.

Se il DT è una specifica eseguibile, per gli input che viene alimentato, dovrebbe produrre gli stessi output che l'oggetto fisico produce per gli stessi dati di input.

Se ciò non si verifica, l'equivalenza funzionale non è stata raggiunta.

Ciò potrebbe verificarsi per una varietà di fattori, come decadimento e affaticamento, variazioni di produzione o altre influenze ambientali che l'oggetto fisico subisce durante il funzionamento ma che il DT no.

Senza una qualche valutazione del livello di equivalenza funzionale è difficile sostenere l'affidabilità.

6) **Componibilità e complessità**: c'è una considerazione di fiducia per quanto riguarda le dimensioni e la complessità del DT per il suo oggetto fisico.

Un DT troppo complicato può creare un problema di componibilità in termini di previsione dell'affidabilità di un sistema composto finale da più di un DT.

Supponiamo che un sistema abbia cinque componenti fisici e ogni componente abbia un DT.

Il collegamento fisico dei cinque componenti può essere semplice, ma la composizione dei cinque DT potrebbe non esserlo, in particolare se i DT contengono informazioni come le tolleranze e gli usi operativi previsti.

Gli standard dovrebbero essere utili per eliminare le informazioni estranee contenute in un DT poiché gli standard possono definire le interconnessioni richieste tra i componenti di un dominio consentendo di modellare e testare la composizione.

Un approccio potrebbe essere quello di separare le classi di informazioni in categorie, come "necessità di sapere" o "estraneo".

7) **Strumentazione e monitoraggio**: la strumentazione di un DT è un vantaggio unico e vantaggioso offerto dai DT.

Mentre uno potrebbe non essere in grado di strumentare l'oggetto fisico, potrebbe essere in grado di strumentare il DT.

Tuttavia, la strumentazione e le sonde non sono così semplici o facili da iniettare correttamente in un DT come ci si potrebbe aspettare; molto si può imparare qui dalla comunità dei software critici per la sicurezza.

Innanzitutto, è necessaria una determinazione di dove iniettare le sonde; questo spesso non è facile e può essere più arte che scienza.

In secondo luogo, anche il numero di sonde da iniettare è una considerazione.

Come mostrato nei sistemi in tempo reale, le sonde possono rallentare le prestazioni e i tempi.

Ciò potrebbe causare un problema per la sincronizzazione tra il DT e l'oggetto fisico.

Detto questo, ci sono modi per ridurre questo impatto facendo in modo che le sonde raccolgano solo dati grezzi e non calcolino i risultati dei test interni, come gli autotest incorporati.

La raccolta delle informazioni "giuste" dallo stato interno di un DT in esecuzione è uno sforzo costoso e soggetto a errori.

8) **Eterogeneità degli standard**: l'eterogeneità dei diversi formati per i DT può causare problemi di componibilità.

Se i fornitori utilizzano in modo improprio formati standardizzati per i DT dei loro componenti, la composizione di DT da diversi fornitori di componenti potrebbe non essere realizzabile.

Questa è una considerazione per la fiducia nei DT composti.

9) **Requisiti non funzionali**: una considerazione sulla fiducia per i sistemi composti da molti componenti si occupa di attributi di qualità spesso denominati "**ilities**".

Questo vale anche per la tecnologia dei DT.

I requisiti funzionali stabiliscono cosa deve fare un sistema; i requisiti negativi stabiliscono ciò che un sistema non deve fare; e i requisiti non funzionali (cioè, le "ilities") tipicamente stabiliscono quale livello di qualità il sistema deve mostrare sia per i requisiti funzionali che per quelli negativi.

Le "ilities" si applicano sia alle "cose" che ai sistemi in cui sono integrate.

Non è chiaro quante "ilities" ci siano, anche se gli esempi includono disponibilità, componibilità, compatibilità, affidabilità, rilevabilità, durabilità, tolleranza ai guasti, flessibilità, interoperabilità, assicurabilità, responsabilità, manutenibilità, osservabilità, privacy, prestazioni, portabilità, prevedibilità, probabilità di fallimento, leggibilità, affidabilità, resilienza, raggiungibilità, sicurezza, scalabilità, sicurezza informatica, sostenibilità, testabilità, tracciabilità, usabilità, visibilità e vulnerabilità.

Il problema per la tecnologia del DT riguarda quanti dei requisiti non funzionali possono essere scritti per i requisiti funzionali e negativi (definendo così il livello di qualità per ciò che il sistema dovrebbe e non dovrebbe fare).

La capacità di scrivere questi requisiti non funzionali influenzerà la capacità di rivendicare l'affidabilità di un oggetto composito.

10. ***PRECISIONE DEL DT****: se l'accuratezza di un DT è discutibile o addirittura ritenuta difettosa, la fiducia è un problema.*

Per il software, specifiche difettose portano a progetti difettosi che portano a implementazioni difettose.

Nella tecnologia del DT, il grado di correttezza del DT è una considerazione di fiducia.

Si pone la domanda se potrebbe essere prudente avere più di un DT creato in modo indipendente per uno specifico oggetto fisico.

Nella programmazione in versione n, viene creata più di un'implementazione software indipendente per sistemi altamente critici che il software impatta perché nessuna singola implementazione può essere considerata adeguatamente affidabile.

Per risolvere questo problema, ogni implementazione indipendente viene eseguita in parallelo e gli output di ciascuna implementazione sono inviati a un votante che quindi decide l'output finale che il sistema riceve.

11. ***TEST****: la testabilità dei DT si riferisce alla misurazione della probabilità che un errore o un difetto venga rilevato durante il test.*

I sistemi che hanno meno probabilità di rivelare la presenza di difetti sono considerati meno testabili.

Gli oggetti fisici sono testabili a diversi livelli utilizzando questa definizione, sebbene i metodi per testare i DT che hanno maggiori probabilità di dimostrare che la rappresentazione digitale è corretta non sono chiari.

Un'opzione è ignorare questa considerazione di fiducia e decidere che un DT non è testabile e, quindi, si pone da solo come "oracolo" o "gold standard".

Inoltre, sebbene i test di solito implichino casi d'uso previsti, è opportuno prendere in considerazione anche i casi di uso improprio.

12. ***CERTIFICAZIONE****: la certificazione di solito avviene in due modi diversi.*

Un tipo certifica il processo utilizzato per lo sviluppo, mentre l'altro certifica il manufatto finale che proviene da quel processo.

Questi due tipi di certificazione sono distinti.

Per la tecnologia del DT, ciò significa che si potrebbe tentare di certificare come è stato creato il DT o certificare l'accuratezza del DT stesso.

La certificazione di un gemello sarà complicata.

Ad esempio, l'industria farmaceutica ha chiarito il problema del sovraccarico di informazioni.

La maggior parte dei farmaci da prescrizione viene fornita con avvertenze su chi può assumerli in base a sesso, età, condizioni di base, interazioni farmacologiche negative e altri fattori.

La maggior parte dei farmaci viene fornita con esclusioni di responsabilità sugli effetti collaterali negativi e su quando interromperne l'uso.

Queste informazioni vengono messe a disposizione di pazienti, medici, farmacisti e altri fornitori di servizi sanitari.

Il problema deriva dalla grande quantità di informazioni note su un farmaco e dalla più vasta quantità di informazioni sconosciute su un farmaco al tempo t che non saranno note fino al tempo t+1.

Inoltre, la maggior parte delle informazioni è comprensibile solo da esperti medici, ma è fondamentale per determinare l'idoneità di un farmaco allo scopo.

La considerazione della fiducia qui per la tecnologia del DT è la quantità di queste informazioni che possono essere fornite in una descrizione del DT senza sovraccaricare un gemello con informazioni estranee che portano a confusione su come usare il gemello o cosa rappresenta il gemello.

13. ***PROPAGAZIONE****: una delle maggiori preoccupazioni per la fiducia in qualsiasi sistema di sistemi è il modo in cui errori e dati corrotti si propagano (a cascata) durante l'esecuzione.*

Il paradigma del DT sperimenta questa considerazione della fiducia, in particolare quando sono composti diversi gemelli che rappresentano diversi oggetti fisici.

Questo potrebbe, forse, suggerire che i gemelli dovrebbero essere avvolti con pre-condizioni e post-condizioni per determinare se l'output di un gemello sarà accettabile come input per un altro gemello.

14. ***CONTRAFFAZIONE****: è possibile che un DT possa essere manomesso o contraffatto.*

Ci sono schemi che potrebbero essere usati per proteggersi da questo.

I DT possono essere sottoposti ad hashing e l'hash può essere pubblicato su una pagina web pubblica; gli utenti di un DT potrebbero eseguire l'hashing della propria copia e confrontarla con l'hash sulla pagina Web pubblica.

Detto questo, le pagine web e altri archivi simili accessibili pubblicamente possono essere violati.

Per aumentare la fiducia qui si potrebbe utilizzare una blockchain e pubblicare un DT hash pubblicamente in una struttura dati immutabile (non potrebbe mai essere modificata nemmeno da aggressori malintenzionati).

In questi modi è possibile scoprire modifiche ai file dei DT.

In alternativa, è possibile archiviare copie identiche di un DT in posizioni separate (ad esempio, in backup offline).

PARTE XVI: IIOT: CYBERS. FOR DISTRIBUTED ENERGY RESOURCES (DER)

[Rif.: NIST SP 1800-32B]

90. ABSTRACT

L'Industrial Internet of Things (IIoT), si riferisce all'applicazione di strumentazione e sensori collegati e altri dispositivi a macchinari e veicoli nei settori dei trasporti, dell'energia e di altre infrastrutture critiche.

Nel settore energetico, le risorse energetiche distribuite (Distributed Energy Resources - DER) come il solare fotovoltaico e le turbine eoliche includono sensori, sistemi di trasferimento dati e comunicazione, strumenti e altri dispositivi disponibili in commercio collegati in rete.

I DER introducono scambi di informazioni tra il sistema di controllo della distribuzione di un'utilità e i DER per gestire il flusso di energia nella rete di distribuzione.

Questa guida pratica esplora come gli scambi di informazioni tra DER su scala commerciale e di utilità e le operazioni della rete di distribuzione elettrica possono essere monitorati e protetti da alcune minacce e vulnerabilità alla sicurezza informatica.

L'NCCoE ha creato un'architettura di riferimento utilizzando prodotti disponibili in commercio per mostrare alle organizzazioni come è possibile applicare diverse funzionalità di sicurezza informatica, tra cui comunicazioni e integrità dei dati, rilevamento di malware, monitoraggio della rete, autenticazione e controllo degli accessi e analisi e visualizzazione basate su cloud per proteggere gli endpoint distribuiti e ridurre la superficie di attacco IIoT per i DER.

91. SOLUTION

L'NCCoE ha collaborato con le parti interessate nel settore dell'elettricità, UMD e fornitori di tecnologie di sicurezza informatica per costruire un ambiente che rappresenta un'utilità di distribuzione interconnessa con una microgrid DER del campus.

All'interno di questo ecosistema, esploriamo come gli scambi di informazioni tra DER e le operazioni della rete di distribuzione elettrica possono essere protetti da alcuni compromessi della sicurezza informatica.

La soluzione di esempio dimostra le seguenti funzionalità:

- ✓ **COMUNICAZIONI E INTEGRITÀ DEI DATI** *per garantire che le informazioni non vengano modificate durante il transito;*
- ✓ **AUTENTICAZIONE E CONTROLLO DEGLI ACCESSI** *per garantire che solo i sistemi noti e autorizzati possano scambiare informazioni;*
- ✓ **REGISTRO DEI COMANDI** *che mantiene un registro indipendente e immutabile degli scambi di informazioni tra la rete di distribuzione e gli operatori DER;*
- ✓ **RILEVAMENTO DI MALWARE** *per monitorare lo scambio di informazioni e l'elaborazione per identificare potenziali infezioni da malware;*
- ✓ **MONITORAGGIO COMPORTAMENTALE** *per rilevare deviazioni dalle norme operative;*
- ✓ **PROCESSI DI ANALISI E VISUALIZZAZIONE** *per monitorare i dati, identificare anomalie e allertare gli operatori.*

La soluzione di esempio documentata nella guida pratica utilizza le tecnologie e le capacità di sicurezza dei nostri collaboratori del progetto.

La soluzione è in linea con gli standard di sicurezza e le linee guida del NIST Cybersecurity Framework; NIST Interagency o Internal Report 7628 Revisione 1: Linee guida per la sicurezza informatica delle reti intelligenti; e l'Institute of Electrical and Electronics Engineers (IEEE) 1547-2018, IEEE Standard for Interconnection and Interoperability of Distributed Energy Resources with Associated Electric Power Systems Interfaces.

92. SECURITY CONTROL MAP AND TECHNOLOGIES

La Tabella 3-1 mappa le caratteristiche di sicurezza della nostra architettura di riferimento alle funzioni, categorie e sottocategorie di sicurezza del NIST Cybersecurity Framework che supporta.

Le tecnologie utilizzate in questo progetto sono mappate nelle sottocategorie del Cybersecurity Framework supportate.

Abbiamo selezionato le sottocategorie che affrontano le minacce, le vulnerabilità e i rischi discussi sopra.

La tua organizzazione può utilizzare la Tabella 3-1 per identificare i corrispondenti controlli NIST SP 800-53 necessari per ottenere i risultati desiderati.

Sebbene la nostra architettura di riferimento si concentri sulle funzioni di protezione e rilevamento del Cybersecurity Framework, nel framework sono presenti più funzioni, categorie e sottocategorie di quante ne compaiano qui.

La tua organizzazione dovrebbe selezionare le sottocategorie e i controlli del Cybersecurity Framework che aiutano a mitigare i rischi di sicurezza informatica specifici della tua azienda.

NOTA: per praticità, la Tabella 3.1 non è stata riportata ed è visibile nel manuale NIST SP 1800-32B

93. CYBERSECURITY WORKFORCE CONSIDERATIONS

La Tabella 3-2 identifica i ruoli di lavoro della sicurezza informatica che più si allineano con le categorie e le sottocategorie di sicurezza del Cybersecurity Framework dimostrate nella nostra architettura di riferimento.

I ruoli di lavoro si basano sul quadro della forza lavoro della National Initiative for Cybersecurity Education (NICE) per la sicurezza informatica (NICE Framework).

Si noti che i ruoli di lavoro mostrati possono essere applicati a più di una categoria di framework di sicurezza informatica NIST.

Ulteriori informazioni su NICE e altri ruoli lavorativi sono disponibili in NIST SP 800-181 Revisione 1, Workforce Framework for Cybersecurity (NICE Framework).

NOTA: per praticità, la Tabella 3.2 non è stata riportata ed è visibile nel manuale NIST SP 1800-32B

94. ARCHITECTURE

Lo standard IEEE 1547-2018, IEEE Standard for Interconnection and Interoperability of Distributed Energy Resources with Associated Electric Power Systems Interfaces richiede che un DER abbia un'interfaccia di comunicazione per lo scambio di informazioni di monitoraggio e controllo con l'operatore dei sistemi di alimentazione elettrica dell'area (Electric Power Systems - EPS).

Lo standard definisce il set minimo di informazioni che il DER deve essere in grado di scambiare con l'operatore di area EPS.

Questa architettura affronta la sicurezza di questi scambi di informazioni.

Questa architettura aiuta a garantire che sia l'operatore DER che l'utilità locale abbiano la certezza che gli scambi di informazioni siano legittimi.

Questa pubblicazione si riferisce all'operatore dell'area EPS come a un'utilità locale.

NOTA: per praticità, il dettaglio di questo capitolo è visibile nel manuale NIST SP 1800-32B

95. SECURITY CHARACTERISTIC ANALYSIS

Questa sezione discute i risultati di una valutazione completa della sicurezza dell'architettura di riferimento mostrata nella Figura 1 e il modo in cui supporta le sottocategorie del Cybersecurity Framework che abbiamo identificato e mappato nella Tabella 3-1.

Lo scopo dell'analisi delle caratteristiche di sicurezza è capire fino a che punto la soluzione di esempio del progetto soddisfa il suo obiettivo di dimostrare che gli scambi di informazioni tra DER e le operazioni della rete di distribuzione elettrica possono essere monitorati e protetti da alcuni compromessi della sicurezza informatica.

Inoltre, cerca di comprendere i vantaggi e gli svantaggi in termini di sicurezza della soluzione di esempio.

NOTA: per praticità, il dettaglio di questo capitolo è visibile nel manuale NIST SP 1800-32B, all'interno del quale sono descritti gli scenari di esempio.

PARTE XVII: ARTIFICIAL INTELLIGENCE [AI] – MACHINE LEARNING [ML]

[Rif.: NIST IR 8360; NIST IR 8269]

Questo NIST Interagency/Internal Report (NISTIR) è ***inteso come un passo verso la protezione delle applicazioni dell'Intelligenza Artificiale (AI)****, in particolare contro le manipolazioni contraddittorie del Machine Learning (ML),* ***sviluppando una tassonomia e una terminologia dell'Adversarial Machine Learning (AML)****.*

L'AML si occupa della progettazione di algoritmi ML in grado di resistere alle sfide di sicurezza, dello studio delle capacità degli aggressori e della comprensione delle conseguenze degli attacchi*.*

Nella sicurezza informatica più in generale (NIST Glossary of Key Information Security Terms, NISTIR 7298, Revision 2), sia la robustezza sia la resilienza sono misurate dal rischio, che è una misura della misura in cui un'entità (ad esempio un sistema) è minacciata da una circostanza o un evento potenziale (ad es. attacco).

Pertanto, questa nozione generale di rischio offre un approccio utile per valutare e gestire la sicurezza dei componenti ML.

Come introdotto nella Guida del NIST per la conduzione delle valutazioni dei rischi (NIST 800-30, revisione 1):

> *La valutazione del rischio è una delle componenti fondamentali di un processo di gestione del rischio organizzativo...*
>
> *Lo scopo delle valutazioni del rischio è informare i decisori e supportare le risposte al rischio identificando:*
>
> *(i) minacce rilevanti alle organizzazioni o minacce dirette attraverso organizzazioni contro altre organizzazioni;*
>
> *(ii) vulnerabilità sia interne che esterne alle organizzazioni;*
>
> *(iii) impatto (vale a dire, danno) alle organizzazioni che può verificarsi dato il potenziale di minacce che sfruttano le vulnerabilità; e*
>
> *(iv) probabilità che si verifichi un danno.*

Su tale base, un approccio basato sul rischio comincerebbe identificando le minacce, le vulnerabilità e gli impatti rilevanti.

Nel caso di AML, ***le minacce sono definite dai tipi di attacchi e dai contesti contraddittori*** *in cui possono verificarsi gli attacchi;* ***le vulnerabilità sono definite dai tipi di difese*** *o dalla loro mancanza, per prevenire o mitigare gli attacchi; e gli* ***impatti sono definiti dalle conseguenze che derivano dagli attacchi e dalle difese associate contro tali attacchi****.*

96. A TAXONOMY AND TERMINOLOGY OF ADVERSARIAL MACHINE LEARNING

La tassonomia si basa su documenti pubblicati di recente che esaminano la letteratura AML e offrono tassonomie di attacchi e difese.

I livelli più alti della tassonomia risultante includono vari aspetti di attacchi e difese, come illustrato dalla Figura 1 nel contesto delle fasi di addestramento e test (inferenza) della pipeline di apprendimento automatico.

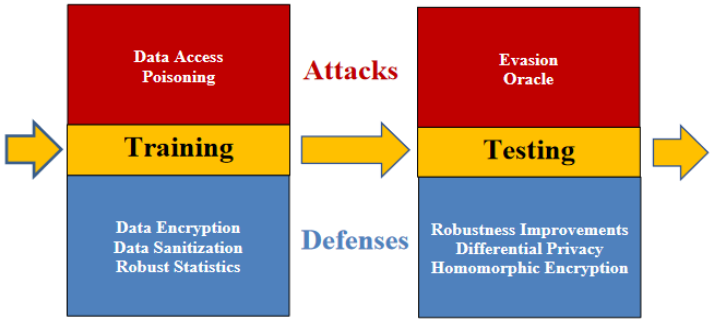


Figure 1. An illustration of example Attacks and Defenses in the Machine Learning Pipeline.

La Figura 2 organizza questi livelli(superiori e inferiori) della tassonomia in modo gerarchico lungo le tre dimensioni di Attacchi, Difese e Conseguenze.

La terza dimensione, Conseguenze, non compare nelle altre tassonomie sopra citate e invece è stata affrontata da altri autori come un aspetto degli Attacchi che si occupa dell'intento dell'avversario.

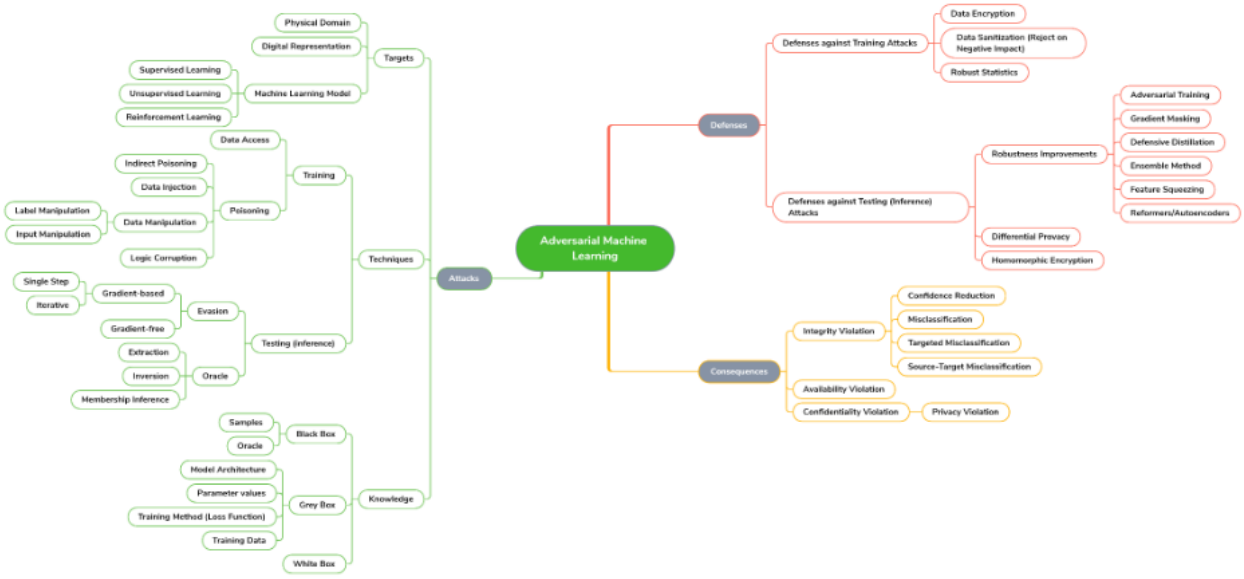


Figure 2. Taxonomy of Attacks, Defenses, and Consequences in Adversarial Machine Learning

1. *Attacks*
   a. *Targets*
      i. *Physical Domain (of input sensors or output actions)*
      ii. *Digital Representation*
      iii. *Machine Learning Model*
         1. *Supervised Learning*
         2. *Unsupervised Learning*
         3. *Reinforcement Learning*
   b. *Techniques*
      i. *Training*
         1. *Data Access*
         2. *Poisoning*
            a. *Indirect Poisoning*
            b. *Direct Poisoning*
               i. *Data Injection*
               ii. *Data Manipulation*

1. *Label Manipulation*
2. *Input Manipulation*

iii. *Logic Corruption*

ii. *Testing (Inference)*

1. *Evasion*
   a. *Gradient-based*
      i. *Single Step*
      ii. *Iterative*
   b. *Gradient-free*
   c. *Oracle*
      i. *Extraction*
      ii. *Inversion*
      iii. *Membership Inference*

c. *Knowledge*

i. *Black Box*

1. *Samples*
2. *Oracle*

ii. *Gray Box*

1. *Model Architecture*
2. *Parameters Values*
3. *Training Method (Loss Function)*
4. *Training Data iii. White Box*

2. *Defenses*

a. *Defenses Against Training Attacks*

i. *Data Encryption*

ii. *Data Sanitization (Reject on Negative Impact)*

iii. *Robust Statistics*

b. *Defenses Against Testing (Inference) Attacks*

i. *Robustness Improvements*

1. *Adversarial Training*
2. *Gradient Masking*
3. *Defensive Distillation*
4. *Ensemble Method*
5. *Feature Squeezing*
6. *Reformers/Autoencoders*

ii. *Differential Privacy*

iii. *Homomorphic Encryption*

3. *Consequences*

a. *Integrity Violation*

i. *Confidence Reduction*

ii. *Misclassification*

iii. *Targeted Misclassification*

iv. *Source-Target Misclassification*

b. *Availability Violation*

c. *Confidentiality Violation*

i. *Privacy Violation*

1 - ATTACKS

I componenti ML possono essere bersagli di attacchi da parte di avversari che utilizzano varie Tecniche e Conoscenze sui sistemi.

TARGETS

Gli obiettivi degli attacchi sono definiti dalle fasi della pipeline ML, tra cui il Dominio Fisico dei sensori di input, la Rappresentazione Digitale per la pre-elaborazione, il modello di Apprendimento Automatico (ML) stesso o il Dominio Fisico delle azioni di output.

I tipi di metodi che generano un modello di apprendimento automatico (Machine Learning Model) includono l'apprendimento supervisionato (Supervised Learning), l'apprendimento non supervisionato (Unsupervised Learning) e l'apprendimento per rinforzo (Reinforcement Learning).

1°. *Nel* **SUPERVISED LEARNING**, *i dati di addestramento sono forniti sotto forma di input etichettati con output corrispondenti e il modello apprende una mappatura tra input e output. L'attività di apprendimento è definita* ***classificazione*** quando gli output assumono valori categoriali *e* ***regressione*** quando gli output assumono valori numerici.

2°. *In* **SUPERVISED LEARNING**, *i dati di addestramento sono input senza etichetta e il modello apprende una struttura sottostante dei dati. Ad esempio, il modello può eseguire il raggruppamento di input in base a una metrica di somiglianza o una riduzione della dimensionalità per proiettare i dati in sottospazi dimensionali inferiori.*

3°. *In* **REINFORCEMENT LEARNING**, *una politica basata sulla ricompensa (reward-based) per agire in un ambiente è appresa dai dati di addestramento rappresentati come sequenze di azioni, osservazioni e ricompense. In alcune applicazioni, Reinforcement Learning può essere combinato con l'apprendimento supervisionato e l'apprendimento non supervisionato.*

TECHNIQUES

*Le tecniche contraddittorie (*ADVERSARIAL TECHNIQUES*) utilizzate per lanciare attacchi contro obiettivi possono applicarsi alle fasi di addestramento o test (*INFERENZA*) del funzionamento del sistema.*

Gli attacchi nella fase di addestramento tentano di acquisire o influenzare i dati di addestramento o il modello stesso.

Negli attacchi di accesso ai dati, è possibile accedere ad alcuni o tutti i dati di addestramento e possono essere utilizzati per creare un modello sostitutivo.

*Questo modello sostitutivo può quindi essere utilizzato per testare l'efficacia di potenziali input prima di inviarli come Attacchi nella fase operativa di Test (*INFERENZA*).*

*Nell'avvelenamento (*POISONING*) , noto anche come attacchi causali (*CAUSATIVE ATTACKS*), i dati o il modello vengono alterati indirettamente o direttamente.*

Nell'avvelenamento indiretto, gli avversari senza accesso ai dati preelaborati utilizzati dal modello di destinazione devono invece avvelenare i dati prima della preelaborazione.

Nell'avvelenamento diretto, i dati vengono alterati da DATA INJECTION *o* DATA MANIPULATION*, oppure il modello viene alterato direttamente da* LOGIC CORRUPTION*.*

In Data Injection, gli input contraddittori sono inseriti nei dati di training originali, modificando in tal modo la distribuzione dei dati sottostanti senza modificare le caratteristiche o le etichette dei dati di training originali.

I campioni contraddittori iniettati possono essere ottimizzati mediante metodi di programmazione lineare che spostano il confine decisionale di un modello centrale (in UNSUPERVISED LEARNING*) o mediante ascesa del gradiente sull'errore di test del modello per degradare l'accuratezza della classificazione (in* SUPERVISED LEARNING*).*

La manipolazione dei dati comporta la modifica in contraddittorio delle etichette di output (Label Manipulation) e dei dati di input (Input Manipulation) dei dati di addestramento originali.

La corruzione logica è compiuta da un avversario che può manomettere l'algoritmo ML e quindi alterare il processo di apprendimento e il modello stesso.

Gli **ATTACCHI NELLA FASE DI TEST (INFERENZA)**, *noti anche come attacchi esplorativi (*EXPLORATORY ATTACKS*), non alterano il modello di destinazione o i dati utilizzati nell'addestramento.*

Invece questi attacchi generano esempi contraddittori come input che sono in grado di eludere la corretta classificazione dell'output da parte del modello, in EVASION ATTACKS, *o raccogliere e dedurre informazioni sul modello o dati di addestramento, in* ORACLE ATTACKS.

In **EVASION ATTACKS**, *l'avversario risolve un problema di ottimizzazione vincolata per trovare una piccola perturbazione dell'input che provoca un grande cambiamento nella funzione di perdita e risulta in una classificazione errata dell'output.*

In **ORACLE ATTACKS**, *un avversario utilizza un'interfaccia di programmazione dell'applicazione per presentare il modello con gli input e per osservare gli output del modello.*

Anche quando l'avversario non ha una conoscenza diretta del modello stesso, gli accoppiamenti input-output ottenuti da ORACLE ATTACKS *possono essere utilizzati per addestrare un modello sostitutivo che opera in modo molto simile al modello di destinazione, a causa della proprietà di trasferibilità esibita da molte architetture di modello.*

Questo modello sostitutivo, a sua volta, può quindi essere utilizzato per generare esempi contraddittori da utilizzare negli attacchi di evasione contro il modello bersaglio.

Gli **ORACLE ATTACKS** *includono* **EXTRACTION ATTACKS**, **INVERSION ATTACKS** *e* **MEMBERSHIP INFERENCE ATTACKS**.

Questi attacchi raccolgono informazioni come output e valori di confidenza, per dedurre parametri o caratteristiche del modello o dei dati.

In **EXTRACTION ATTACKS**, *un avversario estrae i parametri o la struttura del modello dalle osservazioni delle previsioni del modello, includendo tipicamente le probabilità restituite per ogni classe.*

Nel caso di **INVERSION ATTACK**, *le caratteristiche dedotte possono consentire all'avversario di ricostruire i dati utilizzati per addestrare il modello, comprese le informazioni personali che violano la privacy di un individuo.*

In un **MEMBERSHIP INFERENCE ATTACK**, *l'avversario utilizza i ritorni delle query del modello di destinazione per determinare se punti dati specifici appartengono alla stessa distribuzione del set di dati di addestramento, sfruttando le differenze nella confidenza del modello sui punti che sono stati o non sono stati visti durante l'addestramento.*

KNOWLEDGE

Oltre alle tecniche utilizzate per lanciare gli attacchi contro i bersagli, le minacce ai componenti di Machine Learning dipendono anche dalla conoscenza dell'avversario del modello di destinazione.

