Esercitazione S11/L1

In questa esercitazione andremo a svolgere le fasi di mitigation e remediation riguardo un attacco phishing.

Phishing

Il phishing è una tecnica di attacco informatico che mira a ingannare gli utenti per ottenere informazioni sensibili come nomi utente, password, numeri di carte di credito o altri dati personali e aziendali. Gli attacchi di phishing mirano l'essere umano e si basano sull'inganno psicologico. Gli aggressori inviano messaggi che sembrano provenire da fonti affidabili, come banche, servizi online, colleghi o superiori aziendali. Solitamente si utilizzano email contenenti tecniche di manipolazione psicologica, ad esempio:

- Urgenza: "Agisci ora o il tuo account sarà chiuso."
- Autorità: "Sono il tuo amministratore IT, clicca qui per aggiornare la tua password."
- Emozioni: "Hai ricevuto un premio! Richiedilo subito."

Identificazione e analizi del rischio

Come primo step si va a identificare la minacchia e valutare l'impatto potenziale di questa sull'azienda. Vado anche ad identificare le risorse che potrebbero essere compromesse.

L'impatto potenziale sarà di tipo

- Finanziario: Perdite dirette a causa di frodi o costi di recupero dei dati compromessi.
- Operativo: Interruzione dei sistemi e rallentamenti nelle attività aziendali.
- Legale e normativo: Multa per mancata conformità a regolamenti (es. GDPR) in caso di violazioni di dati personali.
- Reputazionale: Danneggiamento della fiducia dei clienti e partner.

Le risorse compromesse saranno

- Credenziali di accesso (email, VPN, strumenti di lavoro).
- Dati sensibili (informazioni dei dipendenti, dati dei clienti, proprietà intellettuale).
- Sistemi IT aziendali (server, database, piattaforme di comunicazione).

Pianificazione della Remediation

Ora andrò a sviluppare un piano di Remediation per avere un piano di risposta agli attacchi phishing. Sviluppando un buon piano sarà applicabile anche per eventi futuri.
La fase di remediation si focalizzerà sulla risoluzione delle vulnerabilità identificate attraverso interventi che correggono o eliminano completamente i problemi di sicurezza.
L'obiettivo della remediation è ripristinare la sicurezza e l'integrità dei sistemi, eliminando le cause delle vulnerabilità.

Sviluppo del Piano di risposta all'attacco di phishing:

- Identificazione e blocco delle email fraudolente: Implementando filtri avanzati per email basati su machine learning e blacklist di domini malevoli. E Analizzare i log email per rilevare modelli sospetti.
- Comunicazione ai dipendenti: Inviare avvisi immediati per informare sull'attacco e su come evitare interazioni con le email sospette. Fornire istruzioni su come segnalare email fraudolente.
- Verifica e monitoraggio dei sistemi: Eseguire scansioni di sicurezza per rilevare malware o attività anomale. Cambiare immediatamente le credenziali compromesse.

Implementazione della Remediation

Dopo aver sviluppato il piano di remediation lo andrò ad applicare,
le soluzioni trovate sono:

- Filtri anti-phishing e soluzioni di sicurezza email: Configurare strumenti come SPF, DKIM e DMARC per autenticare le email. Utilizzare piattaforme di email security con funzionalità avanzate (es. sandboxing per analisi degli allegati).
- Formazione dei dipendenti: Workshop e corsi per riconoscere email sospette (es. errori grammaticali, indirizzi insoliti, richieste urgenti). Simulazioni di attacchi di phishing per sensibilizzare e valutare il livello di attenzione.
- Aggiornamento delle policy di sicurezza: Creare linee guida specifiche per gestire email sospette. Definire procedure standard per segnalare incidenti.

Mitigazione dei Rischi

La fase di mitigation di un attacco di phishing è cruciale per limitare i danni, proteggere le risorse aziendali e prevenire futuri incidenti. Si articola in diverse attività, che combinano tecniche, organizzative e formative.

Identificazione e risposta immediata

- segnalazione e identificazione delle email sospette
- blocco delle email malevole
- isolamento dei sistemi compromessi.

Monitoraggio e controllo dei danni

- verifica delle attività sospette
- modifica delle credenziali compromesse
- scansione per malware

Comunicazione e Coordinamento

- Notificare eventuali mail sospette
- coinvolgimento del team di risposta agli incidenti

Implementazione di Misure Preventive

- protocolli di autenticazione email come SPF, DKIM, e DMARC.
- Autenticazione avanzata (2FA o MFA)
- Segmentazione della rete
- Formazione dei Dipendenti
- Rafforzamento delle Policy di Sicurezza

Misure aggiuntive per ridurre il rischio residuo

- Test di phishing: Effettuare campagne regolari per valutare la reattività dei dipendenti. Fornire feedback immediato e corsi di follow-up in caso di errori.
- Autenticazione a due/multi fattori (2FA o MFA): Implementare 2FA o MFA per tutti i sistemi critici e account aziendali. Utilizzare metodi robusti come applicazioni di autenticazione o chiavi di sicurezza hardware.
- Monitoraggio continuo: Implementare strumenti di threat intelligence per individuare nuove minacce. Mantenere aggiornati i software di sicurezza aziendali.