paloalto NETWORKS

STRATA™
BY PALO ALTO NETWORKS

10 Dinge, die Sie bei Ihrer künftigen Next-Generation Firewall testen sollten

Die Suche nach einer neuen Firewall wirft schwierige Fragen auf: Mit welchem Cybersicherheitsprodukt können Sie die spezifischen Risiken und Chancen Ihres Unternehmens meistern? Und wie lässt sich sicherstellen, dass die Features Ihrer Next-Generation Firewall auch für künftige Herausforderungen und kommende Wachstumsphasen ausgelegt sind?

Aufschlussreiche Antworten liefert hier allein ein Praxistest.

Nicht umsonst sind sich die meisten Sicherheitsexperten darin einig, dass ein auf Enterprise-Lösungen von der Stange basierender Ansatz nicht zielführend ist, weil jedes Unternehmen eine maßgeschneiderte Sicherheitsinfrastruktur mit aufeinander abgestimmten Tools, Diensten und Funktionen benötigt, die sich flexibel an die aktuellen Anforderungen anpassen lassen und dabei stets den versprochenen Schutz bieten.

Deshalb präsentieren wir Ihnen in unserem Whitepaper zehn wichtige Features, die Sie in Ihrer bestehenden Sicherheitsinfrastruktur testen und bei der Auswahl einer Next-Generation Firewall berücksichtigen sollten. Auf dieser Grundlage können Sie im Vorfeld der Entscheidung einen abteilungsübergreifenden Dialog in Gang bringen und gezielt ermitteln, wie einfach die auf dem Markt verfügbaren Next-Generation Firewalls zu implementieren und zu betreiben sind und wie gut sie Ihr Unternehmen heute und in Zukunft schützen.

1. Verhinderung des Diebstahls von Anmeldedaten

Benutzer und ihre Anmeldedaten gehören zu den schwächsten Gliedern der Sicherheitsinfrastruktur eines Unternehmens. Dies zeigt sich unter anderem darin, dass im Verlauf der meisten Cyberangriffe Anmeldedaten gestohlen werden und dass Hackereinbrüche mit gestohlenen Anmeldedaten eine besonders hohe Erfolgsquote haben. Daher ist die effektive Prävention des Diebstahls von Anmeldedaten eine wichtige Maßnahme zur Abwehr von Cyberangriffen.

Warum ist dieses Feature erwägenswert und weshalb lohnt sich ein Test?

Wenn Sie in der Lage sind, diverse Formen des Diebstahls von Anmeldedaten effektiv zu unterbinden, können Sie beispielsweise gezielte Phishing-Angriffe abwehren, die sich üblicherweise gegen Mitarbeiter aus den nichttechnischen Unternehmensbereichen richten und diese mithilfe von in E-Mails eingebetteten Links auf schädliche Websites locken.

Modernisierungsperspektiven

Die meisten Unternehmen führen Mitarbeiterschulungen durch, um derartige Vorfälle in den Griff zu bekommen, haben damit jedoch nur mäßigen Erfolg.

Außerdem müssen die Verantwortlichen vielerorts feststellen, dass konventionelle Sicherheitslösungen mit E-Mail-Filtern und Funktionen zur Erkennung bekannter Phishing-Websites weitgehend wirkungslos bleiben, wenn die Angreifer immer neue URLs für ihre Aktivitäten nutzen und schädliche Links statt per E-Mail einfach über soziale Medien versenden. Hier kann eine Next-Generation Firewall mit auf maschinellem Lernen basierenden Analysefunktionen deutlich effektiveren Schutz bieten, sofern sie neue schädliche Websites automatisch identifiziert und ihre Sicherheitsmechanismen dann entsprechend anpasst.

Allerdings wird es auch dann noch Phishing-Websites geben, die von der Firewall als „unbekannt“ eingestuft werden. Daher ist es für den Schutz Ihres Netzwerks und Ihrer Benutzer unerlässlich, dass Sie spezielle Filterfunktionen implementieren, die die Eingabe geschäftlicher Anmeldedaten auf unbekannten Websites unterbinden.

Empfohlene Fragen für die Ausschreibung:

- Kann die Next-Generation Firewall Benutzer daran hindern, ihre geschäftlichen Anmeldedaten auf unbekannten Websites einzugeben?
- Ist dies ohne die Speicherung der Passwort-Hashwerte auf der Firewall möglich?
- Nutzt die Next-Generation Firewall maschinelles Lernen, um Phishing-Angriffe zu identifizieren und zu unterbinden und JavaScript-basierte Netzwerkbedrohungen mithilfe von Inline-Abwehrfunktionen zu stoppen?
- Wie schnell analysiert die Next-Generation Firewall bisher unbekannte Websites und wie viel Zeit vergeht zwischen der Identifizierung einer Phishing-Website und der Aktualisierung der Schutzmechanismen?
- Erfasst die Next-Generation Firewall sämtliche Versuche der Benutzer, Anmeldedaten in HTTP-POST-Anforderungen zu übermitteln?

2. Vereitelung des Missbrauchs von Anmeldedaten

Hacker können durch Phishing-, Malware-, Social-Engineering- oder Brute-Force-Angriffe sowie den Ankauf gestohlener Passwörter auf dem Schwarzmarkt in den Besitz von Anmeldedaten für geschäftliche Benutzerkonten gelangen. Das verschafft ihnen nicht nur Zugang zu dem betreffenden Unternehmen, sondern erleichtert ihnen auch die Ausbreitung in dessen Infrastruktur und die Erlangung erweiterter Zugriffsrechte für wichtige Anwendungen und Daten.

Warum ist dieses Feature erwägenswert und weshalb lohnt sich ein Test?

Die Implementierung von firewallbasierten Multi-Faktor-Authentifizierungsverfahren (MFA) hindert Angreifer daran, sich mithilfe von gestohlenen Anmeldedaten in Ihrer Infrastruktur auszubreiten. Auf diese Weise können Sie sämtliche Anwendungen und Server vor unbefugtem Zugriff schützen. Außerdem greifen die Sicherheitsmechanismen früher, da die Benutzeridentität bereits verifiziert wird, bevor die Verbindung zur gewünschten Anwendung zustande kommt.

Modernisierungsperspektiven

Viele Unternehmen haben bereits in eine MFA-Lösung investiert, mussten dann jedoch bei der Implementierung feststellen, dass die Integration dieses Kontrollmechanismus in sämtliche Apps mit großen Herausforderungen und einem beträchtlichen Zeitaufwand verbunden ist. Daher wird meist nur eine Handvoll Anwendungen auf diese Weise geschützt (wie beispielsweise VPN-Gateways oder ausgewählte Cloud-Anwendungen), während das Gros weiterhin für Unbefugte mit gestohlenen Anmeldedaten zugänglich ist.

Effektiver Schutz auf der Netzwerkebene

MFA ist ein hervorragendes Tool, das jedoch so eingerichtet werden muss, dass es alle kritischen Anwendungen abdeckt. Wenn Sie effektive MFA-Richtlinien in Ihrer Firewall implementieren, können Sie den Verkehr spezifischer Anwendungen kontrollieren, ohne deren Code modifizieren zu müssen. Dabei sollte die Firewall so konfiguriert sein, dass sämtliche Zugriffsversuche und Datenübertragungen erst nach erfolgreicher Authentifizierung gestattet werden. Auf diese Weise lässt sich verhindern, dass Angreifer die MFA umgehen, wenn sie sich Zugang zu einem unternehmensinternen Endpunkt verschafft haben.

Granulare Kontrolle

Ihre Firewall sollte die Einrichtung granularer MFA-Richtlinien unterstützen, die genau auf die spezifischen Sicherheitsanforderungen bestimmter Benutzer und Anwendungen zugeschnitten sind. Beispielsweise sollten sich Benutzer beim Zugriff auf extrem sensible Anwendungen in kürzeren Abständen authentifizieren müssen als beim Zugriff auf weniger kritische Apps.

Schneller Schutz für Ihre Anwendungen

Firewallrichtlinien bieten die Möglichkeit zur beschleunigten Implementierung von MFA-Verfahren, da hier nur die Netzwerkschutzmechanismen, nicht jedoch die Anwendungen selbst oder deren Bereitstellungsumgebungen angepasst werden müssen. Das erlaubt Ihnen die schnellere Umsetzung einschlägiger Sicherheits- und Compliance-Vorgaben und hindert Angreifer sowohl am Missbrauch gestohlener Zugangsdaten als auch an der weiteren Ausbreitung in Ihrer Infrastruktur.