In **BLACK BOX ATTACKS**, *l'avversario non ha alcuna conoscenza del modello eccetto campioni input-output di dati di addestramento o accoppiamenti input-output ottenuti utilizzando il modello di destinazione come un Oracle.*

In **GREY BOX ATTACKS**, *l'avversario ha informazioni parziali sul modello, che possono includere l'architettura del modello, i valori dei parametri, il metodo di addestramento (funzione di perdita) o i dati di addestramento.*

In **WHITE BOX ATTACKS**, *l'avversario ha una conoscenza completa del modello, inclusi architettura, parametri, metodi e dati. Anche quando un avversario non ha la conoscenza completa necessaria per un attacco White Box, gli attacchi Data Access o Oracle che producono accoppiamenti input-output possono essere utilizzati per addestrare un modello sostitutivo, che funziona in modo molto simile al modello reale a causa della proprietà di trasferibilità esibita da molte architetture modello. Questo modello sostitutivo può quindi essere utilizzato come White Box per generare esempi contraddittori da utilizzare negli attacchi di evasione.*

2 - DEFENSES

Le difese possono essere caratterizzate dal fatto che si applichino agli attacchi lanciati contro le fasi di addestramento o di test (inferenza) del funzionamento del sistema.

In entrambi i casi, i metodi difensivi spesso possono comportare un sovraccarico delle prestazioni e avere un effetto dannoso sull'accuratezza del modello.

Le **DEFENSES AGAINST TRAINING ATTACKS** *che coinvolgono l'accesso ai dati includono tradizionali misure di controllo degli accessi come la crittografia dei dati.*

Le difese contro gli **POISONING ATTACKS** *includono la sanificazione dei dati e statistiche robuste.*

In **DATA SANITIZATION**, *gli esempi contraddittori sono identificati testando l'impatto degli esempi sulle prestazioni di classificazione.*

Gli esempi che causano alti tassi di errore nella classificazione sono quindi rimossi dal training set, in un approccio noto come REJECT ON NEGATIVE IMPACT.

Le **DEFENSES AGAINST TESTING (INFERENCE) ATTACKS** *includono vari miglioramenti della robustezza del modello, tra cui* ADVERSARIAL TRAINING, GRADIENT MASKING, DEFENSIVE DISTILLATION, ENSEMBLE METHODS, FEATURE SQUEEZING *e* REFORMERS/AUTOENCODER.

Sebbene utilizzate come difese contro gli attacchi effettuati nella fase di Test (Inferenza), queste Difese sono schierate dal difensore nella fase di Addestramento che precede il Test (Inferenza).

In **ADVERSARIAL TRAINING**, *gli input contenenti perturbazioni contraddittorie ma con etichette di output corrette sono iniettati nei dati di training al fine di ridurre al minimo gli errori di classificazione causati da esempi contraddittori.*

Il **GRADIENT MASKING** *riduce la sensibilità del modello a piccole perturbazioni negli input calcolando le derivate del primo ordine del modello rispetto ai suoi input e riducendo al minimo queste derivate durante la fase di apprendimento.*

Un'idea simile motiva **DEFENSIVE DISTILLATION**, *in cui un modello di destinazione è utilizzato per addestrare un modello più piccolo che presenta una superficie di output più liscia e* **METODI ENSEMBLE**, *in cui più classificatori sono addestrati insieme e combinati per migliorare la robustezza.*

Allo stesso modo, **FEATURE SQUEEZING**, *mostrato nella Figura 4, utilizza trasformazioni di livellamento delle funzionalità di input nel tentativo di annullare le perturbazioni contraddittorie.*

I riformatori prendono un dato input e lo spingono verso l'esempio più vicino nel set di addestramento, in genere utilizzando reti neurali chiamate Autoencoder, per contrastare le perturbazioni contraddittorie.

Figure 4. An example of Feature Squeezing, which smooths inputs to remove adversarial inputs [

È importante riconoscere che l'avversario può sconfiggere vari ROBUSTNESS IMPROVEMENT DEFENSES *lanciando* DATA ACCESS *o* ORACLE ATTACKS *per ottenere accoppiamenti input-output.*

Questi abbinamenti possono essere successivamente utilizzati per addestrare un modello sostitutivo che non maschera i gradienti o uscite uniformi come il modello di destinazione.

Il modello sostitutivo può quindi essere utilizzato come **WHITE BOX** *per creare esempi contraddittori, sfruttando la proprietà di trasferibilità dei ML-trained models, quindi può essere difficile difendersi dagli di* EVASION ATTACKS *da parte di un avversario in grado di creare un modello sostitutivo.*

PRIVACY

Oltre ai ROBUSTNESS IMPROVEMENTS *sopra menzionati, le* DEFENSES AGAINST TESTING *(*INFERENZA*) includono anche meccanismi di randomizzazione applicati ai dati di addestramento o agli output del modello per fornire garanzie di* DIFFERENTIAL PRIVACY.

La DIFFERENTIAL PRIVACY *formula la privacy come una proprietà soddisfatta da un meccanismo di randomizzazione su coppie di dataset adiacenti.*

In definitiva, la proprietà DIFFERENTIAL PRIVACY *garantisce che gli output del modello non rivelino alcuna informazione aggiuntiva su un singolo record incluso nei dati di addestramento.*

Tuttavia, esiste un compromesso intrinseco delle prestazioni perché l'accuratezza della previsione di un modello è degradata dai meccanismi di randomizzazione utilizzati per ottenere la privacy differenziale.

*Un approccio alternativo è la crittografia omomorfica (***HOMOMORPHIC ENCRYPTION***), che crittografa i dati in una forma che una rete neurale può elaborare senza decifrare i dati. Ciò protegge la privacy di ogni singolo input ma introduce un sovraccarico delle prestazioni computazionali e limita l'insieme delle operazioni aritmetiche a quelle supportate dalla* **HOMOMORPHIC ENCRYPTION**.

3 - CONSEQUENCES

Le conseguenze degli attacchi contro gli obiettivi dipendono dalle difese implementate. Per una data combinazione di Attacco (inclusi OBIETTIVO, TECNICA *e* CONOSCENZA*) e Difesa, le conseguenze possono essere classificate categoricamente come* VIOLATIONS OF INTEGRITY, AVAILABILITY, CONFIDENTIALITY *o* PRIVACY.

In **INTEGRITY VIOLATIONS**, *il processo di inferenza è compromesso, con conseguente* **CONFIDENCE REDUCTION** *della fiducia o* **MISCLASSIFICATION** *a qualsiasi classe diversa dalla classe originale.*

Nel **UNSUPERVISED LEARNING**, *una* INTEGRITY VIOLATION *può produrre una rappresentazione priva di significato dell'input in un estrattore di funzionalità non supervisionato.*

In **REINFORCEMENT LEARNING**, *una* INTEGRITY VIOLATION *può far sì che l'agente di apprendimento agisca in modo poco intelligente o con prestazioni degradate nel suo ambiente.*

Le **AVAILABILITY VIOLATIONS** *inducono riduzioni della qualità (come la velocità di inferenza) o dell'accesso (*DENIAL OF SERVICE*) al punto da rendere il componente ML non disponibile per gli utenti.*

I CONFIDENTIALITY VIOLATIONS *si verificano quando un avversario estrae o deduce informazioni utilizzabili sul modello e sui dati.*

Gli attacchi alle informazioni riservate sul modello includono un EXTRACTION ATTACK *che rivela l'architettura o i parametri del modello o un* ORACLE ATTACK *che consente all'avversario di costruire un modello sostitutivo.*

PRIVACY VIOLATIONS *sono una classe specifica di violazione della riservatezza in cui l'avversario ottiene informazioni personali su uno o più input del modello individuali e legittimi, inclusi o meno nei dati di formazione.*

4 - TERMINOLOGY

Vedi capitolo "3. Terminology" del NIST IR 8269.

97. ACCESS CONTROL POLICY VERIFICATION

La verifica della politica di controllo degli accessi garantisce che non vi siano errori all'interno della politica affinché si perdano o blocchino i privilegi di accesso.

Come test del software, la verifica dei criteri di controllo degli accessi si basa su metodi come la prova del modello, la struttura dei dati, la simulazione del sistema e l'oracolo di test per verificare che la politica funzioni come previsto.

Tuttavia, questi metodi presentano problemi di capacità e prestazioni legati a imprecisioni e complessità limitate dalle tecnologie applicate.

Come test del software, la verifica dei criteri di controllo degli accessi si basa su metodi come la prova del modello, struttura dati, simulazione di sistema e test oracle per verificare la logica funzionale prevista implicita nelle regole di policy.

*Il metodo di prova del modello converte la politica in una macchina a stati finiti (*FINITE STATE MACHINE - FSM*) e verifica i casi di accesso di prova contro di essa per rilevare errori di politica, come conflitto di regole, blocco dell'accesso o perdita di privilegi [SP192].*

1 - MACHINE LEARNING FOR ACCESS CONTROL VERIFICATION

L'apprendimento automatico (Autoapprendimento – Machine Learning) è stato utilizzato per il controllo dei dispositivi, l'analisi del sistema e le previsioni aziendali.

*La classificazione ML consente la generazione o la previsione di classi di destinazione (**TARGET**) per nuovi dati di input utilizzando alcuni dati di addestramento (**TRAINING DATA**) di esempio prodotti eseguendo il sistema invece di dati di input completi.*

Per la verifica dei criteri di controllo degli accessi, ai dati di addestramento sono assegnati i valori degli attributi delle regole dei criteri e l'obiettivo per la classificazione sono le autorizzazioni di accesso (ad es. concessione, negazione e così via) assegnate alle regole.

*I dati sono utilizzati da un algoritmo di classificazione ML per generare un modello di classificazione (**CLASSIFICATION MODEL**).*

*Albero decisionale (**Decision Tree - DT**) e RFC sono due dei principali algoritmi di classificazione ML in grado di verificare la politica di controllo degli accessi perché, tra gli altri algoritmi di classificazione ML, che sono più orientati all'analisi di regressione per dati numerici [MG17], DT e RFC gli algoritmi applicano algoritmi ad albero binario che supportano l'elaborazione dell'analisi di non regressione dei dati binari.*

La Figura 1 mostra un modello di albero binario di esempio generato dall'algoritmo di classificazione RFC.

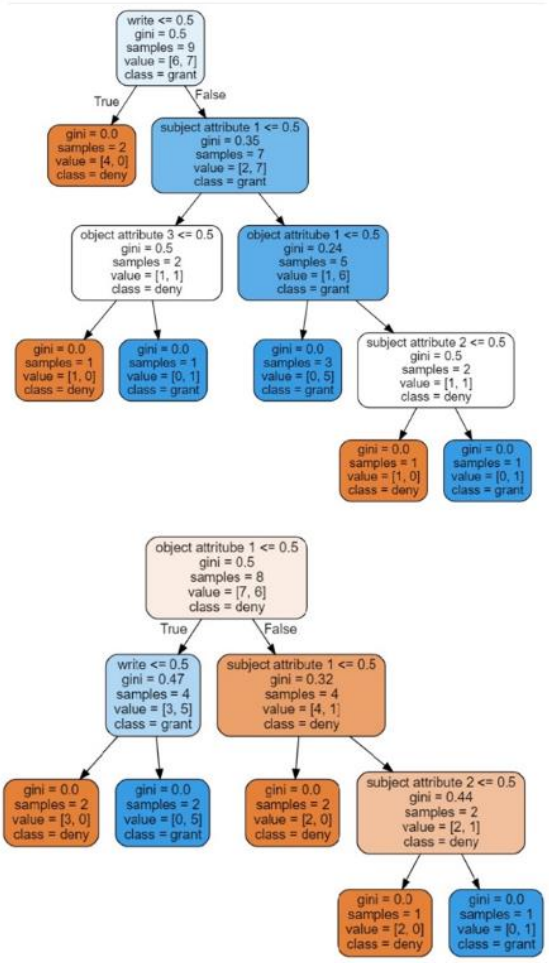


Figure 1: 1a (above), 1b (below) – Subtrees model generated by RFC classifier

Rispetto a DT, un algoritmo RFC è più adatto per la verifica dei criteri di controllo degli accessi perché, dal punto di vista di un modello renderizzato, un algoritmo RFC genera insiemi di sotto alberi decisionali che rappresentano più regole di criteri del modello.

Al contrario, un algoritmo DT genera un modello di albero decisionale singolo che rappresenta una singola regola alla base delle logiche di regole combinate.

I valori degli attributi dei criteri possono essere binari o tipi non binari (ad es. rango, età, ecc.) applicabili a diversi metodi di verifica tradizionali.

Per entrambi gli algoritmi, le verifiche dei criteri hanno solo un valore di attributo binario.

*Il sovradattamento dei modelli non causerà imprecisioni. Tuttavia, per i valori non binari con criteri numerici, ad esempio criteri basati sulla situazione, la classificazione si basa sull'analisi di regressione e l'**overfitting** può causare un'analisi imprecisa.*

A questo proposito, RFC è in grado di ridurre l'overfitting mantenendo la precisione che DT non supporta.

In sintesi, i vantaggi dell'algoritmo RFC rispetto all'algoritmo DT e ai metodi di verifica tradizionali per la verifica dei criteri di controllo degli accessi sono illustrati nella Figura 2.

I numeri allegati alle linee tratteggiate classificano le sfide elencate di seguito, alle quali si risponde con i metodi di classificazione ML di collegamento in quadrati.

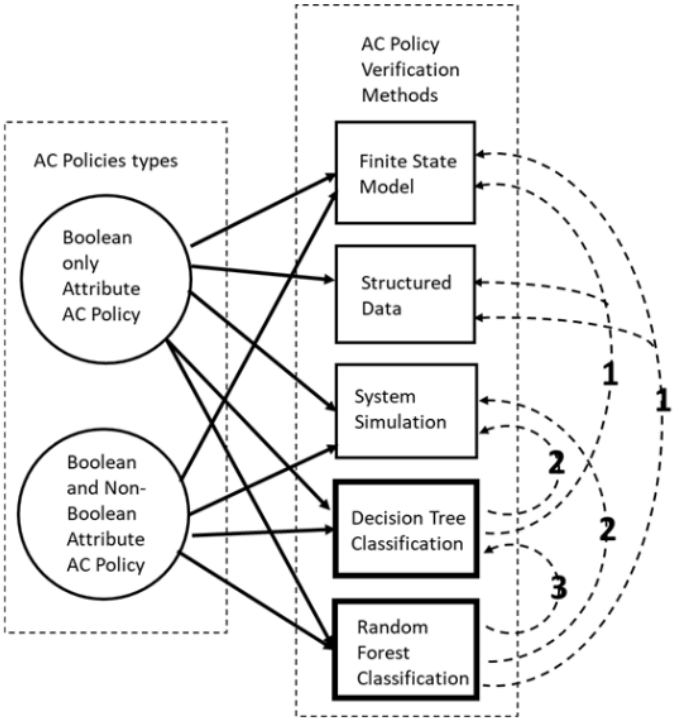


Figure 2: Mapping of access control policy types and verification methods

1. Richiede test case/requisiti o Oracle per scoprire tutti i possibili errori delle policy

2. Difficile da implementare e aggiornare al sistema simulato

3. Non è possibile eseguire il rendering di regole di policy separate dal modello e potrebbe adattarsi eccessivamente a policy con valori degli attributi binari.

Le linee continue indicano i metodi di verifica tradizionali applicabili o gli algoritmi di classificazione ML per le politiche di controllo degli accessi connessi nel cerchio con i tipi di attributi specificati.

Come mostrato nella figura, RFC è l'unico metodo in grado di rispondere a tutte e tre le sfide che altri metodi possono affrontare solo parzialmente.

2 - RFC VERIFICATION APPROACH

L'applicazione dell'algoritmo RFC alla verifica delle policy richiede la preparazione di una tabella dati che contiene la formazione richiesta dalla classificazione e i dati di test trasferiti da regole specifiche della politica di controllo degli accessi.

Nella tabella, ogni colonna contiene un attributo, un'azione o un valore di autorizzazione.

Ogni riga rappresenta una regola dei criteri e l'autorizzazione di accesso si basa sui valori dell'attributo e dell'azione nella riga.

Come mostrato nella Figura 3, le colonne da A a E contengono il valore binario (1, vero, 0, falso) degli attributi del soggetto o dell'oggetto, le colonne F e G contengono le azioni disponibili e la colonna H contiene la concessione (1) o la negazione (0) autorizzazione di accesso per le regole dalle righe da 2 a 21.

	A	B	C	D	E	F	G	H
1	20		7 deny	grant				
2	1	1	1	0	1	0	0	1
3	1	1	1	0	0	1	0	1
4	1	1	1	0	0	0	1	0
5	1	1	0	1	1	0	0	1
6	1	1	0	1	0	1	0	1
7	1	1	0	1	0	0	1	1
8	1	0	1	0	1	0	0	1
9	1	0	1	0	0	1	0	0
10	1	0	1	1	0	0	0	1
11	1	0	1	0	0	0	1	0
12	1	0	0	1	1	0	0	0
13	1	0	0	1	0	1	0	0
14	1	0	0	1	0	0	1	1
15	0	1	1	0	1	0	0	0
16	0	1	1	0	0	1	0	1
17	0	1	1	0	0	0	1	0
18	0	1	0	1	1	0	0	0
19	0	1	0	1	0	1	0	0
20	0	1	0	1	0	0	1	1
21	1	1	0	1	0	1	0	1
22								

AC_test-no_SOA21rules

Figure 3: Access control policy rules specified in a data table

Ad esempio, le colonne A, B, C e D sono attributi del soggetto: "cittadino statunitense", "età maggiore di 18 anni", "avere la formazione" e "avere la patente di guida."

Le colonne E e F sono azioni di accesso disponibili di scrittura e lettura.

La colonna G è un "documento".

La colonna H è uno stato di autorizzazione 1 o 0, che significa "concedi" e "nega".

La dimensione di una tabella di dati, quindi, è il numero di attributi di soggetto e oggetto più il numero di azioni disponibili più uno stato di autorizzazione per il numero totale di regole di controllo dell'accesso.

Le regole di policy sintatticamente ragionevoli possono avere errori semantici (cioè contenere conflitti tra le regole), come le seguenti tre regole di set:

1. *<u>uno dei due è corretto ma non entrambi</u>:*
   - ✓ *l'utente ha l'attributo soggetto* A *oggetto* letto *con l'attributo dell'oggetto* X è concesso*;*
   - ✓ *l'utente ha l'attributo soggetto* A *oggetto* letto *con l'attributo dell'oggetto* X è negato*;*
2. *le ultime due regole sono in conflitto con la prima:*
   - ✓ *l'utente ha l'attributo soggetto* A or B *oggetto* letto *con l'attributo dell'oggetto* X è concesso*;*
   - ✓ *l'utente ha l'attributo soggetto* A *oggetto* letto *con l'attributo dell'oggetto* X è negato*;*
   - ✓ *l'utente ha l'attributo soggetto* B *oggetto* letto *con l'attributo dell'oggetto* X è negato;
3. *Uno dei due è corretto ma non entrambi:*
   - ✓ *l'utente ha l'attributo soggetto* A or B *oggetto* letto *con l'attributo dell'oggetto* X è concesso*;*
   - ✓ *l'utente ha l'attributo soggetto* A and B *oggetto* letto *con l'attributo dell'oggetto* X è negato.

La tabella dati può quindi essere elaborata dall'algoritmo RFC per eseguire il rendering di un modello di sottoalberi RFC (Figura 1), i cui rami di sottoalbero possono essere resi a zero o più regole di policy del modello da percorsi collegati dai nodi dell'albero di attributi, azioni e foglie dell'albero di autorizzazioni.

Dopo la generazione di un modello di sottoalbero RFC, viene eseguita l'analisi della funzione di accuratezza per verificare il modello rispetto ai dati di addestramento per garantire che sia accurato al 100% e per verificare la correttezza semantica delle regole della politica.

Oltre a rilevare le regole sui conflitti di autorizzazione, il modello RFC è in grado di riconoscere (ovvero, non trovare alcun conflitto con) la seguente semantica delle regole di policy:

- ✓ **CONDITION PROPERTY***: Ad esempio, le regole "l'utente ha gli attributi del soggetto A oggetto letto con l'attributo X è concesso" e "l'utente ha gli attributi del soggetto A e B legge l'oggetto con l'attributo X è concesso" non sono in conflitto con la regola "l'utente ha attributi soggetto B oggetto letto con l'attributo X è negato.".*
- ✓ **SOD (SEPARATION OF DUTY) PROPERTY***: ad esempio, la regola "l'utente ha attributi di soggetto A l'oggetto letto con l'attributo X è concesso" non è in conflitto con la regola "l'utente ha oggetto attributi A e B l'oggetto letto con attributo X viene negato.".*
- ✓ **EXCLUSION PROPERTY***: ad esempio, la regola "l'utente ha gli attributi del soggetto A o B oggetto letto con l'attributo X è concesso" non è in conflitto con la regola "l'utente ha gli attributi del soggetto A e l'oggetto letto B con l'attributo X viene negato.".*

La Figura 6 mostra i passaggi per il processo di verifica dei criteri RFC (come descritto nel capitolo "RFC Verification Approach" del NIST IR 8360).

Nel passo 1, la politica in fase di verifica è trasferita, ripulita in una tabella di dati (ad esempio, Figura 3) e inserita nel processo RFC (ad esempio, Figura 4) nel Passo 2.

Questo genera un modello di sottoalbero (ad esempio, Figura 1) che verrà analizzato per l'accuratezza (cioè la correttezza) della politica originale nel passo 3.

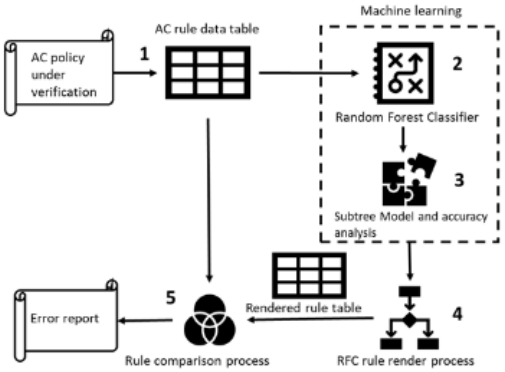


Figure 6: Machine Learning RFC method for access control policy verification

Se il risultato dell'analisi di accuratezza non è 100%, il modello di sottoalbero deve essere ulteriormente elaborato per eseguire il rendering delle regole del modello (ad es. Figura 5) nel passo 4.

Infine, nel passo 5, è possibile abbinare la policy originale per produrre un report di errore (ad esempio, Tabella 1) per le regole della policy che non sono riconosciute o che sono in conflitto con le regole del modello renderizzato.

Il risultato mostra che gli errori in una politica di controllo degli accessi possono essere rilevati quando il risultato dell'analisi di precisione non è del 100%.

3 - APPLICATIONS

Oltre alla verifica delle regole dei criteri di controllo degli accessi, esistono tre tipi principali di applicazioni che il metodo RFC può supportare, come descritto di seguito.

1. **MIGLIORAMENTO DEL METODO DI VERIFICA ESISTENTE** – *Oltre a sostituire l'accesso tradizionale metodi di verifica della politica di controllo, il metodo di verifica RFC può essere utilizzato per migliorare metodi tradizionali verificando la correttezza del modello di policy stesso prima di applicarlo per testare casi nuovi o aggiornati.*
2. **VERIFICA PER CRITERI CON ATTRIBUTI NUMERICI** – *Alcuni controlli di accesso sensibili al contesto politiche, come P-BAC [PBAC] o sistemi di controllo degli accessi basati sulla situazione, hanno attributi come variabili numeriche.*

   Questi attributi non binari misurano valori come numeri, volumi e altri conteggi misurabili per prendere decisioni di accesso per regole di policy, come "se il livello di sicurezza corrente è maggiore di 3, allora l'utente ha l'attributo soggetto X ed è autorizzato ad accedere alla risorsa con oggetto attributo Y", o "se la quantità totale di la spesa è superiore a $50, quindi lo sconto è accessibile ai clienti ma non accessibile ai dipendenti".

   Queste politiche non possono essere verificate con i metodi di verifica tradizionali, incluso un numero infinito di valori di attributo in casi di test/oracle.

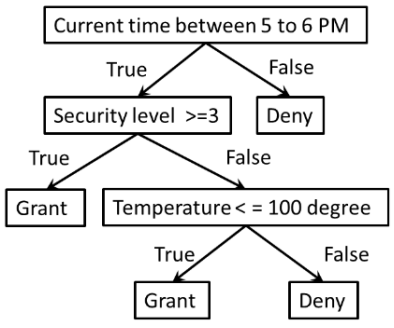


Figure 7: Numerical attribute values in a subtree model

   La verifica RFC metodo per queste politiche è particolarmente utile perché un algoritmo RFC è fondamentalmente attrezzato per la valutazione sui valori di regressione.

   I suoi fattori di ramo per il test dei nodi del sottoalbero le limitazioni dei valori degli attributi, come mostrato nell'esempio della Figura 7, dove il tempo e i valori degli attributi di temperatura possono variare fino a un numero reale illimitato a seconda del risoluzioni delle variabili.
3. **APPLICAZIONE DELLA POLITICA** – *Oltre alla verifica per la politica con attributi numerici come descritto sopra, il metodo RFC può essere utilizzato per i meccanismi di applicazione delle politiche [LDW20] per*

decidere automaticamente le autorizzazioni di una richiesta di accesso che non è stata delineata in alcuna regola della politica, in particolare per le politiche con un'ampia gamma di valori di attributo, perché non è pratico elencare tutte le possibili regole per accogliere tutti i possibili attributi valori nella politica.

Per tali applicazioni, il metodo RFC dovrebbe accettare una richiesta di accesso come dati di test aggiuntivi per eseguire analisi di accuratezza.

Senza il 100%, la richiesta di accesso dovrebbe essere negato.

PARTE XVIII: DIGITAL IDENTITY

98. DIGITAL IDENTITY MODEL

OVERVIEW

L'identità digitale è la rappresentazione univoca di un soggetto impegnato in una transazione online.

*Il processo utilizzato per verificare l'associazione di un soggetto con la sua identità nel mondo reale è chiamato "***Identity Proofing***" e la parte da verificare è chiamata "***Applicant***" (il richiedente).*

*Quando il richiedente completa con successo il processo di correzione, viene indicato come "***Subscriber***" (sottoscrittore).*

La forza della verifica dell'identità è descritta da una misurazione ordinale chiamata IAL *(*Identity Assurance Level*).*

Il livello IAL1 *non richiede la verifica dell'identità, quindi qualsiasi informazione sugli attributi fornita dal richiedente è auto-affermata o dovrebbe essere trattata come auto-affermata e non verificata (anche se fornita da un CSP a un RP).*

IAL2 *e* IAL3 *richiedono la verifica dell'identità e l'RP può richiedere informazioni sull'asserzione CSP sul sottoscrittore, come valori di attributo verificati, riferimenti di attributo verificati o identificatori pseudonimi.*

Queste informazioni aiutano il PR nel prendere decisioni di autorizzazione.

Un RP può decidere di richiedere IAL2 o IAL3, ma può aver bisogno solo di attributi specifici, con il risultato che il soggetto mantiene un certo grado di pseudonimo.

Questo approccio di miglioramento della privacy ha il vantaggio di separare la forza del processo di Verifica da quella del processo di Autenticazione.

Un RP può anche impiegare un approccio di identità federata in cui il RP esternalizza tutta la verifica dell'identità, la raccolta degli attributi e l'archiviazione degli attributi ad un CSP.

*In questo trattato, la parte da autenticare è chiamata "***Claimant"** *(Ricorrente) e la parte che verifica tale identità è chiamata "***Verifier***" (Verificatore).*

Quando un ricorrente dimostra con successo il possesso e il controllo di uno o più autenticatori a un verificatore tramite un protocollo di autenticazione, il verificatore può constatare che il richiedente sia un sottoscrittore valido.

Il verificatore trasmette un'asserzione sul sottoscrittore (pseudonimo o non pseudonimo) al PR.

Tale asserzione include un identificatore e può includere informazioni sull'identità del sottoscrittore, come il nome o altri attributi che sono stati raccolti nel processo di registrazione.

Se il verificatore è anche l'RP, l'asserzione può essere implicita.

L'RP può utilizzare le informazioni autenticate fornite dal verificatore per prendere decisioni di autorizzazione.

L'autenticazione stabilisce la certezza che il richiedente sia in possesso di uno o più autenticatori vincolati alla credenziale, e in alcuni casi nei valori degli attributi del sottoscrittore.

La forza del processo di autenticazione è descritta da una misura ordinale chiamata AAL.

AAL1 richiede l'autenticazione a fattore singolo ed è consentito con una varietà di diversi tipi di autenticatore.

In AAL2, l'autenticazione richiede due fattori di autenticazione per una sicurezza aggiuntiva.

L'autenticazione al livello più alto AAL3 richiede inoltre l'uso di un autenticatore basato su hardware e una resistenza alla rappresentazione del verificatore.

Le varie entità e interazioni che compongono il modello di identità digitale qui utilizzato sono illustrate nella Figura 4-1

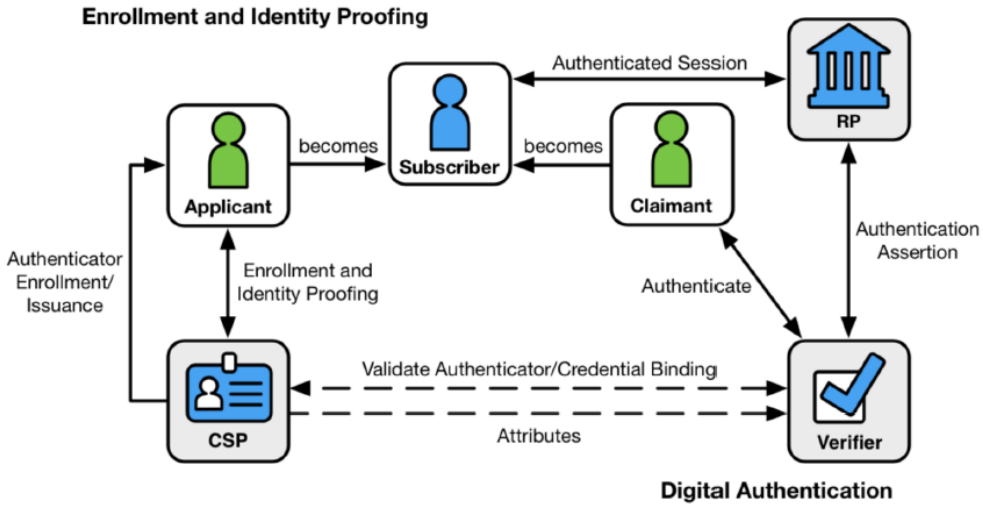


Figure 4-1 Digital Identity Model

Il lato sinistro della Figura 4-1 mostra la registrazione, il rilascio delle credenziali, le attività di gestione del ciclo di vita e i vari stati di un processo di verifica dell'identità e autenticazione.

La consueta sequenza di interazioni è la seguente:

1. *Un richiedente (***Applicant)** *fa richiesta a un CSP attraverso un processo di iscrizione.*
2. *L'identità del CSP prova tale richiedente. In caso di esito positivo della prova, il richiedente diventa un sottoscrittore (***Subscriber)**.
3. *Tra il CSP e il sottoscrittore si inseriscono gli autenticatori e le credenziali corrispondenti.*
4. *Il CSP conserva la credenziale, il suo stato e i dati di registrazione raccolti per tutta la durata della credenziale (almeno). Il sottoscrittore mantiene i suoi autenticatori.*

Il lato destro della Figura 4-1 mostra le entità e le interazioni coinvolte nell'utilizzo di un autenticatore per eseguire l'autenticazione digitale.

