Associazione
tezione Diritti e Libe

pensare web
web partner

CONSULENZE PACI PRIVACY

FABIO TONTI

La protezione delle informazioni del sito web passa attraverso misure di sicurezza tecniche ed organizzative adeguate.

SEMINARIO FORMATIVO
SULLA PROTEZIONE DEI
DATI PERSONALI

CENTRO CONGRESSI SGR RIMINI
18 Dicembre 2019

pensare web
web partner

FacileWP
Multiple Wordpress Managed VPS

Mi presento!

fabio@pensareweb.it

Fabio Tonti

Amministratore delegato e fondatore

Fabio Tonti è specializzato nella consulenza tecnico / commerciale. Imprenditore per natura, Fabio ha oltre 20 anni di esperienza nella comunicazione digitale. E 'stato anche consulente per diverse aziende nazionali aiutandole a definire e attuare strategie di successo di Internet. Fabio ha un talento per la gestione di progetti Web complessi e di successo. La sua responsabilità è la consegna dei progetti in tempo.

Associazione
tezione Diritti e Libe

CONSULENZE PACI PRIVACY

pensare web
web partner

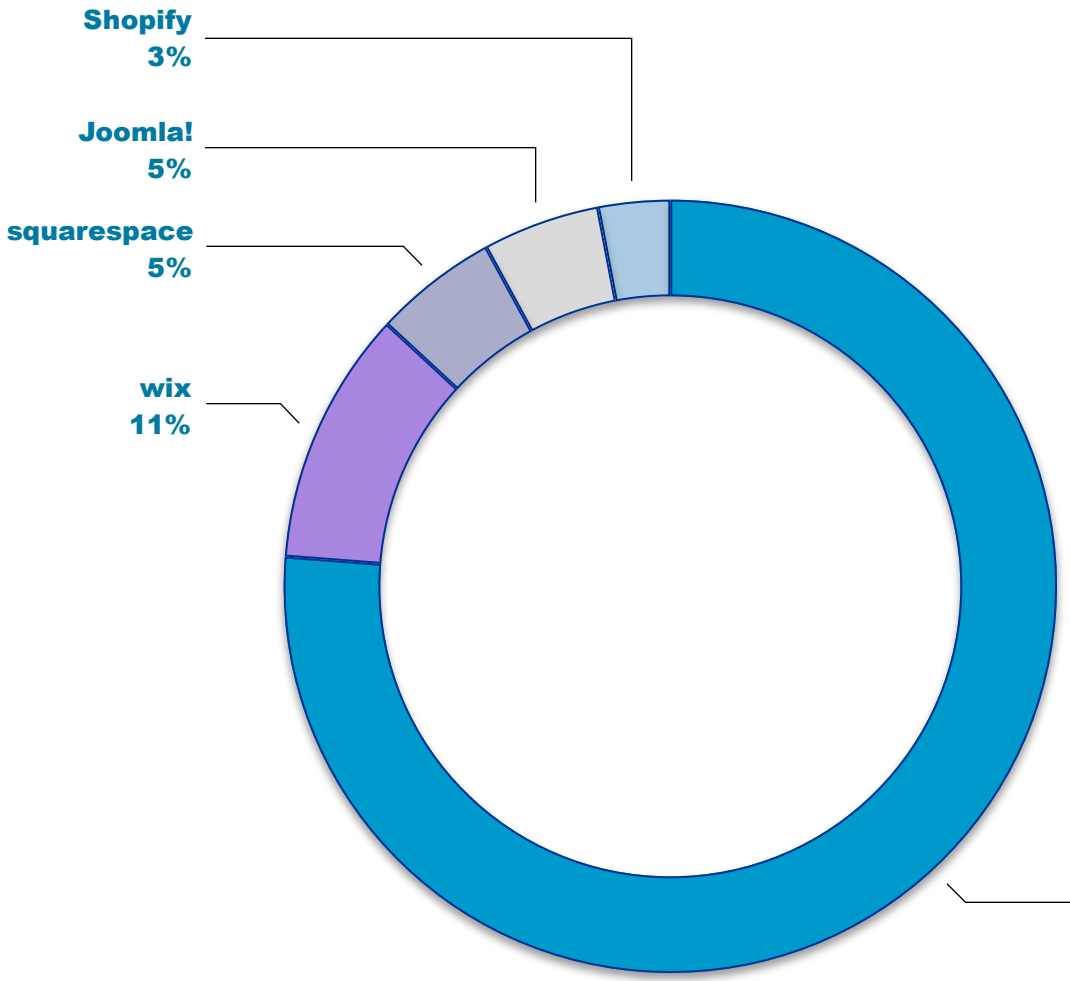
FacileWP
Multiple Wordpress Managed VPS

Parleremo di strumenti pratici per ridurre il rischio di Data Breach

Quanto segue si riferisce solo all'ambito Sito internet aziendale

WordPress

Perchè Wordpress?



