Esercizio S11 L1 del 09/12/24 ***Daniele Paolone***

Minaccia di Phishing

Il *phishing* è una tecnica di attacco informatico che mira a ingannare le persone per ottenere informazioni sensibili, come password, dati bancari, numeri di carta di credito o altre informazioni personali. Gli attacchi di phishing sono comunemente eseguiti tramite email, messaggi di testo o siti web falsi che imitano quelli legittimi.

Funzionamento del phishing:

- Email o messaggio ingannevole: Un attaccante invia un'email o un messaggio che sembra provenire da un'organizzazione affidabile (ad esempio, una banca, un'azienda tecnologica o un sito di e-commerce). Questo messaggio spesso contiene un tono urgente, come "Il tuo account è stato compromesso" o "È necessario aggiornare le tue informazioni".

- Richiesta di azione: L'email o il messaggio chiede alla vittima di cliccare su un link o scaricare un allegato. Il link conduce a un sito web fasullo progettato per somigliare a quello autentico.

- Inserimento delle informazioni: Sul sito fraudolento, alla vittima viene chiesto di inserire dati personali o credenziali di accesso, che vengono poi raccolti dall'attaccante.

- Conseguenze: Gli attaccanti possono utilizzare queste informazioni per accedere agli account della vittima, rubare denaro, fare acquisti non autorizzati o persino commettere furti di identità.

Analisi del Rischio

L'impatto potenziale del phishing su un'azienda può essere significativo e riguardare diversi aspetti operativi, finanziari e legali.

Impatto operativo

- Interruzione delle attività: Se un attacco di phishing compromette account critici, l'accesso ai sistemi aziendali potrebbe essere bloccato o limitato.
  Attacchi con malware (es. ransomware) derivanti da phishing possono paralizzare i sistemi IT.

- Perdita di produttività: I dipendenti potrebbero perdere tempo cercando di risolvere il problema o ripristinare l'accesso ai sistemi.

Impatto finanziario

- Perdite dirette: Furto di fondi aziendali tramite accesso non autorizzato a conti bancari o sistemi di pagamento.
  Costi di recupero dati o di pagamento del riscatto in caso di ransomware.

- Costi indiretti: Spese per consulenti di sicurezza e investigazioni post-attacco. Necessità di implementare misure di sicurezza aggiuntive o aggiornare sistemi compromessi.

- Perdita di opportunità: Riduzione della fiducia dei clienti e delle vendite se i sistemi o i servizi sono compromessi.

Impatto sui dati e sulla conformità normativa

- Violazione di dati sensibili: Accesso non autorizzato a dati personali, finanziari o strategici. Furto di proprietà intellettuale o segreti aziendali.

- Non conformità alle normative: Violazioni di leggi come il GDPR, che richiedono la protezione dei dati personali, possono comportare:

- Obblighi di segnalazione: L'obbligo legale di segnalare le violazioni può amplificare l'impatto reputazionale.

L'impatto del phishing su un'azienda è potenzialmente devastante, con conseguenze su più fronti. Le aziende devono considerare il phishing non solo come un problema IT, ma come un rischio strategico che richiede una combinazione di soluzioni tecnologiche, formazione e policy per essere mitigato. Una preparazione adeguata può ridurre significativamente i danni e i costi di un attacco.

Le risorse che potrebbero essere compromesse da un attacco di phishing possono essere dati vitali per l' azienda o informazioni sui dipendenti. Nello specifico:

- Credenziali di accesso:
  - Username e password per account aziendali, email, strumenti di lavoro o sistemi gestionali.
  - Dati di accesso a sistemi critici (es. ERP, CRM, piattaforme cloud).

- Informazioni personali:
  - Dati anagrafici e numeri di identificazione (es. codice fiscale, numeri di previdenza sociale).
  - Indirizzi, numeri di telefono, informazioni mediche o altre informazioni personali di dipendenti e clienti.

- Informazioni finanziarie:
  - Numeri di conti bancari, carte di credito, dettagli per i pagamenti.
  - Dati legati alla gestione economica, come fatture e ordini.

