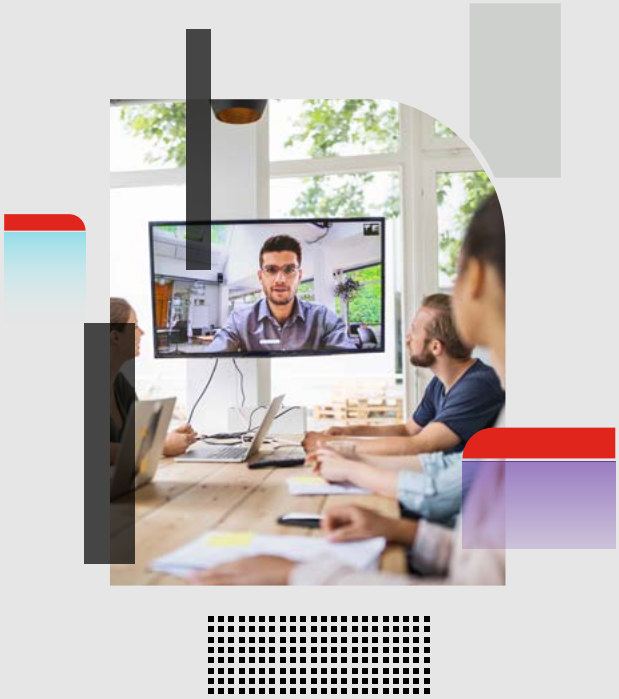
TIPPS VON FORTINET

Fünf vermeidbare Fehler beim Schutz von hybriden Netzwerken



Hybride Netzwerke gibt es mittlerweile in den meisten Unternehmen, nicht zuletzt wegen des Massenumzugs ins Homeoffice während der Pandemie. Laut Gartner hat diese Entwicklung Netzwerke dauerhaft verändert: „Bis 2024 werden Unternehmen bei digitalen Transformationsplänen mindestens fünf Jahre aufholen müssen, um ihre Existenz in den Zeiten nach COVID-19 zu sichern – und das verlangt die permanente Einführung von mehr Remote-Arbeitsplätzen und digitalen Touchpoints.“[1]

Heutige hybride Netzwerke erschweren jedoch eine zentrale Transparenz und Kontrolle, besonders wenn die Sicherheitsstrategie diese Zentralität nicht vorsieht: Im Durchschnitt sind in Unternehmen über 45 verschiedene Security-Tools im Netzwerk installiert (von denen die meisten von unterschiedlichen Anbietern stammen) und bei jedem Sicherheitsvorfall müssen 19 verschiedene Security-Lösungen koordiniert werden. Eine derartige Komplexität führt zwangsläufig zu mangelnder Transparenz, begrenzter Kontrolle und Sicherheitslücken, die Angreifer nur allzu gern ausnutzen.[2]

Die Konsolidierung und Integration von Netzwerk und Security ist der beste Ansatz, um komplexe Umgebungen in den Griff zu bekommen. Mit einer Next Generation Firewall (NGFW) als Rückgrat einer einheitlichen Sicherheitsstrategie lässt sich eine durchgängige Transparenz, ein unkompliziertes Management und eine einfache Kontrolle über das gesamte Netzwerk schaffen. Damit Sie die richtige Lösung für Ihre Anforderungen finden, gibt es jedoch einiges zu beachten.

Fünf häufige Fehler beim Schutz von hybriden Netzwerken

1. Fehler: Eine reine Cloud-Sicherheitslösung soll alles schützen. Manche wollen die vorhandene Security komplett durch eine SASE-Lösung (Secure Access Service Edge) ersetzen. Das Problem: Nur wenige Unternehmen haben eine reine Cloud-Umgebung. Die meisten arbeiten mit einem hybriden Netzwerk und werden dies auch weiterhin tun. Wird jetzt aber auf eine reine Cloud-Security umgestiegen, haben On-Premises-Anwender das Nachsehen.

Laut Gartner sind klassische Datacenter-Edge-Firewalls bei weitem nicht überflüssig, sondern sollten beibehalten werden. Diese Firewalls schützen die herkömmlichen eingehenden Datenfluss-Muster und die restlichen ausgehenden Verbindungen von internen Benutzern, die weiterhin im Firmensitz oder in Niederlassungen arbeiten.[3]

2. Fehler: Die Bedeutung des On-Premises-Rechenzentrums wird nicht erkannt. Aus unterschiedlichsten Gründen können die meisten Unternehmen nicht einfach kritische Dienste vom Rechenzentrum in die Cloud verlagern. Viele Anwendungen müssen für Kunden und Mitarbeiter weiterhin verfügbar sein und lassen sich nur mit klassischen On-Premises-Firewalls wirksam schützen.

