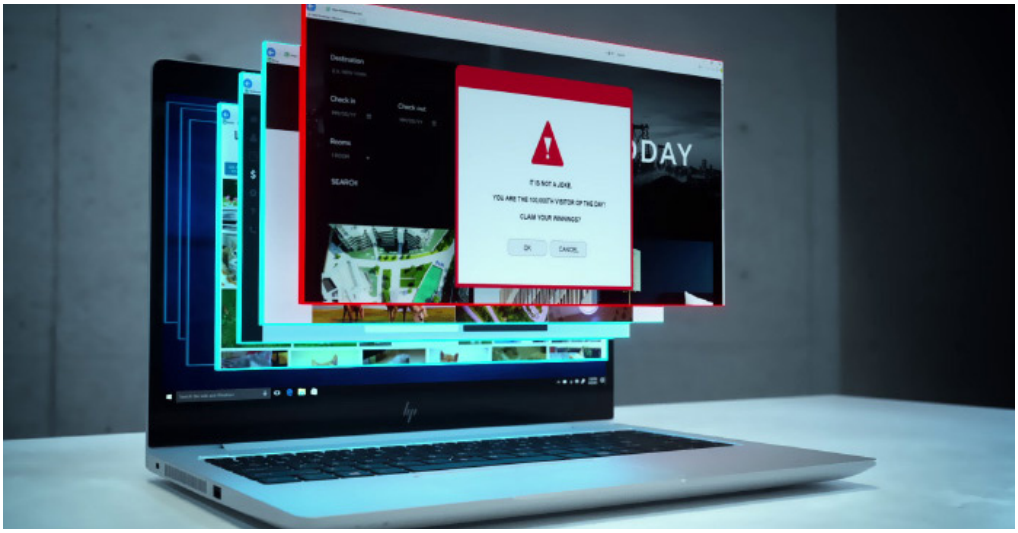
Phishing drabbar inte längre bara e-post

By Maria Augustsson

Läs mer



Webbläsaren öppnar upp en värld av information, men kan även släppa in hot. Vad kan ni göra för att skydda företaget?

Webbläsaren spelar en central roll. I en färsk undersökning där 400 IT-direktörer deltog svarade 68 % att cyberbrottslingarna har blivit så skickliga att deras personal har svårt att skilja mellan säkra och osäkra webbplatser[1]. Därför är det ingen överraskning att 70 % av IT-specialister upplever phishingattacker varje vecka, och inte bara via e-post[2]. Sofistikerade hackare använder nu sociala medier, annonser och webbadresser som ofta felstavas för att lura anställda att avslöja känsliga personuppgifter. Phishingbedrägerierna blir allt svårare att känna igen och företagen kämpar för att skydda personalen från sådana attacker.

Trots en ökad medvetenhet och större investeringar i säkerhetsprogram och utbildning har cyberattackerna ökat med 232 % på bärbara och stationära datorer under de senaste sex åren[3]. Cyberbrottslingarna har siffrorna på sin sida. Det krävs enorma ansträngningar för att skydda data, men det räcker med att en anställd klickar på en skadlig länk för att hela företaget ska falla.

Cyberattacker via sociala medier utgör en stor del av problemet. Plattformar som Facebook och Twitter erbjuder många möjligheter för cyberbrottslingar. Dels är de designade för kommunikation och deltagande, dels är de enkla och billiga att använda. Det är oerhört lätt att skapa falska konton och börja publicera skadligt innehåll, från länkar och datainsamling till landningssidor med opålitliga popupfönster.

De flesta av dessa onlineaktiviteter bygger på phishingtekniker som tidigare var begränsade till e-post. Sociala medier ansluter människor till varandra, och det krävs inte mycket för att skapa en trovärdig profil och dölja sig bland verkliga användare.

Streamingtjänsten Vevo föll nyligen offer för ett massivt dataintrång. En av företagets anställda utsattes för ett phishingbedrägeri på LinkedIn som ledde till att 3,12 TB interna filer läckte ut på nätet. Läckan omfattade videor, företagsdokument, annonsmaterial för sociala medier och information om de artister som hade skivkontrakt med de deltagande skivbolagen[4].

Hackargruppen OurMine tog på sig ansvaret för attacken, som utförts till följd av en dispyt över e-post med en medarbetare på Vevo. Det illustrerar farorna med så kallat **spear-phishing** (harpunfiske) med avsikt att stjäla specifika uppgifter från en viss person. För det mesta utger sig hackare för att vara en vän eller annan betrodd person (till exempel din bank) för att lura offret att lämna ut sina uppgifter. 91 % av attackerna sker på det sättet.

