ETHICAL HACKING · BROCHURE

I tuoi dipendenti sono preparati ad affrontare attacchi progettati per ottenere informazioni sensibili?

Scoprilo con una campagna di *Phishing etico*

CYBERFERO

Cos'è il phishing?

Si tratta di un fenomeno di **truffa informatica** che consiste nel sottrarre le credenziali di autenticazione facendole inserire all'utente stesso in una **pagina falsa** che appare identica a quella di un servizio che il destinatario usa realmente.

Gli attacchi *phishing* di questo tipo sono **difficili da individuare in modo automatico**, perché i link nelle email potrebbero apparire legittimi a una macchina.

L'unico modo per evitare di venire ingannati è **sapere a quali indicatori fare attenzione ed essere sempre all'erta**. Per questo è importante lavorare per aumentare la resilienza del proprio team a questo tipo di attacchi.

Se i dipendenti dell'azienda sono in grado di individuare i tentativi di attacco, i dati della compagnia saranno più al sicuro.

> *L'elemento più facilmente hackerabile è il dipendente distratto o ingenuo. Fornirgli le risorse adeguate protegge lui e tutta l'azienda.*

I dati sono allarmanti

96%
degli attacchi arriva via email

2M+
siti di phishing attivi

$80K
perdita media per azienda

69%
dei breach causati da dipendenti

I vantaggi di una campagna di Phishing etico

01

Testa la difesa aziendale

Testeremo i vostri dipendenti inviando messaggi del tutto simili a quelli di una *campagna phishing*, ma in **ambiente controllato**, senza mai mettere a rischio realmente l'azienda.

Raccoglieremo le risposte e le analizzeremo per generare un report e una **formazione mirata**.

02

Analizza i risultati

La campagna di *Ethical Phishing* produce **report dettagliati** contenenti informazioni essenziali per identificare i punti deboli negli scenari testati.

Alcune informazioni raccolte: numero di aperture messaggi, numero di click, quali credenziali vengono usate, ecc. I dati quantificano anche la **consapevolezza degli utenti** nel riconoscere email sospette.

03

Forma i dipendenti in modo specifico

Organizza una **campagna di formazione e sensibilizzazione** alla sicurezza informatica per i dipendenti.

Conducendo il servizio di *phishing etico* e utilizzando i risultati per personalizzare il programma di formazione, l'intervento risulta essere **molto più efficace**.

Metodologie usate

Raccolta di credenziali

Questo tipo di *phishing* fa leva sull'attacco diretto a persone che non sono del tutto consapevoli delle **tecniche di hacking**.

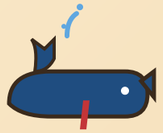
Convinceremo i dipendenti dell'azienda a rivelare le loro credenziali.

Ideale per valutare la **permeabilità dei dipendenti** agli attacchi di *phishing*; le credenziali ottenute possono essere riviste per garantire aderenza a una **policy adeguata**.

Spear phishing

In questo caso l'attacco è diretto a un **gruppo target specifico di individui** (ad es. il dipartimento finanze).

Vengono usate **informazioni specifiche per l'obiettivo** o per gli obiettivi, per rendere il tentativo di *phishing* molto più credibile e selettivo.



Whaling

L'obiettivo dell'attacco sarà a **livello dirigenziale** all'interno dell'organizzazione.

Questi *target* sono particolarmente delicati perché una volta compromessi possono **esercitare una certa influenza** su altri dipendenti, amplificando i danni dell'attacco.

Il nostro approccio

Quali i traguardi da raggiungere

Fare una campagna di *Ethical Phishing* nei confronti di un'azienda che lo richiede significa scoprire i **punti deboli** dell'azienda attraverso l'occhio dell'attaccante, con l'obiettivo finale di effettuare una **vera e propria simulazione di attacco informatico**.

Cosa faremo

L'attività di *phishing* può comprendere fasi di **Social Engineering**, invio di messaggi o anche **telefonate-trappola**, volte a raccogliere informazioni sensibili o dati personali utilizzabili da un attaccante.

Cosa cerchiamo di trovare

La campagna ha l'obiettivo di scoprire **quanto i dipendenti siano sensibili e "raggirabili"** dalle truffe tramite contatti digitali. Capiremo quanto sono restii a divulgare **informazioni personali, codici di accesso o dati finanziari** dell'azienda.

Cosa aspettarsi dopo la campagna

Dopo la campagna e la conseguente **formazione mirata**, i dipendenti saranno in grado di difendere la propria azienda **semplicemente ignorando** i messaggi sospetti, fornendogli gli strumenti per riconoscerli.

La miglior difesa contro il phishing è saperlo riconoscere.

Dal **2011** ci occupiamo di tecnologia Cloud e di sicurezza, affidati a professionisti esperti.

Scegli la sicurezza per la tua azienda

Scopri il servizio sul sito

CYBERFERO

Per ulteriori informazioni, i nostri contatti sono:

Via Statuto 3,
42121 Reggio Emilia (RE)
www.cyberfero.com

Tel. +39 0522 1685330
E-mail: info@cyberfero.com
Pec: cyberfero@pec.it
P. IVA: 03058120357