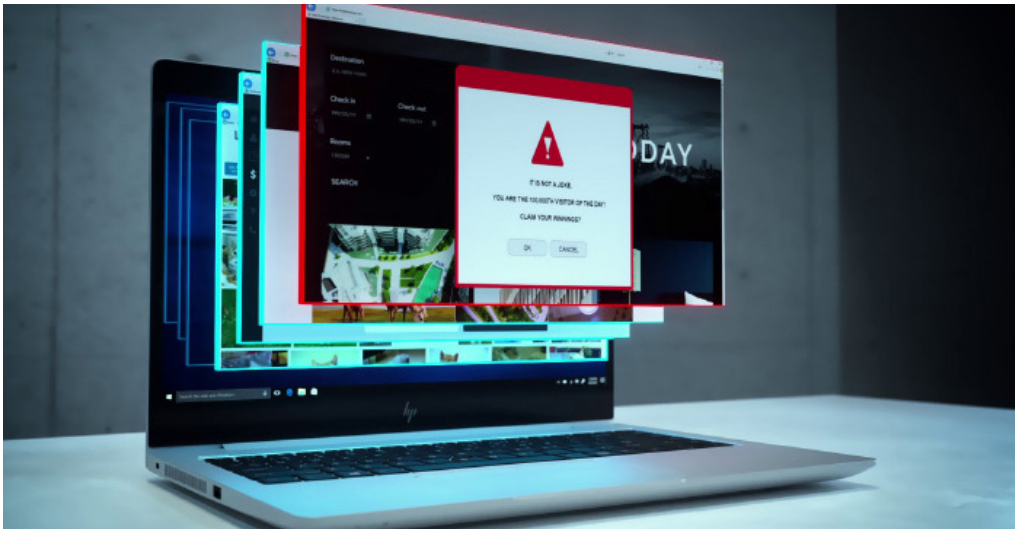
Phishing rammer nå mer enn e-post

Finn ut mer



En nettleser er en portal til en verden av informasjon ... og trusler. Så hva kan du gjøre for å beskytte virksomheten din?

Nettlesere er årsaken til mange problemer. I en fersk undersøkelse blant 400 bedriftsledere sa 68 % at cyberkriminelle nå er så avanserte at medarbeiderne deres har problemer med å skjelne mellom trygge og utrygge nettsteder[1]. Så da er det heller ingen overraskelse å høre at 70 % av IT-spesialister opplever phishing-angrep hver eneste uke – og ikke bare via e-post[2]. Nå bruker avanserte hackere også sosiale medier, annonser og vanlige feilstavelser av nettsteder til å lure medarbeidere til å avsløre sensitiv personlig informasjon. Etter hvert som det blir stadig vanskeligere å oppdage phishing-svindel, må virksomheter kjempe hardere for å beskytte medarbeiderne sine mot slike angrep.

Til tross for større oppmerksomhet overfor phishing og investeringer i sikkerhetsprogramvare og medarbeideropplæring har det vært en økning på hele 232 % i cyberangrep på bærbare og stasjonære PC-er i løpet av de siste seks årene[3]. Cyberkriminelle kommer fremdeles igjennom, for de har tallene på sin side. Det krever en enorm innsats å sikre data, men det er nok at én medarbeider klikker på én ondsinnet kobling for å ødelegge hele virksomheten din.

Cyberangrep i sosial medier utgjør en stor del av dette problemet. Plattformer som Facebook og Twitter er lønnsomme jaktmarker for cyberkriminelle. De er ikke bare utformet for engasjement og kommunikasjon, de er også enkle å bruke og billige i drift. Det er utrolig enkelt å opprette falske kontoer og begynne å legge ut ondsinnet innhold, fra koblinger og datainnsamling til målsider med upålitelige pop-ups.

De fleste av disse internettaktivitetene er basert på phishing-teknikker som før bare ble brukt på e-post. Sosiale medier skaper forbindelser mellom mennesker, og det er ikke vanskelig å etablere en substansiell, troverdig person som følges av genuine brukere av plattformen.

Strømmingstjenesten Vevo ble nylig offer for et massivt databrudd. En av tjenestens medarbeidere ble offer for en LinkedIn-phishingsvindel, noe som førte til at 3,12 TB interne filer ble lekket på nettet. Dette omfattet videoer, kontordokumenter, reklamemateriale, innhold som skulle brukes på sosiale medier og informasjon om artister som var i stallen til deltakende plateselskaper[4].

