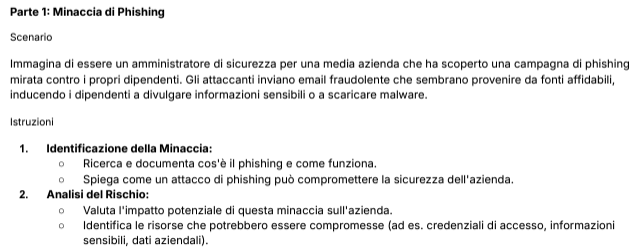
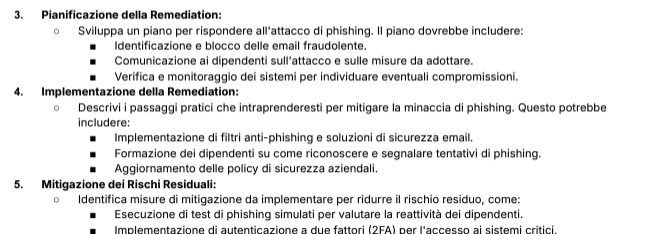
ESERCIZIO: Remediation e Mitigazione di Minacce di Phishing e Attacchi DoS





**IL PHISHING** è una tecnica di attacco informatico in cui un malintenzionato si finge un'entità affidabile per ingannare le persone e indurle a compiere azioni dannose. Solitamente, il phishing viene realizzato tramite email, messaggi di testo (smishing) o falsi siti web. L'obiettivo principale è rubare informazioni sensibili come credenziali di accesso, dati bancari o indurre l'utente a scaricare malware.

**COME FUNZIONA**

**Furto di credenziali,** se un dipendente fornisce credenziali aziendali (es. email, account cloud), l’attaccante può ottenere accesso non autorizzato a sistemi interni, email aziendali e documenti sensibili. **Installazione di malware,** allegati dannosi possono installare: **Ransomware**: Cifra i dati aziendali e richiede un riscatto per ripristinarli.

**Keylogger**: Monitora e registra tutto ciò che viene digitato, incluse password e dati sensibili.

**Backdoor**: Fornisce all'attaccante accesso permanente alla rete aziendale.

**Frode Finanziaria,** L'attaccante può impersonare un dirigente o un fornitore per ingannare i dipendenti e farsi trasferire denaro su conti fraudolenti.

**Violazione della Riservatezza,** I dati sensibili (es. contratti, progetti o dati dei clienti) possono essere estratti e venduti o esposti pubblicamente, causando: danni alla reputazione dell'azienda, sanzioni legali in caso di violazione di normative.

Un attacco phishing è una minaccia concreta per le aziende. Se non mitigato, può portare a furti di dati, perdite finanziarie e danni alla reputazione. La prevenzione richiede formazione continua dei dipendenti e robuste misure tecniche come filtri anti-phishing, autenticazione multi-fattore e monitoraggio costante della rete.

**LE RISORSE COMPROMESSE**

**Credenziali di Accesso**: Account email aziendali, Sistemi IT interni (ERP, CRM, sistemi cloud), Accessi amministrativi e VPN

**Informazioni Sensibili**: Dati aziendali riservati (progetti, contratti, piani strategici), Dati dei clienti (dettagli finanziari e contatti), Dati personali dei dipendenti

**Sistemi e Operazioni**: Sistemi critici per la produzione e gestione aziendale, Comunicazioni interne via email

**Risorse Finanziarie**: Conti bancari aziendali, Sistemi di pagamento e gestione delle fatture.

**PIANIFICAZIONE**

In risposta a una campagna di phishing mirata, è essenziale un piano coordinato per contenere, comunicare e monitorare la minaccia.

**IDENTIFICAZIONE E BLOCCO DELLE EMAIL FRAUDOLENTE**

**Analisi delle email sospette**: Identifica tutte le email fraudolente ricevute dai dipendenti. Analizza i dettagli tecnici, come gli header della mail, i link presenti e gli allegati.

Segnala i domini e gli indirizzi IP utilizzati dagli attaccanti.

**Blocco dei mittenti e dei domini**: Aggiorna i filtri email aziendali (es. gateway di sicurezza email) per bloccare mittenti sospetti e domini utilizzati, Implementa blacklist su firewall e proxy per bloccare gli URL dannosi identificati.

**Disabilitazione di link dannosi**: Se possibile, utilizza strumenti di sicurezza avanzata per neutralizzare link di phishing nelle caselle di posta dei dipendenti, Rimuovi eventuali allegati infetti dai sistemi di posta elettronica aziendale.

**COMUNICAZIONE AI DIPENDENTI E MISURE DA ADOTTARE**

**Comunicazione immediata**: Invia una comunicazione a tutti i dipendenti attraverso canali sicuri (es. intranet aziendale, Teams o Slack), informandoli della campagna phishing in corso, Spiega chiaramente le caratteristiche delle email fraudolente: mittenti sospetti, linguaggio utilizzato e azioni da evitare (es. non cliccare link o scaricare allegati).

