Im toten Winkel der Firewall: 45 Prozent Netzwerk-Traffic unsichtbar

In einer Studie zum Thema Netzwerk-Firewalls hat Sophos ernsthafte Risiken für Unternehmen ausgemacht: IT-Manager aus USA, Europa und Asien konnten 45 Prozent ihres Netzwerk-Traffics nicht eindeutig zuordnen.

Fast jeder vierte Studienteilnehmer konnte 70 Prozent des Netzwerk-Traffics in seiner Organisation nicht identifizieren. Dieser Mangel an Sichtbarkeit bewirkt eine signifikante Sicherheitsherausforderung für heutige Unternehmen und hat Auswirkungen auf das effektive Netzwerk-Management. Im Auftrag von Sophos befragte ein unabhängiges Marktforschungsinstitut mehr als 2.700 IT-Entscheider mittelgroßer Unternehmen in zehn Ländern: Deutschland, Frankreich, UK, USA, Kanada, Mexiko, Australien, Japan, Indien und Südafrika.

Was man nicht sieht, kann man auch nicht verhindern

Bedenkt man die lähmenden Auswirkungen von Cyber-Attacken auf Unternehmen, überrascht es nicht, dass 84 Prozent der Befragten der Aussage zustimmen, dass ein Mangel an Sichtbarkeit von Anwendungen ein ernsthaftes Sicherheitsrisiko darstellt. Fehlt die Möglichkeit, den Netzwerk-Traffic zu identifizieren, bleiben auch Ransomware, unerwünschte Malware, Datendiebstahl und andere hochentwickelte Bedrohungen im Verborgenen. Genauso wie potentiell schadhafte Apps und kriminelle User. Netzwerk-Firewalls mit Signatur-basierter Erkennung sind nicht in der Lage, adäquate Transparenz der App-Traffic zu gewähren. Die Gründe dafür sind vielfältig – angefangen bei einem Anstieg von Verschlüsselungen über Browser-Emulation bis hin zu ausgeklügelten Ausweichtechniken.

„Wenn man nicht sehen kann, was auf dem Netzwerk passiert, kann man auch nie sicher sein, dass die eigene Organisation vor Gefahren geschützt ist“, so Dan Schiappa, Senior Vize Präsident und General Manager Produkte bei Sophos. „Da Regierungen weltweit dazu übergehen härtere Strafen für Datendiebstahl und -verlust einzuführen, wird das Wissen darum, wer und was auf dem eigenen Netzwerk agiert, zunehmend bedeutender. Dieser Zustand kann nicht länger ignoriert werden.“

16 infizierte Geräte pro Monat

Im Durchschnitt verwenden Organisationen sieben Werktage darauf, 16 infizierte Maschinen pro Monat zu beseitigen. Kleinere Unternehmen (100-1.000 Nutzer) benötigen im Durchschnitt fünf Werktage für 13 befallene Geräte, während größere Unternehmen (bis 5.000 Nutzer) rund zehn Werktage für 20 Rechner benötigen, die nicht rund laufen.

„Eine einzige Netzwerk-Panne gefährdet oft zahlreiche Computer. Je schneller man also die Infektion stoppen kann, desto stärker reduziert man den Schaden und die Rekonvaleszenz-Zeit“, so Schiappa. „Raffinierte Exploits wie MimiKatz und EternalBlue zeigten zuletzt jedem, wie entscheidend die Netzwerk-Sicherheit für den Endpoint-Schutz ist und vice versa. Nur direkt geteilte Intelligenz zwischen diesen beiden kann tatsächlich aufdecken, wer und was auf dem eigenen Netzwerk operiert. Unternehmen suchen daher aktuell nach der Art von

integriertem Netzwerk und Endpoint-Schutz, der hochentwickelte Bedrohungen stoppen kann und isolierte Störungen daran hindert, sich in einen immensen Ausbruch zu verwandeln."

Ganz oben auf der Wunschliste der IT-Profis: Firewalls mit Isolationsfunktion
IT-Manager sind sich bewusst, dass Firewalls ein Sicherheitsupgrade benötigen. 79 Prozent der Befragten wünschen sich einen besseren Schutz ihrer aktuellen Firewall. Fast alle (99 Prozent) bevorzugen eine Firewall-Technologie, die automatisch infizierte Computer isolieren kann. 97 Prozent der Befragten favorisieren Endpoint- und Firewall-Schutz von einem Verkäufer, damit ein direkter Austausch von Sicherheitsinformationen gewährleistet ist.

52 Prozent der Befragten sind besorgt über einen Verlust an Produktivität, wenn es zu einem Mangel an Netzwerk-Sichtbarkeit kommt. Wirtschaftliche Produktivität kann negativ beeinflusst werden, wenn die IT nicht in der Lage ist, die Bandbreite kritischer Anwendungen zu priorisieren. Für Industrien, die auf Kunden-Software setzen, um auf deren spezifische Unternehmensbedürfnisse eingehen zu können, kann dieses Unvermögen kostenintensiv sein. 50 Prozent der IT-Profis, die in Kunden-Apps investierten, gaben zu, dass ihre Firewall den Traffic nicht identifizieren konnte und demnach nicht in der Lage war, den ROI zu maximieren. Der Mangel an Sichtbarkeit bewirkt zudem einen toten Winkel für den möglichen Transfer von illegalem oder unangemessenem Content auf gemeinsamen Netzwerken. Das macht Unternehmen verletzlich im Hinblick auf Rechtsstreitigkeiten und Compliance-Fragen.

„Organisationen benötigen eine Firewall, die ihre Investitionen in Unternehmens-kritische und Kunden-Apps schützt, indem sie den Mitarbeitern erlaubt, priorisierten Zugang zu den Anwendungen zu haben, die sie benötigen", rät Schiappa. „Wachsende Netzwerk-Sichtbarkeit erfordert einen radikal anderen Ansatz. Indem man der Firewall ermöglicht, Informationen direkt von der Endpoint-Sicherheit zu erhalten, kann sie alle Anwendungen identifizieren – auch verdeckte oder solche, die von Kunden verwendet werden."

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