Per battere il phishing serve formazione

20 MAGGIO 2025 - Parte I

Se c'è una minaccia alla sicurezza che sembra fuori portata anche per la tecnologia più avanzata, questa è il phishing. Proteggere dai cyber criminali la tua organizzazione formando tutti i dipendenti sul phishing non è un lusso, ma un dovere. Agisci ora!

SONO ORMAI CRONACA gli attacchi phishing che centrano il bersaglio superando filtri, firewall e soluzioni di endpoint security. E se il bersaglio è uno dei tuoi impiegati, un solo suo innocente clic potrebbe significare il disastro per la tua organizzazione.

Ma non crediate che gli attacchi phishing di ultima generazione possano essere, come in passato, individuati per esempio da errori grammaticali nel testo dei messaggi. Oggi i cyber criminali ricorrono all'IA generativa per superare le barriere linguistiche, attivare conversazioni dinamiche e persino adattarsi in tempo reale alla vittima.

Prima di procedere, vale la pena soffermarsi brevemente sulle definizioni.

Che cos'è il phishing?

Il *phishing* è un crimine informatico che si mette in atto contattando le vittime per email, telefono o altri tipi di messaggio testuale. Il malfattore si fa passare per qualcuno legittimamente titolato a chiedere dati sensibili, come informazioni personali, dettagli bancari o password.

Le informazioni carpite sono quindi usate per accedere agli account della vittima e possono comportare furto d'identità e perdite finanziarie.

Che cos'è l'IA generativa

Per *intelligenza artificiale generativa* si intendono gli algoritmi (come ChatGPT) utilizzabili per creare nuovi contenuti delle più varie tipologie: audio, codice, immagini, testi, simulazioni e video. La generazione di contenuti non sarà probabilmente mai più la stessa che conosciamo oggi.

In questo scenario del tutto impensabile solo poco tempo fa, è chiara l'importanza crescente del training sul phishing. Impiegati e collaboratori devono sapere che cosa aspettarsi e conoscere come reagire. È oggi che bisogna prepararsi con la formazione a contrastare la prossima generazione di minacce.

Il phishing tra evoluzione e innovazione

La formazione sul phishing rientra nel più generale piano formativo di security awareness (consapevolezza). Non si tratta semplicemente di insegnare agli impiegati a evitare di cliccare su link sospetti, bensì di spiegare le tattiche che usano i criminali informatici, i segni rivelatori di un attacco e le contromisure da adottare.

In una parola, un buon percorso formativo non si limita a trasferire informazioni, ma **agisce sui comportamenti**. Il nostro **cybertraining** fa esattamente questo: trasforma il comportamento degli utenti da anello debole della catena difensiva a prima linea di difesa contro il cyber crimine.

Non è che le minacce phishing siano nate oggi, sicuramente si stanno però evolvendo. Gli attacchi fanno leva sull'emotività e sul cosiddetto *bias cognitivo* (distorsione cognitiva), una sorta di pregiudizio che porta il cervello umano a semplificare l'interpretazione delle informazioni attraverso il filtro della personale esperienza e delle preferenze.

Efficaci esche psicologiche che aggirano l'approccio razionale e spingono ad agire senza troppo riflettere sono ad esempio:

- **Urgenza** - "Il tuo account verrà chiuso"
- **Autorità** - "Una richiesta dell'AD"
- **Paura** - "Rilevato login non autorizzato"
- **Cortesia** - "Mantieni aggiornati i tuoi dati anagrafici"
- **Curiosità** - "Hai una consegna in attesa"

Sul piano dell'innovazione i criminali informatici hanno trovato alleati preziosi in ChatGPT e altri chatbot basati sull'IA generativa, che permettono sofisticate

personalizzazioni e assicurano una conseguente grande efficacia. Dal lancio di ChatGPT gli attacchi phishing non hanno smesso di crescere.

31.000 MINACCE AL GIORNO
IN MEDIA NEL 2023

Il phishing - lo sottolineiamo ancora - non è un comune, irritante spam, ma qualcosa che può avere conseguenze catastrofiche per le organizzazioni, dalla perdita di dati a danni economici, fino a intaccare la reputazione e bloccare l'operatività: basta la leggerezza di un impiegato per provocare un disastro.

E affidarsi unicamente alle tecnologie di cyber security potrebbe rivelarsi una scelta miope. A che serve continuare a investire sulla protezione del perimetro, se poi sono gli utenti interni a rappresentare il vero punto debole? Trascurare la formazione vuol dire lasciare aperta una vulnerabilità in cui il nemico potrebbe insinuarsi.

La formazione come investimento strategico

Un buon investimento si riconosce dai buoni ritorni. La formazione sul phishing ha tutte le caratteristiche per occupare uno dei primissimi posti nelle scelte aziendali. Vediamole.

- **Riduce drasticamente il numero di attacchi riusciti**

Parecchie statistiche dimostrano che un training costante e continuativo, specie se corredato da simulazioni, riduce significativamente il numero dei dipendenti che cliccano su link malevoli o aprono allegati pericolosi.

- **Crea un "firewall umano" proattivo**

Gli impiegati si trasformano da anello debole della catena a difensori attivi. Imparando a riconoscere le minacce possono fornire in tempo reale resoconti dettagliati sugli attacchi phishing al team IT o alla security, informazioni di grande valore per la *cyber intelligence*.

- **Protegge i dati sensibili**

Riconoscere e fermare gli attacchi phishing prima che vadano a buon fine vuol dire proteggere gli asset aziendali di maggior valore: dati relativi ai clienti, informazioni finanziarie, segreti industriali, proprietà intellettuale, piani strategici.

- **Incide positivamente sulla redditività aziendale (ROI)**

I costi di un piano formativo globale esteso a tutto il personale sono niente se paragonati al costo potenziale di un solo attacco andato a buon fine, che potrebbe facilmente arrivare a centinaia di migliaia se non addirittura a milioni di Euro tra attività di ripristino, spese legali, multe per mancato rispetto di norme e regolamenti, perdita di fatturato.

- **Rafforza la conformità**

Leggi e regolamenti sulla protezione dei dati (come il GDPR) impongono l'acquisizione di awareness (consapevolezza) in tema di security. Un piano documentato di formazione per il personale aiuta a soddisfare questo requisito e dimostra *due diligence*.

- **Accresce la cultura della cybersecurity**

Una formazione regolare su argomenti relativi a specifiche minacce, come il phishing, promuove la cultura della security awareness. Il personale prende coscienza di altre pratiche raccomandabili e contribuisce alla sicurezza aziendale.

- **Migliora la fiducia del personale**

Sapere come riconoscere e contrastare potenziali minacce riduce il livello di ansia del personale nei confronti della cybersecurity. E sentirsi preparati ha un effetto positivo sul morale.

Nella Parte II daremo alcuni suggerimenti su come implementare un piano formativo efficace.

Contatto: Marcello Fontana
commerciale@gotech.it
+39 351 4272010