Phishing gebeurt niet alleen meer per e-mail

Meer informatie

Een webbrowser is een portaal naar een wereld van informatie en bedreigingen. Dus wat kunt u doen om uw bedrijf te beschermen?

Webbrowsers hebben veel om op te letten. In een recent onderzoek van 400 CIO's gaf 68% aan dat cybercriminelen nu zo geraffineerd te werk gaan dat hun personeel moeite heeft het verschil te zien tussen veilige en onveilige websites[2]. In dit licht is het geen verrassing dat bijna 70% van de IT-professionals wekelijks phishingpogingen ervaart, en niet alleen per e-mail[3]. Geraffineerde hackers gebruiken nu social media, advertenties en veelvoorkomende verkeerd gespelde domeinnamen om medewerkers over te halen gevoelige persoonlijke informatie te verstrekken. Nu phishingpogingen steeds moeilijker te herkennen zijn, worstelen bedrijven ermee hun personeel te beschermen tegen deze aanvallen.

Ondanks meer bewustzijn en investeringen in beveiligingssoftware en opleiding van personeel, is het aantal cyberaanvallen op notebooks en desktops met meer dan 100% gestegen[4]. Cybercriminelen komen nog steeds binnen, omdat zij het schaalvoordeel hebben. Er is veel inspanning nodig om gegevens te beschermen, maar er is maar één medewerker nodig die op een foute link klikt om uw bedrijf onderuit te halen.

Cyberaanvallen via social media vormen een groot deel van dit probleem. Platformen als Facebook en Twitter zijn vruchtbare omgevingen voor cybercriminelen. Ze zijn niet alleen ontworpen voor contact en communicatie, maar ook eenvoudig en goedkoop in gebruik. Het is enorm eenvoudig om frauduleuze accounts op te zetten en kwaadwillende inhoud te verspreiden, via links en gegevens die leiden naar landingspagina's met onbetrouwbare pop-ups.

De meeste van deze online activiteiten zijn gebaseerd op phishingtechnieken, die eerder alleen via e-mail werden gebruikt. Social media maakt communicatie tussen mensen mogelijk en er is weinig voor nodig om een betrouwbaar persoon aan te maken met echte gebruikers van de platformen als volgers.

Voor de meeste bedrijven die slachtoffer worden van een phishingaanval, kunnen de gevolgen zowel schadelijk als langdurig zijn. Ze kunnen niet alleen leiden tot verlies van productiviteit en klantgegevens, maar ook tot het verlies van klanten zelf. Het vertrouwen dat uw klanten hebben in uw bedrijf kan een enorme deuk oplopen door een beveiligingslek. Zij vinden u niet langer een betrouwbare beheerder van informatie. En hoewel herstel mogelijk is, zijn de implicaties steeds vaker permanent.

Phishing gebeurt niet alleen meer per e-mail

In het vierde kwartaal van 2017 stegen phishingpogingen op social media met 500%, met een trend van nepaccounts die zich voordeden als klantenservice van grote merken[5]. Deze ontwikkeling staat bekend als hengelphishing, omdat hackers een aas plaatsen en wachten op socialmediagebruikers die erop afkomen. Door gebruik te maken van hetzelfde uiterlijk en een authentiek ogende accountnaam worden de miljoenen gebruikers van webgebaseerde social media vaak misleid door een overtuigende aanval. En zodra een gebruiker erin trapt, stuurt het nepaccount een link naar een phishingwebsite en vraagt hem of haar om in te loggen, zodat de phisher uiteindelijk privégegevens kan bemachtigen.

Een van de manieren om medewerkers te beschermen tegen phishing via social media is om gedragsverandering op het werk te stimuleren. Dit moet uw medewerkers helpen de eenvoudige vergissingen te voorkomen die desastreuze gevolgen kunnen hebben voor uw bedrijf:

1. Beperk interactie tot gebruikers die u kunt vertrouwen
2. Klik niet op links naar een niet-geverifieerde bron
3. Download nooit bestandsbijlagen van social media
4. Activeer twee-staps-authenticatie op alle socialmedia-accounts en apparaten, zo wordt het moeilijker om die te hacken
5. Geef extra training aan medewerkers met veel toegangsrechten of functies met externe contacten

Een ander essentieel aspect van uw beveiligingsplan is de technologie die u gebruikt om veerkrachtig te blijven in de digitale wereld. De HP Elite-serie biedt bijvoorbeeld een serie notebooks, desktop-pc's en workstations die vanaf de basis zijn ontworpen voor beveiliging.

