PHISHING e DENIAL OF SERVICE (DOS)

Alfio Scuderi
alfio94.AS@gmail.com

Sommario

PHISHING

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.

Meccanismo

Le email di phishing spesso contengono link fraudolenti o allegati malevoli. Quando un dipendente clicca su questi link o scarica gli allegati, può inconsapevolmente fornire informazioni sensibili o installare malware.

Impatto aziendale

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.

ANALISI DEL RISCHIO - PHISHING

Impatto potenziale

Perdita di dati, interruzione operativa, danno alla reputazione dell'azienda, e potenziali sanzioni legali.

Risorse a rischio

Credenziali di accesso, dati finanziari, informazioni personali dei dipendenti, sistemi IT critici.

PIANIFICAZIONE DELLA REMEDIATION - PHISHING

Blocco email fraudolente

Utilizza soluzioni di sicurezza per filtrare email sospette, liste nere di domini dannosi e rilevamento di anomalie.

Comunicazione ai dipendenti

Invia comunicazioni immediate, fornendo linee guida su come riconoscere email di phishing e segnalare attività insolite.

Verifica e monitoraggio

Scansione approfondita dei sistemi per individuare compromissioni, analizzare log, e monitorare traffico anomalo.

IMPLEMENTAZIONE DELLA REMEDIATION - PHISHING

Filtri anti-phishing

Installa soluzioni di sicurezza email basati su AI e configura politiche di sicurezza per bloccare contenuti sospetti.

Formazione dei dipendenti

Organizza sessioni di formazione regolari per insegnare ai dipendenti a riconoscere tentativi di phishing.

Aggiornamento delle policy di sicurezza

Modifica le policy aziendali per includere controlli più stringenti sulle comunicazioni elettroniche.

MITIGAZIONE DEI RISCHI RESIDUALI - PHISHING

Test di phishing simulati

Esegui test regolari per valutare la reattività e la consapevolezza dei dipendenti riguardo ai rischi.

Autenticazione a due fattori (2FA)

Implementa la 2FA per tutti i sistemi aziendali critici per aggiungere un ulteriore livello di protezione.

Aggiornamenti regolari

Assicurati che tutti i sistemi aziendali siano aggiornati e patchati regolarmente per ridurre la vulnerabilità.

MONITORAGGIO CONTINUO - PHISHING

Verifica regolare dei sistemi
Monitora continuamente il traffico di rete e i log per individuare attività sospette e rispondere prontamente.

CONCLUSIONE - PHISHING

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)

Cos'è un attacco DoS

Un attacco DoS è un tentativo malevolo di rendere inutilizzabili i servizi di una rete o di un sistema, inondandoli di richieste eccessive o pacchetti malformati.

Meccanismo

L'attaccante invia una grande quantità di traffico verso un server o una rete, causando sovraccarico e interrompendo i servizi legittimi.

ANALISI DEL RISCHIO - DOS

Impatto potenziale

Interruzione dei servizi, perdita di accesso ai sistemi critici, perdita di profitti, danno alla reputazione e aumento dei costi operativi.

Servizi critici compromessi

Server web, applicazioni aziendali come ERP e CRM, reti aziendali.

PIANIFICAZIONE DELLA REMEDIATION - DOS

Identificazione delle fonti dell'attacco

Utilizza strumenti di monitoraggio della rete per analizzare il traffico sospetto e identificare gli IP di origine.

Mitigazione del traffico malevolo

Configura firewall e sistemi di prevenzione delle intrusioni per bloccare gli IP e implementa filtri di traffico a livello di rete.

Rate limiting

Applica il rate limiting per limitare il numero di richieste che un singolo IP può inviare a un servizio.