**Istruzioni pratiche per i dipendenti**: Chiedi di segnalare immediatamente le email sospette al team IT tramite un indirizzo email dedicato o un sistema di ticketing, Fornisci istruzioni su come eliminare email dannose ricevute, Ricorda ai dipendenti di non condividere credenziali o informazioni sensibili via email.

**Sessione di formazione rapida**: Organizza un breve webinar o una guida scritta per insegnare ai dipendenti come riconoscere un attacco phishing e quali comportamenti adottare, Evidenzia segnali tipici delle email fraudolente: URL sospetti, richieste urgenti, mittenti non riconosciuti e allegati insoliti.

**VERIFICA E MONITORAGGIO DEI SISTEMI PER INDIVIDUARE EVENTUALI COMPROMISSIONI**

**Monitoraggio dei log di accesso** Controlla i log di accesso a email aziendali, VPN e sistemi critici per rilevare attività anomale (es. accessi da IP insoliti, tentativi di login falliti), Identifica eventuali account compromessi e procedi con il reset delle credenziali.

**Scansione degli endpoint**: Esegui una scansione antivirus e anti-malware su tutti i dispositivi aziendali per individuare eventuali malware o allegati dannosi scaricati dai dipendenti, Isola immediatamente i dispositivi infetti e procedi con la bonifica.

**Analisi dei sistemi critici**: Verifica l’integrità dei server, delle applicazioni aziendali e dei database per assicurarti che non ci siano state esfiltrazioni di dati o accessi non autorizzati, Monitora la rete per rilevare attività sospette, come il trasferimento di dati inusuali o connessioni anomale verso l’esterno.

**Audit della sicurezza**: Valuta lo stato di salute della sicurezza aziendale attraverso controlli approfonditi su credenziali, privilegi utente e vulnerabilità nei sistemi, Rafforza le misure di protezione nei punti identificati come deboli.

**Report finale dell’incidente**: Documenta l’intero processo di risposta, incluse le email fraudolente rilevate, i sistemi coinvolti e le azioni adottate per mitigare il rischio, Identifica le lezioni apprese e implementa nuove misure preventive per evitare attacchi futuri.

**IMPLEMENTAZIONE DI FILTRI ANTI-PHISHING E SOLUZIONI DI SICUREZZA EMAIL**

**Configurazione di gateway di sicurezza email**: Implementazione di soluzioni avanzate di sicurezza per le email come Proofpoint, Microsoft Defender for Office 365, o Mimecast, Questi sistemi filtrano email sospette, allegati dannosi e URL malevoli, riducendo il numero di email phishing che raggiungono le caselle di posta.

**Abilitazione di controlli avanzati sui link e sugli allegati**: Utilizzo di sandboxing per analizzare allegati e URL in un ambiente isolato prima che vengano consegnati ai destinatari, Attivazione di soluzioni che neutralizzano i link dannosi tramite URL rewriting, impedendo l'accesso a pagine di phishing.

**Blacklist di domini e indirizzi IP malevoli**: Aggiornamento costante dei filtri email con domini, IP e parole chiave identificati nelle campagne phishing, Integrazione con database di minacce pubblici e privati (es. VirusTotal).

**FORMAZIONE DEI DIPENDENTI SU COME RICONOSCERE E SEGNALARE TENTATIVI PHISHING**

**Workshop e sessioni di formazione:** Organizzazione di sessioni pratiche per insegnare ai dipendenti a riconoscere email sospette. Spiegazione dei segnali di phishing:

* + Errori grammaticali o di formattazione.
  + URL sospetti o domini simili a quelli autentici (es. *microsoft-support.com* invece di *microsoft.com*).
  + Richieste urgenti o insolite (es. aggiornare password o inviare dati riservati).
  + Presenza di allegati non richiesti.

**Simulazioni di phishing:** Lancio di campagne simulate di phishing interne per valutare la risposta dei dipendenti e migliorare la loro capacità di identificare email malevole..

**Canali di segnalazione facili e veloci:** Implementazione di un processo chiaro per segnalare email sospette (es. pulsante "Segnala phishing" in Outlook o invio a un indirizzo dedicato). Creazione di un team IT pronto a rispondere rapidamente alle segnalazioni.

**Materiale di supporto continuo:** Creazione di guide visive e checklist facilmente consultabili che riassumano i segnali chiave per riconoscere un’email di phishing, Invio periodico di promemoria con esempi di phishing aggiornati per mantenere alta l’attenzione.

**AGGIORNAMENTO DELLE POLICY DI SICUREZZA AZIENDALI**

Le policy aziendali devono essere aggiornate per includere linee guida e requisiti specifici per la gestione delle minacce phishing. Ecco le azioni principali:

**Policy di gestione delle email**: Vietare l’invio di informazioni sensibili via email, a meno che non siano criptate e autorizzate, Definire procedure per verificare richieste sospette ricevute via email (es. richieste di pagamenti urgenti).