Empfohlene Fragen für die Ausschreibung:

- Unterstützt die Next-Generation Firewall die Implementierung von richtlinienbasierten MFA-Verfahren, die beispielsweise die Vertraulichkeit der vom Benutzer aufgerufenen Anwendung oder Ressource berücksichtigen?
- Lassen sich die MFA-Funktionen der Next-Generation Firewall nahtlos mit verschiedenen ergänzenden Technologien integrieren?
- Wird insbesondere die MFA-Integration über RADIUS oder APIs unterstützt?
- Bietet die Next-Generation Firewall die Möglichkeit zur Erstellung von MFA-Richtlinien für alle Arten von Anwendungen, darunter Client-Server- und Terminal-Anwendungen?
- Sind die MFA-Funktionen der Next-Generation Firewall auf bestimmte Protokolle beschränkt?

3. Dynamische Sicherheitsrichtlinien für dynamische virtuelle Workloads

Wenn Sicherheitsexperten in früheren Jahren Firewall-Richtlinien für die Infrastrukturen von Rechenzentren erstellten und implementierten, gingen sie im Allgemeinen davon aus, dass sich die IP-Adressen der in diesen Umgebungen bereitgestellten Ressourcen nicht ändern würden. Dementsprechend waren ihre Richtlinien statisch und wurden flächendeckend auf einen bestimmten Bereich der Infrastruktur angewandt. Doch mit der fortschreitenden Virtualisierung der Rechenzentren wird dieser Ansatz zunehmend obsolet, da nun schwerpunktmäßig Workloads geschützt werden müssen, die nicht länger an einem bestimmten Standort gehostet oder in einer spezifischen Netzwerktopologie bereitgestellt werden.

Warum ist dieses Feature erwägenswert und weshalb lohnt sich ein Test?

Um Ihr dynamisches virtuelles Rechenzentrum effektiv zu schützen, müssen Sie Firewall-Richtlinien erstellen können, die sich auf die intrinsischen Eigenschaften der Workloads und nicht auf statische IP-Adressen beziehen. Next-Generation Firewalls ermöglichen dies durch dynamische Adressierung.

Modernisierungsperspektiven

In modernen Unternehmen werden ständig neue Workloads eingerichtet, von einer Umgebung in die andere verschoben und nach kurzer Zeit wieder aufgelöst. Das ermöglicht eine optimale Nutzung der zur Verfügung stehenden Rechenkapazitäten, erfordert jedoch zugleich die ständige Neuzuweisung von IP-Adressen. Unter diesen Umständen lassen sich Firewall-Sicherheitsrichtlinien nur dann implementieren und effektiv durchsetzen, wenn Hunderte oder gar Tausende von Adressgruppen mit jeweils eigenen Adressobjekten eingerichtet und dann dynamisch erweitert, verkleinert oder angepasst werden.

Deshalb sollte die von Ihnen gewählte Firewall die Einrichtung und automatisierte Anpassung workloadspezifischer Richtlinien zum Schutz Ihrer virtuellen Maschinen und containerisierten Anwendungen unterstützen.

Die hierfür verwendeten dynamischen Adressgruppen entkoppeln Sicherheitsrichtlinien von spezifischen IP-Adressen und verknüpfen sie stattdessen mit verschiedenen Attributen virtueller Workloads, die modernen Firewalls als sogenannte Tags dienen. Beispielsweise kann ein virtueller Anwendungsserver anhand verschiedener Workload-Attribute als „App-Server“ getaggt werden, sodass sein Datenverkehr von der Firewall unabhängig von seiner momentanen IP-Adresse erkannt wird. Dadurch werden stets die vorgesehenen Sicherheitsrichtlinien auf diesen Workload angewendet, auch wenn er in eine andere Umgebung migriert wird.

Auf diese Weise stärken workloadspezifische Sicherheitsrichtlinien den Schutz Ihres Unternehmens insgesamt. Zugleich reduziert die Nutzung dynamischer Adressgruppen den Arbeitsaufwand des für den Anwendungsbetrieb zuständigen Sicherheitsteams.

Empfohlene Fragen für die Ausschreibung:

- Wie ermöglicht die Next-Generation Firewall die Einrichtung von Sicherheitsrichtlinien, die sich auf die Eigenschaften von virtuellen Maschinen und anderen virtuellen Workloads beziehen?
- Unterstützt die Next-Generation Firewall die Erstellung von Sicherheitsrichtlinien für dynamische Workloads in Private- und Public-Cloud-Umgebungen?
- Kann die Firewall auch dann für die konsistente Durchsetzung von Sicherheitsrichtlinien sorgen, wenn sich die IP-Adressen oder Hosting-Standorte der Workloads im Rechenzentrum ändern?

4. Einfache und effektive Tools für das Firewall-Management

Um die Sicherheitsinfrastruktur schnell an neue geschäftliche Anforderungen anpassen zu können, sollten Ihre Teams in der Lage sein, Firewall-Konfigurationen sowohl vor Ort als auch über eine zentrale Konsole zu modifizieren. Falls dies nicht der Fall ist und die lokalen Administratoren nur ausgewählte Einstellungen verändern können, müssen viele Konfigurationsänderungen an globale oder in anderen Regionen beheimatete Administratorenteams delegiert werden, was wiederum Zeitverzögerungen, Sicherheitslücken, blinde Flecken und unklare Zuständigkeiten nach sich zieht.

Warum ist dieses Feature erwägenswert und weshalb lohnt sich ein Test?

Damit Konfigurationsänderungen ohne Zeitverzögerung und unter Einhaltung der Sicherheitsvorgaben Ihres Unternehmens durch mehrere Administratoren vorgenommen werden können, sollte Ihre Firewall-Managementlösung die Einrichtung rollenbasierter Zugriffskontrollen für alle Features sämtlicher Appliances unterstützen. Auf diese Weise können Sie zum einen sicherstellen, dass lokale Teams vollen Zugriff auf die an ihrem jeweiligen Standort installierten Firewalls haben, wenn diese an spezifische regionale Anforderungen angepasst werden müssen. Zum anderen erhalten globale Administratoren über das zentrale Managementtool einen umfassenden Überblick über die Aktivitäten lokaler IT-Teams und können bei Bedarf Warnmeldungen versenden oder lokale Änderungen außer Kraft setzen, wenn diese gegen Unternehmensvorgaben verstoßen.

Empfehlenswert ist also die Anschaffung von Next-Generation Firewalls, die unabhängig von ihrem jeweiligen Standort und Formfaktor über eine zentrale Konsole verwaltet werden können. Dabei sollte das betreffende Management-Tool nicht nur die Konfiguration, Durchsetzung und Verwaltung von Sicherheitsrichtlinien erleichtern, sondern auch die Logdateien der verschiedenen Firewalls zusammenführen und analysieren, um wichtige Erkenntnisse über den Netzwerk- und Sicherheitsstatus des Unternehmens bereitzustellen und schädliche Aktivitäten aufzudecken, die anderenfalls leicht übersehen werden.

Modernisierungsperspektiven

Granulare Kontrolle und effiziente Änderungsprozesse

In einer Infrastruktur mit mehreren Firewalls kommt es vor, dass verschiedene Administratoren zur selben Zeit Konfigurationsänderungen vornehmen und dass ein Administrator seine Änderungen ausführen möchte, bevor die anderen ihre Modifikationen abgeschlossen haben. Falls Ihre Firewall-Managementlösung keine selektiven Implementierungsprozesse unterstützt, besteht hier die Gefahr, dass die unvollständigen Änderungen ebenfalls implementiert werden. Dadurch können gravierende Probleme entstehen, wenn beispielsweise der Benutzerzugriff auf gesperrte Websites ermöglicht oder der Zugang zu geschäftskritischen Anwendungen blockiert wird. Erschwerend kommt hinzu, dass die halbfertigen Änderungen manuell rückgängig gemacht und korrigiert werden müssen, wenn keine selektive Zurücksetzung möglich ist. Das bedeutet zusätzlichen Arbeitsaufwand und verzögert die Optimierung der Sicherheitsinfrastruktur.

Flächendeckende Verwaltung von Logdateien

Eine zentrale Managementkonsole bietet einen umfassenden Überblick über den aktuellen Zustand der Netzwerk- und Sicherheitsinfrastruktur Ihres Unternehmens und unterstützt die Analyse sicherheitsrelevanter Ereignisse mit aussagekräftigen Kontextinformationen. Hierfür werden in vielen Fällen die Logdateien der in der IT-Umgebung installierten Firewalls erfasst und zusammengeführt. Doch wenn die Zahl der auf diese Weise pro Sekunde verarbeiteten Ereignisse die Kapazität des Managementtools übersteigt, führt das unweigerlich zu Performance-Einbußen.