- wordpress
- wix
- squarespace
- Joomla!
- Shopify

Consapevolezze sugli hacker

“gli hacker non sono intelligenti, hanno solo molta pazienza”

Gli strumenti che vengono utilizzati oggi sono gli stessi che utilizzavano 10 anni fa, ma continuando a usarli su grande scala e monitorando i risultati ogni tanto riescono a pescare qualcuno.

il mezzo più utilizzato dagli hacker attualmente è il phishing

c’è da notare che pescando nella rete spesso non si prendono i “pesci grandi” (che hanno tecniche e organizzazioni al passo dei tempi), ma prendono utenti di piccole organizzazioni che lavorano con i “pesci grandi”

Associazione
tezione Diritti e Libe

CONSULENZE PACI PRIVACY

pensare web
web partner

FacileWP
Multiple Wordpress Managed VPS

vediamo alcune minacce relative al sito aziendale

1a minaccia:
Abuso di privilegi da parte dell'utente.

Quando un esterno riesce a recuperare le credenziali di un altro, magari di un admin.

E’ particolarmente grave quando un utente usa la stessa password ovunque (amazon, eBay, ecc)

Furto di credenziali: quanto è frequente?

Furto di credenziali: un effetto collaterale costoso e dilagante delle violazioni dei dati

tentativi di accesso a causa di attacchi volti a sottrarre credenziali nel 2018

tentativi quotidiani di utilizzare credenziali rubate

degli adulti usano la stessa password o password simili in più account online

RIMEDIO contro il furto delle credenziali

PASSWORD SICURE

MAI USARE UN FOGLIO DI CALCOLO PER TUTTE LE PASSWORD

Creare frasi mnemoniche:

“Io mi chiamo Fabio, ho 1 figlia” diventa: ImcF,h1f

no brute force attack

RIMEDIO contro il furto delle credenziali

password salvate su supporti sicuri

DAL MIGLIORE AL PEGGIORE

1. **Utilizzare il gestore password del proprio pc (portachiavi)**

2. **Utilizzare un gestore password sul pc**
   - **Universal password manager**
   - **1 password**
   - **last pass**
   - **keepass**

RIMEDIO contro il furto delle credenziali

Password Checkup di Google

password.google.com

strumento utile per capire:

- se hai password compromesse
- se hai usato siti compromessi
- quanto sono sicure le password
- quante volte hai usato la stessa password

RIMEDIO contro il furto delle credenziali

AUTENTICAZIONE A DUE FATTORI

2a minaccia

Abuso di risorse

quando il sito viene usato per fare spam

per linkare siti esterni allo scopo di indicizzarli

quando viene usato il vostro hosting per minare criptovalute

RIMEDIO contro l'abuso di risorse

1. **SCELTA DEL CMS**
2. **aggiornamento core CMS e plug-ins**
3. **avere un piano di backup e monitorarli**
4. **monitorare il SEO del sito**
5. **Proteggere i moduli di informazione con Recapcha**
6. **Evitare di impostare "admin" come username dell'amministratore. È il primo bersaglio per il bruteforcing.**
7. **Realizzare invece un account da semplice "subscriber" con username "admin" in modo da "ingannare" i potenziali malitenzionati.**

3a Minaccia

Attacchi all’integrita’ dei sistemi

Attacchi all'integrita' dei sistemi

COSA PUO' SUCCEDERE?