För de flesta företag som faller offer för en phishingattack på samma sätt som Vevo blir konsekvenserna både skadliga och långvariga. Resultatet är oftast att produktivitet och kunduppgifter går förlorade, men även kunder. Kundernas förtroende för företaget kan ta stor skada vid ett dataintrång. I kundernas ögon har företaget förlorat sin trovärdighet vad gäller att skydda deras information. Även om mycket kan räddas, är konsekvenserna ofta permanenta.

Phishing drabbar inte längre bara e-post

Under sista kvartalet 2017 ökade phishingattackerna rekordartat med 500 %, och en vanlig metod var att skapa falska konton och utge sig för att vara kundsupport på välkända företag[5]. Metoden har blivit känd som **angler-phishing** (metfiske) eftersom hackaren kastar ut ett bete och väntar på att sociala medieanvändare ska nappa. Genom att gömma sig bakom ett känt varumärke och ett verklighetstroget kontonamn kan man lura miljontals användare på sociala medier. När användarna interagerar med det falska kontot skickas en länk till en phishingsida där de uppmanas att logga in. Det gör det möjligt för nätfiskaren att komma över privata uppgifter.

Ett av de enklaste sätten att förhindra att företagets anställda utsätts för phishing via sociala medier är att försöka åstadkomma en beteendeförändring på arbetsplatsen. Så här kan personalen undvika att göra enkla misstag som får förödande konsekvenser för företaget:

1. Interagera bara med användare du kan lita på
2. Klicka inte på länkar från overifierade källor
3. Ladda aldrig ned bifogade filer från sociala medier
4. Aktivera tvåfaktorautentisering på alla sociala mediekonton och enheter. Det gör dem svårare att hacka
5. Tillhandahåll särskild utbildning för anställda med omfattande åtkomstbehörigheter eller roller relaterade till sociala medier

En annan viktig aspekt av säkerhetsstrategin är den teknik ni använder för att göra företaget motståndskraftigt mot cyberattacker. HP Elite-familjen består till exempel av bärbara och stationära datorer som har utvecklats med säkerheten i åtanke.

En av funktionerna är HP Sure Click som är tillgänglig på utvalda HP Elite-produkter och som erbjuder förbättrad säkerhet. I stället för att bara varna användare för farliga webbplatser de bör undvika, hindrar den sabotageprogram, utpressningstrojaner och virus från att infektera andra webbflikar och resten av systemet. Varje gång användaren besöker en webbplats aktiveras HP Sure Click. HP Sure Click skapar till exempel en hårdvarubaserad isolerad webbläsarsession varje gång en webbplats besöks, vilket gör det omöjligt för en webbplats att infektera andra flikar eller systemet som helhet.

Men det kan vara lättare sagt än gjort för företag att förändra sin säkerhetsstrategi och få tag på avancerade enheter som de i HP EliteBook 800-serien. Det är där lösningar som HP Device as a Service (DaaS, PC som tjänst) kommer in i bilden. Lösningen är en modern konsumtionsmodell som gör det enklare för företag att förse sina anställda med rätt hårdvara och tillbehör, hantera datorparker med flera olika operativsystem och få tillgång till ytterligare livscykeltjänster. HP DaaS erbjuder enkla men flexibla avtal där man betalar per enhet för att se till så att allt fungerar smidigt och effektivt.

Med ett välutbildat team och säkerhetsoptimerade enheter på plats kan ni skydda er mot cyberkriminalitet på sociala medier, vilket numera utgör ett av de främsta cyberhoten. Hotet kommer bara att växa, så nu är rätt tidpunkt att förbättra företagets försvar.

Företaget kan skyddas, och upptäck fördelarna med HPs säkerhetslösningar

Källor:

1. https://www.bromium.com/company/press-releases/majority-cios-believe-they-are-losing-battle-against-cybercrime.html
2. https://www.engineering.com/DesignerEdge/DesignerEdgeArticles/ArticleID/8355/HP-Nearly-70-of-IT-Professionals-Experience-Weekly-Phishing-Attacks.aspx
3. http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016/
4. https://www.zerofox.com/blog/vevo-hacked-via-linkedin-phishing-campaign/
5. https://www.infosecurity-magazine.com/news/social-media-phishing-attacks-soar/

4AA7-3218SVE, Maj 2018