Hybrides Arbeiten und Netzwerksicherheit: die Firewall-Metamorphose

Immer mehr Unternehmen verlagern Ressourcen und Infrastruktur in die Cloud. Angesichts dieser Entwicklung kommen herkömmliche Firewalls an ihre Grenzen.

Kommentar von Michael Veit, Security Evangelist bei Sophos

Die momentane Entwicklung der modernen Arbeitswelt legt den Schluss nahe, dass sowohl traditionelle als auch Cloud-Umgebungen zu einer Welt zusammenwachsen, in der Anwendungsfälle für hybride Sicherheitsinfrastrukturen die Zukunft der Netzwerksicherheit dominieren werden. Hier können SASE-Ansätze den Unternehmen ein höchstes Maß an Flexibilität bieten, um auf beiden Seiten des Spektrums zu interagieren und zu arbeiten, während der Übergang in diese neue Arbeitswelt voranschreitet.

Folge der aktuellen Entwicklung ist, dass immer mehr Unternehmen Ressourcen und Infrastruktur in die Cloud verlagern. Diese Migration hat die Grenzen herkömmlicher Firewalls aufgezeigt, die nicht mehr in der Lage sind, die für hybride und virtualisierte Umgebungen typischen Sicherheitsprobleme zu bewältigen. Daraus ergeben sich zwei der wichtigsten Anforderungen und Eigenschaften, die eine Netzwerk-Firewall der Zukunft erfüllen muss:

1. Das Management einer zerstreuten Verwaltungs- und Kontrollebene, in der die Steuerung und Kontrolle der Firewall-Funktionen in den eher „traditionellen“ Perimeter-Anwendungsfällen flexibel beibehalten werden kann, während gleichzeitig ein Richtlinienkonstrukt übernommen wird, das auch in der Cloud anwendbar ist. Eine Technologie, die über beide Bereitstellungstypen und Anwendungsfälle hinweg sicherstellen kann, dass die Kundenerfahrung und damit die Übernahme des neuen Ansatzes positiv sein wird, ist deshalb essenziell.

2. Die Skalierbarkeit der Verarbeitungsdatenebene muss ebenfalls ein Schlüsselfaktor sein. Die noch notwendige On-Premise-Bereitstellung erfordert Dinge wie SD-WAN, interne Sicherheitsverarbeitung und Konnektivität – muss aber aufgrund von Upgrades in Konnektivitätsinfrastrukturen wie 5G auch in der Lage sein, noch höhere Geschwindigkeiten als zuvor zu verarbeiten. Wohingegen in der Cloud bereitgestellte Firewalls den plötzlichen Anstieg der Verarbeitungsanforderungen bewältigen müssen, da die Benutzer immer mehr mobil und in verschiedenen Zeitzonen online arbeiten. Daher ist eine Datenebene, die für beide Szenarien funktioniert und gleichzeitig eine ähnliche Benutzererfahrung bietet, ebenfalls sehr wichtig.

In Folge dieser Entwicklung werden wir immer mehr Dienste wie Secure Web Access, Zero Trust Network Access und SAAS Access Security sehen – und sie werden zu einer Hauptstütze für Unternehmen werden, da sie für Kunden bequem sind und bald auch vertraut sein werden. Bei näherer Betrachtung dieser Services wird schnell klar, dass sie sich im Wesentlichen mit dem Zugriff auf öffentliche Websites und öffentliche/private Anwendungen befassen. Die nächste natürliche Entwicklung für diese Angebote wird nun darin bestehen, den gesamten Datenverkehr und alle Daten an diese Dienste zu senden. Es entsteht ein natürlicher Ort, an dem Firewalls as a Service als Angebot hinzugefügt werden können. Während bislang vor allem Großkonzerne diese Plattformen nutzen, stehen die Angebote mittlerweile zu einem immer besseren Preis-Leistungs-Verhältnis zur Verfügung und werden

so auch für KMU-Kunden interessant. Auf diese Weise werden wir letztendlich eine immer größere Verschiebung von On-Premise-Firewalls hin zu SASE-Plattformen sehen.

Allerdings werden Firewalls immer einen Platz im Zero-Trust-Modell haben, sofern wir nicht glauben, dass alle Formen von Netzwerken aufhören zu existieren und die Netzwerk-zu-Netzwerk-Kommunikation sich praktisch auflöst. Momentan stellt die Perimeter-Platzierung für Organisationen einen immer wichtigeren Faktor dar – aber diese Transformation wird nicht von heute auf morgen stattfinden. Genau in diesen Unsicherheiten einer hybriden Arbeitswelt kann das flexible SASE-Modell punkten, Firewalls in verschiedenen Formen einbeziehen und damit kohärent mit den Zero-Trust-Prinzipien arbeiten. Die Möglichkeiten sind hier endlos.

Social Media von Sophos für die Presse
Wir haben speziell für Sie als Journalist*in unsere Social-Media-Kanäle angepasst und aufgebaut. Hier tauschen wir uns gerne mit Ihnen aus. Wir bieten Ihnen Statements, Beiträge und Meinungen zu aktuellen Themen und natürlich den direkten Kontakt zu den Sophos Security-Spezialisten.
Folgen Sie uns auf und

LinkedIn: https://www.linkedin.com/groups/9054356/
Twitter: @sophos_info

Pressekontakt:

Sophos
Jörg Schindler, PR-Manager Central & Eastern Europe
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