

Phishing e DoS

Remediation e Mitigazione di Minacce di Phishing

🌟 Tag: #sicurezza #cybersecurity #phishing #remediation
#mitigazione

1. Identificazione della Minaccia

🌟 Tag: #phishing #vulnerabilità #emailFraudolente

- **Cos'è il phishing e come funziona:**

Il phishing è una tecnica di attacco che sfrutta email fraudolente per indurre le vittime a rivelare informazioni sensibili (come credenziali, dati personali) o a scaricare malware. Spesso, gli attaccanti si spacciano per enti affidabili, utilizzando tecniche di social engineering per convincere i destinatari ad agire rapidamente.

- **Come un attacco di phishing può compromettere la sicurezza dell'azienda:**

Un attacco di phishing può compromettere la sicurezza aziendale esponendo credenziali di accesso, consentendo l'installazione di malware o ransomware, o facilitando il furto di dati sensibili. Questo può portare a perdita di dati aziendali, interruzione dei servizi, e danni reputazionali.

2. Analisi del Rischio

🌟 Tag: #analisiDelRischio #impatto #risorseCompromesse

- **Impatto potenziale sull'azienda:**

La compromissione derivante dal phishing può avere un impatto devastante, inclusi: furto di dati sensibili, violazioni della privacy, danni finanziari, perdita di clienti e multe per la non conformità alle normative di protezione dei dati.

- **Risorse compromesse:**

1. **Credenziali di accesso:** Utilizzate dagli attaccanti per ottenere accesso non autorizzato ai sistemi aziendali.
 2. **Informazioni sensibili:** Dati riservati come informazioni finanziarie, progetti aziendali, dati personali dei dipendenti.
 3. **Dati aziendali:** Documenti, progetti e informazioni critiche che possono essere rubati o manipolati.
-

3. Pianificazione della Remediation



Tag:

#remediation

#phishing

#rispostaAllAttacco

- **Piano di risposta all'attacco di phishing:**

1. **Identificazione e blocco delle email fraudolente:** Utilizzare soluzioni di sicurezza email che identificano e bloccano email sospette o contenenti link/malware malevoli.
 2. **Comunicazione ai dipendenti:** Informare rapidamente i dipendenti riguardo all'attacco e le misure di sicurezza da seguire, come non cliccare su link sospetti o non fornire informazioni personali.
 3. **Verifica e monitoraggio:** Eseguire scansioni di sicurezza per identificare eventuali compromissioni nei sistemi e controllare attività sospette.
-

4. Implementazione della Remediation

 **Tag:** [#implementazione](#) [#mitigazione](#) [#phishing](#)

- **Passaggi pratici per mitigare la minaccia di phishing:**
 1. **Implementazione di filtri anti-phishing:** Attivare soluzioni di sicurezza come gateway email che analizzano il contenuto delle email e bloccano quelle sospette.
 2. **Formazione dei dipendenti:** Avviare sessioni di formazione regolari per educare i dipendenti su come identificare tentativi di phishing e come segnalarli al dipartimento IT.
 3. **Aggiornamento delle policy di sicurezza:** Rivedere e aggiornare le policy di sicurezza esistenti per includere misure specifiche di difesa contro gli attacchi di phishing, come l'obbligo di segnalare email sospette.
-

5. Mitigazione dei Rischi Residuali

 **Tag:** [#mitigazione](#) [#rischioResiduo](#) [#phishingSimulato](#)

- **Misure di mitigazione:**
 1. **Test di phishing simulati:** Condurre regolarmente campagne di phishing simulate per valutare la prontezza dei dipendenti e migliorare la risposta agli attacchi reali.
 2. **Autenticazione a due fattori (2FA):** Implementare 2FA per tutti gli accessi ai sistemi aziendali critici per ridurre il rischio di accessi non autorizzati in caso di furto di credenziali.
 3. **Aggiornamenti e patching:** Assicurarsi che tutti i sistemi aziendali siano sempre aggiornati e che le vulnerabilità note siano patchate per prevenire ulteriori exploit.

