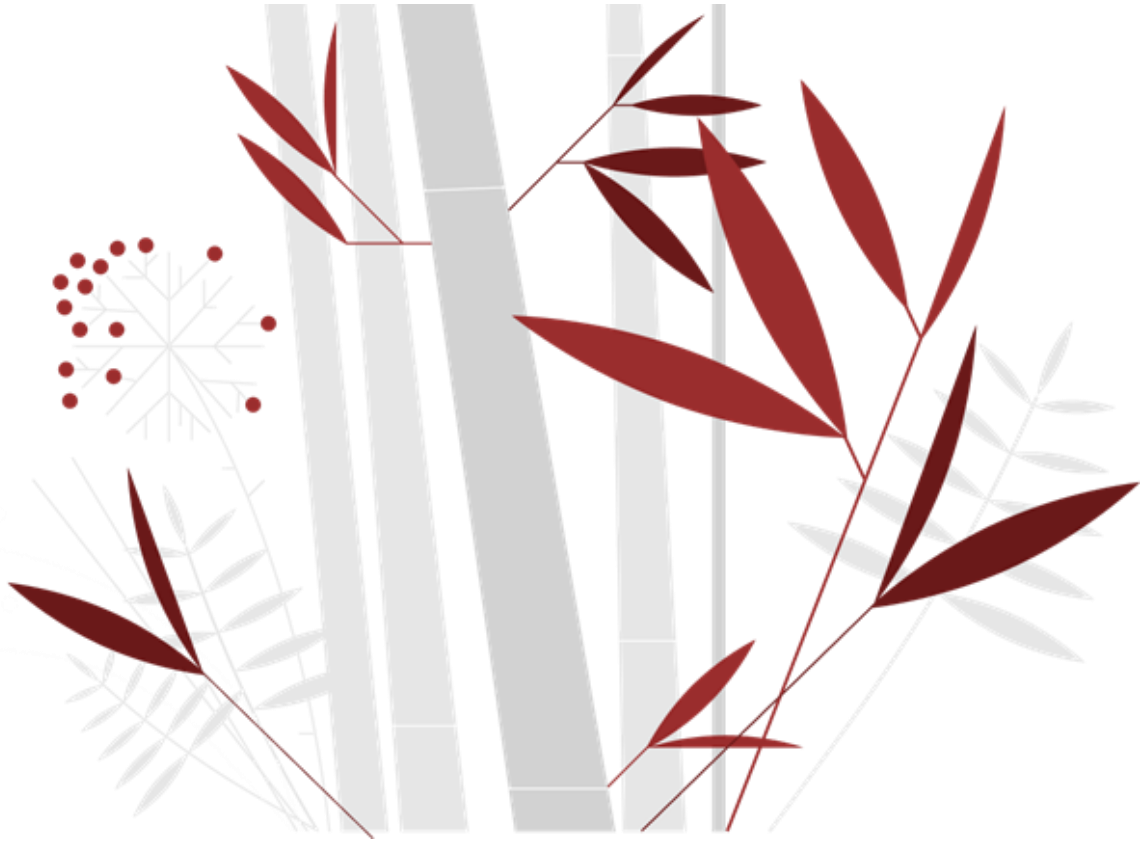
CYBER SECURITY & ETHICAL HACKING

Remediation e Mitigazione

Sara Maimone

S11.L1

09/12/2024



Cos'è il phishing e come funziona?

Il phishing è una tecnica di ingegneria sociale in cui gli attaccanti inviano email, messaggi o persino telefonate che sembrano provenire da fonti affidabili, come colleghi, partner o enti ufficiali. Queste comunicazioni contengono spesso un senso di urgenza per spingere la vittima ad agire rapidamente, ad esempio cliccando su un link che porta a un sito contraffatto o scaricando un allegato infetto.

Ad esempio, in questa campagna specifica, i dipendenti ricevono email apparentemente provenienti dall'ufficio HR, che li invita a completare un aggiornamento sui dati personali tramite un link. Questo link, però, reindirizza a un sito malevolo progettato per rubare le credenziali.

