S11L1

Data: 09/12/24

INFORMAZIONI PRINCIPALI

Esercizio di oggi: Remediation e Mitigazione di Minacce di Phishing e Attacchi DoS

Parte 1: Minaccia di Phishing

Scenario

Immagina di essere un amministratore di sicurezza per una media azienda che ha scoperto una campagna di phishing mirata contro i propri dipendenti. Gli attaccanti inviano email fraudolente che sembrano provenire da fonti affidabili, inducendo i dipendenti a divulgare informazioni sensibili o a scaricare malware.

Istruzioni

1. **Identificazione della Minaccia:**
   - Ricerca e documenta cos'è il phishing e come funziona.
   - Spiega come un attacco di phishing può compromettere la sicurezza dell'azienda.
2. **Analisi del Rischio:**
   - Valuta l'impatto potenziale di questa minaccia sull'azienda.
   - Identifica le risorse che potrebbero essere compromesse (ad es. credenziali di accesso, informazioni sensibili, dati aziendali).

Esercizio di oggi: Remediation e Mitigazione di Minacce di Phishing e Attacchi DoS

Parte 1: Minaccia di Phishing

3. **Pianificazione della Remediation:**
   - Sviluppa un piano per rispondere all'attacco di phishing. Il piano dovrebbe includere:
     - Identificazione e blocco delle email fraudolente.
     - Comunicazione ai dipendenti sull'attacco e sulle misure da adottare.
     - Verifica e monitoraggio dei sistemi per individuare eventuali compromissioni.
4. **Implementazione della Remediation:**
   - Descrivi i passaggi pratici che intraprenderesti per mitigare la minaccia di phishing. Questo potrebbe includere:
     - Implementazione di filtri anti-phishing e soluzioni di sicurezza email.
     - Formazione dei dipendenti su come riconoscere e segnalare tentativi di phishing.
     - Aggiornamento delle policy di sicurezza aziendali.
5. **Mitigazione dei Rischi Residuali:**
   - Identifica misure di mitigazione da implementare per ridurre il rischio residuo, come:
     - Esecuzione di test di phishing simulati per valutare la reattività dei dipendenti.
     - Implementazione di autenticazione a due fattori (2FA) per l'accesso ai sistemi critici.
     - Regolari aggiornamenti e patching dei sistemi per ridurre le vulnerabilità sfruttabili.

Esercizio di oggi: Remediation e Mitigazione di Minacce di Phishing e Attacchi DoS

Parte 2: Attacco DoS (Denial of Service)

Scenario

Immagina di essere un amministratore di sistema per una media azienda che ha subito un attacco DoS (Denial of Service). Gli attaccanti inondano i server aziendali di richieste, rendendo i servizi web inaccessibili agli utenti legittimi.

Istruzioni

1. **Identificazione della Minaccia:**
   - Ricerca e documenta cos'è un attacco DoS e come funziona.
   - Spiega come un attacco DoS può compromettere la disponibilità dei servizi aziendali.
2. **Analisi del Rischio:**
   - Valuta l'impatto potenziale di questa minaccia sull'azienda.
   - Identifica i servizi critici che potrebbero essere compromessi (ad es. server web, applicazioni aziendali).
3. **Pianificazione della Remediation:**
   - Sviluppa un piano per rispondere all'attacco DoS. Il piano dovrebbe includere:
     - Identificazione delle fonti dell'attacco.
     - Mitigazione del traffico malevolo.

Esercizio di oggi: Remediation e Mitigazione di Minacce di Phishing e Attacchi DoS

Parte 2: Attacco DoS (Denial of Service)

4. **Implementazione della Remediation:**
   - Descrivi i passaggi pratici che intraprenderesti per mitigare la minaccia di DoS. Questo potrebbe includere:
     - Implementazione di soluzioni di bilanciamento del carico per distribuire il traffico.
     - Utilizzo di servizi di mitigazione DoS offerti da terze parti.
     - Configurazione di regole firewall per bloccare il traffico sospetto.
5. **Mitigazione dei Rischi Residuali:**
   - Identifica misure di mitigazione da implementare per ridurre il rischio residuo, come:
     - Monitoraggio continuo del traffico di rete per rilevare e rispondere rapidamente a nuovi attacchi.
     - Collaborazione con il team di sicurezza per migliorare le difese contro DoS.
     - Test periodici di resilienza per valutare l'efficacia delle misure di mitigazione adottate.

