Leitfaden zum Kauf einer Firewall der nächsten Generation

Ein detaillierter Leitfaden zur Bewertung von Firewalls für Unternehmensnetzwerke

Im Zuge der rasanten Weiterentwicklung der IT hat sich auch an der Netzwerkgrenze vieles geändert. Die Situation der Daten und Benutzer wird zunehmend unüberschaubar. Die Anzahl der Geräte wächst so rasant, dass die meisten Unternehmen mit der Entwicklung nicht mehr mithalten können. IT-Teams nutzen die Cloud, Big-Data-Analysen, maschinelles Lernen und die Automatisierung, um die Bereitstellung neuer Anwendungen zu beschleunigen und so das Unternehmenswachstum voranzutreiben. Gleichzeitig können Benutzer auf immer mehr Anwendungen zugreifen. Das Ergebnis ist ein überaus komplexes Netzwerk, das erhebliche Geschäftsrisiken birgt. Unternehmen stehen nun vor der Aufgabe dieses Risiko zu minimieren, ohne ihre Geschäftsabläufe zu verlangsamen.

Die Cybersicherheit wird auf eine harte Probe gestellt, da Angreifer laufend versuchen, Betriebsvorgänge zu stören. Investitionen in die Sicherheit scheinen wie ein Fass ohne Boden, während die Auswirkung auf die Risikoreduktion ungewiss ist. In diesem Umfeld bieten separate, nicht integrierte Tools und Technologien Unternehmen keinen ausreichenden Schutz. Sicherheitstools, die nicht für die Automatisierung konzipiert wurden, machen das Eingreifen von Analytikern erforderlich, die erst Informationen aus mehreren nicht verbundenen Quellen manuell zusammenführen müssen, bevor sie entsprechende Maßnahmen setzen können. Diese Ansatz ist nicht zielführend.

Wir benötigen eine Firewallplattform der nächsten Generation als Eckpfeiler einer effektiven Netzwerksicherheitsstrategie. Mit einer Architektur, die auf Prävention setzt, können Sicherheitsteams Best Practices zur Verhinderung von Angriffen nutzen, Automatisierung und Analysen zur Verringerung des manuellen Aufwands einsetzen sowie separate, punktuelle Produkte durch eng integrierte innovative Tools ersetzen, die den Schutz verbessern und dessen Handhabung vereinfachen.

In diesem Paper wird gezeigt, wie eine Firewall zu einer Firewall der nächsten Generation ausgebaut werden kann. Zusätzlich werden die wichtigsten Fähigkeiten aufgeführt, die eine innovative Firewall haben muss, um Ihr Netzwerk und Ihr Unternehmen zu schützen. Abschließend werden zentrale Fragen aufgelistet, die Sie bei einer Angebotsanfrage und der Beurteilung einer Firewall stellen sollten.

Die Entwicklung von Firewalls der nächsten Generation

Früher wurde der Datenverkehr durch Stateful Inspection Firewalls nur anhand des Zielports klassifiziert, wie z. B. TCP-Port 80 für HTTP. Als jedoch der Bedarf an Anwendungserkennung immer größer wurde, fügten viele Anbieter ihren Stateful Inspection Firewalls Tools zur Anwendungstransparenz und andere Software oder Hardware-Blades hinzu und verkauften anschließend die Lösung als Unified Threat Management (UTM). Da diese Funktionen aber im Nachhinein eingebaut wurden und nicht nativ integriert waren, verbesserten diese UTMs nicht den Schutz.

> Gartner prognostizierte, dass bis Ende 2019 90 % der betrieblichen Internetverbindungen für die installierte Basis durch innovative Firewalls geschützt sein würden.[1]

Im Gegensatz zu UTM-Lösungen erkennen innovative Firewalls Anwendungen und treffen Entscheidungen auf der Grundlage von Anwendung, Benutzer und Inhalt. Die integrierte Bauweise erhöht die Sicherheit und vereinfacht den Betrieb. Aufgrund des Erfolgs dieses Modells ist der Begriff „Firewall der nächsten Generation“ heute gleichbedeutend mit „Firewall“.

Erforderliche Fähigkeiten einer Firewall der nächsten Generation

- Identifiziert Anwendungen unabhängig von Port, Protokoll, Umgehungsmethoden oder Verschlüsselung
- Identifiziert Benutzer unabhängig von Gerät oder IP-Adresse
- Entschlüsselt verschlüsselten Datenverkehr
- Schützt in Echtzeit vor bekannten und unbekannten Bedrohungen, die in Anwendungen eingebettet sind
- Liefert vorhersehbaren Multi-Gigabit-Inline-Durchsatz

Die Auswahlkriterien für Firewalls der nächsten Generation lassen sich in drei Bereiche unterteilen: Sicherheitsfunktionen, Betrieb und Leistung. Die Sicherheitsfunktionen beziehen sich auf die Wirksamkeit der Sicherheitskontrollen und die Fähigkeit Ihrer Mitarbeiter, das Risiko zu handhaben, das mit den über Ihr Netzwerk laufenden Anwendungen, einhergeht, ohne die Geschäftsabläufe zu verlangsamen. Was den Betrieb anbelangt, sollte Zugriff auf die Anwendungsrichtlinie bestehen und diese sollte einfach zu verwalten sein. Zusätzlich sollte Automatisierung angewendet werden, um den manuellen Aufwand zu verringern, sodass sich die Sicherheitsteams hochqualifizierten Aufgaben widmen können. Die Leistungskriterien sind einfach erklärt: Die Firewall muss ihre Aufgabe erfüllen und dabei den für Ihre Geschäftsanforderungen nötigen Durchsatz gewährleisten. Deshalb sollten neue Tools eng integriert und leicht zu handhaben sein. Obwohl die spezifischen Anforderungen und Prioritäten innerhalb dieser Kriterien schwanken können, gibt es bestimmte Fähigkeiten, die eine Firewall unbedingt haben muss.

14 Fähigkeiten, die eine Firewall der nächsten Generation haben muss

1. Identifikation von Benutzern und Gewährung von Zugriff

Das Problem

Mitarbeiter, Kunden und Partner verbinden sich mit verschiedenen Datenspeichern innerhalb Ihres Netzwerks sowie mit dem Internet. Diese Personen und ihre zahlreichen Geräte stellen die Benutzer Ihres Netzwerks dar. Für die Sicherheitslage Ihres Unternehmens ist es wichtig, dass Sie in der Lage sind, Ihre Benutzer über die IP-Adresse hinaus zu identifizieren und die Risiken zu erfassen, die diese aufgrund der von ihnen verwendeten Geräte mit sich bringen – insbesondere dann, wenn Sicherheitsrichtlinien umgangen wurden oder neue Bedrohungen in Ihr Netzwerk eingeschleust wurden. Hinzu kommt, dass die Benutzer ständig ihren Standort wechseln und mehrere Geräte, Betriebssysteme und Anwendungsversionen verwenden, um auf die benötigten Daten zuzugreifen. Subnetze mit IP-Adressen werden nur physischen Standorten zugeordnet, nicht einzelnen Benutzern. Wenn sich Benutzer bewegen – auch innerhalb eines Büros –, folgt ihnen die Richtlinie deshalb nicht.

Außerdem enthalten Benutzerverzeichnisse keine Verhaltensmerkmale. Das Risikoprofil eines Benutzers kann sich ändern und Anmeldedaten können gehackt werden. Dennoch bleiben dieselben Zugriffsrechte auf der Grundlage ihrer Rolle bestehen. Da Änderungen an Benutzerverzeichnissen Zeit erfordern, werden riskante oder böswillige Aktivitäten möglicherweise nicht überprüft und stellen eine Gefahr für das Unternehmen dar.

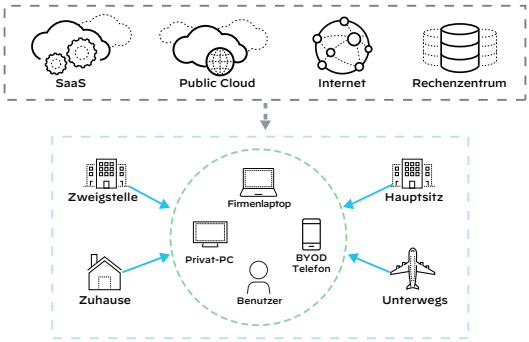

Abbildung 1: Benutzer greifen auf Daten von verschiedenen Geräten und Orten aus zu

1. Adam Hils, Jeremy D'Hoinne, Rajpreet Kaur, „Magic Quadrant for Enterprise Network Firewalls“, Gartner, 10. Juli 2017, https://www.gartner.com/en/documents/3757665/magic-quadrant-for-enterprise-network-firewalls.