Für die Benutzer macht sich dies im Allgemeinen durch das Einfrieren der grafischen Oberfläche oder in Form von Zeitüberschreitungen bei Datenbankabfragen bemerkbar. Derartige Effekte sind angesichts der rasant steigenden Durchsatzraten unserer digitalen Welt keine Seltenheit und können sogar in Umgebungen mit einer einzigen High-End-Firewall auftreten, wenn die zentrale Managementlösung zugleich für die Verwaltung der protokollierten Daten genutzt wird. Ein weitaus höheres Risiko besteht naturgemäß in Infrastrukturen, in denen mehrere Firewalls installiert wurden.

Um dieses Problem in den Griff zu bekommen, schaffen viele Unternehmen eine dedizierte Appliance für das Logdatei-Management an, die dann mit dem Firewall-Managementtool integriert wird. Dadurch müssen die Kapazitäten des Letzteren nicht länger für die Verwaltung von Logdateien verwendet werden und stehen ausschließlich für die Firewall-Administration zur Verfügung. Performance-Einbußen werden vermieden, da die auf der zentralen Managementkonsole bereitgestellten Protokolldaten überwiegend von der Appliance für das Logdatei-Management stammen, während die Rohdaten nur in Ausnahmefällen direkt von den Firewalls abgerufen werden.

Immer auf dem aktuellen Stand

Jedes der zahlreichen Features einer Next-Generation Firewall wurde speziell als Lösung für eine bestimmte Sicherheitsherausforderung wachstumsorientierter Unternehmen entwickelt. Beispielsweise erweisen sich manuelle Konfigurations- und Änderungsprozesse in einer Umgebung mit mehreren installierten Firewalls als ineffizient, risikobehaftet und inkonsistent. Hier ermöglichen Automatisierungsfunktionen eine schnellere und präzisere Reaktion auf neue Cyberbedrohungen.

Nicht umsonst verfügen die meisten Next-Generation Firewalls über Programmierschnittstellen (APIs), die automatisierte Änderungsprozesse unterstützen und dadurch das für die Netzwerksicherheit zuständige Team von aufwendigen und fehleranfälligen manuellen Abläufen entlasten. Allerdings ist dieser Ansatz nur dann erfolgversprechend, wenn die APIs so leistungsstark und flexibel sind, dass alle Firewall-Features automatisch angepasst werden können.

Empfohlene Fragen für die Ausschreibung:

- Können lokale Administratoren die Konfiguration der Appliances an ihrem Standort nach Belieben anpassen, ohne sich zuvor bei einer zentralen Managementlösung anzumelden?
- Können die für die gesamte Infrastruktur zuständigen Administratoren die durch lokale Administratoren vorgenommenen Änderungen überwachen und nachvollziehen?
- Können die Verantwortlichen bestimmen, welche Konfigurationsänderungen auf den Firewalls umgesetzt werden, wenn verschiedene Administratoren zeitgleich Modifikationen vornehmen?
- Können die Verantwortlichen die Änderungen bestimmter Benutzer rückgängig machen und eine frühere funktionierende Konfiguration wiederherstellen, falls es nach der Implementierung von Modifikationen zu Problemen kommt?
- Stellt die Lösung für die Firewall-Administration auf einer zentralen Konsole dedizierte Funktionen für die Verwaltung von Logdateien und das Konfigurationsmanagement bereit?
- Kann das Tool für das Management von Logdateien hohe Durchsatzraten (von bspw. 50.000 Ereignissen pro Sekunde) bewältigen?
- Sind sämtliche Features der Firewall über APIs zugänglich, sodass sich Konfigurationsänderungen automatisieren lassen?

5. Schnelle Bedrohungsabwehr durch automatisierten, integrierten Schutz

Aufgesetzte Punktlösungen sind längst nicht mehr zeitgemäß und führen allzu oft zu komplexen, fragmentierten Sicherheitsinfrastrukturen und -prozessen. Um diese Entwicklung frühzeitig zu unterbinden, benötigen Sie moderne Schutzmechanismen, die von Anfang an miteinander sowie in Ihre Systeme und Betriebsabläufe integriert werden. Besonders nützlich sind dabei automatisierte Abwehr- und Erkennungstools, die sich über APIs mit anderen Komponenten der Sicherheitsinfrastruktur Ihres Unternehmens verknüpfen lassen. Auf diese Weise erhalten Sie im Handumdrehen alle nötigen Kontextinformationen, um Angreifer zu stoppen, bevor sie Schaden anrichten und sensible Unternehmensdaten stehlen können.

Warum ist dieses Feature erwägenswert und weshalb lohnt sich ein Test?

APIs ermöglichen die Automatisierung von Sicherheitsprozessen, die auf dem Zusammenspiel verschiedener Appliances von unterschiedlichen Anbietern basieren. Dadurch werden die Sicherheitsteams von ebenso aufwendigen wie fehleranfälligen manuellen Abläufen entlastet und profitieren zugleich von effektiveren Schutzmechanismen. Um das Potenzial dieses Ansatzes voll ausschöpfen zu können, sollten Sie darauf achten, dass die von Ihnen gewählten Sicherheitstools und -services Warnmeldungen aus verschiedenen Quellen verarbeiten und in Kombination mit anderen integrierten Produkten automatisch die in standardisierten Playbooks festgelegten Schritte ausführen können.

Modernisierungsperspektiven

Wie aus dem Verizon Data Breach Investigation Report 2019 hervorgeht, vergehen bei einem Hackereinbruch lediglich Minuten, bis sich die Angreifer Zugriff auf die ersten Ressourcen verschaffen.[1] Deshalb benötigt Ihr Unternehmen eine moderne Sicherheitsinfrastruktur, deren Komponenten effektiv miteinander kommunizieren, um bekannte und unbekannte Bedrohungen schon im Ansatz zu identifizieren und zu stoppen. Außerdem sollten sämtliche Schritte der Erkennungs- und Abwehrprozesse automatisiert ablaufen, damit die Reaktion auf den Ernstfall so schnell wie möglich erfolgt.

Eine erste wichtige Voraussetzung hierfür sind leistungsstarke APIs, die sowohl einen reibungslosen Datenaustausch zwischen den in Ihrem Rechenzentrum installierten Sicherheitssystemen als auch die Einleitung konzertierter Gegenmaßnahmen ermöglichen. In Anbetracht dessen empfiehlt sich die Wahl eines Anbieters, dessen Produkte nachweislich mit den Lösungen diverser Partnerunternehmen kompatibel und für die API-basierte Integration zertifiziert sind. So können Sie sicher sein, dass die Schutzmechanismen für Ihr Rechenzentrum, Ihre Endpunkte und Ihre E-Mail- und WLAN-Infrastruktur stets optimal ineinandergreifen. Beispielsweise lassen sich die verschiedenen Features und Funktionen einer modernen Firewall mithilfe nativer APIs per Fernzugriff überwachen und dynamisch an Ihr spezifisches Anforderungsprofil anpassen.

1. „Data Breach Investigations Report 2019“, Verizon, Mai 2019, https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf.

Zweitens benötigen moderne Unternehmen intelligente Sicherheitstools, die verdächtige Vorgänge auf der Basis von Verhaltensanalysen erkennen und dadurch auch bisher unbekannte Bedrohungen aufdecken. Dabei sollten diese neuen Tools idealerweise zum einen als cloudbasierte Lösungen mit skalierbarer Kapazität bereitgestellt und zum anderen mit Ihren bestehenden Sicherheitssystemen integriert werden können, damit im Ernstfall in sämtlichen Cloud- und On-Premises-Umgebungen automatisch koordinierte Gegenmaßnahmen in Gang kommen. Außerdem müssen die gewählten Sicherheitslösungen in der Lage sein, Warnmeldungen aus verschiedenen Quellen zu konsolidieren, standardisierte Incident-Response-Ablaufskripte (sogenannte Playbooks) auszuführen und Sicherheitsdaten automatisch zueinander in Bezug zu setzen, um infizierte Hosts anhand ihrer schädlichen Netzwerkaktivitäten zu identifizieren.