*Un sottoscrittore è00000 definito ricorrente (***Claimant)** *quando deve autenticarsi presso un verificatore.*

Le interazioni sono le seguenti:

1. *Il richiedente (***Applicant)** *dimostra al verificatore (***Verifier)** *il possesso e il controllo dell'autenticatore o degli autenticatori tramite un protocollo di autenticazione.*
2. *Il verificatore interagisce con il CSP per convalidare la credenziale che lega l'identità del sottoscrittore al suo autenticatore e per ottenere facoltativamente gli attributi del richiedente.*
3. *Il CSP o verificatore fornisce un'asserzione sul sottoscrittore alla RP, che può utilizzare le informazioni nell'asserzione per prendere una decisione di autorizzazione.*
4. *Viene stabilita una sessione autenticata tra il sottoscrittore e il RP.*

AUTHENTICATORS

Il paradigma classico per i sistemi di autenticazione individua tre fattori come capisaldi di autenticazione:

- *Qualcosa che conosci (ad es. una password).*
- *Qualcosa in tuo possesso (ad es. un badge identificativo o una chiave crittografica).*
- *Qualcosa che sei (ad esempio, un'impronta digitale o altri dati biometrici).*

MFA (Multi-Factor Authentication) *si riferisce all'uso di due o più fattori.*

Altri tipi di informazioni, come i dati sulla posizione o l'identità del dispositivo, possono essere utilizzati da un responsabile della protezione o da un verificatore per valutare il rischio in un'identità dichiarata, ma non sono considerati fattori di autenticazione.

*I segreti contenuti negli autenticatori si basano su coppie di chiavi pubbliche, chiavi asimmetriche, (*Public Key Pairs - Asymmetric Keys*) o segreti condivisi, chiavi simmetriche* (Shared Secrets - Symmetric keys).

Una chiave pubblica e una relativa chiave privata costituiscono una coppia di chiavi pubbliche.

La chiave privata è memorizzata nell'autenticatore ed è utilizzata dal richiedente per dimostrare il possesso e il controllo dell'autenticatore.

Un verificatore, conoscendo la chiave pubblica del richiedente attraverso alcune credenziali (in genere un certificato di chiave pubblica), può utilizzare un protocollo di autenticazione per verificare l'identità del richiedente dimostrando che il richiedente ha il possesso e il controllo dell'autenticatore della chiave privata associato.

I segreti condivisi archiviati negli autenticatori possono essere chiavi simmetriche o segreti memorizzati (ad es. password e PIN), a differenza delle chiavi asimmetriche che gli abbonati non devono condividere con il verificatore.

Le chiavi simmetriche sono generalmente memorizzate in hardware o software che il sottoscrittore controlla, mentre le password sono destinate ad essere memorizzate dal sottoscrittore.

I fattori di autenticazione classificati come qualcosa che conosci non sono necessariamente segreti.

La biometria non costituisce un segreto.

L'uso della biometria per l'autenticazione è consentita solo quando fortemente vincolata a un autenticatore fisico.

L'autenticazione basata sulla conoscenza, in cui al richiedente è chiesto di rispondere a domande che sono presumibilmente note solo al richiedente, non costituisce un segreto accettabile per l'autenticazione digitale.

Un sistema di autenticazione digitale può incorporare più fattori in due modi:

1. *Il sistema può essere implementato in modo che al verificatore vengano presentati più fattori; oppure*
2. *Alcuni fattori possono essere utilizzati per proteggere un segreto che verrà presentato al verificatore.*

Ad esempio, il primo modo può essere soddisfatto abbinando un segreto memorizzato (quello che sai) con un dispositivo di banda (quello che hai). Entrambi gli output dell'autenticatore vengono presentati al verificatore per autenticare il ricorrente.

Il secondo modo considera un componente hardware (l'autenticatore) che contiene una chiave crittografica (il segreto dell'autenticatore) in cui l'accesso è protetto da un'impronta digitale. Se utilizzata con il biometrico, la chiave crittografica produce un output che viene utilizzato per autenticare il ricorrente.

Come notato sopra, la biometria, quando impiegata come singolo fattore di autenticazione, non costituisce segreti accettabili per l'autenticazione digitale, ma hanno il loro posto nell'autenticazione delle identità digitali.

AUTHENTICATION PROCESS

Il processo di autenticazione inizia con il ricorrente che dimostra al verificatore il possesso e controllo di un autenticatore che è vincolato all'identità asserita tramite un protocollo di autenticazione.

Una volta dimostrato il possesso e il controllo, il verificatore si accerta che la credenziale rimanga valida, di solito, interagendo con il CSP.

I meccanismi situati presso il verificatore possono mitigare gli attacchi online contro segreti, come password e PIN, limitando la velocità con cui un aggressore può effettuare tentativi di autenticazione o ritardare in altro

modo tentativi errati. In genere, ciò viene fatto tenendo traccia e limitando il numero di tentativi non riusciti, poiché la premessa di un attacco online è che la maggior parte dei tentativi fallirà.

Il verificatore è un ruolo funzionale, ma è spesso implementato in combinazione con il CSP, il RP, o entrambi. Se il verificatore è un'entità separata dal CSP, è spesso desiderabile garantire che il verificatore non conosca il segreto dell'autenticatore del sottoscrittore nel processo di autenticazione, o garantire almeno che il verificatore non abbia accesso illimitato ai segreti archiviati dal CSP.

RELYING PARTIES

Un RP si basa sui risultati di un protocollo di autenticazione per stabilire la fiducia nell'identità o negli attributi di un sottoscrittore allo scopo di condurre una transazione online.

Gli RP possono utilizzare l'identità autenticata di un sottoscrittore (pseudonimo o non pseudonimo), IAL, AAL e FAL (FAL che indica la forza del protocollo di asserzione) e altri fattori per decidere l'autorizzazione.

Il verificatore e l'RP possono essere la stessa entità o possono essere entità separate. Se sono entità separate, l'RP normalmente riceve un'asserzione dal verificatore.

L'RP garantisce che l'asserzione provenga da un verificatore di fiducia dell'RP.

L'RP elabora anche qualsiasi informazione aggiuntiva nell'asserzione, come attributi personali o tempi di scadenza.

L'RP è l'arbitro finale riguardo al fatto che una specifica asserzione presentata da un verificatore soddisfi i criteri stabiliti dall'RP per l'accesso al sistema indipendentemente da IAL, AAL o FAL.

99. PROCESS FLOW

Flusso di base per la verifica dell'identità.

1°. RESOLUTION*: raccolta degli attributi e delle prove.*

- ✓ *Distinzione univoca dell'individuo.*
- ✓ *Esempi*
  a. *Il CSP raccoglie le PII dal richiedente (ad esempio nome, indirizzo, data di nascita, e-mail e numero di telefono).*
  b. *Il CSP raccoglie anche due forme di prova dell'identità, come la patente di guida e il passaporto. Ad esempio, utilizzando la fotocamera di un laptop, il CSP può acquisire una foto di entrambi i lati di entrambi i documenti di identità.*

2°. VALIDATION*: validazione degli attributi e delle prove raccolte.*

- ✓ *Autenticità, validità e accuratezza delle informazioni sull'identità della persona.*
- ✓ *Esempi*
  a. *Il CSP convalida le informazioni raccolte precedentemente verificandone una fonte autorevole.*
  b. *Il CSP interroga le fonti emittenti dei documenti e convalida le corrispondenze delle informazioni.*

3°. VERIFICATION*: verifica degli attributi e delle prove raccolte.*

- ✓ *Confermato e accertato il collegamento tra l'identità dichiarata e l'esistenza del soggetto che presenta le prove.*
- ✓ *Esempi*
  a. *Il CSP invia un codice di registrazione al numero di telefono convalidato del richiedente, l'utente fornisce il codice di registrazione al CSP e il CSP conferma la corrispondenza, verificando che l'utente sia in possesso e controllo del numero di telefono convalidato.*

b. Il richiedente è stato verificato con successo.

100. IDENTITY RESOLUTION, VALIDATION, AND VERIFICATION

Questa sezione elenca i requisiti per risolvere, convalidare e verificare un'identità e qualsiasi prova di identità fornita.

I requisiti hanno lo scopo di garantire che l'identità dichiarata sia l'identità effettiva del soggetto che tenta di iscriversi al CSP e che gli attacchi scalabili che colpiscono una vasta popolazione di individui iscritti richiedano tempi e costi maggiori rispetto al valore delle risorse che il sistema sta proteggendo.

IDENTITY RESOLUTION

L'obiettivo della risoluzione dell'identità è distinguere in modo univoco un individuo all'interno di una data popolazione o contesto.

La risoluzione effettiva dell'identità utilizza il più piccolo insieme di attributi necessari per risolvere un individuo univoco. Fornisce al CSP un importante punto di partenza nel processo complessivo di verifica dell'identità, per includere l'individuazione iniziale di potenziali frodi, ma non rappresenta in alcun modo una transazione completa e di successo per la verifica dell'identità.

IDENTITY EVIDENCE COLLECTION AND VALIDATION

L'obiettivo della convalida dell'identità è raccogliere le prove di identità più appropriate (ad esempio, passaporto o patente di guida) dal richiedente e determinarne l'autenticità, la validità e l'accuratezza.

L'obiettivo della convalida dell'identità è raccogliere le prove di identità più appropriate (ad esempio, passaporto o patente di guida) dal richiedente e determinarne l'autenticità, la validità e l'accuratezza.

La convalida dell'identità si compone di tre fasi del processo:

1. *raccolta delle prove di identità appropriate,*
2. *conferma che le prove sono autentiche e genuine,*
3. *conferma che i dati contenuti nelle prove di identità siano validi, attuali e relativi a un soggetto reale.*

La tabella accanto (vedi tabella 5-1 NIST SP 800-63A) elenca i punti di forza, che vanno da UNACCEPTABLE *a* SUPERIOR, *delle prove di identità raccolte per stabilire un'identità valida.*

Salvo diversa indicazione, per ottenere una data forza l'evidenza DEVE (SHALL), *come minimo, soddisfare tutte le qualità elencate.*

TABLE 5-1 STRENGTHS OF IDENTITY EVIDENCE

Strength	Qualities of Identity Evidence
Unacceptable	No acceptable identity evidence provided.

Weak	• The issuing source of the evidence did not perform identity proofing.
	• The issuing process for the evidence means that it can reasonably be assumed to have been delivered into the possession of the applicant.
	• The evidence contains:
	  ○ At least one reference number that uniquely identifies itself or the person to whom it relates, **OR**
	  ○ The issued identity evidence contains a photograph or biometric template (of any modality) of the person to whom it relates.

Fair	• The issuing source of the evidence confirmed the claimed identity through an identity proofing process.
	• The issuing process for the evidence means that it can reasonably be assumed to have been delivered into the possession of the person to whom it relates.
	• The evidence:
	  ○ Contains at least one reference number that uniquely identifies the person to whom it relates, **OR**
	  ○ Contains a photograph or biometric template (any modality) of the person to whom it relates, **OR**
	  ○ Can have ownership confirmed through KBV.
	• Where the evidence includes digital information, that information is protected using approved cryptographic or proprietary methods, or both, and those methods ensure the integrity of the information and enable the authenticity of the claimed issuing source to be confirmed.
	• Where the evidence includes physical security features, it requires proprietary knowledge to be able to reproduce it.
	• The issued evidence is unexpired.

Strong	• The issuing source of the evidence confirmed the claimed identity through written procedures designed to enable it to form a reasonable belief that it knows the real-life identity of the person. Such procedures are subject to recurring oversight by regulatory or publicly-accountable institutions. For example, the Customer Identification Program guidelines established in response to the USA PATRIOT Act of 2001 or the Red Flags Rule, under Section 114 of the Fair and Accurate Credit Transaction Act of 2003 (FACT Act). • The issuing process for the evidence ensured that it was delivered into the possession of the subject to whom it relates. • The issued evidence contains at least one reference number that uniquely identifies the person to whom it relates. • The full name on the issued evidence must be the name that the person was officially known by at the time of issuance. Not permitted are pseudonyms, aliases, an initial for surname, or initials for all given names.

	• The:
	  ○ Issued evidence contains a photograph or biometric template (of any modality) of the person to whom it relates, **OR**
	  ○ Applicant proves possession of an AAL2 authenticator, or equivalent, bound to an IAL2 identity, at a minimum.
	• Where the issued evidence includes digital information, that information is protected using approved cryptographic or proprietary methods, or both, and those methods ensure the integrity of the information and enable the authenticity of the claimed issuing source to be confirmed.
	• Where the issued evidence contains physical security features, it requires proprietary knowledge and proprietary technologies to be able to reproduce it.
	• The evidence is unexpired.

Superior	• The issuing source of the evidence confirmed the claimed identity by following written procedures designed to enable it to have high confidence that the source knows the real-life identity of the subject. Such procedures are subject to recurring oversight by regulatory or publicly accountable institutions. • The issuing source visually identified the applicant and performed further checks to confirm the existence of that person;. • The issuing process for the evidence ensured that it was delivered into the possession of the person to whom it relates. • The evidence contains at least one reference number that uniquely identifies the person to whom it relates. • The full name on the evidence must be the name that the person was officially known by at the time of issuance. Not permitted are pseudonyms, aliases, an initial for surname, or initials for all given names. • The evidence contains a photograph of the person to whom it relates. • The evidence contains a biometric template (of any modality) of the person to whom it relates. • The evidence includes digital information, the information is protected using approved cryptographic or proprietary methods, or both, and those methods ensure the integrity of the information and enable the authenticity of the issuing source to be confirmed. • The evidence includes physical security features that require proprietary knowledge and proprietary technologies to be able to reproduce it. • The evidence is unexpired.

VALIDATING IDENTITY EVIDENCE

Il CSP ottiene le prove di identità (accuracy, authenticity, integrity) ed effettua la verifica presso fonti autorevoli affinché:

- *sia autentico e non contraffatto o falso;*
- *contenga informazioni corrette;*
- *contenga informazioni relative a un argomento della vita reale.*

La tabella 5-2 (del NIST SP 800-63A) elenca i punti di forza, che vanno da UNACCEPTABLE *a* SUPERIOR*, della convalida dell'identità eseguita dal CSP per convalidare le prove presentate per l'attuale sessione di copertura e le informazioni ivi contenute.*

Table 5-2 Validating Identity Evidence

Strength	Method(s) Performed by the CSP
Unacceptable	• Evidence validation was not performed, or validation of the evidence failed.
Weak	• All personal details from the evidence have been confirmed as valid by comparison with information held or published by an authoritative source.
Fair	• Attributes contained in the evidence have been confirmed as valid by comparison with information held or published by the issuing source or authoritative source(s), **OR** • The evidence has been confirmed as genuine using appropriate technologies, confirming the integrity of physical security features and that the evidence is not fraudulent or inappropriately modified, **OR** • The evidence has been confirmed as genuine by trained personnel, **OR** • The evidence has been confirmed as genuine by confirmation of the integrity of cryptographic security features.
Strong	• The evidence has been confirmed as genuine: o using appropriate technologies, confirming the integrity of physical security features and that the evidence is not fraudulent or inappropriately modified, **OR** o by trained personnel and appropriate technologies, confirming the integrity of the physical security features and that the evidence is not fraudulent or inappropriately modified, **OR** o by confirmation of the integrity of cryptographic security features. • All personal details and evidence details have been confirmed as valid by comparison with information held or published by the issuing source or authoritative source(s).
Superior	• The evidence has been confirmed as genuine by trained personnel and appropriate technologies including the integrity of any physical and cryptographic security features. • All personal details and evidence details from the evidence have been confirmed as valid by comparison with information held or published by the issuing source or authoritative source(s).

IDENTITY VERIFICATION

L'obiettivo della verifica dell'identità è di confermare e di stabilire un collegamento tra l'identità dichiarata e l'esistenza reale del soggetto che presenta le prove.

IDENTITY VERIFICATION METHODS

La Tabella 5-3 descrive in dettaglio i metodi di verifica necessari per ottenere un livello di qualità della verifica.

Il CSP DEVE (SHALL) *aderire ai requisiti indicati nel capitolo immediatamente successivo se* KBV *utilizzato per verificare un'identità.*

Table 5-3 Verifying Identity Evidence

Strength	Identity Verification Methods
Unacceptable	Evidence verification was not performed or verification of the evidence failed. Unable to confirm that the applicant is the owner of the claimed identity.
Weak	The applicant has been confirmed as having access to the evidence provided to support the claimed identity.
Fair	• The applicant's ownership of the claimed identity has been confirmed by: o KBV. See Section 5.3.2. for more details, **OR** o a physical comparison of the applicant to the strongest piece of identity evidence provided to support the claimed identity. Physical comparison performed remotely SHALL adhere to all requirements as specified in SP 800-63B, Section 5.2.3, **OR** o biometric comparison of the applicant to the identity evidence. Biometric comparison performed remotely SHALL adhere to all requirements as specified in SP 800-63B, Section 5.2.3.
Strong	• The applicant's ownership of the claimed identity has been confirmed by: o physical comparison, using appropriate technologies, to a photograph, to the strongest piece of identity evidence provided to support the claimed identity. Physical comparison performed remotely SHALL adhere to all requirements as specified in SP 800-63B, Section 5.2.3, **OR** o biometric comparison, using appropriate technologies, of the applicant to the strongest piece of identity evidence provided to support the claimed identity. Biometric comparison performed remotely SHALL adhere to all requirements as specified in SP 800-63B, Section 5.2.3.
Superior	The applicant's ownership of the claimed identity has been confirmed by biometric comparison of the applicant to the strongest piece of identity evidence provided to support the claimed identity, using appropriate technologies. Biometric comparison performed remotely SHALL adhere to all requirements as specified in SP 800-63B, Section 5.2.3.

KNOWLEDGE-BASED VERIFICATION (KBV) REQUIREMENTS

I seguenti requisiti si applicano ai passaggi di verifica dell'identità per IAL2.

1. *Il CSP* NON DEVE (SHALL NOT) *utilizzare* KBV (KNOWLEDGE-BASED VERIFICATION) *per verificare l'identità di un richiedente rispetto a più di un elemento di prova dell'identità convalidato.*
2. *Il CSP* DEVE (SHALL) *utilizzare solo informazioni che si prevede siano note solo al richiedente e la fonte autorevole, per includere tutte le informazioni necessarie per iniziare il processo KBV.*
   Le informazioni accessibili liberamente, a pagamento di pubblico dominio o tramite il mercato nero NON DEVONO essere utilizzate.
3. *Il CSP* DEVE (SHALL) *consentire a un'identità risolta e convalidata di rinunciare a KBV e sfruttare un altro processo per la verifica.*
4. *CSP* DOVREBBE (SHOULD) *eseguire KBV verificando la conoscenza della storia delle transazioni recenti in cui il CSP è un partecipante.*
   Il CSP DEVE (SHALL) *garantire che le informazioni sulle transazioni hanno almeno 20 bit di entropia. Ad esempio, per raggiungere i requisiti minimi di entropia, il CSP potrebbe chiedere al richiedente la verifica*

dell'importo/i e del/i numero/i di transazione/i di un micro-deposito/i su un conto bancario valido, purché il numero totale di cifre è sette o più.

5. *Il CSP* PUÒ (MAY) *eseguire KBV ponendo al richiedente domande per dimostrare di essere il proprietario delle informazioni richieste.*
   Tuttavia, si applicano i seguenti requisiti:
   a. *KBV* DOVREBBE (SHOULD) *essere basato su più fonti autorevoli.*
   b. *CSP* DEVE (SHALL) *richiedere un minimo di quattro domande KBV, ognuna delle quali richiede una risposta corretta per completare con successo il passaggio KBV.*
   c. *CSP* DOVREBBE (SHOULD) *richiedere domande KBV a risposta libera.*
      Il CSP PUÒ (MAY) *consentire domande a scelta multipla, tuttavia, se vengono fornite domande a scelta multipla, il CSP* DEVE (SHALL) *richiedere un minimo di quattro opzioni di risposta per domanda.*
   d. *CSP* DOVREBBE (SHOULD) *consentire due tentativi al richiedente per completare il KBV ma non più di tre.*
   e. *CSP* DEVE (SHALL) *far scadere le sessioni KBV dopo due minuti di inattività per domanda.*
      In caso di timeout della sessione, il CSP DEVE (SHALL) *riavviare l'intero processo KBV e considerarlo un tentativo fallito.*
   f. *CSP* NON DEVE (SHALL NOT) *presentare la maggior parte delle domande KBV diversive (cioè quelle in cui "nessuna delle precedenti" è la risposta corretta).*
   g. *CSP* NON DOVREBBE (SHOULD NOT) *porre le stesse domande KBV nei tentativi successivi.*
   h. *CSP* NON DEVE (SHALL NOT) *porre una domanda KBV che fornisca informazioni che potrebbero aiutare a rispondere a qualsiasi futura domanda KBV in una singola sessione o in una sessione successiva dopo un tentativo fallito.*
   i. *CSP* NON DEVE (SHALL NOT) *utilizzare domande KBV per le quali le risposte non cambiano (ad esempio, "Qual è stata la tua prima auto?").*
   j. *CSP* DEVE (SHALL) *garantire che qualsiasi domanda KBV non riveli una* PII (PERSONALLY IDENTIFIABLE INFORMATION) *che il richiedente non abbia già fornito, né informazioni personali che, se combinate con altre informazioni in una sessione KBV, potrebbero comportare un'identificazione univoca.*

REQUIREMENTS FOR SUPERVISED REMOTE IN-PERSON PROOFING

I CSP possono utilizzare processi di verifica remota per raggiungere livelli comparabili di fiducia e sicurezza agli eventi di persona.

La verifica dell'identità remota e le transazioni di registrazione DEVONO (SHALL) *soddisfare i seguenti requisiti, oltre ai requisiti di convalida e verifica IAL3 specificati nella tabella "*TABLE 4-1 IAL REQUIREMENTS SUMMARY*" descritta più avanti, il CSP:*

1. DEVE (SHALL) *monitorare l'intera sessione di verifica dell'identità, dalla quale il richiedente* NON DEVE (SHALL NOT) *discostarsi, ad esempio mediante una trasmissione video continua ad alta risoluzione del richiedente.*
2. DEVE *(*SHALL*) avere un operatore live che partecipi a distanza con il richiedente per l'intera sessione di verifica dell'identità.*
3. DEVE *(*SHALL*) richiedere che tutte le azioni intraprese dal richiedente durante la sessione di verifica dell'identità siano chiaramente visibili all'operatore remoto.*
4. DEVE *(*SHALL*) richiedere che tutte le verifiche digitali delle prove (ad esempio, tramite chip o tecnologie wireless) siano eseguite da scanner e sensori integrati.*
5. DEVE *(*SHALL*) richiedere agli operatori di aver seguito un programma di formazione per rilevare potenziali frodi e per eseguire correttamente una sessione di verifica remota supervisionata.*

6. DEVE *(SHALL) impiegare il rilevamento di manomissioni fisiche e le caratteristiche di resistenza appropriate per l'ambiente in cui si trova.*
7. DEVE *(SHALL) garantire che tutte le comunicazioni avvengano su un canale protetto reciprocamente autenticato.*

101. IDENTITY ASSURANCE LEVELS (IAL)

La garanzia dell'identità di un sottoscrittore è descritta utilizzando uno dei tre IAL*:*

- IAL1*: non è necessario collegare il richiedente a una specifica identità.*
  Tutti gli attributi forniti in combinazione con le attività del soggetto sono auto-affermati o dovrebbero essere trattati come auto-affermati (compresi gli attributi che un CSP asserisce a un RP).
  Gli attributi auto-affermati non sono né convalidati né verificati.
- IAL2*: le prove supportano l'esistenza nel mondo reale dell'identità dichiarata e verificano che il richiedente sia adeguatamente associato a questa identità.*
  IAL2 introduce la necessità di una verifica dell'identità remota o fisicamente presente. Gli attributi potrebbero essere asseriti dai CSP agli RP a sostegno dell'identità pseudonima con attributi verificati.
  Un CSP che supporta IAL2 può supportare le transazioni IAL1 se l'utente acconsente.
- IAL3*: La presenza fisica è richiesta per la prova dell'identità.*
  Gli attributi identificativi devono essere verificati da un rappresentante CSP autorizzato e formato.

La tabella seguente riassume i requisiti per ciascuno dei livelli di garanzia dell'autenticatore.

TABLE 4-1 IAL REQUIREMENTS SUMMARY

Requirement	IAL1	IAL2	IAL3
Presence	No Requirements	In-person and unsupervised remote.	In-person and supervised remote.
Resolution	No Requirements	• The minimum attributes necessary to accomplish identity resolution. • KBV may be used for added confidence.	Same as IAL2
Evidence	No identity evidence is collected.	• One piece of SUPERIOR or STRONG evidence depending on strength of original proof and validation occurs with issuing source, **OR** • Two pieces of STRONG evidence, **OR** • One piece of STRONG evidence plus two (2) pieces of FAIR evidence.	• Two pieces of SUPERIOR evidence, **OR** • One piece of SUPERIOR evidence and one piece of STRONG evidence depending on strength of original proof and validation occurs with issuing source, **OR** • Two pieces of STRONG evidence plus one piece of FAIR evidence.
Validation	No validation	Each piece of evidence must be validated with a process that is able to achieve the same strength as the evidence presented.	Same as IAL2
Verification	No verification	Verified by a process that is able to achieve a strength of STRONG.	Verified by a process that is able to achieve a strength of SUPERIOR.
Address Confirmation	No requirements for address confirmation	Required. Enrollment code sent to any address of record. Notification sent by means different from enrollment code.	Required. Notification of proofing to postal address.
Biometric Collection	No	Optional	Mandatory
Security Controls	N/A	• SP 800-53 • Moderate Baseline (or equivalent federal or industry standard).	• SP 800-53 • High Baseline (or equivalent federal or industry standard).

102. AUTHENTICATOR ASSURANCE LEVELS (AAL)

La capacità di una transazione di autenticare è caratterizzata da una misura ordinale nota come AAL (AUTHENTICATOR ASSURANCE LEVEL)*.*

Un'autenticazione più forte (un AAL *più alto) richiede che gli attori malintenzionati dispongano di capacità migliori e impieghino maggiori risorse per sovvertire con successo il processo di autenticazione.*

Di seguito viene fornita una sintesi di alto livello dei requisiti tecnici per ciascuno degli AAL.

- AAL 1: *fornisce una certa garanzia che il richiedente controlli un autenticatore associato all'account del sottoscrittore.*
  AAL1 *richiede l'autenticazione a un fattore o a più fattori utilizzando un'ampia gamma di tecnologie di autenticazione disponibili.*
  L'autenticazione valida richiede che il sottoscrittore dimostri il possesso e il controllo dell'autenticatore attraverso un protocollo di autenticazione sicuro.
  AAL1 richiede l'autenticazione a un fattore o a più fattori utilizzando un'ampia gamma di tecnologie di autenticazione disponibili.
  L'autenticazione riuscita obbliga il richiedente a dimostrare il possesso e il controllo dell'autenticatore tramite un protocollo di autenticazione sicuro.
- AAL 2: *fornisce un'elevata sicurezza che il richiedente controlli gli autenticatori collegati all'account del sottoscrittore.*
  La prova del possesso e del controllo di due diversi fattori di autenticazione è richiesta tramite il/i protocollo/i di autenticazione sicuro.
  Sono richieste tecniche crittografiche approvate.
- AAL 3: *fornisce un'elevata sicurezza che il richiedente controlli gli autenticatori collegati all'account del sottoscrittore.*
  L'autenticazione presso AAL3 si basa sulla prova del possesso di una chiave tramite un protocollo crittografico.
  L'autenticazione AAL3 richiede un autenticatore basato su hardware e un autenticatore che fornisca resistenza alla rappresentazione del verificatore.
  Per autenticarsi presso AAL3*, i richiedenti sono tenuti a dimostrare il possesso e il controllo di due distinti fattori di autenticazione tramite protocolli di autenticazione sicuri.*
  Sono necessarie tecniche crittografiche approvate.

SUMMARY OF REQUIREMENTS

La tabella seguente riassume i requisiti per ciascuno degli AAL

Requirement	AAL1	AAL2	AAL3
Permitted Authenticator Types	Memorized Secret; Look-Up Secret; Out-of-Band; SF OTP Device; MF OTP Device; SF Crypto Software; SF Crypto Device; MF Crypto Software; MF Crypto Device	MF OTP Device; MF Crypto Software; MF Crypto Device; or Memorized Secret plus: • Look-Up Secret • Out-of-Band • SF OTP Device • SF Crypto Software • SF Crypto Device	MF Crypto Device; SF Crypto Device plus Memorized Secret; SF OTP Device plus MF Crypto Device or Software; SF OTP Device plus SF Crypto Software plus Memorized Secret
FIPS 140 Verification	Level 1 (Government agency verifiers)	Level 1 (Government agency authenticators and verifiers)	Level 2 overall (MF authenticators) Level 1 overall (verifiers and SF Crypto Devices) Level 3 physical security (all authenticators)
Reauthentication	30 days	12 hours or 30 minutes inactivity; MAY use one authentication factor	12 hours or 15 minutes inactivity; SHALL use both authentication factors
Security Controls	SP 800-53 Low Baseline (or equivalent)	SP 800-53 Moderate Baseline (or equivalent)	SP 800-53 High Baseline (or equivalent)
MitM Resistance	Required	Required	Required
Verifier-Impersonation Resistance	Not required	Not required	Required
Verifier-Compromise Resistance	Not required	Not required	Required
Replay Resistance	Not required	Not required	Required
Authentication Intent	Not required	Recommended	Required
Records Retention Policy	Required	Required	Required
Privacy Controls	Required	Required	Required

103. AUTHENTICATOR AND VERIFIER REQUIREMENTS

In questo capitolo si fornisce una indicazione sui requisiti specifici per ogni tipo di autenticatore.

REQUIREMENTS BY AUTHENTICATOR TYPE

MEMORIZED SECRETS

Un autenticatore segreto memorizzato, comunemente indicato come PASSWORD *o, se numerico,* PIN*, è un valore segreto destinato a essere scelto e memorizzato dall'utente.*

I segreti memorizzati devono essere di complessità e segretezza tali da non consentire a un utente malintenzionato di indovinare o scoprire in altro modo il valore corretto del segreto.

*Un segreto memorizzato è qualcosa "*CHE CONOSCI*"* (Vedi MULTI-FACTOR AUTHENTICATION MFA).

I segreti memorizzati DEVONO *(*SHALL*) essere lunghi almeno 8 caratteri se scelti dal sottoscrittore, quelli scelti casualmente dal CSP o dal verificatore* DEVE *(*SHALL*) avere una lunghezza minima di 6 caratteri e* POSSONO *(*MAY*) essere interamente numerici.*

Se il CSP o il verificatore non consente un segreto memorizzato scelto in base alla sua comparsa su una lista nera di valori compromessi, il sottoscrittore DEVE *(*SHALL*) scegliere un segreto memorizzato diverso.*

Non DOVREBBERO *(*SHOULD*) essere imposti altri requisiti di complessità per i segreti memorizzati.*

LOOKUP SECRETS

Un autenticatore segreto di ricerca è un record fisico o elettronico che memorizza una serie di segreti condivisi tra il richiedente e il CSP.