Die Lösung

Benutzer- und Gruppeninformationen müssen direkt in die Technologieplattformen integriert werden, die heutige Unternehmen schützen. Ihre nächste Firewall muss in der Lage sein, die Benutzeridentität von verschiedenen Quellen zu beziehen, darunter virtuelle private Netzwerke (VPNs), Access Controller für drahtlose lokale Netzwerke (WLANs), Verzeichnisserver, E-Mail-Server und Erfassungsportale. Wenn bekannt ist, wer welche Anwendungen in Ihrem Netzwerk verwendet und wer möglicherweise eine infizierte Datei überträgt, können Sicherheitsrichtlinien nachgeschärft und Reaktionszeiten bei Zwischenfällen verkürzt werden. Ihre Firewall muss Richtlinien zulassen, um Anwendungen auf der Grundlage von Benutzern oder Benutzergruppen – ob für aus- oder eingehenden Datenverkehr – sicher freigeben zu können. So könnte beispielsweise nur Ihre IT-Abteilung die Erlaubnis erhalten, Tools wie SSH, Telnet und FTP zu verwenden. Benutzerbasierte Richtlinien sind Anwendern zugeordnet und folgen ihnen unabhängig davon, welche Geräte sie verwenden und ob sie sich gerade im Hauptfirmensitz, in einer Zweigstelle oder zu Hause aufhalten. Doch die Entwicklung von Richtlinien auf der Basis von Benutzerinformationen im Verzeichnis ist nicht ausreichend. Sie sollten in der Lage sein, den Benutzerzugriff entsprechend sich ändernder Situationen dynamisch zu regeln. Dies sollte unabhängig davon möglich sein, ob die Änderung eine Folge neuer Kompromissindikatoren (IOCs) oder einer betrieblichen Notwendigkeit ist, wie z. B. die Gewährung von temporärem Zugriff für eine Benutzergruppe.

2. Verhindern von Diebstahl und Missbrauch von Anmeldedaten

Das Problem

Benutzer und ihre Anmeldedaten gehören zu den schwächsten Gliedern der Sicherheitsinfrastruktur eines Unternehmens. Laut dem Bericht von Verizon zum Datenmissbrauch im Jahr 2019 waren 29 % der Sicherheitsverletzungen in den zwölf Monaten des Berichtszeitraums auf gestohlene und/oder schwache Passwörter zurückzuführen[2] Mit gestohlenen Anmeldedaten als Teil ihrer Angriffswerkzeuge steigen die Chancen der Hacker auf einen erfolgreichen Angriff und ihr Risiko, ertappt zu werden, sinkt. Um den Diebstahl von Zugangsdaten zu verhindern, verlassen sich die meisten Unternehmen auf die Schulung ihrer Mitarbeiter, die von Natur aus anfällig für menschliche Fehler ist. Technologieprodukte nutzen häufig die Identifizierung bekannter Phishingsites und das Filtern von E-Mails.

Abbildung 2: Untersuchungsergebnisse von Verizon im Data Breach Investigations Report 2019 zu gestohlenen Anmeldedaten

Diese Methoden können jedoch umgangen werden. Bei der Suche nach bekannten betrügerischen Websites können neue Websites übersehen werden und Angreifer können der E-Mail-Filtertechnologie entgehen, indem sie Links über Social Media versenden. Angreifer können Anmeldedaten einfach durch Phishing, Malware, Social Engineering oder Brute Force stehlen und sie sogar auf dem Schwarzmarkt kaufen. Diese Anmeldedaten können von Angreifern dann verwendet werden, um Zugang zu einem Netzwerk zu erlangen, sich darin lateral zu bewegen und ihre Rechte für den unerlaubten Zugriff auf Anwendungen und Daten zu erweitern.

Die Lösung

Unternehmen sollten nach einer Firewall Ausschau halten, die eine auf maschinellem Lernen basierende Analyse nutzt, um Websites zu identifizieren, die Zugangsdaten stehlen. Wenn im Zuge der Analyse eine Website als bösartig identifiziert wird, sollte die Firewall aktualisiert werden und diese Website blockieren. Dennoch wird es immer wieder neue Phishingwebsites geben, die als „unbekannt" gelten. Ihre nächste Firewall muss Ihnen deshalb die Möglichkeit bieten, die Übermittlung firmeninterner Anmeldedaten an unbekannte Websites zu blockieren. Sie sollten auch eine Firewall wählen, die sensible Daten und Anwendungen schützt, indem sie eine Multi- Faktor-Authentifizierung (MFA) anwendet und Angreifer dadurch hindert, gestohlene Anmeldedaten zu missbrauchen. Durch die Integration mit gängigen MFA-Anbietern kann Ihre Firewall Anwendungen und deren sensible Daten, einschließlich Legacy-Anwendungen, schützen.

3. Sichere Aktivierung aller Anwendungen und Kontrollfunktionen

Das Problem

Immer mehr Anwendungen, wie Instant Messaging, Peer-to-Peer-Filesharing oder Voice-over-IP, können auf nicht standardisierten Ports oder Hopping-Ports ausgeführt werden. Darüber hinaus greifen Benutzer von verschiedenen Geräten und Standorten aus auf verschiedene Typen von Anwendungen zu, darunter auch SaaS-Anwendungen (Software-as-a-Service). Einige dieser Anwendungen werden genehmigt, einige toleriert und andere nicht genehmigt. Doch Benutzer sind immer mehr IT-affin und können die Ausführung von Anwendungen über nicht standardisierte Ports durch Protokolle wie RDP und SSH erzwingen.

Darüber hinaus stellen neue Anwendungen den Benutzern eine Vielzahl von Funktionen zur Verfügung, die zwar die Kundentreue fördern, aber möglicherweise unterschiedliche Risikoprofile aufweisen. Beispielsweise ist WebEx® zwar ein nützliches Businesstool, doch die Verwendung von WebEx Desktop Sharing, das Zugriff auf einen Mitarbeiter-Desktop durch eine externe Quelle gewährt, kann einen unternehmensinternen oder rechtlichen Complianceverstoß darstellen. Gmail® und Google Drive sind ebenfalls gute Beispiele. Sobald ein Benutzer bei Gmail angemeldet ist, was möglicherweise von der Unternehmensrichtlinie erlaubt wird, kann er mühelos zu YouTube® oder Google Fotos wechseln, was möglicherweise nicht mehr erlaubt ist. Sicherheitsadministratoren wünschen sich vollständige Kontrolle über die Nutzung dieser Anwendungen und legen Richtlinien fest, um bestimmte Arten von Anwendungen und Anwendungsfunktionen zuzulassen oder zu kontrollieren und andere abzulehnen.

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

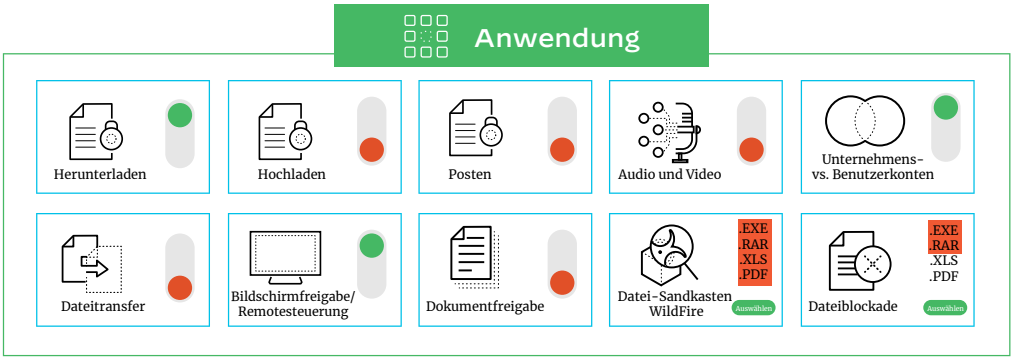

Abbildung 3: Verwendung der Steuerungsanwendung in der Richtlinie

Die Lösung

Ihre nächste Firewall muss in der Lage sein, den Datenverkehr unterteilt nach Anwendung auf allen Ports zu klassifizieren, und zwar permanent und automatisch. Sie sollten sich dabei nicht mit der Suche nach den Ports herumschlagen müssen, die von jeder Anwendung üblicherweise verwendet werden. Die Firewall muss einen vollständigen Einblick in die Nutzung der Anwendungen bieten und gleichzeitig Funktionen bereitstellen, mit denen deren Nutzung erfasst und kontrolliert werden kann (siehe Abbildung 3). Beispielsweise sollte die Firewall die Verwendung von Anwendungsfunktionen wie Audio Streaming, Remotezugriff und das Posten von Dokumenten verstehen und in der Lage sein, diese Verwendung durch detaillierte Regeln zu steuern, z. B. andere Berechtigungen zum Hochladen als zum Herunterladen und für Chats und den Dateitransfer zu verwenden. Dies muss auf kontinuierlicher Basis geschehen. Eine einmalige Klassifizierung des Datenverkehrs ist nicht ausreichend, da hierbei nicht berücksichtigt wird, dass diese häufig verwendeten Anwendungen Sitzungen gemeinsam nutzen und mehrere Funktionen unterstützen können. Wenn in einer Sitzung eine andere Funktion oder ein anderes Merkmal verwendet wird, muss die Firewall erneut eine Richtlinienprüfung durchführen. Eine fortlaufende Statusverfolgung ist ein Muss für Ihre nächste Firewall. Dabei müssen die von jeder Anwendung unterstützten Funktionen sowie die verschiedenen damit verbundenen Risiken erfasst werden.

