DAS VERBORGENE RISIKO MODERNER FIREWALLS

So verhindern Sie, dass Schwachstellen in Ihrer Firewall bei einem Angriff ausgenutzt werden

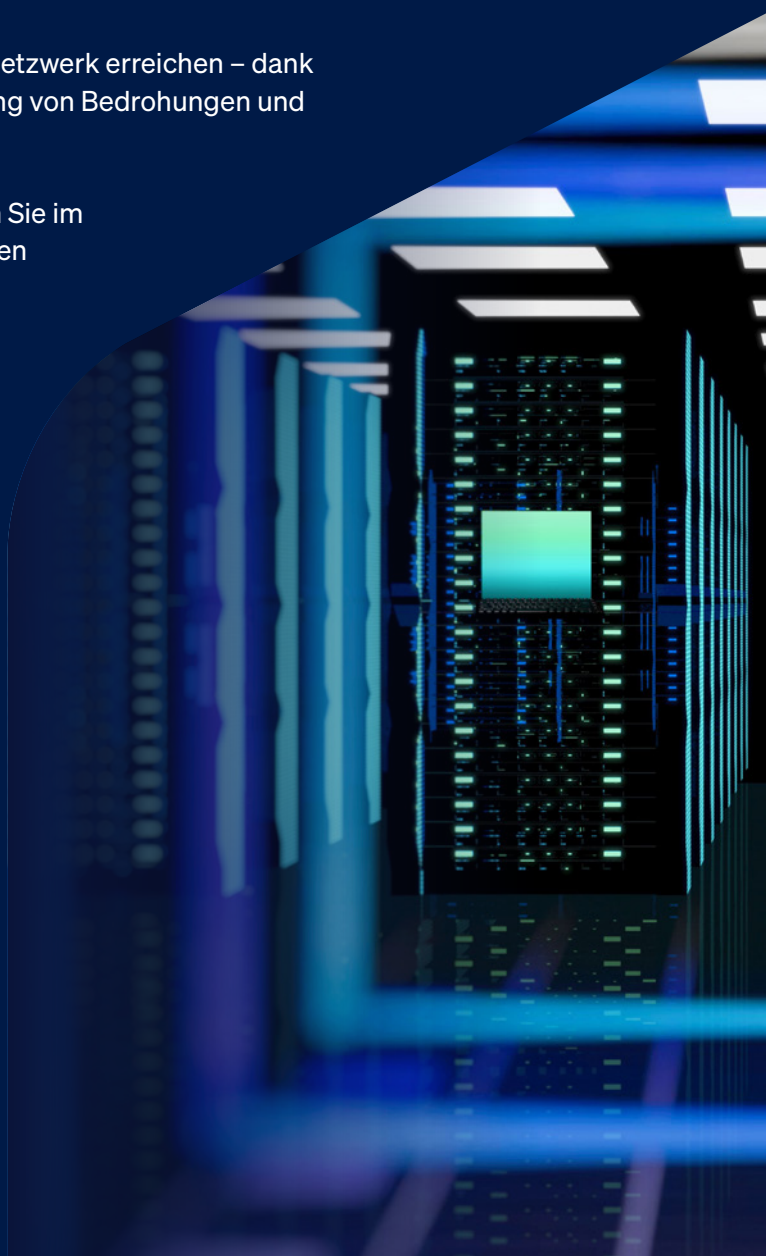
Kurzfassung

Netzwerk-Firewalls sind in einem noch nie dagewesenen Ausmaß gezielten Angriffen ausgesetzt. Fast täglich sehen wir Schlagzeilen über eine ausgenutzte neue Sicherheitslücke in einer Firewall. Dies offenbart eine beunruhigende Tatsache: Firewalls – also genau jene Systeme, die zum Schutz von Netzwerken entwickelt wurden – stellen ein erhebliches Risiko dar und sind zu bevorzugten Zielen für komplexe Angriffe geworden[1]. Diese Angriffe nutzen nicht nur Schwachstellen in der Firewall-Software selbst aus, sondern auch grundlegende Mängel im unternehmensweiten Umgang mit Netzwerksicherheit.

Dieses Whitepaper stellt ein umfassendes, auf drei Säulen basierendes Rahmenkonzept für moderne Netzwerksicherheit vor, mit dem Bedrohungen vor, während und nach der Netzwerkbereitstellung bekämpft werden können:

- **Härtung:** Reduzieren Sie Ihre Angriffsfläche proaktiv durch „Secure by Design"-Prinzipien, automatisierte Patches, Konfigurationsprüfungen und Zero Trust-Access Controls.
- **Schutz:** Blockieren Sie Bedrohungen, bevor sie das Netzwerk erreichen – dank fortschrittlicher Überprüfung, KI-gestützter Erkennung von Bedrohungen und leistungsstarker Sicherheit ohne Kompromisse.
- **Erkennung und Reaktion:** Identifizieren und isolieren Sie im Netzwerk aktive Angreifer automatisch, bevor sie einen Angriff abschließen können.

Die meisten Netzwerksicherheitslösungen konzentrieren sich in erster Linie auf den Schutz, wodurch die Netzwerkinfrastruktur anfällig bleibt. Sie kann einen aktiven Angriff nicht erkennen und dementsprechend auch nicht darauf reagieren. Dieses Whitepaper bietet Netzwerksicherheitsexperten und IT-Teams einen praktischen Leitfaden für die effektive Umsetzung aller drei Säulen.