Il richiedente utilizza l'autenticatore per cercare i segreti appropriati necessari per rispondere a una richiesta del verificatore. Ad esempio, il verificatore può chiedere a un richiedente di fornire un sottoinsieme specifico delle stringhe numeriche o di caratteri stampati su una carta in formato tabella.

*Un'applicazione comune dei segreti di ricerca è l'uso di "*Recovery Keys*" memorizzate dal sottoscrittore per l'uso in caso di smarrimento o malfunzionamento di un altro autenticatore.*

*Un segreto di ricerca è qualcosa "*CHE HAI*"* (Vedi MULTI-FACTOR AUTHENTICATION MFA).

I CSP che creano autenticatori segreti di ricerca DEVONO *(*SHALL*) utilizzare un generatore di bit casuale approvato per generare l'elenco dei segreti e* DEVONO *(*SHALL*) consegnare l'autenticatore in modo sicuro al sottoscrittore.*

I segreti di ricerca DEVONO *(*SHALL*) avere almeno 20 bit di entropia e* POSSONO *(*MAY*) essere distribuiti dal CSP di persona, per posta all'indirizzo di registrazione del sottoscrittore o tramite distribuzione online.*

Se distribuiti online, i segreti di ricerca DEVONO *(*SHALL*) essere distribuiti su un canale sicuro in conformità con i requisiti vincolanti post-iscrizione.*

Se l'autenticatore utilizza i segreti di ricerca in sequenza da un elenco, il sottoscrittore PUÒ *(*MAY*) disporre dei segreti utilizzati, ma solo dopo una corretta autenticazione.*

OUT OF BAND DEVICES

Un autenticatore OUT-OF-BAND *è un dispositivo fisico indirizzabile in modo univoco e in grado di comunicare in modo sicuro con il verificatore su un canale di comunicazione distinto, denominato canale secondario.*

*Il dispositivo è posseduto e controllato dal richiedente e supporta la comunicazione privata su questo canale secondario, separato dal canale principale per l'autenticazione elettronica (*E-AUTHENTICATION*).*

Un autenticatore Out-of-Band *è qualcosa che (*CHE HAI*).* (Vedi MULTI-FACTOR AUTHENTICATION MFA).

L'autenticatore OUT-OF-BAND *può funzionare in uno dei seguenti modi:*

- *Il richiedente trasferisce un segreto ricevuto dal dispositivo Out-of-Band tramite il canale secondario al verificatore utilizzando il canale principale.*
  Ad esempio, il richiedente può ricevere il segreto sul proprio dispositivo mobile e digitarlo (in genere un codice a 6 cifre) nella sessione di autenticazione.
- *Il richiedente trasferisce un segreto ricevuto tramite il canale principale al dispositivo Out-of-Band per la trasmissione al verificatore tramite il canale secondario.*
  Ad esempio, il richiedente può visualizzare il segreto nella sessione di autenticazione e digitarlo in un'app sul proprio dispositivo mobile o utilizzare una tecnologia come un codice a barre o un codice QR per effettuare il trasferimento.

- *Il richiedente confronta i segreti ricevuti dal canale principale e dal canale secondario e conferma l'autenticazione tramite il canale secondario.*

Lo scopo del segreto è associare in modo sicuro l'operazione di autenticazione sul canale primario e secondario.

Quando la risposta avviene tramite il canale di comunicazione primario, il segreto stabilisce anche il controllo del ricorrente sul dispositivo OUT-OF-BAND.

L'autenticatore OUT-OF-BAND DEVE *(*SHALL*) stabilire un canale separato con il verificatore per recuperare il segreto o la richiesta di autenticazione.*

Questo canale è considerato OUT-OF-BAND *rispetto al canale di comunicazione principale (anche se termina sullo stesso dispositivo) a condizione che il dispositivo non trasmetta informazioni da un canale all'altro senza l'autorizzazione del richiedente.*

Il dispositivo OUT-OF-BAND DOVREBBE *(*SHOULD*) essere indirizzabile in modo univoco e la comunicazione sul canale secondario* DEVE *(*SHALL*) essere crittografata a meno che non sia inviata tramite la rete telefonica pubblica commutata (*PUBLIC SWITCHED TELEPHONE NETWORK - PSTN*).*

I metodi che non dimostrano il possesso di un dispositivo specifico, come VOICE-OVER-IP (VOIP) *o* E-MAIL, SHALL NOT *essere utilizzati per l'autenticazione OUT-OF-BAND.*

SINGLE-FACTOR OTP DEVICE

Un dispositivo OTP *(*ONE TIME PASSWORD*) a fattore singolo genera OTP.*

Questa categoria include dispositivi hardware e generatori OTP basati su software installati su dispositivi come i telefoni cellulari.

Questi dispositivi hanno un segreto incorporato che viene utilizzato come "seme" per la generazione di un OTP *e non richiede l'attivazione tramite un secondo fattore.*

L'OTP viene visualizzato sul dispositivo e immesso manualmente per la trasmissione al verificatore, **dimostrando così il possesso e il controllo del dispositivo**.

*Un dispositivo OTP a fattore singolo è qualcosa (*CHE POSSIEDI*).* (Vedi MULTI-FACTOR AUTHENTICATION MFA)

I dispositivi OTP a fattore singolo sono simili agli autenticatori segreti di ricerca con l'eccezione che i segreti sono generati crittograficamente e indipendentemente dall'autenticatore e dal verificatore e confrontato dal verificatore.

*Il segreto è calcolato in base a un "*nonce*" che può essere basato sul tempo o da un contatore sull'autenticatore e sul verificatore.*

Gli autenticatori OTP a fattore singolo contengono due valori persistenti.

1°. *È una chiave simmetrica interna che rimane per tutta la vita del dispositivo.*

2°. *È un "*nonce*" modificato ogni volta che è utilizzato l'autenticatore oppure si basa su un orologio in tempo reale.*

La chiave segreta e il suo algoritmo DEVE *(*SHALL*) fornire almeno il livello di sicurezza minimo specificato nell'ultima revisione di SP 800-131A (112 bit alla data di questa pubblicazione).*

Il nonce DEVE *essere di lunghezza sufficiente per garantire che sia univoco per ogni operazione del dispositivo nel corso della sua vita.*

Gli autenticatori OTP, in particolare i generatori OTP basati su software, DOVREBBERO *(*SHOULD*) scoraggiare e* NON DEVONO *(*SHALL NOT*) facilitare la clonazione della chiave segreta su più dispositivi.*

L'output dell'autenticatore si ottiene utilizzando un cifrario a blocchi o una funzione HASH *per combinare la chiave e il* nonce *in modo sicuro.*

L'output dell'autenticatore PUÒ *(*MAY*) essere troncato a un minimo di 6 cifre decimali (circa 20 bit di entropia).*

Se il nonce *utilizzato per generare l'output dell'autenticatore è basato su un orologio in tempo reale, esso* DEVE *(*SHALL*) essere cambiato almeno una volta ogni 2 minuti.*

Il valore OTP associato a un dato nonce DEVE *(*SHALL*) essere accettato una sola volta.*

MULTI-FACTOR OTP DEVICE

Un dispositivo OTP a più fattori genera OTP da utilizzare nell'autenticazione dopo l'attivazione tramite un fattore di autenticazione aggiuntivo.

Ciò include dispositivi hardware e generatori OTP basati su software installati su dispositivi come i dispositivi mobili telefoni.

Il secondo fattore di autenticazione può essere ottenuto attraverso una sorta di pad di ingresso integrato, un lettore biometrico integrato (ad es. interfaccia del computer (ad es. porta USB).

L'OTP viene visualizzato sul dispositivo e immesso manualmente per la trasmissione al verificatore.

*Ad esempio, un dispositivo OTP può visualizzare 6 caratteri alla volta, dimostrando così "*IL POSSESSO E IL CONTROLLO*" del dispositivo.*

*Il dispositivo OTP a più fattori è qualcosa "*CHE HAI*" e* DEVE *(*SHALL*) essere attivato da qualcosa che "*TU SAI*" o qualcosa "*CHE SEI*".* (Vedi MULTI-FACTOR AUTHENTICATION MFA)

Gli autenticatori OTP a più fattori funzionano in modo simile agli autenticatori OTP a fattore singolo, tranne per il fatto che richiedono l'inserimento di un segreto memorizzato o l'uso di una biometria per ottenere l'OTP dall'autenticatore. Ogni utilizzo dell'autenticatore DEVE *(*SHALL*) richiedere l'input del fattore aggiuntivo.*

Oltre alle informazioni di attivazione, gli autenticatori OTP a più fattori contengono due valori persistenti.

1°. *È una chiave simmetrica che persiste per tutta la vita del dispositivo.*

2°. *È un* NONCE *che viene modificato ogni volta che viene utilizzato l'autenticatore o si basa su un orologio in tempo reale.*

La chiave segreta e il suo algoritmo DEVONO *(*SHALL*) fornire almeno il livello di sicurezza minimo specificato nell'ultima revisione di SP 800-131A (112 bit alla data di questa pubblicazione).*

Il NONCE DEVE *(*SHALL*) essere di lunghezza sufficiente per garantire che sia univoco per ogni operazione del dispositivo nel corso della sua vita.*

Gli autenticatori OTP, in particolare i generatori OTP basati su software, DOVREBBERO *(*SHOULD*) scoraggiare e* NON DEVONO *(*SHALL NOT*) facilitare la clonazione della chiave segreta su più dispositivi.*

L'output dell'autenticatore è ottenuto utilizzando un cifrario a blocchi approvato o una funzione hash per combinare la chiave e il NONCE *in modo sicuro e* PUÒ *(*MAY*) essere troncato a un minimo di 6 cifre decimali (circa 20 bit di entropia).*

Se il NONCE *utilizzato per generare l'output dell'autenticatore è basato su un orologio in tempo reale, il nonce* DEVE *(*SHALL*) essere modificato almeno una volta ogni 2 minuti.*

Il valore OTP associato a un dato nonce DEVE *(*SHALL*) essere accettato solo una volta.*

Qualsiasi segreto memorizzato utilizzato dall'autenticatore per l'attivazione DEVE *(*SHALL*) essere un segreto numerico scelto casualmente con una lunghezza di almeno 6 cifre decimali oppure un altro segreto memorizzato e* DEVE *(*SHALL*) essere limitato in base alla frequenza come specificato nel capitolo "*RATE LIMITING (THROTTLING)*" descritto più avanti.*

Un fattore di attivazione biometrico DEVE *(*SHALL*) soddisfare i requisiti indicati nel capitolo "*USE OF BIOMETRIC*" descritto più avanti, compresi i limiti su il numero di errori di autenticazione consecutivi.*

La chiave non crittografata e il segreto di attivazione o il campione biometrico — e qualsiasi dato biometrico derivato dal campione biometrico come una sonda prodotta attraverso l'elaborazione del segnale — DEVONO *(*SHALL*) essere azzerati immediatamente dopo che è stata generata una OTP.*

SINGLE-FACTOR CRYPTOGRAPHIC SOFTWARE

Un autenticatore crittografico software a fattore singolo è una chiave crittografica archiviata su disco o su un altro supporto "soft".

L'autenticazione è eseguita dimostrando il possesso e il controllo della chiave.

L'output dell'autenticatore dipende fortemente dal protocollo crittografico specifico, ma generalmente è un tipo di messaggio firmato.

L'autenticatore crittografico software a fattore singolo è qualcosa "CHE HAI". (Vedi MULTI-FACTOR AUTHENTICATION MFA).

Gli autenticatori crittografici software a fattore singolo incapsulano una o più chiavi segrete univoche per l'autenticatore.

La chiave DEVE *(*SHALL*) essere archiviata in un archivio adeguatamente sicuro e disponibile per l'applicazione di autenticazione (ad es. archivio chiavi,* TPM - *Trusted Platform Module -oppure* TEE - *Trusted Execution Environment -se disponibile).*

La chiave DEVE *(*SHALL*) essere fortemente protetta contro la divulgazione non autorizzata mediante l'uso di controlli di accesso che limitano l'accesso alla chiave solo ai componenti software sul dispositivo che richiedono l'accesso.*

Gli autenticatori software crittografici a fattore singolo DOVREBBERO *(*SHOULD*) scoraggiare e* DEVONO *(*SHALL*) facilitare la clonazione della chiave segreta su più dispositivi.*

SINGLE-FACTOR CRYPTOGRAPHIC DEVICES

Un dispositivo crittografico a fattore singolo è un dispositivo hardware che esegue operazioni crittografiche utilizzando chiavi crittografiche protette e fornisce l'output dell'autenticatore tramite connessione diretta all'endpoint utente.

Il dispositivo utilizza chiavi crittografiche simmetriche o asimmetriche incorporate e non richiede l'attivazione tramite un secondo fattore di autenticazione.

L'autenticazione è eseguita dimostrando il possesso del dispositivo tramite il protocollo di autenticazione.

L'output dell'autenticatore è fornito dalla connessione diretta all'endpoint utente ed è fortemente dipendente dal dispositivo e dal protocollo crittografici specifici, ma in genere è un tipo di messaggio firmato.

Un dispositivo crittografico a fattore singolo è qualcosa "CHE HAI". (Vedi MULTI-FACTOR AUTHENTICATION MFA).

SINGLE-FACTOR CRYPTOGRAPHIC DEVICE AUTHENTICATORS

Gli autenticatori di dispositivi crittografici a fattore singolo incapsulano una o più chiavi segrete univoche per il dispositivo e NON DEVONO *(*SHALL NOT*) essere esportabili (ovvero, non possono essere rimosse dal dispositivo).*

L'autenticatore opera firmando un challenge nonce *presentato tramite un'interfaccia diretta del computer (ad esempio, una porta USB).*

In alternativa, l'autenticatore potrebbe essere un processore adeguatamente sicuro integrato con l'endpoint dell'utente stesso (ad esempio, un TPM hardware).

Sebbene i dispositivi crittografici contengano software, differiscono dagli autenticatori di software crittografico in quanto sono tutti incorporati il software è sotto il controllo del CSP o dell'emittente e che l'intero autenticatore è soggetto a tutti i requisiti FIPS 140 applicabili presso l'AAL in fase di autenticazione.

La chiave segreta e il suo algoritmo DEVONO *(*SHALL*) fornire almeno la lunghezza minima di sicurezza specificata nell'ultima revisione di SP 800-131A (112 bit alla data di questa pubblicazione).*

Il challenge nonce DEVE *(*SHALL*) avere una lunghezza di almeno 64 bit.*

Gli autenticatori di dispositivi crittografici a fattore singolo DOVREBBERO *(*SHOULD*) richiedere un input fisico (ad esempio, la pressione di un pulsante) per funzionare.*

Ciò fornisce una difesa contro il funzionamento involontario del dispositivo, che potrebbe verificarsi se l'endpoint a cui è connesso viene compromesso.

SINGLE-FACTOR CRYPTOGRAPHIC DEVICE VERIFIERS

I verificatori di dispositivi crittografici a fattore singolo generano un challenge nonce*, lo inviano all'autenticatore corrispondente e utilizzano l'output dell'autenticatore per verificare il possesso del dispositivo.*

L'output dell'autenticatore dipende fortemente dal dispositivo crittografico e dal protocollo, ma generalmente è un tipo di messaggio firmato.

Il verificatore dispone di chiavi crittografiche simmetriche o asimmetriche corrispondenti a ciascun autenticatore.

Mentre entrambi i tipi di chiavi DEVONO *(*SHALL*) essere protetti contro la modifica, le chiavi simmetriche* DEVONO *(*SHALL*) essere inoltre protette contro la divulgazione non autorizzata.*

Il challenge nonce DEVE *(*SHALL*) avere una lunghezza di almeno 64 bit e* DEVE *(*SHALL*) essere unico per l'intero ciclo di vita dell'autenticatore oppure statisticamente univoco.*

L'operazione di verifica DEVE *(*SHALL*) utilizzare la crittografia approvata.*

MULTI-FACTOR CRYPTOGRAPHIC SOFTWARE

Un autenticatore crittografico software a più fattori è una chiave crittografica archiviata su disco o su un altro supporto "soft" che richiede l'attivazione tramite un secondo fattore di autenticazione.

L'autenticazione viene eseguita dimostrando il possesso e il controllo della chiave.

L'output dell'autenticatore dipende fortemente dal protocollo crittografico specifico, ma generalmente è un tipo di messaggio firmato.

*L'autenticatore crittografico software a più fattori è qualcosa "*CHE HAI*" e* DEVE *(*SHALL*) essere attivato da qualcosa "*CHE CONOSCI*" o qualcosa "*CHE SEI*".* (Vedi MULTI-FACTOR AUTHENTICATION MFA)

Gli autenticatori crittografici software a più fattori incapsulano una o più chiavi segrete univoche per l'autenticatore e accessibili solo attraverso l'input di un fattore aggiuntivo, un segreto memorizzato o una biometria.

La chiave DOVREBBE *(*SHOULD*) essere conservata in un luogo adeguatamente sicuro disponibile per l'applicazione di autenticazione (ad esempio, archiviazione portachiavi, TPM, TEE).*

La chiave DEVE *(*SHALL*) essere fortemente protetta contro la divulgazione non autorizzata mediante l'uso di controlli di accesso che limitano l'accesso alla chiave solo ai componenti software sul dispositivo che richiedono l'accesso.*

Gli autenticatori software crittografici a più fattori DOVREBBERO *(*SHOULD*) scoraggiare e* NON DEVONO *(*SHALL NOT*) facilitare la clonazione della chiave segreta su più dispositivi.*

Ogni operazione di autenticazione che utilizza l'autenticatore DEVE *(*SHALL*) richiedere l'input di entrambi i fattori.*

Qualsiasi segreto memorizzato utilizzato dall'autenticatore per l'attivazione DEVE *(*SHALL*) essere un valore numerico scelto casualmente di almeno 6 cifre decimali di lunghezza o un altro segreto memorizzato che soddisfi i requisiti indicati nel precedente capitolo "*Memorized Secrets*" e* DEVE *(*SHALL*) essere limitato in base alla frequenza come specificato nel capitolo "*Rate Limiting (Throttling)*" descritto più avanti.*

Un fattore di attivazione biometrico DEVE *(*SHALL*) soddisfare i requisiti indicati nel capitolo "*Use of Biometric*" descritto più avanti, compresi i limiti al numero di fallimenti di autenticazione consecutivi.*

La chiave non crittografata e il segreto di attivazione o il campione biometrico (compresi tutti i dati biometrici derivati dal campione biometrico come una sonda prodotta attraverso l'elaborazione del segnale) DEVONO *(*SHALL*) essere azzerati immediatamente dopo l'avvenuta transazione di autenticazione.*

*I requisiti di un verificatore di software crittografico a più fattori sono identici a quelli di un verificatore di dispositivi crittografici a fattore singolo, descritti nel precedente capitolo "*Single-Factor Cryptographic Devices*".*

La verifica dell'output da un autenticatore software crittografico a più fattori dimostra l'uso del fattore di attivazione.

MULTI-FACTOR CRYPTOGRAPHIC DEVICES

Un dispositivo crittografico a più fattori è un dispositivo hardware che esegue operazioni crittografiche che utilizzano una o più chiavi crittografiche protette e richiede l'attivazione tramite un secondo fattore di autenticazione.

L'autenticazione viene eseguita dimostrando il possesso del dispositivo e il controllo della chiave.

L'output dell'autenticatore è fornito dalla connessione diretta all'endpoint utente ed è fortemente dipendente dal dispositivo e dal protocollo crittografici specifici, ma in genere è un tipo di messaggio firmato.

*Il dispositivo crittografico multifattoriale è qualcosa "*CHE HAI*" e* DEVE *(*SHALL*) essere attivato da qualcosa "*CHE CONOSCI*" o qualcosa "*CHE SEI*".* (Vedi MULTI-FACTOR AUTHENTICATION MFA)

Gli autenticatori di dispositivi crittografici a più fattori utilizzano hardware a prova di manomissione per incapsulare una o più chiavi segrete uniche per l'autenticatore e accessibili solo attraverso l'immissione di un fattore aggiuntivo, un segreto memorizzato o un biometrico.

L'autenticatore opera utilizzando a chiave privata che è stata sbloccata dal fattore aggiuntivo per firmare una sfida nonce presentata tramite un'interfaccia diretta del computer (ad esempio, una porta USB).

In alternativa, l'autenticatore potrebbe essere un processore adeguatamente sicuro integrato con l'endpoint dell'utente stesso (ad esempio, un TPM hardware).

Sebbene i dispositivi crittografici contengano software, differiscono dal software crittografico autenticatori in quanto tutto il software incorporato è sotto il controllo del CSP o dell'emittente e che il l'intero autenticatore è soggetto a qualsiasi requisito FIPS 140 applicabile all'AAL selezionato.

La chiave segreta e il suo algoritmo DEVONO *(*SHALL*) fornire almeno la lunghezza minima di sicurezza specificata nell'ultima revisione di SP 800-131A (112 bit alla data di questa pubblicazione).*

Il challenge nonce DEVE *(*SHALL*) avere una lunghezza di almeno 64 bit e* DEVE *(*SHALL*) essere utilizzata la crittografia approvata.*

Ogni operazione di autenticazione che utilizza l'autenticatore DOVREBBE *(*SHOULD*) richiedere l'input del fattore aggiuntivo.*

L'input del fattore aggiuntivo PUÒ *(*MAY*) essere effettuato tramite input diretto sul dispositivo o tramite una connessione hardware (ad es. USB, smartcard).*

Qualsiasi segreto memorizzato utilizzato dall'autenticatore per l'attivazione DEVE *(*SHALL*) essere scelto casualmente valore numerico di almeno 6 cifre decimali di lunghezza o altro segreto memorizzato che soddisfi i requisiti indicati nel precedente capitolo "*Look-Up Secrets*" e* DEVE *(*SHALL*) essere limitato in base alla velocità come specificato nel capitolo "*Rate Limiting (Throttling)*" descritto più avanti.*

Un fattore di attivazione biometrico DEVE *(*SHALL*) soddisfare i requisiti indicati nel capitolo "*Use of Biometric*" descritto più avanti, compresi i limiti al numero di fallimenti di autenticazione consecutivi.*

La chiave non crittografata e il segreto di attivazione o il campione biometrico (compresi tutti i dati biometrici derivati dal campione biometrico come una sonda prodotta attraverso l'elaborazione del segnale) DEVONO *(*SHALL*) essere azzerati immediatamente dopo l'avvenuta transazione di autenticazione.*

*I requisiti per un verificatore di dispositivi crittografici a più fattori sono identici a quelli per un verificatore di dispositivi crittografici a fattore singolo, descritti nel precedente capitolo "*Single-Factor Cryptographic Devices*".*

La verifica dell'output dell'autenticatore da un dispositivo crittografico a più fattori dimostra l'uso del fattore di attivazione.

GENERAL AUTHENTICATOR REQUIREMENTS

Di seguito si descrivono i requisiti generali per gli autenticatori.

PHYSICAL AUTHENTICATORS

Il CSP DEVE *(*SHALL*) fornire ai sottoscrittori istruzioni su come proteggere adeguatamente l'autenticatore contro furto, comportamento o smarrimento.*

Inoltre, DEVE *(*SHALL*) fornire un meccanismo per revocare o sospendere l'autenticatore immediatamente dopo la notifica da parte del sottoscrittore che si sospetta la perdita o il furto dell'autenticatore.*

RATE LIMITING (THROTTLING)

Quando richiesto dalle descrizioni del tipo di autenticatore, il verificatore DEVE *(*SHALL*) implementare I controlli per proteggersi dagli attacchi di ipotesi online.*

Se non diversamente specificato nella descrizione di un dato autenticatore, il verificatore DEVE *(*SHALL*) limitare i tentativi di autenticazione falliti consecutivi su un singolo account a non più di 100.*

Tecniche aggiuntive POSSONO *(*MAY*) essere utilizzate per ridurre la probabilità che un utente malintenzionato blocchi il legittimo richiedente a causa della limitazione della velocità.*

Queste includono:

- *Richiedere al richiedente di completare il* CAPTCHA (COMPLETELY AUTOMATED PUBLIC TURING TEST TO TELL COMPUTER AND HUMANS APART) *prima di tentare l'autenticazione.*
- *Richiedere al richiedente di attendere in seguito a un tentativo fallito per un periodo di tempo che aumenta man mano che l'account si avvicina al limite massimo consentito per tentativi falliti consecutivi (ad esempio, da 30 secondi a un'ora).*
- *Accettare solo le richieste di autenticazione che provengono da una lista bianca di indirizzi IP da cui il sottoscrittore è stato autenticato in precedenza con successo.*
- *Utilizzare altre tecniche di autenticazione basate sul rischio o adattive per identificare se il comportamento dell'utente rientra o non rientra nelle norme tipiche. Queste potrebbero, ad esempio, includere l'uso dell'indirizzo IP, la geolocalizzazione, i tempi dei modelli di richiesta o i metadati del browser.*

Quando il sottoscrittore si autentica con successo, il verificatore DOVREBBE *(*SHOULD*) ignorare qualsiasi precedente tentativo fallito per quell'utente dallo stesso indirizzo IP.*

USE OF BIOMETRICS

*L'uso della biometria (qualcosa "*che sei*") nell'autenticazione include sia la misurazione di caratteristiche fisiche (ad es. impronte digitali, iride, caratteristiche facciali) e caratteristiche comportamentali (ad es. cadenza di battitura).*

*Entrambe le classi sono considerate modalità biometriche, sebbene modalità diverse possano differire nella misura in cui stabiliscono l'intento di autenticazione come descritto nel capitolo "*Authentication Intent*" descritto più avanti.*

Di seguito alcune motivazioni per un uso limitato della biometria nella Autenticazione.

1. *Il False Match Rate (FMR) biometrico non fornisce fiducia nell'autenticazione del sottoscrittore stesso. Inoltre, FMR non tiene conto degli attacchi di spoofing.*
2. *Il confronto biometrico è probabilistico, mentre gli altri fattori di autenticazione sono deterministici.*
3. *Gli schemi di protezione dei modelli biometrici forniscono un metodo per revocare le credenziali biometriche paragonabile ad altri fattori di autenticazione (ad esempio, certificati PKI e password).*

4. *Le caratteristiche biometriche non costituiscono segreti.*
   Possono essere ottenute online o tramite una foto di qualcuno con un telefono con fotocamera (ad es. immagini facciali) con o senza la loro consapevolezza, da oggetti toccati da qualcuno (ad es. impronte digitali latenti) o catturata con immagini ad alta risoluzione (ad es. modelli dell'iride).
   *Sebbene le tecnologie di rilevamento degli attacchi di presentazione (*Presentation Attack Detection PAD*) (ad es. rilevamento della vitalità) possano mitigare il rischio di questi tipi di attacchi, è necessaria un'ulteriore fiducia nel sensore o nell'elaborazione biometrica per garantire che il PAD operi in conformità con le esigenze del CSP e del sottoscrittore.*

Per l'uso della biometria in combinazione con altre tecniche di autenticazione, vedi NIST SP 800-63B.

ATTESTATION

Un'attestazione è un'informazione trasmessa al verificatore in merito a una persona direttamente collegata all'autenticatore o all'endpoint coinvolto in un'operazione di autenticazione.

Le informazioni trasmesse dall'attestazione POSSONO *(*MAY*) includere anche:*

- *la provenienza (ad es. certificazione del produttore o del fornitore), la salute e l'integrità del autenticatore ed endpoint;*
- *funzionalità di sicurezza dell'autenticatore;*
- *caratteristiche di sicurezza e prestazioni dei sensori biometrici;*
- *modalità del sensore.*

Le informazioni di attestazione POSSONO *(*MAY*) essere utilizzate come parte della decisione di autenticazione basata sul rischio di un verificatore.*

VERIFIER IMPERSONATION RESISTANCE

*Gli attacchi di simulazione del verificatore, a volte indicati come "***ATTACCHI DI PHISHING***", sono tentativi da parte di verificatori e RP (Relying Party) fraudolenti per ingannare un richiedente incauto inducendolo ad autenticarsi su un sito Web di impostori.*

Un protocollo di autenticazione resistente alla rappresentazione del verificatore DEVE *(*SHALL*) stabilire un canale protetto autenticato con il verificatore e* DEVE *(*SHALL*) legare in modo forte e irreversibile un identificatore di canale che è stato negoziato per stabilire il canale protetto autenticato all'output dell'autenticatore (ad esempio, firmando i due valori insieme utilizzando una chiave privata controllata dal richiedente la cui chiave pubblica è nota al verificatore).*

Il verificatore DEVE *(*SHALL*) convalidare la firma o altre informazioni utilizzate per dimostrare la resistenza al tentativo di simulazione del verificatore. Ciò impedisce all' impostore, anche se ha ottenuto un certificato che rappresenta il verificatore effettivo, di riprodurre tale autenticazione su un diverso canale protetto autenticato.*

Gli algoritmi crittografici approvati DEVONO *(*SHALL*) essere utilizzati per stabilire la resistenza alla rappresentazione del verificatore laddove richiesto.*

Le chiavi utilizzate a questo scopo DEVONO *(*SHALL*) fornire almeno il livello di sicurezza minimo specificato nell'ultima revisione di SP 800-131A (112 bit alla data di questa pubblicazione).*

Un esempio di protocollo di autenticazione resistente alla rappresentazione del verificatore è l'autenticazione del client TLS, perché il client firma l'output dell'autenticatore insieme ai messaggi precedenti dal protocollo univoco per la particolare connessione TLS negoziata.

Gli autenticatori che comportano l'inserimento manuale di un output dell'autenticatore, come gli autenticatori fuori banda e OTP, NON DEVONO *(*SHALL NOT*) essere considerati resistenti alla rappresentazione del verificatore perché l'immissione manuale non vincola l'output dell'autenticatore alla sessione specifica da autenticare.*

In un attacco MitM (Man in the Middle)*, un verificatore impostore potrebbe riprodurre l'output dell'autenticatore OTP al verificatore e autenticarsi correttamente.*

VERIFIER-CSP COMMUNICATIONS

Nelle situazioni in cui il verificatore e il CSP sono entità separate (come mostrato dalla linea tratteggiata nella figura 4-1 (vedi NIST SP 800-63-3), le comunicazioni tra il verificatore e il CSP DEVONO *(*SHALL*) avvenire attraverso un canale sicuro autenticato reciprocamente (come un client -connessione TLS autenticata) utilizzando la crittografia approvata.*

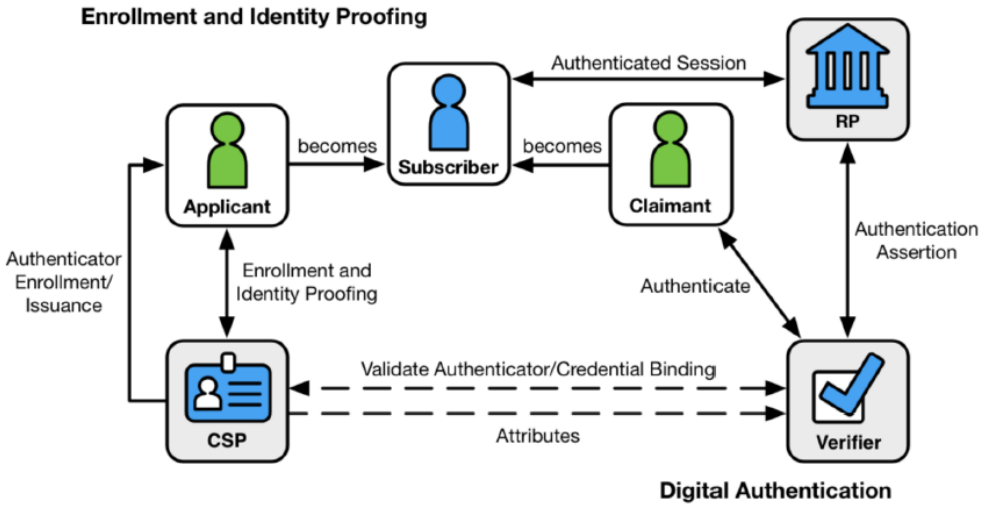


Figure 4-1 Digital Identity Model

VERIFIER-COMPROMISE RESISTANCE

L'utilizzo di alcuni tipi di autenticatori richiede che il verificatore memorizzi una copia del segreto dell'autenticatore. Ad esempio, un autenticatore OTP richiede che il verificatore generi in modo indipendente l'output dell'autenticatore per il confronto con il valore inviato dal richiedente.