4. Schließen gefährlicher Lücken der Richtlinie

Das Problem

Legacy-Firewalls ziehen zum Genehmigen und Blockieren von Datenverkehr den Port und die IP-Adresse heran. Dieser Ansatz ist jedoch mangelhaft, da durch portbasierte Regeln sowohl nützliche als auch schädliche Anwendungen die Firewall passieren können. Anwendungen können eine portbasierte Firewall leicht passieren, indem sie zwischen den Ports hin- und herspringen und SSL und SSH oder bekannte offene Ports wie 80 und 443 verwenden. Im Laufe der Zeit häufen sich bei Kunden tausende von portbasierten Regeln auf deren Firewalls an. Diese Regeln werden dann in dieser bestehenden Form auf Firewalls der nächsten Generation migriert. Diese Regeln hinterlassen jedoch gefährliche Sicherheitslücken bei Richtlinien. Immer mehr Kunden verstehen, dass sie für effektive Sicherheit zu anwendungsbasierten Regeln wechseln müssen. Dies erfordert aber einen erheblichen manuellen Aufwand und aufgrund des Mangels an Fachpersonal im Bereich der Cybersicherheit verfügen die meisten Unternehmen nicht über die nötigen Ressourcen. Dadurch steigt das Sicherheitsrisiko erheblich, was den Ausfall der Betriebstätigkeit zur Folge haben kann. Laut Gartner werden bis 2023 99 % der gehackten Firewalls durch fehlerhafte Konfigurationen der Firewall und nicht durch eine fehlerhafte Firewall verursacht.[3]

Die Lösung

Achten Sie bei Ihrer nächsten Firewall auf eine unkomplizierte Regel- und Richtlinienverwaltung. Dies umfasst beispielsweise die Anzeige der Anwendungen, die in Ihrem Netzwerk ausgeführt werden, die Zuordnung zu den Legacy-Regeln und Hilfe beim Ersetzen der Legacy-Regeln. Eine Firewall der nächsten Generation sollte Ihr Sicherheitsteam dabei unterstützen, Legacy-Regeln ohne Mühe durch intuitive, anwendungsbasierte Richtlinien zu ersetzen. Da Regeln, die auf der Identifikation der Anwendungen basieren, leicht verständlich sind und ohne viel Aufwand erstellt und bei sich ändernden Geschäftsanforderungen angepasst werden können, werden Konfigurationsfehler minimiert, die Sie anfällig für Sicherheitsverletzungen machen. Solche Richtlinien erhöhen die Sicherheit und nehmen bei der Verwaltung wesentlich weniger Zeit in Anspruch.

5. Sicher verschlüsselter Datenverkehr

Das Problem

Der Großteil des Webdatenverkehrs von Unternehmen ist heutzutage verschlüsselt. Gerade diese Verschlüsselung wird von Angreifern ausgenutzt, um Bedrohungen vor der Sicherheitsüberwachung zu verbergen. Das bedeutet, dass selbst Unternehmen mit ausgereiften, umfassenden Sicherheitseinrichtungen gehackt werden können, wenn sie den verschlüsselten Datenverkehr nicht überwachen. Darüber hinaus werden SSL und TLS nahezu universell eingesetzt und Benutzer können es problemlos so konfigurieren, dass nicht arbeitsbezogene Aktivitäten verborgen werden.

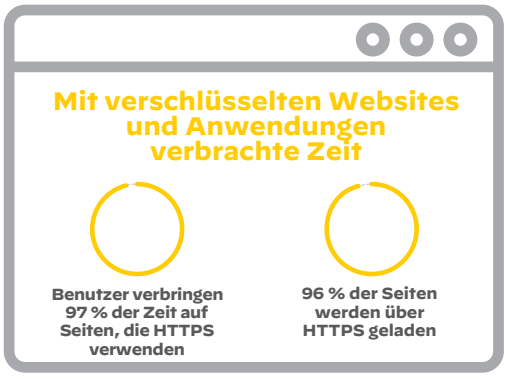

Abbildung 4: Untersuchungsergebnisse 2019 von Google zum verschlüsselten Datenverkehr[4]

3. Rajpreet Kaur, Adam Hils, John Watts, „Technology Insight for Network Security Policy Management“, Gartner, 21. Februar 2019, https://www.gartner.com/doc/3902564/technology-insight-network-security-policy.
4. „Google Transparency Report: HTTPS encryption on the web“, Google, Inc., heruntergeladen am 5. Februar 2020, https://transparencyreport.google.com/https/overview?hl=en.

Die Lösung

Die Fähigkeit, SSL zu entschlüsseln, ist eine wesentliche Sicherheitsfunktion. Die wichtigsten Faktoren, auf die Sie achten sollten, sind die Fähigkeit, sowohl ein- als auch ausgehenden Datenverkehr auf jedem Port zu erkennen und zu entschlüsseln, die Richtlinienkontrolle bei der Entschlüsselung und die Hardware- und Softwareelemente, die nötig sind, um die Entschlüsselung auf zehntausenden gleichzeitigen SSL-Verbindungen durchzuführen, ohne die Leistung zu beeinträchtigen. Ihre nächste Firewall muss so flexibel sein, dass gewisse Arten von verschlüsseltem Datenverkehr – wie HTTPS von nicht klassifizierten Websites – leicht über Richtlinien zu entschlüsseln sind, während andere Typen – wie Webdatenverkehr von bekannten Finanzdienstleistungsunternehmen – entsprechend den Datenschutzstandards unangetastet bleiben.

Eine innovative Firewall sollte Sicherheit und Loadbalancing für entschlüsselte Datenflüsse auf mehreren Sicherheitsvorrichtungen ermöglichen, um zusätzliche Sicherheit zu bieten. Dadurch werden dedizierte SSL-Offloader überflüssig, was die Komplexität des Netzwerks verringert und die Entschlüsselung vereinfacht. Eine innovative Firewall muss die Entschlüsselung fortschrittlicher Protokolle wie TLS 1.3 und HTTP/2 unterstützen, die immer weitere Verbreitung finden. Detailliere Informationen über diese wichtige Fähigkeit finden Sie in Decryption: Why, Where and How.

6. Stoppen komplexer Bedrohungen zur Verhinderung erfolgreicher Cyberangriffe

Das Problem

Der Großteil der heutigen Malware – einschließlich Varianten von Ransomware – verwendet fortschrittliche Methoden, wie z. B. das Einbringen schädlicher Nutzdaten in herkömmliche Dateien oder das Verpacken von Dateien, um sie zu verbergen, mit dem Ziel, schädliche Programme oder Exploits an Netzwerksicherheitseinrichtungen und -tools vorbeizuschleusen. Unternehmen setzen für dynamische Analysen zwar zunehmend virtuelle Sandkästen ein, Angreifer haben aber Wege gefunden, diese zu umgehen. Sie verwenden Methoden, die nach gültigen Benutzeraktivitäten, Systemkonfigurationen oder Indikatoren für bestimmte Virtualisierungstechnologien suchen. Mit dem Entstehen eines Cyberkriminalitätsuntergrunds kann außerdem jeder Angreifer, ob Anfänger oder Fortgeschrittener, Plug-and-Play-Bedrohungen erwerben, die darauf abzielen, Malwareanalyseeinrichtungen zu identifizieren und zu umgehen.

