PHISHING

Fase 1: Identificazione della Minaccia

- **Cos'è il phishing**: Il phishing è un tipo di attacco informatico in cui un attore malintenzionato tenta di ingannare le vittime per ottenere informazioni sensibili come credenziali di accesso, numeri di carte di credito o dati aziendali. Questo avviene principalmente tramite email che sembrano provenire da fonti affidabili.
- **Come funziona il phishing**: Le email di phishing spesso contengono link fraudolenti o allegati malevoli. Quando un dipendente clicca su questi link o scarica gli allegati, può fornire inconsapevolmente informazioni sensibili o installare malware che compromette la sicurezza dei sistemi aziendali.
- **Impatto su un'azienda**: Un attacco di phishing riuscito può compromettere l'integrità dei dati aziendali, permettere l'accesso non autorizzato a sistemi critici, o portare alla perdita di informazioni sensibili come credenziali di accesso, piani aziendali, o dati finanziari.

Fase 2: Analisi del Rischio

- **Impatto potenziale**: Se l'attacco ha successo, può comportare perdita di dati, interruzione operativa, danno alla reputazione dell'azienda, e potenziali sanzioni legali. Nel caso di furto di credenziali, gli attaccanti potrebbero accedere a sistemi aziendali critici e sottrarre o alterare informazioni riservate.
- **Risorse a rischio**: Tra le risorse compromesse ci sono:
    - Credenziali di accesso dei dipendenti
    - Dati finanziari e piani aziendali
    - Informazioni personali dei dipendenti
    - Sistemi IT critici, come server, reti e database.

Fase 3: Pianificazione della Remediation

- **Identificazione e blocco delle email fraudolente**: Utilizza soluzioni di sicurezza per filtrare email sospette, come l'inserimento nella lista nera di domini dannosi e l'uso di tecniche di rilevamento di anomalie nelle email.
- **Comunicazione ai dipendenti**: Invia comunicazioni immediate a tutto il personale, informandoli dell'attacco e delle misure da seguire, come ignorare email sospette e segnalare attività insolite. Fornisci linee guida su come riconoscere email di phishing.
- **Verifica e monitoraggio**: Esegui una scansione approfondita dei sistemi aziendali per individuare compromissioni, analizzando log e monitorando traffico anomalo. Potenzia i controlli di sicurezza sui sistemi più critici.

Fase 4: Implementazione della Remediation

1. **Implementazione di filtri anti-phishing**: Installa soluzioni di sicurezza email come filtri basati su intelligenza artificiale, e configura politiche di sicurezza per bloccare contenuti sospetti.
2. **Formazione dei dipendenti**: Organizza sessioni di formazione regolari per insegnare ai dipendenti a riconoscere tentativi di phishing. Questo include verificare il mittente delle email, evitare di cliccare su link sconosciuti e non scaricare allegati sospetti.
3. **Aggiornamento delle policy di sicurezza aziendale**: Modifica le policy aziendali per includere controlli più stringenti sulle comunicazioni elettroniche, regolamentando l'uso di dispositivi aziendali per email e accesso ai sistemi sensibili.

Fase 5: Mitigazione dei Rischi Residuali

- **Test di phishing simulati**: Regolarmente esegui test di phishing simulati per valutare la reattività e la consapevolezza dei dipendenti riguardo ai rischi di phishing. Questi test aiutano a identificare eventuali lacune nella formazione e nelle procedure.
- **Autenticazione a due fattori (2FA)**: Implementa la 2FA per tutti i sistemi aziendali critici. Questo aggiunge un ulteriore livello di protezione anche se le credenziali sono compromesse.
- **Aggiornamenti regolari**: Assicurati che tutti i sistemi aziendali siano aggiornati e patchati regolarmente per ridurre la vulnerabilità a potenziali exploit utilizzati dai cyber criminali.

Fase 6: Monitoraggio Continuo

- **Verifica regolare dei sistemi**: Monitora continuamente il traffico di rete e i log per individuare attività sospette e rispondere prontamente a eventuali attacchi. Utilizza software di rilevamento delle intrusioni (IDS) e analisi comportamentale per identificare possibili minacce.

Conclusione

La prevenzione e la risposta a una campagna di phishing richiedono un approccio multilivello, che comprende la formazione dei dipendenti, l'implementazione di tecnologie di sicurezza e il monitoraggio continuo. La combinazione di soluzioni tecniche e consapevolezza del rischio tra i dipendenti è fondamentale per mitigare il rischio di phishing e proteggere l'integrità dell'azienda

DENIAL OF SERVICE (DOS)

Fase 1: Identificazione della Minaccia

- **Cos'è un attacco DoS**: Un attacco DoS (Denial of Service) è un tentativo malevolo di rendere inutilizzabili i servizi di una rete o di un sistema, inondandoli di richieste eccessive o pacchetti malformati, fino a esaurire le risorse del server. Questo tipo di attacco compromette la disponibilità dei servizi, rendendoli inaccessibili agli utenti legittimi.
- **Come funziona**: L'attaccante invia una grande quantità di traffico verso un server o una rete, causando sovraccarico e interrompendo i servizi legittimi. Gli attacchi DoS possono sfruttare vulnerabilità di protocolli, reti o applicazioni per amplificare il danno.