A causa della possibilità che il verificatore venga compromesso e che i segreti archiviati vengano rubati, i protocolli di autenticazione, che non richiedono al verificatore di archiviare in modo permanente i segreti che potrebbero essere utilizzati per l'autenticazione, sono considerati più forti.

Un verificatore potrebbe essere compromesso in un modo diverso, ad esempio essere manipolato per accettare sempre un particolare output dell'autenticatore.

La resistenza alla compromissione del verificatore può essere ottenuta in diversi modi, ad esempio:

- *utilizzare un autenticatore crittografico che richieda al verificatore di memorizzare una chiave pubblica corrispondente a una chiave privata detenuta dall'autenticatore;*
- *memorizzare l'output previsto dell'autenticatore in forma hash.*

Per essere considerate resistenti alla compromissione del verificatore, le chiavi pubbliche memorizzate dal verificatore DEVONO *(*SHALL*) essere associate all'uso di algoritmi crittografici approvati e* DEVONO *(*SHALL*) fornire almeno il livello di sicurezza minimo specificato nell'ultima revisione di SP 800-131A (112 bit alla data di questa pubblicazione).*

REPLAY RESISTANCE

Un processo di autenticazione resiste agli attacchi di REPLAY *se è impraticabile ottenere con successo l'autenticazione registrando e riproducendo un precedente messaggio di autenticazione.*

La resistenza alla riproduzione si aggiunge alla natura resistente alla riproduzione dei protocolli del canale protetto autenticato, poiché l'output potrebbe essere rubato prima dell'ingresso nel canale protetto.

I protocolli che utilizzano NONCE *o* CHALLENGE *per dimostrare la "freschezza" della transazione sono resistenti agli attacchi di* REPLAY *poiché il verificatore rileverà facilmente quando i vecchi messaggi del protocollo sono riprodotti poiché non conterranno i* NONCE *appropriati o i dati sulla tempestività.*

Esempi di autenticatori resistenti alla riproduzione sono i dispositivi OTP, gli autenticatori crittografici e i segreti di ricerca. Al contrario, i segreti memorizzati non sono considerati resistenti alla riproduzione perché l'output dell'autenticatore, il segreto stesso, viene fornito per ogni autenticazione.

AUTHENTICATION INTENT

Un processo di autenticazione dimostra L'INTENTO *se richiede al soggetto di rispondere esplicitamente a ciascuna richiesta di autenticazione o riautenticazione.*

L'obiettivo dell'intento di autenticazione è di rendere più difficile l'uso degli autenticatori fisici collegati direttamente (ad es. dispositivi) all'insaputa del soggetto, ad esempio tramite malware sull'endpoint.

L'intento di autenticazione PUÒ *(*MAY*) essere stabilito in diversi modi:*

- *i processi di autenticazione che richiedono l'intervento del soggetto: ad esempio, un richiedente che inserisce un output di autenticazione da un dispositivo OTP;*
- *i dispositivi crittografici che richiedono l'azione dell'utente: ad esempio, la pressione di un pulsante.*

A seconda della modalità, la presentazione di una biometria può o meno stabilire l'autenticazione intento. La presentazione di un'impronta digitale normalmente stabilirebbe l'intento, mentre l'osservazione del volto del ricorrente utilizzando una fotocamera normalmente non lo sarebbe da sola. Allo stesso modo, è meno probabile che la biometria comportamentale stabilisca l'intento di autenticazione perché non sempre richiedono un'azione specifica da parte del richiedente.

RESTRICTED AUTHENTICATORS

L'uso di un autenticatore RESTRICTED *(Limitato) richiede che l'organizzazione attuatore valuti, comprenda e accetti i rischi associati a tale autenticatore e riconosca che il rischio probabilmente aumenti nel tempo.*

È responsabilità dell'organizzazione determinare il livello di rischio accettabile per i propri sistemi e dati associati e definire eventuali metodi per mitigare i rischi eccessivi.

Se in qualsiasi momento l'organizzazione determina che il rischio per qualsiasi parte è inaccettabile, allora tale autenticatore NON DOVRÀ *(*SHALL NOT*) essere utilizzato.*

Inoltre, il rischio di un errore di autenticazione è in genere sostenuto da più parti, tra cui l'organizzazione di attuazione, le organizzazioni che si affidano alla decisione di autenticazione e il sottoscrittore.

Poiché il sottoscrittore può essere esposto a rischi aggiuntivi quando un'organizzazione accetta un autenticatore RESTRICTED *e il sottoscrittore può avere una comprensione e una capacità limitate di controllare tale rischio, il CSP* DEVE *(*SHALL*):*

1. *offrire ai sottoscrittori almeno un autenticatore alternativo che non sia* RESTRICTED *e può essere utilizzato per l'autenticazione all'AAL richiesto;*
2. *fornire un avviso significativo agli abbonati in merito ai rischi per la sicurezza dell'autenticatore* RESTRICTED *e alla disponibilità di alternative non* RESTRICTED*;*
3. *affrontare qualsiasi rischio aggiuntivo per i sottoscrittori nella sua valutazione del rischio;*
4. *Sviluppare un piano di migrazione per garantire la possibilità che l'autenticatore* RESTRICTED *non sia più accettabile in futuro e includere questo piano di migrazione nella sua dichiarazione di accettazione dell'identità digitale.*

104. AUTHENTICATOR LIFECYCLE MANAGEMENT

Durante il ciclo di vita dell'autenticatore del sottoscrittore possono verificarsi numerosi eventi che influiscono sull'uso di tale autenticatore.

Questi eventi includono vincolo, smarrimento, furto, duplicazione non autorizzata, scadenza e revoca.

AUTHENTICATOR BINDING

Il legame dell'autenticatore si riferisce alla creazione di un'associazione tra un autenticatore specifico e l'account di un sottoscrittore, che consente di utilizzare l'autenticatore, possibilmente insieme ad altri autenticatori, per autenticarsi per quell'account.

Gli autenticatori DEVONO *(*SHALL*) essere vincolati agli account dei sottoscrittori da:*

- ✓ *Rilascio da parte del CSP nell'ambito dell'immatricolazione; oppure*
- ✓ *Associazione di un autenticatore fornito dal sottoscrittore che sia accettabile per il CSP.*

Per tutto il ciclo di vita dell'identità digitale, i CSP DEVONO *(*SHALL*) mantenere un registro di tutti gli autenticatori che sono o sono stati associati a ciascuna identità.*

Il CSP o il verificatore DEVE *(*SHALL*) mantenere le informazioni richieste per limitare i tentativi di autenticazione quando richiesto.*

Il CSP DEVE *(*SHALL*) inoltre verificare il tipo di autenticatore fornito dall'utente (ad esempio, dispositivo crittografico a fattore singolo rispetto a dispositivo crittografico a più fattori) in modo che i verificatori possano determinare la conformità ai requisiti in ogni AAL.*

Il record creato dal CSP DEVE *(*SHALL*) contenere la data e l'ora in cui l'autenticatore è stato associato all'account e* DOVREBBE *(*SHOULD*) includere informazioni sulla fonte dell'associazione (ad esempio, indirizzo IP, identificatore del dispositivo) di qualsiasi dispositivo associato alla registrazione.*

Se disponibile, il record DOVREBBE *(*SHOULD*) contenere anche informazioni sulla fonte delle autenticazioni non riuscite, tentate con l'autenticatore.*

Quando un nuovo autenticatore è vincolato a un account di sottoscrittore, il CSP DEVE *(*SHALL*) garantire che il protocollo vincolante e il protocollo per la fornitura delle chiavi associate siano eseguiti a un livello di sicurezza commisurato all'AAL al quale verrà utilizzato l'autenticatore.*

Ad esempio, i protocolli per il provisioning delle chiavi DEVONO *(*SHALL*) utilizzare canali protetti autenticati o essere eseguiti di persona per proteggersi dagli attacchi* MAN-IN-THE-MIDDLE.

L'associazione di autenticatori a più fattori DEVE *(*SHALL*) richiedere la MFA (Multi-Factor Authentication) o equivalente (ad esempio, l'associazione con la sessione in cui è stata appena completata la verifica dell'identità) per vincolare l'autenticatore.*

Le stesse condizioni si applicano quando una coppia di chiavi viene generata dall'autenticatore e la chiave pubblica viene inviata al CSP.

BINDING AT ENROLLMENT

I seguenti requisiti si applicano quando un autenticatore è vincolato a un'identità a seguito di una transazione di verifica dell'identità riuscita.

È richiesto l'uso di MFA per il rilascio di qualsiasi dato personale ed è importante che gli autenticatori siano vincolati agli account degli sottoscrittori al momento dell'iscrizione, consentendo l'accesso ai dati personali, compresi quelli stabiliti dalla prova di identità.

Il CSP DEVE *(*SHALL*) associare almeno uno e* DOVREBBE *(*SHOULD*) associare almeno due autenticatori fisici (qualcosa che hai) all'identità online del sottoscrittore, oltre a un segreto memorizzato o a uno o più dati biometrici.*

L'associazione di più autenticatori è preferibile per recuperare dalla perdita o dal furto dell'autenticatore principale del sottoscrittore.

Sebbene tutte le informazioni identificative siano auto-affermate presso IAL1, la conservazione del materiale online o della reputazione online rende indesiderabile la perdita del controllo di un account a causa della perdita di un autenticatore.

Il secondo autenticatore consente di recuperare in modo sicuro da una perdita di autenticatore.

Per questo motivo, un CSP DOVREBBE *(*SHOULD*) associare almeno due autenticatori fisici alle credenziali del sottoscrittore anche su IAL1.*

In IAL2 e superiori, le informazioni di identificazione sono associate all'identità digitale e il sottoscrittore ha subito un processo di verifica dell'identità.

Di conseguenza, gli autenticatori dello stesso AAL dell'IAL desiderato DEVONO *(*SHALL*) essere vincolati all'account.*

Ad esempio, se il sottoscrittore ha completato con successo la verifica in IAL2, gli autenticatori AAL2 o AAL3 sono appropriati per l'associazione all'identità IAL2.

Mentre un CSP PUÒ (MAY) *associare un autenticatore AAL1 a un'identità IAL2, se il sottoscrittore è autenticato presso AAL1, il CSP* NON DEVE *(*SHALL NOT*) esporre informazioni personali, anche se auto-affermate, al sottoscrittore.*

La disponibilità di autenticatori aggiuntivi fornisce metodi di backup per l'autenticazione se un autenticatore viene danneggiato, perso o rubato.

Se l'iscrizione e l'associazione non possono essere completate in un unico incontro fisico o transazione (cioè, all'interno di un'unica sessione protetta), DEVONO *(*SHALL*) essere utilizzati i seguenti metodi per garantire che la stessa parte agisca come richiedente durante tutti i processi:*

PER LE TRANSAZIONI A DISTANZA

1) Il richiedente Deve (Shall) identificarsi in ogni nuova transazione vincolante presentando un segreto temporaneo che è stato stabilito durante una transazione precedente o inviato al numero di telefono, indirizzo e-mail o indirizzo postale del richiedente.

2) I segreti dell'autenticatore a lungo termine Devono (Shall) essere rilasciati al richiedente solo all'interno di una sessione protetta.

PER LE TRANSAZIONI DI PERSONA

1. *Il richiedente* DEVE *(*SHALL*) identificarsi di persona utilizzando un segreto come descritto nella transazione a distanza (1) di cui sopra, o tramite l'uso di un dispositivo biometrico registrato durante un incontro precedente.*
2. *I segreti temporanei* NON DEVONO *(*SHALL NOT*) essere riutilizzati.*
3. *Se il CSP rilascia segreti di autenticazione a lungo termine durante una transazione fisica,* NON DEVONO *(*SHALL NOT*) essere caricati localmente su un dispositivo fisico rilasciato di persona al richiedente o consegnato in modo da confermare l'indirizzo di registrazione.*

POST- ENROLLMENT BINDING

Di seguito si descrive l'associazione di un autenticatore all'account di un sottoscrittore.

BINDING OF AN ADDITIONAL AUTHENTICATOR AT EXISTING AAL

Ad eccezione dei segreti memorizzati, i CSP e i verificatori DOVREBBERO *(*SHOULD*) incoraggiare i sottoscrittori a mantenere almeno due autenticatori validi di ciascun fattore che utilizzeranno.*

Ad esempio, un sottoscrittore che di solito utilizza un dispositivo OTP come autenticatore fisico PUÒ (MAY) *anche ricevere un numero di autenticatori segreti di ricerca o registrare un dispositivo per l'autenticazione out-of-band, nel caso in cui l'autenticatore fisico venga perso, rubato o danneggiato.*

Il CSP DOVREBBE *(*SHOULD*) consentire l'associazione di autenticatori aggiuntivi all'account di un sottoscrittore.*

Prima di aggiungere il nuovo autenticatore, il CSP DEVE *(*SHALL*) prima richiedere al sottoscrittore di autenticarsi presso l'AAL (o un AAL superiore) in cui verrà utilizzato il nuovo autenticatore.*

Quando viene aggiunto un autenticatore, il CSP DOVREBBE *(*SHOULD*) inviare una notifica al sottoscrittore tramite un meccanismo indipendente dalla transazione che lega il nuovo autenticatore (ad esempio, e-mail a un indirizzo precedentemente associato al sottoscrittore).*

Il CSP PUÒ (MAY) *limitare il numero di autenticatori che può essere vincolato in questo modo.*

ADDING AN ADDITIONAL FACTOR TO A SINGLE-FACTOR ACCOUNT

Se l'account del sottoscrittore ha un solo fattore di autenticazione vincolato (ad esempio, a IAL1/AAL1*) e deve essere aggiunto un ulteriore autenticatore di un diverso fattore di autenticazione, il sottoscrittore* PUÒ (MAY) *richiedere che l'account venga aggiornato a* AAL2*.*

La IAL *rimarrebbe a* IAL1*.*

Prima di vincolare il nuovo autenticatore, il CSP DEVE *(*SHALL*) richiedere al sottoscrittore di autenticarsi a* AAL1*.*

Il CSP DOVREBBE *(*SHOULD*) inviare una notifica dell'evento al sottoscrittore tramite un meccanismo indipendentemente dalla transazione che lega il nuovo autenticatore (ad esempio, e-mail a un indirizzo precedentemente associato al sottoscrittore).*

REPLACEMENT OF A LOST AUTHENTICATION FACTOR

Se un sottoscrittore perde tutti gli autenticatori di un fattore necessario per completare il multifattore autenticazione ed è stata verificata l'identità presso IAL2 o IAL3, il sottoscrittore DEVE *(*SHALL*) ripetere il processo di verifica dell'identità descritto in SP 800-63A.*

*Un processo di correzione abbreviato, confermando il vincolo del ricorrente (*CLAIMANT*) alle prove precedentemente fornite,* PUÒ (MAY) *essere utilizzato se il CSP ha conservato le prove del processo di verifica originale in base a una valutazione del rischio per la privacy come descritto in SP 800-63A Sezione 4.2.*

Il CSP DEVE *(*SHALL*) richiedere al richiedente di autenticarsi utilizzando un autenticatore del fattore rimanente, se presente, per confermare il legame con l'identità esistente.*

Il ripristino dei fattori di autenticazione presso IAL3 DEVE *(*SHALL*) essere effettuato di persona o tramite un processo remoto supervisionato come descritto in SP 800-63A Sezione 5.3.3.2 e* DEVE *(*SHALL*) verificare i dati biometrici raccolti durante il processo di verifica originale.*

La sostituzione di un segreto memorizzato perché perso o dimenticato è problematica perché è molto comune.

Se una biometria è associata all'account, l'autenticatore biometrico e fisico associato DOVREBBE *(*SHOULD*) essere utilizzato per stabilire un nuovo segreto memorizzato.*

In alternativa al suddetto processo di riprovazione quando non vi è alcun vincolo biometrico all'account, il CSP PUÒ (MAY) *associare un nuovo segreto memorizzato con autenticazione utilizzando due autenticatori fisici, insieme a un codice di conferma che è stato inviato a uno degli indirizzi del sottoscrittore di registrazione.*

Il codice di conferma DEVE *(*SHALL*) essere composto da almeno 6 caratteri alfanumerici casuali generati da un generatore di bit casuale approvato [SP 800-90Ar1].*

Quelli inviati a un indirizzo postale registrato DEVONO *(*SHALL*) essere validi per un massimo di 7 giorni, ma* POSSONO (MAY) *essere resi validi fino a 21 giorni tramite un processo di eccezione per accogliere indirizzi al di fuori della portata diretta del servizio postale.*

I codici di conferma inviati con mezzi diversi dalla posta fisica DEVONO *(*SHALL*) essere validi per un massimo di 10 minuti.*

BINDING TO A SUBSCRIBER-PROVIDED AUTHENTICATOR

Un sottoscrittore può già possedere autenticatori adatti per l'autenticazione in un particolare AAL.

Ad esempio, potrebbero avere un autenticatore a due fattori di un provider di social network, considerato AAL2 *e* IAL1 *e vorrebbe utilizzare tali credenziali in un* RP *che richiede* IAL2.

Il CSP DOVREBBE *(*SHOULD*), ove possibile, consentire l'uso di autenticatori forniti dal sottoscrittore in al fine di alleviare l'onere per il sottoscrittore di gestire un gran numero di autenticatori.*

L'associazione di questi autenticatori DEVE *(*SHALL*) essere eseguita come descritto nel precedente paragrafo "*BINDING OF AN ADDITIONAL AUTHENTICATOR AT EXISTING AAL*".*

In situazioni in cui la forza dell'autenticatore non è auto-evidente (ad esempio, tra autenticatori a fattore singolo e multifattore di un dato tipo), il CSP DOVREBBE *(*SHOULD*) assumere l'uso dell'autenticatore più debole a meno che non sia in grado di stabilire che l'autenticatore più forte è infatti in uso (ad esempio, da verifica con l'emittente o il produttore dell'autenticatore).*

RENEWAL

Il CSP DOVREBBE *(*SHOULD*) vincolare un autenticatore aggiornato un periodo di tempo appropriato prima della scadenza di un autenticatore esistente.*

Il processo per questo DOVREBBE *(*SHOULD*) conformarsi strettamente al processo di associazione dell'autenticatore iniziale (ad esempio, conferma dell'indirizzo di registrazione).*

A seguito dell'utilizzo riuscito del nuovo autenticatore, il CSP PUÒ (MAY) *revocare l'autenticatore che sta sostituendo.*

LOSS, THEFT, DAMAGE, AND UNAUTHORIZED DUPLICATION

Gli autenticatori compromessi includono quelli che sono stati persi, rubati o soggetti a duplicazione non autorizzata.

Un'eccezione degna di nota è un segreto memorizzato che è stato dimenticato senza altre indicazioni di essere stato compromesso, è come se fosse stato ottenuto da un attaccante.

La sospensione, la revoca o la distruzione degli autenticatori compromessi DOVREBBE *(*SHOULD*) verificarsi con la massima rapidità possibile dopo il rilevamento.*

Le agenzie DOVREBBERO *(*SHOULD*) stabilire limiti di tempo per questo processo.*

Per facilitare la segnalazione sicura della perdita, del furto o del danneggiamento di un autenticatore, il CSP DOVREBBE *(*SHOULD*) fornire al sottoscrittore un metodo di autenticazione al CSP utilizzando un backup o un autenticatore alternativo.*

Questo autenticatore di backup DEVE *(*SHALL*) essere un segreto memorizzato o un autenticatore fisico.*

Oppure PUÒ (MAY) *essere usato, ma è richiesto un solo fattore di autenticazione per questo rapporto.*

In alternativa, il sottoscrittore PUÒ (MAY) *stabilire un canale protetto autenticato verso il CSP e verificare le informazioni raccolte durante il processo di verifica.*

Il CSP PUÒ (MAY) *scegliere di verificare un indirizzo di registrazione (cioè, e-mail, telefono, postale) e sospendere gli autenticatori segnalati come compromessi.*

La sospensione DEVE *(*SHALL*) essere reversibile se il sottoscrittore si autentica con successo al CSP utilizzando un autenticatore valido (cioè non sospeso) e richiede la riattivazione di un autenticatore sospesa.*

Il CSP PUÒ (MAY) *fissare un limite di tempo dopo quale un autenticatore sospeso non può più essere riattivato.*

EXPIRATION

I CSP POSSONO (MAY) *emettere autenticatori che scadono ma questi* NON DEVONO *(*SHALL NOT) *essere utilizzabili per l'autenticazione.*

Quando viene tentata un'autenticazione utilizzando un autenticatore scaduto, il CSP DOVREBBE *(*SHOULD) *dare le indicazioni al sottoscrittore che il fallimento dell'autenticazione è dovuta alla scadenza piuttosto che a qualche altra causa.*

Il CSP DEVE *(*SHALL) *richiedere agli sottoscrittori di consegnare o provare la distruzione di qualsiasi autenticatore fisico contenente certificati di attributo firmati dal CSP non appena possibile dopo la scadenza o il ricevimento di un autenticatore rinnovato.*

REVOCATION AND TERMINATION

La revoca di un autenticatore - a volte indicata come terminazione, specialmente nel contesto degli autenticatori PIV - si riferisce alla rimozione del legame tra un autenticatore e una credenziale che il CSP mantiene.

Il CSP DEVE *(*SHALL) *revocare prontamente il vincolo degli autenticatori quando un'identità online cessa di esistere (ad esempio, la morte del sottoscrittore, la scoperta di un sottoscrittore fraudolento), quando richiesto dal sottoscrittore, o quando il CSP determina che il sottoscrittore non soddisfa più i suoi requisiti di idoneità.*

Il CSP DEVE *(*SHALL) *richiedere ai sottoscrittori di cedere o certificare la distruzione di qualsiasi autenticatore fisico contenente attributi certificati firmati dal CSP non appena possibile dopo la revoca o la cessazione.*

Ciò è necessario per bloccare l'utilizzo degli attributi certificati dell'autenticatore in situazioni offline tra revoca/cessazione e scadenza della certificazione.

105. SESSION MANAGEMENT

Una volta che si è verificato un evento di autenticazione, è spesso desiderabile consentire al sottoscrittore di continuare a utilizzare l'applicazione attraverso più interazioni successive senza richiedere loro di ripetere l'evento di autenticazione.

Per facilitare questo comportamento, una sessione può essere avviata in risposta a un evento di autenticazione e continuare la sessione fino al momento in cui viene terminata.

SESSION BINDING

Si verifica una sessione tra un sottoscrittore, tramite browser, e l'RP o CSP a cui il sottoscrittore sta accedendo (ovvero l'host della sessione).

Un segreto di sessione DEVE *(*SHALL) *essere condiviso tra i software del sottoscrittore e il servizio a cui si accede. Questo segreto lega le due estremità della sessione, consentendo al sottoscrittore di continuare a utilizzare il servizio nel tempo.*

Il segreto DEVE *(*SHALL) *essere presentato direttamente dal software del sottoscrittore oppure il possesso del segreto* DEVE *(*SHALL) *essere dimostrato utilizzando un meccanismo crittografico.*

Il segreto utilizzato per il binding della sessione DOVREBBE *(*SHOULD) *essere generato dall'host della sessione in risposta diretta a un evento di autenticazione.*

Una sessione DOVREBBE *(*SHOULD) *ereditare le proprietà AAL dell'evento di autenticazione che ha attivato la sua creazione.*

Una sessione PUÒ *(*MAY) *essere considerata ad un AAL inferiore rispetto all'evento di autenticazione ma* NON DEVE *(*SHALL NOT) *essere considerata a un AAL superiore rispetto all'evento di autenticazione.*

I segreti utilizzati per l'associazione della sessione sono:

1. DEVE *(*SHALL) *essere generato dall'host di sessione durante un'interazione, in genere immediatamente dopo l'autenticazione;*

2. DEVE (SHALL) *essere generato da un generatore di bit casuale e contenere almeno 64 bit di entropia.*
3. DEVE (SHALL) *essere cancellato o invalidato dal soggetto della sessione quando il sottoscrittore si disconnette.*
4. DOVREBBE (SHOULD) *essere cancellato sull'endpoint del sottoscrittore quando l'utente si disconnette o quando si ritiene che il segreto sia scaduto.*
5. NON DOVREBBE (SHOULD NOT) *essere collocato in posizioni non sicure come l'archiviazione locale HTML5 a causa della potenziale esposizione dell'archiviazione locale ad attacchi* **XSS (CROSS-SITE SCRIPTING)**.
6. DEVE (SHALL) *essere inviato e ricevuto dal dispositivo utilizzando un canale protetto autenticato.*
7. DEVE (SHALL) *scadere e non essere accettato dopo i tempi specificati e appropriato per l'AAL.*
8. NON DEVE (SHALL NOT) *essere disponibile per comunicazioni non sicure tra l'host e l'endpoint del sottoscrittore.*
   Le sessioni autenticate NON DEVONO (SHALL NOT) *ricorrere a un trasporto non sicuro, come da* **HTTPS** *a* **HTTP**, *dopo l'autenticazione.*

Gli URL o POST DEVE (SHALL) *contenere un identificatore di sessione che* DEVE (SHALL) *essere verificato dall'RP per assicurarsi che le azioni intraprese al di fuori della sessione non influiscano sulla sessione protetta.*

BROWSER COOKIES

I cookie del browser sono il meccanismo predominante mediante il quale sarà creata e tracciata una sessione per un sottoscrittore che accede a un servizio.

Il Cookie:

1. DEVE (SHALL) *essere contrassegnato per essere accessibile solo su sessioni sicure (HTTPS).*
2. DEVE (SHALL) *essere accessibile al minimo insieme pratico di nomi host e percorsi.*
3. DOVREBBE (SHOULD) *essere contrassegnato per essere inaccessibile tramite JavaScript (Http Only).*
4. DOVREBBE (SHOULD) *essere contrassegnato per scadere al, o subito dopo, il periodo di validità della sessione.*
   Questo requisito ha lo scopo di limitare l'accumulo di cookie, ma NON DEVE (SHALL NOT) *imporre timeout di sessione.*

ACCESS TOKENS

Un token di accesso è utilizzato per consentire ad un'applicazione di accedere ad una serie di servizi per conto di un sottoscrittore a seguito di un evento di autenticazione.

La presenza di un token di accesso NON DEVE (SHALL NOT) *essere interpretata dal PR come presenza del sottoscrittore, in assenza di altre segnalazioni.*

Il token di accesso e tutti i token di aggiornamento associati POSSONO (MAY) *essere validi per molto tempo dopo che la sessione di autenticazione è terminata e il sottoscrittore ha lasciato l'applicazione.*

DEVICES IDENTIFICATION

Altri metodi di identificazione sicura del dispositivo, inclusi ma non limitati a TLS, associazione di token o altri meccanismi, POSSONO (MAY) *essere utilizzati per attivare una sessione tra un sottoscrittore e un servizio.*

REAUTHENTICATION

La continuità delle sessioni autenticate DEVE (SHALL) *essere basata sul possesso di un segreto di sessione rilasciato dal verificatore al momento dell'autenticazione ed eventualmente aggiornato durante la sessione.*

La natura di una sessione dipende dall'applicazione, tra cui:

1. *una sessione del browser web con un cookie di "sessione", oppure*
2. *un'istanza di un'applicazione mobile che conserva un segreto di sessione.*

I segreti di sessione DEVONO *(*SHALL*) essere non persistenti, cioè,* NON DEVONO *(*SHALL NOT*) essere mantenuti dopo un riavvio dell'applicazione associata o un riavvio del dispositivo host.*

La riautenticazione periodica delle sessioni DEVE *(*SHALL*) essere eseguita per confermare la presenza continua del sottoscrittore a una sessione autenticata (cioè, senza che il sottoscrittore non si sia disconnesso).*

Prima della scadenza della sessione, il limite di tempo per la riautenticazione DEVE *(*SHALL*) essere esteso richiedendo al sottoscrittore il/i fattore/i di autenticazione specificato nella Tabella 7-1.*

Quando una sessione è stata terminata, a causa di un timeout o di un'altra azione, all'utente DEVE *(*SHALL*) essere richiesto di stabilire una nuova sessione autenticandosi nuovamente.*

Nota: in AAL2, è richiesto un segreto memorizzato o biometrico, e non un autenticatore fisico, perché il segreto della sessione è qualcosa che "HAI" ed è necessario un fattore di autenticazione aggiuntivo per continuare la sessione.

Table 7-1 - AAL Reauthentication Requirements

AAL	Requirement
1	Presentation of any one factor
2	Presentation of a memorized secret or biometric
3	Presentation of all factors

106. THREATS AND SECURITY CONSIDERATIONS

Esistono due categorie generali di minacce al processo di registrazione: furto d'identità e compromissione o illecito del fornitore dell'infrastruttura.

Per motivi pratici, c si concentra sulle minacce di imitazione o furto d'identità, poiché le minacce all'infrastruttura sono affrontate dai tradizionali controlli di sicurezza.

Le minacce al processo di registrazione o presentazione del sottoscrittore al sistema includono attacchi di rappresentazione e minacce ai meccanismi di trasporto per la verifica dell'identità, l'associazione dell'autenticatore e il rilascio delle credenziali.

La Tabella 7-1 elenca le minacce relative alla registrazione e alla verifica dell'identità.

Table 7-1 Enrollment and Identity Proofing Threats

Activity	Threat/Attack	Example
Enrollment	Falsified identity proofing evidence	An applicant claims an incorrect identity by using a forged driver's license.
	Fraudulent use of another's identity	An applicant uses a passport associated with a different individual.
	Enrollment repudiation	A subscriber denies enrollment, claiming that they did not enroll with the CSP.

AUTHENTICATOR THREAT

Le minacce agli autenticatori possono essere classificate in base agli attacchi ai tipi di fattori di autenticazione che comprendono l'autenticatore.

TABLE 8-1 AUTHENTICATOR THREATS

Authenticator Threat/Attack	Description	Example
Assertion Manufacture or Modification	The attacker generates a false assertion	Compromised CSP asserts identity of a claimant who has not properly authenticated
	The attacker modifies an existing assertion	Compromised proxy that changes AAL of an authentication assertion
Theft	A physical authenticator is stolen by an Attacker.	A hardware cryptographic device is stolen.
		An OTP device is stolen.
		A look-up secret authenticator is stolen.
		A cell phone is stolen.