Wird auf diese Weise eine potenzielle Infektion aufgedeckt, so ist es – drittens – von großem Vorteil, wenn in der Unternehmensinfrastruktur automatisierte Quarantäne-Prozesse implementiert sind, die die betroffenen Hosts umgehend isolieren. Das lässt sich beispielsweise mithilfe einer Richtlinie bewerkstelligen, die sämtliche von infizierten Hosts ausgehenden Netzwerkzugriffsversuche blockiert, während sie umgekehrt Analysten und Incident-Response-Teams Zugang zu den verdächtigen Geräten gewährt. Alternativ können auf allen infizierten Systemen automatisch MFA-Verfahren implementiert werden, sodass nur legitime Benutzer – nicht jedoch die Angreifer – Zugriff auf die dort verfügbaren Unternehmensdaten und -anwendungen erhalten.

Wie hier ersichtlich wird, reduzieren automatisierte Sicherheitslösungen mit leistungsstarken APIs nicht nur die Zahl der manuellen Prozesse und die zur Abwehr akuter Bedrohungen benötigte Zeit, sondern leisten außerdem einen entscheidenden Beitrag zur Eindämmung erfolgreicher Angriffe. Deshalb sollten Sie bei der Entscheidung für einen Sicherheitsanbieter unbedingt darauf achten, dass der gewählte Partner Automatisierungsfunktionen und von Haus aus integrierte APIs bereitstellt, die Ihr Sicherheitsteam entlasten und seinen Mitgliedern mehr Zeit zur Umsetzung strategischer Initiativen verschaffen. Damit senken Sie unter anderem das Risiko vermeidbarer manueller Fehler und stärken letztlich die Sicherheit Ihres gesamten Unternehmens.

Empfohlene Fragen für die Ausschreibung:

- Kann die Firewall bzw. Firewall-Managementlösung bei Erfassung eines sicherheitsrelevanten Ereignisses ein Ticket im Änderungsmanagementsystem erstellen?
- Kann die Firewall bzw. Firewall-Managementlösung einen Quarantäneprozess für infizierte mit dem WLAN verbundene Hosts auslösen?
- Lässt sich die Firewall komplett über eine API programmieren?
- Kann die Firewall über die APIs der WLAN-Controller Informationen über die mit dem Netzwerk verbundenen Benutzer und Hosts abrufen?
- Unterstützt der Sicherheitsanbieter die datengestützte automatische Erzeugung von Bedrohungssignaturen in allen Phasen eines Angriffs?
- Kann die Firewall Sicherheitsdaten aus verschiedenen Quellen abgleichen, um infizierte Hosts in Ihrem Netzwerk zu identifizieren und dann unter Quarantäne zu stellen?
- Können Sie mithilfe der Firewall Multi-Faktor-Authentifizierungsverfahren implementieren, die den Missbrauch von Anmeldedaten und unbefugte Zugriffe auf geschäftskritische Anwendungen verhindern?

6. Schutz vor getarnten und unbekannten Angriffen

Jedes Jahr werden Millionen neuer Malware-Varianten und schädlicher Websites entdeckt. Das erweist sich als Problem für konventionelle Sicherheitslösungen, die bei bisher unbekannten Bedrohungen zumeist erst greifen, wenn das Unternehmensnetzwerk bereits infiltriert wurde. Selbst wenn die Anpassung der Schutzmechanismen nach der Aufdeckung nur fünf Minuten dauert, kann sich die Infektion in dieser Zeit von einem Computer auf 10.000 Geräte ausbreiten.

Erschwerend kommt hinzu, dass viele Malware-Entwickler mittlerweile verschiedene Umgehungstechniken einsetzen und ihren Schadcode beispielsweise in legitime Dateien einbetten, in komprimierter Form an signaturbasierten Erkennungstools vorbeischleusen oder dank eingebauter Standby-Funktionen bei Sandbox-Prüfungen als harmlos erscheinen lassen. Auf diese Weise hebeln die Angreifer verschiedene gängige Analysemethoden aus, mit denen Sicherheitsteams verdächtige Aktivitäten aufdecken. Zu diesem Zweck untersuchen sie virtuelle Sandbox-Umgebungen, um einerseits Einblicke in den Code von Malware-Analysetools zu gewinnen und andererseits die zulässigen Benutzeraktivitäten, Systemkonfigurationen, typischen VM-Speichergrößen sowie Indikatoren für bestimmte Virtualisierungs- und Emulationstechnologien auszulesen.

So ist es zu erklären, dass zahlreiche aktuelle Bedrohungen gezielt die Schwachstellen der von vielen Malware-Analysetools und Hypervisoren verwendeten Open-Source-Technologien ausnutzen. Und da diese Innovationen oft im florierenden kriminellen Untergrund zum Kauf angeboten werden, können auch weniger versierte Hacker Zugang zu sofort einsatzbereiten Angriffstools mit Funktionen zur Erkennung und Umgehung von Analyseumgebungen erlangen. Deshalb sind moderne Lösungen zur Aufdeckung und Abwehr getarnter Malware heute wichtiger denn je.

Warum ist dieses Feature erwägenswert und weshalb lohnt sich ein Test?

Wenn Ihre Schutzmechanismen erst nach der Infiltration des ersten Systems greifen, wird die blitzschnelle Ausbreitung neuartiger Bedrohungen zur realen Gefahr für Ihr gesamtes Unternehmen. Einige konventionelle Lösungen verhindern dies, indem sie verdächtige Dateien zunächst zurückhalten und analysieren, beeinträchtigen dadurch jedoch sowohl die Benutzererfahrung als auch den reibungslosen Ablauf der Geschäftsprozesse.

Zudem nutzen neuere Malware-Varianten und Exploits in der Regel raffinierte Methoden zur Umgehung gängiger Netzwerksicherheitssysteme wie Firewalls und Sandbox-Lösungen. Daher ist ein optimaler Malware-Schutz nur mit Produkten zu erreichen, die derartige Umgehungs- und Tarnmechanismen erkennen und automatisch unschädlich machen können.

Modernisierungsperspektiven

Inline-Schutz gegen bisher unbekannte Bedrohungen

Da sich unbekannte Malware-Varianten mittlerweile in Minutenschnelle exponentiell ausbreiten können, ist die Eindämmung neuartiger Bedrohungen mithilfe von Offline-Analysen und periodischen Updates der Firewall-Regeln nicht länger effektiv. Stattdessen benötigen moderne Unternehmen eine Next-Generation Firewall, die auf maschinellem Lernen basierenden Inline-Schutz für sämtliche Anwendungen bereitstellt und eine Erstinfektion durch die Prävention von Phishing-Angriffen und anderen getarnten Bedrohungen verhindert, ohne dass die geschäftliche Produktivität darunter leidet.

Bare-Metal-Analysen

Eine moderne Sicherheitsplattform sollte verschiedene Verfahren zur Aufdeckung von Umgehungstechniken miteinander verknüpfen. Beispielsweise hat sich die Kombination von dynamischen Sandbox- und Bare-Metal-Analysen als besonders effektiv erwiesen, wenn es um die Identifizierung von Malware-Varianten mit der Fähigkeit zur Erkennung von Analyseumgebungen geht.

Der Grund: Bei einer Bare-Metal-Analyse werden verdächtige Dateien in einer realen Hardware-Umgebung ausgeführt und beobachtet. Dadurch können schädliche Aktivitäten ausgelöst und aufgedeckt werden, die in einer virtuellen Umgebung verborgen geblieben wären. Alle Malware-Funktionen zur Erkennung virtueller Maschinen erweisen sich bei dieser Art der Analyse als wirkungslos.

Finger weg von Open-Source-Hypervisoren

Wenn Sie sich für eine Next-Generation Firewall mit einem proprietären Hypervisor entscheiden, mindern Sie die Erfolgsaussichten raffinierter Malware-Angriffe. Denn die meisten Angreifer testen und perfektionieren ihren Schadcode mithilfe von gängigen Open-Source-Analyseumgebungen.

Mehr Sicherheit durch effektivere Signaturen

Konventionelle signaturbasierte Anti-Malware-Lösungen identifizieren bekannte Bedrohungen anhand bestimmter Variablen wie Hashwerte, Dateinamen oder URLs. Das eröffnet Angreifern die Möglichkeit, ihren Schadcode vor den entsprechenden Sicherheitssystemen zu verbergen, indem sie ihn geringfügig ändern oder in die Entwicklung polymorpher Malware-Varianten einfließen lassen. Denn eine Identifizierung der „neuen", unbekannten Schadprogramme ist auf Basis der alten Signaturen nicht möglich.