 **Chiavi:**

[phishing, vulnerabilità, remediation, mitigazione, rischio, sicurezza, autenticazione]

Remediation e Mitigazione di Minacce di Phishing e Attacchi DoS - Parte 2: Attacco DoS (Denial of Service)

🌟 Tag: #sicurezza #cybersecurity #DoS #remediation #mitigazione

1. Identificazione della Minaccia

🌟 Tag: #attaccoDoS #vulnerabilità #inondamentoTraffico

- **Cos'è un attacco DoS e come funziona:**

Un attacco **DoS (Denial of Service)** è un attacco in cui l'aggressore tenta di rendere un servizio o una rete non disponibile agli utenti legittimi. Lo fa sovraccaricando il server o la rete con un elevato volume di traffico, saturando le risorse disponibili e impedendo alle richieste legittime di essere soddisfatte.

- **Come un attacco DoS può compromettere la disponibilità dei servizi aziendali:**

Gli attacchi DoS compromettono la disponibilità dei servizi aziendali, rendendoli inaccessibili agli utenti legittimi. Questo può portare a interruzioni nei servizi critici, perdita di produttività e danni reputazionali, oltre a impatti economici causati dalla perdita di opportunità commerciali.

2. Analisi del Rischio

🌟 Tag: #analisiDelRischio #impatto #serviziCritici

- **Impatto potenziale sull'azienda:**

L'impatto di un attacco DoS può essere molto grave. L'inaccessibilità dei servizi web potrebbe portare alla perdita di clienti, interruzioni di

servizio, danni alla reputazione e potenziali perdite finanziarie, soprattutto se i servizi aziendali dipendono pesantemente dalla connettività web.

- **Servizi critici che potrebbero essere compromessi:**
 1. **Server web aziendali:** L'infrastruttura web è spesso l'obiettivo primario degli attacchi DoS, impedendo agli utenti di accedere ai siti aziendali.
 2. **Applicazioni aziendali:** I sistemi di gestione delle risorse (ERP), applicazioni di e-commerce o strumenti interni critici possono diventare inaccessibili, compromettendo la continuità operativa.
 3. **Servizi di posta elettronica:** Anche la posta elettronica può subire un'interruzione, ostacolando le comunicazioni interne ed esterne.
-

3. Pianificazione della Remediation

🌟 Tag: [#remediation](#) [#DoS](#) [#rispostaAllAttacco](#)

- **Piano di risposta all'attacco DoS:**
 1. **Identificazione delle fonti dell'attacco:** Utilizzare strumenti di monitoraggio della rete per identificare le origini del traffico malevolo.
 2. **Mitigazione del traffico malevolo:** Impiegare soluzioni di mitigazione del traffico, come filtri firewall avanzati o servizi esterni che deviano il traffico malevolo, proteggendo i server principali dall'essere sovraccaricati.
-

4. Implementazione della Remediation

🌟 Tag: [#implementazione](#) [#mitigazione](#) [#DoS](#)

- **Passaggi pratici per mitigare la minaccia di DoS:**
 1. **Bilanciamento del carico:** Implementare soluzioni di bilanciamento del carico che distribuiscono il traffico su più server per evitare il sovraccarico di un singolo punto della rete.
 2. **Utilizzo di servizi di mitigazione DoS di terze parti:**
Collaborare con provider specializzati come Cloudflare o Akamai per deviare e filtrare il traffico malevolo.
 3. **Regole firewall avanzate:** Configurare regole specifiche nel firewall per bloccare il traffico sospetto, come il rate limiting, che limita il numero di richieste provenienti da una singola fonte in un determinato periodo di tempo.
-

5. Mitigazione dei Rischi Residuali

🌟 Tag: [#mitigazione](#) [#rischioResiduo](#) [#monitoraggio](#) [#testResilienza](#)

- **Misure di mitigazione:**
 1. **Monitoraggio continuo del traffico di rete:** Implementare strumenti di monitoraggio in tempo reale per rilevare picchi sospetti di traffico e reagire prontamente a nuovi attacchi.
 2. **Collaborazione con il team di sicurezza:** Assicurarsi che il team di sicurezza sia costantemente aggiornato sulle ultime tecniche di attacco e sui metodi di mitigazione.
 3. **Test periodici di resilienza:** Eseguire test di resilienza della rete per valutare l'efficacia delle misure di mitigazione e fare le dovute correzioni in base ai risultati dei test.
-

6. Documentazione e Report

🌟 Tag: [#documentazione](#) [#report](#) [#phishing](#) [#DoS](#)

- **Contenuti del report:**

1. **Descrizione delle minacce di phishing e DoS:** Riassumere le caratteristiche e i metodi di attacco di phishing e DoS, spiegando come queste minacce possano compromettere la sicurezza aziendale.
2. **Analisi del rischio per entrambe le minacce:** Valutare i rischi associati a ciascuna minaccia, identificando i servizi critici e le risorse aziendali a rischio.
3. **Piano di remediation dettagliato:** Fornire un piano dettagliato di risposta per phishing e DoS, con misure specifiche per bloccare, mitigare e risolvere gli attacchi.
4. **Misure di mitigazione:** Descrivere le misure adottate per ridurre il rischio residuo e prevenire future minacce, inclusi i test di phishing simulati e il monitoraggio continuo del traffico di rete.