Impatto sulla sicurezza aziendale

Le conseguenze di un attacco di phishing possono essere devastanti per un'azienda. Se un dipendente cade nella trappola, l'azienda potrebbe subire una compromissione delle credenziali che permette agli attaccanti di accedere ai sistemi interni. Questo potrebbe portare a:

1. **Esposizione di dati sensibili**, come informazioni sui clienti, strategie aziendali o dettagli finanziari.
2. **Installazione di malware**, come ransomware, che blocca l'accesso ai dati aziendali fino al pagamento di un riscatto.
3. **Perdita di fiducia da parte dei clienti e dei partner**, che può influire sulla reputazione aziendale.
4. **Costi significativi** per rispondere all'incidente e rafforzare le difese.

Come affrontare l'attacco: il piano di remediation

Affrontare una campagna di phishing richiede un approccio rapido ma strutturato, che prevede diverse fasi.

1. Identificazione e blocco delle email fraudolente

Per prima cosa, è essenziale utilizzare i sistemi di sicurezza per identificare e bloccare le email sospette. Ad esempio:

- Configurare strumenti come **SPF, DKIM e DMARC** per verificare l’autenticità delle email in entrata.
- Analizzare i log dei server di posta per individuare l'origine delle email fraudolente e aggiungerla alla blacklist.

In parallelo, i dipendenti vanno avvisati del rischio. Una comunicazione chiara deve spiegare l’attacco in corso, mostrare esempi di email malevole e fornire istruzioni su come comportarsi (es. non cliccare sui link, non scaricare allegati sospetti e segnalare immediatamente le email sospette).

2. Monitoraggio dei sistemi per verificare eventuali compromissioni

Mentre si affronta l'attacco, è fondamentale verificare che i sistemi non siano già stati compromessi. Questo può includere:

- Controllo delle attività di accesso per rilevare tentativi di login sospetti.
- Scansioni dei dispositivi aziendali per malware o software non autorizzati.

Implementazione delle misure correttive

Oltre a rispondere all'attacco in corso, è necessario implementare misure preventive per ridurre il rischio futuro.

1. Rafforzare la sicurezza delle email

L'utilizzo di un gateway di sicurezza per le email può aiutare a filtrare i messaggi potenzialmente dannosi prima che raggiungano i dipendenti. Questi strumenti possono analizzare i contenuti delle email in cerca di segni di phishing, come link abbreviati o mittenti sospetti.

2. Formazione dei dipendenti

I dipendenti devono essere educati a riconoscere i segnali di phishing. Ad esempio:

- Controllare l'indirizzo del mittente per verificare che sia autentico.
- Passare il cursore sopra i link per vedere l'URL reale prima di cliccare.
- Diffidare di email che richiedono azioni immediate e forniscono un senso di urgenza.

Una sessione di formazione interattiva può aiutare, magari includendo simulazioni di phishing per valutare la loro capacità di identificare le minacce.

3. Aggiornamento delle policy di sicurezza

Le policy aziendali devono essere riviste per includere procedure specifiche per gestire il phishing, come:

- Obbligo di utilizzo di password complesse e univoche.
- Implementazione di autenticazione a due fattori (**2FA**) per tutti i sistemi critici.
- Creazione di una politica di gestione delle email sospette.

Riduzione dei rischi residui

Una volta affrontato l'attacco e implementate le misure correttive, è importante continuare a monitorare e testare l'efficacia delle difese. Tra le attività da considerare:

1. **Simulazioni di phishing periodiche:** inviare email simulate ai dipendenti per testare la loro attenzione e capacità di risposta.
2. **Aggiornamenti regolari dei sistemi:** garantire che tutte le applicazioni e i sistemi operativi siano aggiornati con le ultime patch di sicurezza.
3. **Backup regolari:** mantenere backup aggiornati e protetti dei dati aziendali, in modo da poterli ripristinare rapidamente in caso di incidente.

Questo approccio sistematico permette non solo di rispondere all’attacco in corso, ma anche di rafforzare la resilienza dell'azienda contro minacce future.