Mitigation and Remediation

Per l'esercitazione odierna viene immaginato uno scenario in cui il nostro compito sarà quello di comprendere le fasi di mitigation e remediation di due minacce comuni, quali **phishing** ed attacchi **DoS**.

Primo Scenario

Amministratori di sicurezza peer una media azienda, abbiamo scoperto una campagna di phishing mirata ai dipendenti dell'azienda, in cui vengono inviate email fraudolente che sembrano provenire da fonti affidabili.

Nell'agire nei confronti di questa minaccia, verranno utilizzati 5 punti fondamentali.

1. Identificazione della minaccia

Prima di poter agire bisogna comprendere con cosa si ha a che fare. In questo caso si parlerà di un attacco phishing, ma cos'è esattamente?

Il **phishing** è una tecnica di attacco informatico in cui un possibile attaccante invia mail, messaggi o utilizza metodi di comunicazione (chiamate con modificatore di voce ad esempio) che sembrano provenire da fonti affidabili, riuscendo quindi a trarre la vittima in inganno.

L'obiettivo sarà quello di indurre la vittima a fornire credenziali di accesso, divulgare informazioni sensibili, oppure scaricare malware attraverso link o allegati.

2. Analisi del rischio

In caso di questi possibili scenari, un attacco phishing potrebbe quindi sfruttare le credenziali di accesso dei dipendenti per intrufolarsi nei sistemi aziendali, e quindi poter potenzialmente caricare **malware** (o anche ransomware o altre tipologie di malware), **causare perdite finanziarie** o ancora **esporre informazioni sensibili** dell'azienda stessa o dei clienti.

Per fare un esempio tangibile, se dovesse essere caricato un ransomware ad esempio, si potrebbero bloccare i sistemi critici, criptando qualunque cosa per poi chiedere un riscatto, dopo il quale, si potrebbe comunque non ricevere alcuna chiave di decriptazione. Oltre il danno la beffa.

Una lista di risorse compromettibili potrebbe essere:

- **Credenziali di accesso (email, sistemi interni).**
- **Dati aziendali sensibili (strategie, documenti riservati).**
- **Dati personali di dipendenti e clienti.**

- **Sistemi critici, come ERP o CRM.**

3. **Pianificazione della Remediation**

È quindi bene studiare un piano di **Remediation** che sia efficace e possa salvaguardare l'azienda da questa problematica. Per quanto l'anello più debole sia proprio l'essere umano si può comunque adoperare una soluzione che possa attenuare il problema.

La prima cosa da fare è **informare i dipendenti dell'accaduto**, fornendo **istruzioni** su come agire e distribuendo linee guida al fine di poter riconoscere possibili tentativi di phishing, come ad esempio controllare se siano stati passati i controlli di **SPF, DKIM e DMARC**.

Un'altra cosa da fare è **implementare filtri anti spam** ed analizzare le intestazioni delle email sospette bloccando quindi gli IP sorgente una volta identificati.

Controllare i log dei sistemi in modo da individuare eventuali accessi anomali od attività sospette, ed isolare eventuali dispositivi compromessi per **limitare** la diffusione dell'attacco.

4. I**mplementazione della Remediation**

Al fine di attuare il piano di Remediation, si passa quindi all'implementazione dei punti sopra citati, formando quindi anzitutto il personale, avviando un programma di sensibilizzazione mostrando loro come riconoscere email di phishing.

Nota bene è verificare che **SPF DMARK e DKIM**, citati precedentemente siano correttamente attivi.

Altro punto altrettanto importante quello **di aggiornare le policy di sicurezza**, imponendo regole più rigide sulle password, nonché la **MFA**; è inoltre opportuno che tutti i dipendenti abbiano i permessi minimi, adatti a svolgere una specifica mansione, in modo da limitare l'accesso ai dati sensibili.

5. Mitigazione dei Rischi Residuali

Al fine di limitare al minimo i danni e prevenire eventuali future problematiche, è possibile effettuare dei **test di phishing simulati**, in modo da verificare se effettivamente il personale rispetta le regole e si attiene ai concetti che sono stati loro spiegati.

È nota bene anche assicurarsi che le **ultime patch** (dopo aver effettuato un collaudo in sandbox) siano tutte installate, ed ottima abitudine, è quella di eseguire **backup regolari**, in modo da avere sempre un piano B in caso di problematiche varie.

Attacchi DoS

1. Definizione

Un attacco **Dos** (**Denial of Service**) per definizione è un attacco che mira a rendere i servizi aziendali inaccessibili, sovraccaricando i server con richieste false o esagerate.

Un attacco **DoS è in grado di bloccare i servizi online**, causando **interruzioni** delle attività aziendali, rendendo **inaccessibili sistemi critici**, nonché possibili perdite di entrate, finanziarie, o danni reputazionali.

2. Analisi del Rischio

L'impatto di un attacco DoS può essere catastrofico, e causare seri danni all'interno dell'azienda. Alcuni punti fortemente impattati da un simile attacco possono essere **mancati accessi ai sistemi sia per i clienti che per i dipendenti**, o ancora, seri danni alla **fiducia** della stessa clientela, questo soprattutto, se i tempi in cui i server saranno down, verranno protratti.

I servizi maggiormente compromettibili sono quindi server web ed applicazioni aziendali, ma altrettanto lo sono Database e sistemi di comunicazione interni.

3. Piano di remediation

È impossibile prevenire un attacco DoS, ma è comunque possibile controbattere o preparare delle contromisure.

Anzitutto c'è bisogno di **analizzare i log** per tracciare l'IP o gli IP sorgenti dell'attacco.

È bene inoltre stabilire all'interno del firewall delle **regole precise** in modo da limitare il traffico in arrivo. Implementare **IDS** ed **IPS** è anche un ottimo punto da considerare

Successivamente come risposta è possibile implementare tecnologie di r**ate-limiting**, e, fortemente consigliato, utilizzare la tecnica del **bilanciamento dl carico**.

Altre possibili soluzioni possono essere utilizzare servizi come **Cloudflare**, o **AWS shield**, parlando quindi di **Cloud**, uno dei pilastri informatici.

4. Implementazione della Remediation

Nell'implementare quindi il piano di remediation, è quindi opportuno considerare le possibili soluzioni sopra citate, quindi parlando di bilanciamento del carico, cloud e l'implemento di sistemi anti intrusione **IDS/IPS**, ed implementarle.

5. Mitigazione dei rischi residuali

In seguito all'implemento selle soluzioni sopra considerate, è bene continuare a **monitorare costantemente il traffico** mediante l'ausilio di strumenti di analisi appositi.

È inoltre possibile **simulare un attacco DoS** in modo da verificare le capacità di difesa della nostra rete, effettuando quindi un test di resilienza.

Ultima ma non per importanza è bene coinvolgere il team di sicurezza per implementare **soluzioni proattive.**