- *Qualcosa che "*CONOSCI*" potrebbe essere divulgato a un malintenzionato.*
  L'attaccante potrebbe indovinare un segreto memorizzato.
  Se l'autenticatore è un segreto condiviso, l'autore dell'attacco potrebbe ottenere l'accesso al CSP o al verificatore e ottenere il valore del segreto o eseguire un attacco del dizionario su un hash di tale valore.
  Un malintenzionato può osservare l'immissione di un PIN o di un codice di accesso, trovare una registrazione scritta o una voce di registro di un codice di accesso, un codice di accesso, installare del software malevolo (ad esempio, un registratore di tastiera) per acquisire il segreto.
  Inoltre, un utente malintenzionato può determinare il segreto tramite attacchi offline su un database di password gestito dal verificatore.
- *Qualcosa che "*POSSIEDI*" potrebbe essere perso, danneggiato, rubato al proprietario o clonato da un malintenzionato.*
  Ad esempio, un malintenzionato che ottiene l'accesso al computer del proprietario potrebbe copiare un autenticatore software.
  Un autenticatore hardware potrebbe essere rubato, manomesso o duplicato.
  I segreti Out-of-Band possono essere intercettati da un malintenzionato e utilizzati per autenticare la propria sessione.
- *Qualcosa che "*SEI*" potrebbe essere replicato.*
  Ad esempio, un utente malintenzionato può ottenere una copia del l'impronta digitale del sottoscrittore e costruire una replica.

Nella tabella seguente è elencata solo la parte iniziale delle minacce all'autenticatore per l'autenticazione digitale; la tabella completa è nel capitolo 8.1 del NIST SP 800-63B.

THREAT MITIGATION STRATEGIES

TABLE 7-1 ENROLLMENT AND IDENTITY PROOFING THREATS

La tabella 7-1 (vedi NIST SP 800-63A) elenca le strategie per mitigare le minacce al processo di iscrizione e rilascio.

Le minacce di registrazione possono essere scoraggiate rendendo più difficile la rappresentazione o aumentando la probabilità di rilevamento.

Questa raccomandazione riguarda principalmente i metodi per rendere più difficile rappresentazione; tuttavia, prescrive alcuni metodi e procedure che possono aiutare dimostrare chi ha perpetrato rappresentazione.

Ad ogni livello, vengono impiegati metodi per determinare che esiste una persona con l'identità dichiarata, che il richiedente è persona avente diritto all'identità dichiarata e che il richiedente non può in seguito ripudiare l'iscrizione.

Con l'aumentare del livello di sicurezza, i metodi impiegati forniscono una crescente resistenza all'imitazione casuale, sistematica e dall'interno.

Activity	Threat/Attack	Mitigation Strategy
Enrollment	Falsified identity proofing evidence	CSP validates physical security features of presented evidence.
		CSP validates personal details in the evidence with the issuer or other authoritative source.
	Fraudulent use of another's identity	CSP verifies identity evidence and biometric of applicant against information obtained from issuer or other authoritative source.
		Verify applicant-provided non-government-issued documentation (e.g., electricity bills in the name of the applicant with the current address of the applicant printed on the bill, or a credit card bill) to help achieve a higher level of confidence in the applicant's identity.
	Enrollment repudiation	CSP saves a subscriber's biometric.

la

a una

la

TABLE 8-2 MITIGATING AUTHENTICATOR THREATS

I meccanismi correlati che aiutano a mitigare le minacce identificate sopra sono riassunti nella Tabella 8-2 qui accanto.

Nella tabella è elencata solo la parte iniziale delle azioni necessarie a mitigare le minacce; la tabella completa è nel capitolo 8.2 del NIST 800-63B.

Authenticator Threat/Attack	Threat Mitigation
Theft	Use multi-factor authenticators that need to be activated through a memorized secret or biometric.
	Use a combination of authenticators that includes a memorized secret or biometric.
Duplication	Use authenticators from which it is difficult to extract and duplicate long-term authentication secrets.
Eavesdropping	Ensure the security of the endpoint, especially with respect to freedom from malware such as key loggers, prior to use.
	Avoid use of non-trusted wireless networks as unencrypted secondary out-of-band authentication channels.

SP

Diverse altre strategie possono essere applicate per mitigare le minacce descritte nella Tabella 8-1:

- *Molteplici fattori rendono più difficili da realizzare gli attacchi riusciti. Se un utente malintenzionato deve rubare un autenticatore crittografico e indovinare un segreto memorizzato, il lavoro per scoprire entrambi i fattori potrebbe essere troppo elevato.*
- *Possono essere impiegati meccanismi di sicurezza fisica per proteggere un autenticatore rubato dalla duplicazione. I meccanismi di sicurezza fisica possono fornire prove di manomissione, rilevamento e risposta.*
- *Richiedere l'uso di segreti memorizzati a lungo che non compaiono nei dizionari comuni può costringere gli aggressori a provare ogni possibile valore.*
- *È possibile utilizzare controlli di sicurezza del sistema e della rete per impedire a un utente malintenzionato di accedere a un sistema o installare software dannoso.*
- *La formazione periodica può essere eseguita per garantire che gli abbonati comprendano quando e come segnalare una compromissione — o sospetto di compromissione — o in altro modo riconoscere modelli di comportamento che potrebbero indicare che un utente malintenzionato sta tentando di compromettere il processo di autenticazione.*
- *È possibile utilizzare tecniche fuori banda per verificare la prova del possesso di dispositivi registrati (ad es. telefoni cellulari).*

AUTHENTICATOR RECOVERY

Il punto debole in molti meccanismi di autenticazione è il processo seguito quando un sottoscrittore perde il controllo di uno o più autenticatori e deve sostituirli.

In molti casi, le opzioni disponibili per autenticare il sottoscrittore sono limitate e le preoccupazioni economiche (ad esempio, i costi di mantenimento dei call center) motivano l'uso di metodi di autenticazione di backup poco costosi e spesso meno sicuri.

Nella misura in cui il ripristino dell'autenticatore è assistito dall'uomo, esiste anche il rischio di attacchi di ingegneria sociale.

Per mantenere l'integrità dei fattori di autenticazione, è essenziale che non sia possibile sfruttare un'autenticazione che coinvolge un fattore per ottenere un autenticatore di un fattore diverso. Ad esempio, un segreto memorizzato non deve essere utilizzabile per ottenere un nuovo elenco di segreti di ricerca.

SESSION ATTACKS

Gli attacchi di dirottamento alla sessione a seguito di un evento di autenticazione possono avere impatti sulla sicurezza.

Le linee guida per la gestione della sessione, indicate in precedenza, sono essenziali per mantenere l'integrità della sessione contro gli attacchi, come XSS *(*CROSS-SITE SCRIPTING*).*

Un'altra minaccia post-autenticazione, la falsificazione delle richieste tra siti (CROSS-SITE REQUEST FORGERY - CSRF*), sfrutta le tendenza ad avere più sessioni attive contemporaneamente.*

È importante incorporare e verificare un identificatore di sessione nelle richieste Web per impedire che un URL o una richiesta validi vengano attivati involontariamente o in modo dannoso.

PARTE XIX: TECNOLOGIA 5G

107. SCOPO DEL 5G

[Fonte: GSMA – Securing the 5G Era]

Scopo del 5G è quello di aprire la rete a un insieme più ampio di servizi e consentire agli operatori mobili di sostenere questi servizi.

È un'opportunità per proteggere i servizi e i consumatori da molte delle minacce odierne.

Il 5G viene fornito con molti controlli di sicurezza integrati in base alla progettazione, sviluppati per migliorare la protezione sia dei singoli consumatori sia delle reti mobili.

Il progresso della tecnologia e l'uso di nuove architetture e funzionalità come lo slicing della rete, la virtualizzazione e il cloud introdurranno nuove minacce che richiedono l'implementazione di nuovi tipi di controlli.

Questa generazione di sistema di telecomunicazioni mira a fornire:

1) *Banda larga mobile potenziata,*
2) *Massive comunicazioni di tipo macchina,*
3) *Comunicazioni ultra affidabili e a bassa latenza.*

L'obiettivo è:

- ✓ *essere più veloci;*
- ✓ *essere più affidabili;*
- ✓ *gestire la scala dei dispositivi prevista per l'Internet delle cose Mobile (MIoT);*
- ✓ *consentire la trasformazione digitale della nostra società, dei processi aziendali e della produzione.*

Per consentire ciò, il 5G fornirà:

1) *slicing (porzioni o parti) multi-rete,*
2) *multi-livello di servizi e*
3) *capacità di rete multi-connettività.*

Per consentire la flessibilità, l'agilità e le economie di scala richieste, queste tecnologie saranno fornite tramite ambienti virtuali e containerizzati. ***Questo è un modo rivoluzionario di lavorare per l'industria****.*

Il 5G ha progettato controlli di sicurezza per sostenere molte delle minacce affrontate nelle odierne reti 4G/3G/2G.

Questi controlli includono nuove funzionalità di autenticazione reciproca, protezione avanzata dell'identità dell'abbonato e meccanismi di sicurezza aggiuntivi.

Il 5G offre al settore mobile un'opportunità senza precedenti per elevare i livelli di sicurezza della rete e del servizio.

Il 5G fornisce misure preventive per limitare l'impatto sulle minacce note, ma l'adozione di nuove tecnologie di rete introduce potenziali nuove minacce da gestire per il settore.

Questo articolo discute diversi controlli di sicurezza dell'era 5G, comprese le loro limitazioni, per questo motivo è richiesto un certo livello di conoscenza tecnica.

108. INTRODUZIONE

Alcuni aspetti della protezione dei componenti 5G e dell'utilizzo mancano di standard e linee guida, rendendo più difficile per gli operatori e gli utenti della rete 5G sapere cosa deve essere fatto e come può essere realizzato.

Questo documento, sulla sicurezza informatica, descrive come una combinazione di funzionalità di sicurezza 5G e di controlli di sicurezza di terze parti possa essere utilizzata per implementare le capacità di sicurezza di cui le organizzazioni hanno bisogno per salvaguardare l'utilizzo della rete 5G.

Inoltre, cercherà anche di identificare le lacune negli standard di sicurezza informatica 5G che dovrebbero essere affrontate.

Questa bozza preliminare spiega perché stiamo costruendo la soluzione di esempio per affrontare le sfide della sicurezza informatica 5G, inclusa l'analisi del rischio da eseguire e le capacità di sicurezza che la soluzione di esempio consentirà e dimostrerà.

L'attuale sviluppo degli standard di sicurezza informatica 5G si concentra principalmente sulla sicurezza delle interfacce interoperabili basate su standard tra i componenti 5G.

Gli standard 5G non specificano le protezioni di sicurezza informatica da implementare sui componenti informatici (IT) sottostanti che supportano e gestiscono il sistema 5G.

Questa mancanza di informazioni aumenta la complessità per le organizzazioni che intendono sfruttare il 5G.

Con l'architettura 5G basata sulla tecnologia cloud, i sistemi 5G potrebbero potenzialmente sfruttare le solide funzionalità di sicurezza disponibili nelle architetture di cloud computing per proteggere i dati e le comunicazioni 5G.

*Secondo GSMA, per assicurare la progettazione dovrebbero essere sviluppati degli standard che adottino i principi "**SECURE BY DESIGN**", che portano a:*

- *Uso dell'autenticazione reciproca*

Confermando che mittente e destinatario abbiano una fiducia reciproca stabilita e la relazione end-to-end sia protetta.

- *Una presunta rete "aperta".*

Rimozione di qualsiasi presupposto di sicurezza da prodotti o processi sovrapposti.

- *Un riconoscimento che tutti i collegamenti potrebbero essere sfruttati.*

Imporre la crittografia del traffico inter/intra-rete, assicurando che le informazioni crittografate siano inutili quando vengono intercettate.

Sebbene questa sia una pratica comune nelle soluzioni per altri servizi, come l'on-line banking, si tratta di un importante cambiamento di paradigma rispetto alle pratiche di telecomunicazioni mobili esistenti. Di conseguenza, le reti 5G dovrebbero offrire al consumatore una protezione maggiore rispetto alle reti 4G/3G/2G esistenti.

109. INTERESSATI

Questo volume è destinato ai gestori di tecnologia, sicurezza e privacy che si occupano di come identificare, comprendere, valutare e mitigare i rischi per le reti 5G.

Le informazioni si rivolgono a tre tipi di organizzazioni.

1) *OPERATORI DI RETE MOBILE COMMERCIALE*

   La trattazione fornirà loro una migliore comprensione delle funzionalità di sicurezza cloud che sono già disponibili nei sistemi forniti dai fornitori.

   Queste funzionalità di sicurezza abilitate all'hardware vanno oltre ciò che gli standard 5G attualmente specificano e possono fornire una protezione complementare in questo momento.

   Questo è sempre più importante man mano che le operazioni si spostano su piattaforme e software di base e poiché la tecnologia di rete mobile si fonde con l'IT.

2) *POTENZIALI OPERATORI DI RETE 5G PRIVATI*

   Le reti private 5G dovrebbero diventare una realtà, come nelle università e nelle grandi aziende.

   Qualsiasi organizzazione che consideri l'implementazione e la gestione della propria rete 5G dovrà gestire la propria sicurezza utilizzando un approccio basato sul rischio.

   Il volume spiegherà una gamma di funzionalità di sicurezza e i rischi che ciascuna funzionalità aiuta a mitigare, fornendo informazioni preziose ai fini della gestione dei rischi delle organizzazioni.

3) *ORGANIZZAZIONI CHE UTILIZZANO E GESTISCONO LA TECNOLOGIA ABILITATA AL 5G*

   Prima che le organizzazioni adottino tecnologie abilitate al 5G, dovrebbero prendere decisioni sulla gestione dei rischi per la sicurezza informatica in merito al loro utilizzo, gestione e manutenzione.

   Le informazioni contenute nel volume dovrebbero aiutare a informare tali decisioni.

   Questo volume può essere utile per i partecipanti agli sforzi relativi agli standard relativi al 5G (ad esempio, da organizzazioni che sviluppano standard) che desiderano identificare le lacune negli standard per informare il loro lavoro futuro.

   Anche i ricercatori sulla sicurezza informatica che vogliono costruire banchi di prova per la ricerca sulla sicurezza informatica 5G potrebbero trovare utile questo volume come riferimento.

110. MODELLI DI IMPIEGO 5G

[Fonte: GSMA – Securing the 5G Era]

Gli standard 5G descrivono una serie di modelli di implementazione.

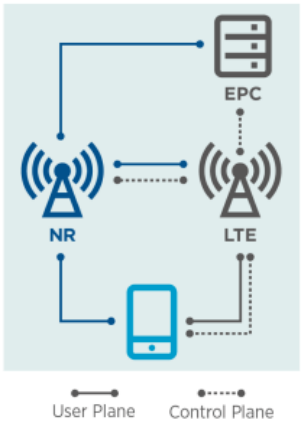
Sebbene ci siano piani per implementare almeno 5 opzioni aggiuntive in futuro, l'unica opzione attualmente implementata è la cosiddetta modalità non standalone (non-standalone (NSA) mode), più precisamente denominata EN-DC.

È qui che le stazioni base 5G sono integrate con una rete 4G esistente che lavora in tandem con stazioni base LTE e collegate al core LTE, basandosi sulle misure e sulle protezioni fornite dal core LTE.

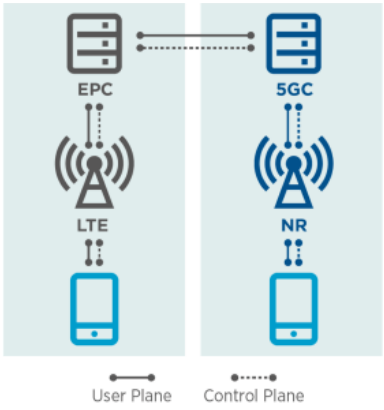
La prossima fase dell'implementazione del 5G sarà probabilmente la modalità Stand Alone (Stand Alone [SA] mode), più precisamente SA NR, costituita da una nuova rete radio 5G (NR) connessa a una rete principale 5G (5GC).

Il passaggio a un Core 5G consentirà di realizzare tutte le funzionalità di sicurezza delle specifiche 5G.

Sebbene sia riconosciuto che i nuovi paradigmi (architettura nativa del cloud, basata sui servizi) introdurranno nuove sfide per la sicurezza.



NON-STANDALONE (NSA) DEPLOYMENT



STANDALONE (SA) DEPLOYMENT

**77% degli operatori intervistati prevede di implementare SA 5G entro i prossimi tre anni (Fonte: GSMAi, 2019*)

111. PROTEZIONE DELL'ABBONATO E DEL SERVIZIO

[Fonte: GSMA – Securing the 5G Era]

Il 5G migliora la riservatezza e l'integrità dei dati di utenti e dispositivi.

A differenza delle precedenti generazioni di sistemi mobili 5G:

- *Protegge la riservatezza dei messaggi NAS (Non Access Stratum) tra il dispositivo e la rete. Di conseguenza, non è più possibile tracciare le apparecchiature utente (User Equipment [UE]) utilizzando le attuali metodologie di attacco sull'interfaccia radio; protezione contro gli attacchi di Man In The Middle (MITM) e false stazioni base (Stingray/IMSI catcher).*
- *Introduce un meccanismo di protezione chiamato* ***Home Control****. Ciò significa che l'autenticazione finale del dispositivo su una rete visitata viene completata dopo che la rete domestica ha verificato lo stato di autenticazione del dispositivo nella rete visitata. Questo miglioramento preverrà vari tipi di frode in roaming che hanno ostacolato storicamente gli operatori e supporterà il requisito dell'operatore di autenticare correttamente i dispositivi ai servizi.*
- *Supporta l'autenticazione unificata su altri tipi di rete di accesso, ad es. WLAN, che consente alle reti 5G di gestire connessioni precedentemente non gestite e non protette. Ciò include la possibilità di eseguire una riautenticazione dell'UE quando si sposta tra diverse reti di accesso o di servizio.*
- *Introduce il controllo dell'integrità del piano utente, assicurando che il traffico utente non sia modificato durante il transito.*
- *Migliora la protezione della privacy con l'uso di coppie di chiavi pubbliche/private (chiavi di ancoraggio) per nascondere l'identità dell'abbonato e derivare le chiavi utilizzate nell'architettura del servizio.*

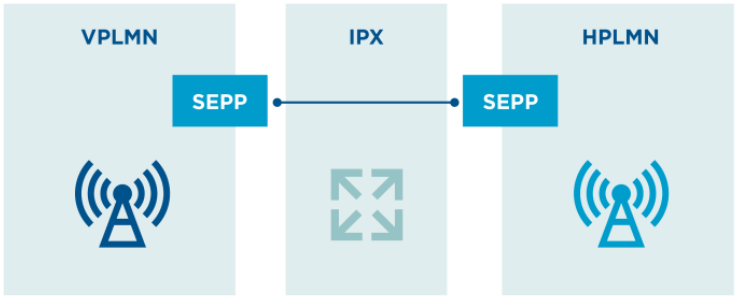
112. PROTEZIONE DELLA RETE

[Fonte: GSMA – Securing the 5G Era]

INTEGRITÀ DEI DATI DI SEGNALAZIONE

Il 5G introduce un nuovo elemento dell'architettura di rete: il SECURITY EDGE PROTECTION 0PROXY (SEPP).

Il SEPP protegge il perimetro della rete domestica, fungendo da gateway di sicurezza sulle interconnessioni tra la rete domestica e le reti visitate.



Il SEPP è progettato per:

1. *fornire sicurezza a livello di applicazione e protezione da intercettazioni e attacchi di riproduzione;*
2. *fornire autenticazione end-to-end, integrità e protezione della riservatezza tramite firme e crittografia di tutti i messaggi in roaming HTTP/2;*
3. *offrire meccanismi di gestione delle chiavi per impostare le chiavi crittografiche richieste ed eseguire le procedure di negoziazione delle capacità di sicurezza;*
4. *eseguire il filtraggio e il controllo dei messaggi, l'occultamento della topologia e la convalida degli oggetti JSON; compreso il controllo delle informazioni su più livelli con le informazioni sull'indirizzo sul livello IP.*

Inoltre, è stata introdotta una maggiore sicurezza dei servizi di roaming internazionale per superare i rischi per la sicurezza esistenti legati all'utilizzo di SS7 e Diameter.

113. NUOVO STACK DI PROTOCOLLO IT

[Fonte: GSMA – Securing the 5G Era]

Storicamente le reti degli operatori hanno utilizzato principalmente protocolli proprietari per la gestione della rete.

5GC passa a uno stack di protocollo basato su IP, consentendo l'interoperabilità con un numero più ampio di servizi e tecnologie in futuro.

I seguenti protocolli, schemi e processi saranno adottati in 5GC:

- *HTTP/2 su N32, sostituendo Diameter dal punto di riferimento S6a;*
- *TLS come ulteriore livello di protezione che fornisce comunicazioni crittografate tra tutte le funzioni di rete (NF) all'interno di una rete mobile pubblica terrestre (PUBLIC LAND MOBILE NETWORK [PLMN]);*
- *TCP come protocollo del livello di trasporto in sostituzione del SCTP.*
- *Framework RESTful con OpenAPI 3.0.0 come Interface Definition Language (IDL)*

Poiché questi protocolli sono utilizzati nel più ampio settore IT, è probabile che il loro utilizzo:

- *porti a una breve vulnerabilità alla sequenza temporale di sfruttamento e a un maggiore impatto delle vulnerabilità che si trovano all'interno di questi protocolli;*

- *ampli il potenziale pool di attaccanti; le reti core 4G e in particolare 3G traggono vantaggio dal fatto che gli aggressori abbiano poca esperienza con gli standard di proprietà utilizzati al loro interno.*

Gli schemi di segnalazione delle vulnerabilità, come il programma GSMA Coordinated Vulnerability Disclosure (CVD) programme, dovranno gestire l'ampliamento della portata di questi protocolli.

Una volta individuato, il tempo necessario per correggere le vulnerabilità rilevanti dovrebbe essere breve.

114. TECNOLOGIE VANTAGGIATE DAL 5G

[Fonte: GSMA – Securing the 5G Era]

VIRTUALIZZAZIONE

L'architettura di rete 5GC sarà basata sui servizi, il che significa che le operazioni della rete centrale possono essere eseguite tramite funzioni esterne alla rete dell'operatore, ad es. la nuvola (Cloud).

Questo è un importante cambiamento rispetto ai controlli di sicurezza della rete di base consolidati, tuttavia offre all'operatore l'opportunità di sfruttare le tecnologie di virtualizzazione.

Con questa opportunità arrivano nuovi vettori di minaccia con cui confrontarsi.

Dovrebbero essere presi in considerazione i tradizionali controlli della virtualizzazione, compreso l'isolamento del tenant e delle risorse.

Controlli di isolamento adeguati riducono il rischio di fuga di dati e l'impatto delle epidemie di malware consapevoli della virtualizzazione.

Vulnerabilità a livello di microprocessore hanno evidenziato che l'isolamento della locazione all'interno di un ambiente virtuale non è garantito, poiché tali inquilini dovrebbero essere alloggiati insieme in base ai requisiti di sicurezza, ad es. non ospitare inquilini di sicurezza di livello inferiore con quelli di sicurezza di alto livello.

La containerizzazione è una tecnologia di virtualizzazione a livello di sistema operativo che sta prendendo piede.

Il sistema operativo host limita l'accesso del container alle risorse fisiche, come CPU, storage e memoria, in modo che un singolo container non possa consumare tutte le risorse fisiche di un host. Riducendo così l'impatto degli attacchi alla disponibilità contro la piattaforma.

Tutte le tecnologie di virtualizzazione consentono la segmentazione della rete e l'isolamento delle risorse, garantendo la sicurezza e riducendo l'impatto di attacchi riusciti.

SERVIZI CLOUD

Basandosi su servizi virtualizzati, il cloud è un abilitatore chiave del 5G; l'architettura 5G è stata progettata per essere nativa del cloud in quanto offre elasticità e scalabilità.

L'uso della tecnologia cloud può complicare la catena di approvvigionamento e la catena di responsabilità.

È necessario seguire pratiche di codifica sicura per garantire che i dati non vengano trapelati e che il codice non possa essere utilizzato per sfruttare il provider di servizi cloud o la rete dell'operatore.

SEZIONAMENTO DELLA RETE

Lo slicing della rete consente all'operatore di personalizzarne il suo comportamento, adattando (slicing) la rete per servire casi d'uso specifici utilizzando lo stesso hardware.

È possibile prevedere diversi livelli di isolamento che vanno da un singolo nodo della rete centrale all'accesso radio completamente dedicato.

Ciascun tipo di isolamento deve essere integrato in fase di progettazione. Ad esempio, una fetta di rete per la chirurgia remota deve considerare la costante identificazione e autorizzazione reciproca per bloccare le minacce

MITM (MAN IN THE MIDDLE), ma una fetta per la gestione dei contenuti AR/VR non richiederà lo stesso livello di sicurezza.

MOBILE IOT

Sebbene l'IoT sia già prevalente nelle reti 2G/3G/4G, il numero di connessioni IoT aumenterà esponenzialmente nel 5G.

Più grande non significa che i controlli di sicurezza debbano cambiare in modo significativo, tuttavia devono essere ridimensionati.

L'IoT deve essere codificato, distribuito e gestito in modo sicuro durante tutto il suo ciclo di vita.

La maggior parte dei servizi IoT condivide un'architettura comune e, in quanto tale, gli attacchi a cui sarà sottoposto ciascun servizio probabilmente rientreranno in tre scenari di attacco comuni:

1. *attacchi ai dispositivi (endpoint) tramite le applicazioni in esecuzione sul dispositivo, attacchi remoti da Internet e tramite attacco fisico;*
2. *attacchi alle piattaforme di servizio (es. cloud);*
3. *attacchi ai collegamenti di comunicazione (es. Cellular, WLAN, BLE air interface ecc.).*

ARTIFICIAL INTELLIGENCE (AI)

L'IA dovrebbe essere ampiamente utilizzata nelle reti 5G e dovrebbe favorire la sicurezza.

Gli operatori dovrebbero sfruttare Machine Learning (ML) e Deep Learning (DL) per automatizzare il rilevamento di minacce e frodi.

L'uso dell'IA è particolarmente rilevante se si considerano i volumi di dati che le reti 5G genereranno.

L'IA potrebbe essere un modo più fattibile per mitigare i precedenti attacchi sconosciuti in tempo reale e può anche essere utilizzata per alimentare reti di autoriparazione in cui il sistema è in grado di identificare i problemi e intraprendere azioni automatizzate per fornire la soluzione.

Tuttavia, questa tecnologia è disponibile anche per l'attaccante e sono previsti attacchi basati sull'IA.

115. DESCRIZIONE/COMPONENTI DELL'ARCHITETTURA DEL SISTEMA DI RIFERIMENTO

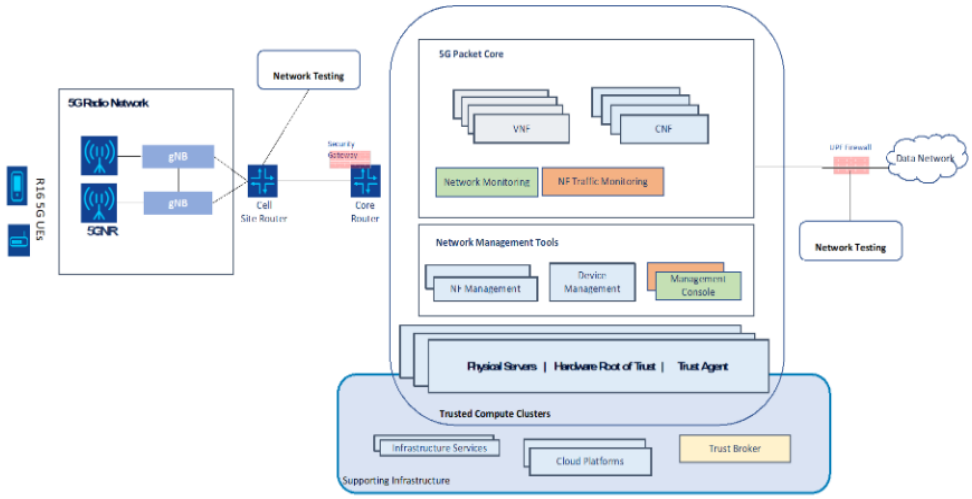
Questa sezione:

- *presenta i diagrammi preliminari dell'architettura per la progettazione del sistema, inclusi i diagrammi logici e fisici;*
- *spiega i componenti principali dell'architettura e riassume lo scopo delle interazioni dei componenti;*
- *inizia con l'architettura di implementazione 5G di alto livello e approfondisce le architetture della soluzione di sicurezza proposta.*
- *spiega le idee di base dell'architettura e non fornisce dettagli esaurienti di ogni componente dell'architettura e delle sue implicazioni sulla sicurezza ma saranno descritte nelle sezioni successive di questo volume e ne discutono le capacità di sicurezza dei componenti in modo più dettagliato.*

HIGH LEVEL ARCHITECTURE

La Figura 3-1 illustra l'architettura di alto livello dell'implementazione NCCoE 5G.

Figure 3-1 High-Level Architecture



Sul lato sinistro del diagramma c'è la rete d'accesso radio 5G.

*È costituito da apparecchiature utente (ovvero dispositivi mobili che utilizzano la rete 5G); radio e antenne; unità in banda base (*BASEBAND UNITS [BBU]*) note come* GNODEB (GNB)*, che generano segnali RF.*

A destra della rete di accesso radio, il diagramma mostra la rete di BACK HAUL*, la connessione tra la rete di accesso radio (cells site) e la rete centrale (data center).*

Il router del sito cellulare e il router principale denotano le due estremità della rete di Back Haul nella nostra implementazione di riferimento.

La terminazione della rete di Back Haul è un gateway di sicurezza opzionale, rappresentato come un firewall. Questo firewall fornisce un tunnel IPsec per proteggere la segnalazione e le comunicazioni del piano utente tra la rete di accesso radio e il core del pacchetto 5G.

Il data center, rappresentato al centro, ospita vari componenti che controllano e gestiscono la rete.

Il core del pacchetto 5G è costituito da numerose funzioni di rete 5G con varie responsabilità (ad es. autenticazione, mobilità, ricarica).

I protocolli e le funzioni del pacchetto core sono specificati negli standard 3GPP*.*

Il data center fornisce anche i servizi di base necessari per la configurazione, la gestione e la manutenzione di tutti i componenti di rete. Ciò include sia i servizi di infrastruttura (ad es. NETWORK *FILE SYSTEM [NFS],* FILE TRANSFER PROTOCOL *[FTP],* NETWORK TIME PROTOCOL *[NTP],* DOMAIN NAME SYSTEM *[DNS]) sia gli strumenti di gestione.*

Infine, il lato destro del diagramma mostra un firewall che collega il data center alla rete dati. Questo firewall protegge le funzioni di rete all'interno della rete centrale nel centro dati dagli attacchi basati su IP (Internet Protocol) provenienti da Internet. Inoltre, il firewall fornisce la topologia nascosta per gli indirizzi IP, quindi non sono direttamente accessibili da Internet.

