*Sophos publiceert resultaten van onderzoek The Dirty Secrets of Network Firewalls*

**‘Bedrijven lopen gevaar door ongeïdentificeerd netwerkverkeer’**

* IT-managers niet in staat 45% van het netwerkverkeer van hun bedrijf te identificeren
* 84% van de bedrijven zijn ervan overtuigd dat gebrek aan zichtbaarheid van applicaties een niet te verwaarlozen probleem vormt
* 52% van de bedrijven zegt ook bezorgd te zijn om verlies aan productiviteit ten gevolge van niet-gewenste of nutteloze applicaties die niet op netwerk zichtbaar zijn

Brussel, 18 april 2018– **Uit het wereldwijde Sophos-onderzoek ‘The Dirty Secrets of Network Firewalls’ blijkt dat IT-managers niet in staat zijn om 45% van het netwerkverkeer binnen hun organisatie te identificeren; in werkelijkheid kan één op de vier managers 70% van het netwerkverkeer niet identificeren. Dit gebrek aan zichtbaarheid stelt bedrijven voor grote beveiligingsuitdagingen en heeft impact op effectief netwerkbeheer.**

Gelet op de desastreuze gevolgen van zakelijke cyberaanvallen is het niet verwonderlijk dat 84% van de respondenten het erover eens is dat het gebrek aan zichtbaarheid van de applicaties een ernstig veiligheidsissue vormt. Als ze niet kunnen weten wat er op hun netwerk gebeurt, zijn IT-managers blind voor ransomware, ongekende malware, datalekken en andere geavanceerde bedreigingen, potentieel schadelijke applicaties én malafide gebruikers. Netwerkfirewalls met signature-based opsporing kunnen onmogelijk voldoende zichtbaarheid garanderen op het verkeer en dit, omwille van diverse factoren, zoals een verhoogd gebruik van encrypties, browseremulatie en geavanceerde ontwijktechnieken.

“Wanneer je niet alles op je netwerk ziet, kun je er ook nooit zeker van zijn dat je bedrijf perfect beveiligd is,” zegt Dan Schiappa, Senior Vice President en General Manager Products bij Sophos. “IT-professionals zijn te lang blind geweest en cybercriminelen hebben hiervan gebruik gemaakt. Nu regeringen wereldwijd zware straffen opleggen voor datalekken en -verliezen wordt het belangrijk te weten wat er op het netwerk gebeurt.”

Bedrijven geven gemiddeld zeven werkdagen per maand aan het opschonen van zestien geïnfecteerde apparaten. Volgens het onderzoek zouden bedrijven met tussen de 100 en 1.000 gebruikers gemiddeld vijf werkdagen vrijmaken aan het opschonen van dertien toestellen en grotere bedrijven (1001 tot 5.000 gebruikers) gemiddeld tien werkdagen aan het opschonen van twintig apparaten per maand.

“Een enkele inbreuk in het netwerk brengt vaak meerdere computers in gevaar. Hoe sneller je een infectie een halt kunt toeroepen, hoe meer de schade kan worden beperkt en de tijd die nodig is om de computers op te schonen,” verklaart Schiappa. “Bedrijven zijn op zoek naar next-generation geïntegreerde network- en endpoint security die geavanceerde bedreigingen een halt kunnen toeroepen en voorkomen dat een geïsoleerd incident ontaardt in een grote uitbraak. Geavanceerde producten als MimiKatz en EternalBlue hebben de wereld eraan herinnerd dat network security essentieel is voor de endpoint security en omgekeerd. Alleen directe [intelligence sharing](https://www.sophos.com/en-us/lp/synchronized-security.aspx) tussen beide kan de echte aard van wie en wat er op het netwerk bezig is aan het licht brengen.”

IT-managers zijn zich ervan bewust dat de firewalls een upgrade nodig hebben op het vlak van beveiliging. Uit het onderzoek bleek immers dat 79% van de ondervraagde IT-managers een betere beveiliging verwacht van hun gebruikelijke firewall. 99% wil een firewalltechnologie die geïnfecteerde computers automatisch isoleert en 97% wil een endpoint- en firewall security van dezelfde leverancier zodat de gegevens met betrekking tot de veiligheidsstatus direct kunnen worden gedeeld.

**Beveiliging is niet het enige issue**

52% van de ondervraagden vond dat, naast veiligheidsrisico’s, verlies aan productiviteit belangrijk is als men over netwerkzichtbaarheid spreekt. De productiviteit kan lijden onder het feit dat de IT niet bij machte is om voor kritieke toepassingen prioriteit te verlenen aan bandbreedte.

Bij bedrijven die vertrouwen op maatwerksoftware die voldoet aan hun specifieke behoeften, kan de onmogelijkheid om voorrang te verlenen aan deze taakgerichte kritieke toepassingen voor minder belangrijk verkeer hen duur komen te staan. 50% van de IT-professionals die hadden geïnvesteerd in maatwerksoftware geeft toe dat hun firewall niet bij machte was het verkeer te identificeren en dat ze dus hun ROI niet konden optimaliseren. Een gebrek aan zichtbaarheid maakt bovendien blind voor potentiële transfers van illegale of ongepaste gegevens op de bedrijfsnetwerken, die zouden kunnen leiden tot procedures en nalevingsproblemen.

“Bedrijven hebben meer dan behoefte aan een [firewall](https://www.sophos.com/en-us/press-office/press-releases/2017/10/sophos-xg-firewall-delivers-a-breakthrough-in-network-visibility-with-synchronized-app-control.aspx) die hun investering in bedrijfskritische en maatwerkapplicaties beveiligt door het personeel de mogelijkheid te bieden toegang te krijgen tot de applicaties die ze nodig hebben,” voegt Schiappa eraan toe. “Een verhoogde netwerkzichtbaarheid vereist een totaal andere benadering. Door de firewall toe te laten rechtstreeks informatie te hebben vanuit de endpoint security, kunnen alle applicaties positief worden geïdentificeerd. Dus ook obscure en maatwerkapplicaties.”

Het onderzoek “The Dirty Secrets of Network Firewalls” werd in oktober en november 2017 gevoerd door Vanson Bourne, een onafhankelijke specialist in marktonderzoek. Hiervoor werden 2.700 IT DMU’s in tien landen en vijf continenten bevraagd (VS, Canada, Mexico, Frankrijk, Duitsland, UK, Australië, Japan, India, Zuid-Afrika). Alle respondenten waren aan het werk in bedrijven met 100 tot 5.000 gebruikers.

**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:**

Sandra Van Hauwaert, [sandra@square-egg.be](mailto:sandra@square-egg.be), GSM 0497 251816