PROGETTO S3/L5

L'impostazione di un programma di formazione per educare i dipendenti di Epicodesecurity sui rischi degli attacchi di ingegneria sociale, in particolare del phishing, è fondamentale per migliorare la posizione complessiva della sicurezza informatica dell'azienda. Di seguito è riportato un piano completo che copre la spiegazione del phishing, i parametri chiave per identificare le e-mail di phishing e la creazione di un phishing controllato a scopo di formazione pratica.

Programma di formazione:

1. Introduzione al phishing:

OBBIETTIVO: garantire che i dipendenti comprendano il concetto di phishing e i suoi potenziali rischi.

CONTENUTO:
- Definizione di phishing.
- Tattiche di phishing comuni (e-mail, siti Web, telefonate).
- Esempi reali e casi di studio.

2. Parametri chiave per identificare il phishing:

OBBIETTIVO: fornire ai dipendenti le conoscenze necessarie per riconoscere potenziali tentativi di phishing.

CONTENUTO:

- Indirizzo e-mail del mittente:
    - Controlla eventuali errori di ortografia o variazioni nel dominio.
    - Verificare la legittimità del mittente effettuando riferimenti incrociati.

- Contenuto dell'e-mail:
    - Cerca saluti generici o un linguaggio urgente.
    - Controlla gli errori grammaticali.
    - Diffidare di allegati o collegamenti imprevisti.

- URL:
    - Passa il mouse sopra i link per visualizzare in anteprima l'URL effettivo.
    - Verificare la legittimità del sito Web controllando i certificati SSL.

- Allegati:
    - Evitare di aprire allegati provenienti da fonti sconosciute o inaspettate.

- Richieste di informazioni sensibili:
    - Prestare attenzione nel fornire informazioni personali o sensibili.

- Spoofing:
    - Convalida la legittimità delle e-mail che dichiarano di provenire da fonti attendibili.

3. Formazione sulle funzionalità del server di posta elettronica (ad esempio SPF):

OBBIETTIVO: familiarizzare i dipendenti con le funzionalità di sicurezza della posta elettronica per identificare potenziali phishing.

CONTENUTO:

- SPF (quadro delle politiche del mittente):
    - Spiega come SPF aiuta a verificare la legittimità del dominio del mittente.

4. Esercizio di phishing simulato:

OBBIETTIVO: fornire esperienza pratica ai dipendenti attraverso un phishing controllato.

CONTENUTO:

- Pianificazione:
    - Ottieni l'approvazione del direttore.
    - Seleziona uno scenario pertinente e non minaccioso per l'e-mail di phishing simulata.

- Esecuzione:
    - Invia un'e-mail di phishing controllata a tutti i dipendenti.
    - Includi elementi comuni di phishing (ad esempio urgenza, richiesta di informazioni personali e un link sospetto).

- Feedback:
    - Monitorare le risposte e raccogliere dati su chi ha cliccato sul collegamento o ha fornito informazioni.
    - Fornisci un feedback immediato a coloro che sono caduti nel phishing simulato.

- Formazione:
    - Condurre una sessione di follow-up per discutere del phishing simulato.
    - Condividi approfondimenti, lezioni apprese e rafforza le migliori pratiche.

5. Consapevolezza continua:

OBBIETTIVO: promuovere una cultura di consapevolezza della sicurezza informatica.

CONTENUTO:
- Aggiorna regolarmente i dipendenti sulle tattiche di phishing emergenti.
- Incoraggiare la segnalazione di e-mail sospette.

- Condurre periodiche sessioni di aggiornamento formativo.

Combinando le conoscenze teoriche con esercizi pratici, i dipendenti di Epicodesecurity possono essere meglio preparati a identificare e mitigare i rischi di attacchi di ingegneria sociale, in particolare di phishing.