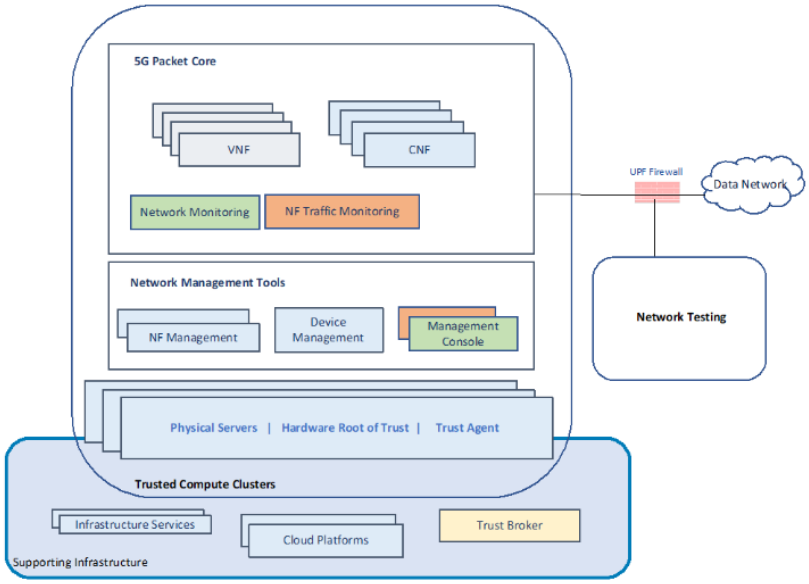
I nodi di test di rete mostrati nella Figura 3-1 consentono la convalida end-to-end dell'infrastruttura, dei servizi e della sicurezza convergenti wireless e cablata. Ad esempio, l'infrastruttura può essere sollecitata utilizzando connessioni simultanee di dati, video o voce osservando la velocità di connessione e il throughput degli utenti simulati.

Un nodo di test può fornire diversi tipi di traffico: legittimo, DDOS *(*DISTRIBUTED DENIAL OF SERVICE*) e malware. Può simulare protocolli applicativi del mondo reale e consente la personalizzazione e la manipolazione dei dati grezzi.*

DATA CENTER ARCHITECTURE

La Figura 3-2 fornisce una vista più dettagliata dell'architettura del data center specifica per l'implementazione 5G.

FIGURE 3-2 DATA CENTER ARCHITECTURE



Altre reti 5G potrebbero abilitare le stesse funzionalità descritte di seguito in un'architettura diversa o con tecnologie diverse.

Nella nostra soluzione proposta, il data center distribuisce tutte le funzioni di rete core a pacchetto 5G (NETWORK FUNCTION [NF]) come NF basate su macchine virtuali (VIRTUAL MACHINE BASED [VNF]) o NF basate su container (CONTAINER BASED [CNF]) utilizzando tecnologie di cloud computing.

Le piattaforme di calcolo che ospitano queste NF sono cluster di server con processori dei prodotti.

Il data center supporta e fornisce anche la connettività per gli strumenti e i prodotti utilizzati per fornire visibilità e controllo della sicurezza nel traffico di rete.

Questo è importante per il monitoraggio e l'applicazione sia dell'infrastruttura IT di supporto che dell'applicazione e del traffico di segnalazione che attraversa il sistema 5G.

Il data center utilizza più set di strumenti, servizi e piattaforme di cloud computing per abilitare la funzionalità dei carichi di lavoro di cui è responsabile per l'hosting.

Questa infrastruttura IT di supporto è mostrata nell'area "Supporting Infrastructure & Services" nella parte inferiore del diagramma.

Questi tipi di componenti sono spesso ignorati quando si parla di sistemi 5G, ma sono fondamentali per la sicurezza e le operazioni.

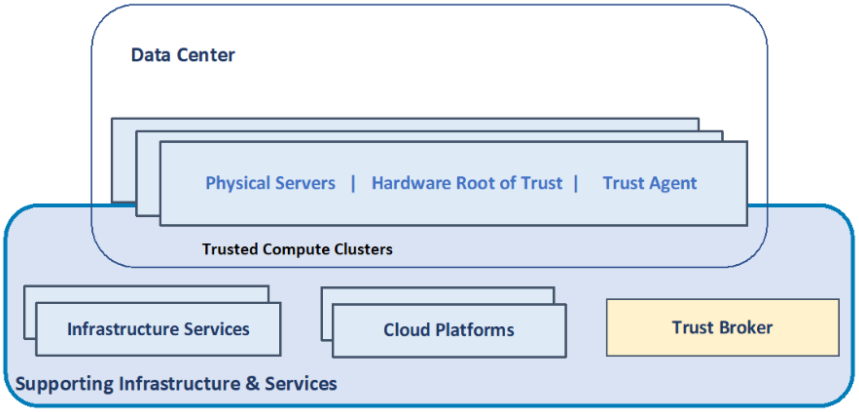
Questa infrastruttura IT è simile a quella utilizzata per le implementazioni di cloud computing e contiene le funzionalità di sicurezza descritte in questo documento.

Tutte le funzioni IT di supporto necessarie (servizi di directory, autorità di certificazione, file server, workstation di manutenzione, time server, servizi di backup e ripristino, ecc.) sono incluse nella "Service Box" di infrastruttura.

TRUSTED COMPUTE CLUSTER ARCHITECTURE

La Figura 3-3 illustra il sottoinsieme dell'ambiente di elaborazione fisico all'interno dell'architettura del data center 5G chiamato Trusted Compute Clusters. Questo nome indica che i server dispongono di funzionalità di root di attendibilità hardware abilitate.

FIGURE 3-3 TRUSTED COMPUTE CLUSTER ARCHITECTURE



Un server con HARDWARE ROOT OF TRUST (HROT) accoppiato con un hypervisor abilitato o un sistema operativo e un container runtime costituiscono la base per una piattaforma di elaborazione più sicura.

Questa piattaforma sicura:

1. *misura l'integrità del firmware, del sistema operativo (OS) e del gestore della macchina virtuale (Virtual Machine Manager [VMM]) all'avvio;*
2. *previene i rootkit o altri attacchi di basso livello,*
3. *stabilisce l'affidabilità del software del server e delle piattaforme host.*

Uno o più Trusted Compute Cluster possono essere utilizzati come base di elaborazione che ospiterà i carichi di lavoro delle funzioni di rete 5G come VNF o CNF.

Gli HRoT abilitano capacità di sicurezza aggiuntive per l'infrastruttura che supporta il 5G oltre a quanto definito nelle specifiche 3GPP.

Queste funzionalità includono controlli basati su hardware per:

1. *misurare l'integrità della piattaforma per ciascun server nell'infrastruttura;*
2. *assegnare etichette specifiche per ciascun server nell'infrastruttura per imporre l'isolamento dei carichi di lavoro critici;*
3. *attestare la misurazione e l'etichetta di ciascun server rispetto alle politiche, inserendo i risultati in un agente di orchestrazione delle politiche per segnalare, avvisare o applicare regole in base agli eventi.*

Queste funzionalità sono abilitate da più componenti nel diagramma, tra cui:

1. *meccanismi hardware per misurare crittograficamente i moduli hardware e firmware che compongono ciascun server;*
2. *un modulo di sicurezza hardware per memorizzare le misure crittografiche su ciascun server;*
3. *un meccanismo su ciascun server in grado di comunicare con il modulo di sicurezza hardware integrato e di riportare le misurazioni a un Trust Broker, abilitato dal sistema operativo o da software di terze parti;*
4. *un server di attestazione remoto, o Trust Broker, che raccoglie le misurazioni dei server nei Trusted Compute Clusters, assegna etichette a ciascun server e si integra con gli scheduler del carico di lavoro dei Trusted Compute Clusters.*

Questi componenti sono integrati insieme in modo che i carichi di lavoro 5G siano distribuiti su hardware affidabile designato per funzionalità specifiche.

Le tecnologie HRoT per gli scheduler del carico di lavoro utilizzano le misurazioni e le etichette della piattaforma come fattore di posizionamento del carico di lavoro.

Le funzionalità descritte in questa sezione si basano sulle tecniche descritte in NIST IR 8320, Hardware Enabled Security: Abilitazione di un approccio a più livelli alla sicurezza della piattaforma per casi d'uso di cloud ed edge computing.

Implementazioni di prototipi specifici per l'attestazione remota e la pianificazione e il posizionamento del carico di lavoro sono disponibili in NIST IR 8320A e NIST IR 8320B.

116. RISK ASSESSMENT

Questa sezione è preliminare e ancora in fase di sviluppo e cataloga le capacità di sicurezza tecnica incluse in questo progetto.

Successivamente, sono discusse le minacce e le vulnerabilità che ciascuna delle funzionalità di sicurezza tecnica intende affrontare.

Una volta completata, questa sezione fornirà un'analisi del rischio per l'architettura di riferimento e le sue funzioni e capacità di supporto.

Queste informazioni potrebbero essere utilizzate da un'organizzazione per informare la propria analisi del rischio e il processo decisionale in merito a come rispondere a ciascun rischio (ad esempio mitigare, accettare, trasferire, evitare).

SECURITY CATEGORY

Le categorie di sicurezza, descritte nella tabella 3-1, sono descrizioni di alto livello utilizzate per catalogare le capacità di sicurezza tecnica presa in considerazione da questa implementazione.

Queste categorie sono importanti e rilevanti per le reti 5G sia commerciali che private e includono sia le funzionalità di sicurezza definite dagli standard 3GPP, sia le capacità di sicurezza disponibili nell'infrastruttura cloud di supporto della rete.

TABLE 3-1 SECURITY CATEGORIES

Security Category	Reference
Infrastructure Security Category (ISC)	
Hardware Roots of Trust Packet Core	ISC-1
Hardware Roots of Trust Virtualized RAN	ISC-2
Infrastructure Recommended Practice	ISC-3
5G Standalone Security Category (5GSC)	
Subscriber Privacy	5GSC-1
Radio Network Security	5GSC-2
Authentication Enhancements	5GSC-3
Interworking & Roaming Security	5GSC-4
API Security	5GSC-5
Network Slicing Security	5GSC-6
Application Security	5GSC-7
Internet Security Protocol Recommended Practice	5GSC-8

SECURITY CAPABILITIES

Il termine capacità di sicurezza è utilizzato per descrivere una caratteristica di sicurezza tecnica importante e rilevante per le reti 5G commerciali o private.

Le funzionalità di sicurezza, descritte nella Tabella 3-2, nel contesto di questo documento includono sia le funzionalità di sicurezza definite dagli standard 3GPP sia le funzionalità di sicurezza disponibili nell'infrastruttura cloud di supporto della rete.

Per ciascuna capacità, la Tabella 3-2 elenca il suo identificatore di sottoriferimento univoco e fornisce una breve descrizione, che spiega anche la capacità.

TABLE 3-2 SECURITY CAPABILITIES

Security Capability	Subreference	Description
Infrastructure Security Categories		
Hardware Roots of Trust Packet Core, ISC-1		
Hardware-Based Platform Measurement	ISC-1.1	Measure platform integrity for each server in the infrastructure using hardware-based controls.
Hardware-Based Labeling	ISC-1.2	Assign specific labels for each server in the infrastructure using hardware-based controls.
Remote Platform Attestation	ISC-1.3	Attest each server's trust measurements and asset tags against policies, and allow services like workload orchestrators access to these findings so the results can be used as factors in workload placement/migration.
Network Function Orchestration Enforcement	ISC-1.4	Deploy and migrate NFs to servers that match platform measurements and labels.
Network Function Image Encryption	ISC-1.5	Encrypt each NF's image, and release the decryption keys only to servers that meet trust policies.
Infrastructure Recommended Practice, ISC-3		
Infrastructure Security Monitoring	ISC-3.1	Provide the visibility across the infrastructure needed to continuously monitor communications patterns, see threats within the extended network, and detect and respond to threats using methods such as behavioral modeling and supervised and unsupervised machine learning.
Network Segmentation	ISC-3.2	Ensure that the infrastructure design and implementation support keeping the different types of network traffic separate from each other.
5G Standalone Security Categories		
Subscriber Privacy, 5GSC-1		
Subscription Permanent Identifier (SUPI) Protection	5GSC-1.1	Encrypt the 5G SUPI with the public key of the home operator to create the Subscription Concealed Identifier (SUCI).
Reallocation of Temporary IDs	5GSC-1.2	Refresh a user device's temporary ID after initial registration, on every mobility registration update, and after use in paging.
Initial NAS Message Security	5GSC-1.3	After the initial service request message, security sensitive messages are re-sent encrypted in a Non-Access Stratum (NAS) Container so sensitive UE-specific information is not sent in the clear.
No SUPI-Based Paging	5GSC-1.4	Use a temporary identifier (5G-S-TMSI) as the basis of paging timing, not a permanent identifier (SUPI).
Respond to Identity Request with SUCI	5GSC-1.5	The network can request SUPI, but the UE only responds with SUCI and never sends SUPI.
Radio Network Security, 5GSC-2		
User Plane Integrity Protection	5GSC-2.1	Apply integrity protection to user plane traffic over the air at the full data rate using 5G's new capabilities.
Cryptographic Algorithms Recommended Practice	5GSC-2.3	Use strong algorithms for the air interface based on US operator-recommended practices.
Authentication Enhancements, 5GSC-3		
Native Extensible Authentication Protocol (EAP) Support	5GSC-3.1	Use access-agnostic authentication via EAP Method for 3rd Generation Authentication (EAP-AKA') to enable mutual authentication between the UE and the network, and to provide keying material that can be used between the UE and the serving network and between the UE and the home network in subsequent security procedures. While EAP support is new in 5G, the evolution of LTE's authentication, referred to as 5G AKA, will also be evaluated. Special EAP configurations like EAP-Transport Layer Security (EAP-TLS) are of interest for future project phases.
Non-3GPP Access	5GSC-3.2	Maintain one security context in the 5G core network for access from both 3GPP networks and non-3GPP networks, e.g., wireless local area networks (WLANs).

Hardware-Based Credential Storage	5GSC-3.3	Store pre-shared keys and credentials in the USIM software container running on tamper-resistant hardware in UEs in either embedded or physical Universal Integrated Circuit Cards (UICCs), commonly referred to as Subscriber Identity Module (SIM) cards.
Security Anchor Function (SEAF)	5GSC-3.4	The Security Anchor Function (SEAF) is collocated with the Access and Mobility Management Function (AMF) to provide primary authentication. The SEAF plays an important role in authentication while roaming and for non-3GPP access.
API Security, 5GSC-5		
API Security for Network Exposure Function (NEF)	5GSC-5.1	Securely expose network services such as voice, data connectivity, charging, and subscriber information to trusted (internal) and untrusted (third-party) applications over application programming interfaces (APIs), with standards defined and recommended practices for API security applied according to security profiles for Transport Layer Security (TLS) implementation and usage following the provisions given in clause 6.2 of 3GPP Technical Specification (TS) 33.210 [1].
Application Security, 5GSC-7		
Subscriber Traffic Security Monitoring	5GSC-7.1	Have complete visibility across the control and user planes. Correlate between UE traffic and permanent equipment identifiers (PEIs) and SUPIs.
User-Plane Security Enforcement	5GSC-7.2	Enforce authorized access for 5G implementing segmentation policies based on SUPI/PEI, Network Slice, Applications, and data. Provide inline network security protections for UE.
Internet Security Protocol Recommended Practice, 5GSC-8		
IPsec/NDS IP	5GSC-8.2	Protect communication between network entities/elements at the network layer via authentication and cryptographic secured Internet Protocol Security (IPsec) tunnels (e.g., communication within RAN, between RAN and core – backhaul, mid-haul and fronthaul and access from untrusted non-3GPP network to 5G core network).

MITIGATED THREATS AND VULNERABILITIES

Ciascuna funzionalità di sicurezza nella Tabella 3-2 ha lo scopo di aiutare a mitigare determinati tipi di minacce e vulnerabilità in modo da ridurre il rischio complessivo a un livello accettabile.

Questa sezione esplora le funzionalità di sicurezza in ordine e per ognuna, riassume le vulnerabilità e le minacce corrispondenti che aiuta ad affrontare e spiega brevemente come mitiga le minacce e le vulnerabilità.

INFRASTRUCTURE SECURITY

Hardware Roots of Trust Packet Core, ISC-1		
	Minaccia/Vulnerabilità	**Mitigazione**
ISC-1.1, misurazione della piattaforma basata su hardware	*Il BIOS (Basic Input/Output System) o il codice del firmware potrebbero essere alterati o sostituiti con codice dannoso dando a un utente malintenzionato il pieno controllo del sistema (ad esempio, un rootkit). Ulteriori componenti hardware possono essere aggiunti al sistema per consentire a utenti non autorizzati di accedere al sistema o ai suoi dati*	*Le misurazioni crittografiche basate su hardware forniscono un meccanismo per verificare l'integrità della composizione del sistema. È possibile misurare il BIOS, il firmware e i componenti hardware collegati in modo che sia noto lo stato di avvio noto e qualsiasi cambiamento o modifica possa essere facilmente rilevato.*

	all'insaputa del proprietario del sistema.	
ISC-1.2, Etichettatura basata su hardware	*Senza alcun tipo di etichettatura dei sistemi che comprendono un pool di risorse di calcolo, i carichi di lavoro NF virtuali o containerizzati possono essere istanziati su qualsiasi host all'interno del pool di risorse. Le etichette software vengono spesso applicate a sistemi o insiemi di sistemi per designarli per carichi di lavoro specifici; tuttavia, le etichette vengono spesso applicate a livello di sistema operativo, che può essere aggirato su un sistema compromesso.*	*L'etichettatura dei sistemi basata su hardware fornisce etichette univoche definite dall'utente applicate ai sistemi. Queste etichette possono aiutare a identificare un sistema in base a qualsiasi insieme di attributi, ad esempio informazioni sulla posizione e identificatori univoci per carichi di lavoro specifici. Inoltre, queste etichette, dette anche asset tag, sono firmate crittograficamente e archiviate in hardware a prova di manomissione, che può essere utilizzato per dimostrare l'integrità e la proprietà di queste etichette.*
ISC-1.3, Attestazione piattaforma remota	*I data center sono generalmente costituiti da migliaia di server e tenerne traccia e il rispettivo firmware è un compito arduo per un operatore. Senza la gestione centralizzata delle piattaforme server, potrebbero essere apportate modifiche non approvate al loro firmware e non essere rilevate dall'operatore del data center.*	*L'attestazione della piattaforma remota fornisce l'imposizione di quali componenti possono essere eseguiti su piattaforme server su tutti i sistemi hardware in un data center. Sebbene ISC-1.1 e ISC-1.2 forniscano meccanismi di integrità, non affrontano il monitoraggio centralizzato di tutti i sistemi. La possibilità di verificare rispetto a un elenco di autorizzazioni collettivo di piattaforme server e dei componenti firmware associati, rispetto a un sistema locale che applica una politica della catena di approvvigionamento, offre agli operatori maggiore flessibilità e controllo in modo crittograficamente protetto. Questi meccanismi di applicazione possono incorporare le misurazioni e l'etichettatura della piattaforma basata su hardware in queste politiche di sicurezza. Inoltre, il server di attestazione remoto può anche essere considerato un Trust Broker poiché altri servizi possono interrogarlo per ottenere lo stato di attendibilità dei server nel data center.*
ISC-1.4, Applicazione dell'orchestrazione delle funzioni di rete	*I carichi di lavoro NF potrebbero potenzialmente essere istanziati o migrati su server di elaborazione con vulnerabilità o versioni firmware non consentite o al di fuori di un confine logico.*	*I pianificatori dell'orchestrazione del carico di lavoro integrati con un broker fiduciario utilizzano le misurazioni dell'attendibilità e i tag delle risorse come fattori di posizionamento del carico di lavoro. Questo aiuta a garantire che i carichi di lavoro NF vengano istanziati o migrati solo su server di calcolo con misurazioni di affidabilità conformi e tag asset che hanno la loro fiducia radicata nell'hardware.*

ISC-1.5, Crittografia dell'immagine della funzione di rete	*Le immagini del carico di lavoro sono spesso archiviate in una posizione di archiviazione condivisa e possono contenere informazioni riservate o proprietarie. Una violazione dei dati potrebbe verificarsi se le immagini vengono consultate o copiate su un altro sito da un utente non autorizzato.*	*Le immagini del carico di lavoro NF vengono crittografate nella posizione di archiviazione condivisa e solo i server di elaborazione che soddisfano i criteri di sicurezza predefiniti hanno accesso alle chiavi di decrittografia quando ospitano il carico di lavoro NF. Ciò garantisce che solo la piattaforma di hosting possa decrittografare un'immagine del carico di lavoro e accedere alle sue informazioni. Inoltre, la politica di sicurezza per l'accesso alle chiavi di decrittografia include fattori come lo stato di attendibilità e il tag asset e si integra con Trust Broker per ottenere queste informazioni prima di rilasciare una chiave di decrittografia.*
Infrastructure Recommended Practice, ISC-3		
	Minaccia/Vulnerabilità	**Mitigazione**
SC-3.1, Monitoraggio della sicurezza delle infrastrutture	*Le minacce all'infrastruttura potrebbero includere un malintenzionato o un insider che tenta di ottenere o ottenere un accesso non autorizzato senza essere rilevato. Esempi di attacchi potrebbero includere DDoS, man in the middle, escalation dei privilegi, ransomware, rilevamento di anomalie comportamentali, malware e minacce interne. Senza capacità di monitoraggio o rilevamento per trovarli, questi attacchi potrebbero continuare a persistere o peggiorare.*	*Utilizza gli strumenti di monitoraggio della sicurezza dell'infrastruttura che consentono visibilità e informazioni dettagliate sull'infrastruttura e aiutano a identificare le attività sospette. Gli strumenti possono fornire un modo efficiente per rilevare e tenere traccia dei rischi per la sicurezza in modo che l'organizzazione possa intraprendere azioni preventive.*
ISC-3.2, Segmentazione della rete	*Diversi tipi di traffico attraversano la rete 5G, come operazioni infrastrutturali, gestione NF e dati utente. Senza la segmentazione della rete, un normale utente 5G potrebbe potenzialmente interagire con i componenti gestionali e operativi della rete 5G.*	*La segmentazione della rete applica i controlli di accesso a diverse porzioni della rete 5G. Questa tecnica crea segmenti di rete isolati per ogni tipo di traffico all'interno della rete 5G per impedire l'accesso non autorizzato ad altri tipi di traffico.*

5G STANDALONE SECURITY

Subscriber Privacy, 5GSC-1		
	Minaccia/Vulnerabilità	**Mitigazione**
GSC-1.1, Protezione	*Un catcher International Mobile Subscriber Identity (IMSI) è un tipo di*	*Se utilizzata senza lo schema di cifratura nullo, questa funzione 5G crittografa*

dell'identificatore permanente dell'abbonamento (SUPI).	*stazione base falsa utilizzata per intercettare le informazioni di identificazione dell'abbonato di telefoni cellulari. Essenzialmente una torre mobile "falsa" che impersona il fornitore di servizi, inganna un telefono facendogli inviare la sua identità di abbonato permanente LTE chiamata IMSI. Il falso operatore della stazione base può utilizzare queste informazioni per tracciare la posizione degli abbonati mobili.*	*l'identificatore permanente dell'abbonamento 5G (Subscription Permanent Identifier [SUPI]) con la chiave pubblica dell'operatore di casa per creare l'identificatore nascosto dell'abbonamento (Subscription Concealed Identifier [SUCI]). Ciò impedisce che l'identificatore permanente (Permanent Identifier [SUPI]) sia inviato in chiaro e rende le informazioni inutilizzabili per il tracciamento degli abbonati.*
5GSC-1.2, Riallocazione di ID temporanei	*Negli attacchi informatici passivi degli abbonati, gli attori malintenzionati raccolgono più identificatori temporanei univoci globali (Global Unique Temporary Identifiers [GUTI]) che possono essere utilizzati per scopi diversi. Un esempio è verificare la presenza di un abbonato in una determinata area e un altro è rivelare i suoi movimenti passati in quell'area e consentire il tracciamento dei movimenti futuri. Quando gli ID temporanei come GUTI non sono aggiornati abbastanza frequentemente, diventano ID quasi permanenti.*	*Questa funzione 5G fornisce un aggiornamento coerente dell'identificatore temporaneo di un dispositivo utente nelle seguenti condizioni: procedure di paging, registrazione iniziale e aggiornamento della registrazione della mobilità. La rete può essere configurata per allocare anche una nuova GUTI dopo ogni richiesta di servizio dell'UE (**User Equipment**). La disposizione più sicura è quando una UE ottiene una nuova GUTI ogni volta che ha utilizzato la sua GUTI in chiaro sull'interfaccia radio. Ciò garantisce che gli ID temporanei non possano essere utilizzati per il monitoraggio degli abbonati.*
5GSC-1.3, Sicurezza messaggio NAS iniziale	*Gli strati inferiori specifici della tecnologia radio (ad esempio, comunicazione tra UE e gNB) del protocollo di comunicazione sono chiamati strato di accesso (Access Stratum [AS]), mentre gli strati superiori radio-agnostici (ad esempio, comunicazione tra UE e Core) sono chiamati strato di non accesso (Non-Access Stratum [NAS]). Il messaggio NAS iniziale è il primo messaggio NAS inviato dopo che l'UE è passata dallo stato inattivo. La richiesta di servizio è un tipo di messaggio NAS iniziale. Se tutte le parti di un messaggio NAS iniziale vengono inviate in chiaro, alcune informazioni specifiche dell'UE potrebbero essere sfruttate.*	*Gli standard 5G impongono che quando l'UE non ha un contesto di sicurezza NAS (cioè, non ha chiavi di crittografia o integrità valide), invii un insieme limitato di elementi di informazione (chiamati IE di testo in chiaro), compresi quelli necessari per stabilire la sicurezza nel messaggio iniziale. D'altra parte, quando l'UE ha già un contesto di sicurezza (cioè, ha chiavi di crittografia o integrità valide), l'UE deve inviare un messaggio che ha il messaggio NAS iniziale completo cifrato in un contenitore NAS insieme agli IE in chiaro, con l'integrità dell'intero messaggio è protetta.*
5GSC-1.4, nessun cercapersone basato su SUPI	*La rete avvisa un cellulare per chiamate o messaggi in arrivo utilizzando un messaggio cercapersone. Nelle precedenti generazioni di reti mobili, questo messaggio di paging poteva contenere l'identificatore permanente dell'abbonato. Gli attacchi al protocollo di paging possono avere*	*Prima del 5G, i tempi di paging erano in genere determinati sulla base di un identificatore a lungo termine (permanente) (IMSI). Il 5G determina sempre i tempi di paging in base a un identificatore temporaneo (chiamato 5G-S-TMSI). In altre parole, il 5G non ha il paging basato su SUPI.*

	gravi ripercussioni. Ad esempio, potrebbe consentire a un aggressore di dedurre la posizione di una vittima in base all'identificatore permanente della vittima o iniettare avvisi di emergenza fabbricati.	
5GSC-1.5, Rispondere alla richiesta di identificazione con SUCI	*In LTE, la rete può richiedere l'identità di una UE durante determinate procedure e impostare specificamente il tipo di ID mobile richiesto come identificatore permanente (IMSI). L'UE è quindi tenuta a rispondere con un messaggio di risposta di identità contenente l'IMSI richiesto nel testo in chiaro. Ciò potrebbe consentire a una stazione base falsa di recuperare l'identità permanente dell'UE.*	*In 5G, la rete non può impostare il tipo di ID mobile richiesto come identificatore permanente in chiaro (SUPI). Tuttavia, può impostare il tipo di ID mobile richiesto come identificatore permanente nascosto (SUCI). Ciò significa che nel messaggio di risposta, l'UE sarà in grado di nascondere il suo identificatore permanente se l'operatore ha abilitato questa caratteristica di sicurezza configurando uno schema SUCI appropriato.*
Radio Network Security, 5GSC-2		
	Minaccia/Vulnerabilità	**Mitigazione**
5GSC-2.1, Protezione dell'integrità del piano utente	*L'integrità del traffico del piano utente tra il dispositivo e la rete non era protetta nelle generazioni precedenti. Ad esempio, in un noto attacco LTE denominato aLTEr, un attore malintenzionato può modificare il payload del messaggio e può reindirizzare le richieste DNS e quindi eseguire un attacco di spoofing DNS.*	*Nel 5G, la protezione dell'integrità del piano utente tra il dispositivo e la rete è stata introdotta come nuova funzionalità, a complemento della protezione della riservatezza esistente del traffico del piano utente. L'abilitazione della protezione dell'integrità del piano utente previene questo tipo di minaccia. Il supporto di questa funzionalità è obbligatorio sia per il dispositivo che per la rete, mentre l'utilizzo è facoltativo e sotto il controllo dell'operatore.*
5GSC-2.3, Pratica consigliata per algoritmi crittografici	*Un operatore di rete è limitato agli algoritmi crittografici supportati nelle apparecchiature distribuite nelle sue reti. Se gli algoritmi configurati per l'uso dovessero risultare in qualche modo deboli, il sistema potrebbe essere a rischio.*	*Il 5G supporta gli stessi algoritmi crittografici disponibili per l'uso in LTE. Secondo le specifiche 3GPP, le apparecchiature di rete 5G devono supportare un algoritmo basato su Advanced Encryption Standard (AES) e un algoritmo basato su SNOW3G. Il sistema supporta il passaggio tra algoritmi implementati nell'apparecchiatura di rete. Questo interruttore potrebbe essere attivato se l'algoritmo configurato per l'uso in una rete risulta debole. Ciò porta una certa agilità intrinseca dell'algoritmo al sistema 5G.*
Authentication Enhancements, 5GSC-3		
	Minaccia/Vulnerabilità	**Mitigazione**
GSC-3.1, Native Extensible	*Nelle generazioni precedenti, solo AKA veniva utilizzato per l'autenticazione*	*Gli standard 5G specificano l'uso dell'autenticazione indipendente*

