Una PMI vista da un attaccante informatico

Dott. Mauro Andreolini
mauro.andreolini@unimore.it

INTRODUZIONE

Chi sono

([andreoli@UNIMORE ~]$ whoami)

Nome: Mauro Andreolini
Ruolo: Ricercatore Universitario
Passioni:

- Sistemi Operativi.
- Sicurezza Informatica.
- Programmazione.
- CTF.

Le mie esperienze professionali

(CyberChallenge)

Team "HackInMore", 2023

2023-: Responsabile nodo UNIMORE per la CyberChallenge

https://cyberchallenge.it

Responsabilità:

- Organizzazione burocratica.
- Logistica.
- Didattica (frontale e lab.).
- Supporto morale.

Team "HackInMore" , 2024

Le mie esperienze professionali
(Cyber Academy)

2016-: Docente presso la Cyber Academy (Fondazione San Filippo Neri, FIM UNIMORE)

https://cyber.unimore.it/

Corsi:

Sistemi Operativi.

Penetration Testing.

Studenti Cyber Academy, 2018

Le mie esperienze professionali

(Master Cyber Defense presso Scuola Telecomunicazioni FF.AA. Chiavari)

2013-2019: Docente presso il Master “Cyber Defense” presso la Scuola Telecomunicazioni FF.AA. Chiavari (STELMILIT).

Corsi:

- Sistemi Operativi.
- Penetration Testing.

Sede STELMILIT

Le mie esperienze professionali
(Attività di consulenza)

2014-: attività di consulenza per PMI e PA.

- VAPT.
- Red Teaming.
- Blue Teaming.
- Incident Response.

Una premessa
(Doverosa!)

Sono un appassionato di Sicurezza Informatica.

- Non sono un operatore professionista certificato della cyber security.
- Non sono un "hacker" (nell'accezione dei media).

Ciò che segue è ciò che ho visto in oltre dieci anni di consulenza professionale e coaching.

- Your mileage may vary.

Gli ambiti considerati

(10000 feet view)

Nella mia esperienza professionale ho avuto modo di constatare manchevolezze nei seguenti ambiti.

- Infrastruttura.
- Software.
- Gestione dei dati.
- Gestione del personale.

INFRASTRUTTURA

Sistemi obsoleti

(Rendono la violazione del sistema fattibile da attaccanti non esperti)

Osservazione:

uso di sistemi operativi obsoleti in produzione (Windows XP, Windows Server 2003, Ubuntu 10.04).

Giustificazioni:

"il software di controllo dell'attuatore non funziona altrimenti."

Rischio:

violazione del sistema tramite programmi pubblicamente disponibili.

Assenza di asset management

(Semplifica la vita agli attaccanti)

Osservazione:

i sistemi informatici non sono censiti;

spesso esistono sistemi "dimenticati" e vulnerabili.

Giustificazioni:

"quella macchina la uso ogni tanto per fare dei test."

Rischio:

(ab)uso del sistema per raggiungere nuovi asset;

(ab)uso del sistema per trafugare dati.

Assenza di isolamento

(Gli apparati sono raggiungibili tra loro, anche in reti diverse)

Osservazione:

i sistemi informatici non sono opportunamente isolati (segmentazione delle reti)

Giustificazioni:

”tanto il firewall impedisce gli ingressi nel sistema.”

Rischio:

una volta ottenuto accesso ad una macchina, l’attaccante ha spesso visione completa dell’infrastruttura informatica.

→ “Pivoting” nelle reti interne (amministrazione, produzione).

SOFTWARE

Software scritto “in house”

(Mai sottovalutare un amministratore improvvisatosi programmatore)

Osservazione:

i sistemi informatici non sono opportunamente isolati (segmentazione delle reti)

Giustificazioni:

”tanto il firewall impedisce gli ingressi nel sistema.”

Rischio:

una volta ottenuto accesso ad una macchina, l’attaccante ha spesso visione completa dell’infrastruttura informatica.

→ “Pivoting” nelle reti interne (amministrazione, produzione).

GESTIONE DEI DATI

(Mancata) gestione delle password

(Free logins for everyone!)

Osservazione:

le password sono scritte in chiaro su carta (post-it, fogli, diari)

le password sono semplici (**`P4ssw0rd123!`** è un classico)

le password sono usate per più servizi

l'autenticazione multifattore, questa sconosciuta

Giustificazioni:

"così me la ricordo"

Rischio:

una volta ottenute credenziali, l'attaccante accede ad un portafoglio di sottosistemi diversi

(Mancata) gestione dei backup

(Il sogno di ogni ransomware)

Osservazione:

backup? Quali backup?
il sistema che ospita il backup è agganciato all'infrastruttura;
non è mai stato provato un ripristino.

Giustificazioni:

"non ho tempo di guardarci, devo produrre e fatturare"
"il software di backup è costosissimo e funziona benissimo"

Rischio:

in seguito ad un incidente informatico l'azienda rischia di perdere i propri dati (talvolta, purtroppo, per sempre)

(Mancata) cifratura di dati in transito/a riposo

(Il sogno di una spia)

Osservazione:

dati (spesso sensibili) sono trasmessi e memorizzati in chiaro o offuscati in modo invertibile

Giustificazioni:

"non ho tempo di guardarci, devo produrre e fatturare"

Rischio:

un attaccante che ha accesso ai servizi è in grado di ottenere l'intera proprietà intellettuale e informazioni sensibili sui dipendenti (per poi spesso rivenderli al migliore offerente).

GESTIONE DEL PERSONALE

Carenza di igiene informatica
(Personale non IT)

Osservazione:

i dipendenti “non IT” non hanno una cultura di sicurezza e reagiscono infastiditi alle contromisure di prevenzione

Giustificazioni:

”devo lavorare, non ho tempo da perdere”

”toh, un attachment, fammi vedere che cosa contiene”

”oddio, una denuncia, fammi vedere di cosa si tratta”

Rischio:

elevata efficacia degli attacchi di phishing

→ Furto di credenziali, (più raramente) esecuzione di codice

Carenza di igiene informatica
(Personale IT)

Osservazione:

i dipendenti “IT” hanno una cultura di sicurezza di base e reagiscono infastiditi ai collaudi di sicurezza

Giustificazioni:

”questo sistema è aggiornato, perché lo testi?”

”hai testato questo sistema fuori orario, ti segnalo al GARR”

”questo sistema è irraggiungibile, perché lo stati testando?”

Rischio:

elevata probabilità di introduzione di misconfigurazioni nella infrastruttura.

Carenza di igiene informatica
(Dirigenza)

Osservazione:

i dirigenti aziendali vedono la sicurezza come un costo da sostenere e non come una opportunità di investimento.

Giustificazioni:

"la sicurezza non fattura"

Rischio:

la sicurezza fatturerà (in negativo, con cifre a sei zeri) in caso di incidente informatico grave.

CONCLUSIONI

Una riflessione conclusiva
(Siamo sulla strada giusta, ma c'è ancora molto da fare)

La situazione è sensibilmente migliorata dal 2014.

Resta tuttavia ancora molto da fare.

È necessario un **approccio sinergico** tra management e tecnologia.

- Management: implementazione dei processi industriali.
- Tecnologia: adozione delle best practict per garantire funzioni, prestazioni, sicurezza ai sistemi.

L'Università può aiutare in questo processo facendo da trait d'union tra i due mondi.

GRAZIE PER L'ATTENZIONE!