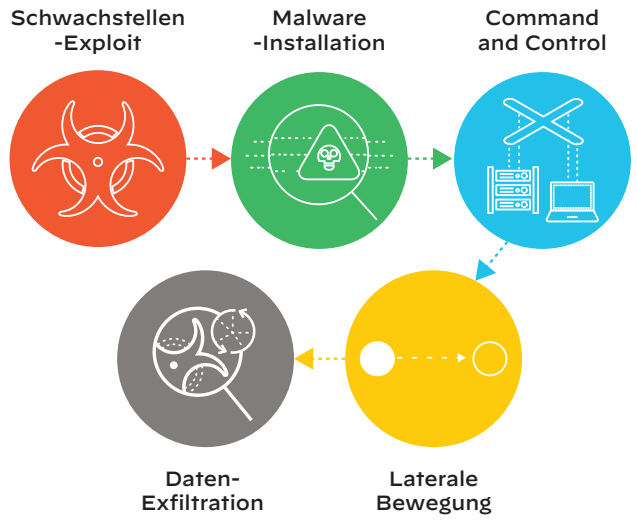

Abbildung 5: Hindernisse bei jedem Schritt, um erfolgreiche Angriffe zu verhindern

Die Lösung

Ihre Firewall sollte mit ihren integrierten Sicherheitsdiensten in der Lage sein, bekannte Bedrohungen automatisch abzuwehren. Auch unbekannte Bedrohungen müssen automatisch analysiert und bekämpft werden. Ihr Unternehmen benötigt einen Dienst, der Verhaltensmuster durch verlässliche Analysen und die Integration mit anderen Teilen Ihrer Sicherheitsinfrastruktur in Verbindung bringen kann. Auf diese Weise können Bedrohungen an jedem Punkt des Angriffszyklus identifiziert werden, und nicht nur dann, wenn Angreifer zum ersten Mal in Ihr Netzwerk eindringen. Durch das Blockieren bekannter riskanter Dateitypen oder des Zugriffs auf bösartige URLs, bevor diese Ihr Netzwerk gefährden können, verringert sich die Angriffsfläche für Bedrohungen in Ihrem Netzwerk. Ihre Firewall sollte Sie vor bekannten Exploits von Sicherheitslücken, Malware und Command-and-Control-Aktivitäten (C2) schützen, ohne dass Sie mehrere Geräte verwalten oder warten müssen, die jeweils immer nur eine Funktion haben. Signaturen sollten automatisch aktualisiert werden, sobald neue Malware auftaucht. So bleiben Sie geschützt und Ihre Sicherheits- und Notfallteams können sich auf relevante Aufgaben konzentrieren.

Eine innovative Firewall, die mehrere Analysemethoden zur Erkennung unbekannter Bedrohungen verwendet, einschließlich statischer Analyse mit maschinellem Lernen, dynamischer Analyse und Bare-Metal-Analyse, ist in der Lage, Angriffe treffsicher zu ermitteln und Umgehungsmanöver zu verhindern. Statt Signaturen, die auf bestimmten Attributen basieren, sollten Firewalls inhaltsbasierte Signaturen verwenden, um verschiedene Varianten, polymorphe Malware oder C2-Aktivitäten zu erkennen. Darüber hinaus sind C2-Signaturen, die auf der Analyse ausgehender Kommunikationsmuster basieren, wesentlich effektivere Schutzmaßnahmen, die extrem schnell skaliert werden können, wenn sie automatisch erstellt werden. Schließlich ist auch eine aus der Cloud bereitgestellte Sicherheitsinfrastruktur für die Gewährleistung der Sicherheit von entscheidender Bedeutung. Diese Sicherheitsstruktur ermöglicht die Erkennung und Abwehr von Bedrohungen im gesamten Netzwerk, an Endpunkten und in Clouds. Darüber hinaus bietet sie Ihnen Zugriff auf ein offenes Ökosystem vertrauenswürdiger Innovatoren.

7. Stoppen von Angriffen, die DNS verwenden

Das Problem

Das DNS ist ein enorm großer, oft übersehener Kanal, der für die Einschleusung von Malware, für C2 und für Daten-Exfiltration genutzt werden kann. Angreifer nutzen das weitläufige DNS-System aus und verwenden es an mehreren Punkten für einen Angriff. Laut Unit 42, dem Team für Bedrohungsforschung von Palo Alto Networks, werden fast 80 % der Malware über DNS eingeschleust, um eine Kommunikation mit einem C2-Server aufzubauen. Angreifer richten zuverlässige Befehlskanäle ein, die schwer zu identifizieren oder zu entfernen sind, da DNS eine extrem verlässliche Verbindung zu DNS-Servern herstellen kann. Sobald eine Verbindung aufgebaut ist, können Angreifer den DNS-Datenverkehr nutzen, um Malware in ein Netzwerk einzuschleusen oder Daten auszuschleusen. Zusätzlich entwickeln Angreifer Domain Generation Algorithms (DGAs), die automatisch tausende schädliche Domänen erstellen, die für C2 verwendet werden können. Da Angreifer ihre Attacken zunehmend automatisieren, ist es fast unmöglich, diese Bedrohungen zu erkennen und zu stoppen.

Die Lösung

Ihr Unternehmen kann Angriffe, die DNS verwenden, nicht einfach auf eine schwarze Liste setzen, da diese Taktik oft auf relativ statischen Bedrohungsfeeds beruht, die von bekannten schädlichen Domains gesendet werden. Ohne Analyse ist es unmöglich, extrem dynamische schädliche Domains vorherzusagen. Um Angriffe zu stoppen, die das DNS ausnutzen, ist eine Firewall der nächsten Generation erforderlich, die prädiktive Analytik und maschinelles Lernen anwendet, um unbekannte schädliche Domains dynamisch zu identifizieren.

8. Schutz der wachsenden mobilen Belegschaft

Das Problem

Die Zahl der mobilen Arbeitskräfte nimmt weiter zu, ebenso wie die Nutzung von Mobilgeräten zur Verbindung mit Geschäftsanwendungen, häufig über öffentliche Netzwerke und Geräte, was komplexen Bedrohungen Tür und Tor öffnet. Das Sicherheitsrisiko ist erhöht, wenn sich die Benutzer außerhalb des Unternehmens aufhalten, da es keine Netzwerkfirewall gibt, die Angriffe abwehrt. Das Problem wird noch komplexer, wenn die Auswirkungen von Cloud- und BYOD-Praktiken (Bring your own Device) berücksichtigt werden. Darüber hinaus mangelt es Remotestandorten und kleinen Zweigstellen oft an einheitlichen Sicherheitseinrichtungen, weil es betrieblich ineffizient und kostspielig ist, Firewalls dorthin zu verlegen oder den Datenverkehr zum Firmenhauptsitz zurückzuleiten.

Unterstützung aller Betriebssysteme

Angesichts des Trends hin zu BYOD und einer zunehmend mobilen Belegschaft ist die vollständige Unterstützung von Windows®-, macOS®-, Android®- und Linux-Umgebungen und -Daten von entscheidender Bedeutung. Die umfassende Unterstützung ermöglicht es Unternehmen, bekannte und unbekannte Malware verlässlich zu abzuwehren, unabhängig davon, welche Betriebssysteme Benutzer verwenden.

Die Lösung

Ihre mobilen Mitarbeiter und Remotearbeitsplätze benötigen Zugriff auf Anwendungen von Standorten weit außerhalb Ihres Netzwerks. Zusätzlich müssen sie vor gezielten Cyberangriffen, schädlichen Anwendungen und Websites, Phishing, C2-Datenverkehr sowie unbekannten Bedrohungen geschützt werden. Dies erfordert lückenlose Sicherheitseinrichtungen. Ihre nächste Firewall muss das erforderliche Maß an Transparenz, Bedrohungsabwehr und Umsetzung von Sicherheitsrichtlinien aufweisen, um Ihre weit verteilten Benutzer und Standorte zu schützen. Dazu muss die Firewall innovative Funktionen in der Cloud bereitstellen und sie schützen, ohne dass physische Hardware eingesetzt werden muss.

9. Erweiterung der Sicherheit auf expandierende Cloud-Umgebungen

Das Problem

Überall befinden sich Daten und Anwendungen – in Ihrem Netzwerk ebenso wie in der Cloud. Laut dem State of the Cloud Report™ von RightScale aus dem Jahr 2019 nutzen 84 % der Unternehmen mehrere Public, Private und/oder Hybrid Clouds – im Schnitt fünf verschiedene.[5] In Verbindung mit SaaS-Umgebungen müssen Unternehmen nun sensible Daten im Netzwerk und in einer Vielzahl von Cloud-Umgebungen schützen. Hinzu kommt, dass Legacy-Sicherheitstools und -methoden, die für statische Netzwerke entwickelt wurden, nicht für die Zusammenarbeit mit cloudnativen Tools oder Funktionen ausgelegt sind. Darüber hinaus bieten native Sicherheitsdienste von Cloud-Anbietern, wie Google Cloud Platform (GCP™), Amazon Web Services (AWS®) und Microsoft Azure® in der Regel nur Layer-4-Schutz und sind auf den jeweiligen Cloud-Anbieter beschränkt.

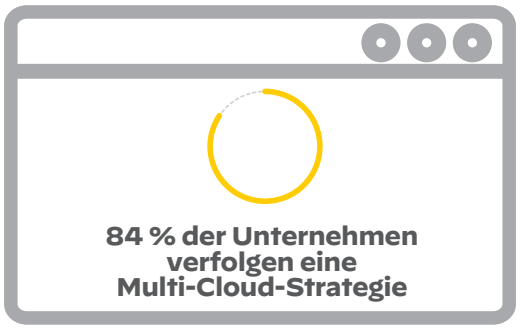

Abbildung 6: Untersuchungsergebnisse von RightScale zur Multi-Cloud-Strategie

Die Lösung

Um erfolgreich zu sein, benötigt Ihr Unternehmen eine Cloud-Sicherheitseinrichtung, die die Richtlinien konsequent vom Netzwerk in die Cloud erweitert, den Zugriff und die laterale Bewegung (Ost-West) von Malware innerhalb der Cloud verhindert, die Verwaltung vereinfacht und die Verzögerung der Sicherheitsrichtlinien bei unterschiedlichen Cloud-Workloads minimiert. Ihre nächste Firewall muss die residenten Anwendungen und Daten mit demselben Sicherheitsstatus schützen, der auch in Ihrem physischen Netzwerk vorhanden ist. Um Multi-Cloud-Implementierungen zu schützen, muss die Firewall eine Vielzahl von Cloud- und Virtualisierungsumgebungen unterstützen, darunter alle wichtigen Public-Cloud-Anbieter und virtualisierte Private Clouds. Die Firewall muss sich mit nativen Cloud-Diensten wie Amazon Lambda und Azure sowie mit Automatisierungstools wie Ansible® und Terraform® integrieren lassen, damit Ihre Cloud-First-Entwicklungsprojekte geschützt sind.