Die aktuelle Bedrohungslage

Firewalls stehen unter Beschuss

Netzwerk-Firewalls befinden sich an der Grenze zwischen vertrauenswürdigen internen Netzwerken und der von Angriffen geprägten Außenwelt. Dadurch werden sie zu besonders beliebten Zielen. Die Schlagzeilen berichten von einer stetigen Flut von Angriffen auf große Firewall-Anbieter – einige nutzen dabei bereits bekannte Sicherheitslücken aus, die in Produktionsumgebungen nach wie vor nicht gepatcht sind, andere zielen auf suboptimale Standardkonfigurationen oder Konstruktionsfehler ab, die leicht auszunutzende Schwachstellen schaffen[2].

Frontier AI hat die Debatte um Cyberangriffe, die auf agentischer KI beruhen, weiter angeheizt. Das Modell „Claude Mythos“ von Anthropic hat innerhalb weniger Wochen über 2.000 neue Zero-Day-Schwachstellen aufgedeckt, was sowohl für Angreifer als auch für Abwehrteams einen entscheidenden Wendepunkt einläutet.

Während sich die Schlagzeilen rund um Frontier AI darauf konzentrieren, dass KI Sicherheitslücken in großem Umfang aufspürt, ist viel wichtiger, dass KI die Reaktionszeit verkürzt – und damit das Zeitfenster zwischen der Aufdeckung einer Sicherheitslücke und dem Business Impact verringert. Dadurch können Angreifer schneller, in größerem Umfang und mit weniger Hindernissen vorgehen als zuvor.

Die Folgen reichen weit über einzelne Unternehmen hinaus. Wenn Angreifer eine Firewall kompromittieren, verschaffen sie sich nicht nur direkten Zugriff auf das Netzwerk, sondern potenziell auch auf Zugangsdaten sowie auf die Lieferanten und Kunden des Unternehmens – und erhalten so praktisch die Schlüssel zum Unternehmens-Ökosystem.

Über 2.000

Zero-Day-Schwachstellen, die Mythos in nur sieben Wochen entdeckt hat

Die drei Säulen der Netzwerksicherheit

Wirksame Netzwerksicherheit erfordert einen ganzheitlichen Ansatz, der Bedrohungen über ihren gesamten Lebenszyklus hinweg berücksichtigt: vor, während und nach der Netzwerkbereitstellung. Dadurch entstehen drei eigenständige, aber miteinander verbundene Abwehrsäulen:

HÄRTUNG

ANGRIFFSFLÄCHE REDUZIEREN

Implementieren und verwalten Sie Lösungen, die gezielt Risiken minimieren, die Angriffsfläche reduzieren und Ihre Infrastruktur gegen Angriffe härten

SCHUTZ

ANGRIFFE BLOCKIEREN, BEVOR SIE INS NETZWERK GELANGEN

Nutzen Sie bestmöglichen Schutz, um Angreifer und Exploits zu erkennen und deren Eindringen ins Netzwerk zu verhindern

ERKENNUNG UND REAKTION

AKTIVE ANGRIFFE SOFORT STOPPEN

Identifizieren und isolieren Sie aktive Angreifer mit automatischen Erkennungs- und Reaktionsmaßnahmen

Die entscheidende Lücke

Die meisten Netzwerk-Firewalls konzentrieren sich fast ausschließlich auf den Echtzeit-Schutz durch Datenverkehrsfilter, Bedrohungsabwehr und Intrusion Prevention Systems. Diese Funktionen sind zweifelsfrei unverzichtbar. Unternehmen sind jedoch anfälliger, wenn sie sich ausschließlich auf die Echtzeit-Traffic-Überwachung konzentrieren.

Die täglichen Schlagzeilen zeigen, dass es den meisten Firewalls und IT-Teams nicht gelingt, ihre Umgebung wirksam zu härten, d. h. die Angriffsfläche zu verringern. Firewalls bleiben anfällig, „Patch-Müdigkeit“ ist weit verbreitet, End-of-Life-Produkte werden weiterhin an wichtiger Stelle eingesetzt, und Remote Access VPN dominiert trotz seiner Sicherheitsmängel nach wie vor. Gleichzeitig fehlen in den meisten Firewall-Bereitstellungen die Funktionen zur Erkennung und Abwehr häufig gänzlich. Diese dienen dazu, aktive Angriffe zu stoppen, bevor sie Auswirkungen haben können.

Um dieses Ungleichgewicht zu beheben, muss der Fokus bewusst auf die vernachlässigten Säulen gerichtet werden, insbesondere auf die Härtung, die das Fundament eines resilientem Sicherheitsstatus bildet.

Härtung der Netzwerkinfrastruktur – Risikominderung

Bei der Härtung geht es darum, die Angriffsfläche proaktiv zu verringern und Schwachstellen zu beseitigen, bevor Angreifer diese aufdecken und ausnutzen können.

Wesentliche Strategien zur Härtung

1. **Risiken minimieren:** Überprüfen Sie regelmäßig Systeme und Infrastrukturen, die mit dem Internet verbunden sind, und reduzieren Sie so die Anzahl potenzieller Angriffspunkte.

