PENTESTERRA

PHISHING SIMULATION

I Tuoi Dipendenti Cliccherebbero su un'Email Vera?

Simulazione di phishing costruita su OSINT reale - ruolo, interessi, attività pubblica - non un template generico spedito a tutti.

COS'È UNA PHISHING SIMULATION, IN BREVE

È il test della sicurezza informatica (cyber) del tuo anello più debole: le persone. Ogni scenario è costruito partendo da informazioni pubbliche reali sul bersaglio - ruolo, strumenti, progetti, interessi personali - per misurare il rischio reale, non una percentuale di click su un'email che nessuno avrebbe mai aperto.

OSINT

Ogni scenario è costruito sul contesto, non su un template

1:1

Spear phishing su target nominati e realmente studiati

Attack Chain

Una credenziale catturata continua l'attacco, non finisce lì

LA SITUAZIONE OGGI

CHI SEI

Sei il CISO, l'HR security lead o il responsabile awareness di un'azienda che deve sapere se i propri dipendenti cadrebbero davvero in un'email di phishing scritta come la scriverebbe un attaccante reale, non un template generico.

COSA È SUCCESSO

La formazione di awareness dell'anno scorso ha avuto un tasso di completamento oltre il 90%, e nessuno ricorda una parola. Un'unica email convincente resta la via più veloce per entrare nella maggior parte delle aziende.

IL PROBLEMA

Non sai, con certezza, se i tuoi dipendenti resisterebbero a un phishing costruito con la stessa cura con cui lo costruirebbe un vero attaccante. Una simulazione generica con un'email da "reimposta la password" misura poco o nulla del rischio reale.

PERCHÉ FA MALE

Una credenziale catturata con un'unica email convincente può dare a un attaccante l'accesso iniziale a tutta la tua rete. Un audit, un cliente o un assicuratore cyber possono chiedere prova che il rischio umano sia misurato come un controllo di sicurezza, non trattato come un esercizio HR isolato.

DOVE VUOI ARRIVARE

STATO DESIDERATO

Vuoi sapere, con prova concreta, quanto i tuoi dipendenti resisterebbero a un phishing mirato e realistico - e cosa succede davvero dopo un click, non solo una percentuale.

LA SOLUZIONE

Una **Phishing Simulation** con scenari costruiti da OSINT reale sul bersaglio - ruolo, progetti, interessi personali - un toolkit di campagna completo con tracciamento per destinatario, e una credenziale catturata che prosegue nell'attack chain per mostrare l'impatto reale.

PERCHÉ È DIVERSO

Non stai comprando l'ennesimo simulatore di phishing con template generici. Stai lavorando con [NOME AZIENDA] - fornitore certificato, italiano, con quasi 20 anni di storia nel settore della sicurezza informatica. Probabilmente ci conosci già, o conosci qualcuno - un collega, un fornitore, un concorrente - che è già stato nostro cliente. Molti dei tuoi concorrenti diretti si stanno già rivolgendo a noi. E ogni pretesto nasce da OSINT reale sul bersaglio - ruolo, progetti, interessi personali - mentre una credenziale catturata prosegue nello stesso motore di attack chain usato dal resto della piattaforma, per mostrare l'impatto reale di un click, non solo una percentuale.

PROVA CONCRETA

Il risultato è un report PDF completo, pronto da consegnare, con tassi di apertura, click e invio per team, ruolo e anzianità. Se emergono gap più ampi, ti proponiamo le misure aggiuntive per colmarli: vulnerability assessment, penetration test di rete o applicativo, revisione DevGuard del codice.

Opt-in

Interessi e hobby pubblici usati solo con consenso, per personalizzare il pretesto

Non distruttivo

Nessuna credenziale reale viene mai autenticata o conservata

Per Team

Risultati misurabili per reparto, ruolo e anzianità

COSA INCLUDE DAVVERO

Scenari costruiti su OSINT reale, un toolkit di campagna completo, e un collegamento diretto con il resto dell'attack chain.

Contestuale, non spam da template

Il pretesto nasce da informazioni pubbliche reali sul bersaglio, non da un blast generico.

- Scenari costruiti da OSINT reale: ruolo, progetti, strumenti, contesto professionale pubblico e interessi personali
- Targeting consapevole del ruolo e del reparto
- Spear phishing su target di alto valore nominati, non solo campagne di massa
- Riutilizza lo stesso livello di intelligence usato per pentest e reporting

Toolkit di campagna completo

Profili di invio, landing page, libreria di template e schedulazione in un unico posto.

- Landing page e flussi di cattura credenziali, non distruttivi
- Profili di invio con controllo di dominio e header
- Libreria di template riutilizzabile tra campagne
- Tracciamento di apertura, click e invio per singolo destinatario

Rischio umano come controllo misurato

La simulazione di phishing è un test di controllo di sicurezza, non un esercizio HR.

- Tassi di click e invio per team, ruolo e anzianità
- Campagne ripetute per misurare la deriva nel tempo
- Collegamento diretto al follow-up della formazione di awareness
- Evidenza adatta a compliance e audit

Parte di un attack chain, non un silo

Una credenziale o sessione catturata è un artefatto, non solo una riga in un report.

- Gli artefatti di credenziali e sessione alimentano il motore di attack chain
- Mostra cosa fa davvero un attaccante dopo il click, non solo che ha cliccato
- Si incrocia con i finding di external exposure e di rete
- Un unico report che copre persone e infrastruttura insieme

PENTESTERRA

PHISHING SIMULATION

COSA RICEVI

- ✓ Un report PDF completo con tassi di apertura, click e invio per team e ruolo
- ✓ Scenari di phishing personalizzati costruiti su OSINT reale, con consenso
- ✓ Tracciamento per destinatario, dalla consegna all'eventuale invio credenziali
- ✓ Collegamento diretto con l'attack chain per mostrare l'impatto reale di un click
- ✓ Executive summary pronto per il tuo consiglio o per un cliente enterprise

COME FUNZIONA

1

Definiamo il target

Un reparto, un ruolo, o individui specifici - stabiliamo insieme lo scope.

2

Costruiamo il pretesto

Scenario personalizzato da OSINT reale sul bersaglio, con consenso.

3

Lanciamo la campagna

Tracciamento per destinatario, dalla consegna all'eventuale click.

4

Ti consegniamo il report

Un PDF completo con i risultati prioritizzati e le azioni da intraprendere.

Scopri se i tuoi dipendenti resistono a un phishing reale

Un report completo, pronto da presentare a clienti, auditor o al tuo consiglio di amministrazione.

Richiedi la tua Phishing Simulation →

info@pentesterra.com · pentesterra.com/phishing-simulation