**Persbericht**

**Cyberbeveiliging in 2017**

**Opvallendste trends volgens security vendor Sophos**

Brussel, 20 december 2016 – **In 2016 zagen we een enorm aantal cyberaanvallen met een uiterst divers karakter, van een prominente denial-of-service (DDoS)-aanval die gebruik maakte van met internet verbonden beveiligingscamera’s tot een vermeende hack bij de Democraten tijdens de Amerikaanse verkiezingen. Verder traden er datalekken op bij een groeiend aantal grote en kleine organisaties, waarbij de privégegevens van een significant aantal mensen werden gestolen. Nu het einde van het jaar nadert, werpen we ons licht op de manier waarop cyberaanvallen zich in 2017 verder zullen ontwikkelen.**

**Sophos stelt hieronder 12 actuele en opkomende trends in cyberaanvallen**

**#1 Het aantal DDoS-aanvallen via het Internet of Things zal toenemen.**

In 2016 gaf het Mirai-botnet blijk van het vernietigende potentieel van DDoS-aanvallen die gebruikmaken van onveilige IoT (Internet of Things)-apparaten. De cybercriminelen achter het Mirai-botnet maakten gebruik van slechts een klein aantal apparaten en kwetsbaarheden in combinatie met basistechnieken voor het raden van wachtwoorden. Voor cybercriminelen is het een koud kunstje om de schaalomvang van hun aanvallen te vergroten vanwege het grote aantal IoT-apparaten met programmatuur, slecht onderhouden besturingssystemen en applicaties met alom bekende kwetsbaarheden. U kunt het komende jaar dan ook meer IoT-exploits verwachten, betere technologie voor het raden van wachtwoorden en inzet van meer besmette IoT-apparaten voor het uitvoeren van DDoS-aanvallen of mogelijk het hacken van andere apparatuur binnen uw netwerk.

**#2 Een verschuiving van exploits naar gerichte sociale aanvallen.**

Cybercriminelen worden steeds handiger in het maken van misbruik van de ultieme kwetsbaarheid - *mensen*. Met steeds geavanceerdere en overtuigende gerichte aanvallen proberen ze gebruikers ertoe over te halen om zichzelf te laten besmetten. Vaak wordt gebruikgemaakt van e-mailberichten die de ontvanger bij naam noemen en beweren dat deze een uitstaande schuld moet voldoen. Cybercriminelen brengen een schokeffect teweeg, doen zich voor als autoriteit of geven zich uit als rechtshandhavers. Dit zijn veel voorkomende en uiterst effectieve tactieken. Deze e-mailberichten bevatten een kwaadaardige link waarop ontvangers in paniek kunnen klikken. Daarmee stellen ze zich bloot aan een cyberaanval. Vroeger waren dit soort phishing-berichten makkelijk te spotten vanwege de vele taalfouten, maar inmidels zijn ze bijna niet meer van echt te onderscheiden.

**#3 Financiële infrastructuren lopen steeds meer kans om getroffen te worden door een cyberaanval.**

Het gebruik van gerichte phishing- en ‘whaling’-aanvallen blijft groeien. Deze aanvallen maken gebruik van gedetailleerde informatie over topmensen binnen bedrijven om werknemers over te halen om geld over te maken aan fraudeurs of om rekeninggegevens prijs te geven. We verwachten dat er meer aanvallen zullen worden uitgevoerd op kritische financiële infrastructuren, zoals de aanval die in februari 2016 plaatsvond en de centrale bank van Bangladesh voor 81 miljoen dollar aan schade berokkende. Bij deze aanval waren met SWIFT verbonden instellingen betrokken. SWIFT gaf recentelijk toe dat er sprake is geweest van meer van dergelijke aanvallen, en sprak de verwachting uit dat er nog meer zullen volgen. In een uitgelekte brief aan cliënten stelde het: "Er is sprake van uiterst hardnekkige, adaptieve en geavanceerde bedreigingen, en het einde is nog lang niet in zicht".