- Proprietà intellettuale:
  - Progetti, brevetti, segreti commerciali, strategie aziendali.
  - Materiale riservato su nuovi prodotti o iniziative in sviluppo.

- Infrastruttura IT:
  - Rete interna, server e database
  - Computer, smartphone, tablet o altri dispositivi che possono essere infettati da malware (es. keylogger, ransomware).

Pianificazione della Remediation

Identificazione e blocco delle email fraudolente

1. Analizzare le email sospette segnalate dai dipendenti o rilevate dai sistemi di sicurezza.
2. Identificare i mittenti fraudolenti, domini sospetti e pattern ricorrenti.
3. Aggiornare i filtri di sicurezza per bloccare ulteriori email da questi mittenti o domini.
4. Utilizzare strumenti di threat intelligence per verificare se l'attacco è parte di una campagna più ampia.

Comunicazione ai dipendenti

1. Notifica tempestiva:
    - Informare i dipendenti dell'attacco in corso attraverso email, intranet aziendale o canali ufficiali.
    - Specificare il tipo di minaccia e fornire esempi di email di phishing.

2. Istruzioni operative:
    - Chiedere di non interagire con email sospette (cliccare link o aprire allegati).
    - Fornire indicazioni su come segnalare email fraudolente al reparto IT o tramite uno strumento dedicato.
3. Rassicurazione:
    - Sottolineare che il team IT sta lavorando per risolvere il problema e minimizzare i rischi.

Verifica e monitoraggio dei sistemi

1. Analizzare i log di sistema per individuare attività sospette, come tentativi di accesso non autorizzato o download di file non usuali.
2. Verificare i sistemi critici per individuare eventuali compromissioni o installazioni di malware.
3. Isolare gli account compromessi e forzare il reset delle credenziali.
4. Attivare un monitoraggio continuo per rilevare ulteriori tentativi di attacco.

Implementazione della Remediation

Filtri anti-phishing e soluzioni di sicurezza

1. Implementare soluzioni avanzate di sicurezza per le email:
    - Filtri anti-phishing per bloccare email sospette basate su pattern, URL o allegati.
    - Sandbox per analizzare allegati e link in ambienti isolati prima di consegnarli ai destinatari.
2. Configurare tecnologie come SPF, DKIM e DMARC per autenticare le email aziendali e prevenire spoofing.
3. Abilitare sistemi di protezione endpoint (EDR) per rilevare e rispondere a minacce su dispositivi aziendali.

Formazione dei dipendenti

1. Organizzare sessioni di formazione mirate su:
    - Come riconoscere email di phishing (es. mittenti sospetti, errori grammaticali, richieste urgenti).
    - L'importanza di non cliccare link o scaricare allegati sconosciuti.
    - L'uso corretto degli strumenti di segnalazione.

2. Creare una cultura di sicurezza tramite campagne di sensibilizzazione regolari.

Aggiornamento delle policy di sicurezza

1. Rafforzare le policy aziendali relative alla gestione delle email:
    - Obbligo di utilizzare sistemi di crittografia per dati sensibili.
    - Procedure per il reporting immediato di incidenti.

2. Introdurre linee guida per l'utilizzo di dispositivi personali e applicazioni non approvate.

Mitigazione dei Rischi Residuali

Test di phishing simulati

1. Eseguire test periodici simulando attacchi di phishing:
    - Valutare la capacità dei dipendenti di riconoscere e segnalare email sospette.
    - Identificare le aree in cui è necessaria ulteriore formazione.

2. Utilizzare i risultati per perfezionare la formazione e aggiornare le policy.

Autenticazione a due fattori (2FA)

1. Implementare il 2FA per tutti gli accessi ai sistemi critici e alle email aziendali.

2. Utilizzare token fisici o applicazioni di autenticazione per una maggiore sicurezza.

3. Aggiornamenti regolari

1. Garantire che tutti i sistemi, software e dispositivi siano aggiornati con le ultime patch di sicurezza.

2. Monitorare costantemente le vulnerabilità note e implementare misure correttive.

Backup e ripristino

1. Eseguire backup regolari e sicuri dei dati aziendali.

2. Testare periodicamente il processo di ripristino per garantire la disponibilità dei dati in caso di attacco.