STORMSHIELD

MEINUNGEN

FIREWALL FÜR UNTERNEHMEN: ZURÜCK ZU DEN WURZELN

Stéphane Prevost
Product Marketing Manager, Stormshield

Die Bedeutung von Firewall für Unternehmen ist heute unbestritten. Doch Edge-Firewalls reichen nicht länger aus, um der Raffinesse moderner Bedrohungen entgegenzutreten. Wie kann man in einem sich ständig verändernden Umfeld eine Firewall in eine Netzwerkarchitektur integrieren? Wie kann man sie am besten nutzen?

Platzierung einer Firewall, Netzwerksegmentierung, Zero-Trust-Ansatz, zentrale Steuerung und Überwachung; alles über den optimalen Einsatz einer Firewall in Ihrer Netzwerkarchitektur.

BEDARFSANALYSE UND UNTERSUCHUNG DES ZU SCHÜTZENDEN PERIMETERS

Die Firewall ist eine der Säulen der Perimetersicherheit von Unternehmen. Die ursprünglich als undurchdringliche Mauer rund um das Netzwerk konzipierte Technologie hat sich seither weitgehend gewandelt. Um auf die sich verändernde Bedrohungslage zu reagieren und alle Versuche einer – bei Malware beliebten – lateralen Verbreitung abzuwehren, mussten Systemadministratoren den Einsatz von Firewalls überdenken und neue Schutzebenen hinzufügen.

Denn die richtige Platzierung einer Firewall innerhalb einer Netzwerkarchitektur richtet sich nach dem jeweiligen Sicherheitsbedarf. Die traditionelle Firewall an der Außengrenze eines Netzwerks ist zwar nach wie vor ein unverzichtbarer Bestandteil des Sicherheitsarsenals, sie reicht jedoch nicht mehr aus, um ein gutes Sicherheitsniveau zu erreichen. Die Weiterentwicklung der Arbeitswelt („digitale Nomaden/Nomadinnen", Telearbeit, SaaS und andere Cloud-Infrastrukturen) in Verbindung mit der Raffinesse von Cyberbedrohungen zwingt Unternehmen dazu, den Einsatz von Firewalls auszuweiten: Heute müssen sie einen Schritt weiter gehen und Firewalls an verschiedenen Stellen ihres Sicherheitsperimeters einsetzen. Dieser Sicherheitsperimeter entwickelt sich jedoch weiter und besteht aus heterogenen Elementen, sowohl intern als auch extern.

Doch **was sind strategisch sinnvolle Standorte für eine Firewall?** Am Übergang zum Internet, an der Außengrenze oder im Kern eines Netzwerks, in der Cloud…? Die Möglichkeiten sind vielfältig und hängen von Ihren individuellen Sicherheitszielen sowie von den Funktionen Ihrer Firewalls ab. Gemäß dem Prinzip der tiefen Verteidigung ist es ratsam, mindestens zwei Firewalls zu implementieren, um eine vertrauenswürdige Zone (DMZ, *entmilitarisierte Zone*) einzurichten. Eine doppelte Barriere, die einen zusätzlichen Schutzschild auf der Ebene der (potenziell schädlichen) Datenströme ermöglicht. Das Ziel besteht darin, mehrere Vertrauensebenen aufzubauen: vom Internet über das LAN bis hin zu Rechenzentren und anderen Cloud-Umgebungen.

Und die Firewalls der nächsten Generation (NGFW) ermöglichen es, die Sicherheit von Netzwerkarchitekturen noch weiter zu erhöhen, insbesondere durch Netzwerksegmentierung und den *Zero-Trust-Ansatz*. Erläuterungen.

DIE BEDEUTUNG DER NETZWERKSEGMENTIERUNG UND VON *ZERO TRUST*

Weshalb ist die Segmentierung von Netzwerken so wichtig? Weil die Vorgehensweise von Cyberkriminellen eine Erkundungs- oder Aufklärungsphase einschließt. Nachdem sie in einen Computer eingedrungen und diesen infiltriert haben, scannen sie die an das Netzwerk angeschlossenen Geräte, um sich auf eine mögliche Gegenwehr vorzubereiten. Um das weitere Vorrücken der Eindringlinge zu verhindern, müssen das Haupt- sowie die Unternetzwerke streng segmentiert werden. Durch die Unterteilung in separate Zonen können Administratoren eine strenge Kontrolle auf der Zugangsebene sowie auf der Ebene der Datenströme durchsetzen.

