**Persbericht**

**Wereldwijd onderzoek Sophos:**

**“IT-managers worden overspoeld met cyberaanvallen vanuit alle richtingen”**

Brussel, 10 juli 2019 – **In het wereldwijde onderzoek** [**The Impossible Puzzle of Cybersecurity**](https://secure2.sophos.com/en-us/medialibrary/Gated-Assets/white-papers/sophos-impossible-puzzle-of-cybersecurity-wp.pdf) **dat in opdracht van Sophos is uitgevoerd, blijkt dat IT-managers worden overstelpt met cyberaanvallen vanuit alle richtingen. Het onderzoek toont ook aan dat zij hiermee worstelen door gebrek aan expertise, budget en up-to-date technologie. De enquête werd voorgelegd aan 3.100 IT *decision makers* van middelgrote bedrijven in de VS, Canada, Mexico, Colombia, Brazilië, het Verenigd Koninkrijk, Frankrijk, Duitsland, Australië, Japan, India en Zuid-Afrika.**

**Cybercriminelen: meerdere aanvalsmethoden**

Het onderzoek geeft aan hoe aanvalstechnieken variëren en verschillende fases kennen. Een op de vijf ondervraagde IT-managers wist niet dat ze werden aangevallen, en door de diversiteit aan aanvalsmethoden kan geen enkele verdedigingsstrategie wonderen verrichten.

Chester Wisniewski, principal research scientist bij Sophos: "Cybercriminelen ontwikkelen aanvalsmethoden en gebruiken vaak meerdere payloads voor winstmaximalisatie. Software-exploits vormden het eerste *point of entry* in 23 procent van de gevallen, maar ze werden ook op verscheidene manieren gebruikt in 35 procent van alle aanvallen. Dit toont aan hoe exploits worden gebruikt in meerdere fasen van de aanvalsketen. Organisaties die alleen extern patchen, zijn intern kwetsbaar. Cybercriminelen gebruiken dit en andere beveiligingslekken in hun voordeel."

Het brede assortiment, de fasering én de schaal van de aanvallen blijken effectief: zo werd 53 procent slachtoffer van een cyberaanval getroffen door een phishing e-mail en 30 procent door ransomware. 41 procent geeft aan een datalek te hebben ervaren.

**Zwakke schakels**

Op basis van het onderzoek is het niet verrassend dat 75 procent van de IT-managers misbruik van software, niet-gepatchte kwetsbaarheden en zero-day bedreigingen beschouwt als de voornaamste beveiligingsrisico’s. 50 procent ziet phishing als een groot beveiligingsrisico. Het is alarmerend dat slechts 16 procent van de IT-managers supply chain als een belangrijk beveiligingsrisico aanstipt, waardoor een extra zwakke plek wordt blootgelegd die cybercriminelen waarschijnlijk zullen opnemen in hun aanvalsrepertoire.

**Gebrek aan veiligheidsexpertise, budget én up-to-date technologie**

Volgens het Sophos-onderzoek geven IT-managers aan dat gemiddeld 26 procent van hun tijd aan security wordt besteed. Toch is 86 procent het erover eens dat beveiligingsexpertise kan worden verbeterd en 80 procent wil een sterker team om beveiligingsincidenten op te sporen, te onderzoeken en erop te reageren. Het werven van securitytalent is ook een probleem: 79 procent bevestigt dat het vinden van mensen met cybersecurityexpertise een uitdaging is.

Wat budget betreft, zegt 66 procent dat het cyberbeveiligingsbudget van de organisatie (inclusief mensen en technologie) lager is dan het zou moeten zijn. Het hebben van de huidige technologie is een ander probleem: 75 procent is het erover eens dat het up-to-date blijven met cybersecurity-technologie een uitdaging is voor hun organisatie. Dit gebrek aan beveiligingsexpertise, budget en up-to-date technologie geeft aan dat IT-managers moeite hebben om op cyberaanvallen te reageren in plaats van proactief te plannen en op de toekomst te anticiperen.

**Gesynchroniseerde beveiliging lost** [**Impossible Puzzle of Cybersecurity**](https://secure2.sophos.com/en-us/medialibrary/Gated-Assets/white-papers/sophos-impossible-puzzle-of-cybersecurity-wp.pdf) **op**

Met cyberdreigingen van supply chain-aanvallen, phishing e-mails, software-exploits, kwetsbaarheden, onveilige draadloze netwerken en nog veel meer, hebben organisaties een beveiligingsoplossing nodig die hen helpt onvolmaaktheden te verhelpen en eerder onzichtbare bedreigingen te identificeren. Sophos Synchronized Security, een geïntegreerd systeem, biedt deze broodnodige zichtbaarheid voor bedreigingen door Sophos’ endpoint-, netwerk-, mobiele, WiFi- en coderingsproducten te integreren om informatie in realtime te delen en automatisch op incidenten te reageren.

**Over het onderzoek**

Het onderzoek [Impossible Puzzle of Cybersecurity](https://secure2.sophos.com/en-us/medialibrary/Gated-Assets/white-papers/sophos-impossible-puzzle-of-cybersecurity-wp.pdf)werd in december 2018 en januari 2019 door Vanson Bourne uitgevoerd, een onafhankelijke marktonderzoek-specialist. In dit onderzoek zijn 3.100 IT-besluitvormers in twaalf landen geïnterviewd en de VS, Canada, Mexico, Colombia, Brazilië, het Verenigd Koninkrijk, Frankrijk, Duitsland, Australië, Japan, India en Zuid-Afrika. Alle respondenten waren van organisaties met tussen de 100 en 5.000 werknemers.

**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, contacteer:**Sandra Van Hauwaert, Square Egg Communications, [sandra@square-egg.be](mailto:sandra@square-egg.be), GSM 0497251816.