Der Gartner-Bericht bestätigt dies und nennt auch die Probleme bei Sicherheitslösungen von Cloud-Anbietern: „Eine signifikante Minderheit der Unternehmen hält diese Angebote verglichen mit Lösungen von Drittanbietern für unausgereift. Manchmal werden NVA-Versionen (Network Virtual Appliance) dieser Drittanbieter direkt in Public-Cloud-IaaS-Instanzen implementiert." Weiter heißt es in dem Bericht: „Betreiber von Private und Public Clouds bieten native Firewall-, WAF- und ADC-Lösungen sowie einen DDoS-Schutz (Distributed Denial of Service) an."[4,5]

„Für öffentlich zugängliche Anwendungen, die in privaten Rechenzentren gehostet werden, wird IT-Verantwortlichen ein klassisches Enterprise-Firewall-Edge-Design empfohlen."[6]

Hybride Netzwerke brauchen eine Security-Lösung, die nativ in jeder Umgebung funktioniert. Nur so lassen sich alle Netzwerk-Ränder einheitlich schützen sowie netzwerkweit Bedrohungsinformationen austauschen und Sicherheitsrichtlinien konsequent durchsetzen. Die Grundlage dafür bildet eine gemeinsame Netzwerk-Firewall-Plattform, die an jedem Netzwerk-Edge bereitgestellt wird – auf dem Unternehmensgelände, im Rechenzentrum, in Niederlassungen, in Private und Public Clouds – und zudem als cloudbasierter Security-Dienst mobile und Remote-Mitarbeiter schützt.

3. Fehler: Statt einer ganzheitlichen Security wird auf erstklassige Einzellösungen gesetzt. Der Mythos, dass sich mit vielen sehr guten Einzelprodukten eine höhere Sicherheit am Netzwerk-Rand erreichen lässt, hält sich leider hartnäckig. Tatsächlich führt ein solcher Ansatz meistens zu einem Stückwerk aus zu vielen Insellösungen, die das Netzwerk unnötig komplex machen und Bedrohungsdaten nur rudimentär austauschen können. Für ein starkes Sicherheitsprofil ist ein solcher Ansatz kontraproduktiv – weil viele Einzelprodukte nie das gleiche hohe Maß an Transparenz und Sicherheit bieten können wie eine Lösung, die für die Zusammenarbeit entwickelt wurde. Nur integrierte Security-Ökosysteme, bei denen der Austausch umsetzbarer Bedrohungsinformationen von Grund auf vorgesehen ist, können robuste, koordinierte und zeitnahe Reaktionen auf Cyber-Ereignisse bieten.

Ein einheitliches System „aus einem Guss" ist immer sicherer als die Summe seiner vieler einzelner Lösungen. Wie würde z. B. ein Security-Konglomerat aus mehreren sehr guten Einzellösungen reagieren, wenn jemand bei einem als sicher eingestuftem Laptop einen unautorisierten USB-Stick einsetzt? Die meisten isolierten Netzwerk-Sicherheitsprodukte können das weder erkennen noch darauf reagieren. Aber eine EDR-Lösung für den Endpunkt-Schutz und die Bedrohungsreaktion macht genau das: Sie wurde von Grund auf für die Zusammenarbeit mit anderen Sicherheitssystemen entwickelt und kann die NGFW über diesen Richtlinienverstoß informieren. Die NGFW kann dann die Richtlinie durchsetzen und z. B. das Gerät isolieren oder vom Netzwerk trennen. So etwas ist jedoch nur mit einem Security-Ökosystem möglich, das auf einer gemeinsamen Security-Plattform aufbaut, umsetzbare Bedrohungsinformationen mit allen Sicherheitslösungen teilt und Richtlinien dort durchsetzen kann, wo es am effektivsten ist.

4. Fehler: Kein ganzheitliches Konzept. Hybride Architekturen entwickeln sich ständig weiter – und das führt zu einer erweiterten Angriffsfläche, weniger Transparenz und höheren Risiken. Erschwerend kommt hinzu, dass schon bald 95 % des Datenverkehrs verschlüsselt sein werden.[5] Die meisten Netzwerk-Firewalls können jedoch keinen verschlüsselten Datenverkehr überprüfen, ohne den Durchsatz stark zu verlangsamen, was wiederum heutige Anwendungen in die Knie zwingt. Wer aber nur 5 % des Datenverkehrs wirklich überwachen kann, ist von einem wirksamen Netzwerk-Schutz weit entfernt. IT-Verantwortliche brauchen deshalb eine leistungsstarke NGFW-Lösung, die sich netzwerkweit skalieren und betreiben lässt – ohne bei rechenintensiven Vorgängen wie der SSL-Inspektion, Bedrohungserkennung oder der automatisierten Behebung von Sicherheitsproblemen das Netzwerk auszubremsen.