Chiavi:

[DoS, phishing, sicurezza, mitigazione, monitoraggio, firewall, resilienza, remediation]

“Schermata del 2024-10-21 14-49-30 1.png” non trovato.

L'immagine rappresenta una cattura di pacchetti in Wireshark che mostra un attacco **DoS (Denial of Service)**. Ecco una descrizione dettagliata dei dati inclusi nella tabella:

- **No.:** Numero sequenziale dei pacchetti catturati.
- **Time:** L'orario esatto in cui il pacchetto è stato ricevuto, con precisione di microsecondi.
 - Es: "2024-07-19 06:51:17.946205" indica che il primo pacchetto è stato ricevuto il 19 luglio 2024 alle 06:51 e 17 secondi, con una frazione di 946205 microsecondi.

- **Source:** L'indirizzo IP sorgente da cui proviene il pacchetto. In questo caso, alternano tra due indirizzi: `192.168.1.1` e `192.168.1.2`.
- **Destination:** L'indirizzo IP di destinazione, che in questo caso è costantemente `10.0.0.1`.
- **Protocol:** Il protocollo utilizzato dai pacchetti, che in questo caso è **TCP**.
- **Length:** La lunghezza del pacchetto in byte, che è costantemente **60** byte per ogni pacchetto registrato.
- **Info:** Una breve descrizione del pacchetto. Qui ogni pacchetto è indicato come "DoS attack packet", il che implica che si tratta di pacchetti generati come parte di un attacco DoS.

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		

Non è visibile direttamente nell'immagine una porta specifica, ma considerando che si tratta di pacchetti **TCP**, è probabile che questi pacchetti stiano bersagliando una porta specifica del server **10.0.0.1**. Di solito, nei log Wireshark o negli attacchi DoS, si tenta di sovraccaricare porte comuni, come:

- **80** per il traffico HTTP
- **443** per il traffico HTTPS
- **53** per il traffico DNS
- **22** per il traffico SSH

Ecco una sintesi degli strumenti che un addetto alla sicurezza informatica può utilizzare prima, durante e dopo un attacco di phishing o DoS, basata sul contenuto del PDF caricato 【14†source】 :

Prima di un Attacco - Prevenzione



Tag:

#prevenzione

#strumenti

#phishing

#DoS

1. **Filtri Anti-Phishing:** Soluzioni di sicurezza come gateway email che analizzano i contenuti sospetti e bloccano email fraudolente.
 2. **Simulazione di Phishing:** Condurre campagne simulate per addestrare i dipendenti a riconoscere tentativi di phishing.
 3. **Autenticazione a Due Fattori (2FA):** Implementare 2FA per ridurre il rischio di accesso non autorizzato in caso di furto di credenziali.
 4. **Firewall Avanzati:** Configurare firewall con regole specifiche per bloccare traffico sospetto, inclusi strumenti di rate limiting.
 5. **Bilanciamento del Carico:** Usare sistemi di bilanciamento del carico per distribuire il traffico su più server ed evitare sovraccarichi causati da attacchi DoS.
-

Durante un Attacco - Risposta all'Incidente



Tag:

#risposta

#strumenti

#monitoraggio

#incident-response

1. **Monitoraggio del Traffico di Rete:** Utilizzare strumenti come Wireshark per identificare e tracciare il traffico sospetto, specialmente in caso di attacchi DoS.
2. **Mitigazione del Traffico Malevolo:** Impiegare servizi di mitigazione DoS come Cloudflare o Akamai per deviare e filtrare il traffico malevolo.