10. Einsatz einer Zero-Trust-Strategie

Das Problem

Konventionelle Sicherheitsmodelle gehen von der überholten Annahme aus, dass alles, was sich innerhalb eines Unternehmensnetzwerks befindet, vertrauenswürdig ist. Diese Modelle sind so konzipiert, dass sie die Netzwerkaußengrenze schützen. Bedrohungen, die in das Netzwerk gelangen, bleiben dabei aber unbemerkt und können sensible, wertvolle Geschäftsdaten gefährden. In der digitalen Welt ist Vertrauen ein Schwachpunkt.

Die Lösung

Wenn Sie nach einer innovativen Firewall suchen, ziehen Sie eine Firewall in Betracht, die als Segmentierungsgateway fungieren kann, um eine Zero-Trust-Architektur zu ermöglichen. Zero Trust ist eine Cybersicherheitsstrategie, bei der Vertrauen eliminiert wird. In einer Zero-Trust-Welt gibt es keine vertrauenswürdigen Geräte, Systeme oder Personen. Bei diesem Ansatz identifizieren Sie die Daten, Inhalte, Anwendungen und Dienste, die für das Unternehmen am wichtigsten sind, legen fest, wer oder was auf der Grundlage der spezifischen Funktion im Unternehmen Zugriff haben soll, und verwenden das Prinzip der geringsten Privilegien. Zu diesem Zweck verwenden Sie Netzwerksegmentierung, granulare Sicherheitsrichtlinien auf Layer 7, Benutzerzugriffskontrolle und Bedrohungsschutz.

5. « 2019 State of the Cloud Report », RightScale, 27 février 2019, https://resources.flexera.com/web/media/documents/rightscale-2019-state-of-the-cloud-report-from-flexera.pdf.

Ihre nächste Firewall sollte sich direkt an Zero Trust ausrichten und verschiedene Fähigkeiten besitzen. Dazu zählen die Ermöglichung eines sicheren Zugriffs für alle Benutzer unabhängig vom Standort, die Überprüfung des gesamten Datenverkehrs, die Durchsetzung von Richtlinien für Zugriffe nach dem Prinzip der geringsten Privilegien und die Erkennung und Verhinderung komplexer Bedrohungen. Dadurch werden die Zugriffsmöglichkeiten für Angreifer, ob innerhalb oder außerhalb Ihres Unternehmens, auf kritische Inhalte erheblich eingeschränkt. In diesem Webinar erfahren Sie, wie Sie ein Zero-Trust-System effektiv implementieren können.

11. Konsistente Zugriffskontrolle und -richtlinie auf Clouds und bei On-Premise, Remote- und mobilen Netzwerken

Das Problem

Unternehmen besitzen eine Fülle punktueller Produkte, um den verschiedenen Netzwerk- und Sicherheitsanforderungen gerecht zu werden. Jedes Produkt verfügt über eine eigene Richtlinie und Benutzeroberfläche zur Verwaltung, was zusätzliche Kosten, Komplexität und Sicherheitslücken verursacht. Darüber hinaus sind diese Produkte nicht integriert und können keine Informationen über Netzwerk- und Anwendungszugriffe oder Richtlinienverstöße weiterleiten und auch keine konsolidierten Protokolle liefern. Unternehmen finden es mitunter auch schwierig, neue Firewalleinrichtungen im großen Maßstab zu integrieren, konsistente Sicherheitsrichtlinien einzurichten und Richtlinienänderungen auf tausenden von Firewalls zu implementieren. Dieser Ansatz verursacht Lücken in der Sicherheits- und Netzwerkleistung, was Engpässe bei Personal und Budget zur Folge hat.

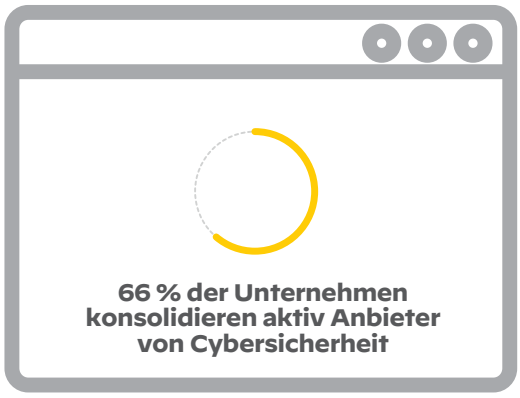

Abbildung 7: ESG-Forschungsergebnisse zur Konsolidierung der Anbieter von Cybersicherheit

Die Lösung

Laut ESG Research konsolidieren 66 % der Unternehmen aktiv Netzwerkverkehr anzuzeigen, Konfigurationen zu verwalten, globale Richtlinien bereitzustellen und Berichte über die Anzahl der Anbieter von Cybersicherheitsdiensten, mit denen sie geschäftlich zu tun haben.[6] Um erfolgreich zu sein, müssen Sie in der Lage sein, die Bereitstellung konsistenter, zentralisierter Sicherheitsrichtlinien auf zehntausenden Firewalls – einschließlich Remotestandorten, mobilen Benutzern und SaaS-Anwendungen – durch zentrale Verwaltung, konsolidierte Sicherheitsaufgaben und gestraffte Funktionen zu operationalisieren. Beispielsweise sollten Sie die Möglichkeit haben, über eine einzige Konsole den gesamten Datenverkehrsmuster und Sicherheitsvorfälle zu erstellen. Sie benötigen Reportingfunktionen, mit denen Ihre Sicherheitsmitarbeiter Netzwerk-, Anwendungs- und Nutzerverhalten im Kontext analysieren und darauf basierend fundierte Entscheidungen treffen können.

Wenn diese Fähigkeiten aus der Cloud bereitgestellt werden, erhalten Ihre Teams die Netzwerk- und Sicherheitsinfrastruktur, die in einer Architektur nötig ist, die für alles konzipiert ist: Datenverkehr, Anwendungen und Benutzer, und zwar unabhängig von ihrem Standort. In der heutigen, sich ständig ändernden Bedrohungslandschaft ist es unter Umständen nicht praktikabel, dass ein einziger Sicherheitsanbieter Ihre umfassenden Sicherheits- und Geschäftsanforderungen erfüllt. In diesem Fall ist die Fähigkeit, sich in die Daten und Innovationen Dritter zu integrieren und diese zu nutzen, von entscheidender Bedeutung. Achten Sie bei Sicherheitsanbietern auf die Erweiterbarkeit und Programmierbarkeit deren Lösung. In diesem E-Buch erfahren Sie über einen neuen Ansatz zur Sicherung von cloudfähigen Unternehmen sowie über Geschwindigkeit und Agilität bei Netzwerken und beim Unternehmensschutz.

12. Automatisierung von Routineaufgaben und Beachtung wichtiger Bedrohungen

Das Problem

Ein Bericht von Cybersecurity Ventures aus dem Jahr 2017 schätzt, dass es bis 2021 3,5 Millionen unbesetzte Stellen im Bereich der Cybersicherheit geben wird.[7] Hinzu kommt die Abhängigkeit von zu vielen manuellen Prozessen für den täglichen Sicherheitsbetrieb, wie das Aufspüren von Daten, die Untersuchung von Falschmeldungen und die Einleitung von Gegenmaßnahmen. Die manuelle Analyse und Korrelation der großen Zahl von Sicherheitsereignissen bremst die Schadensbehebung, erhöht die Fehlerwahrscheinlichkeit und ist schwer skalierbar. Sicherheitsteams können leicht in der Menge der Warnungen untergehen und die kritischen, umsetzbaren übersehen. Hinzu kommt ein drohender Mangel an qualifizierten Fachleuten in der Cybersicherheit. Big-Data-Analysen legen zwar verborgene Muster, Korrelationen und andere Einblicke offen und versorgen Sicherheitsteams mit verwertbaren Informationen, doch Sie benötigen dennoch die richtigen Daten. Die Daten müssen von überall her bezogen werden – aus Netzwerken, Endpunkten, SaaS-Anwendungen, Public Clouds, Private Clouds, Rechenzentren usw. – und für Analysen zur Verfügung stehen.