Documentazione e Report

- Compila un report che includa:
  - Descrizione delle minacce di phishing e DoS.
  - Analisi del rischio per entrambe le minacce.
  - Piano di remediation dettagliato per entrambe le minacce.
  - Misure di mitigazione adottate per entrambe le minacce.

7

Wireshark che cattura un attacco Dos:

No.	Time	Source	Destination	Protocol	Length	Info
1	2024-07-19 06:51:17.946205	192.168.1.1	10.0.0.1	TCP	60	DoS attack packet
2	2024-07-19 06:51:18.946205	192.168.1.2	10.0.0.1	TCP	60	DoS attack packet
3	2024-07-19 06:51:19.946205	192.168.1.1	10.0.0.1	TCP	60	DoS attack packet
4	2024-07-19 06:51:20.946205	192.168.1.2	10.0.0.1	TCP	60	DoS attack packet
5	2024-07-19 06:51:21.946205	192.168.1.1	10.0.0.1	TCP	60	DoS attack packet
6	2024-07-19 06:51:22.946205	192.168.1.2	10.0.0.1	TCP	60	DoS attack packet
7	2024-07-19 06:51:23.946205	192.168.1.1	10.0.0.1	TCP	60	DoS attack packet
8	2024-07-19 06:51:24.946205	192.168.1.2	10.0.0.1	TCP	60	DoS attack packet
9	2024-07-19 06:51:25.946205	192.168.1.1	10.0.0.1	TCP	60	DoS attack packet
10	2024-07-19 06:51:26.946205	192.168.1.2	10.0.0.1	TCP	60	DoS attack packet

INDICE

1. **INTRODUZIONE E TRACCIA.....PAG.1**
2. **INDICE.....PAG.2**
3. **Phishing and the “path” Taken.....PAG.3**
4. **DoS (TCP FLOOD).....PAG.**
5. **Report.....PAG.**

IDENTIFICAZIONE DELLA MINACCIA

Iniziamo con il dire che il Phishing èun attacco in cui l'aggressore invia e-mail "fraudolente", mascherandosi da entità (o vendors) affidabili, per ingannare le vittime e rubare dati sensibili come credenziali o informazioni personali e può compromettere la sicurezza aziendale, portando al furto di dati critici, perdita economica e danni reputazionali.

ANALISI DI RISCHIO

Per valutare "l'impatto" possiamo dire che gli attacchi (Phishing) possono influire negativamente sulla produttività aziendale e sul rapporto di fiducia con i clienti (Ri-formazione del personale on-demand ma il danno reputazionale ormai è andato.)
Gli asset invece vulnerabili dell'azienda sono vari, tra cui Le credenziali dei dipendenti, i dati finanziari e le informazioni sensibili relative a clienti o progetti. (variando di criticità, for example se ci rubano la lista di quando viene il ragazzo a rimettere la roba nella macchinetta, non sarà critico quanto le informazioni personali dei clienti).

PIANIFICAZIONE DELLA REMEDIATION

Uno degli obbiettivi principali della remediation è prevenire i tentativi di phishing educando i dipendenti e implementando strumenti di protezione.

Come azioni possiamo fare Simulazioni di phishing per testare la "consapevolezza" dei dipendenti e la configurazione di filtri per bloccare e-mail sospette.

IMPLEMENTAZIONE DELLA REMEDIATION

Come interventi possiamo usare (ed aggiornare) dei sistemi di posta elettronica con dei filtri anti-phishing avanzati. Questi, utilizzano tecnologie come il machine learning e l'analisi comportamentale per identificare e bloccare e-mail sospette. Analizzano contenuti, allegati, URL e metadati per rilevare tentativi di phishing in tempo reale.

Inoltre, introdurre i dipendenti all'autenticazione multi-fattore (MFA) per ridurre i rischi di compromissione non è mai una brutta idea.

Lastly but not least, organizzare "workshop" per insegnare a riconoscere e segnalare le e-mail sospette.

MITIGAZIONE RISCHIO RESIDUO

Per la mitigazione del rischio residuo possiamo monitorare in modo continuo le attività sospette (sui sistemi di posta elettronica) e utilizare strumenti di analisi dei link per prevenire i click su URL dannosi. (anche virustotal per gli URL as an example o plugin sul browser, come addon)

E per finire i "Fornitori" possono fornire soluzioni come sistemi SIEM (Security Information and Event Management) o EDR (Endpoint Detection and Response) per identificare rapidamente attività sospette e attacchi di phishing, inoltre garantiscono che gli strumenti siano sempre aggiornati con le ultime "definitions" delle minacce, aiutando a rilevare anche i nuovi attacchi o varianti di phishing ancora non conosciute.