2. **Sorgen Sie dafür, dass Systeme „Secure by Design“ sind:** Wählen Sie Produkte, b ei deren Entwicklung Sicherheit im Vordergrund stand.

3. **Prüfen Sie Konfigurationen und halten Sie Software/Firmware auf dem neuesten Stand:** Sorgen Sie durch kontinuierliches Monitoring für die Einhaltung von Sicherheitsvorgaben.

4. **Beseitigen Sie kompromittierte Identitäten als Angriffsvektor:** Sichern Sie den Zugriff und die Authentifizierung. Setzen Sie die Multi-Faktor-Authentifizierung (MFA) unternehmensweit ein und stellen Sie von VPN auf Zero Trust Network Access (ZTNA) um.

Risiken minimieren

Überprüfen Sie regelmäßig Ihre Netzwerkinfrastruktur und ermitteln Sie, in welcher Phase des Lebenszyklus sich die einzelnen Komponenten befinden. Sollte sich eine davon dem End-of-Life nähern, muss sie proaktiv ausgetauscht werden. Die Kosten für die Erneuerung veralteter Technologie sind weitaus geringer als die potenziellen Folgen eines Ransomware-Angriffs, der nicht mehr unterstützte Systeme ausnutzt.

Dies ist auch eine gute Gelegenheit, Ihre Netzwerkinfrastruktur zu vereinfachen und zu konsolidieren. Wenn Sie für Firewall, VPN, ZTNA, SD-WAN, DNS und Webfilterung auf separate Geräte zurückgreifen, sollten Sie diese Funktionen möglicherweise auf einer einzigen Plattform zusammenfassen. Wenn sich weniger Geräte und Lösungen in Ihrer Umgebung befinden, reduzieren Sie die Komplexität, steigern die Effizienz und verbessern die allgemeine Resilienz.

Ebenso wichtig ist es, Ihre Infrastruktur auf dem neuesten Stand zu halten. Firmware- und Software-Updates enthalten häufig wichtige Sicherheitspatches für Schwachstellen, die Angreifer ausnutzen könnten. Auch wenn deren Anwendung Zeit in Anspruch nimmt, ist dies weitaus weniger disruptiv als die Folgen eines Ransomware-Angriffs und deren Bereinigung.

Systeme, die „Secure by Design“ sind

Unternehmen benötigen sichere Produkte ebenso sehr wie Sicherheitsprodukte.

Die Cybersecurity-Branche muss sich einer grundlegenden Tatsache stellen: Unternehmen benötigen sichere Produkte ebenso sehr wie Sicherheitsprodukte. Wenn Angreifer es auf Tools abgesehen haben, die zur Abwehr entwickelt wurden, benötigen Unternehmen Sicherheitsprodukte, die selbst sicher sind. Unternehmen sollten auf Anbieter setzen, die einen echten Fokus auf Sicherheit und Transparenz nachweisen – einschließlich der transparenten Offenlegung von Sicherheitsverletzungen. Dies mag zwar für alle Seiten unangenehm sein, ist aber das richtige Vorgehen.

Zu den wichtigsten Grundsätzen von „Secure by Design“ gehören:

- Standardmäßige Integration von MFA in alle Systeme
- Beseitigung von Standardpasswörtern und -Zugangsdaten
- Implementierung automatisierter Sicherheitspatches, die Betriebsunterbrechungen auf ein Minimum reduzieren
- Schnelle und transparente Verfahren zur Offenlegung von Schwachstellen
- Regelmäßige Sicherheitsaudits und Penetrationstests
- In die Produktentwicklung integrierte Verfahren für einen sicheren Entwicklungszyklus

Konfiguration prüfen und Systeme auf dem neuesten Stand halten

Netzwerk-Firewalls sind komplex, was sie anfällig für Fehlkonfigurationen und riskante Einstellungen macht, die unbeabsichtigte Einfallstore für Angreifer schaffen. Die Herausforderung besteht darin, zu erkennen, was falsch konfiguriert ist und wo diese Sicherheitslücken bestehen. Manchmal ist das Problem offensichtlich, doch häufiger bleiben die Schwachstellen verborgen, bis sie ausgenutzt werden. Die meisten Firewalls bieten keinerlei Einblicke in riskante Konfigurationseinstellungen. Besorgen Sie sich ein Produkt, das Ihnen dies bietet.

Die „Patch-Müdigkeit“ ist ein echtes Problem, muss aber nicht sein. Herkömmliche Patching-Verfahren verursachen einen erheblichen operativen Aufwand. Schwachstellen können jederzeit aufgedeckt werden, und dank künstlicher Intelligenz geschieht dies mittlerweile in alarmierendem Tempo. Die Häufigkeit, mit der Updates durchgeführt werden müssen, kann Administratorteams schnell überfordern. Die meisten Firewalls werben mit „automatischen Updates“, doch in der Regel müssen Administratoren dafür weiterhin Ausfallzeiten einplanen, Firmware installieren und die Geräte neu starten.

