Persbericht

**Sophos voegt Deep Learning toe aan Sophos Email Advanced**

*• Sophos Email door Artificial Intelligence versterkt*

*• Beschermt e-mails van Microsoft Office365, Google G-Suite en Exchange 2003+*

*• Nieuwe anti-phishing-authenticatie met behulp van SPF, DKIM en DMARC*

*• Cloud-managed bescherming via Sophos Central*

Brussel, 13 juni 2018 - **Sophos lanceert Sophos Email Advanced, de eerste oplossing voor e-mailbeveiliging die voorspellende beveiliging biedt door middel van Active Threat Protection (ATP), anti-phishing email-authenticatie en outbound scanning en policy support.**

Een SophosLabs-onderzoek heeft onlangs uitgewezen dat 75% van de malware in een organisatie voor die organisatie ‘uniek’ is en duidt erop dat de meeste aanvallen zero-day zijn. De enige manier om dit te bestrijden, is met het *deep learning* neurale netwerk dat is geïntegreerd in de Sophos Email-sandboxtechnologie om zo kwaadwillende, onbekende bestanden die in e-mails zijn verzonden te identificeren.

E-mail blijft een primaire aanvalsmethodiek voor cybercriminelen om ​​‘spear-phishing’, gelokaliseerde of 'spray and pray'-campagnes te starten. Sophos verwerkt dagelijks gegevens uit meer dan tien miljoen inboxen die door Sophos Email worden beschermd. Ongeveer 80% van de e-mails die zijn gecategoriseerd als spam, blijken een schadelijke payload te bevatten. Zoals we de afgelopen jaren hebben gezien, is e-mail ook de belangrijkste methode voor het verspreiden van ransomware.

Een ander recent Sophos-onderzoek heeft aangetoond dat meer dan 50% van de organisaties wereldwijd de afgelopen twaalf maanden een ransomware-aanval heeft doorstaan. Sophos Email Advanced bevat de CryptoGuard-technologie in de sandbox om ransomware te stoppen voordat deze in de inbox van werknemers terechtkomt. Een andere primaire verdediging tegen ransomware en phishing-aanvallen is *Time-of-Click*-bescherming. Hierbij wordt de URL gescand op het moment van de muisklik, zodat ongeziene en vertraagde aanvallen worden voorkomen. Outbound scannen en meerzijdige policy support kunnen voorkomen dat een organisatie onbedoeld malware doorstuurt of spam verzendt naar zakelijke relaties en op die manier de reputatie van een organisatie beschermt.

*"Met de groei van cloudgebaseerde platforms waaronder Office365 en Google G-Suite hebben organisaties een geavanceerde beveiligingsoplossing nodig die zero-day bedreigingen en geavanceerde malware opspoort. Ransomware as a Service en ‘malwaresets’ maken het voor cybercriminelen gemakkelijker meer complexe, gerichte aanvallen via e-mail uit te voeren,* " licht Bill Lucchini toe, Senior Vice President en General Manager Messaging Security Group bij Sophos. *"IT heeft slimmere, meer voorspelbare security nodig om hedendaagse bedreigingen op te sporen en te stoppen. Het Sophos Central cloud-gebaseerde beheer van Sophos Email Advanced kan de hoogste niveaus van beveiliging bieden om elk e-mailplatform te beveiligen, zodat elke gebruiker zijn inbox weer kan vertrouwen. "*

Sophos Email is een belangrijke pijler van een geïntegreerd gegevensbeveiligingssysteem voor de eindgebruiker, wanneer het via het Sophos Central-beheerplatform wordt beheerd. IT-professionals kunnen Intercept X-endpointbeveiliging naast Sophos Email Advanced en Phish Threat-trainingen gebruiken, waarbij een sterkere verdediging ontstaat om bedreigingen op te sporen en gebruikers te trainen. ‘Threat data’ van Sophos Email Advanced kunnen via Synchronized Security bijdragen aan de algehele informatie binnen SophosLabs.

**Active Threat Protection (ATP):**

• Sophos Sandstorm cloud-sandbox en geavanceerde URL-bescherming;

• ‘AI’ ingebouwd in Sandboxing van Sophos Email is in staat onbekende malware op te sporen en tegen te houden;

• Geavanceerde URL-bescherming die de reputatie van de website of e-mailkoppelingen controleert vóór de bezorging op het moment van aanklikken.

**Anti-Phishing Email Authentication**

• Combinatie van SPF, DKIM en DMARC-authenticatietechnieken en analyse van e-mailheaders;

• Sender Policy Framework (SPF) om te verifiëren wie e-mails van een bepaald domein kan verzenden;

• DKIM (Domain Keys Identified Mail) -authenticatiesysteem voor e-mail op basis van asymmetrische cryptografische sleutels;

• DMC (Domain Message Authentication Reporting & Conformance) om te bepalen wat te doen als berichten mislukken via SPF of DKIM.

**Outbound Scanning and Multi-Policy Support**

• Spam- en virusscanning van uitgaande e-mailscans om onbedoelde verspreiding van bedreigingen te voorkomen en reputatie te beschermen;

• Aangepaste security policies kunnen binnen enkele minuten voor individuen, groepen of het hele domein worden gemaakt.

**Deployment and Data Processing Location Options**

• Beschikbaar via Sophos Central cloudgebaseerd beheerplatform;

• Sophos Secure Email Gateways kunnen worden geïmplementeerd als een on-premise appliance of binnen de nieuwste versie van de Sophos XG Firewall;

• Message processing centers in Ierland, de VS en Duitsland;

• Sophos Sandstorm-locaties in Ierland, de VS en Japan.

**Voor meer informatie, interviewmogelijkheden of beeldmateriaal:**Square Egg, Sandra Van Hauwaert, sandra@square-egg.be, GSM 0497 251816

**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).