Persbericht

# **“Cybercriminelen meest waarschijnlijk op servers en netwerken gepakt; *point of entry* en tijdstip blijven mysterie”**

Brussel, 5 maart 2019 - **Sophos concludeert in zijn wereldwijde onderzoek 7 Uncomfortable Truths of Endpoint Security dat IT-managers cybercriminelen eerder vangen op bedrijfsservers en -netwerken dan ergens anders. In feite ontdekten IT-managers dat 37 procent van hun belangrijkste cyberaanvallen op hun servers en 37 procent op hun netwerken plaatsvindt. Slechts 17 procent werd ontdekt op endpoints en 10 procent werd gevonden op mobiele apparaten.**

Chester Wisniewski, principal research scientist bij Sophos: "Servers slaan niet alleen financiële data op, maar ook die van werknemers en andere gevoelige documenten. Sinds vorig jaar gelden strenge AVG-wetten, en daarom zijn de beveiligingsniveaus voor servers historisch hoog. Het is logisch dat IT-managers zich richten op het beschermen van bedrijfskritieke servers om aanvallers ervan te weerhouden netwerken binnen te dringen. IT-managers kunnen endpoints niet negeren, omdat de meeste cyberaanvallen juist daar beginnen. Aan de andere kant kan een verrassend aantal IT-managers simpelweg steeds niet vaststellen hoe en wanneer bedreigingen het systeem binnenkomen."

Volgens het onderzoek kan twintig procent van de IT-managers die vorig jaar het slachtoffer werden van een of meer cyberaanvallen niet vaststellen hoe de aanvallers toegang kregen; 17 procent weet niet hoelang bedreigingen in de buurt waren voordat deze werden ontdekt. Om dit gebrek aan zichtbaarheid te verbeteren, hebben IT-managers Endpoint Detection and Response (EDR) nodig die het uitgangspunt van bedreigingen en digitale voetafdrukken van criminelen binnen een netwerk blootleggen.

"Wanneer IT-managers de oorsprong van een aanval niet herkennen, kunnen ze risico’s niet minimaliseren of aanvalsketens onderbreken", vervolgt Wisniewski. "EDR helpt IT-managers bij het identificeren van risico’s almede het opzetten van een plan aan beide uiteinden. Wanneer IT meer gericht is op opsporing, kan EDR sneller vinden, blokkeren en verhelpen; wanneer IT nog steeds een security basis aan het opbouwen is, is EDR een integraal onderdeel dat de broodnodige *threat intelligence* oplevert."

Volgens de enquête spenderen organisaties die elke maand een of meer beveiligingsincidenten onderzoeken gemiddeld 48 dagen per jaar om deze te onderzoeken. Het is geen verrassing dat IT-managers de identificatie van verdachte gebeurtenissen (27 procent), alert management (18 procent) en het prioriteren van verdachte gebeurtenissen (13 procent) als de drie belangrijkste functies zien die ze nodig hebben van EDR-oplossingen.

"De meeste *spray and pray*-cyberaanvallen kunnen binnen enkele seconden op endpoints worden gestopt zonder alarm te slaan. Volhardende aanvallers, inclusief doelgerichte ransomware zoals SamSam, nemen de tijd die ze nodig achten een ​​systeem te infiltreren door zwakke wachtwoorden te vinden op systemen die op afstand kunnen worden beoordeeld. Denk daarbij aan onder meer RDP, VNC en VPN. Vervolgens krijgen ze voet aan grond en verroeren zich niet totdat de schade is aangericht. Als IT-managers diepgaande maatregelen nemen met EDR, kunnen ze ook sneller incidenten onderzoeken en deze informatie hergebruiken. Zodra cybercriminelen weten dat bepaalde soorten aanvallen werken, gebruiken ze deze meestal opnieuw binnen organisaties. Het aan het licht brengen en blokkeren van patronen kan bijdragen aan het terugdringen van het aantal dagen dat IT-managers besteden aan het onderzoeken van potentiële incidenten."

57 procent van de respondenten geeft in het onderzoek aan dat ze van plan waren binnen een periode van een jaar een EDR-oplossing te implementeren; 80 procent van de IT-managers zou willen dat ze een sterker team om zich heen hadden.

**Over het onderzoek**

De 7 Uncomfortable Truths of Endpoint Security-enquête werd uitgevoerd door Vanson Bourne in december 2018 en januari 2019. Dit onderzoek interviewde 3.100 IT-beleidsmakers in 12 landen en op zes continenten: 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:**

Sandra Van Hauwaert, Square Egg Communications, sandra@square-egg.be, GSM 0497 251816