ESERCIZIO 2: REMEDIATION E MITIGAZIONE DI ATTACCHI DOS (TCP FLOOD)

L’esercizio 2 evidenzia un attacco DOS (TCP Flood) e parte con l'aggressore che invia una grande quantità di richieste TCP SYN al server. L'obiettivo è esaurire le risorse del server e renderlo inaccessibile. Durante l'attacco, l'aggressore non completa mai l'handshake TCP (cioè non invia mai il pacchetto finale ACK). In alcuni casi, l'aggressore può inviare un pacchetto RST/ACK dopo il SYN/SYN-ACK, interrompendo il processo di handshake, per poi ripetere il ciclo sulla stessa porta e con il protocollo TCP.

Può causare il blocco dei servizi essenziali alla business continuity, anche critici. L’azienda potrebbe perdere parecchio fatturato se il server non funziona, ergo i clienti non comprano sul sito (in caso di banca o di servizi più “specifici” ci può essere anche un danno reputazioale in quanto il cliente non potrà ritirare i soldi magari, o effettuare un bonifico.)

ANALISI DEL RISCHIO

I target dell’attacco di solito sono i server “critici” come web server, applicazioni aziendali o sistemi di “gestione” (AS400) necessari alla business continuity e per la valutazione dell’impatto, guardiamo i servizi interrotti e la difficoltà per i clienti (come detto prima) ma anche per i dipendenti a completare determinate “azioni”.

PIANIFICAZIONE DELLA REMEDATION

Gli obbiettivi principali sono ridurre l’impatto dell’attacco proteggendo l’infrastruttura e migliorando la “resilienza” della nostra rete. Possiamo iniziare con il configurare il Firewall per limitare l’accesso (Blocco di indirizzo ip/porta attaccata se non necessaria alla business continuity example, perchè telnet è aperta se non la stiamo usando?) Inoltre un sistema di mitigazione DOS come load balancer o strumenti anti-DDOS come CloudFare che offre non solo load balancing, ma anche tecniche di filtraggio per separare le richieste legittime da quelle “malevole”.

IMPLEMENTAZIONE DELLA REMEDIATION

Possiamo appunto Identificare gli IP responsabili e bloccarli tramite firewall e Filtrare le porte non necessarie o usate per l'attacco (like we said before) e possiamo configurare un rate limit per limitare il numero di connessioni da ogni IP (max 1) o usare tecnologie come cloudfare che funzionano da scrubbing center. (filtrano i pacchetti e ri-mandano solamente quelli validi)

MITIGAZIONE DEL RISCHIO RESIDUO

Implementare sistemi di monitoraggio continui come IDS E IPS aiutano molto per rilevare attività sospette in tempo reale. La differenza è che uno avverte e basta, mentre l'altro può anche "agire". Un integrazione con SIEM (Security Information and Event Management) per aggregare i dati provenienti da più fonti in un sistema centralizzato (per una visione d'insieme) per facilitare l'analisi e la risposta immediata. Sia di revisione su LOG o in "live".

Per finire possiamo lavorare con il nostro fornitore del servizio internet (ISP) per mitigare gli attacchi a monte (Ogni ISP offre soluzioni diverse,Implementazione di soluzioni DDoS Blocco degli IP sospetti e Filtraggio a monte prima che arrivano al nostro server)

Report

Phishing:

- **Descrizione:** L'attacco mirava a compromettere le credenziali aziendali.
- **Azioni:** Implementati filtri avanzati, MFA e programmi di formazione per il personale.

Le misure adottate hanno ridotto il rischio di phishing, migliorando la consapevolezza e la resilienza.

DoS (TCP Flood):

- **Descrizione:** Attacco TCP flood identificato dai log (di rete)
- **Azioni:** Regole firewall configurate, load balancing, rate limiting e collaborazione con l'ISP per bloccare l'origine dell'attacco (e possibile integrazione con un SIEM per una continua analisi.

La combinazione di soluzioni tecniche e collaborazione con partner esterni ha ridotto l'impatto e migliorato la protezione per eventi futuri.