S11L1

1- Identificazione della Minaccia

Definizione:
Il phishing è una tecnica utilizzata dai cybercriminali per ingannare le persone e ottenere informazioni sensibili, come username, password, numeri di carte di credito o altri dati personali. Solitamente, avviene attraverso email che sembrano provenire da fonti affidabili (ad esempio, banche, aziende o colleghi).

Come avviene:

Email fraudolente: Un messaggio sembra provenire da un'entità legittima, ma contiene link o allegati malevoli.

Siti falsi: I link portano l'utente su un sito web che imita quello originale per spingerlo a inserire le sue credenziali.

Allegati dannosi: Scaricando un file allegato, si può installare malware sul dispositivo.

Gli attacchi di phishing possono:

- Rubare le credenziali dei dipendenti, consentendo agli attaccanti di accedere ai sistemi aziendali.
- Distribuire malware all'interno della rete aziendale, causando interruzioni o danni.
- Esporre dati sensibili, come informazioni su clienti o progetti interni.
- Ridurre la fiducia di clienti e partner nell'azienda se l'attacco diventa pubblico.

2- Analisi del Rischio

Impatto potenziale della minaccia sull'azienda

Un attacco di phishing riuscito può avere conseguenze gravi, tra cui:

Perdita di dati sensibili: Ad esempio, informazioni finanziarie o personali di dipendenti e clienti.

Interruzione delle attività: Malware o accessi non autorizzati possono bloccare il normale funzionamento.

Danni reputazionali: Clienti e partner potrebbero perdere fiducia nell'azienda.

Perdite economiche: Spese per il recupero dei dati, ripristino dei sistemi e potenziali multe.

Risorse compromesse

Credenziali: Accesso alle email aziendali, ai server o a sistemi di gestione interna.

Dati aziendali sensibili: Come informazioni sui clienti, documenti interni, o segreti commerciali.

Infrastruttura IT: Server e reti potrebbero essere danneggiati o controllati da attaccanti.

3- Pianificazione della Remediation

Piano d'azione per rispondere all'attacco di phishing

Identificazione e blocco delle email fraudolente:

- Utilizzare filtri di sicurezza per rilevare e bloccare email sospette.
- Analizzare i messaggi fraudolenti per identificare l'origine e comprendere il tipo di attacco.

Comunicazione ai dipendenti:

- Informare tutti i dipendenti dell'attacco in corso.
- Fornire indicazioni pratiche su come riconoscere email sospette (ad esempio, controllare il mittente e i link).

Verifica e monitoraggio dei sistemi:

- Controllare se le credenziali di dipendenti sono state compromesse.
- Monitorare i log dei sistemi per individuare attività insolite.

4- Implementazione della Remediation

Passaggi pratici per mitigare il phishing

Implementazione di filtri anti-phishing:

- Configurare sistemi di protezione per le email (come antivirus e filtri anti-spam) per bloccare i messaggi fraudolenti prima che arrivino ai dipendenti.

Formazione dei dipendenti:

- Organizzare sessioni pratiche per insegnare ai dipendenti a:

- Riconoscere messaggi sospetti (errori grammaticali, richieste urgenti, mittenti sconosciuti).
- Segnalare i tentativi di phishing al reparto IT.

Aggiornamento delle policy di sicurezza:

Introdurre procedure obbligatorie, come l'autenticazione a due fattori (2FA), per accedere ai sistemi aziendali.

Limitare l'accesso ai dati sensibili solo a dipendenti autorizzati.

5- Mitigazione dei Rischi Residuali

Misure per ridurre il rischio futuro

Test di phishing simulati:

- Esegui esercitazioni periodiche per verificare la capacità dei dipendenti di riconoscere email di phishing. Questi test aiutano anche a migliorare le procedure aziendali.

Autenticazione a due fattori (2FA):

- Richiedi ai dipendenti di utilizzare un secondo metodo di verifica (ad esempio, un codice inviato al cellulare) per accedere ai sistemi aziendali. Questo protegge gli account anche in caso di furto delle credenziali.

Aggiornamenti regolari:

- Mantieni software e sistemi aggiornati per correggere vulnerabilità note.
- Installa patch di sicurezza il prima possibile.

In conclusione:

Affrontare minacce come il phishing richiede un equilibrio tra prevenzione e risposta immediata. Mentre è essenziale bloccare e mitigare gli attacchi in corso, la vera sicurezza si costruisce attraverso formazione, tecnologie avanzate e un approccio proattivo. Un'azienda preparata non solo riduce i rischi, ma rafforza anche la fiducia nel proprio sistema di sicurezza, rendendosi più resiliente alle sfide future.