75% aller Malwareattacken auf Unternehmen sind Unikate – Sophos Email Advanced schützt mit Deep Learning-Funktion

Wiesbaden, 19. Juni 2018 – Sophos setzt mit Sophos Email Advanced auf vorausschauenden Schutz beim Thema Email-Sicherheit. Ausgestattet ist die Lösung mit aktivem Bedrohungsschutz (ATP), Anti-Phishing Email-Authentifikation sowie Ausgangs-Scan und Richtlinien-Support.

Nach Untersuchungen der SophosLabs sind rund 75 Prozent der Schadsoftware in einer Organisation ein Unikat, was darauf hindeutet, dass die Mehrheit der Angriffe Zero-Day-Attacken sind. Der einzige Weg, diese zu bekämpfen, besteht in der Nutzung eines selbst lernenden, neuronalen Netzwerks, das in die Sophos Email Sandbox Technologie integriert ist. So können neue, noch unbekannte Malware-Dateien in Emails schnell identifiziert werden.

Email als primärer Angriffsvektor für Spear-Phishing
Email bleibt der primäre Angriffsvektor für Cyberkriminelle, um eine Spear Phishing, lokal eingegrenzte oder „Spray and Pray"-Kampagne umzusetzen. Spear Phishing ist eine Phishingmethode, mit der gezielt Organisationen oder Personen zwecks Finanzbetrugs angegriffen werden. Eine „Spray and Pray"-Attacke baut hingegen auf eine möglichst breite Streuung und setzt darauf, dass in der Masse irgendein Opfer darauf hereinfällt. Sophos verarbeitet täglich Daten von mehr als zehn Millionen Posteingängen, die von Sophos Email geschützt werden. Schätzungsweise 80 Prozent der Emails, die als Spam kategorisiert sind, wurden mit schadhaften Payloads (also die schädlichen Auswirkungen der Software) identifiziert. Wie sich in den letzten Jahren zeigte, sind Emails auch die beliebteste Methode, um Ransomware zu verbreiten.

Ransomware stoppen, bevor sie in der Inbox landet. Und ungewollt beim Kunden.
Eine kürzlich veröffentliche Studie von Sophos zeigte, dass mehr als 50 Prozent der Unternehmen weltweit in den letzten zwölf Monaten unter einer Ransomware-Attacke litten. Sophos Email Advanced beinhaltet die CryptoGuard-Technologie in einer Sandbox, um Ransomware zu stoppen bevor sie überhaupt in die Posteingänge der Mitarbeiter gelangen kann. Eine andere direkte Form der Verteidigung gegen Ransomware und Phishing-Angriffe ist der Time-of-Click-Schutz, der die URL in dem Moment scannt, in dem sie angeklickt wird. Das verhindert heimliche und verzögerte Attacken. Ausgehender Scan und umfangreicher Richtlinien-Support können eine gefährdete Organisation davor bewahren, unbeabsichtigt Schadsoftware oder Spam an Kunden oder Partner weiterzuleiten. Diese Funktionen reduzieren den Einfluss einer Attacke auf eine größere Nutzergruppe und schützen so die Reputation.

Die Lösung: Bedrohungen vorab erkennen
„Mit dem Wachstum cloudbasierter Plattformen wie Office365 und Google G-Suite benötigen Organisationen eine erweiterte Sicherheitslösung, die Zero-Day-Bedrohungen und hochentwickelte Schadsoftware erkennt. Ransomware-as-a-Service (RaaS) und Malware-Bausätze haben es Cyberkriminellen erleichtert, komplexe, zielgerichtete Angriffe via Email individuell anzupassen", bewertet Bill Lucchini, Senior Vice President und General Manager Messaging Security Group bei Sophos. „Mit dem wahrscheinlichen Wachstum von Office365 und Cloud-basierter Email muss die IT auf clevere, vorausschauende Sicherheit setzen, um

Bedrohungen zu entdecken und zu stoppen. Das mit Sophos Central verwaltete Sophos Email Advanced liefert den höchsten Sicherheitslevel, um jegliche Email-Plattform zu schützen."

Die neuen Funktionen von Sophos Email auf einen Blick:

Aktiver Bedrohungsschutz (Active Threat Protection)

- Sophos Sandstorm-Cloud-Sandbox und weiterentwickelter URL Schutz
- Die Deep-Learning-Funktion in der Sandbox entdeckt und blockiert bisher unerkannte Schadsoftware.
- Time-of-Click im URL-Schutz prüft die Webseiten-Bewertung oder Email-Links vorab und im Moment des Anklickens. Vorteil: Blockade von schleichenden und verzögerten Attacken

Anti-Phishing Email Authentifikation

- Kombination von SPF, DKIM, und DMARC Authentifikations-Technologien und Email-Header Analyse
- Sender Policy Framework (SPF) zur Bestimmung und Verifizierung, wer Emails von einer bestimmten Domain verschicken darf
- Domain Keys Identified Mail (DKIM), ein Email-Authentifikationssystem, das auf asymmetrischer Verschlüsselung beruht
- Domain Message Authentification Reporting & Conformance (DMARC), um festzulegen, was zu tun ist, wenn Nachrichten gegen SPF verstoßen

Abgehender Email-Scan und Umfassender Richtlinien-Support

- Spam- und Viren-Scan aller ausgehenden Emails, um unbeabsichtigte Verbreitung von Bedrohungen zu verhindern und das eigene Ansehen zu schützen
- Entwicklung individueller, gruppen- oder bereichsspezifischer Sicherheitsrichtlinien

Verfügbarkeit

Sophos Email Advanced ist für registrierte Sophos Partner weltweit erhältlich. Weitere Informationen liefert die Sophos Webseite.

Über Sophos

Mehr als 100 Millionen Anwender in 150 Ländern verlassen sich auf Sophos' Complete-Security-Lösungen als den besten Schutz vor komplexen IT-Bedrohungen und Datenverlust. Sophos bietet dafür preisgekrönte Verschlüsselungs-, Endpoint-Security-, Web-, Email-, Mobile- und Network Security-Lösungen an, die einfach zu verwalten, zu installieren und einzusetzen sind. Das Angebot wird von einem weltweiten Netzwerk eigener Analysezentren, den SophosLabs, unterstützt.
Sophos hat seinen Hauptsitz in Boston, USA, und Oxford, Großbritannien. In Deutschland hat das Unternehmen seinen Hauptsitz in Wiesbaden und ist in Österreich und der Schweiz je an einem Standort vertreten. Weitere Informationen unter www.sophos.de.

Pressekontakt

Sophos
Jörg Schindler, PR Manager CEEMEA

joerg.schindler@sophos.com, +49-721-25516-263

TC Communications
Arno Lücht, +49-8081-954619
Thilo Christ, +49-8081-954617
Ulrike Masztalerz, +49-30-55248198
Ariane Wendt +49-172-4536839
sophos@tc-communications.de