Unternehmen sollten sich eine einfache Frage stellen: Warum können Updates nicht wirklich automatisch erfolgen? Die Antwort lautet, dass die meisten Anbieter ihre Software nicht so konzipiert haben, dass sie Over-the-Air-Sicherheitsupdates in Echtzeit unterstützt. Moderne Architekturansätze können jedoch automatisierte Hotfix-Funktionen ermöglichen, die:

- Sicherheitspatches automatisch und ohne Eingreifen eines Administrators installieren.
- Keine Ausfallzeiten oder Neustarts erfordern.
- Die Lücke zwischen den großen Updates für die Firmware schließen.
- Das Zeitfenster, in dem Sicherheitslücken bestehen, von Monaten auf Stunden oder Tage verkürzen.

Fehlerhafte Konfigurationen stellen einen weiteren häufigen Angriffspunkt dar. Komplexe Firewallregelsätze, unzureichend dokumentierte Richtlinienänderungen und im Laufe der Zeit auftretende Konfigurationsabweichungen können unbeabsichtigt Access Points offenlassen, die eigentlich gesichert sein sollten.

Die Herausforderung liegt in der Identifizierung: Woher wissen Administratoren, was falsch konfiguriert ist? Herkömmliche Firewalls bieten keinen Einblick in die Sicherheit der Konfiguration. Zu den modernen Ansätzen gehören automatisierte Funktionen für den Health Check, die:

- Die Firewall-Konfiguration kontinuierlich anhand etablierter Best Practices und CIS-Benchmarks überprüfen.
- Über das Dashboard einen Überblick über bestandene und nicht bestandene Prüfungen bieten.
- Jedem bewerteten Punkt einen Schweregrad zuweisen.
- Die Detailansicht aktivieren, um Einstellungen schnell anzupassen oder beabsichtigte Ausnahmen zu dokumentieren.

Diese Funktionen bieten eine Transparenz, die herkömmlichen Firewalls fehlt, und gewährleisten, dass der Sicherheitsstatus auch dann optimal bleibt, wenn sich die Konfigurationen im Laufe der Zeit ändern.

Beseitigung kompromittierter Identitäten als Angriffsvektor

67 % der von Sophos im Jahr 2025 analysierten Vorfälle gingen auf kompromittierte Zugangsdaten zurück[3], weshalb die Abwehr identitätsbasierter Angriffe eine zentrale Priorität bei der Härtung darstellt. Dies erfordert die Umsetzung der Zero-Trust-Prinzipien: nichts und niemandem vertrauen, alles überprüfen.

Unternehmen, die nach wie vor auf Remote Access VPN setzen, sollten die Abkehr von dieser Lösung als vorrangige Priorität betrachten. ZTNA bietet eine moderne Alternative zu VPN, die den Zero-Trust-Prinzipien entspricht. Anstatt einen pauschalen Netzwerkzugriff zu gewähren, bietet ZTNA granularen Zugriff auf bestimmte Anwendungen und Ressourcen. Sollte ein Gerät kompromittiert werden, kann ZTNA den Zugriff automatisch einschränken oder sperren, bis die Bereinigung des Geräts abgeschlossen ist.

Selbst wenn ein Angreifer ein über ZTNA verbundenes Gerät kompromittiert, erhält er nur Zugriff auf die spezifischen Anwendungen, für die der jeweilige Benutzer berechtigt ist – nicht auf das gesamte Netzwerk. Der Sicherheitsperimeter verschiebt sich dorthin, wo er tatsächlich benötigt wird: in geschäftskritischen Anwendungen und Daten.

67 %

der Vorfälle, die Sophos im Jahr 2025 analysierte, gingen auf eine kompromittierte Identität zurück

ZTNA bietet gegenüber VPN sechs wesentliche Vorteile:

1. **MFA-Durchsetzung:** Für jeden Zugriff ist ausnahmslos MFA erforderlich, wodurch kompromittierte Zugangsdaten und Brute-Force-Angriffe als mögliche Angriffsvektoren ausgeschlossen werden.

2. **Gerätestatus – Teil der Zugriffsrichtlinie:** Die Compliance und der Integritätsstatus der Geräte werden im Rahmen der Zugriffsentscheidungen kontinuierlich überprüft.

3. **Überall einsetzbar:** ZTNA funktioniert gleichermaßen gut, unabhängig davon, ob sich die Benutzer im Unternehmensnetzwerk befinden oder von unterwegs arbeiten, und bietet somit einheitliche Sicherheit unabhängig vom Standort.

4. **Transparente Konnektivität:** Moderne ZTNA-Implementierungen bieten transparente, zuverlässige Verbindungen ohne die Verbindungsprobleme, unter denen VPNs häufig leiden.

5. **Umfassender Einblick:** Unternehmen erhalten einen klaren Überblick darüber, auf welche Ressourcen Benutzer zugreifen, was eine bessere Kapazitätsplanung und Lizenzverwaltung ermöglicht.

6. **Einfachere Verwaltung:** Das Hinzufügen und Entfernen von Benutzern, die Bereitstellung neuer Anwendungen sowie die Verwaltung von Zugriffsrichtlinien sind mit ZTNA einfacher als mit einem herkömmlichen VPN.

Im Rahmen der Sicherheitsmaßnahmen müssen Remote Access VPN abgeschafft und eine Zero-Trust-Architektur mit durchgängiger MFA-Durchsetzung bereitgestellt werden.