In dieser Hinsicht erweisen sich hashwertbasierte Erkennungsverfahren als besonders problematisch, da 99 % der Malware-Hashes – laut dem Verizon Data Breach Investigations Report 2019 – nur für maximal 58 Sekunden Bestand haben.[2] Hier machen sich die Angreifer offensichtlich die Tatsache zunutze, dass der Hashwert eines Schadprogramms schon durch geringfügigste Code-Korrekturen verändert werden kann, was eine Erkennung durch hashwertbasierte Anti-Malware-Systeme verhindert.

Deshalb sollten moderne Next-Generation Firewalls statt der klassischen attributbezogenen Signaturen lernfähige Vorhersagemodelle und inhaltsbasierte Signaturen verwenden, um modifizierte Malware, polymorphe Schadprogramme und Command-and-Control-Aktivitäten (C2-Aktivitäten) aufzudecken. Mit diesem Ansatz lassen sich ganze Malware-Familien mit Tausenden unterschiedlicher Varianten unschädlich machen, ohne dass für jede einzelne Variante eine eigene Signatur erstellt werden muss.

Außerdem kann die C2-Kommunikation mit Schadprogrammen auch dann unterbunden werden, wenn der entsprechende Traffic von den Angreifern im DNS-Verkehr versteckt oder über immer neue, automatisch eingerichtete URLs abgewickelt wird. Denn im Gegensatz zu schnell veraltenden URL-spezifischen Signaturen bieten die auf Analysen von ausgehenden Kommunikationsmustern basierenden C2-Signaturen einen erheblich effektiveren Schutz, der sich zudem automatisch anpassen und auf die gesamte Infrastruktur ausdehnen lässt.

Starker Schutz durch die Kombination verschiedener Analyseverfahren

Viele hartnäckige und raffinierte Hacker investieren in die Entwicklung von Zero-Day-Exploits und anderen völlig neuartigen Schadprogrammen, die durch signaturbasierte Erkennungssysteme nicht identifiziert werden können.

Wenn Ihr Unternehmen zum Ziel eines solchen Angriffs wird, bleibt Ihnen nur wenig Zeit, um die Bedrohung aufzudecken und durch die rasche Anpassung sämtlicher Sicherheitssysteme einzudämmen. Daher benötigen Sie eine Lösung, die auf maschinellen Lernverfahren basierende statische Analysen, dynamische Analysen und Bare-Metal-Analysen miteinander kombiniert. Durch die parallele Nutzung dieser automatisierten Verfahren erleichtern Sie die präzise und effiziente Erkennung und Abwehr von Bedrohungen, geben Ihren Mitarbeitern mehr Zeit für anspruchsvollere Aufgaben und heben das Sicherheitsniveau des gesamten Unternehmens.

Empfohlene Fragen für die Ausschreibung:

- Verfügt die Next-Generation Firewall über auf maschinellem Lernen basierende Funktionen zur Abwehr unbekannter schädlicher Dateien, Malware-Varianten und dateiloser Angriffe, die PowerShell® und andere Skriptsprachen missbrauchen?
- Bietet die Next-Generation Firewall auf maschinellem Lernen basierenden Inline-Schutz vor schädlichen Websites, JavaScript-Angriffen und Phishing-Kampagnen zum Diebstahl von Anmeldedaten?
- Wie schnell übermittelt das mit der Firewall integrierte cloudbasierte Malware-Analysesystem nach der Aufdeckung einer Bedrohung die entsprechenden Signaturen?
- Nutzt die Next-Generation Firewall signaturunabhängige Verfahren und Technologien zur Abwehr bisher unbekannter Angriffe?
- Steht neben der cloudbasierten Sandbox-Umgebung auch eine Bare-Metal-Umgebung für Malware-Analysen bereit?
- Nutzt das mit der Firewall verknüpfte cloudbasierte Malware-Analysesystem einen speziell zur Aufdeckung von Anti-Sandbox-Malware entwickelten Hypervisor?
- Erstellt das mit der Firewall verknüpfte Malware-Analysetool nach der Aufdeckung von Schadcode automatisch …
  - … inhaltsbasierte Antivirussignaturen, mit denen sich ganze Malware-Familien einschließlich unbekannter Varianten blockieren lassen?
  - … musterbasierte Anti-Spyware-Signaturen, mit denen sich die Kommunikation mit bekannten und unbekannten C2-Servern aufdecken lässt?
- Unterstützt das mit der Firewall verknüpfte Malware-Analysesystem die Untersuchung von Windows®-, Android®-, macOS®- und Linux-Dateien?

2. „Data Breach Investigations Report 2019", Verizon, Mai 2019, https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf.

7. Individuell anpassbarer Firewall-Schutz

Firewalls können extern erstellte Listen mit Regeln und Richtlinien importieren, die ihren Schutz auf die darin spezifizierten Objekte ausdehnen. Das erleichtert Firewall-Administratoren die rasche Anpassung der Sicherheitssysteme an neue Bedrohungen, Anforderungen und Vorgaben, was insbesondere dann von Nutzen ist, wenn kriminelle Hacker automatisierte oder getarnte Angriffsmethoden nutzen.

Warum ist dieses Feature erwägenswert und weshalb lohnt sich ein Test?

Wenn Sie dynamische Listen in Ihre Next-Generation Firewall integrieren und zur automatischen Anpassung der Schutzmechanismen nutzen, heben Sie das Sicherheitsniveau Ihres Unternehmens schnell und effizient. Denn die von Ihrem Firewall-Anbieter gepflegten Listen lassen sich manuell aktualisieren und mit externen Bedrohungsdaten erweitern. Das bietet Ihnen den Vorteil, dass Sie Firewallregeln und -richtlinien über die dynamische Liste modifizieren können und die vorgenommenen Änderungen dann automatisch von allen an die Liste angebundenen Firewall-Appliances übernommen werden.

Modernisierungsperspektiven

Dynamische Listen

Sobald eine bisher unbekannte Bedrohung identifiziert wird, fällt dem Firewall-Administrator die Aufgabe zu, den Firewall-Schutz durch die Erstellung einer neuen Regel oder Richtlinie entsprechend zu erweitern. Sofern hierfür keine automatisierten Abläufe zur Verfügung stehen, muss der zeitaufwendige und fehleranfällige manuelle Änderungsprozess für jedes verdächtige Objekt auf jeder Firewall im Netzwerk wiederholt werden.

Sie können jedoch den mit diesen Aufgaben verbundenen Arbeits- und Zeitaufwand erheblich reduzieren, indem Sie dynamische Listen nutzen. In diese werden vom Anbieter Ihrer Next-Generation Firewall – und bei Bedarf auch anderen externen Stellen – kontinuierlich schädliche oder verdächtige IP-Adressen eingepflegt, sodass die von ihnen ausgehenden Hackeraktivitäten durch die Firewall blockiert werden können.

Dynamische Benutzergruppen

Durch die Einrichtung dynamischer Benutzergruppen implementieren Sie automatische Mechanismen zur Überwachung und Eindämmung anomaler oder schädlicher Nutzeraktivitäten. Dabei gleicht die Firewall das beobachtete Benutzerverhalten automatisch mit den in der Gruppendefinition festgelegten Kriterien (Tags) ab, erweitert und aktualisiert die Liste der Mitglieder dann automatisch und setzt die vorgesehenen Richtlinien durch, um beispielsweise verdächtige Verhaltensweisen zu unterbinden. Das bietet gegenüber der Verwendung statischer Gruppenobjekte den Vorteil, dass die Sicherheitsinfrastruktur unmittelbar auf Änderungen im Benutzerverhalten und potenzielle Bedrohungen reagieren kann, ohne dass dafür manuelle Modifikationen der Richtlinien erforderlich sind.

Auf diese Weise leisten dynamische Benutzergruppen einen entscheidenden Beitrag zur automatisierten, stringenteren Durchsetzung von Sicherheitsrichtlinien, zur flexiblen Anpassung der Firewall-Funktionen an neue Anforderungen und zur Eindämmung unnötiger Zugriffsrechte. Zudem werden Administratoren in die Lage versetzt, die Liste der Gruppenmitglieder ad hoc zu modifizieren und die Zugriffsrechte der Benutzer in Abhängigkeit ihrer Aktivitäten einzuschränken.

Bedrohungsdatenfeeds von Drittanbietern

Moderne Unternehmen abonnieren Bedrohungsdatenfeeds von Drittanbietern, um ständig über potenzielle Gefahren und die Urheber und Methoden raffinierter Angriffe auf dem Laufenden zu sein. Dadurch erhalten sie große Mengen von Rohdaten, die als Gefahrenindikatoren die frühzeitige Abwehr bisher unbekannter Bedrohungen und damit die Verhinderung von Hackereinbrüchen und Infektionen ermöglichen.

