STORIA DI UN CASO REALE

Daniele Romagnoli
IT Architect
PCSNet Marche Srl

Chi siamo

- Nati nel 1994 come società di formazione
- Dal 1999 siamo un Partner ICT a 360°
- Forte partnership con Microsoft
  - Uno dei pochissimi partner con competenze certificate su ambienti Cloud (Azure / Microsoft 365), OnPremise e Formazione
  - Grandi investimenti nella security (Azure AD Premium, Defender for Endpoint, Defender for Office 365, Azure Sentinel, DLP, Azure Site Recovery)
- Gestione di infrastrutture, formazione, sviluppo software
- Focalizzazione su clienti di medie e grandi dimensioni

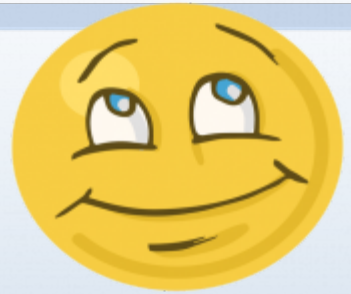
INTRODUZIONE

- Farò una ricostruzione di un caso reale
  - Ripercorrendo le varie fasi dell'attacco …
  - … ma soprattutto per capire cosa avrebbe potuto fare l'azienda
- L'azienda attaccata è una PMI
  - Circa 500 utenti
  - 50 server
  - 6 host di virtualizzazione, sito principale e disaster recovery
  - Circa 30 TB di dati
  - Firewall di ultima generazione

Imparare dagli errori

- Da questo attacco derivano molti spunti di riflessione
- Li abbiamo usati per generare un modello che stiamo proponendo ai nostri clienti
- Applicabile ad aziende di piccole dimensioni o enterprise
- Modello scalabile, da applicare totalmente o in parte
- Mix di software e servizi di consulenza

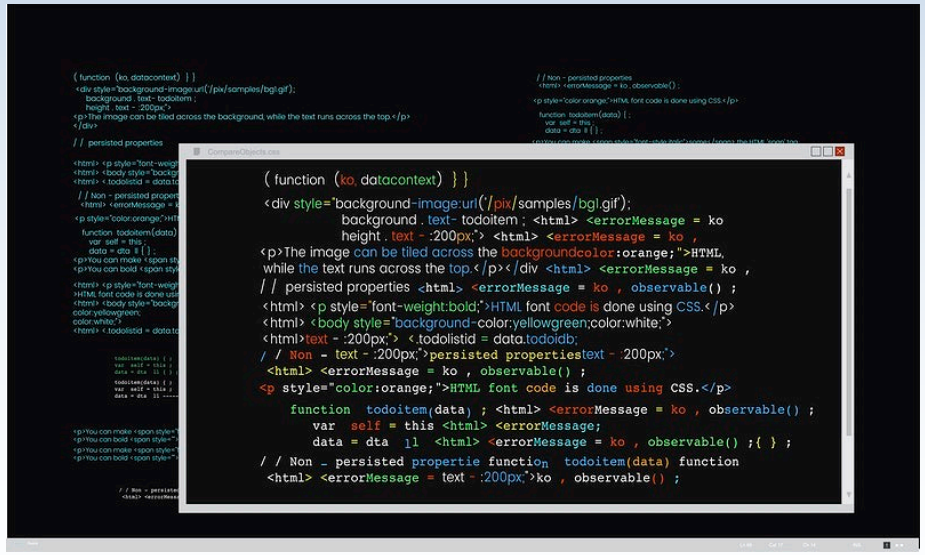
ATTENZIONE!



- Alcune parti di questo racconto possono creare ansia
  - Vi ho avvisati!
- SPOILER ….
  - E’ finita nel migliore dei modi

L'inizio ...