Schutz – Abwehr von Bedrohungen am Gateway

Sorgen Sie für umfassende Schutzmaßnahmen, um Bedrohungen zu erkennen und abzuwehren, bevor sie das Netzwerk erreichen. Dazu gehören eine erweiterte TLS Inspection, die KI-gestützte Erkennung von Zero-Day-Bedrohungen sowie eine intelligente Traffic-Analyse, bei der eine hohe Leistung ohne Kompromisse bei der Sicherheit gewährleistet wird.

Moderne Sicherheitsanforderungen

- **Leistungsstarke TLS 1.3 Inspection:** Der Großteil des Web-Traffics ist mittlerweile verschlüsselt, und Angreifer verstecken Malware sowie den Command-and-Control-Traffic zunehmend in verschlüsselten Kanälen. Firewalls müssen den TLS-Traffic intelligent entschlüsseln und prüfen und dabei richtlinienbasierte Regeln anwenden, die Sicherheitsanforderungen mit Datenschutzaspekten und den Auswirkungen auf die Performance in Einklang bringen.

- **Hardware-Beschleunigung:** Kryptografische Vorgänge und die Überprüfung des Traffics erfordern viel Rechenleistung. In modernen Firewall-Architekturen sollten Hardware-Beschleunigungsprozesse für vertrauenswürdige Anwendungen und Verschlüsselungsvorgänge eingesetzt werden. So werden Ressourcen für die eingehende Überprüfung von nicht vertrauenswürdigem Traffic frei.

- **KI-gestützter Schutz vor Zero-Day-Bedrohungen:** Die kennungsbasierte Erkennung ist nach wie vor wichtig, reicht jedoch gegen neue Bedrohungen nicht aus. Eine KI-gestützte Analyse statischer Dateien in Kombination mit dynamischem Sandboxing zur Laufzeit kann Zero-Day-Bedrohungen erkennen und blockieren, bevor sie das Netzwerk erreichen – Bedrohungen, die herkömmliche kennungsbasierte Systeme gänzlich übersehen würden.

Die Schutzfunktionen UND die Performance sollten sich im Laufe der Zeit verbessern – nicht nachlassen. Firewalls, die auf programmierbaren Architekturen basieren, erhalten durch Software-Updates sowohl Sicherheits- als auch Performance-Verbesserungen, wodurch Kunden länger von ihren Hardware-Investitionen profitieren. Im Gegensatz zu herkömmlichen Firewalls, die mit jeder neuen Sicherheitsfunktion langsamer werden, behalten moderne Architekturen ihre Performance durch kontinuierliche Optimierung bei oder steigern sie sogar.

Erkennung und Reaktion – Aktive Angriffe abwehren

Wenn Angreifer Abwehrmaßnahmen durchbrechen, werden sie umgehend aufgespürt und die Bedrohung automatisch eingedämmt. Durch Network Detection and Response (NDR) in Verbindung mit produktübergreifender Koordination können kompromittierte Systeme identifiziert und isoliert werden, bevor Angreifer ihre Ziele erreichen.

Network Detection and Response (NDR)

Network Detection and Response nutzt KI und Verhaltensanalysen, um aktive Angreifer zu identifizieren, die sich bereits im Netzwerk befinden. Im Gegensatz zu Perimeter-Sicherheitslösungen, die eingehenden Traffic analysieren, untersucht NDR die Muster des internen Netzwerk-Traffics auf Anzeichen für Komprimittierungen:

- Ungewöhnliche laterale Bewegungen zwischen den Systemen
- Command-and-Control-Kommunikation mit verdächtigen externen Hosts
- Ungewöhnliche Datenzugriffsmuster
- Versuche zur Rechteausweitung
- Auskundschaftungsmaßnahmen zur Überprüfung interner Ressourcen

NDR war bislang eine Funktion der Enterprise-Klasse, die separate Produkte und erhebliche Investitionen erforderte. Zukunftsorientierte Unternehmen integrieren NDR-Funktionen mittlerweile direkt in ihre Firewall-Plattformen und machen diese wichtige Funktion damit auch mittelständischen Unternehmen zugänglich.

Automatisierte Reaktion

Bei einer Erkennung ohne Gegenmaßnahmen werden die Administratoren lediglich darüber informiert, dass ihre Systeme kompromittiert wurden – oft zu spät, um Schaden abzuwenden. Automatisierte Reaktionsfunktionen ermöglichen eine sofortige Eindämmung.

Wenn irgendwo in der Sicherheitsinfrastruktur eine Bedrohung erkannt wird – sei es durch die Firewall, den Endpoint-Schutz, die E-Mail-Sicherheit oder einen MDR-Analysten –, benötigen Sie eine Sicherheitslösung, die eine automatisierte Reaktion über alle integrierten Sicherheitsprodukte hinweg koordiniert. Dadurch kann verhindert werden, dass ein kompromittiertes Gerät mit anderen Systemen kommuniziert. Der Zugriff auf Anwendungen und Daten wird gesperrt und laterale Bewegungen werden verhindert.

