Esercizio 21 Ottobre

1. Identificazione della Minaccia

Cos'è il Phishing e Come Funziona: Il phishing è un tipo di attacco informatico in cui gli hacker inviano email fasulle che sembrano provenire da fonti affidabili, come colleghi, banche o altre aziende, per rubare informazioni personali o aziendali. Queste email spesso contengono link che portano a siti falsi o allegati infetti con malware. Se una persona cade nel tranello, può dare agli hacker accesso a dati importanti o installare malware sul proprio computer.

Come un Attacco di Phishing può Compromettere la Sicurezza dell'Azienda: Un attacco di phishing può mettere a rischio la sicurezza aziendale in vari modi. Se un dipendente condivide per errore le proprie credenziali, un hacker potrebbe accedere ai sistemi interni dell'azienda, rubare dati sensibili o diffondere malware all'interno della rete aziendale. Questo potrebbe causare perdite economiche, violazione di dati riservati e danni all'immagine dell'azienda.

2. Analisi del Rischio

Impatto Potenziale di Questa Minaccia: Le conseguenze di un attacco di phishing possono essere molto serie:

Perdite economiche: Se gli hacker accedono ai conti aziendali o bloccano i sistemi con ransomware, l'azienda potrebbe dover pagare per risolvere il problema.

Danni all'immagine: La perdita di dati sensibili può far perdere la fiducia dei clienti.

Interruzione del lavoro: Un malware può causare il blocco dei sistemi aziendali, interrompendo le attività quotidiane.

Sanzioni legali: Se vengono rubati dati personali dei clienti, l'azienda potrebbe dover affrontare problemi legali.

Risorse che Potrebbero Essere Compromesse:

Credenziali di accesso: Gli hacker potrebbero accedere ai sistemi aziendali usando le password dei dipendenti.

Dati sensibili: Come informazioni su clienti, progetti o piani strategici.

Infrastruttura IT: Server, reti e dispositivi potrebbero essere compromessi o infettati con malware.

3. Pianificazione della Remediation

Piano per Rispondere all'Attacco di Phishing:

Identificare e Bloccare le Email Fraudolente: Bisogna subito implementare sistemi di sicurezza che riescano a filtrare le email sospette. Collaborare con il provider di posta per bloccare i mittenti dannosi e analizzare le email sospette.

Comunicare con i Dipendenti: È fondamentale avvisare subito tutti i dipendenti che è in corso una campagna di phishing e spiegare loro cosa fare. Dovrebbero essere istruiti su come riconoscere email sospette (come controllare il mittente, diffidare di richieste urgenti o allegati strani) e a chi segnalare eventuali email dubbie.

Verificare e Monitorare i Sistemi: Si deve controllare attentamente se ci sono state compromissioni nei sistemi aziendali, analizzando i log di accesso e monitorando il traffico di rete per individuare eventuali comportamenti sospetti.

4. Implementazione della Remediation

Cosa Fare per Mitigare il Phishing:

Sistemi di Sicurezza Email: Si devono installare software di sicurezza per la posta elettronica che siano in grado di rilevare email di phishing e bloccarle prima che raggiungano i dipendenti. È utile configurare protocolli come SPF, DKIM e DMARC, che aiutano a verificare l'autenticità delle email e prevenire attacchi di spoofing (ovvero quando un hacker falsifica il mittente di un'email).

Formazione dei Dipendenti: I dipendenti devono essere formati su come riconoscere email di phishing. Si possono fare corsi di formazione in cui si mostrano esempi concreti di email false e si spiegano i segnali a cui fare attenzione, come link strani o errori grammaticali.

Aggiornamento delle Policy di Sicurezza: Le politiche di sicurezza devono essere aggiornate, assicurandosi che tutti sappiano come comportarsi in caso di attacco e come proteggere i propri account. È importante stabilire protocolli chiari per la segnalazione di email sospette e la gestione delle minacce.

5. Mitigazione dei Rischi Residuali

Cosa Fare per Ridurre il Rischio Residuo:

Simulazioni di Phishing: È utile organizzare test periodici in cui si inviano email di phishing simulate ai dipendenti per vedere come reagiscono. Questo serve a valutare il livello di consapevolezza e individuare chi ha bisogno di ulteriore formazione.

Autenticazione a Due Fattori (2FA): Implementare l'autenticazione a due fattori sui sistemi aziendali più importanti può aggiungere un livello di sicurezza in più. Anche se un hacker riesce a rubare una password, avrà comunque bisogno di un secondo fattore di autenticazione (come un codice inviato al cellulare) per accedere.

Aggiornamenti e Patching: Tenere sempre aggiornati i software e applicare le patch di sicurezza non appena disponibili aiuta a ridurre la possibilità che gli hacker sfruttino vulnerabilità conosciute nei sistemi aziendali.