- il sito smette di funzionare a causa di un attacco al core del CMS o ad un suo plug-in

- viene inserito una serie di post nel sito

- viene inserito del codice malevolo nel server

RIMEDI per l’integrità dei sistemi e informazioni

Le possibili tecniche di attacco sono molteplici, perciò è necessario usare contemporaneamente diverse tecniche difensive

1. **Sistema di autenticazione a 2 Fattori**
2. **Firewall**
3. **Intrustion detection system**
4. **Backup**
5. **Aggiornamento del CMS e Plug-ins**

RIMEDI per l'integrità dei sistemi e informazioni

TUTTE QUESTE ATTIVITA' SONO REALIZZATE CON:

Firewall per wordpress, in parte gratuito

In particolare sono utili 3 funzioni:

- il robot che funge da IDS
- il blocco da ip in black list
- la brute force protection

Wordfence™
Securing your WordPress website

RIMEDI per l'integrità dei sistemi e informazioni

protocollo SSL sul sito

RIMEDI per l'integrità dei sistemi e informazioni

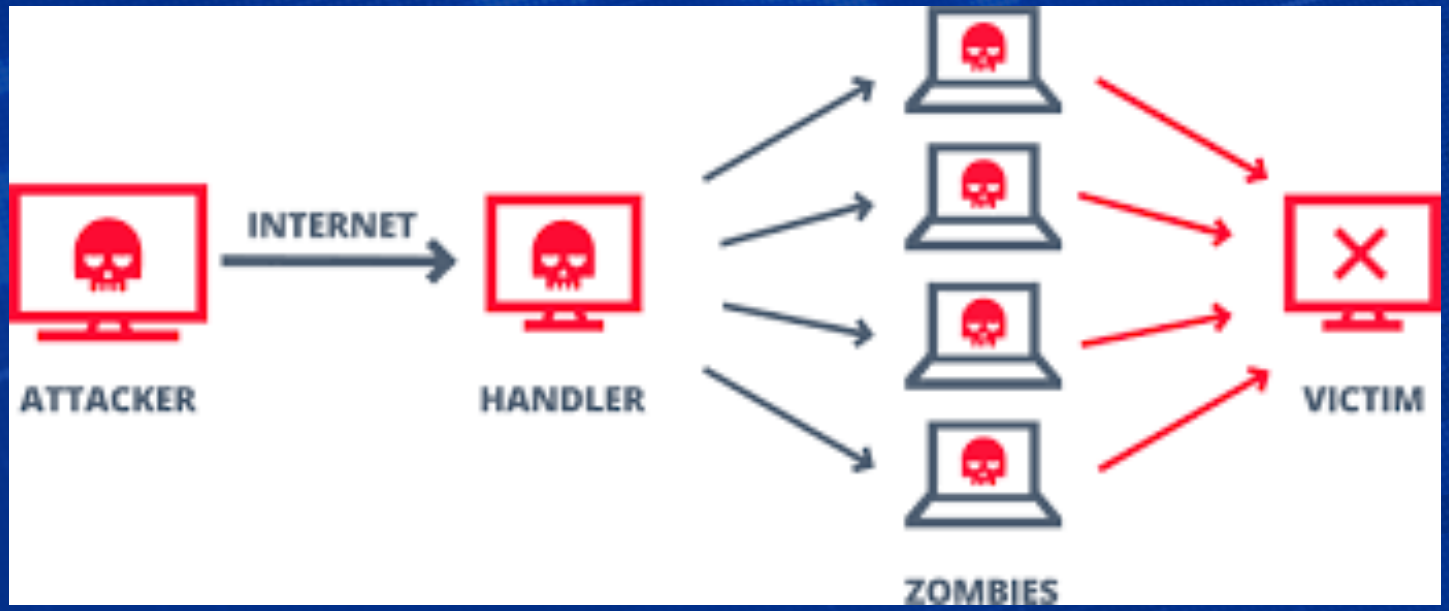
i vari tipi di certificato SSL

- **DV** (validazione a livello di dominio)
- **EV** (Validazione estesa)
- **WILDCARD** (validazione estesa a tutti i sottodomini)

4a Minaccia

Compromissione delle comunicazioni.

Ad esempio, attacco D-dos



RIMEDIO contro il D-DOS

CONTRO L'ATTACCO D-DOS DEVE INTERVENIRE UN FORNITORE DI SERVIZI, come:

HOSTING

CONNETTIVITA'

5a Minaccia

PERDITA INFORMAZIONI (DEL SITO E BACKUP)