Diese automatisierte Reaktion ist besonders außerhalb der Geschäftszeiten von großem Nutzen, da 88 % der Ransomware-Angriffe in dieser Zeit[4] durchgeführt werden. Sehen wir uns das „Freitagabend-Szenario“ an: Ein Angreifer verschafft sich am späten Freitagabend Zugang zu einem Gerät, sobald das Sicherheitspersonal nicht mehr vor Ort ist. Ohne automatisierte Reaktion hat der Angreifer das gesamte Wochenende Zeit für laterale Bewegungen, kann seine Rechte ausweiten und Ransomware bereitstellen. Das Unternehmen entdeckt den Angriff am Montagmorgen, sobald verschlüsselte Dateien und Lösegeldforderungen auftauchen.

88%

der Ransomware-Angriffe werden außerhalb der Geschäftszeiten bereitgestellt

Dank einer automatisierten produktübergreifenden Reaktion führt die erste Kompromittierung zu einer sofortigen Isolierung. Der Angreifer befindet sich in einem Segment in Quarantäne und kann weder vorrücken noch sich bewegen. Die Sicherheitsteams kehren am Montagmorgen zu einem aktiven Alert zurück, der sich auf eine eingedämmte Bedrohung bezieht, und nicht auf einen groß angelegten Ransomware-Vorfall.

Sophos Firewall: Eine Komplettlösung

Das hier skizzierte Drei-Säulen-Modell stellt zwar bewährte Sicherheitsverfahren dar, doch für eine effektive Umsetzung bedarf es einer Infrastruktur, die alle drei Säulen unterstützt.

Sophos Firewall zeichnet sich als eine der wenigen Lösungen aus, die in allen drei Bereichen erhebliche Investitionen getätigt hat und zahlreiche Funktionen bietet, die Kunden anderswo nicht finden.

Monitoring der Systemintegrität

Die Sicherheitsteams von Sophos überwachen alle bereitgestellten Systeme kontinuierlich auf Anzeichen von Angriffen und beschleunigen so die Reaktion und Bereinigung.

Kontinuierlicher Health Check

Ermittelt risikoreiche Konfigurationen anhand von Best-Practice-Benchmarks und liefert priorisierte Empfehlungen für eine schnellere Behebung.

Automatische Hotfixes und sichere Updates

Sicherheitspatches können „Over the Air“ auf Sophos Firewall übertragen und automatisch ohne Ausfallzeiten installiert werden.

Alle Firmware-Updates sind sicher verschlüsselt und signiert, um ihre Integrität und Authentizität zu gewährleisten.

Gehärtete Systeme

Sichere, sofort einsatzbereite Bereitstellung

Integriertes MFA- und ZTNA-Gateway

Gehärtete, containerisierte Services und Portale

Ein gehärteter Kernel und eine gehärtete Steuerungsebene beseitigen ganze Kategorien von Schwachstellen

Sichere Remote-Verwaltung

Der verschlüsselte Verwaltungszugriff über Sophos Central beseitigt unnötige Sicherheitslücken in der Firewall.

Für maximalen Schutz werden alle Backups sicher in Sophos Central gespeichert und doppelt verschlüsselt.

Konzipiert für maximale Sicherheit

Sophos Firewall erfüllt die Anforderungen an die Systemhärtung durch einen umfassenden „Secure by Design“-Ansatz. Dabei wird der Aufwand beseitigt, der üblicherweise mit der Aufrechterhaltung einer sicheren Infrastruktur verbunden ist.

Automatisierte Hotfix-Funktion: Der Patch-Müdigkeit ein Ende setzen

Die einzigartige automatisierte Hotfix-Funktion von Sophos Firewall verändert das Zeitfenster, in dem Schwachstellen ausgenutzt werden können, grundlegend:

- Sicherheitspatches werden automatisch „Over the Air“ bereitgestellt, sobald Sophos sie entwickelt und validiert hat.
- Die Patches werden ohne Eingreifen eines Administrators installiert.
- Es sind keine Ausfallzeiten oder Neustarts erforderlich.
- Hotfixes schließen die Lücke zwischen größeren Firmware-Releases und gewährleisten so einen kontinuierlichen Schutz.

Dieser architektonische Vorteil verkürzt das Zeitfenster, in dem eine Schwachstelle ausgenutzt werden kann, von Monaten auf Stunden oder Tage. Sobald Sophos eine Sicherheitslücke entdeckt und behebt, sind alle Sophos Firewall-Kunden sofort geschützt – ohne dass sie darauf warten müssen, dass Administratoren Termine frei haben oder Wartungsfenster einplanen.

Kein anderer großer Firewall-Anbieter bietet eine wirklich automatisierte Sicherheitspatch-Installation ohne Ausfallzeiten an. Diese Funktion allein stellt bereits eine bahnbrechende Verbesserung im Bereich der Härtung dar.

Integritätsprüfung: Laufende Konfigurationsprüfung

Die Health Check-Funktion von Sophos Firewall bietet eine beispiellose Transparenz über die Konfiguration:

- Überprüft kontinuierlich Dutzende von Firewall-Konfigurationseinstellungen anhand von CIS-Benchmarks und Best Practices der Branche.
- Zeigt bestandene und nicht bestandene Prüfungen direkt auf dem Dashboard des Control Center an.
- Weist jedem bewerteten Punkt einen Schweregrad zu (kritisch, hoch, mittel, niedrig).
- Aktiviert die Detailansicht, um Einstellungen schnell anzupassen oder beabsichtigte Ausnahmen zu dokumentieren.
- Wird automatisch aktualisiert, sobald sich Best Practices weiterentwickeln.

