Remediation e Mitigazione delle Minacce di Phishing e Attacchi DoS

In qualità di amministratore della sicurezza per una media azienda, può capitare di trovarsi a fronteggiare minacce informatiche sempre più sofisticate, tra cui due delle più comuni e insidiose: **il phishing** e **gli attacchi Denial of Service (DoS)**.

La gestione efficace di queste minacce richiede non solo una pronta risposta, ma anche una strategia preventiva ben articolata per mitigare i rischi residui.

Di seguito, analizzerò entrambe le minacce utilizzando il seguente approccio:

- **identificazione**
- **analisi del rischio**
- **pianificazione della remediation**
- **implementazione**
- **mitigazione dei rischi residui**

Phishing

IDENTIFICAZIONE DELLA MINACCIA → Il phishing è una **tecnica malevola** ampiamente diffusa, **basata sull'inganno**. Gli attaccanti inviano **email fraudolente che imitano comunicazioni legittime**, con l'obiettivo di indurre gli utenti a rivelare dati sensibili, come credenziali di accesso, o a **cliccare su link che installano malware**. In uno scenario aziendale, un attacco di phishing può compromettere gravemente la sicurezza, permettendo a malintenzionati di accedere ai sistemi interni, esfiltrare informazioni riservate o causare danni all'infrastruttura.

ANALISI DEL RISCHIO → Valutando il rischio, risulta evidente che **le risorse più vulnerabili sono le credenziali degli utenti, i dati aziendali riservati e la reputazione dell'intera azienda**. Anche un singolo clic su un link malevolo da parte di un dipendente può essere sufficiente per aprire una breccia nei sistemi informatici.

PIANIFICAZIONE DELLA REMEDIATION → Per rispondere efficacemente a un attacco di phishing, **è fondamentale sviluppare un piano di remediation che includa diverse azioni coordinate**:

- **identificare e bloccare le email fraudolente** tramite sistemi di filtraggio avanzato.
- **informare tempestivamente i dipendenti** sull'attacco in corso, fornendo indicazioni chiare su come comportarsi.
- **avviare un'attività di verifica e monitoraggio dei sistemi aziendali** per rilevare eventuali compromissioni.

IMPLEMENTAZIONE → Una volta avviata la risposta, **l'implementazione concreta della remediation prevede l'utilizzo di soluzioni di sicurezza per le email e l'attivazione di filtri anti-phishing aggiornati**. È altrettanto importante condurre attività formative per sensibilizzare i dipendenti, affinché sappiano riconoscere e segnalare tentativi sospetti.

Infine, **le policy di sicurezza interne vanno aggiornate per riflettere l'esperienza e prevenire nuovi attacchi simili.**

MITIGAZIONE DEI RISCHI RESIDUI → Nonostante tutte queste misure, esisterà sempre un rischio residuo. Per ridurlo ulteriormente, **si possono organizzare simulazioni di phishing per testare la prontezza del personale**. L'implementazione dell'**autenticazione a due fattori (2FA)** è un'altra misura chiave per impedire accessi non autorizzati anche nel caso in cui le credenziali venissero compromesse. Infine, l'**aggiornamento costante dei sistemi** e l'applicazione puntuale delle patch di sicurezza contribuiscono a limitare le vulnerabilità sfruttabili.

Attacchi DoS

IDENTIFICAZIONE DELLA MINACCIA → Un attacco **Denial of Service (DoS)** è una strategia utilizzata da attori malevoli per **compromettere la disponibilità dei servizi informatici**, inondando i server con un'enorme quantità di traffico inutile. L'obiettivo è **saturare le risorse del sistema** (CPU, memoria o larghezza di banda) fino a renderlo **inaccessibile agli utenti legittimi**.

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

Nel caso specifico, l'analisi dei pacchetti di rete tramite **Wireshark** mostra una serie continua e ravvicinata di **pacchetti TCP** diretti all'indirizzo IP `10.0.0.1` provenienti alternativamente dagli indirizzi `192.168.1.1` e `192.168.1.2`.