**#4 Misbruik van de inherent onveilige infrastructuur van het internet.**

Alle internetgebruikers maken gebruik van basisprotocollen die uit een ver verleden stammen. Het feit dat deze protocollen op een dergelijk grote schaal worden gebruikt maakt het vrijwel onmogelijk om ze te moderniseren of vervangen. Deze sterk verouderde protocollen vormden geruime tijd de ruggengraat van het internet en bedrijfsnetwerken. Sommige daarvan rammelen aan alle kanten. Zo zouden aanvallen op het BGP (Border Gateway Protocol) een groot deel van het internet kunnen verstoren, kapen of platleggen. Zo werd in oktober via een groot netwerk van IoT-apparaten een DDoS-aanval uitgevoerd om Dyn. Daarmee werd deze DNS-provider uit de lucht gehaald en viel de toegang tot een groot deel van het internet weg. Dit was een van de grootste aanvallen tot dusver, en de hackers die er de verantwoordelijkheid voor opeisten gaven aan dat dit nog maar een voorproefje was. Grote internetproviders en bedrijven kunnen diverse maatregelen treffen om hier iets aan te doen. Deze maatregelen kunnen echter geen serieuze schade voorkomen als kwaadwillende personen of overheden ervoor kiezen om misbruik te maken van kwetsbaarheden die diep in het internet zijn ingebakken.

**#5 Aanvallen krijgen een steeds complexer karakter.**

Aanvallen combineren steeds vaker uiteenlopende technische en sociale elementen en worden voorafgegaan door een langdurige en voorzichtige verkenning van het netwerk van organisaties. Cybercriminelen besmetten diverse servers en workstations alvorens gegevens te stelen of agressief toe te slaan. Deze aanvallen worden nauwgezet beheerd door experts, hebben een strategische in plaats van tactische opzet en kunnen uitzonderlijk grote schade aanrichten. Ze zien er totaal anders uit dan de vooraf geprogrammeerde, geautomatiseerde malware-aanvallen die we gewend waren. Moderne aanvallers gaan uiterst geduldig te werk en weten detectiemechanismen te omzeilen.

**#6 Steeds meer aanvallen maken gebruik van ingebouwde beheertalen en -tools.**

We bemerken een toename van het aantal exploits dat gebruikmaakt van PowerShell, de programmeertaal van Microsoft voor het automatiseren van beheertaken. Deze scripttaal kan worden gebruikt om beveiligingsoplossingen te omzeilen die uitvoerbare bestanden inspecteren. Verder groeit het aantal aanvallen die gebruikmaken van tools voor penetratietests en beheertools die reeds binnen het netwerk aanwezig zijn, niet te hoeven worden gehackt en mogelijk ook niet verdacht zijn. Deze krachtige tools vragen om even krachtige beveiligingsmechanismen.

**#7 Ransomware ontwikkelt zich verder.**

Steeds meer gebruikers beginnen oog te krijgen voor de kans op ransomware-aanvallen via e-mail. Cybercriminelen gaan daarom op zoek naar andere aanvalskanalen. Een aantal van hen experimenteert momenteel met ransomware die lange tijd na het betalen van losgeld opnieuw toeslaat. Andere hackers maken gebruik van ingebouwde tools en malware die niet de vorm hebben van uitvoerbare bestanden omzeilen van oplossingen voor endpoint-beveiliging die zich op dergelijke ‘executables’ richten. Recente voorbeelden van ransomware boden aan om bestanden te ontsleutelen nadat het slachtoffer de ransomware had uitgewisseld met twee vrienden en die vrienden betaald hadden voor het ontsleutelen van hun bestanden. Ontwikkelaars van ransomware beginnen nu ook gebruik te maken van andere technieken dan encryptie. Zo kunnen ze e-mailberichten verwijderen of headers van bestanden manipuleren. Verder is het ook nog mogelijk dat gebruikers worden getroffen door ‘oude’ ransomware waarvoor ze geen losgeld meer kunnen betalen omdat de opgegeven betalingslocaties niet langer werken.

**#8 De opkomst van persoonlijke IoT-aanvallen.**

Gebruikers van IoT-apparaten voor huishoudens merken het mogelijk niet eens of maakt het niet uit dat hun babyfoon wordt gekaapt om iemands website aan te vallen. Maar zodra cybercriminelen de controle hebben overgenomen van een apparaat binnen een thuisnetwerk, kunnen ze hun tentakels uitslaan naar andere apparaten, zoals laptops die belangrijke privégegevens bevatten. Er valt te verwachten dat dit vaker zal gebeuren, omdat steeds meer aanvallen gebruikmaken van camera’s en microfoons om huishoudens te bespioneren. Cybercriminelen weten altijd nieuwe manieren te vinden om geld te verdienen.

