Rapporto sulla Minaccia di Phishing

1. Identificazione della Minaccia

Descrizione del Phishing:

Il phishing è una tecnica di attacco informatico in cui gli aggressori utilizzano email, messaggi o siti web ingannevoli per indurre le persone a rivelare informazioni sensibili, come credenziali di accesso, dati finanziari o informazioni personali. Gli attacchi di phishing spesso imitano entità fidate, come colleghi, fornitori o istituzioni ufficiali, per creare un senso di urgenza o legittimità.

Come Funziona il Phishing:

1. Preparazione dell'Attacco: Gli aggressori progettano email o siti web fraudolenti che sembrano legittimi.
2. Consegna: Queste email vengono inviate agli individui bersaglio, spesso con link o allegati dannosi.
3. Interazione: Le vittime cliccano sui link o scaricano gli allegati, compromettendo inconsapevolmente i loro sistemi o fornendo informazioni sensibili.
4. Esfiltrazione: I dati rubati vengono utilizzati per accedere ad account, distribuire malware o condurre ulteriori attacchi.

Impatto sulla Sicurezza Aziendale:

- Accesso non autorizzato a sistemi o reti.
- Furto di dati aziendali sensibili o credenziali dei dipendenti.
- Distribuzione di malware o ransomware nella rete.
- Perdite finanziarie dovute a frodi o violazioni di dati.
- Danni reputazionali e perdita di fiducia da parte dei clienti.

2. Analisi del Rischio

Impatto Potenziale:

- Perdite Finanziarie: Furto diretto di denaro o costi relativi alla gestione della violazione.
- Interruzione Operativa: Tempi di inattività causati da ransomware o sistemi compromessi.
- Conseguenze Legali: Mancato rispetto delle normative sulla protezione dei dati (es. GDPR, HIPAA).
- Danni Reputazionali: Perdita di fiducia tra clienti, partner e dipendenti.

Asset Compromettibili:

- Credenziali di accesso dei dipendenti.
- Dati sensibili dei clienti (es. PII, dettagli di pagamento).

- Informazioni proprietarie aziendali (es. segreti commerciali).
- Registri finanziari e informazioni contabili.
- Accesso a sistemi e database interni.

3. Pianificazione della Remediation

Piano per Rispondere all'Attacco di Phishing:

1. Identificazione e Blocco delle Email Fraudolente:
   - Implementare soluzioni di filtro email in tempo reale.
   - Utilizzare feed di intelligence per bloccare domini e IP di phishing noti.
   - Monitorare e mettere in quarantena le email sospette per ulteriori ispezioni.

2. Comunicazione con i Dipendenti:
   - Inviare avvisi immediati ai dipendenti sulla campagna di phishing.
   - Fornire esempi di email fraudolente per aiutare i dipendenti a identificarle.
   - Istruire i dipendenti sui passaggi da seguire in caso sospettino un'email dannosa (es. segnalarla all'IT).

3. Test e Monitoraggio dei Sistemi:
   - Condurre scansioni approfondite per identificare indicatori di compromissione (IoC).
   - Utilizzare sistemi SIEM (Security Information and Event Management) per monitorare attività sospette.
   - Verificare gli account degli utenti per tentativi di accesso non autorizzati.

4. Implementazione della Remediation

Passaggi Pratici per Mitigare la Minaccia:

1. Misure Tecniche:
   - Distribuire soluzioni avanzate di sicurezza email e anti-phishing (es. SPF, DKIM, DMARC).
   - Abilitare l'analisi degli URL e la scansione degli allegati nei sistemi email.
   - Configurare firewall per bloccare il traffico dannoso.

2. Educazione dei Dipendenti:
   - Condurre sessioni di formazione obbligatorie sulla consapevolezza del phishing.
   - Condividere suggerimenti per identificare le email di phishing (es. controllare gli indirizzi dei mittenti, evitare link sospetti).
   - Fornire un canale dedicato per segnalare email sospette.

3. Aggiornamenti delle Politiche:
   - Applicare politiche di password robuste e richiedere aggiornamenti regolari.
   - Aggiornare le politiche di sicurezza per affrontare minacce come il phishing e l'ingegneria

sociale.
- Limitare i permessi degli utenti per minimizzare i danni potenziali in caso di compromissione degli account.