Dieses proaktive Konfigurations-Monitoring stellt sicher, dass der Sicherheitsstatus auch dann optimal bleibt, wenn sich die Konfigurationen im Laufe der Zeit ändern. Administratoren erhalten umgehend Alarme über potenziell riskante Einstellungen, noch bevor Angreifer diese entdecken und ausnutzen können.

Remote Integrity Monitoring

Sophos ist das einzige Unternehmen, das seine gesamte Sophos Firewall-Installationsbasis überwacht. Dank eines integrierten Sophos Extended Detection and Response (XDR)-Sensors für Linux können wir die Systemintegrität überwachen, u. a. auf:

- Unbefugte Konfigurationsänderungen
- Regelexporte
- Manipulation von Dateien
- Versuche, Schadprogramme auszuführen

Dank dieses integrierten Sensors können die Sicherheitsteams von Sophos die gesamte Installationsbasis von Kunden proaktiv auf Anzeichen von Angriffen überwachen – eine zusätzliche Sicherheitsschicht, die derzeit kein anderer Firewall-Anbieter bietet. Bei der Erkennung von Bedrohungen kann Sophos sofort reagieren, um Kunden bei der Bereinigung zu unterstützen. Gleichzeitig werden automatisierte Hotfixes bereitgestellt, um alle anderen Kunden zu schützen.

Integrierte Multi-Faktor-Authentifizierung und Zero Trust Network Access

Sophos Firewall integriert MFA in alle administrativen Access Points und verfügt über ein integriertes ZTNA-Gateway, wodurch die Einführung und Bereitstellung von ZTNA sowie die Abkehr von anfälligen Remote Access VPNs vereinfacht werden.

Starke Performance, erstklassiger Schutz

Zwar bieten viele Anbieter leistungsstarke Schutzfunktionen an, Sophos Firewall setzt jedoch auf einen anderen Ansatz: Kunden erhalten umfassenden Schutz ohne Leistungseinbußen, die Unternehmen oft dazu zwingen, wichtige Sicherheitsfunktionen zu deaktivieren.

Xstream-FastPath-Architektur

Die programmierbare Xstream-Architektur von Sophos Firewall verwaltet den Traffic auf intelligente Weise und sorgt so sowohl für maximale Sicherheit als auch für maximale Performance. Dieser Ansatz stellt sicher, dass durch die Aktivierung umfassender Sicherheitsfunktionen – darunter TLS Inspection, Sandboxing und IPS – die Performance nicht beeinträchtigt wird. Sophos Firewall verfügt zudem über einen KI-gestützten Schutz vor Zero-Day-Bedrohungen, um die neuesten Bedrohungen zu erkennen.

Kontinuierliche Verbesserungen bei Performance und Schutz

Im Gegensatz zu herkömmlichen Firewalls, die mit jeder neuen Sicherheitsfunktion langsamer werden, ermöglicht die programmierbare Architektur von Sophos Firewall durch Software-Updates sowohl mehr Schutz **als auch** eine bessere Performance. Kunden profitieren von kontinuierlichen Verbesserungen ihrer Hardware-Investitionen, ohne dass eine Aufrüstung der Geräte erforderlich ist – Schutz und Performance, die sich im Laufe der Zeit verbessern, anstatt nachzulassen.

Einzigartige Erkennung und Reaktion

Die meisten Netzwerk-Firewalls bieten praktisch keine Funktionen zur Erkennung und Reaktion. Sobald ein Angreifer die Perimeter-Sicherheitsmaßnahmen durchbricht, haben herkömmliche Firewalls nicht die erforderlichen Mechanismen, um den Angriff zu erkennen oder darauf zu reagieren. Dies stellt eine kritische Sicherheitslücke dar, die Unternehmen für komplexe Angriffe anfällig macht.

Sophos Firewall zeichnet sich durch automatisierte Funktionen zur Erkennung und Reaktion aus.

Integrierte Network Detection and Response (NDR)

Network Detection and Response war bislang eine Funktion, die ausschließlich in großen Unternehmen zum Einsatz kam und separate Produkte sowie erhebliche Investitionen erforderte. Sophos Firewall umfasst NDR als Standardfunktion im Rahmen der allgemeinen Schutz-Subscription:

Dadurch erhalten Unternehmen jeder Größe Zugang zu einer Bedrohungserkennung der Enterprise-Klasse. So wird sichergestellt, dass Angreifer, denen das Durchbrechen der Perimeter-Sicherheitsmaßnahmen gelingt, identifiziert werden können, bevor sie ihre Ziele erreichen.

Synchronized Security: Produktübergreifende automatisierte Reaktion

Eine Erkennung ohne Gegenmaßnahmen informiert die Administratoren lediglich darüber, dass ihre Systeme kompromittiert wurden – oft zu spät, um Schaden abzuwenden. Die „Synchronized Security"-Funktion von Sophos Firewall sorgt für eine automatisierte, koordinierte Reaktion über die gesamte Sicherheitsinfrastruktur hinweg.

