Report Remediation&Mitigation di Minacce di Phishing

1. Identificazione della Minaccia

Cos'è il phishing e come funziona

Il phishing è una tecnica di attacco informatico che mira a ingannare gli utenti per ottenere informazioni sensibili come credenziali di accesso, dati finanziari o informazioni personali. Gli attaccanti inviano email fraudolente che sembrano provenire da fonti legittime, come colleghi, istituti finanziari o fornitori fidati. Queste email spesso includono link a siti web falsi o allegati contenenti malware.

Tipi di phishing

1. **Email Phishing:** Email false inviate a un vasto numero di destinatari, spesso con messaggi generici e link a siti fraudolenti.
2. **Spear Phishing:** Attacchi mirati a specifici individui o organizzazioni, con messaggi personalizzati per aumentare la credibilità.
3. **Whaling:** Variante dello spear phishing che prende di mira dirigenti o persone con ruoli di alto profilo all'interno di un'organizzazione.
4. **Smishing:** Phishing tramite SMS o messaggi di testo che contengono link malevoli.
5. **Vishing:** Phishing telefonico in cui l'attaccante tenta di ottenere informazioni sensibili tramite una chiamata.
6. **Clone Phishing:** L'attaccante invia una versione clonata di un'email legittima già ricevuta dalla vittima, sostituendo allegati o link con versioni malevoli.

Esempi di phishing:

- **Email falsa da una banca:** Gli attaccanti inviano un'email che sembra provenire dalla banca dell'utente, chiedendo di confermare i dati di accesso per "motivi di sicurezza". L'email contiene un link a un sito web che imita quello ufficiale della banca.
- **Fatture fraudolente:** Un'azienda riceve un'email con una falsa fattura da un fornitore apparente, contenente un allegato con malware.
- **Richiesta di aggiornamento password:** Un dipendente riceve un'email apparentemente dal reparto IT, che richiede di cliccare su un link per aggiornare la password aziendale.

Come un attacco di phishing può compromettere la sicurezza dell'azienda:

- Accesso non autorizzato ai sistemi aziendali tramite credenziali rubate.
- Furto di dati sensibili, come informazioni sui clienti, piani aziendali o segreti industriali.
- Diffusione di malware, ransomware o altri software dannosi nella rete aziendale.
- Perdita di fiducia da parte dei clienti e danni alla reputazione dell'azienda.

---

2. Analisi del Rischio

Impatto potenziale sull'azienda:

- **Economico:** Costi associati alla risposta all'incidente, ripristino dei sistemi e potenziali multe per violazione di normative sulla protezione dei dati.
- **Operativo:** Interruzione delle attività aziendali e perdita di produttività.
- **Reputazionale:** Diminuzione della fiducia dei clienti e danni all'immagine pubblica dell'azienda.

Esempi di impatto:

- **Furto di credenziali:** Se un dipendente fornisce credenziali aziendali in seguito a un attacco di phishing, gli attaccanti potrebbero accedere a sistemi critici, interrompendo operazioni fondamentali come l'accesso ai database dei clienti o ai sistemi ERP.
- **Diffusione di ransomware:** Un allegato infetto scaricato tramite un'email di phishing può bloccare l'accesso ai file aziendali fino al pagamento di un riscatto, paralizzando l'intera infrastruttura.

Risorse che potrebbero essere compromesse:

- **Credenziali di accesso:** Permettono l'accesso non autorizzato ai sistemi aziendali.
- **Informazioni sensibili:** Come dati personali di clienti, segreti industriali o piani strategici.
- **Database:** Archivi contenenti informazioni vitali per il funzionamento dell'azienda.
- **Sistemi IT:** Infrastrutture essenziali che possono essere danneggiate o rese inaccessibili.

---

3. Pianificazione della Remediation

Piano per rispondere all'attacco di phishing:

1. **Identificazione e blocco delle email fraudolente**
    - **Filtri anti-phishing avanzati:** Utilizzare strumenti di protezione email che analizzano l'header della email, il contenuto, e i link per identificare segnali di phishing. Questi strumenti eseguono un controllo incrociato dei domini sospetti e segnalano le email provenienti da fonti non verificate.
    - **Segnalazione automatica dei domini compromessi:** Creare regole automatiche nel server di posta per identificare indirizzi email con dominio sospetto. Ad esempio, se una banca legittima ha sempre il dominio "banca.com", un'email che proviene da "banca-com.com" verrà automaticamente identificata come potenziale phishing e bloccata.
    - **Utilizzo di blacklist e threat intelligence feeds:** Abilitare l'integrazione con blacklist dinamiche e servizi di threat intelligence per tenere traccia di nuovi domini e indirizzi IP associati a phishing.

2. **Comunicazione ai dipendenti**
    - **Alert tempestivo:** Inviare un'email ufficiale con oggetto come "Attacco di phishing in corso, non cliccare su link sospetti!" che include esempi concreti di email phishing in corso e le azioni che i dipendenti devono intraprendere (ad esempio, "Non cliccate su alcun link, segnate l'email come phishing").
    - **Creazione di un portale interno per segnalazioni:** Implementare un sistema automatizzato in cui i dipendenti possono segnalarci le email sospette tramite un pulsante di "segnala phishing" che invia un alert al team di sicurezza.