Ogni pacchetto ha una lunghezza di **60 byte**, ed è etichettato come **"DoS attack packet"**, confermando che il traffico è parte di un attacco artificiale mirato.

Questa tipologia di attacco, se non gestita tempestivamente, **può portare all'interruzione completa dei servizi web aziendali**, danneggiando la produttività interna e l'affidabilità percepita dagli utenti esterni.

ANALISI DEL RISCHIO → L'impatto di un attacco DoS può essere **critico**, in quanto non compromette direttamente l'integrità o la riservatezza dei dati, ma **blocca l'accesso ai servizi**, causando perdite economiche, interruzione dei processi aziendali e danni reputazionali.

Nel contesto di una media impresa, i servizi più esposti e vulnerabili sono:

- **Server web aziendali**, che possono smettere di rispondere a richieste legittime;
- **Applicazioni interne**, fondamentali per il lavoro quotidiano dei dipendenti;
- **Servizi cloud** o integrati con fornitori esterni, che possono essere coinvolti o rallentati dagli effetti dell'attacco.

PIANIFICAZIONE DELLA REMEDIATION →Per affrontare un attacco DoS in modo efficace, è essenziale definire una **pianificazione strategica** della remediation. Le azioni prioritarie comprendono:

- **Identificazione delle fonti dell'attacco**, attraverso l'analisi del traffico di rete con strumenti come Wireshark e firewall con funzionalità di ispezione approfondita;
- **Mitigazione del traffico malevolo**, reindirizzando o filtrando il flusso dei pacchetti sospetti prima che raggiungano i sistemi critici.

IMPLEMENTAZIONE → L'implementazione operativa richiede l'applicazione immediata di contromisure tecniche, tra cui:

- L'**implementazione di soluzioni di bilanciamento del carico**, che permettono di distribuire le richieste su più server, evitando la saturazione di un singolo nodo;
- L'utilizzo di **servizi di protezione offerti da fornitori esterni**, che si occupano di filtrare e mitigare il traffico dannoso prima che raggiunga l'infrastruttura aziendale, rappresenta una soluzione efficace soprattutto in caso di attacchi ad alta intensità (es. Cloudflare);
- La **configurazione di regole firewall specifiche**, per bloccare indirizzi IP sospetti o comportamenti anomali nel traffico (es. stessa frequenza, stesso tipo di pacchetto, come visto nello screenshot).

MITIGAZIONE DEI RISCHI RESIDUI → Dopo l'attacco, resta fondamentale **ridurre il rischio che episodi simili si ripetano** o causino danni maggiori. Le azioni consigliate includono:

- Il **monitoraggio continuo del traffico di rete**, con sistemi di rilevamento delle intrusioni (IDS) e strumenti SIEM per identificare tempestivamente pattern sospetti;

- La **collaborazione stretta con il team di sicurezza IT**, per aggiornare costantemente le configurazioni e sviluppare un piano di risposta incidenti efficace;

- L'esecuzione di **test periodici di resilienza**, ovvero simulazioni controllate di attacchi DoS per verificare la reazione dei sistemi e l'efficacia delle contromisure implementate.

Conclusione

La gestione delle minacce informatiche, come il phishing e gli attacchi DoS, rappresenta oggi una priorità strategica per qualsiasi organizzazione, a prescindere dalle sue dimensioni. Come abbiamo visto, ogni fase richiede un approccio integrato che combini competenze tecniche, strumenti adeguati e una forte componente di prevenzione.

Intervenire prontamente è fondamentale, ma lo è altrettanto predisporre misure proattive che riducano la probabilità di un attacco futuro o che ne limitino l'impatto. La consapevolezza del personale, l'adozione di soluzioni tecnologiche aggiornate e la collaborazione tra i reparti IT e sicurezza costituiscono i pilastri su cui costruire una difesa aziendale solida ed efficace.

Solo attraverso un impegno continuo e una visione strategica è possibile proteggere il patrimonio informativo e garantire la continuità operativa, rafforzando allo stesso tempo la resilienza digitale dell'organizzazione.