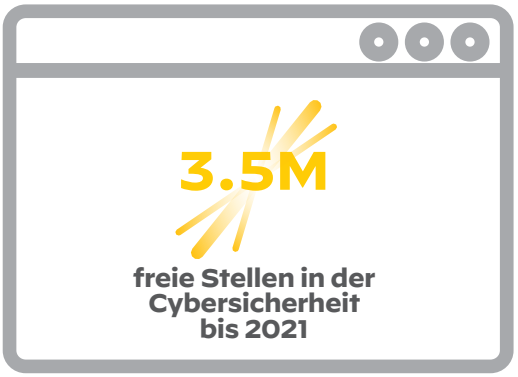

Abbildung 8: Untersuchungsergebnis von Cybersecurity Ventures zu Arbeitsplätzen im Bereich der Cybersicherheit

6. „The Cybersecurity Technology Consolidation Conundrum“, 26. März 2019, https://www.esg-global.com/blog/the-cybersecurity-technology-consolidation-conundrum.
7. „Cybersecurity Jobs Report 2018-2021“, Cybersecurity Ventures, 31. Mai 2017, http://cybersecurityventures.com/jobs.

Die Lösung

Durch den Einsatz präziser Analysen zur Verbesserung der Automatisierung können Sie auf einfache Weise Best Practices wie Zero Trust anwenden, Routineaufgaben rationalisieren und sich auf Geschäftsprioritäten konzentrieren, wie z. B. die schnellere Bereitstellung von Anwendungen, die Verbesserung von Prozessen oder die Jagd nach Bedrohungen. Automatisierung kann in drei Bereiche unterteilt werden:

1. **Workflowautomatisierung:** Die Firewall muss Standard-APIs exponieren, damit sie über etwaige andere Tools und Skripte programmiert werden kann. In der Cloud muss die Firewall in Tools wie Ansible und Terraform integriert werden können. Darüber hinaus muss die Firewall in der Lage sein, ohne manuelle Eingriffe unter Verwendung von Geräte-APIs Workflows auf anderen Geräten in Ihrem Sicherheitsökosystem zu starten.
2. **Richtlinienautomatisierung:** Die Firewall muss die Fähigkeit haben, Richtlinien an alle Änderungen in Ihrer Umgebung anzupassen, wie z. B. wenn Anwendungen auf virtuellen Rechnern verschoben werden. Sie muss auch die Möglichkeit haben, Bedrohungsinformationen aus Quellen Dritter aufzunehmen und automatisch auf der Grundlage dieser Informationen aktiv zu werden.
3. **Sicherheitsautomatisierung:** Ihre Umgebung muss in der Lage sein, unbekannte Bedrohungen aufzudecken und die Firewall zu schützen, sodass neue Bedrohungen automatisch blockiert werden.

Einige Bedrohungen sind in Daten verborgen. Wenn Sie sich diese Daten unabhängig von Standort und Bereitstellungstyp genauer ansehen, stoßen Sie möglicherweise auf Bedrohungen, die dort lauern. Mit Automatisierung haben Sie die Möglichkeit, Bedrohungen präzise zu identifizieren, eine rasche Prävention zu gewährleisten, die Effizienz zu steigern, das Know-how Ihrer Fachkräfte besser zu nutzen und die Sicherheit Ihres Unternehmens zu verbessern.

13. Koordination von Erkennungs- und Analysefunktionen mit anderen Sicherheitstools

Das Problem

Ausgeklügelte Angriffe beschränken sich nicht auf nur eine einzige Komponente Ihrer Architektur. Stattdessen besteht ihr Ziel darin, von den Endpunkten lateral zu Ihrem Netzwerk, Ihren Clouds und anderen Datenstrukturen durchzudringen, um auf wertvolle Daten zuzugreifen und diese zu exfiltrieren. Deshalb bringen isolierte Sicherheitsansätze, die nur einen Ausschnitt Ihrer Infrastruktur sehen und verstehen können, nur suboptimale Ergebnisse. Solche Ansätze beschränken die Anwendbarkeit von Analysen und zwingen Sicherheitsanalytiker dazu, zwischen Benutzeroberflächen hin und her zu wechseln im Versuch, sich manuell ein Bild vom Angriff zu machen – ein Unterfangen, das sowohl zeitaufwändig als auch fehleranfällig ist.

Die Lösung

Da die Anzahl der benötigten Sicherheitsfunktionen zunimmt, steigt auch der potenzielle Wert von Plattformen und Geräten, die eine sinnvolle Integration zwischen ihnen bieten können. Wenn Ihre Firewall als Sensor und Enforcement Point für eine umfassendere, auf maschinellem Lernen basierende Analyseplattform fungieren kann (wie bei einer XDR-Lösung), kann Ihr Sicherheitsteam komplexe Angriffe wirkungsvoller und effizienter erkennen, beheben und verhindern. Ihre nächste Firewall sollte in XDR integrierbar sein, damit sowohl Ihr Netzwerk als auch Ihr Sicherheitsteam das volle Ausmaß eines Angriffs verstehen, Bedrohungskontext und Informationen austauschen und automatisierte Reaktionen sowie eine Richtliniendurchsetzung zwischen der Firewall und anderen Enforcement Points veranlassen können.

14. Verbesserter Schutz der Konnektivität

Da immer mehr Unternehmen auf Digitalisierung setzen und Anwendungen in die Cloud verlagern, stehen IT-Teams vor der Herausforderung, Unternehmensstandorte und Niederlassungen schnell, zuverlässig und sicher mit kritischen Unternehmensressourcen zu verbinden. Software-Defined Wide Area Networking (SD-WAN) ermöglicht die Erhöhung der Bandbreite und gleichzeitig die Verbesserung von Konnektivität und Leistung, was für immer mehr Unternehmen von Interesse ist. Gartner prognostizierte, dass SD-WAN bis zum Jahr 2020 75 % der Aktualisierungen der WAN-Infrastruktur ausmachen wird.[8] SD-WAN bietet zwar viele Vorteile, bringt aber auch viele Herausforderungen mit sich, wie z. B. verminderte oder überhöhte Sicherheit, eine unerwartete Komplexität bei der Architektur und der Bereitstellung sowie unvorhersehbare Leistung.

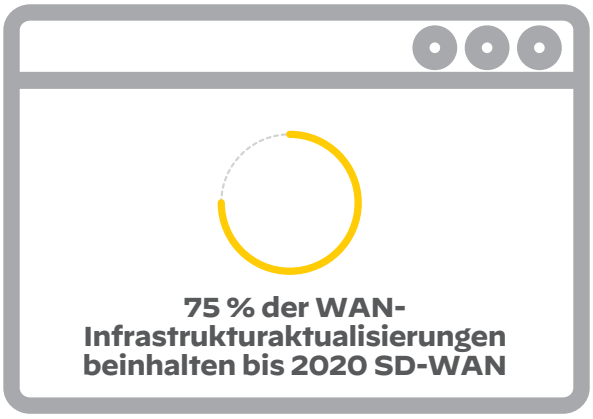

Abbildung 9: Untersuchungsergebnisse von Gartner zur Implementierung von SD-WAN

Die Lösung

Ihre nächste Firewall sollte in Ihren Zweigstellen den gleichen durchgängigen Schutz bieten wie in Ihrem Rechenzentrum und Ihren Cloud-Umgebungen. Unternehmen können SD-WAN sicher integrieren, indem sie eine Firewall implementieren, die nativ in das SD-WAN integriert ist. Damit kann die Konnektivität und Sicherheit des Unternehmens von einem zentralen Ort aus gesteuert werden. Dies kann auch helfen, dieselben konsistenten Sicherheitsrichtlinien vom Netzwerkkern auch in den Zweigstellen durchzusetzen. Da die Konfiguration und Überwachung des SD-WAN sowie die Prozesse rund um Benutzer- und Anwendungsrichtlinien der Firewall an einem zentralen Ort vereint sind, verhindern Unternehmen Sicherheitslücken und profitieren von verbessertem Schutz, größerer Einfachheit und höherer Effizienz. In diesem E-Buch können Sie nachlesen, wie Sie mit einem SD-WAN konsistenten Schutz erzielen.

8. Mike Toussaint, Ted Corbett, Andrew Lerner, „6 Critical Questions to Ask on SD-WAN“, Gartner, 6. Juni 2018, https://www.gartner.com/en/documents/3877766/6-critical-questions-to-ask-on-sd-wan.

Auswahl einer innovativen Firewall durch Angebotseinholung

Empfohlene Fragen und Erwägungen bei der Angebotsanfrage

Firewalls der nächsten Generation müssen eine breite Palette von Fähigkeiten bieten, um effiziente, effektive Sicherheit zu gewährleisten. Gleichzeitig müssen sie mit anderen wichtigen Präventions-, Erkennungs- und Reaktionstools in der gesamten Infrastruktur integrierbar sein. In diesem Abschnitt erhalten Sie eine umfassende Checkliste zu diesen Anforderungen, die Ihnen hilft, die Qualität der von Ihnen erwogenen Firewallplattformen zu evaluieren. Sie können diese Checkliste als Vorlage verwenden und an die Bedürfnisse Ihres Unternehmens anpassen. So sind Sie in der Lage, diejenigen Anbieter zu identifizieren, die den besten Schutz für Ihr Unternehmen bieten.

