CERBEYRA
your safe digital future

Phishing Simulator

Il servizio gestito per testare la consapevolezza degli utenti e rafforzare la difesa aziendale

Gli attacchi di phishing: una minaccia concreta

Gli attacchi di phishing sono tra le minacce più frequenti e pericolose per le aziende. Spesso **sfruttano la distrazione o l'inesperienza degli utenti** per ottenere accesso a **informazioni riservate** o compromettere l'**infrastruttura IT**.

Per rispondere a questa esigenza, **Cerbeyra mette a disposizione un servizio di Phishing Simulator completamente gestito**, progettato per testare in modo sicuro la reazione delle persone a tentativi di phishing simulati e migliorare la loro capacità di riconoscerli.

Un servizio su misura, progettato insieme al partner

Il servizio viene attivato **in collaborazione con il partner**, a partire da **una sessione iniziale di onboarding** in cui **il team Cerbeyra guida l'analisi degli obiettivi del cliente** e aiuta a scegliere gli scenari di attacco più rilevanti.

In base al contesto aziendale, è possibile simulare campagne ispirate a:

- Email di corrieri (es. "Il tuo pacco non è stato consegnato")
- Comunicazioni LinkedIn o altri social
- Finti avvisi di sicurezza o recupero credenziali

Anche la grafica delle email può essere adattata per massimizzare il realismo dell'attacco simulato.

Tre fasi per una simulazione efficace

1. Verifica tecnica iniziale
Analisi della configurazione del mail server del cliente, verifica dei record SPF, DKIM e DMARC. **Suggerimenti su eventuali adeguamenti** per garantire la corretta ricezione delle email simulate, evitando blocchi o spam.

2. Esecuzione della campagna simulata
Invio delle email agli utenti target, monitoraggio delle azioni compiute: apertura dell'email, clic su link, compilazione moduli, segnalazione del phishing.

3. Report e follow-up
Report dettagliati con indicatori aggregati e anonimizzati, identificazione dei comportamenti a rischio, suggerimenti per eventuali azioni correttive o percorsi formativi personalizzati.

Perché adottare il Phishing Simulator

- **Valuta la reale consapevolezza degli utenti**
- **Individua le vulnerabilità comportamentali** prima che siano sfruttate da un **attacco reale**
- **Aumenta la resilienza aziendale** con un approccio formativo concreto
- **Nessun rischio per l'infrastruttura**: tutto avviene in ambiente controllato

Tecnologia sicura e conforme

Il simulatore utilizza **infrastrutture dedicate e tecniche di invio email conformi alle best practice di deliverability**. Il team Cerbeyra fornisce supporto completo nella configurazione e nella gestione delle eccezioni lato server di posta (Exchange, Microsoft 365, Google Workspace ecc.).

I dati raccolti sono trattati nel rispetto della privacy e non vengono mai usati per finalità diverse dalla simulazione stessa.

Un modulo della suite di Cyber Threat Intelligence: **Cognitive Security Cerbeyra**

Il **Phishing Simulator** è parte della nostra strategia di **Cognitive Security** inclusa nella piattaforma di **Cyber Threat Intelligence** ma con un add-on, la possibilità di avere un **servizio completamente gestito**. Un support a 360° per:

- Campagne di simulate per rafforzare l'awareness dei dipendenti continue
- Dashboard di rischio comportamentale per campagna e per utente
- Possibilità di effettuare corsi di Cerbeyra Academy mirati di Cognitive Security

L'obiettivo è ridurre il rischio umano, spesso sottovalutato, ma **determinante per la sicurezza aziendale**.

CERBEYRA
your safe digital future

Cerbeyra S.p.A. - Gruppo Vianova S.p.A
Via Libeccio 48/F - Z.I. Cotone
55049 Viareggio (LU)
P.IVA e CF 01766360463

www.cerbeyra.com | info@cerbeyra.com | 0584.43671