5. Mitigazione dei Rischi Residui

Mitigazioni Aggiuntive:

1. Test Simulati di Phishing:
- Condurre regolari simulazioni di phishing per valutare la consapevolezza dei dipendenti.
- Utilizzare i risultati per personalizzare le future sessioni di formazione.

2. Autenticazione a Due Fattori (2FA):
- Richiedere l'autenticazione a due fattori per accedere a tutti i sistemi e dati critici.
- Utilizzare token hardware o app di autenticazione per maggiore sicurezza.

3. Aggiornamenti e Patch di Sistema:
- Assicurarsi che tutti i sistemi, software e dispositivi siano aggiornati con le ultime patch di sicurezza.
- Rivedere regolarmente e affrontare le vulnerabilità nell'infrastruttura aziendale.

Rapporto sull'Analisi e Mitigazione di un Attacco DoS

1. Analisi Wireshark dell'attacco DoS

Dalle acquisizioni Wireshark:

1. L'attacco è stato condotto utilizzando pacchetti TCP ripetuti che prendevano di mira il server in 10.0.0.1.
2. Sono state coinvolte nell'attacco più fonti (192.168.1.1 e 192.168.1.2), ciascuna delle quali inviava pacchetti identici a intervalli brevi.
3. I pacchetti avevano una dimensione uniforme di 60 byte, coerente con i tipici modelli di attacco DoS.

Osservazioni:

1. Volume di traffico elevato:

   Un flusso continuo di pacchetti ha travolto il server di destinazione.

2. Fonti multiple:

   Indica una natura distribuita dell'attacco (caratteristiche simili a DDoS).

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

2. Descrizione della Minaccia DoS

Un attacco Denial of Service (DoS) è un tentativo malevolo di rendere inaccessibili servizi o risorse di rete sovraccaricando un server, un'applicazione o una rete con un volume

eccessivo di richieste. Questo sovraccarico causa rallentamenti significativi o l'inaccessibilità totale dei servizi legittimi per gli utenti.

L'attacco DoS catturato tramite Wireshark mostra una serie di pacchetti TCP inviati in modo continuo da due indirizzi IP (192.168.1.1 e 192.168.1.2) verso un singolo obiettivo (10.0.0.1). Ogni pacchetto ha una lunghezza di 60 byte ed è classificato come "DoS attack packet".

3. Analisi del Rischio

Impatti Potenziali:

1. L'inaccessibilità del server compromette le operazioni aziendali quotidiane.

2. I clienti potrebbero non essere in grado di accedere ai servizi online, causando una perdita di ricavi.

3. L'incapacità di rispondere agli attacchi potrebbe ridurre la fiducia dei clienti.

Servizi Critici Compromessi:

1. Server Web: Potenziale perdita di accesso ai siti aziendali.

2. Applicazioni Aziendali: Interruzioni delle applicazioni interne ed esterne utilizzate da dipendenti e clienti.

4. Piano di Remediation

Identificazione delle Fonti:

Utilizzando Wireshark, sono stati identificati i seguenti IP come sorgenti dell'attacco:

- 192.168.1.1

- 192.168.1.2

Mitigazione del Traffico Malevolo:

1. Filtraggio degli IP: Configurare regole firewall per bloccare il traffico proveniente dagli IP identificati.

2. Limitazione della Larghezza di Banda: Impostare limitazioni di banda per prevenire ulteriori sovraccarichi.

5. Implementazione della Remediation

1. Soluzioni di Bilanciamento del Carico: Implementare un bilanciatore di carico per distribuire il traffico in arrivo su più server.

2. Servizi di Mitigazione DoS di Terze Parti: Utilizzare soluzioni come Cloudflare per proteggere i server.

3. Configurazione del Firewall:

- Bloccare gli IP identificati.

- Configurare regole per rilevare modelli di traffico sospetti.

6. Mitigazione dei Rischi Residui

1. Monitoraggio Continuo: Impiegare strumenti di monitoraggio della rete per identificare rapidamente nuovi attacchi.

2. Collaborazione con il Team di Sicurezza: Migliorare le difese contro attacchi futuri.

3. Test di Resilienza Periodici: Valutare regolarmente l'efficacia delle misure di mitigazione adottate.