Identifikation von Benutzern und Gewährung von Zugriff

Kann Ihre Firewall:

- eine konsistente Sicherheitsrichtlinie für mobile Benutzer bereitstellen?
- Benutzer schützen, die sich nicht hinter einer innovativen Firewall befinden?
- mithilfe mehrerer physischer/virtueller Firewalls eine ständig aktive VPN-Verbindung unterstützen?
- über die Cloud den Schutz näher zum Benutzer bringen?

Verhindern von Diebstahl und Missbrauch von Anmeldedaten

Kann Ihre Firewall:

- die Eingabe von Unternehmensanmeldedaten auf unbekannten Websites verhindern?
- Benutzer daran hindern, Unternehmensanmeldedaten einzugeben, ohne eine Kopie des Hashes in der Firewall zu speichern?
- zuvor unbekannte Phishingwebsites schnell analysieren und den Schutz entsprechend aktualisieren?
- Benutzerversuche erfassen, bei denen Anmeldedaten in HTTP-POST-Anfragen übermittelt werden?
- Multi-Faktor-Authentifizierung (MFA) als Teil der Zugangskontrollrichtlinie unterstützen, die von der Sensibilität der Ressource abhängt, auf die zugegriffen wird?
- viele unterschiedliche Wahlmöglichkeiten bei den Technologien von MFA-Partnern bieten?
- API-Integrationen mit Technologien von MFA-Partnern unterstützen?
- eine MFA-Richtlinie für jede beliebige Anwendung, einschließlich Web-, Client-Server- und Terminal-Anwendungen, unterstützen?
- MFA-Fähigkeit bei allen Protokollen unterstützen, anstatt auf bestimmte Protokolle beschränkt zu sein ?

Sichere Aktivierung aller Anwendungen und Kontrollfunktionen

- Kann Ihre Firewall Anwendungen erkennen, die sich der Erkennung entziehen, da sie nicht standardisierte Ports verwenden, Port Hopping betreiben oder so konfiguriert sind, dass sie auf einem anderen Port laufen?
- Ist bei der Datenverkehrsklassifizierung die erste Aufgabe, die die Firewall ausführt, die Erkennung der Anwendung oder des Netzwerkports?
  - » Sind die Mechanismen zur Anwendungserkennung Teil der Klassifizierung des Datenverkehrs im Firewallkern (d. h. standardmäßig aktiviert)?
  - » Hängen die Mechanismen zur Anwendungserkennung vom Standardport der Anwendung ab?
  - » Können die Signaturen auf alle Ports angewendet werden? Wird der Prozess automatisch oder manuell konfiguriert?
- Wenn der Datenverkehr zum ersten Mal auf das Gerät trifft, wird er zuerst anhand des Ports (z. B. Port 80, der somit als HTTP angenommen wird) oder anhand der Anwendung klassifiziert (z. B. Gmail®)?
- Lassen Sie sich im Detail beschreiben, wie die Firewall Anwendungen korrekt identifiziert:
  - » Abgesehen von den Signaturen, welche anderen Mechanismen werden zur Klassifizierung des Datenverkehrs verwendet?
  - » Wie groß ist der Bereich der Anwendung und der Protokolldecodernutzung?
  - » Wie werden SSL- und SSH-Entschlüsselung und -Steuerung implementiert?
  - » Werden die Mechanismen der Datenverkehrsklassifizierung auf allen Ports gleich angewendet?
- Welche Mechanismen werden verwendet, um Anwendungen wie UltraSurf oder verschlüsseltes P2P aufzuspüren, die Sicherheitseinrichtungen absichtlich umgehen?
- Wird die Anwendungserkennung in der Firewall oder in einem sekundären Prozess nach der Klassifizierung am Port ausgeführt?
- Wird der Status der Anwendung getrackt? Wenn ja, wie wird dies genutzt, um eine konsistente Kontrolle der Anwendung und der damit verbundenen sekundären Funktionen zu gewährleisten?
- Bildet die Identität der Anwendung die Grundlage der Firewallsicherheitsrichtlinie oder ist die Anwendungskontrolle ein sekundäres Mittel der Richtlinie?
- Wie oft wird die Anwendungsdatenbank aktualisiert? Handelt es sich dabei um ein dynamisches Update oder ein Upgrade mit Systemneustart?

Schließen gefährlicher Lücken der Richtlinie

- Wird die Stateful-Inspection-Datenverkehrsklassifizierung separat vor der Anwendungserkennung durchgeführt? Wie werden nach der Identifizierung einer Anwendung Änderungen des Anwendungsstatus überwacht, erfasst und in der Richtlinie genutzt?
- Wie bietet die Anwendungsdatenbankhierarchie (flach, mehrstufig usw.) Funktionen in der übergeordneten Anwendung für detailliertere Aktivierungsrichtlinien?
- Welche Kontrollebenen gibt es bei den einzelnen Anwendungen und ihren Funktionen?
- Können portbasierte Kontrollen für alle Anwendungen in der Anwendungsdatenbank implementiert werden, sodass ein Administrator die Beziehung zwischen Anwendung und Port über Richtlinien steuern kann? Beispiel:
  - » Können Sie sicherstellen, dass nur das IT-Personal SSH und RDP verwenden darf?
  - » Ist es möglich, Malware innerhalb der Anwendung auch auf einem nicht standardmäßigen Port zu erkennen und zu blockieren?
- Welche Repositories für Unternehmensidentitäten werden für benutzerbasierte Kontrollen unterstützt?
- Gibt es eine API für die Integration von kundenspezifischen oder nicht standardmäßigen Identitätsinfrastrukturen?
- Wie können Benutzer und Gruppen die richtlinienbasierte Steuerung in Terminaldienstumgebungen implementieren?
- Sofern vorhanden, was sind die Unterschiede bei den Optionen zur Anwendungsaktivierung für Hardware und virtualisierte Instanzen?

Sicher verschlüsselter Datenverkehr

- Nach welchem Verfahren werden verschlüsselte Anwendungen auf allen Ports – auch auf nicht standardmäßigen – identifiziert?
- Welche Möglichkeiten zur Richtliniensteuerung stehen zur Verfügung, um Anwendungen, die SSL verwenden, selektiv zu entschlüsseln, zu prüfen und zu kontrollieren?
- Wird die bidirektionale SSL-Identifikation, -Entschlüsselung und -Untersuchung unterstützt?
- Ist die SSL-Entschlüsselung ein Standardmerkmal oder eine kostenpflichtige Zusatzleistung? Ist ein dediziertes Gerät erforderlich?
- Wird die SSH-Steuerung (ein Mittel zum Zugriff auf Remotegeräte) unterstützt? Wenn ja, mit welcher Steuerungstiefe?
- Welche Mechanismen werden verwendet, um Anwendungen, die Sicherheitssysteme umgehen, wie UltraSurf und Tor, zu identifizieren?
- Wie erkennt das Produkt automatisch einen Angreifer, der einen nicht standardisierten Port zur Umgehung des Sicherheitssystems benutzt?

Stoppen komplexer Bedrohungen zur Verhinderung erfolgreicher Cyberangriffe

- Unterstützt Ihr cloudbasiertes Malwareanalysesystem mehrere Analysemethoden, einschließlich der Bare-Metal-Analyse zur Erkennung von Malware, die Sandkasten umgehen kann?
- Verwendet Ihr cloudbasiertes Malwareanalysesystem einen im Unternehmen codierten Hypervisor, um Malware abzuwehren, die Sandkasten umgehen?
- Erstellt Ihr Malwareanalysesystem nach der Malwareanalyse Bedrohungsabwehrsignaturen, wie z. B:
  - » Contentbasierte AV-Signaturen zur Abwehr bekannter und unbekannter Malwarevarianten?
  - » Auf Mustern basierende Anti-Spyware-Signaturen zur Erkennung von Datenverkehr an bekannte und unbekannte C2-Infrastrukturen?
- Unterstützt Ihr cloudbasiertes Malwareanalysesystem die Malwareanalyse für Dateitypen der Betriebssysteme Windows®, Android® und macOS®?
- Ist Ihre Firewall der nächsten Generation in der Lage, ausführbare Dateien und andere riskante Dateitypen von unbekannten Anwendungen und URLs zu blockieren, um Ransomwareangriffe zu verhindern?
- Kann Ihre Firewall der nächsten Generation alle bekannten IOCs (d. h. IPs, Domains und URLs) automatisch und dynamisch in eine schwarze Liste importieren, um bekannte Ransomwarevarianten proaktiv abzuwehren?
- Werden durch die Integration der Threat Intelligence Cloud in Ihre innovative Firewall dynamische Updates für bösartige URLs unterstützt, die in der Malwarekategorie der URL-Filter-Datenbank mit Ransomware in Verbindung stehen?
- Kann Ihre Firewall etwas über Bedrohungs- oder Ransomwareverhaltensmuster von Ihrer Endpoint-Protection-Software lernen und umgekehrt?