Allerdings nimmt die manuelle Umsetzung der eingehenden Bedrohungsdaten in Firewall-Regeln und -Richtlinien oft mehr Zeit in Anspruch, als den dünn besetzten Sicherheitsteams zur Verfügung steht. Denn zum einen müssen die Daten aus den diversen Feeds auf ihre Aktualität überprüft und eventuell in ein anderes Format umgewandelt werden. Und zum anderen müssen bestimmte Indikatoren zu Mustern zusammengefasst und mit Kontextinformationen angereichert werden, um die nötige Trennschärfe zu erreichen und einen relevanten Beitrag zur Aufdeckung akuter Bedrohungen zu leisten. Nur wenn die Bedrohungsdaten auf diese Weise validiert und aufbereitet wurden, können sie von den Sicherheitsteams zur Einrichtung effektiver flächendeckender Schutzmaßnahmen gegen spezifische Bedrohungen genutzt werden. Ansonsten besteht die Gefahr, dass die auf den Sicherheitspunkten implementierten Kontrollmechanismen nicht greifen und das Potenzial der Datenfeeds ungenutzt bleibt.

Infolgedessen ist eine datengestützte Stärkung der Sicherheit bei gleichzeitiger Reduzierung des Risikos manueller Fehler ausschließlich durch Automatisierung möglich. Mithilfe automatischer Verfahren können Sie Bedrohungsindikatoren ohne Zeitverlust mit Kontextinformationen anreichern, um sie schnell in effektive Schutzmechanismen zu übersetzen und den Angreifern so immer einen Schritt voraus zu sein.

Empfohlene Fragen für die Ausschreibung:

- Unterstützt die Next-Generation Firewall die automatische Erstellung von Sicherheitsrichtlinien mithilfe dynamischer Listen und Benutzergruppen?
- Kann der Schutz der Next-Generation Firewall dynamisch auf der Grundlage externer und interner Bedrohungsdatenfeeds angepasst werden, ohne dass dafür Richtlinien modifiziert werden müssen?
- Stehen Aufbereitungsfunktionen zur Verfügung, mit denen sich die Bedrohungsdaten aus verschiedenen Feeds aggregieren, konsolidieren und deduplizieren lassen, bevor sie in die Firewall eingespeist werden?
- Kann die Next-Generation Firewall im Zusammenspiel mit anderen Komponenten Ihrer Sicherheitsinfrastruktur veraltete Bedrohungssignaturen mithilfe von Timeouts automatisch außer Kraft setzen?
- Können Sie die Next-Generation Firewall mit Bedrohungsdatenfeeds speisen, um proaktiv Indikatoren zur Aufdeckung der neuesten Advanced Persistent Threats zu implementieren?
- Können Sie eingehende Bedrohungsdaten im Hinblick auf ihre Zuverlässigkeit bewerten, um einen erhöhten Arbeitsaufwand durch eine große Zahl von Fehlalarmen zu vermeiden?

8. Abwehr komplexer Bedrohungen und Angriffe

Derzeit ist zu beobachten, dass sowohl die Vielfalt der Bedrohungen als auch die Zahl der gefährdeten Geräte wächst. Besonders große Risiken gehen unter anderem von Phishing-Kampagnen, dem Diebstahl und Missbrauch von Anmeldedaten, Denial-of-Service-Angriffen, Ransomware-Infektionen sowie Malware mit Backdoor- und Command-and-Control-Funktionen aus. Erschwerend kommt hinzu, dass das Internet der Dinge (IoT) die Angriffsfläche der Unternehmen vergrößert und dadurch zunehmend ins Visier der Hacker rückt. So hat der IoT Threat Report 2020 unserer Unit 42 gezeigt, dass ganze 57 Prozent der IoT-Geräte anfällig für mittelschwere und schwere Angriffe und damit eine leichte Beute für Angreifer sind. Dabei dienen die infizierten Geräte oft als Sprungbrett für die weitere Ausbreitung auf andere Systeme im Netzwerk.

Warum ist dieses Feature erwägenswert und weshalb lohnt sich ein Test?

Ein einzelnes Sicherheitsprodukt bietet keinen ausreichenden Schutz gegen die vielfältigen aktuellen Bedrohungen. Deshalb benötigen Sie eine mehrschichtige Sicherheitsinfrastruktur, die laufende Angriffe in verschiedenen Phasen effektiv unterbinden kann. Nur wenn Sie Ihr Unternehmen mit von Haus aus automatisierten und miteinander integrierten Sicherheitslösungen schützen, bekommen Sie Malware, Ransomware und andere Bedrohungen in den Griff. Außerdem profitieren Sie so von der Möglichkeit, Ihren Netzwerkschutz um neue Komponenten zu erweitern, die sich nahtlos in Ihre Sicherheitsinfrastruktur einfügen.

Das erleichtert beispielsweise die Sicherung von IoT-Geräten, die nach Angaben des Analystenteams Unit 42 von Palo Alto Networks stolze 30 Prozent aller mit dem Unternehmensnetzwerk verbundenen Geräte (exklusive der Smartphones) ausmachen. Diese Geräte stellen ein großes Sicherheitsrisiko dar, da sie mit dem Unternehmensnetzwerk verbunden sind und vielfach Schwachstellen aufweisen, die sich nicht oder nur mit großen Schwierigkeiten patchen lassen.

Modernisierungsperspektiven

Es gibt keine Wunderwaffe

Um raffinierte Angriffe effektiv abwehren zu können, benötigen Sie sowohl einen umfassenden Überblick über den Datenverkehr in Ihrem Netzwerk und den Anwendungsbetrieb als auch die Möglichkeit zur Implementierung und Durchsetzung benutzerspezifischer und inhaltsbasierter Richtlinien. Darüber hinaus sollten Sie in Sicherheitsprodukte investieren, die vor bekannten und unbekannten Malware-Varianten und Exploits schützen, die C2-Kommukation unterbinden und den Zugriff auf bekannte schädliche Websites und Phishing-URLs blockieren.

Die Zeit als entscheidende Faktor

Nur durch Automatisierung lassen sich Angriffe schon in frühen Phasen unterbinden, bevor das gesamte Unternehmen betroffen ist. Das gilt zum einen für die Analyseverfahren zur Identifizierung unbekannter Bedrohungen, schädlicher Dateien und verdächtiger URLs, zum anderen für die daran anschließende Erstellung und flächendeckende Implementierung entsprechender Schutzmechanismen in sämtlichen Netzwerken und Cloud-Umgebungen sowie auf allen Endpunkten. Auf diese Weise können Sie beispielsweise dafür sorgen, dass alle Angriffsvektoren rasch gegen die neueste Version einer bestimmten Ransomware immunisiert werden.

Ein reibungsloses Zusammenspiel

Neben der Automatisierung ist der reibungslose Informationsaustausch zwischen den verschiedenen Sicherheitstools ein weiterer wichtiger Aspekt der effektiven Abwehr von Bedrohungen. So können Sie durch die nahtlose Integration Ihrer Lösungen sicherstellen, dass bekannte und unbekannte Malware-Varianten und Exploits schnellstmöglich erkannt und infizierte Hosts umgehend identifiziert und isoliert werden. Dadurch beschleunigen Sie die Eindämmung akuter Angriffe.

Ergänzend sollten Sie in zuverlässige Bedrohungsdaten investieren, die zur dynamischen Aktualisierung des Firewall-Schutzes gegen schädliche IP-Adressen, Domains und URLs genutzt werden können.

Minimierung IoT-spezifischer Risiken

Da die Zahl und Vielfalt der mit dem Unternehmensnetzwerk verbundenen Geräte ständig wächst, haben viele Sicherheitsteams Schwierigkeiten, das von diesen möglichen Angriffsvektoren ausgehende Risiko durch geeignete Schutzmaßnahmen zu minimieren. Um hier Abhilfe zu schaffen, benötigen Sie eine Sicherheitslösung, die nicht nur Ihr Netzwerk segmentiert, sondern auch sämtliche IoT-Geräte klassifiziert, patcht und überwacht und zugleich dafür sorgt, dass jedes IoT-Gerät ausschließlich Zugriff auf die vorgesehenen Ressourcen erhält und den richtigen Netzwerksegmenten zugewiesen wird. Damit leisten Sie einen wichtigen Beitrag zur Minimierung der Angriffsfläche Ihres Unternehmens und senken das Risiko für andere Ressourcen.