Die Einrichtung einer vertrauenswürdigen Zone, von der oben die Rede war, ist ein „*Sonderfall der Segmentierung*“, so **Simon Dansette,** Product Manager bei Stormshield. „*Sie hat den Vorteil, dass das Netzwerk für einen bestimmten Bedarf unterteilt werden kann, indem alle lateralen Bewegungen blockiert werden*.“ Und wie **Sébastien Viou,** Direktor für Cybersicherheit und Produktmanagement bei Stormshield, in Erinnerung ruft, „*ist die Protokollunterbrechung ein Prinzip, das darauf abzielt, alle Netzwerk-, Transport- und Anwendungsströme durch ihre Interpretation und Umschreibung zu stören. Im Wesentlichen muss es unmöglich sein, ein direktes Routing zwischen den beiden Firewalls durchzuführen*.“ Das Prinzip der doppelten Barriere besteht also nicht darin, mehrere Firewalls „*aufzustapeln, in der Hoffnung, dass eine Firewall die Schwachstellen der anderen blockiert*“, sondern „*vertrauenswürdige Zonen zu schaffen, einheitliche Sicherheitsregeln anzuwenden und gleichzeitig den darin stattfindenden Austausch zu kontrollieren*“. In sensiblen Industrieumgebungen ermöglicht diese Netzwerksegmentierung mehrere Maßnahmen: Einerseits isoliert sie IT- und OT-Umgebungen und stoppt so die laterale Verbreitung von Ransomware, die eine IT-Infrastruktur infiziert hat und versucht, sich in Produktionsumgebungen breit zu machen. Andererseits kann diese Segmentierung bis ins Herz der OT, also in die Nähe der Maschinen und Automaten, hinreichen, wobei eine granulare Filterung der Datenströme angewandt wird, die selbst die gesendeten Befehle abdecken kann.

Um die Legitimität der Benutzer und Maschinen, die sich mit Netzwerken verbinden, sicherzustellen, können Unternehmen ergänzend das sogenannte *Zero-Trust-Konzept* anwenden. **Die *Zero-Trust*-Philosophie beruht auf dem Prinzip, dass Benutzer und Netzwerkkomponenten nicht standardmäßig als vertrauenswürdig eingestuft werden, sondern bei jeder Anfrage nach Zugriff auf Ressourcen ihre Identität und Legitimität nachweisen müssen.** So bezieht die *Zero-Trust-Network-Access*-Architektur (ZTNA) sowohl Benutzer als auch Geräte in die Authentifizierung und Autorisierung des Netzwerkzugriffs ein. Der Zugriff erfolgt also granular und ist spezifisch auf die Anforderungen des Benutzers zugeschnitten. „*In einer Zero-Trust-Architektur muss die Firewall zunächst mit starken Authentifizierungstechnologien integriert werden, um den Benutzer zu identifizieren. Aber sie muss auch prüfen, ob die zu authentifizierende Workstation gesund ist*“, erklärt Simon Dansette. Dank dieser Philosophie bieten die neuesten Firewall-Modelle eine Benutzerzugriffskontrolle, anstatt nur nach IPs zu filtern (wie es bei traditionellen Firewalls der Fall ist). Die Regeln zur Filterung des Daten-Traffics ermöglichen dann granulare Sicherheitsrichtlinien in Echtzeit. Simon Dansette meint: „*Lösungen wie EDR und Firewalls interagieren heute miteinander, damit Benutzer sich anmelden können. Diese Mechanismen ermöglichen es, den Authentifizierungsprozess weiterzuentwickeln.*“ Die Firewall der nächsten Generation wird somit zu einem Schlüsselelement der *Zero Trust-Architektur*.