- Telefonata alle 7 del mattino di Domenica ...
  - Utente: «Ciao, abbiamo l'ERP che non ci fa accedere»
  - Admin: «OK, controllo subito»



Come sono entrati

- Classico messaggio di phishing
- Un utente di una sede estera ha abboccato ed inserito le credenziali
- L'utente non ha dato peso all'accaduto
- Con quelle credenziali l'attaccante ha avuto accesso in VPN verso l'azienda

Spunti di riflessione …

- Gli utenti vanno formati!
  - Nessuno darebbe le chiavi di casa al proprio figlio senza dirgli quali sono i rischi!
  - L'utente deve essere consapevole che l'IT deve essere informato in caso di possibili incidenti di sicurezza
- Abbiamo proprio bisogno che la VPN sia sempre attiva?
  - Limitando il periodo di possibile accesso si limitano i rischi

… ancora

- Autenticazione MFA!
  - Al giorno d'oggi non possiamo prescindere dall'autenticazione a più fattori
  - Meglio se con possibilità di analizzare la richiesta (ad esempio se il PC è a dominio, la posizione geografica da cui effettua l'accesso …)
- Sistema Antispam / Antivirus pressoché obbligatorio

Dopo l'ingresso

- Il gruppo di hacker non ha agito subito
  - Ha spiato la rete per diversi giorni
- Ha cercato di individuare i servizi critici
- Ha cercato di individuare i PC degli amministratori IT
  - Alla ricerca di file con le password, ad esempio …
- Ogni tanto ha provato a lanciare qualche script per catturare informazioni

Spunti di riflessione …

- Le connessioni VPN devono avere un limite di tempo
- E’ molto pratico chiamare un server SRV-FILE o SRV-MAIL o SRV-VSPHERE, ma poco sicuro
  - Anonimizziamo i servizi, va bene anche AZ25X89 come nome
- Un sistema SIEM si sarebbe accorto di quanto stava accadendo
- Ancora meglio se in abbinamento con un SOC
- Le password … non mettiamole nei file, usiamo servizi ad hoc

L’attacco

- Gli obiettivi sono stati molteplici
  - Rendere inutilizzabili i sistemi
  - Criptare i file
  - Trafugare dati
- Insomma … fare male

Attacco ai sistemi …

- Prima di tutto i backup …
  - Attaccata la macchina Veeam
  - Cancellati tutti i backup
  - Cancellati i Data Store dalla SAN
- C'è sempre l'Immutable …
  - In parte … hanno individuato le credenziali e cambiato la password per accedere al server
  - I backup nel cloud non sono stati toccati … ma aspettare il recupero di 20 TB di dati nuoce gravemente alla salute

… continua …

- Attacco all'infrastruttura
  - Accesso diretto agli host Vmware
    - Password cambiate
    - Aggiunta di script per la cancellazione dei dischi in caso di spegnimento delle macchine virtuali
  - Accesso al sito di Disaster Recovery
    - Bloccata la replica e manomessi gli host

Spunti di riflessione

- Gli strumenti di management NON DEVONO essere accessibili dalla rete client
  - E’ comodo accedere a tutti i tool dal proprio PC, ma molto pericoloso
  - Segmentazione della rete!!!
- Anche per gli strumenti di amministrazione utilizzare la MFA
- Usare una tecnologia di Disaster Recovery differente da quelle già in uso (e magari in cloud)

Criptare i file e trafugare dati

- Sono stati lanciati i classici Ransomware
- Lanciati script per prelevare dati dai file server e spedirli a siti remoti

Spunti di riflessione (poi basta)

- I classici antivirus non bastano più
  - Bisogna dotarsi di un sistema XDR
  - Che ci avrebbe aiutato anche ad individuare i primi movimenti sospetti
- L'accesso verso Internet è necessario che sia sempre attivo?

Quindi ???

- Quindi l'azienda era totalmente down … L'attaccante ha raggiunto il suo obiettivo!
- Ma …
  - C'erano ancora gli snapshot della SAN!

- SPUNTO DI RIFLESSIONE:
  - Fare attenzione alla configurazione degli snapshot, tenere gli snapshot per diversi giorni!

Veloce recap (in ordine sparso)

- MFA per VPN e strumenti di management
- Limitare gli orari di VPN ed uscita Internet
- Dotarsi di un sistema XDR
- Aumentare la retention degli snapshot della SAN
- Segmentazione della rete
- Disaster Recovery cloud
- Naming convention complessa per i servizi
- Dotarsi di un SIEM
- Dotarsi di un NOC
- Formazione degli utenti

Microsoft GOLD CERTIFIED Partner

GRAZIE!

Bit servizi e formazione PCS net MARCHE