Kein Radar für App-Traffic: die Probleme von Firewalls

Die Entwicklungen von Firewalls steht vor ganz neuen Herausforderungen. Verschiebungen in der Bedrohungslandschaft, ein dramatischer Anstieg in Anzahl und Komplexität von Technologien, mit denen System-Administratoren sich auseinandersetzen müssen, und nicht zu vergessen: eine Flut an Daten. Die modernen Firewalls können zwar heute weitaus mehr, doch auch viele sogenannte Next-Gen-Lösungen haben eine Problem: App-Traffic.

Wiesbaden, 11. Januar 2018. Eine kürzlich durchgeführte Befragung von IT-Administratoren zeigt die Probleme derzeitiger Firewalls auf: Administratoren müssen sich sehr lange mit ihnen auseinandersetzen, um die für sie nötigen Informationen zu erhalten. Die derzeitigen Firewalls bieten keine adäquate Sicht in Bedrohungen und Netzwerk-Risiken an. Und: Sie sind so komplex, dass die vielen Funktionen gar nicht sinnvoll genutzt werden können.

Für die Netzwerk-Sicherheit bedeutet das noch einmal eine radikal neue Betrachtungsweise, denn sie muss:

- ermöglichen, dass Sicherheitssysteme zusammenarbeiten können
- einen vereinfachter und stromlinienförmiger Workflow schaffen und
- das enorme Datenvolumen sichten und nach Wichtigkeit identifizieren.

Problem 1: Komplexe Funktionen und mangelnde Integration von Sicherheitslösungen
Ursprünglich lieferten Firewalls basic Netzwerk-Pakete, die filterten und weiterleiteten, basierend auf Hosts, Ports und Protokollen. Die erzwangen quasi eine Grenze zwischen dem Netzwerk und dem Rest der Welt und patrouillierten an der Grenze. Sie waren effektiv darin, den Kontakt mit den Services auf den Computer und die Netzwerke zu limitieren, die Zugang zueinander haben mussten. Damit reduzierten sie auch die Angriffsfläche für Hacker und Schadsoftware von aussen.
Die heutigen Gefahren haben sich aber auf die Bereiche verlagert, die Firewalls mit ihrer Funktionalität gar nicht schützen können: Sicherheitslücken in Apps und auf Servern, oder mit Hilfe von Emails oder Webseiten, Datenverluste und der Notwendigkeit, die Netzwerk-Performanz zu optimieren.
Natürlich hat sich auch das Können von Firewalls verbessert. Die Verschiebung der Bedrohungen von Ports und Netzwerkprotokollen zu Applikationen und dem Nutzer selbst hat eine neue Kategorie von Netzwerkschutz hervorgebracht, die so genannten next-generation Firewalls. Sie verfügen über tiefgreifende Überwachungsfunktionen für verschlüsselten wie unverschlüsselten Datenverkehr, Schutz vor Netzwerkeindringlingen, App-Kontrolle und nutzerbasierten Strategien. Die SysAdmins können VoIP Traffic oder CRM Software über Streaming-Medien priorisieren oder Nutzer von peer-to-peer Datenaustausch- Applikationen blockieren oder identifizieren.

Problem 2: 60 Prozent von App-Traffic bleibt unidentifiziert laut Sophos Umfrage
Diese Art der Kontrolle basiert auf der Fähigkeit der Firewall, Apps erfolgreich zu identifizieren mithilfe von Mustern und Signaturen. Doch manche Apps ändern ihre Muster permanent, um das Sicherheitssystem zu umgehen. Andere bleiben unentdeckt durch Verschlüsselung oder Maskierung zum Beispiel als Web-Browser. Die Signatur-Erkennung kann auch dann fehl schlagen, wenn eine App upgedated wird und das Traffic-Muster sich ändert. Auch die next-gen Firewall kann den Traffic aus Applikationen größtenteils nicht einordnen und kontrollieren, weil die schlichtweg den App-Datenverkehr gar nicht erkennt. Der Traffic erscheint als HTTP, HTTPS, TLS oder anderen nicht hilfreichen Kategorien, die man dann in seinem App-Kontrollreport vorfindet.

Sophos führte kürzlich eine Umfrage in mittelgroßen Unternehmen durch, um herauszufinden, wie hoch der Anteil an Datenverkehr ist, der unidentifiziert und damit unkontrolliert bleibt. Fast 70 Prozent der Befragten setzen eine next-gen Firewall oder UTM mit App-Bewusstsein ein. Im Durchschnitt sind 60 Prozent des Traffic unerkannt. Mehr noch: viele Unternehmen gaben an, dass bis zu 90 Prozent ihres App-Traffic unidentifiziert bleibt.
Die Mehrheit der Befragten (82 Prozent) zeigte sich ernsthaft besorgt über diese Ergebnisse.

Die Studie von Sophos gibt aber noch mehr preis: Die Apps, die den Befragten am meisten Sorgen bereiteten, weil sie entweder eine große Sicherheitsschwachstelle sind oder gegen Vorschriften verstoßen könnten, durch unangemessenen oder illegalen Inhalt oder Bandbreitenverlust:

- Instant Messanger und Konferenz-Apps wie Skype und Team Viewer
- BitTorrent und andere peer-to-peer Clients
- Proxy und Tunnel Clients wie Ultrasurf, Hotspot Shield und Psiphon
- Spiele und deren Plattformen wie Steam

Wie sieht die Lösung aus?
Netzwerk-Sicherheit benötigt einen neuen Denkansatz: die Integration komplexer Technologien und eine neue Generation von Firewalls, die die bestehenden Probleme der aktuellen Firewalls bei ihrer Entwicklung berücksichtigt und die sich mit den neuen Bedrohungen auseinandersetzt. Sophos hat genau diesen Schritt mit Synchronized App Control bei seiner XG Firewall gemacht und verschafft Klarheit und Kontrolle über den gesamten Anwendungsverkehr im Unternehmensnetzwerk. Synchronized App Control identifiziert automatisch alle unbekannten Programme, in dem sich Endpoint und Firewall intelligent untereinander austauschen. So können unerwünschte Anwendungen einfach blockiert bzw. unterstützte Anwendungen priorisiert werden

Mehr Informationen zu dem Thema gibt es in dem englischen White Paper „Keep your network under control“.

Über Sophos
Sophos ist führender Anbieter von Endpoint- und Network-Security-Lösungen der nächsten Generation. Als Pionier der Synchronized Security entwickelt Sophos sein innovatives Portfolio an Endpoint-, Netzwerk-, Verschlüsselungs-, Web-, E-Mail- und mobilen Security-Lösungen, die miteinander kommunizieren. Mehr als 100 Millionen Anwender in 150 Ländern verlassen sich auf Lösungen von Sophos mit hervorragendem Schutz vor anspruchsvollen Bedrohungen und Datenverlust. Sophos Produkte sind exklusiv über den weltweiten Channel mit mehr als 26.000 registrierten Partnern erhältlich. Sophos hat seinen Hauptsitz in Oxford, Großbritannien, und wird an der Londoner Börse unter dem Symbol "SOPH" öffentlich gehandelt. 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 +172 4536839
sophos@tc-communications.de