3. **Identificazione delle Email Fraudolente:** Utilizzare soluzioni di sicurezza email per identificare e bloccare email phishing in tempo reale.
 4. **Comunicazione ai Dipendenti:** Durante un attacco phishing, informare rapidamente i dipendenti sulle misure da adottare, come evitare di cliccare su link sospetti.
-

Dopo un Attacco - Remediation e Mitigazione dei Rischi Residuali

🔑 Tag: #remediation #mitigazione #resilienza

1. **Scansioni di Sicurezza:** Effettuare verifiche post-attacco per identificare eventuali compromissioni nei sistemi.
2. **Patching e Aggiornamenti:** Garantire che tutte le vulnerabilità note siano risolte con patch tempestive per prevenire future compromissioni.
3. **Test Periodici di Resilienza:** Eseguire test di resilienza della rete per valutare l'efficacia delle misure di mitigazione e fare aggiustamenti in base ai risultati.
4. **Report degli Attacchi:** Redigere un report dettagliato sugli eventi phishing e DoS per documentare le vulnerabilità e i passi correttivi adottati.

🔑 Chiavi:

[strumenti di sicurezza, phishing, DoS, firewall, monitoraggio, remediation, mitigazione]

Tools

Prima di un Attacco - Prevenzione



Tag:

#prevenzione

#phishing

#DoS

#software

1. **Proofpoint:** Una delle migliori soluzioni per la protezione delle email aziendali contro phishing e ransomware.
 2. **Mimecast:** Soluzione completa per la sicurezza delle email, che blocca le minacce come phishing e spoofing.
 3. **PhishMe:** Strumento per simulare attacchi di phishing e addestrare i dipendenti a riconoscerli.
 4. **Duo Security:** Software per l'autenticazione a due fattori (2FA) che riduce i rischi legati al furto di credenziali.
 5. **Palo Alto Networks:** Firewall di nuova generazione che offre un'ampia gamma di funzioni di prevenzione per attacchi avanzati.
 6. **Cisco ASA:** Un firewall aziendale con funzionalità avanzate di difesa contro minacce e traffico sospetto.
 7. **Zscaler:** Strumento che fornisce protezione per email, web e cloud, bloccando minacce come phishing prima che raggiungano l'utente.
-

Durante un Attacco - Risposta all'Incidente



Tag:

#risposta

#incident-response

#software

1. **Wireshark:** Strumento di analisi del traffico di rete che permette di identificare comportamenti anomali e tracciare pacchetti durante un attacco DoS o phishing.
2. **Splunk:** Piattaforma per l'analisi dei log che aiuta a individuare pattern di attacco e anomalie nel traffico di rete.
3. **Snort:** IDS/IPS (Intrusion Detection and Prevention System) open-source per rilevare e prevenire intrusioni di rete.
4. **Suricata:** IDS/IPS avanzato, simile a Snort, ma con capacità di analisi multi-thread per la gestione di volumi di traffico elevati.
5. **Cloudflare:** Fornitore di servizi di mitigazione DoS e protezione avanzata contro attacchi di tipo denial-of-service e traffico malevolo.

6. **Akamai**: Soluzione per la protezione di reti e applicazioni web da attacchi DoS, garantendo disponibilità anche sotto attacco.
-

Dopo un Attacco - Remediation e Mitigazione

🔑 Tag: [#remediation](#) [#mitigazione](#) [#software](#)

1. **Cortex XDR**: Strumento di analisi e risposta agli incidenti che permette di rilevare e rispondere automaticamente alle minacce, aggregando dati da endpoint, reti e cloud.
 2. **QRadar (IBM)**: SIEM (Security Information and Event Management) utilizzato per raccogliere e analizzare eventi di sicurezza, utile per la gestione e risposta agli attacchi.
 3. **ArcSight**: Altro potente strumento SIEM che aiuta nella correlazione di eventi e gestione degli incidenti post-attacco.
 4. **Rapid7 InsightIDR**: Strumento che fornisce monitoraggio continuo e risposta rapida agli incidenti di sicurezza, con focus su attività di remediation.
 5. **Tenable Nessus**: Strumento di scansione delle vulnerabilità che aiuta a identificare e correggere le vulnerabilità che possono essere state sfruttate durante l'attacco.
 6. **OpenVAS**: Un'alternativa open-source a Nessus per la scansione delle vulnerabilità e la gestione del rischio.
-

🔑 Chiavi:

[software sicurezza, phishing, DoS, firewall, IDS, IPS, SIEM, remediation, simulazione phishing]