Empfohlene Fragen für die Ausschreibung:

- Kann die Next-Generation Firewall Ransomware-Angriffe verhindern, indem sie ausführbare Dateien und andere risikobehaftete Dateitypen blockiert, wenn diese von unbekannten Anwendungen und URLs stammen?
- Kann die Next-Generation Firewall Angriffe auf IoT-Geräte abwehren?
- Kann die Next-Generation Firewall automatisch Gefahrenindikatoren (wie IP-Adressen, Domainnamen und URLs) importieren und dynamisch in ihre Sperrliste aufnehmen, um Ihr Unternehmen vor allen bekannten Ransomware-Varianten zu schützen?
- Kann der Malware-Filter der Next-Generation Firewall mithilfe integrierter Bedrohungsdatenfeeds dynamisch um schädliche URLs erweitert werden, die im Zusammenhang mit Ransomware-Angriffen beobachtet wurden?
- Kann die Sperrliste der Next-Generation Firewall mithilfe integrierter Bedrohungsdatenfeeds automatisch um die DNS-Signaturen schädlicher Domains erweitert werden, die im Zusammenhang mit Ransomware-Angriffen beobachtet wurden? Können alternativ auch automatisch DNS-Sinkholes für die betreffenden Domains eingerichtet werden?
- Kann die Next-Generation Firewall Bedrohungsdaten und Indikatoren für verdächtige Aktivitäten mit Ihrer Lösung für den Endpunktschutz austauschen?
- Können Sie mit der Next-Generation Firewall sämtliche – auch bisher unbekannte – IoT-Geräte in Ihrem Netzwerk überwachen?
- Kann die Next-Generation Firewall den IoT-Verkehr vom Rest des Netzwerks isolieren, damit gekaperte IoT-Geräte nicht zum Einfallstor für Hacker werden?
- Liefert Ihnen die Next-Generation Firewall auf Risikoanalysen basierende Empfehlungen für neue Richtlinien, die dann automatisch implementiert werden können?

9. Konsistenter, standortunabhängiger Schutz für Benutzer und Anwendungen

Immer mehr Benutzer nutzen Mobilgeräte, um von entfernten Standorten in aller Welt auf geschäftliche Anwendungen zuzugreifen. Zugleich steigt die Zahl der in Cloud-Umgebungen und Filialinfrastrukturen gehosteten Apps, die dasselbe Maß an Sicherheit und Konnektivität benötigen wie die in Ihrem Rechenzentrum bereitgestellten Softwarelösungen. Trotzdem sind viele Unternehmen weiterhin nicht in der Lage, den Internet-Datenverkehr externer Benutzer und den Verkehr Ihrer Cloud-Anwendungen effektiv zu überwachen und zu sichern.

Warum ist dieses Feature erwägenswert und weshalb lohnt sich ein Test?

Ihr Unternehmen sollte allen Benutzern einheitlichen Schutz bieten, ohne dass dafür standortabhängige Sicherheitsprofile erstellt werden müssen. Dies empfiehlt sich nicht zuletzt deshalb, weil Sicherheitsrichtlinien effektiver sind, wenn sie auf konsistente Weise – das heißt mithilfe zentraler Tools und auf der Grundlage eines unternehmensweit gültigen Frameworks – implementiert und durchgesetzt werden. Außerdem erhalten Ihre Sicherheitsteams so mehr Kontrolle über sämtliche geschäftlich genutzten Geräte.

Modernisierungsperspektiven

Jedes an verschiedenen Standorten agierende Unternehmen benötigt ein SD-WAN, das die für den Netzwerkbetrieb Verantwortlichen in die Lage versetzt, maßgeschneiderte Datenverbindungen zu Filialen und Cloud-Instanzen einzurichten, die allen Benutzern das nötige Maß an Konnektivität bereitstellen. In diesem Zusammenhang erweist es sich als großer Vorteil, wenn die von Ihnen gewählte Next-Generation Firewall in Filialinfrastrukturen als SD-WAN-Edge-Gerät und an den Hauptstandorten als SD-WAN-Hub fungieren kann. Dabei sollten die SD-WAN-Funktionen auf einfache Weise von einer zentralen Netzwerksicherheitskonsole aus verwaltet werden können.

Ein derartiges SD-WAN ermöglicht nicht nur die Einrichtung anwendungsspezifischer Routing-Richtlinien, sondern erleichtert den WAN-Administratoren außerdem die an aktuellen Netzwerkanforderungen orientierte Erstellung und Aktualisierung von Sicherheitsregeln in Echtzeit. Darüber hinaus unterstützt es die einfache, ressourcen- und kostensparende Remote-Einrichtung und -Konfiguration neuer Edge-Systeme sowie den direkten, latenzarmen Zugriff auf Cloud-Ressourcen (ohne Umleitung des entsprechenden Verkehrs über einen zentralen Hub).

Achten Sie also bei der Sichtung entsprechender Produkte darauf, dass diese die Implementierung einheitlicher Schutzmaßnahmen für interne und externe Benutzer ermöglichen und dank vielfältiger Bereitstellungsoptionen an allen Standorten eingerichtet werden können. So treiben Sie den Aufbau einer Sicherheitsinfrastruktur voran, die sämtliche Benutzer mithilfe von Cloud-Services und Firewalls überall auf der Welt vor bekannten und unbekannten Bedrohungen schützt.

Empfohlene Fragen für die Ausschreibung:

- Kann die Next-Generation Firewall die implementierten Sicherheitsrichtlinien auch auf den Geräten mobiler Benutzer durchsetzen?
- Wie werden Benutzer geschützt, die nicht durch die Next-Generation Firewall gesichert sind, weil sie sich an einem externen Standort aufhalten?
- Kann die Next-Generation Firewall bei Bedarf als SD-WAN-Edge-Gerät fungieren?
- Lässt sich die Next-Generation Firewall per Fernzugriff einrichten und bereitstellen?
- Unterstützt die Next-Generation Firewall die Einrichtung dauerhafter VPN-Verbindungen über mehrere physische und/oder virtuelle Appliances?
- Kann die Next-Generation Firewall mobile Benutzer mithilfe cloudbasierter Sicherheitsmechanismen direkt an ihren jeweiligen Standorten schützen?

10. Eignung für Zero Trust

Bisher war es gängige Praxis, Benutzer als „vertrauenswürdig“ oder „nicht vertrauenswürdig“ einzustufen und ihnen dementsprechend Zugang zum Netzwerk zu gewähren oder zu verweigern. Dieser Ansatz hat jedoch den Nachteil, dass sich einmal als vertrauenswürdig klassifizierte Personen frei in der Infrastruktur bewegen können – selbst wenn es sich um eingedrungene Hacker, böswillige Insider oder Benutzer mit allzu großzügig bemessenen Zugriffsrechten handelt –, falls das Netzwerk nicht segmentiert oder durch zusätzliche richtlinienbasierte Zugangskontrolle geschützt ist. Das erleichtert es Angreifern, Anmelde- und Unternehmensdaten zu stehlen, geistiges Eigentum zu rauben und Malware einzuschleusen. Zero Trust minimiert dieses Risiko, indem der Vertrauensstatus abgeschafft wird. Das Motto dieses Ansatzes lautet „Never trust, always verify“ – Glauben Sie nichts ungeprüft.

Warum ist dieses Feature erwägenswert und weshalb lohnt sich ein Test?

Zero Trust ist ein äußerst effektiver Ansatz zur Sicherung moderner Netzwerke, der auf der Minimierung von Zugriffsrechten und der standortunabhängigen Prüfung von Benutzern, Geräten, Inhalten und Anwendungen basiert. Diese Methodologie eignet sich zum einen als Roadmap für den Aufbau eines segmentierten Netzwerks, zum anderen als Ausgangspunkt für die Entwicklung einer effektiven Präventionsstrategie, die sich in der gesamten Unternehmensinfrastruktur – einschließlich aller Netzwerke, Endpunkte und Clouds – umsetzen lässt. Das eröffnet Ihren Sicherheitsteams die Möglichkeit, die Definition, Verwaltung, Durchsetzung und Pflege entsprechender Zero-Trust-Richtlinien mithilfe integrierter Sicherheitstools unternehmensweit zu automatisieren.