Authentication Protocol (EAP) Support	*primaria per autenticare reciprocamente l'UE e la rete. La chiave non era associata al nome della rete di servizio. Pertanto, potrebbero verificarsi vari tipi di problemi di sicurezza, come una rete di servizio compromessa e/o una chiave utilizzata per l'accesso non autorizzato, ad esempio roaming e frodi non in roaming.*	*dall'accesso utilizzando EAP-AKA' per consentire l'autenticazione reciproca tra l'UE e la rete e fornire materiale di codifica che può essere utilizzato tra l'UE e la rete di servizio nelle successive procedure di sicurezza. EAP-AKA' lega il nome della rete di servizio alla chiave, impedendo l'accesso non autorizzato. EAP-AKA' è supportato per le tecnologie di accesso 3GPP e non 3GPP. Si noti che EAP-AKA' impedisce anche di ridurre gli attacchi a versioni precedenti di EAP.*
5GSC-3.2, Accesso non 3GPP	*Gli abbonati alla rete 5G possono accedere ai servizi 5G tramite reti di accesso non 3GPP. Le reti non 3GPP700, come il Wi-Fi, possono essere soggette a vari tipi di attacchi alla sicurezza, inclusi punti di accesso falsi per il dirottamento di sessioni utente legittime e attacchi di intercettazione.*	*Un contesto di sicurezza comune viene mantenuto nella rete principale 5G quando una UE si connette da entrambe le reti 3GPP e non 3GPP. In 5G, la funzione di interlavoro non 3GPP (N3IWF) viene utilizzata per l'accesso da reti non 3GPP non attendibili. Per gli accessi non 3GPP, i tunnel IPsec possono essere utilizzati per proteggere l'abbonato e segnalare il traffico dal punto di accesso non 3GPP all'N3IWF.*
5GSC-3.3, archiviazione delle credenziali basata su hardware	*Gli standard 5G specificano che le chiavi a lungo termine e la chiave pubblica della rete domestica devono essere archiviate nell'Universal Subscriber Identity Module (USIM) nell'UE. L'USIM è un contenitore software in esecuzione su un UICC, spesso indicato come scheda SIM. Per le reti 5G che utilizzano EAP-AKA o 5G-AKA, tutte le chiavi crittografiche eccetto la chiave di crittografia SUCI nei protocolli 3GPP sono derivate dalla chiave a lungo termine precondivisa. Una USIM può essere rimovibile (scheda SIM fisica) o incorporata (eSIM). Le chiavi a lungo termine memorizzate nel dispositivo sono bersagli preziosi per gli avversari. Se le chiavi sono compromesse, il traffico di abbonati 3GPP protetto e il traffico di segnalazione possono essere intercettati dall'avversario. Alcuni esempi di attacchi noti contro le chiavi sono attacchi del canale laterale.*	*La protezione della chiave a lungo termine è importante. La sicurezza fisica dei dispositivi mobili può proteggere le chiavi dagli attacchi del canale laterale. In 5G, agli USIM viene fornita una chiave crittografica a lungo termine e pre-condivisa denominata K. Questa chiave è archiviata all'interno dell'USIM a prova di manomissione e all'interno della rete principale (in Authentication Credential Repository and Processing Function [ARPF]) . La riservatezza della chiave a lungo termine è protetta all'interno dell'USIM e dell'ARPF e la chiave non è mai resa disponibile in chiaro al di fuori di tali posizioni. Si noti che la stessa capacità esiste nelle precedenti generazioni di reti 3GPP come 4G.*
5GSC-3.4, Funzione di ancoraggio di sicurezza (SEAF)	*Nelle precedenti generazioni di reti 3GPP, la componente SEAF (Security Anchor Functions) non era presente. Negli scenari di roaming, la rete di servizio (nella Public Land Mobile Network [PLMN] visitata) potrebbe prendere decisioni sull'autenticazione delle UE. Ciò ha creato una superficie*	*• 5G introduce i metodi di autenticazione EAP-AKA' e 5G-AKA utilizzando SEAF che prevengono gli attacchi di cui sopra abilitando il controllo domestico dell'autenticazione UE. La funzione del server di autenticazione (AUSF) nella*

	di attacco in cui un avversario potrebbe utilizzare una rete di servizio non attendibile per autorizzare in modo fraudolento le UE.	*PLMN domestica prende la decisione finale sull'autenticazione UE.* • *SEAF supporta l'autenticazione primaria dell'UE. SEAF supporta anche la riautenticazione dell'UE quando si sposta tra diverse reti di accesso (RAN nella stessa PLMN) o addirittura serve reti (in scenari di roaming) senza dover rieseguire l'autenticazione completa.* • *SEAF detiene la chiave di ancoraggio o la chiave radice per ciascuna UE in entrambi gli scenari in roaming e non in roaming. La chiave di ancoraggio è associata al nome della rete di servizio. SEAF deve autenticarsi presso l'AUSF della rete domestica. Riceve la chiave di ancoraggio dall'AUSF nella PLMN domestica durante la procedura di autenticazione e riautenticazione primaria dell'UE se l'autenticazione ha esito positivo.*
API Security, 5GSC-5		
	Minaccia/Vulnerabilità	**Mitigazione**
GSC-5.1, Sicurezza API per la funzione di esposizione alla rete (NEF)	• *Nelle precedenti generazioni di reti 3GPP, la sicurezza per un meccanismo di esposizione della rete standardizzato non era definita. Anche se la Service Capability Exposure Function (SCEF) è stata introdotta nelle specifiche 3GPP R13 per standardizzare l'accesso alle API di terze parti, è stata utilizzata principalmente per i servizi relativi ai dispositivi Internet of Things (NB-IoT) a banda stretta.* • *Le informazioni sensibili nella rete come il nome della rete dati (DNN), le informazioni sull'assistenza alla selezione di singole sezioni di rete (S-NSSAI) e i dati degli abbonati come SUPI possono essere involontariamente esposti tramite l'interfaccia N33.*	*NEF funge da gateway sicuro per le funzioni applicative (AF) di terze parti (interne) e non attendibili (esterne) per esporre vari servizi come analisi, instradamento del traffico utente, posizione UE, raggiungibilità e informazioni relative alla mobilità. Autentica e autorizza i servizi richiesti dagli AF. Gli standard 5G impongono l'integrità, la riproduzione e la protezione della riservatezza per la comunicazione tra NEF e AF. Gli standard 5G impongono inoltre la connessione da NEF ad AF per supportare TLS e l'uso dell'autenticazione reciproca basata su certificati tra AF di terze parti e NEF. NEF maschera le informazioni sensibili sulla rete 5G come DNN, S-NSSAI e le informazioni sensibili sugli abbonati come SUPI dagli AF di terze parti.*
Application Security, 5GSC-7		
	Minaccia/Vulnerabilità	**Mitigazione**
5GSC-7.1, Monitoraggio della sicurezza del traffico degli abbonati	*Sebbene gli operatori di rete mobile e le imprese abbiano visibilità sul loro traffico di mobilità, gli attori malintenzionati possono aggirare i meccanismi di rilevamento di un operatore. Ciò crea vulnerabilità per i centri operativi di rete e di sicurezza (rispettivamente NOC e SOC) incapaci*	*L'ispezione del traffico del piano utente e del piano di controllo consente una visibilità contestuale del traffico di rete. L'ispezione degli eventi Packet Forwarding Control Protocol (PFCP) o dei messaggi SMF (Session Management Function) e la loro correlazione con i tunnel GTP-U*

	di rilevare l'uso delle risorse di rete da parte di un attore malintenzionato. I dispositivi di rete infetti utilizzano in modo dannoso le risorse di rete per il traffico Command-and-Control (C2), che influisce sulle prestazioni della rete e delle applicazioni. Durante gli eventi di sicurezza come gli attacchi DDoS generati dall'UE, i team di risposta alla sicurezza non sono in grado di correlare il traffico botnet o il traffico correlato agli DDoS ai singoli abbonati o alle apparecchiature.	*(General Packet Radio Service) Tunneling Protocol User (GTP-U) consente di mappare SUPI e PEI al traffico di rete. Quando queste informazioni sono associate ai risultati di C2, gli analisti di SOC e NOC di ispezione di vulnerabilità, antivirus e botnet hanno una visione chiara degli utenti malintenzionati. Una volta che queste informazioni sono state raccolte e analizzate da più fonti e monitorate nel tempo, è possibile stabilire una chiara comprensione di quali tipi di dispositivi e utenti causano problemi e cosa provoca tali problemi. Ciò si traduce in un'analisi della causa principale più rapida per gli incidenti di sicurezza della rete.*
5GSC-7.2, Applicazione della sicurezza del piano utente	*• Il malware può essere distribuito tramite una serie di meccanismi, come download incorporati in e-mail o contenuto SMS (Short Message Service), download da siti Web o applicazioni dannosi o persino da hardware dannoso.* *• Il software dannoso installato su UE può causare una serie di problemi sulla rete. Il software dannoso può utilizzare la rete per comunicare con i server C2, causando congestione sulla rete mobile. L'apparecchiatura utente infetta può anche essere utilizzata come botnet per causare a801 Attacco DDoS contro il 5G Core o risorse e applicazioni di rete.* *• L'UE sulla rete può essere utilizzata per accedere ed esfiltrare dati sensibili. L'UE potrebbe anche essere utilizzata per attaccare o accedere a servizi di rete non autorizzati. Con il traffico controllato, UE può anche essere utilizzata per accedere a siti Web dannosi o utilizzare applicazioni SaaS (Software-as-a-Service) non approvate.*	*• Per interrompere la distribuzione di malware da Internet, il traffico in ingresso deve essere ispezionato da un'appliance di sicurezza in grado di eseguire l'analisi del malware e il controllo dei file. L'utilizzo di metodi di rilevamento basati sulle firme è un modo accurato per rilevare il malware noto. Per identificare rapidamente il malware sconosciuto, l'utilizzo di un approccio multi-metodo è il più accurato, associando l'analisi statica e dinamica all'apprendimento automatico per ridurre la latenza e i tempi di elaborazione.* *• Ispezionare il traffico del piano utente e analizzarlo rispetto a firme C2 note, domini dannosi noti e algoritmi di generazione di domini è un ottimo modo per identificare il traffico C2. L'implementazione di un'appliance di sicurezza in grado di rilevare e prevenire questo tipo di traffico aiuta a garantire la continuità della rete.* *• Il modo migliore per proteggere dati, applicazioni, risorse e servizi è rimuovere la fiducia implicita attraverso l'architettura zero trust (ZTA) per le reti 5G. La corretta implementazione di 5G ZTA richiede l'implementazione di politiche di controllo granulari su un Policy Enforcement Point (PEP). Il PEP dovrebbe ispezionare tutto il traffico del piano utente e consentire solo il traffico benigno che supporta i casi d'uso aziendali. Le politiche di controllo granulare sono definite con un soggetto completo di attributi 5G come SUPI,*

		PEI, applicazione o servizio. L'implementazione del PEP in N3 combinato con i dati di N4 o N11 consente di correlare e applicare le politiche che contengono SUPI e PEI.
Internet Security Protocol Recommended Practice, 5GSC-8		
	Minaccia/Vulnerabilità	**Mitigazione**
5GSC-8.2, IPsec/NDS IP	*• Quando IPsec non viene utilizzato nella rete 5G, i dati sensibili degli abbonati e i dati di segnalazione potrebbero essere vulnerabili alle intercettazioni se inviati non crittografati, ad esempio, connessioni di backhaul e su rete di accesso non 3GPP.* *• Quando IPsec viene utilizzato con una configurazione errata, è possibile creare una connessione non sicura utilizzando protocolli o algoritmi deboli o compromessi. Ad esempio, le chiavi precondivise (PSK) potrebbero consentire a una terza parte di decrittografare il traffico intercettato se una rete è configurata per l'utilizzo di chiavi deboli. Le chiavi potrebbero essere trapelate se inviate tramite connessioni non protette o se archiviate non crittografate. Il protocollo Internet Key Exchange versione 1 (IKEv1) potrebbe essere vulnerabile agli attacchi dei dizionari offline se viene utilizzato un PSK debole. Sia IKEv1 che IKEv2 potrebbero essere vulnerabili agli attacchi di amplificazione DDoS a causa di un'implementazione errata del protocollo.*	*• IPsec è una suite di standard aperti per garantire comunicazioni private su reti pubbliche. Si tratta di un comune controllo di sicurezza a livello di rete generalmente utilizzato per crittografare il traffico IP tra host in una rete e per creare una rete privata virtuale (VPN). I tunnel IPsec vengono utilizzati nelle reti 5G per fornire agli abbonati e al traffico di segnalazione integrità, riservatezza e protezione della riproduzione per la connessione backhaul e altre connessioni, come l'accesso alla rete non 3GPP non attendibile. Gli standard 3GPP impongono l'uso dell'integrità dei dati e della protezione anti-riproduzione per IPsec. La riservatezza è facoltativa per IPsec in determinati scenari. Per un elenco completo delle opzioni di configurazione consigliate per i protocolli IPsec e IKE, fare riferimento alla tabella 1 di "NIST SP 800-77".* *• Gli standard 5G specificano che IPsec potrebbe essere utilizzato per proteggere i non SBI.*

117. DIMOSTRAZIONE DELLE CARATTERISTICHE DI SICUREZZA

Questa sezione descriverà come ogni scenario dimostra la caratteristica/categoria di sicurezza e le capacità/proprietà di sicurezza associate.

Questa sezione sarà scritta per una futura bozza.

PRESUPPOSTI E LIMITAZIONI

Questa sezione sui limiti dello scenario dimostrativo verrà scritta per una bozza futura.

SCENARI DI DIMOSTRAZIONE FUNZIONALE

Questa sezione descriverà brevi scenari di dimostrazione funzionale.

Includerà tutti gli scenari funzionali che sono abilitati dall'attuale architettura del sistema e indicherà quelli aggiuntivi che sono pianificati per dopo.

Il funzionamento di ciascuna funzionalità di sicurezza per la soluzione di esempio sarà verificato nel contesto dello scenario dimostrativo descritto di seguito, nonché per ulteriori scenari da aggiungere a una bozza futura.

SCENARIO 1 - IMPLEMENTAZIONE 5G SA UTILIZZANDO UN'UNICA PLMN

Questa sezione fornirà una breve panoramica delle apparecchiature, dell'architettura e del flusso delle chiamate utilizzati in questo scenario.

La funzionalità di dati, voce e video verrà testata per il caso non in roaming.

Dettagli specifici saranno descritti nel piano dimostrativo funzionale.

DATA CALL

Questa sezione fornirà una breve panoramica dell'impostazione della chiamata dati.

Informazioni dettagliate sulla procedura di test e sui risultati dei test per la chiamata dati 5G saranno descritte nel piano di dimostrazione funzionale.

Nel mondo reale, questo test equivale a un abbonato che naviga in un sito Web su Internet o invia un'e-mail a un altro abbonato.

VOICE OVER IP CALL

Questa sezione fornirà una breve panoramica dell'impostazione della chiamata VoIP.

Informazioni dettagliate sulla procedura di test e sui risultati dei test per la chiamata 5G VoIP saranno descritte nel piano di dimostrazione funzionale.

Nel mondo reale, questo test equivale a un abbonato che effettua una chiamata VoIP su Internet a un altro abbonato.

VIDEO STREAMING

Questa sezione fornirà una breve panoramica dello streaming video

Informazioni dettagliate sulla procedura di test e sui risultati dei test per lo streaming video 5G saranno descritte nel piano di dimostrazione funzionale.

Nel mondo reale, questo test equivale a un abbonato che effettua una richiesta di video on demand per un particolare file video a un server di streaming video su Internet.

RISULTATI

Questa sezione evidenzierà in che modo le capacità di sicurezza istanziate nella dimostrazione dell'architettura del sistema affrontano i rischi per la sicurezza che si intendeva supportare.

Questa sezione sarà scritta per una futura bozza.

118. APPENDICE A – SECURITY CONTROL MAP

Questa appendice fornirà tabelle che mappano le capacità di sicurezza informatica delle tecnologie utilizzate per la prima fase della soluzione di esempio alla guida NIST applicabile.

Questa appendice sarà aggiunta a una futura bozza.

119. APPENDICE B – FUTURE CAPABILITIES

Ci sono molte funzionalità di sicurezza aggiuntive che saranno incorporate durante questo progetto.

La sezione Security Capabilities descrive quelli che sono previsti per la prima fase del progetto.

Questa appendice descrive funzionalità di sicurezza aggiuntive pianificate provvisoriamente per la fase successiva.

Security Capability	Subreference	Description
Infrastructure Security		
Hardware Roots of Trust Packet Core, ISC-1		
Network Function Policy Enforcement	ICS-1.6	Technically enforce policies that define the servers in the compute environment where NFs can run based on trust values and asset tags.
5G Standalone Security		
Radio Network Security, 5GSC-2		
CU/DU Split	5GSC-2.2	Split gNB into Central Unit (CU) and Distributed Unit (DU), with the CU performing security functions (confidentiality/integrity) and being located closer to the core.
Security Visibility	5GSC-2.4	Enable applications to check the security being applied to the radio connection.
256-Bit Algorithms	5GSC-2.5	Use stronger cryptographic algorithms on this interface once they are adopted by 3GPP SA3.
Interworking & Roaming Security, 5GSC-4		
Security Edge Protection Proxy (SEPP)	5GSC-4.1	Implement application-layer security for the service layer information exchanged between two PLMNs. Provide security functions for integrity, confidentiality, replay protection, mutual authentication, authorization, negotiation of cipher suites, and key management, as well as the notion of topology hiding and spoofing protection.
5G to LTE Interworking Mobility Within the Same Operator Network	5GSC-4.2	Use secure procedures and security demarcations to secure LTE to 5G interworking as defined in 3GPP 23.501 [18]. Includes protecting the transmission of security keying materials between LTE and 5G.
5G to LTE Interworking Mobility Across Operator Networks	5GSC-4.3	Protects handovers involving 5G to LTE internetworking across two operators' network using N26 because 4G does not offer subscription identities encryption, so a UE moving from 5G to LTE will be subject to IMSI catching attacks. GSMA has not finalized work on 5G SA to LTE roaming across different operators.

API Security, 5GSC-5		
Common API Framework (CAPIF)	5GSC-5.2	Use secure interfaces, such as TLS-PSK, TLS-PKI and TLS-OAuth, provided by a common API interface between internal functions and external functions. Use CAPIF Core Function (CCF) to manage all internal and external APIs.
Network Slicing Security, 5GSC-6		
Network Slice Resource Isolation	5GSC-6.1	Enable the creation of multiple logical networks over the same physical infrastructure. Demonstrate orchestrated deployment and configuration of network functions to provide services that are required for a specific usage scenario. Tie into infrastructure security capabilities to isolate slice resources.
Network Slice Additional Authentication	5GSC-6.2	Perform secondary authentication with Network Slice Specific Authentication and Authorization Function (NSSAAF) to check if the user is authorized to use that slice (3GPP TS 29.526). Do additional authentication of subscriber identity.
Application Security, 5GSC-7		
Application Security Onboarding	5GSC-7.3	Ensure that applications are onboarded securely and that communications between applications are secure. Leverage the zero trust concept.
Internet Security Protocol Recommended Practice, 5GSC-8		
TLS Security	5GSC-8.1	Implement TLS security where possible to protect NF communication at the transport layer via mutual authentication and transport security. Ensure protection of the communication's confidentiality and integrity, and implement anti-replay measures.
DNSSEC	5GSC-8.3	Use DNS Security Extensions (DNSSEC) to protect the integrity of any 5G-related DNS communication.
OAuth for Service-Based Architecture (SBA)	5GSC-8.4	Use the OAuth 2.0 framework at the API layer to ensure that only authorized network functions are permitted access to a service offered by another NF. Use CAPIF with TLS-Oauth for all internal and external APIs.

RIFERIMENTI

1. *CMMC – Cybersecurity Maturity Model Certification – Carnegie Mellon University & The Johns Hopkins University Applied Physics Laboratory LLC – Copyright 2020*
2. *Progetto DECODE: https://decodeproject.eu/*
3. *EU Blockchain Observatory and Forum – An initiative of the European Commission: Blockchain and GDPR*
4. *CNIL - Blockchain & GDPR: Solutions for a responsible use of the blockchain in the context of personal data*
5. *2015 IEEE – Blockchain: Decentralizing Privacy: Using Blockchain to Protect Personal Data dal sito https://ieeexplore.ieee.org/document/7163223*
6. *ENISA WP2018 O.2.2.5: Reinforcing trust and security in the area of electronic communication and online services – December 2018*
7. *CSDE - The C2 Consensus on IoT Device Security Baseline Capabilities (Council to Secure the Digital Economy)*
8. *Kryptowire Discovered Mobile Phone Firmware that Transmitted PII without User Consent or Disclosure*
9. *Smart Grid Task Force 2012-14 - Expert Group 2: Regulatory Recommendations for Privacy, Data Protection and Cyber-Security in the Smart Grid Environment*
10. *OWASP Top 10-2013 – The Ten Most Critical Web Application Security Risks*
11. *CWE (Common Weakness Enumeration) 2011 CWE/SANS Top 25 Most Dangerous Software Errors*
12. *Checkmarx – Source Code Analisys Technologies*
13. *PCI Mobile Payment Acceptance Security Guidelines for Merchants as End-Users*

14. *PCI Mobile Payment Acceptance Security Guidelines for Developers*
15. *WP 248 rev.01 - Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679*
16. *(Toward) A Secure System Engineering Methodology – Model Main and Model Appendices [Authors: Chris Salter, NSA, salter@thematrix.ncsc.mil; O. Sami Saydjari, DARPA, ssaydjari@darpa.mil; Bruce Schneier, Counterpane Systems, schneier@counterpane.com; Jim Wallner, NSA, jmwalln@missi.ncsc.mil]*
    - *This paper is based on research done by a working group sponsored by the National Security Agency (NSA)*
17. *Linee Guida - Developing Cyber Resilient System: A System Security Engineering Approach - Computer Security [rielaborazione di Aldo Pedico del NIST SP 800-160 vol. 1 e 2 – Febbraio 2020; file «17 – NIST SP 800-160 – Dev. Cyber Resilient Sys»]*
    - *Linee guida per lo sviluppo di sistemi Ciberresilienti*
18. *Linee Guida - Adeguamento Tecnologico al GDPR [Aldo Pedico – v1.0 – Settembre 2016]*
    - *Linee guida per l'adeguamento al Reg. UE 2016/679*
19. *EDPB Guidelines 1/2018: on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation 2016/679*
20. *WP180: per le applicazioni RFID adottato 11 FEB 2011, http://ec.europa.eu/justice/data–protection/article–29/documentation/opinion– recommendation/files/2011/wp180_annex_en.pdf*
21. *Regolamento di Esecuzione (UE) 2018/151*
    - *Il presente regolamento specifica ulteriormente gli elementi che i fornitori di servizi digitali devono prendere in considerazione nell'identificazione e nell'adozione delle misure volte a garantire un livello di sicurezza delle reti e dei sistemi informativi che essi utilizzano nel contesto dell'offerta di servizi di cui all'allegato III della direttiva (UE) 2016/1148; esso precisa ulteriormente anche i parametri da prendere in considerazione al fine di determinare se un incidente ha un impatto rilevante sulla fornitura di tali servizi.*
22. *Regolamento Generale per la Protezione dei Dati [Reg. (UE) 2016/679]*
23. *Regolamento (UE) 2019/881 «Regolamento sulla Cibersicurezza»*
24. *Computer Technology Research Corp. – Enterprisewide Network Security – Effective Implementation and International Standard - ed. 1994*
25. *CMMC – Cybersecurity Maturity Model Certification – Carnegie Mellon University & The Johns Hopkins University Applied Physics Laboratory LLC – Copyright 2020*

    Modello per la certificazione o autocertificazione del sistema di cibersicurezza
26. *Threat Modeling for Cloud Data Center Infrastructures - Nawaf Alhebaishi[1,2], Lingyu Wang[1], Sushil Jajodia[3], and Anoop Singhal[4]*

    [[1]Concordia Institute for Information Systems Engineering Concordia University, [2]Faculty of Computing and Information Technology, King Abdulaziz University, [3]Center for Secure Information Systems, George Mason University, [4]Computer Security Division, National Institute of Standards and Technology]
    1) *Modellizzazione minacce in ambiente cloud;*
    2) *Applicazione metriche di sicurezza basate rispettivamente sull'albero di attacco e sui grafici di attacco per quantificare ulteriormente le minacce modellate*
27. *NIST: Framework for Improving Critical Infrastructure (2014)*
    1) *Guidare le attività di cybersecurity e considerare i rischi di cybersecurity come parte dei processi di gestione dei rischi dell'organizzazione.*
    2) *È composto da tre parti: il Framework Core, il Profile Framework e i livelli di implementazione del Framework.*
    3) *Il Core è un insieme di attività, risultati e riferimenti informativi sulla cibersicurezza che sono comuni a tutti i settori di infrastrutture critiche, fornendo la guida dettagliata per lo sviluppo di singoli profili organizzativi.*
    4) *Aiuta l'organizzazione ad allineare le sue attività di sicurezza informatica con i suoi requisiti aziendali, tolleranze di rischio e risorse.*
    5) *I livelli forniscono alle organizzazioni un meccanismo per visualizzare e comprendere le caratteristiche del loro approccio alla gestione del rischio di sicurezza informatica.*

6) *Applicare i principi e le migliori pratiche di gestione dei rischi per migliorare la sicurezza e la resilienza delle infrastrutture critiche.*

28. *NIST SP 800–30 - Guide for Conducting Risk Assessments*

    Descrive:

    1) *i modelli di rischio;*
    2) *i processi di gestione e le valutazioni del rischio;*
    3) *le attività necessarie per preparare e condurre una valutazione del rischio;*
    4) *le fonti di minaccia, gli eventi di minaccia; le vulnerabilità; le probabilità che si verifichino eventi di minaccia; gli impatti e la determinazione del rischio.*

29. *NIST SP 800-37 – Risk Management Framework for Information Systems and Organizations – A System life Cycle Approach for Security and Privacy*
30. *NIST SP 800-39 – Managing Information Security Risk – Organization, Mission and Information System View*
31. *NIST SP 800-53 - Security & Privacy Controls for Information Systems and Organizations*
    1) *Descrive: i concetti fondamentali associati ai controlli di sicurezza e privacy; la struttura dei controlli e come sono organizzati i controlli nel catalogo consolidato; le designazioni di controllo; la relazione tra controlli di sicurezza e privacy; e affidabilità e sicurezza*
    2) *Fornisce: un catalogo consolidato di controlli di sicurezza e privacy; una sezione di discussione per spiegare lo scopo di ciascun controllo*
    3) *Privacy Assessment Procedures, Penetration Testing*
32. *NIST SP 800-53A – Assessing Security and Privacy Controls and Organizations*
33. *NIST SP 800-63-3 – Implementation Resources*
34. *NIST SP 800-63A - Digital Identity Guidelines Enrollment and Identity Proofing*
35. *NIST SP 800-63B - Digital Identity Guidelines Authentication and Lifecycle Management*
36. *NIST SP 800-63C – Federation and Assertion*
37. *NIST SP 800-82 – Guide to Industrial Control Systems (ICS) Security*
38. *NIST SP 800-98 - Linee guida per la protezione dei sistemi di identificazione a radiofrequenza (RFID).*
39. *NIST SP 800-121 Rev.1 - Guida alla sicurezza Bluetooth*
40. *NIST SP 800-122 – Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*
41. *NIST SP 800-133 Recommendation for Cryptographic Key Generation*
42. *NIST SP 800-160 - Systems Security Engineering - Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems*

    Scopo:

    1) *fornire una base per formalizzare una disciplina per l'ingegneria della sicurezza dei sistemi in termini di principi, concetti e attività;*
    2) *promuovere una mentalità comune per fornire sicurezza per qualsiasi sistema, indipendentemente dalla sua portata, dimensione, complessità o fase del ciclo di vita del sistema;*
    3) *fornire considerazioni e dimostrare come i principi, i concetti e le attività di ingegneria della sicurezza dei sistemi possano essere applicati in modo efficace alle attività di ingegneria dei sistemi;*
    4) *far progredire il campo dell'ingegneria della sicurezza dei sistemi promulgandolo come una disciplina che può essere applicata e studiata;*
    5) *fungere da base per lo sviluppo di programmi educativi e formativi, tra cui lo sviluppo di certificazioni individuali e altri criteri di valutazione professionale; ed infine*
    6) *fornire un metodo rigoroso per la progettazione della Ciberresilienza*

43. *NIST – Mitigating Cybersecurity Risk in Telehealth Smart Home Integration*
44. *NIST SP 800-161 - Supply Chain Risk Management Practices for Federal Information Systems and Organizations*
45. *NIST SP 800-171 - Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*

    Linee guida al fine di proteggere i dati:

1) *fornisce una metodologia, gli assunti fondamentali per sviluppare i requisiti della sicurezza;*
2) *fornisce la struttura dei requisiti;*
3) *fornisce l'adattamento dei criteri applicati agli standard del NIST e le linee guida per ottenere i requisiti;*
4) *suddivide in 14 famiglie i requisiti di sicurezza.*

46. *NIST SP 800-172 – Enhanced Security Requirements for Protecting CUI (Controlled Unclassified Information)*
    Requisiti (Controlli) di sicurezza forniti alle agenzie federali americane al fine di proteggere le informazioni delle CUI
47. *NIST SP 800-207 Zero Trust Architecture*
48. *NIST – Planning for a Zero Trust Architecture: A Starting Guide for Administrators*
49. *NIST SP 800-209 Security Guidelines for Storage Infrastructure*
50. *NIST SP 800-218 - Secure Software Development Framework (SSDF) - Recommendations for Mitigating the Risks of Software Vulnerabilities Use Cases*
51. *NIST SP 1800-13 – Mobile Application Single Sign-On (SSO): Improving Authentication for Public Safety First Responders*
52. *NIST SP 1800-16 - Securing Web Transactions: TLS Server Certificate Management*
53. *NIST SP 1800-24 - Securing Picture Archiving and Communication System (PACS): Cybersecurity for the Healthcare Sector*
54. *NIST SP 1800-30 - Securing Telehealth Remote Patient Monitoring Ecosystem*
55. *NIST SP 1800-32B – Securing the Industrial Internet of Things: Cybersecurity for Distributed Energy Resources*
56. *NIST SP 1800-34B – Validating the Integrity of Computing Devices*
57. *NIST IR 8144 - Assessing Threats to Mobile Devices & Infrastructure - The Mobile Threat Catalogue*
    1) *Delinea un catalogo di minacce ai dispositivi mobili e alle relative infrastrutture mobili per supportare lo sviluppo e l'implementazione delle funzionalità di sicurezza mobile, delle migliori pratiche e delle soluzioni di sicurezza per proteggere meglio la tecnologia informatica aziendale (IT);*
    2) *Suddivide e cataloga le minacce in tipologie, incentrate su applicazioni mobili, stack di rete e infrastrutture associate, catena di fornitura di dispositivi mobili e software; integrando informazioni esplicative e di vulnerabilità con accanto le strategie di mitigazione applicabili.*
58. *NIST IR 8183 – Cybersecurity Framework Manufacturing Profile*
59. *NIST IR 8228 - Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks*
60. *NIST IR 8259 - Funzionalità di sicurezza informatica dei dispositivi IoT - Linea di base*
61. *NIST IR 8272 – Impact Analysis Tool for Interdependent Cyber Supply Chain Risks [Interdependency Tool]*
    - *Questo strumento (disponibile gratuitamente) ha lo scopo di creare una comprensione del rischio di un'organizzazione, misurando l'impatto nei loro ambienti specifici [Cyber Supply Chain Risk Management (C-SCRM)]*
62. *NIST IR 8269 – A Taxonomy and Terminology of Adversarial Machine Learning*
63. *NIST IR 8286 - Integrating Cybersecurity and Enterprise Risk Management (ERM)*
64. *NIST IR 8286A - Identifying and Estimating Cybersecurity Risk for Enterprise Risk Management (ERM)*
65. *NIST IR 8320 - Hardware Enabled Security: Enabling a Layered Approach to Platform Security for Cloud and Edge Computing Use Cases*
66. *NIST IR 8334 – Using Mobile Device Biometrics for Authenticating First Responders*
67. *NIST IR 8344 – Ontology for Authentication*
68. *NIST IR 8356 – Consideration for Digital Twin Technology and Emerging Standards*
69. *NIST IR 8360 – Machine Learning for Access Control Policy Verification*
70. *NIST - Framework for Improving Critical Infrastructure – February 12, 2014*
71. *ISO/IEC 27005:2018 International Standard, Information Technology - Security techniques - Information Security Management*
    1) *context establishment in Clause 7;*
    2) *risk assessment in Clause 8;*
    3) *risk treatment in Clause 9; – risk acceptance in Clause 10;*

4) *risk communication in Clause 11*;
5) *risk monitoring and review in Clause 12*.
6) *Examples of typical threats*
7) *Vulnerabilities and methods for vulnerability assessment*
8) *Information security risk assessment approaches*

72. *ISO/IEC 29101 – I.T. – Sec. tech. – Privacy arch. framework Tech. de l'information – Tech. de sécurité – Arch. de référence de la protection de la vie privée*
73. *ISO/IEC 29134: Information technology – Security techniques – Privacy Impact Assessment Guidelines*
74. NIST SP 1800-33 - 5G Cybersecurity
75. GSMA Securing 5G Era