5 Top-Tipps zur Auswahl der richtigen Firewall

Inhalt

Es ist an der Zeit, Ihre Firewall-Lösung zu überdenken. Machen Sie sie zur flexiblen, zuverlässigen Sicherheitsgrundlage in einer neuen Welt aus hybriden und verteilten Umgebungen.

1. Schauen Sie über den Tellerrand hinaus

Wie sieht eine moderne Firewall aus? Sie ist vollständig in Ihre Netzwerkinfrastruktur integriert und verfügt vor allen Dingen über eine zentrale Benutzeroberfläche, mit der sich Richtlinien überall durchsetzen lassen. Firewalls der nächsten Generation bieten plattformübergreifend einheitliche Richtlinien, Informationen zu Mobilgeräten, Kontext und Threat-Intelligence. So verfügen Sie über die notwendige Transparenz, um die Verbindungen zu Ihrem Netzwerk über angreifbare mobile Apps und Endpunkte effektiv zu schützen.

2. Erhalten Sie Einblicke in Ihren verschlüsselten Datenverkehr

Um zu sehen, was in verschlüsseltem Datenverkehr vor sich geht, musste dieser bisher zunächst vollständig entschlüsselt werden. Dies ist ein teurer und aufwendiger Prozess, der mit betrieblichen und rechtlichen Hürden verbunden ist. Letztendlich ist Ihr Netzwerk und Ihre Infrastruktur somit äußerst anfällig für Cyberangriffe wie Datenexfiltrationen (Datenschutzverletzungen) und Ransomware.

Die echte Herausforderung bestand also darin, einen Weg zur Identifizierung von schädlichen Aktivitäten innerhalb von verschlüsseltem Datenverkehr zu finden. Ihre neue Firewall sollte dazu auf jeden Fall in der Lage sein. Idealerweise sollte sie maximale Transparenz bei minimaler Verschlüsselung bieten – und das zu einem günstigen Preis.

3. Geben Sie sich nur mit umfassender Threat-Intelligence zufrieden

Die Angriffsfläche vieler Unternehmen nimmt zu und Bedrohungen, bei denen Netzwerke, Zweigstellen und (oftmals) angreifbare und veraltete Infrastrukturen ins Visier genommen werden, werden immer komplexer. Jedes Intelligence-Framework sollte Cyberkriminellen also immer einen Schritt voraus sein. Es sollte daher Bedrohungen wie Spam, Malware oder andere Angriffsarten stets zuverlässig korrekt identifizieren können.

Diese Informationen sollten Ihrer Firewall als Handlungsgrundlage dienen, um dynamischen Kontext über Geräte, Standorte und BenutzerInnen in Ihrem Netzwerk bereitzustellen.

4. Setzen Sie auf integrierte Security Resilience

Hybride Umgebungen, in denen BenutzerInnen routinemäßig mit angreifbaren Geräten und Apps auf Ihr Netzwerk zugreifen, bieten Hackern zahlreiche Einfallstore in Ihr Netzwerk. Dies gilt insbesondere für veraltete Infrastruktur, die sich besonders gut als Angriffsziel eignet. Die Lösung für dieses Problem liegt im Aufbau von Security Resilience.

Wer über Security Resilience verfügt, sichert das Herzstück seiner hochverfügbaren Sicherheitsinfrastruktur – nämlich seine Firewall – umfassend ab, um Warnungen und Aufgaben basierend auf dem jeweiligen Risikoniveau priorisieren, zuverlässige Prognosen erstellen und stündliche Sicherheitsupdates und Reaktionen auf unvorhergesehene Angriffe automatisieren zu können. Dies spart Zeit, Nerven und Geld.

5. Entscheiden Sie sich für einen ganzheitlichen Ansatz

Warum sollten Sie sich nur auf die Firewall konzentrieren, anstatt mehrere leistungsstarke Tools für mehr Transparenz, Kontext und Einheitlichkeit beim Datenverkehrs- und Intelligence-Management zu verwenden? Mit den richtigen Tools können Sie die Performance Ihrer Firewall steigern, um so ohne zusätzliche Kosten mehr Einblicke zu erhalten und Zusammenhänge besser zu verstehen.

Die mangelnde Vernetzung von Services, mehreren Dashboards und Architekturen macht das Bedrohungsmanagement enorm komplex. Deshalb sollten Sie sich für eine Firewall und ergänzende Tools entscheiden, mit denen Sie schneller die richtigen Entscheidungen treffen, die Verweildauer reduzieren und aussagekräftige und verwertbare Metriken liefern können.

Erfahren Sie, wie Sie mit Cisco Secure Firewall Ihren Sicherheitsstatus verbessern und Ihr Unternehmen vor zunehmend komplexen Bedrohungen schützen können:

Mehr zu Cisco Secure Firewall

Hauptgeschäftsstelle Nord- und Südamerika
Cisco Systems, Inc.
San Jose, CA

Hauptgeschäftsstelle Asien-Pazifik-Raum
Cisco Systems (USA) Pte. Ltd.
Singapur

Hauptgeschäftsstelle Europa
Cisco Systems International BV Amsterdam,
Niederlande

Cisco verfügt über mehr als 200 Niederlassungen weltweit. Die Adressen mit Telefon- und Faxnummern finden Sie auf der Cisco Website unter **www.cisco.com/go/offices**.

Gedruckt in den USA C95-3416352-00 01/23