Hier spielt Ihre künftige Next-Generation Firewall eine zentrale Rolle, da sie als Segmentierungs-Gateway dient und in dieser Funktion die Implementierung von Layer-7-Richtlinien übernimmt. Dabei hängt die optimale Position der Kontrollpunkte von Ihren geschäftlichen Anforderungen, den beobachteten Datenverkehrsmustern und den bestehenden Abhängigkeiten zwischen Datenbeständen, Endgeräten und Anwendungen ab.

Modernisierungsperspektiven

Bei der Umsetzung des Zero-Trust-Ansatzes muss zuerst die zu schützende Oberfläche definiert werden, die sich aus den wichtigsten und wertvollsten Datenbeständen, Ressourcen, Anwendungen und Diensten im Netzwerk zusammensetzt.

Dann wird mithilfe der Next-Generation Firewall und eines speziellen Sensornetzes ein schützender Mikroperimeter um diese Oberfläche errichtet, sodass jedes eingehende und ausgehende Datenpaket geprüft werden kann. Dadurch wird der konventionelle Perimeterschutz am Netzwerkrand um Kontroll- und Überwachungsmechanismen für den unternehmensinternen Nord-Süd- und Ost-West-Verkehr ergänzt. Begleitend sollten Sie MFA und andere Authentifizierungsverfahren implementieren, damit nur befugte Benutzer Zugriff erhalten.

Auf diese Weise entsteht Schritt für Schritt die vielschichtige Sicherheitsinfrastruktur, die das Kernstück des Zero-Trust-Ansatzes bildet und neben den bereits genannten Tools auch leistungsstarke Monitoring- und Sicherheitslösungen zur Abwehr komplexer Bedrohungen umfasst. Damit sollten Sie effektive Zugriffskontrollen einrichten, anomale oder schädliche Benutzeraktivitäten erkennen, Richtlinien unternehmensweit aktualisieren und verdächtige Vorgänge umgehend unterbinden können.

Empfohlene Fragen für die Ausschreibung:

- Kann die Next-Generation Firewall als Segmentierungs-Gateway fungieren?
- Unterstützt die Next-Generation Firewall die Überwachung, Entschlüsselung und Überprüfung des gesamten Datenverkehrs?
- Können Sie mithilfe der Next-Generation Firewall Layer-7-Richtlinien erstellen und durchsetzen?

Bonus: Flexible Bereitstellungsoptionen, auch für Container-Umgebungen

Zahlreiche Unternehmen setzen nach wie vor auf physische Appliances, um die Eingangs- und Ausgangspunkte ihrer konventionellen Rechenzentren und Hochleistungsnetzwerke zu kontrollieren. Zugleich kommen vielerorts virtuelle Appliances zum Einsatz, die die Sicherung und Überwachung des Ost-West-Verkehrs in hochgradig dynamischen softwaredefinierten Rechenzentren ermöglichen.

Diese Zweiteilung wird nun aufgebrochen, da sich durch die zunehmende Nutzung von Containern neue Herausforderungen rund um die Netzwerksicherheit ergeben, die nach neuen Lösungen verlangen. Denn wenn cloudnative Apps mit älteren Anwendungen verknüpft und flächendeckend bereitgestellt werden, unterliegen sie denselben Sicherheits- und Compliance-Anforderungen wie der Rest der Anwendungs- und Unternehmensinfrastruktur.

Warum ist dieses Feature erwägenswert und weshalb lohnt sich ein Test?

Viele Firewall-Produkte bieten nur begrenzten Schutz für containerisierte Anwendungen. Einige lassen sich zwar mit Orchestrierungstools für Container-Umgebungen integrieren, erlauben jedoch lediglich die Überwachung kompletter Knoten oder Cluster und stellen ausschließlich grundlegende Port- und Protokoll-Filter bereit. So verfügen cloudnative Firewalls über einfache, auf der Sperrung von Ports basierende Funktionen zur Container-Mikrosegmentierung, die allerdings nicht die Abwehr von Bedrohungen ermöglichen. Andererseits lassen viele konventionelle Next-Generation Firewalls die native Integration mit Container- und Orchestrierungs-Frameworks vermissen, die für einen effektiven Schutz dieser hochgradig dynamischen Umgebungen erforderlich wäre.

Modernisierungsperspektiven

Eine speziell für Container-Umgebungen und den Schutz von containerisierten Rechenzentren ausgelegte Next-Generation Firewall muss Ihnen erstens die Möglichkeit zur Überwachung, Prüfung und Kontrolle des Datenverkehrs zwischen den Pods und Containern eines Clusters bieten. Zweitens sollten ihre Sicherheitsmechanismen auch dann greifen, wenn Container auf Online-Ressourcen wie GitHub®-Repositorys zugreifen, damit stets sichergestellt ist, dass jeder Container auch tatsächlich mit dem vorgesehen Repository kommuniziert und keinen gefälschten oder schädlichen Code herunterlädt. Und drittens sollte der Anbieter zusätzlich zur Container-Firewall funktionsgleiche Next-Generation Firewalls für physische und virtuelle Umgebungen bereitstellen, sodass sich auch die Hybrid-Rechenzentren moderner Unternehmen konsistent schützen lassen.

Empfohlene Fragen für die Ausschreibung:

- Schützt die Firewall unternehmensintern gehostete, cloudbasierte und containerisierte Anwendungen mit denselben Netzwerksicherheits- und Abwehrmaßnahmen?
- Wurde die Firewall speziell für die Bereitstellung in Kubernetes®-Clustern und die nahtlose Integration in CI- und CD-Prozesse (Continuous Integration/Continuous Deployment) entwickelt?
- Lässt sich die Firewall mit softwaredefinierten Netzwerklösungen (SDN) integrieren, sodass die im PCI-Standard vorgeschriebenen Sicherheits-, Schutz- und Segmentierungsfunktionen an Remote-Standorten bereitgestellt werden können?

Umfassende Sicherheit

Versierte Hacker nutzen immer neue raffinierte Methoden für komplexe, gezielte und gut getarnte Angriffe auf diverse Umgebungen.

Deshalb sollten Sie sicherstellen, dass Ihre neue Next-Generation Firewall und die dazugehörigen Sicherheitsprodukte umfassenden Schutz bieten und die nachfolgend aufgeführten Kriterien erfüllen.

Moderne, effektive Technologien

Setzen Sie auf branchenführende Technologien zur schnellen, automatischen Erkennung und Abwehr bekannter und unbekannter Bedrohungen, um Daten und Benutzer in jeder Angriffsphase unabhängig von ihrem jeweiligen Standort konsistent und risikoadäquat zu schützen. Dabei sollten Sie insbesondere darauf achten, dass sich die von Ihnen gewählten Produkte schnell und flexibel an neue Risiken und dynamische Workloads anpassen lassen.

Effiziente Betriebsprozesse

Wenn das von Ihnen gewählte Produkt automatisierte Bereitstellungsprozesse und die API-basierte Integration unterstützt, müssen Ihre Teams weniger Zeit auf fehleranfällige manuelle Routineaufgaben verwenden und können sich auf strategische Initiativen konzentrieren. Außerdem sollten Sie sicherstellen, dass Ihre neue Firewall ohne übermäßigen personellen und finanziellen Aufwand in diversen Umgebungen implementiert werden kann und sich nahtlos in Ihre Sicherheitsinfrastruktur einfügt.

Reaktionsschneller Kundenservice durch erfahrene Experten

Gut geschulte und reaktionsschnelle Service- und Supportteams erleichtern Ihren Mitarbeitern die Einarbeitung und unterstützen sie sowohl bei der langfristigen Stärkung Ihrer Sicherheitsinfrastruktur als auch bei der Realisierung einer maximalen Rendite für Ihre Investition.

Damit lässt sich abschließend feststellen: Wenn Sie die Anschaffung einer neuen Firewall planen oder erwägen, sollten Sie die Features und Funktionen infrage kommender Produkte in enger Zusammenarbeit mit sämtlichen Sicherheitsteams Ihres Unternehmens testen.

Orientieren Sie sich dabei an den in diesem Whitepaper aufgezählten Kriterien, um sicherzugehen, dass Ihre nächste Firewall alle aktuellen und künftigen Anforderungen erfüllt.

Sind Sie bereit, Ihre nächste Firewall zu testen? Dann melden Sie sich für den Ultimate Test Drive an.

paloalto NETWORKS

Oval Tower, De Entrée 99–197
1101 HE Amsterdam
Niederlande

Telefon: +31 20 888 1883

www.paloaltonetworks.de

10-things-to-test-in-your-future-next-generation-firewall-wp-062420-de