Hacking-gruppen OurMine påtok seg ansvaret for angrepet etter en krangel via e-post med en Vevo-medarbeider. Dette viser faren med **spyd-phishing**, et målrettet angrep der målet er å stjele spesifikk informasjon fra et spesifikt mål. Som regel gir hackere seg ut for å være en venn eller pålitelig kilde (f.eks. banken din) for å lure målet til å gi fra seg informasjon. Dette utgjør 91 % av angrepene.

Phishing rammer nå mer enn e-post

For de fleste virksomheter som blir ofre for et phishing-angrep kan, som for Vevo, konsekvensene være både skadelige og langsiktige. De kan ikke bare føre til tap av medarbeiderproduktivitet og kundedata, men også til tap av kunder. Kundenes tillit til virksomheten din kan reduseres betydelig av et sikkerhetsbrudd – for dem er du ikke lenger et pålitelig sted å oppbevare informasjon. Selv om dette av og til kan ordnes opp i, skjer det stadig oftere at konsekvensene er permanente.

I 4. kvartal i 2017, hadde phishing-angrep i sosiale medier en rekordstor økning på hele 500 %, og trenden var å opprette falske kontoer som ga seg ut for å være kundestøtten til kjente selskaper[5]. Denne typen angrep ble kjent som **fiske-phishing** fordi hackere la ut et agn og bare ventet på at brukere av sosiale medier skulle bite på. Ved å bruke samme type logoer og varemerker og et kontonavn som virker ekte, lykkes phisherne i å lure mange av de millioner brukere som bruker nettbaserte sosiale medier med overbevisende angrep. Så snart brukeren responderer, sender den falske kontoen en kobling til et phishing-nettsted og ber brukeren logge seg på. Da har phisheren snart nådd sitt endelige mål: å få tilgang til privat informasjon.

En av de enkleste måtene å forhindre at medarbeiderne dine utsettes for phishing via sosiale medier, er å iverksette endringer i nettatferd på arbeidsplassen. Dette kan hjelpe medarbeiderne dine til å unngå å gjøre enkle feil som kan ha ødeleggende konsekvenser for virksomheten:

1. Begrens samhandlingen til brukere du kan stole på
2. Ikke klikk på koblinger fra en kilde som ikke er verifisert
3. Last aldri ned filvedlegg fra sosiale medier
4. Aktiver to-faktor- godkjenning av alle kontoer på sosiale medier og enheter – det gjør det vanskeligere å hacke dem
5. Gi ekstra opplæring til medarbeidere med utvidede tilgangsprivilegier eller sosialt orienterte roller

Et annet viktig aspekt av sikkerhetsplanen din er å se på den teknologien du bruker for å være motstandsdyktig mot cyberangrep. HP Elite-serien er for eksempel bærbare og stasjonære PC-er som er utformet for optimal sikkerhet fra bunnen av.

En av disse funksjonene er HP Sure Click, og den er tilgjengelig på utvalgte HP Elite-plattformer som har en helt ny og annerledes tilnærming til trygg nettlesing. I stedet for bare å flagge farlige nettsteder for at brukerne skal unngå dem, forhindrer denne funksjonen at skadelig programvare, krypteringsvirus (ransomware) og virus infiserer andre nettleserfaner og resten av systemet. Når brukeren starter en nettlesingsøkt, vil HP Sure Click utløses av hvert enkelt nettsted som besøkes. For eksempel: hver gang et nettsted besøkes oppretter HP Sure Click en maskinvarebasert, isolert nettlesingsøkt, noe som eliminerer muligheten for at et nettsted kan infisere andre faner eller systemet selv.

For virksomheter kan det ofte være lettere sagt enn gjort å endre sikkerhetsstrategi og ta i bruk slike banebrytende enheter som HP EliteBook 800-serien, med valgfrie 8. generasjons Intel® Core™-prosessorer. Det er her en løsning som HP Device as a Service (DaaS) kommer inn. Det er en moderne PC-forbruksmodell som gjør det enklere for kommersielle organisasjoner å utstyre sine medarbeidere med riktig maskinvare og tilbehør, administrere enhetssystemer med flere OS og få ytterligere livssyklus-tjenester. Med HP DaaS får du enkle, men likevel fleksible planer, til én pris per enhet, slik at alt går greit og effektivt.

Et godt opplært team og enheter som er optimalisert for maksimal sikkerhet vil i sin tur hjelpe deg med å bekjempe cyberkriminalitet på sosiale medier, en av vår tids største cybertrusler. Dette problemet kommer bare til å bli større og mer alvorlig, så det er nå du bør oppgradere forsvaret ditt.

Se alle fordelene HPs sikkerhetsløsninger gir virksomheten din.

Kilder:

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/

4AA7-3218NOE, Mai 2018