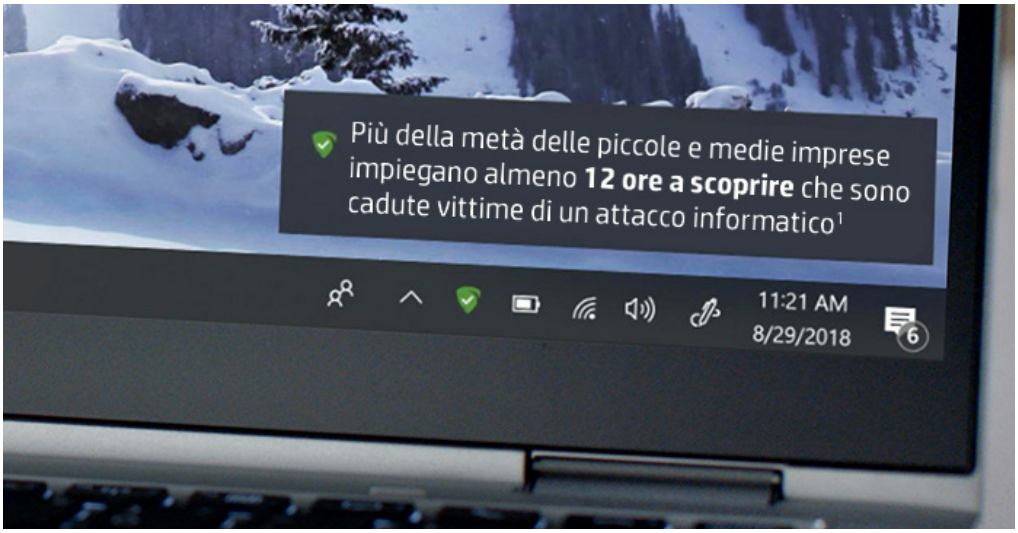
Il phishing non riguarda più solo le e-mail

Scopri di più



Il browser web è una porta di accesso a un mondo di informazioni... e minacce. Cosa puoi fare per proteggere la tua azienda?

I browser web sono responsabili di molte cose. In un recente sondaggio a cui hanno partecipato 400 CIO, il 68% ha dichiarato che i criminali informatici sono diventati così sofisticati, che il personale ha grosse difficoltà a distinguere i siti sicuri da quelli ingannevoli[2]. Sapendo questo, non sorprende che quasi il 70% dei professionisti IT subisca attacchi di phishing con cadenza settimanale, e non solo via e-mail[3]. Ora gli hacker più sofisticati usano i social media, le pubblicità e comuni errori ortografici dei siti web per indurre i dipendenti a svelare dati personali sensibili. Poiché le truffe di phishing divengono sempre più difficili da individuare, le aziende faticano a proteggere la loro forza lavoro da questi attacchi.

Nonostante la maggiore consapevolezza e i crescenti investimenti in software di sicurezza e formazione dei dipendenti, il numero di attacchi informatici verso notebook e computer desktop è aumentato di oltre il 100%[4]. I criminali informatici continuano ad avere successo, perché i numeri sono dalla loro parte. Proteggere i dati richiede un enorme sforzo, e basta che un solo dipendente faccia clic su un collegamento ingannevole per far crollare l'intera azienda.

Gli attacchi informatici tramite social media rivestono un ruolo importante in questo scenario. Le piattaforme come Facebook e Twitter costituiscono un terreno fertile per i criminali informatici. Oltre ad essere progettate per coinvolgere gli utenti, sono anche semplici ed economiche da usare. È facilissimo creare profili fraudolenti e iniziare a postare contenuti dannosi, da collegamenti e raccolte di dati, a pagine di destinazione con falsi pop-up.

La maggior parte di queste attività online si basa sulle tecniche di phishing, che una volta riguardavano solo le e-mail. I social media consentono collegamenti tra persone, e non ci vuole molto per costruire un personaggio fake ma credibile, seguito da utenti autentici delle piattaforme.

Per la maggior parte delle aziende vittime di un attacco di phishing, le conseguenze possono essere dannose e avere ricadute lunghe nel tempo. Il risultato può essere una compromissione della produttività dei dipendenti, la sottrazione di dati dei clienti e la perdita dei clienti stessi. La fiducia dei tuoi clienti verso la tua azienda potrebbe subire una forte scossa a causa di una violazione della sicurezza: potreste non essere più considerati affidabili. E sebbene si possa recuperare, molto spesso le ricadute sono permanenti.

Il phishing non riguarda più solo le e-mail

Nell'ultimo trimestre del 2017, gli attacchi di phishing tramite social media sono cresciuti del 500%, con una tendenza che vede profili fake che si presentano come l'assistenza clienti di grandi marchi[5]. Questo sviluppo è noto come angler-phishing (letteralmente "phishing del pescatore"), perché gli hacker lanciano un'esca e aspettano che l'utente del social media vada da loro. Con l'uso dello stesso marchio e di un nome profilo che sembra autentico, milioni di persone che si fidano dei social media si fanno spesso truffare da questi attacchi. Poi, non appena l'utente intraprende una conversazione, l'account fittizio gli invia un collegamento a un sito di phishing e chiede l'accesso, consentendo al responsabile dell'attacco di raggiungere il suo obiettivo finale: ottenere i dati privati dell'utente.

