Perché i Criminal hacker amano il Social engineering?

Il 2019 ha confermato il trend di crescita delle Cyber minacce su tutti i fronti, con un aumento significativo sia nella frequenza degli attacchi sia nella loro magnitudine.

Un anno che ha visto casi di punta come **Capital One** o **Maersk** e – spesso – a margine di questi eventi di alto profilo molti hanno puntato il dito contro la scarsa resilienza nei confronti degli attacchi dei Criminal Hacker, soprattutto da parte del "comune lavoratore".

Ma siamo così sicuri che sia veramente questo l'anello debole della catena che potenzialmente potrebbe trasformare la nostra società nella prossima **Equifax**?

Non è neppure detto che anche quando l'end user si affida alle policy e alle procedure prefissate, seguendole alla lettera, riesca ad uscire indenne da una ben orchestrata campagna di phishing.

Il caso più lampante – per farci un'idea – è stato quello del'ex Capo di gabinetto della Casa Bianca, nonché campaign manager di **Hilary Clinton, John Podesta.**

Nel suo caso Podesta ha pensato che l'e-mail di reset della password di Google che aveva ricevuto avesse un aspetto ben più che sospetto, ma il responsabile IT della campagna o dando il suo lasciapassare o scrivendo male la sua risposta ha indotto il sig. Podesta a fornire le sue credenziali ai Criminal hacker.

Si tratta di un caso esemplare – e probabilmente non unico – di qualcuno che agisce in buona fede, compiendo le azioni

prescritte dagli esperti e diventando comunque una vittima.

Perché i Criminal hacker amano il Social engineering

Non è difficile capire come i Criminal hacker siano sempre molto affezionati alle tecniche di Social Engineering:

- **Ci sono molti bersagli**: Va da sé che per avere successo i Criminal Hacker hanno bisogno di una superficie d'attacco il più ampia possibile. In termini generali, ci sono sicuramente più utenti che sistemi. Inoltre, molti sistemi non sono direttamente accessibili via Internet, ma la maggior parte degli utenti finali lo sono. I siti di social-media offrono agli aggressori anche strumenti di ricognizione efficaci, difficili da prevenire, individuare o anche isolare.
- **I loro bersagli hanno già ciò che cercano:** Quando gli aggressori prendono di mira i sistemi, il loro percorso verso il bottino può essere tortuoso. Devono trovare un sistema che possono compromettere, ottenere i privilegi da amministratore e/o ruotare verso un altro sistema e continuare a mappare l'ambiente per scoprire dove si trovano i dati preziosi. Il processo può essere estremamente ripetitivo e richiedere molto tempo. I singoli utenti, invece, offrono un percorso abbastanza diretto ai dati desiderati. Se siete alla ricerca di file personali, perché non ottenerli da qualcuno delle Risorse Umane? Se cercate un rendiconto finanziario, non è il dipartimento finanziario il punto di partenza logico?
- **Gli attacchi di Social engineering sono leve molto forti:** Mentre alcune campagne si basano ancora su argomenti e oggetti molto vecchi e molto ovvi – e sono quindi molto facili da evitare (chi casca ancora nelle mail di "Sei il milionesimo cliente!) – molti attacchi

moderni di social-engineering sono così avanzati e taylorizzati da sembrare autentici. Questo è particolarmente significativo in un ambiente aziendale perché il contesto è tale che le conseguenze derivanti dal non agire potrebbero essere gravi se lo scenario fosse legittimo. Per esempio, e-mail che sembrano provenire da supervisori che richiedono azioni o informazioni, o notifiche da parte dell'IT in merito a modifiche delle password sono cose che semplicemente non possono essere ignorate nella normale conduzione degli affari interne all'azienda senza un grave impatto.

Come rimediare?

Ovviamente dinnanzi alle minacce poste dalle campagne di Social Engineering il rimedio più comunemente proposto e più efficace è una maggiore sensibilizzazione degli utenti finali. Ma se l'Awerness è sicuramente parte della soluzione, è solo uno dei diversi elementi di una difesa efficace.

Per esempio:

Implementazione di un'autenticazione (più)forte: sottrarre le credenziali è un obiettivo frequente del Social engineering e il furto di credenziali ha un ruolo di primo piano in molte violazioni di maggiore spicco negli ultimi anni. Un'autenticazione più forte – che si tratti di crittografia, autenticazione multifattoriale (MFA) o di una combinazione dei due – significa che un attacco riuscito non produrrà necessariamente nulla di utile. Vale anche la pena sottolineare che, mentre in tempi di PSD2 non è più ufficialmente raccomandabile l'SMS come secondo fattore di autenticazione, anche misure deboli di 2FA (2 factor authentication) sono meglio di 0.

White-listing delle applicazioni a rischio: l'installazione o l'esecuzione di malware è un altro obiettivo comune degli attacchi di social-engineering. Anche se la lista dei software

in White listing può essere lunga e difficile da compilare, la maggior parte delle organizzazioni dovrebbe sapere quale software stanno effettivamente eseguendo sui loro sistemi. L'applicazione di successo di tale protocollo non è mai facile, ma rende molto più difficile l'esecuzione di software dannoso e permette agli esperti di Cyber Security e ad altri membri dei team di sicurezza di concentrare i loro sforzi su una superficie di attacco molto più piccola.

Segmentare la rete aziendale: L'essere umano è fallibile e di conseguenza in una certa percentuale lo saranno anche le difese che progetta. Un certo numero di attacchi di alto profilo nel corso degli ultimi anni è stato caratterizzato da malware in grado di muoversi lateralmente attraverso le reti, aumentando significativamente sia il danno complessivo che il tempo necessario per il Data Recovery. La segmentazione di rete, come la white-list delle applicazioni, è un esercizio non banale per la maggior parte delle organizzazioni, ma è facilmente una delle migliori "polizze assicurative" per quei momenti in cui un attacco ha successo.

In un certo senso, la difesa contro gli attacchi di Social engineering deve assumere gli stessi caratteri di quella adottata tempo fa per la sicurezza sulle strade. In primo luogo devono essere formati gli utenti in modo da renderli competenti, ma al contempo dobbiamo renderci conto che gli errori saranno sempre parte del nostro essere umani e per questo si migliorano le infrastrutture e gli strumenti.

Integrare la formazione per migliorare l'Awerness con le capacità degli esperti di Cyber Security rendono più facile fare la cosa giusta e più difficile fare la cosa sbagliata; il tutto unito ad un Cyber Security Framework resiliente per eliminare o ridurre i danni durante un evento catastrofico.

https://www.key4biz.it/perche-i-criminal-hacker-amano-il-social-engineering/277772/