Die Anwendung spezifischer oder gemeinsamer Regeln, die Aktualisierung von Geräten, das (physische oder virtuelle) Monitoring und die Überwachung sowie die Vervielfachung der Firewalls in den Unternehmen zwingt Systemadministratoren dazu, ihre Art der Verwaltung zu überdenken und von einer einheitlichen zu einer zentralisierten Steuerung überzugehen. Ein Tool, das heute unverzichtbar ist.

DIE NOTWENDIGE ZENTRALE STEUERUNG VON FIREWALLS

Ob an der Außengrenze oder im Kern eines Netzwerks, vor Ort in Industrieanlagen oder in der Cloud: Die Anzahl der Firewalls und ihre Platzierungen haben sich derart vervielfacht, dass ihre Verwaltung schnell zu einer komplexen Aufgabe werden kann. Bereitstellung, Konfiguration, Wartung, Patchmanagement… Laut Simon Dansette ermöglicht es eine zentrale Steuerung, „*die Komplexität der Verwaltung von verschiedenen Firewall-Verbindungen zu reduzieren sowie den Zeitaufwand für die Netzwerkadministration und somit die inhärenten Kosten zu senken*".

Die zentrale Verwaltung vereinfacht auch die Durchsetzung von Sicherheitsstandards, indem sie sicherstellt, dass alle Sicherheitsrichtlinien einheitlich auf alle Firewalls im Netzwerk angewendet werden. Für MSSPs und IT-Wiederverkäufer erweist sie sich als vorteilhaft, denn **die zentrale Verwaltung ermöglicht es, die Konfiguration mehrerer Firewalls in einem einzigen Tool vorzunehmen und sie über eine einzige Plattform** verwalten zu können. Änderungen erfolgen einfach und schnell, was mehr Sicherheit für ihre Kunden sowie eine Produktivitätssteigerung für ihre Teams bedeutet.

Die Zentralisierung der Protokollverwaltung ermöglicht auch die Visualisierung von Kennzahlen in einer einzigen Übersicht. was die Überwachung und das Reporting vereinfacht. Wenn die Protokolle in einer einzigen Plattform gesammelt, gespeichert und archiviert werden, fällt es dem Systemadministrator leichter, Konfigurationsprobleme zu erkennen und zu beheben. Simon Dansette meint: „*Die Zentralisierung bietet einen Gesamtüberblick – diese unterstützt Unternehmen dabei, die Ursachen für Probleme zu analysieren und dann in der beanstandeten Firewall zu korrigieren. Das Troubleshooting bereitet Systemadministratoren weniger Schwierigkeiten und spart Zeit in stressigen Momenten.*"

Und was ist morgen? Es lässt sich beobachten, dass nicht nur Netzwerkschutzpunkte, sondern auch Schutzpunkte für Endgeräte in Unternehmen steigen. Dennoch zeigt der wiederholte Erfolg von Cyberangriffen auch, wie wenig effektiv dieser Ansatz ist. Denn die Vielzahl an Erkennungslösungen führt zu zahlreichen und vielfältigen Ereignissen mit Verhaltensweisen, die für Administratoren schwer zu interpretieren und zu korrelieren sind. Ein Mangel an Sichtbarkeit, der die Reaktionsfähigkeit einschränkt und sich in der Praxis in einem niedrigeren Schutzniveau äußert. Um darauf zu reagieren und ein umfassenderes Management zu ermöglichen, wurden XDR-Angebote (*eXtended Detection & Response*) entwickelt. Ein dreifaches Versprechen: Risiken verringern, die von den verschiedenen Cybersicherheitslösungen gemeldeten Ereignisse korrelieren und die Cyber-Betriebsproduktivität von Unternehmen verbessern.

STORMSHIELD

Stormshield, eine hundertprozentige Tochtergesellschaft von Airbus CyberSecurity, bietet innovative End-to-End-Sicherheitslösungen zum Schutz von Netzwerken (Stormshield Network Security), Desktops (Stormshield Endpoint Security) und Daten (Stormshield Data Security). **www.stormshield.com**