Fase 2: Analisi del Rischio

- **Impatto potenziale**: L'attacco DoS può comportare interruzione dei servizi, perdita di accesso ai sistemi critici, e perdita di profitti. Inoltre, può danneggiare la reputazione dell'azienda e aumentare i costi operativi per mitigare l'attacco. Nei casi più gravi, un attacco DoS prolungato può influenzare la fiducia dei clienti e delle parti interessate.
- **Servizi critici compromessi**:
    - **Server web**: I server che gestiscono i siti web aziendali o le applicazioni online possono essere colpiti, impedendo agli utenti di accedere a servizi o informazioni.
    - **Applicazioni aziendali**: Sistemi interni come ERP (Enterprise Resource Planning), CRM (Customer Relationship Management) o database possono subire un'interruzione, causando rallentamenti o blocchi nei flussi di lavoro.
    - **Rete aziendale**: Il traffico malevolo può saturare la banda disponibile, interrompendo l'accesso a Internet e ai servizi di rete.

Fase 3: Pianificazione della Remediation

- **Identificazione delle fonti dell'attacco**: Utilizza strumenti di monitoraggio della rete come Wireshark per analizzare il traffico sospetto e identificare gli indirizzi IP da cui proviene l'attacco.
    - Esempio: Nel log catturato da Wireshark, si nota che gli IP **192.168.1.1** e **192.168.1.2** stanno inondando il server con pacchetti TCP, con destinazione **10.0.0.1**. Questi IP sono probabilmente parte dell'attacco.
- **Mitigazione del traffico malevolo**:
    - **Blocco del traffico sospetto**: Configura firewall e sistemi di prevenzione delle intrusioni (IPS) per bloccare gli IP identificati come fonti dell'attacco
- **Mitigazione del traffico malevolo (continua)**:
    - **Filtri di traffico**: Implementa filtri a livello di rete per limitare la quantità di traffico proveniente da fonti sospette. Configura soglie di traffico per le richieste ai servizi critici e applica regole che possono bloccare richieste sospette.
    - **Rate limiting**: Applica il rate limiting per limitare il numero di richieste che un singolo IP può inviare a un servizio in un determinato periodo di tempo. Questo aiuta a proteggere i server da sovraccarichi.

Fase 4: Implementazione della Remediation

1. **Implementazione di soluzioni di bilanciamento del carico**:
    - Distribuisci il traffico in entrata su più server per evitare che un singolo server venga sovraccaricato. Le soluzioni di bilanciamento del carico possono aiutare a gestire le richieste in modo più efficiente e garantire la disponibilità dei servizi.
2. **Utilizzo di servizi di mitigazione DoS offerti da terze parti**:
    - Valuta l'implementazione di servizi di mitigazione DoS da provider esterni specializzati. Questi servizi possono filtrare il traffico prima che raggiunga l'azienda, proteggendo i server da attacchi volumetrici.
3. **Configurazione di regole firewall**:
    - Imposta regole specifiche nel firewall per bloccare il traffico proveniente da indirizzi IP sospetti e per limitare i tipi di pacchetti consentiti. Ad esempio, potresti bloccare pacchetti TCP su porte non utilizzate o inondare richieste da IP che superano una certa soglia.

Fase 5: Mitigazione dei Rischi Residuali

- **Monitoraggio continuo del traffico di rete**:
    - Implementa strumenti di monitoraggio della rete che possono analizzare e identificare anomalie in tempo reale. Usa dashboard per la visualizzazione del traffico e per ricevere alert su comportamenti sospetti.
- **Collaborazione con il team di sicurezza**:
    - Collabora con il team di sicurezza IT per rivedere le misure di protezione esistenti e migliorarle. Organizza incontri regolari per discutere nuove minacce e aggiornamenti sulle politiche di sicurezza.
- **Test periodici di resilienza**:
    - Esegui test regolari di resilienza per valutare l'efficacia delle misure di mitigazione. Questi test possono includere simulazioni di attacchi DoS per verificare la capacità dell'infrastruttura di resistere a condizioni di carico estremo.

Fase 6: Documentazione e Report

Compila un report completo che includa:

1. **Descrizione delle minacce di phishing e DoS**:
    - Presenta una panoramica dei due tipi di attacchi, evidenziando le loro caratteristiche, modalità di funzionamento e impatti sull'azienda.
2. **Analisi del rischio per entrambe le minacce**:
    - Valuta l'impatto potenziale e identifica i servizi critici a rischio per ciascuna minaccia. Sottolinea la necessità di un approccio coordinato per la sicurezza.
3. **Piano di remediation dettagliato**:

- Include i dettagli delle azioni di remediation per entrambi i tipi di attacco, specificando le tecniche e le soluzioni da implementare, i passaggi pratici e le misure di mitigazione dei rischi residui.

Esempio di Log Wireshark durante un attacco DoS

Ecco un esempio di come potrebbe apparire un log di Wireshark durante 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

Questo log mostra pacchetti TCP provenienti da due indirizzi IP (192.168.1.1 e 192.168.1.2) che inviano richieste ripetute al server di destinazione (10.0.0.1), indicando un attacco DoS in corso.

Conclusione

La minaccia degli attacchi DoS richiede un approccio proattivo e reattivo per garantire la disponibilità dei servizi aziendali. L'identificazione tempestiva delle minacce, l'implementazione di misure di mitigazione e la continua formazione e preparazione del personale sono essenziali per ridurre il rischio e garantire la resilienza dell'infrastruttura IT aziendale.