**#9 De toename van malvertising en besmetting van ecosystemen voor internetadvertenties.**

Malvertising, een techniek die malware verspreidt via online advertentie-netwerken en internetpagina’s, is al jarenlang in omloop. In 2016 was er echter sprake van een opleving. Dit wijst op grotere problemen binnen het advertentie-ecosysteem. Een voorbeeld hiervan is klikfraude, waarbij adverteerders betalen voor clicks die niet afkomstig zijn van internetgebruikers die werkelijk belangstelling hebben in de advertentie. Malvertising zelfs de aanzet gegeven tot klikfraude door tegelijkertijd gebruikers te besmetten en geld van adverteerders af te troggelen.

**#10 Encryptie heeft ook zijn nadelen.**

Nu encryptie op brede schaal wordt ingezet, wordt het steeds moeilijker voor beveiligingsproducten om dataverkeer te inspecteren. Dit maakt het eenvoudiger voor cybercriminelen om onopgemerkt de beveiliging te passeren. Vanzelfsprekend vinden cybercriminelen creatieve nieuwe manieren om misbruik te maken van encryptie. Beveiligingsoplossingen zullen voor een hechte integratie moeten zorgen van de netwerk- en client-beveiliging om incidenten snel te kunnen detecteren nadat code op endpoints is ontsleuteld.

**#11 Het aantal exploits van gevirtualiseerde en cloud-systemen groeit**.

Aanvallen op fysieke hardware (zoals Rowhammer) vergroten de kans op gevaarlijke nieuwe exploits die op gevirtualiseerde cloud-systemen zijn gericht. Cybercriminelen kunnen misbruik maken van de host of guests op een shared host, systemen voor toegangsrechten aanvallen en mogelijk ook toegang krijgen tot de gegevens van andere systemen. Gezien de groeiende populariteit van Docker en het hele container- (of ‘serverloze’) ecosysteem zullen cybercriminelen actief naar kwetsbaarheden te zoeken die ze kunnen misbruiken.

**#12 Cyberaanvallen op overheden en samenlevingen**.

Cyberaanvallen worden steeds vaker uit politieke overwegingen uitgevoerd. Samenlevingen lopen daarmee een steeds grotere kans op desinformatie (zoals ‘nepnieuws’) en misbruik van stemcomputers. Onderzoekers hebben bijvoorbeeld aangetoond hoe aanvallen een lokale kiezer in staat kunnen stellen om ongemerkt verschillende malen te stemmen. Zelfs als overheden geen aanvallen uitvoeren op de verkiezingssystemen van hun opponenten is alleen al de perceptie dat deze aanvallen mogelijk zijn een krachtig wapen.

**Connect with Sophos**

[Twitter](http://soph.so/CfuKd)

[LinkedIn](http://soph.so/Cfv36)

[Facebook](http://soph.so/CfvaA)

[Google+](https://plus.google.com/+sophos)

[Spiceworks](http://soph.so/Cgbwa%20)

[YouTube](http://www.youtube.com/user/sophoslabs)

[Sophos Blog](http://blogs.sophos.com/)

[Naked Security News](http://nakedsecurity.sophos.com/)

**Over Sophos**

Meer dan 100 miljoen gebruikers in 150 landen rekenen op Sophos voor de beste bescherming tegen complexe bedreigingen en dataverlies. Sophos levert security- en databeschermingsoplossingen die eenvoudig in te zetten, te beheren en te gebruiken zijn. Zo biedt Sophos prijswinnende oplossingen aan voor endpoint security, web security, e-mail security, network security, mobile security en encryptie. Deze worden ondersteund door Sophos Labs, een wereldwijd netwerk van threat intelligence centra. Het hoofdkwartier van Sophos bevindt zich in Oxford (UK) en in Boston (VS). Meer informatie over Sophos op: [www.sophos.com](http://www.sophos.com/).

**Voor meer informatie, interviewmogelijkheden of beeldmateriaal:**

Square Egg, Sandra Van Hauwaert, [Sandra@square-egg.be](mailto:Sandra@square-egg.be), 0032 497 251816