Wenn ein Sophos-Produkt eine Bedrohung erkennt – sei es Firewall, Endpoint Protection, Email Security, Workspace Protection oder ein MDR-Analyst –, führt Synchronized Security automatisch folgende Schritte durch:

- Verhindert, dass das kompromittierte Gerät mit anderen Systemen kommuniziert.
- Verhindert den Zugriff auf Anwendungen und Daten.
- Verhindert laterale Bewegungen im Netzwerk.
- Dämmt die Bedrohung ein, bis Sicherheitsteams die Ursache analysieren und die Bereinigung durchführen können.

Das „Freitagabend-Szenario" verdeutlicht den entscheidenden Nutzen automatisierter Reaktionen:

Ohne automatisierte Reaktion: Ein Angreifer verschafft sich am späten Freitagabend Zugang zu einem Gerät, sobald das Sicherheitspersonal nicht mehr vor Ort ist. Der Angreifer hat das gesamte Wochenende Zeit für laterale Bewegungen, kann seine Rechte ausweiten und Ransomware bereitstellen. Das Unternehmen entdeckt den Angriff am Montagmorgen, sobald verschlüsselte Dateien und Lösegeldforderungen auftauchen.

Mit Synchronized Security: Die erste Kompromittierung löst eine sofortige automatische Isolierung aus. Der Angreifer befindet sich in einem Segment in Quarantäne und kann nicht vorrücken. Die Sicherheitsteams kehren am Montagmorgen zu einem aktiven Alert zurück, der sich auf eine eingedämmte Bedrohung bezieht, und nicht auf einen groß angelegten Ransomware-Vorfall.

Diese Funktion zur automatisierten Reaktion ist besonders wertvoll für Unternehmen, bei denen Security Operations rund um die Uhr nicht möglich sind – also genau jene mittelständischen Unternehmen, die bislang von herkömmlichen NDR-Anbietern vernachlässigt wurden.

Fazit

Verringert meine Firewall das Risiko oder führt sie Risiken erst ein?

Netzwerk-Firewalls sind einem beispiellosen Angriffsdruck ausgesetzt. Schlagzeilen, die Schwachstellen bei mehreren großen Anbietern aufdecken, offenbaren eine unangenehme Wahrheit: Die Systeme, die für den Schutz von Netzwerken entwickelt wurden, sind zu bevorzugten Zielen für Angreifer geworden.

Das in diesem Whitepaper vorgestellte Drei-Säulen-Modell – Härtung, Schutz sowie Erkennung und Reaktion – bietet einen umfassenden Ansatz für Netzwerksicherheit, bei dem Bedrohungen vor, während und nach ihrem Auftreten bekämpft werden. Leider konzentrieren sich die meisten Firewall-Anbieter fast ausschließlich auf die Säule „Schutz“, wodurch kritische Lücken bei der Härtung sowie bei der Erkennung und Reaktion entstehen.

Um diesen Rahmen effektiv umzusetzen, bedarf es einer Infrastruktur, die die Anforderungen aller drei Säulen gleichermaßen erfüllt. Unternehmen sollten Anbieter von Firewalls anhand folgender Kriterien bewerten:

- **Fokus auf „Secure by Design“** mit Nachweisen für die Umsetzung, nicht nur bloße Versprechungen
- **Automatisierte Patch-Funktionen**, die Ausfallzeiten und Patch-Müdigkeit vermeiden
- **Konfigurationsprüfung**, die Einblick in den Sicherheitsstatus bietet
- **Integrierte Zero-Trust**-Funktionen, einschließlich MFA und ZTNA
- **Network Detection and Response** zur Identifizierung akuter Bedrohungen
- **Automatisierte Reaktionsfunktionen**, die Bedrohungen ohne menschliches Eingreifen eindämmen

Die Kosten für den Austausch veralteter oder unzureichender Infrastruktur sind deutlich geringer als die Kosten für die Folgen und Behebung eines Ransomware-Angriffs, bei dem bekannte Schwachstellen ausgenutzt werden. Handeln Sie jetzt, bevor Ihr Unternehmen zum Thema der nächsten Schlagzeile wird.

Sicherheit ist eine gemeinsame Verantwortung. Anbieter müssen sichere Produkte entwickeln. Unternehmen müssen diese richtig bereitstellen, sorgfältig warten und aus dem Verkehr ziehen, sobald sie das End-of-Life erreicht haben. Wenn beide Seiten ihren Verpflichtungen nachkommen, entsteht ein deutlich sichereres Ökosystem.

Die entscheidende Frage, die Sie sich stellen müssen: **Verringert meine Firewall das Risiko oder führt sie Risiken erst ein?**

Die Antwort hängt davon ab, ob Ihre Infrastruktur alle drei Säulen der modernen Netzwerksicherheit abdeckt – oder ob sie kritische Lücken aufweist, die Angreifer nur allzu gerne ausnutzen.

1, 2, 3 ,4 Active Adversary Report 2026 – Sophos

SOPHOS

Weitere Informationen zu Sophos Firewall finden Sie unter **sophos.com/firewall**

Sales DACH (Deutschland, Österreich, Schweiz)
Tel.: +49 611 58580
E-Mail: **sales@sophos.de**