Ihre Lösung sollte die neuesten Verschlüsselungsstandards wie TLS 1.3 sowie mit TLS 1.2 verschlüsselten Datenverkehr unterstützen. Neben maximaler Transparenz ist noch ein anderer Faktor wichtig: ob Ihre Lösung fit für die Zukunft ist. Eine gute Sicherheitslösung muss lernfähig sein. Sie sollte den Zustand von sich dynamisch ändernden Ressourcen, die überall im Netzwerk verstreut sind, erkennen und sich in Echtzeit anpassen können. Und sie muss berücksichtigen, wie verschiedene Clouds aufgebaut und konfiguriert sind. Ansonsten können Sie nur schwer standardisierte Sicherheitsrichtlinien für verschiedene Cloud-Anbieter durchsetzen. Achten Sie daher genau darauf, ob eine NGFW-Lösung den ständig wechselnden Zustand von Private- und Public-Cloud-Ressourcen erkennen kann. Die NGFW sollte für eine konsequente, einheitliche End-to-End-Security für Ihre gesamte hybride IT-Architektur sorgen, damit Ihr Unternehmen von einem starken, einheitlichen Sicherheitsprofil profitiert.

5. Fehler: Pauschaler „Vertrauensvorschuss“ beim Netzwerk-Zugang. Klassische flache Netzwerke sind meistens gut vor Angriffen von außen geschützt. Kann aber ein Cyberkrimineller trotzdem in das Netzwerk eindringen, gibt es kaum etwas, was ihn dann aufhält. Unternehmen sollten deshalb eine NGFW-Lösung wählen, die mehr als nur den Netzwerk-Rand schützt. Ideal ist eine NGFW, die Ihre Angriffsfläche zweifach verringert: mit einer internen Netzwerk-Segmentierung gegen äußere Angriffe über den Nord-Süd-Datenverkehr und mit einer Mikrosegmentierung, die die Ausbreitung netzwerkinterner Bedrohungen durch den Ost-West-Datenverkehr stoppt.

Zusätzlich zu dieser dynamischen Netzwerk-Segmentierung muss eine NGFW das gewährte Vertrauen dynamisch anpassen können – je nachdem, wie sich Benutzer und Geräte verhalten. Für diese Verhaltenskontrolle sind Tools wie Benutzer- und Entitätsverhaltensanalysen (UEBA) unverzichtbar. Auch sollte die Firewall einem Benutzer oder Gerät das gewährte Vertrauen entziehen können, wenn sich diese verdächtig verhalten.

Eine NGFW muss sich außerdem mit Lösungen für einen Zero-Trust-Access (ZTA) und einen Zero-Trust-Network-Access (ZTNA) integrieren lassen. Nur so kann die Firewall den Zugriff auf Netzwerk-Ressourcen engmaschig und pro Anwendungssegmentierung kontrollieren. Weiter sollte die NGFW ein Management von sogenannten „Headless“-Geräten bieten – Geräte ohne eigene Steuerung, wie man sie im Internet der Dinge (IoT) oder industriellen Internet der Dinge (IIOT) findet. Dafür muss die Firewall nahtlos in Ihre NAC-Lösung für die Netzwerk-Zugangskontrolle integrierbar sein. Das gewährleistet, dass jedes Gerät, jede Anwendung und jede Transaktion erfasst und geschützt werden.

Hybride Netzwerke brauchen eine Netzwerk-Firewall, die für das digitale Zeitalter entwickelt wurde

Hybride Netzwerke erfordern eine NGFW, die vom Design her selbst in stark dezentralen und dynamischen Umgebungen eine einheitliche Security, Transparenz und Kontrolle gewährleistet. Unternehmen sollten eine Lösung wählen, die an jedem Netzwerk-Rand eingesetzt werden kann und in verschiedenen Formfaktoren erhältlich ist. Auch sollte die Firewall nahtlos in das Netzwerk integrierbar sein, eine konsequente, einheitliche Durchsetzung von Richtlinien bieten, Bedrohungsinformationen in Echtzeit austauschen und Reaktionen auf Bedrohungen koordinieren können. Denn nur ein solches „Komplettpaket“ schafft die Voraussetzungen, dass Sicherheitsrichtlinien konsequent und von Ende zu Ende für Anwendungen und Workflows durchsetzbar sind. Für Unternehmen bietet eine solche NGFW entscheidende Vorteile: umfassende Transparenz und Kontrolle über sich ständig verändernde Netzwerke mit einer ausgezeichneten Benutzererfahrung, während gleichzeitig Remote-Arbeitsplätze, Homeoffices und mobile Mitarbeiter optimal geschützt sind.

[1] Gartner: „Forecast Analysis: Remote and Hybrid Workers, Worldwide“. Ranjit Atwal, et al., 2. Juni 2021 (Seite 1).

[2] Kim Samra: „IBM Study: Security Response Planning on the Rise, But Containing Attacks Remains an Issue“. IBM, 30. Juni 2020.

[3] Gartner: „How the Shift From Firewall Appliances to Hybrid Cloud Firewalling Will Change Selection Criteria“. Aaron McQuaid, 10. März 2021 (Seite 1).

[4] Ebd. (Seite 5)

[5] Ebd. (Seite 5)

[6] Ebd. (Seite 11)

25. August 2021, 18:14 Uhr
745599-A-0-DE