Een van deze beveiligingsfuncties is HP Sure Click[6], beschikbaar op bepaalde HP Elite-notebookapparaten en -workstations, waarmee veilig browsen anders wordt benaderd. In plaats van gevaarlijke websites voor gebruikers te markeren houdt dit ook malware, ransomware en virussen tegen zodat ze geen andere tabbladen of het verdere systeem kunnen besmetten. Als een gebruiker een browsersessie opent, zal elke bezochte website HP Sure Click gebruiken. Elke keer dat een website bezocht wordt, maakt HP Sure Click bijvoorbeeld een hardwarematige, geïsoleerde browsersessie, zodat een bepaalde website niet andere tabbladen of het gehele systeem kan besmetten.

HP Sure Click beschermt gebruikers zelfs tegen geïnfecteerde malware die verborgen zit in Office- en pdf-bestanden. Stel, uw medewerkers ontvangen een geïnfecteerde pdf per e-mail, dan kunnen ze het veilig openen met de wetenschap dat HP Sure Click het zal isoleren in een hardwarematige container, en wordt voorkomen dat de infectie zich buiten het bestand kan verspreiden. U hoeft zich minder zorgen te maken over online bedreigingen als deze beveiligingsoplossing in uw pc-vloot is ingebouwd.

Als het gaat om bedrijven die hun beveiligingsstrategie willen wijzigen en gebruik willen maken van deze moderne apparaten, zoals de HP EliteBook x360 met optionele 8e generatie Intel® Core™ i7-processoren, lijkt dat gemakkelijker gezegd dan gedaan. Dan komt een oplossing als HP Device as a Service (DaaS)[7] goed van pas. Het is een modern pc-gebruikersmodel dat het voor commerciële bedrijven eenvoudiger maakt om hun medewerkers uit te rusten met de juiste hardware en accessoires, netwerken met meerdere besturingssystemen te beheren en aanvullende lifecycle-services af te sluiten. HP DaaS biedt eenvoudige, maar flexibele plannen, tegen één vergoeding per apparaat om alles soepel en efficiënt te laten verlopen.

Uiteindelijk helpen een goed opgeleid team en apparaten die geoptimaliseerd zijn voor beveiliging u de strijd aan te gaan met cybercriminaliteit via social media, een van de grootste cyberdreigingen ter wereld. Het probleem wordt alleen maar groter en gevaarlijker, daarom is dit het moment om uw beveiliging te verbeteren.

Ontdek de voordelen van HP beveiligingsoplossingen voor uw bedrijf.

Bronnen:

1. Osterman Research, gesponsord door 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 is beschikbaar op de meeste HP pc's en ondersteunt Microsoft® Internet Explorer, Google Chrome en Chromium™. Ondersteunde bijlagen zijn Microsoft Office (Word, Excel, PowerPoint) en pdf-bestanden in alleen-lezen-modus, als Microsoft Office of Adobe Acrobat geïnstalleerd zijn.

7. HP DaaS-plannen en/of bijgeleverde onderdelen kunnen per regio of per geautoriseerde HP DaaS Servicepartner verschillen. Neem contact op met uw HP vertegenwoordiger of geautoriseerde DaaS-partner voor specifieke details op uw locatie. Voor HP services gelden de van toepassing zijnde HP servicevoorwaarden, die bij aankoop aan de klant worden verstrekt of getoond. Mogelijk heeft de klant volgens de geldende lokale wetgeving nog andere rechten. De Algemene Servicevoorwaarden van HP en de HP garantie op uw HP product maken geen inbreuk op deze wettelijk vastgelegde rechten.

4AA7-317NLE, april 2019