Nätfiske drabbar inte längre bara e-post

Läs mer

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

Webbläsaren spelar en central roll. I en nyligen genomförd undersökning där 400 IT-direktörer deltog svarade 68 % att cyberbrottslingar har blivit så skickliga att deras personal har svårt att skilja mellan säkra och osäkra webbplatser[2]. Därför är det ingen överraskning att 70 % av IT-specialister får hantera nätfiskeattacker varje vecka, och inte bara via e-post[3]. Sofistikerade hackare använder nu sociala medier, annonser och webbadresser som ofta felstavas för att lura anställda att avslöja känsliga personuppgifter. Nätfiskebedrägerierna blir allt svårare att känna igen och företagen kämpar för att skydda personalen från sådana attacker.

Trots en ökad medvetenhet och investeringar i säkerhetsprogram och utbildning av medarbetare har cyberattacker på bärbara och stationära datorer ökat med mer än 100 %[4]. Cyberbrottslingarna tar sig igenom, eftersom de 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 skapar stora 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 nätfisketekniker som tidigare var begränsade till e-post. Sociala medier ansluter människor till varandra, och det krävs inte mycket för att skapa en trovärdig profil som kan dölja sig bland verkliga användare.

För de flesta företag som faller offer för en nätfiskeattack på samma sätt som Vevo gjorde, 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.

Nätfiske drabbar inte längre bara e-post

Under sista kvartalet 2017 ökade nätfiskeattackerna 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 nätfiskesida där de uppmanas att logga in. Det gör det möjligt för nätfiskaren att få tillgång till privata uppgifter.

Ett av de enklaste sätten att förhindra att företagets anställda utsätts för nätfiske 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, vilket 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-serien till exempel är en serie bärbara datorer, stationära datorer och arbetsstationer som har skapats med säkerhet från grunden.

En av dessa funktioner är HP Sure Click[6] som är tillgänglig på utvalda modeller i HPs Elite-serie och som erbjuder förbättrad säkerhet på ett nytt sätt. I stället för att bara varna användare om infekterade webbplatser de bör undvika, hindrar den malware, ransomware och virus från att infektera andra webbläsarflikar och resten av systemet. Varje gång en användare 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.

HP Sure Click skyddar till och med användare från infekterad malware som är dold i Office- och PDF-filer. Till exempel om medarbetare får en infekterad PDF-fil i ett e-mail så kan de tryggt öppna denna eftersom de vet att de har HP Sure Click som kommer att isolera den i en hårdvarubaserad behållare och se till att infektionen inte sprider sig utanför filen. Med denna säkerhetslösning inbyggd är onlinehot inte längre något att oroa sig för.

Men det kan vara lättare sagt än gjort för företag att förändra sin säkerhetsstrategi och få tag på avancerade enheter som HP EliteBook x360, med valbar 8:e generationens Intel® Core™ i7-processorer. Det är här lösningar som HP Device as a Service (DaaS)[7] 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 tjänster. HP DaaS erbjuder enkla men flexibla prisplaner där man betalar per enhet för att se till så att allt fungerar smidigt och effektivt.

Med ett välutbildat team och säkerhets-optimerade 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.

Upptäck fördelarna med HPs säkerhetslösningar för ditt företag.

Källor:

1. Osterman Research, sponsrat av Malwarebytes "Second Annual State of Ransomware Report: US Survey Results", juli 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 finns på de flesta av HPs datorer och stödjer Microsoft® Internet Explorer och Chromium™. De bilagor som stöds är bland annat Microsoft Office (Word, Excel, PowerPoint) och PDF-filer i skrivskyddat läge, när Microsoft Office eller Adobe Acrobat är installerade.

7. Planer och/eller medföljande komponenter kan variera per region eller per auktoriserad HP DaaS Service Partner. Kontakta en lokal HP-representant eller auktoriserade DaaS-partner för specifika detaljer som gäller för aktuell plats. HP-tjänster styrs av HPs gällande användarvillkor för tjänster som tillhandahållits eller angivits till kunden vid inköpstillfället. Kunden kan ha ytterligare lagstadgade rättigheter enligt gällande lokala lagar, och sådana rättigheter påverkas inte på något sätt av HPs användarvillkor eller HPs begränsade garanti som medföljer HP-produkten.

4AA7-317SVSE, april 2019