Milano, 21 ottobre 2022 - Fra le minacce informatiche più conosciute e diffuse rientra senza dubbio il cosiddetto “phishing”, ossia l’invio di e-mail di massa progettate per raccogliere credenziali da un ampio gruppo di persone. La logica di base è che se un criminale riesce a raggiungere un numero sufficiente di persone con una campagna di phishing, statisticamente qualcuno “abboccherà all’amo”. Un tranello insomma collaudato, contro il quale Cisco ha formulato una vera e propria GUIDA articolata in 5 consigli per prevenire e contrastare questo fenomeno.

Prima di vederla, cerchiamo di comprendere come funziona nel dettaglio il phishing moderno. I passaggi fondamentali sono:

1. Tutto inizia con una e-mail o un'altra comunicazione fraudolenta (ad esempio un SMS) nella quale il mittente sembra essere affidabile, inviata allo scopo di attirare una vittima.
2. Se l'inganno riesce, la vittima viene persuasa a fornire informazioni riservate, spesso su un sito web truffa.
3. Qualche volta, nel computer del malcapitato viene anche scaricato un malware.

Quali sono i pericoli degli attacchi di phishing?

A volte ai criminali informatici è sufficiente ottenere informazioni sulla carta di credito o su altri dati personali della vittima a scopo di lucro. Altre volte, le e-mail di phishing vengono inviate per rubare le credenziali di accesso dei dipendenti o altre informazioni utili a sferrare un attacco più sofisticato contro un'azienda specifica. Attacchi informatici come il ransomware o minacce avanzate persistenti (APT) spesso iniziano proprio con il phishing.

Come sensibilizzare gli utenti nei confronti degli attacchi di phishing?

Un modo per proteggere la propria organizzazione dal phishing è una adeguata formazione specifica che coinvolga tutti i dipendenti, compresi i dirigenti di alto livello che spesso sono essi stessi un obiettivo. È importante insegnare loro come riconoscere una e-mail di phishing e cosa fare quando ne ricevono una; altrettanto fondamentali sono gli esercizi di simulazione per valutare come i dipendenti reagiscono a un attacco di phishing nelle sue diverse fasi.

I vari tipi di phishing

Spear phishing

Lo spear phishing prende di mira singoli individui e non un gruppo di persone. I criminali informatici spesso cercano le loro vittime sui social media o su altri siti, in questo modo è più semplice personalizzare le comunicazioni affinché sembrino autentiche. Lo spear phishing è spesso il primo passo per superare le difese di un'azienda e realizzare un attacco mirato.

Whaling

Parliamo di whaling quando gli attaccanti prendono di mira un "pesce grosso", ad esempio un CEO. Spesso questi criminali trascorrono molto tempo a profilare il bersaglio, per trovare il momento e i mezzi opportuni con cui sottrarre le credenziali di accesso. Il whaling è un attacco particolarmente critico,

poiché i dirigenti di alto livello hanno accesso a numerose informazioni aziendali.

Pharming

Analogamente al phishing, il pharming dirotta gli utenti verso un sito web fraudolento che sembra perfettamente in regola. Tuttavia, in questo caso, le vittime non devono nemmeno fare clic su un link malevolo per accedere al sito fasullo. Gli attaccanti possono infettare il computer dell'utente o il server DNS del sito e reindirizzare l'utente a una pagina web fittizia anche se è stato digitato l'URL corretto.

Deceptive phishing

Il deceptive phishing, letteralmente phishing ingannevole, è il tipo di phishing più comune. In questo caso, un attaccante tenta di ottenere dalle vittime informazioni riservate da utilizzare per rubare denaro o lanciare altri attacchi. Una e-mail falsa proveniente da una banca che chiede di fare clic su un link e verificare i dettagli del proprio conto corrente è un esempio molto comune di deceptive phishing.

La GUIDA CISCO contro il PHISHING

1. Implementare un solido processo di autenticazione

L’autenticazione a più fattori (MFA) riduce significativamente il rischio di accesso non autorizzato ai dati, ma non tutti i metodi di autenticazione sono uguali. L'utilizzo di chiavi di sicurezza WebAuthn o FIDO2 offre il massimo livello di garanzia per un accesso sicuro. Inoltre, un ulteriore livello di sicurezza potrebbe essere la richiesta di inserire un codice univoco dal dispositivo di accesso nell'app Duo Mobile.

2. Ridurre la dipendenza dalle password con il Single Sign-On (SSO)

Il Single sign-on consente al contempo l'accesso continuo a più applicazioni con un solo set di

credenziali. Con un minor numero di credenziali da ricordare, gli utenti sono meno propensi a riutilizzare o creare password deboli che possano essere facilmente prese di mira dai criminali informatici.

3. Creare e mantenere aggiornato un inventario dettagliato dei dispositivi

È difficile impedire l'accesso da dispositivi di cui non si è a conoscenza. La visibilità di tutti i dispositivi che accedono alle varie risorse è il primo passo per garantire che ogni tentativo di accesso sia legittimo.

4. Applicare i criteri di accesso adattivi

È cruciale garantire che gli utenti giusti, con i dispositivi giusti, accedano alle applicazioni giuste. Perciò si rende necessaria la creazione di policy di sicurezza granulari attraverso cui è possibile applicare un modello di accesso a privilegi minimi e consentire che gli utenti e i loro dispositivi soddisfino standard rigorosi prima di poter accedere alle risorse critiche.

5. Monitoraggio continuo di attività di accesso insolite

L’utilizzo dell'analisi comportamentale può rivelarsi fondamentale nel monitorare i modelli di accesso unici degli utenti. Questa pratica aiuta a individuare le attività sospette e a bloccare le violazioni prima ancora che si verifichino.