**Obbligo di Multi-Factor Authentication (MFA)**: Richiedere l’implementazione dell’autenticazione a più fattori per tutti gli account aziendali (email, VPN, sistemi cloud), riducendo l’impatto di eventuali credenziali compromesse.

**Policy di gestione delle credenziali**: Imporre il cambio periodico delle password aziendali e vietare l’utilizzo di password duplicate tra account aziendali e personali, Implementare policy per la creazione di password robuste (es. almeno 12 caratteri, con lettere, numeri e simboli).

**Procedure di risposta agli incidenti**: Aggiornare il piano di risposta agli incidenti per includere azioni specifiche contro il phishing, come l’isolamento rapido di account compromessi, la bonifica di endpoint infetti e il ripristino delle credenziali.

**Rafforzamento della cultura della sicurezza**: Promuovere una cultura della cybersecurity tramite aggiornamenti regolari, simulazioni e campagne di sensibilizzazione, Includere policy chiare che richiedano ai dipendenti di segnalare immediatamente qualsiasi email sospetta.

### **Misure di Mitigazione per Ridurre il Rischio Residuo da Phishing**

### Per mitigare ulteriormente il rischio residuo dopo aver affrontato una campagna di phishing, è necessario implementare misure di controllo continuo, tecniche e organizzative. Le seguenti azioni mirano a rafforzare la resilienza aziendale e a prevenire attacchi futuri.

### **1. ESECUZIONE DI TEST PHISHING SIMULATI**

### **Obiettivo**: Valutare la capacità dei dipendenti di riconoscere e reagire correttamente a tentativi di phishing.

### **Implementazione**: Creazione di campagne simulate di phishing utilizzando strumenti dedicati come GoPhish, Microsoft Attack Simulation Training (Microsoft 365) o piattaforme equivalenti, Inviare email di phishing realistiche ai dipendenti in momenti inattesi, ma controllati, per testare la loro risposta.

### Monitorare: Percentuale di dipendenti che cliccano sui link, Percentuale di segnalazioni al team IT

### **Feedback e formazione**: Fornire ai dipendenti feedback immediato quando cadono nel test simulato, Offrire sessioni di formazione aggiuntiva a coloro che risultano più vulnerabili. **Valutazione periodica**: Pianificare test simulati ogni trimestre per monitorare i miglioramenti e individuare nuovi rischi.

### **2. IMPLEMENTAZIONE DELL’AUTENTICAZIONE A DUE FATTORI (2FA/MFA)**

**Obiettivo**: Proteggere l’accesso ai sistemi critici anche in caso di compromissione delle credenziali.

**Implementazione**: Abilitare l’autenticazione a due fattori (2FA) o multi-fattore (MFA) su tutti i sistemi aziendali critici:

* + - VPN e accessi remoti.
    - Sistemi ERP, CRM e database aziendali.
    - Console di amministrazione IT e servizi cloud.

Utilizzare app di autenticazione come Microsoft Authenticator, Google Authenticator o soluzioni hardware come YubiKey per generare codici univoci temporanei.

**Applicazione universale**: Rendere la 2FA obbligatoria per tutti i dipendenti e collaboratori esterni con accesso ai sistemi aziendali.

**Verifica periodica**: Controllare l’implementazione della 2FA e assicurarsi che non ci siano account esclusi per errore.

### **3. REGOLARI AGGIORNAMENTI E PATCHING DEI SISTEMI**

**Obiettivo**: Ridurre le vulnerabilità sfruttabili dai cybercriminali per introdurre malware tramite phishing.

**Implementazione**:

**Patch Management**: Adottare una politica di aggiornamento regolare per sistemi operativi, software applicativi e dispositivi aziendali, Utilizzare strumenti centralizzati come WSUS (Windows Server Update Services), SCCM o piattaforme di gestione delle patch di terze parti,

**Gestione delle vulnerabilità**: Eseguire periodicamente scansioni delle vulnerabilità utilizzando strumenti come Nessus, Qualys o OpenVAS, Identificare e mitigare rapidamente le vulnerabilità critiche prima che possano essere sfruttate.

**Aggiornamento antivirus e anti-malware**: Mantenere aggiornate le firme dei software antivirus/anti-malware aziendali e garantire una protezione in tempo reale su tutti gli endpoint.

**Gestione del software obsoleto**: Identificare e rimuovere software non supportati o non aggiornati che potrebbero rappresentare una vulnerabilità.

### **4. MONITORAGGIO CONTINUO E AUTOMAZIONE DELLA SICUREZZA**

* Implementare un **SIEM (Security Information and Event Management)** per raccogliere e analizzare log di sistema e rilevare attività anomale.
* Abilitare il **monitoraggio continuo della rete e degli endpoint** con soluzioni come **EDR (Endpoint Detection and Response)** o **XDR (Extended Detection and Response)**.
* Automatizzare risposte rapide alle minacce tramite **playbook di sicurezza** per identificare e isolare endpoint compromessi.

.