3. **Verifica e monitoraggio dei sistemi**
    - **Scansione con antivirus e antimalware:** Eseguire scansioni su tutti i sistemi aziendali per rilevare malware che potrebbe essere stato installato tramite allegati infetti o link fraudolenti. Utilizzare software per individuare e rimuovere minacce.
    - **Monitoraggio dei log di accesso:** Verificare i log di accesso sui sistemi aziendali per rilevare accessi non autorizzati che potrebbero derivare dall'uso di credenziali compromesse. Strumenti come Splunk possono essere configurati per allertare immediatamente su attività sospette.

---

4. Implementazione della Remediation

Passaggi pratici per mitigare la minaccia di phishing:

1. **Implementazione di soluzioni di sicurezza email:**

- **SPF, DKIM, DMARC:** Implementare questi protocolli per proteggere i domini aziendali e prevenire che gli attaccanti possano falsificare il mittente di un'email. SPF (Sender Policy Framework) specifica quali server possono inviare email per un dominio. DKIM (DomainKeys Identified Mail) aggiunge una firma crittografica alle email per verificarne l'integrità. DMARC (Domain-based Message Authentication, Reporting, and Conformance) definisce come gestire i messaggi che non passano i controlli SPF/DKIM.

  Esempio: Un attaccante cerca di inviare un'email usando l'indirizzo aziendale "segreteria@azienda.com", ma grazie alla configurazione DMARC, l'email viene respinta dal server del destinatario poiché non proviene dal server autorizzato.

- **Protezione avanzata con sandboxing:** Gli allegati sospetti vengono automaticamente inviati a un ambiente isolato (sandbox) per l'analisi. Soluzioni come Cuckoo Sandbox possono eseguire il codice al sicuro, rilevando comportamenti dannosi prima che raggiungano i destinatari.

  Esempio: Un dipendente riceve un allegato in un'email sospetta; invece di aprirlo direttamente, il sistema lo invia a una sandbox per analisi prima di permetterne l'apertura.

2. **Formazione dei dipendenti:**
   - **Sessioni di formazione interattiva:** Organizzare workshop e webinar mensili sui rischi del phishing, illustrando casi reali e spiegando tecniche di riconoscimento, come controllare il mittente, evitare link sospetti e utilizzare strumenti di verifica come Virustotal.

     Esempio: Durante una formazione, viene mostrato un esempio di email che appare legittima ma contiene errori ortografici, un url sospetto e una richiesta urgente, aiutando i dipendenti a riconoscere segnali di allarme.

   - **Simulazioni di phishing:** Creare simulazioni di attacchi di phishing inviando email simili a quelle reali. Analizzare i risultati e premiare chi ha segnalato correttamente le email sospette, e fornire corsi di recupero a chi ha cliccato sul link fraudolento.

3. **Aggiornamento delle policy di sicurezza aziendali:**
   - **Protocolli di segnalazione rapida:** Creare un canale di comunicazione dedicato e linee guida per la segnalazione rapida di potenziali attacchi di phishing. I

dipendenti devono sapere esattamente chi contattare e come procedere nel caso in cui ricevano email sospette.
- **Politiche di accesso alle informazioni sensibili:** Implementare il principio del minimo privilegio, limitando l'accesso a informazioni sensibili solo a coloro che ne hanno bisogno per il loro lavoro. Ad esempio, i dati finanziari possono essere accessibili solo al reparto contabilità.

---

5. Mitigazione dei Rischi Residuali

Misure per ridurre il rischio residuo:

1. **Simulazione di Phishing:**
   - **Campagne di phishing regolari:** Utilizzare piattaforme per lanciare campagne di phishing simulate su base mensile o trimestrale. Analizzare il tasso di clic sui link fraudolenti e fornire formazione mirata per i dipendenti che sono stati ingannati.

     Esempio: Durante una simulazione, il 20% dei dipendenti clicca su un link falso che porta a una pagina di login finta. Il team IT invia subito un promemoria sui rischi e su come riconoscere segnali di phishing.

2. **Implementazione di autenticazione a due fattori (2FA):**
   - **Abilitare 2FA su tutte le applicazioni aziendali sensibili:** Implementare 2FA per l'accesso a sistemi aziendali come email, sistemi ERP, e piattaforme di gestione file.

     Esempio: Se un dipendente ha le credenziali compromesse tramite phishing, l'implementazione di 2FA richiede comunque una seconda forma di autenticazione (come un codice inviato tramite SMS o un'app di autenticazione) per l'accesso ai sistemi aziendali.

3. **Aggiornamenti e patching regolari:**
   - **Implementazione di un piano di patching continuo:** Aggiornare regolarmente i sistemi operativi, i software di sicurezza e le applicazioni aziendali per proteggersi dalle vulnerabilità note che potrebbero essere sfruttate in combinazione con un attacco di phishing.

     Esempio: Se viene scoperta una vulnerabilità in un software di posta elettronica che potrebbe permettere l'esecuzione di codice dannoso da un'email di phishing,

un piano di patching rapido garantirà che tutti i sistemi siano protetti prima che gli attaccanti possano sfruttarla.

Con talimisure, l'azienda può ridurre drasticamente i rischi residui di un attacco di phishing, proteggendo le risorse aziendali e migliorando la consapevolezza dei dipendenti.

Per concludere

La prevenzione e la mitigazione degli attacchi di phishing richiedono un approccio olistico che combini tecnologie avanzate, formazione continua e policy aziendali solide. Implementando le misure descritte in questo report, l'azienda sarà in grado di ridurre significativamente il rischio di compromissione.