Stoppen von Angriffen, die DNS verwenden

- Unterstützt die Integration von cloudbasierten Bedrohungsdaten in der neuen Firewall dynamische Updates für schädliche Domains im Zusammenhang mit Ransomware, indem DNS-Signaturen automatisch auf eine schwarze Liste gesetzt oder an einen Sinkhole-Server geleitet werden?

Schutz der wachsenden mobilen Belegschaft

- Was sind im Detail die verfügbaren Optionen für den Schutz von Remotebenutzern, einschließlich aller notwendiger Komponenten?
  - » Wenn eine Clientkomponente notwendig ist, wie wird sie bereitgestellt?
- Was sind Ihre Anforderungen an die Dimensionierung? Wie viele Benutzer können gleichzeitig unterstützt werden?
- Ist die Sicherheitsfunktion für Remotebenutzer für den Client transparent?
- Wie wird die Richtliniensteuerung für Remotebenutzer implementiert (in der Firewallrichtlinie, in einer separaten Richtlinie/einem separaten Gerät usw.)?
- Welche Funktionen und Schutzmöglichkeiten bieten die Remote-Einrichtungen (SSL, Anwendungssteuerung, IPS usw.)?
- Kann Ihre Firewall die Verbindung der Benutzer aufrechterhalten, um eine konsequente Richtliniendurchsetzung unabhängig vom Standort zu gewährleisten?
- Wie können Sie Benutzer mobiler Geräte ansprechen? Werden Sie in der Lage sein, eine konsistente Richtlinienumsetzung zu gewährleisten, unabhängig davon, ob sich Benutzer in externen Netzwerken oder internen drahtlosen Netzwerken befinden?
- Kann die Firewall BYOD-Aktivitäten setzen, wie z. B. die sichere Freigabe von privaten und firmeneigenen Laptops, Telefonen und Tablets?

Erweiterung der Sicherheit auf expandierende Cloud-Umgebungen

- Wie erstellt die innovative Firewall Sicherheitsrichtlinien auf der Grundlage von VM-Attributen von Arbeitslasten (virtueller Rechner, VM)?
- Kann die neue Firewall Sicherheitsrichtlinien für dynamische Arbeitslasten sowohl in Private Clouds als auch in Public Clouds erstellen?
- Kann die neue Firewall konsistente Sicherheitsrichtlinien für Arbeitslasten gewährleisten, selbst wenn sich ihre IP-Adressen oder Standorte im Rechenzentrum ändern?
- Wie wird in virtuellen Umgebungen der Datenverkehr im virtuellen Rechner (VM) klassifiziert (Ost-West, Nord-Süd)?
  - » Was sind die Integrationspunkte innerhalb der virtualisierten Umgebung?
  - » Wie sieht der Prozess der Erstellung von Sicherheitsrichtlinien für neu erstellte virtuelle Rechner aus?
  - » Welche Funktionen sind verfügbar, um Verschiebungen, Hinzufügungen und Änderungen auf virtuellen Rechnern zu erfassen?
  - » Welche Funktionen stehen für die Integration in Automatisierungs- und Orchestrierungssystemen zur Verfügung?

Einsatz einer Zero-Trust-Strategie

- Ermöglicht Ihnen Ihre neue Firewall der nächsten Generation, kontextbasierte Richtlinien zu erstellen, um zu bestimmen, wer oder was auf Ihre Schutz-Benutzeroberfläche zugreifen kann?
- Wie nutzt die innovative Firewall die Netzwerksegmentierung, verhindert laterale Bewegungen, bietet Layer-7-Bedrohungsschutz und vereinfacht granulare Benutzerzugriffskontrolle?
- Überprüft die innovative Firewall den gesamten Datenverkehr auf böswillige Inhalte und unbefugte Aktivitäten und erfasst über Layer 7 Vorfälle sowohl innerhalb als auch außerhalb des Netzwerks sowie in Cloud-Umgebungen?

Konsistente Zugriffskontrolle und -richtlinie auf allen Clouds sowie bei On-Premise, Remote- und mobilen Netzwerken

- Können lokale Administratoren direkt an der Einrichtung arbeiten und bei Bedarf Konfigurationen ändern, ohne sich bei einer zentralen Verwaltung anzumelden?
- Können zentrale Administratoren die von lokalen Administratoren vorgenommenen Änderungen überwachen und einsehen?
- Können Sie selbst entscheiden, welche Konfigurationsänderungen von Firewalladministratoren an den Firewalls bereitgestellt werden?
- Sollte eine Implementierung nicht funktionieren, können Sie dann Änderungen einzelner Benutzer wieder rückgängig machen und rasch eine funktionierende Konfiguration wiederherstellen?
- Ist im zentralen Firewallverwaltungssystem die Protokollverwaltung von der Konfigurationsverwaltung des Netzkerns getrennt und bietet dennoch umfassende Einblicke mithilfe einer zentralen Komponente?
- Können Ihre Logmanager Protokolle mit hohem Durchsatz (z. B. 50.000 LPS) aufnehmen?
- Besitzt Ihre Firewall für jede Funktion APIs, so dass Sie Konfigurationsänderungen automatisieren können?

Automatisierung von Routineaufgaben und Beachtung wichtiger Bedrohungen

- Unterstützt Ihr Sicherheitsanbieter die Fähigkeit zur automatischen Generierung von Präventionssignaturen über den gesamten Angriffslebenszyklus für alle Daten, die für Angriffe relevant sind?
- Kann Ihre Firewall infizierte Hosts im Netzwerk korrelieren und identifizieren und sie unter Quarantäne stellen, um ihren Zugriff im Netzwerk einzuschränken?
- Kann Ihre Firewall MFA aktivieren, um den Missbrauch von Anmeldedaten zu verhindern und kritische Anwendungen zu schützen?
- Kann Ihre Firewall die im Netzwerk erkannten Bedrohungen mit Daten in Verbindung bringen, die von globalen Bedrohungsinformationen stammen?

Koordination von Erkennungs- und Analysefunktionen mit anderen Sicherheitstools

Kann Ihre Firewall oder Ihr Manager:

- in einem Änderungsverwaltungssystem ein Ticket wegen eines bösartigen Ereignisses auf der Firewall erstellen?
- Eine Quarantänemaßnahme für einen infizierten Host im drahtlosen Netzwerk aktivieren?

Kann Ihre Firewall:

- vollständig per API programmiert werden?
- Benutzer-ID-Informationen über APIs von Wireless-Controllern über Hosts erfassen, die sich mit drahtlosen Netzwerken verbinden?
- dynamisch Drittpartei- oder benutzerdefinierte Bedrohungsdatenfeeds in die Firewall ohne Richtlinien-Commits integrieren?

Kann Ihre Sicherheitsarchitektur:

- die Aggregation, Konsolidierung und Deduplizierung von Bedrohungsfeeds durchführen, bevor die Indikatoren an Ihre Firewall weitergeleitet werden?
- in die neue Firewall integriert werden, um die Entfernung abgelaufener Bedrohungsindikatoren zu automatisieren und die Nutzung veralteter Bedrohungsdaten zu verhindern?
- Ihnen ermöglichen, Bedrohungsindikatoren aus den letzten APT-Kampagnen gezielt auszuwählen und Bedrohungsfeeds proaktiv in Ihre neue Firewall zu integrieren?
- Ihnen ermöglichen, cloudbasierte Bedrohungsdaten und IOCs (Indicators of Compromise) auf einer Vertrauensbewertung basierend mit Daten anzureichern, um den operativen Aufwand für die Handhabung von Falschmeldungen zu reduzieren?

Verbesserter Schutz der Konnektivität

- Mit welchen Funktionen unterstützt die neue Firewall die Sicherheit der End-to-End-Kommunikation?
- Wie gewährleistet die neue Firewall die Sicherheit des direkten Internetzugangs (DIA)?
- Wie erzwingt die neue Firewall Sicherheitsrichtlinien für Cloud-Dienste und Anwendungen, die an Zweigstellen gesendet werden?
- Wie verbessert die neue Firewall die Sicherheit von Cloud-Anwendungen und -Diensten, auf die von einer Zweigstelle aus zugegriffen wird?

Sind Sie bereit, Ihre nächste Firewall zu evaluieren? Unterziehen Sie sich einem abschließenden Test.

paloalto NETWORKS

3000 Tannery Way
Santa Clara, CA 95054

Zentrale: +1/408/75 34 000
Vertrieb: +1/866/32 04 788
Support: +1/866/89 89 087

www.paloaltonetworks.com