Uno dei modi per evitare che i dipendenti cadano nella rete del phishing tramite social media è indurre un cambiamento dei comportamenti in azienda. I seguenti accorgimenti dovrebbero essere sufficienti per evitare le minacce più comuni e frequenti:

1. Limitare le interazioni online per conto dell'azienda agli utenti di cui ci si può fidare
2. Non fare clic su collegamenti che provengono da fonti non verificate
3. Non scaricare allegati dai social media
4. Abilitare un'autenticazione a due fattori su tutti gli account dei social media e sui dispositivi: sarà più difficile violarli
5. Fornire una formazione approfondita ai dipendenti che hanno privilegi di accesso elevati o ruoli che si interfacciano con i social

Un altro aspetto da non sottovalutare del tuo piano di sicurezza è l'analisi della tecnologia che utilizzi per garantire la resilienza informatica. La linea HP Elite, ad esempio, offre una serie di notebook, computer desktop e workstation progettati allo scopo di garantire la sicurezza, fin dalle fondamenta.

Una delle funzioni di sicurezza presenti è HP Sure Click[6], disponibile su dispositivi notebook e workstation HP Elite selezionati, che affronta in modo efficace e innovativo i rischi della navigazione online. Invece di limitarsi a evidenziare i siti pericolosi in modo che gli utenti li evitino, impedisce al malware, al ransomware e ai virus di infettare le altre schede del browser e il sistema nel suo complesso. Quando un utente avvia una sessione del browser, ogni sito visitato attiva HP Sure Click. Ad esempio, ogni volta che si visita un sito web, HP Sure Click crea una sessione di navigazione basata su hardware e isolata, che elimina la possibilità che un sito web infetti le altre schede o il sistema stesso.

Inoltre, HP Sure Click protegge gli utenti dai malware infetti nascosti all'interno di file Office e PDF. Supponiamo che i tuoi impiegati abbiano ricevuto un file PDF infetto tramite e-mail. Lo hanno potuto aprire in sicurezza sapendo che HP Sure Click lo avrebbe isolato in un contenitore basato su hardware e avrebbe impedito la diffusione dell'infezione all'esterno del file. Grazie a questa soluzione di sicurezza integrata nel tuo parco dispositivi, le minacce online rappresentano una preoccupazione in meno.

Fare in modo che le aziende cambino la loro strategia di sicurezza e acquisiscano dispositivi all'avanguardia, come HP EliteBook x360, con processori opzionali Intel® Core™ i7 di ottava generazione, può non essere una opzione immediatamente accessibile. In questi casi sono utili soluzioni come HP Device as a Service (DaaS)[7]. HP DaaS è un moderno modello di approvvigionamento informatico che semplifica il modo in cui le organizzazioni possono fornire ai dipendenti l'hardware e gli accessori giusti, gestire parchi dispositivi con diversi sistemi operativi e ricevere servizi aggiuntivi per il ciclo di vita. HP DaaS offre piani semplici ma flessibili, a una tariffa per dispositivo perché tutto funzioni con la massima efficienza.

Avere un team ben formato e dispositivi ottimizzati per la sicurezza ti aiuterà a combattere la criminalità informatica tramite social media, una delle principali minacce del momento. Vista la tendenza degli attacchi a crescere di frequenza e intensità, è giunto il momento di alzare le tue difese.

Scopri i vantaggi delle soluzioni per la sicurezza HP per la tua azienda.

Fonti:

1. Osterman Research, sponsorizzata da Malwarebytes "Second Annual State of Ransomware Report: US Survey Results", luglio 2017
2. https://www.bromium.com/company/press-releases/majority-cios-believe-they-are-losing-battle-against-cybercrime.html
3. http://www8.hp.com/us/en/hp-news/press-release.html?id=1763561#.WLTLYjsrI2y
4. http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016
5. https://www.infosecurity-magazine.com/news/social-media-phishing-attacks-soar
6. HP Sure Click è disponibile sulla maggior parte dei PC HP e supporta Microsoft® Internet Explorer, Google Chrome e Chromium™. Gli allegati supportati includono i file Microsoft Office (Word, Excel, PowerPoint) e PDF in modalità di sola lettura, se Microsoft Office o Adobe Acrobat sono installati.
7. I piani HP DaaS e/o i componenti inclusi possono variare per regione o in base al partner di servizio HP DaaS autorizzato. Per informazioni specifiche sulla vostra zona, contattate il rappresentante HP locale o un partner DaaS autorizzato. I servizi HP sono regolati dai termini e dalle condizioni di servizio applicabili di HP, forniti o indicati al cliente al momento dell'acquisto. Il cliente può disporre di ulteriori diritti legali in base alle leggi vigenti nel Paese in cui risiede e tali diritti non sono in alcun modo influenzati dai termini e dalle condizioni del servizio o dalla garanzia limitata HP fornita con il prodotto HP acquistato.

4AA7-317ITIT, aprile 2019