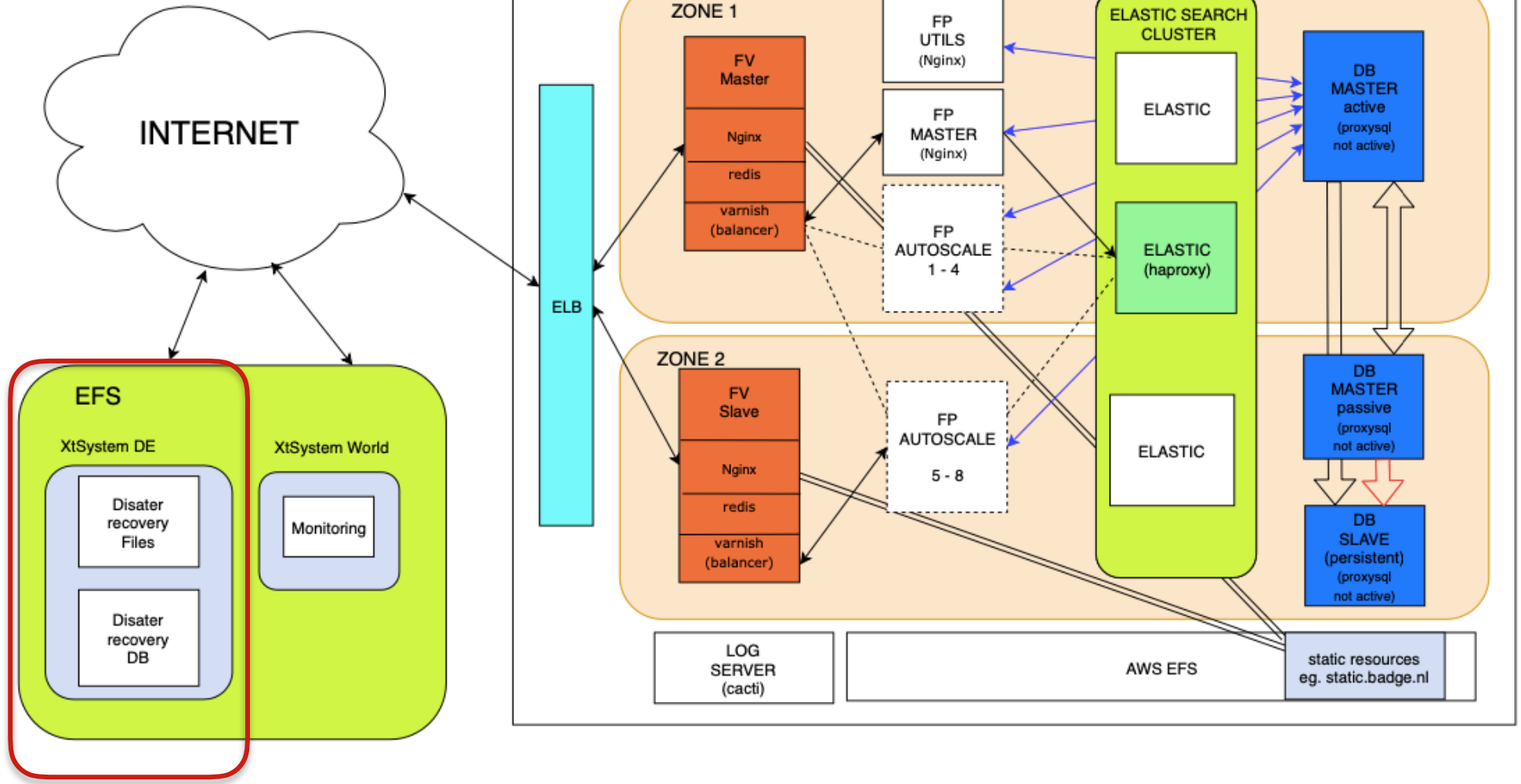
attenzione agli account sul cloud senza un backup esterno o un disaster recovery!

"il 95% dei danni a livello di security è causato dai dipendenti dell'azienda"

RIMEDIO contro la perdita di un sito sul cloud

FARE UN SECONDO BACKUP DI DISASTER RECOVERY FUORI DAL CLOUD

pensareweb
web partner



FacileWP
Multiple Wordpress Managed VPS

ALTRI TOOLS

utili per la protezione dai data breach

FacileWP
Multiple Wordpress Managed VPS

Website Reputation Checker

URLVoid

This service helps you detect potentially malicious websites.

Check the online reputation/safety of a website.

Need to scan an IP address? Try IPVoid

Enter website or URL here

Scan Website

Data submitted here is shared with security companies (terms of use).

FacileWP
Multiple Wordpress Managed VPS

SUCURI
Real People. Real Security.

- analizza se il sito è in una **BlackList,**
- effettua una scansione **Malware**
- individua diverse infezioni presenti in un sito internet

FacileWP
Multiple Wordpress Managed VPS

No Malware Found
Our scanner didn't detect any malware

Site is not Blacklisted
9 Blacklists checked

Scan Info
https://www.pensareweb.it/

IP Address: 213.152.201.120
Host: www.pensareweb.it
Running on: Apache

SUCURI
Real People. Real Security.

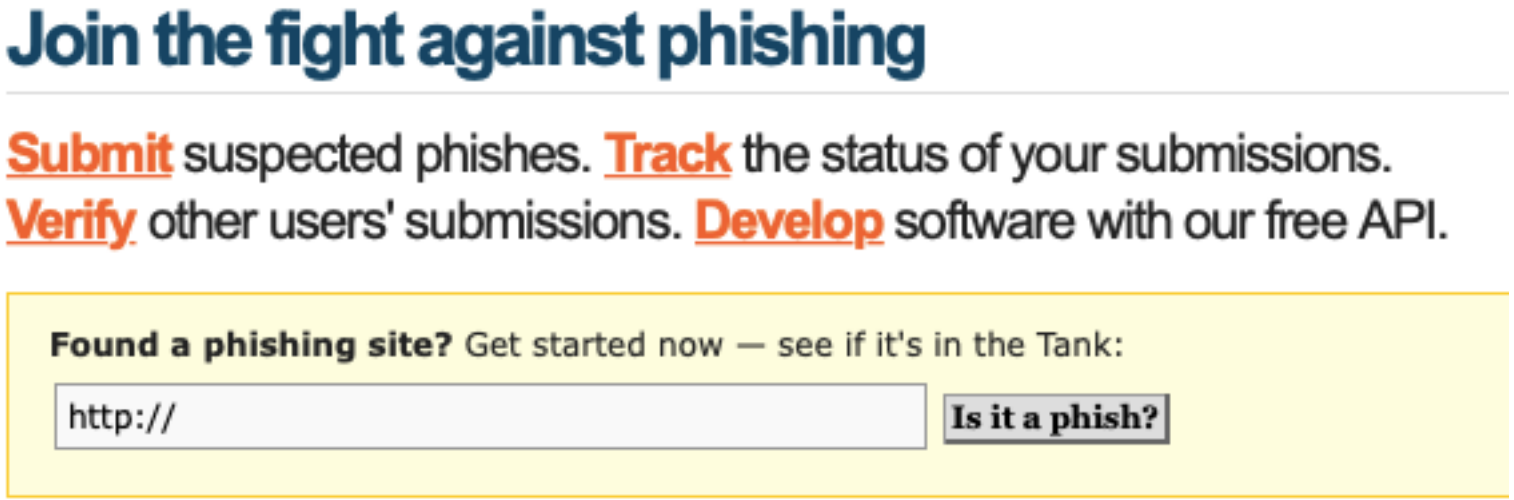
Website Malware & Security

Blacklisted:	NO
Malware:	NO
Malicious javascript:	NO
Malicious iframes:	NO
Drive-By Downloads:	NO
Anomaly detection:	NO
IE-only attacks:	NO
Suspicious redirections:	NO
Blackhat SEO Spam:	NO

Website Blacklist Status

- Domain clean by Google Safe Browsing: www.pensareweb.it - Reference
- Domain clean by Norton Safe Web: www.pensareweb.it - Reference
- Domain clean by McAfee: www.pensareweb.it - Reference
- Domain clean by Sucuri Labs: www.pensareweb.it - Reference
- Domain clean by ESET: www.pensareweb.it - Reference
- Domain clean by PhishTank: www.pensareweb.it - Reference
- Domain clean by Yandex: www.pensareweb.it - Reference
- Domain clean by Opera: www.pensareweb.it - Reference

PhishTank



E’ una community dove verificare e segnalare un sito di phishing

it.TrustPilot.com

FacileWP
Multiple Wordpress Managed VPS

iThemes Security

E’ un alternativa a Wordfence ed è utile per:

- schedulare scansioni di sicurezza di WordPress,
- attivare il reCapcha di Google,
- gestire le password in modo intelligente

Associazione
tezione Diritti e Libe

CONSULENZE PACI PRIVACY

pensare web
web partner

FacileWP
Multiple Wordpress Managed VPS

Fabio Tonti

GRAZIE

www.pensareweb.it
www.facilewp.it