illumio

Der Stand der Security Segmentierung

So schützen sich Unternehmen vor lateraler Bewegung

Inhalt

illumio

Die Realität aktueller Cyberrisiken ist offensichtlich.

Motivierte Angreifer werden stets einen Weg in Ihr Unternehmen finden. Sie setzen auf bislang unbekannte Malware, nutzen effiziente Phishing-Kampagnen zum Abgreifen von Mitarbeiter-Anmeldedaten, missbrauchen Container, die ungesichert im Internet abgelegt wurden oder greifen verwundbare Software an.

Zur Normalität gehört heute aber auch, dass Angreifer sich nach dem Eindringen ins Netzwerk lateral bewegen und versuchen, wichtiges geistiges Eigentum oder vertrauliche Kundendaten zu stehlen. In anderen Fällen versuchen sie hingegen, Daten mithilfe von sich selbst lateral verbreitender Ransomware zu verschlüsseln, oder sie legen es darauf an, vertrauliche Informationen zu zerstören. Wenn die Angreifer beginnen, sich lateral im Netzwerk auszubreiten, kann aus einem kleinen Zwischenfall schnell eine schwerwiegende Sicherheitsverletzung werden.

Es gibt aber auch eine gute Nachricht.

Klug geführte Unternehmen investieren schon seit Längerem in eine moderne, gestaffelte Abwehr. Dazu gehört die Netzwerksegmentierung, die Angreifer an lateraler Bewegung innerhalb des Netzwerks hindert und Eindringlingen keine Möglichkeit zum Ausweichen lässt. Angesichts der Bedeutung von Segmentierung wollten wir wissen, wie stark sie innerhalb einer Schutzstrategie eingesetzt wird. Deshalb führten wir mit Virtual Intelligence Briefing (ViB) eine Umfrage dazu durch, wie Unternehmen die Segmentierung heute umsetzen und auf welche Schwierigkeiten sie dabei stoßen. Diese Umfrage wurde von ViB unabhängig durchgeführt. Diese interaktive Online-Community konzentriert sich auf neue und schnell wachsende Technologien und besteht aus mehr als 1,2 Millionen IT-Fachleuten und Entscheidungsträgern, die ihre Meinungen zu verschiedensten IT-Bereichen (einschließlich IT-Sicherheit) über komplexe Umfragen austauschen.

Das haben wir erfahren:

- Die heutige IT ist hybrid und nutzt lokale Rechenzentren sowie mehrere Cloud-Umgebungen.
- Bei der Behebung schwerwiegender Sicherheitsverletzungen verlassen wir uns immer noch zu sehr darauf, dass es schon nicht so schlimm wird. Mehr als die Hälfte der Umfrageteilnehmer setzt keine Segmentierung ein und hat das in den nächsten sechs Monaten auch nicht vor.
- Zwei Drittel der Umfrageteilnehmer sind der Meinung, dass die Firewall eine veraltete und kostenintensive Lösung für Segmentierung ist. Diese 90er-Jahre-Technologie kann exorbitant teuer sein.
- Überraschung! Firewall-Technologie ist nicht DevOps-freundlich und unterstützt die im Jahr 2020 aktuellen Geschäftsabläufe nicht.

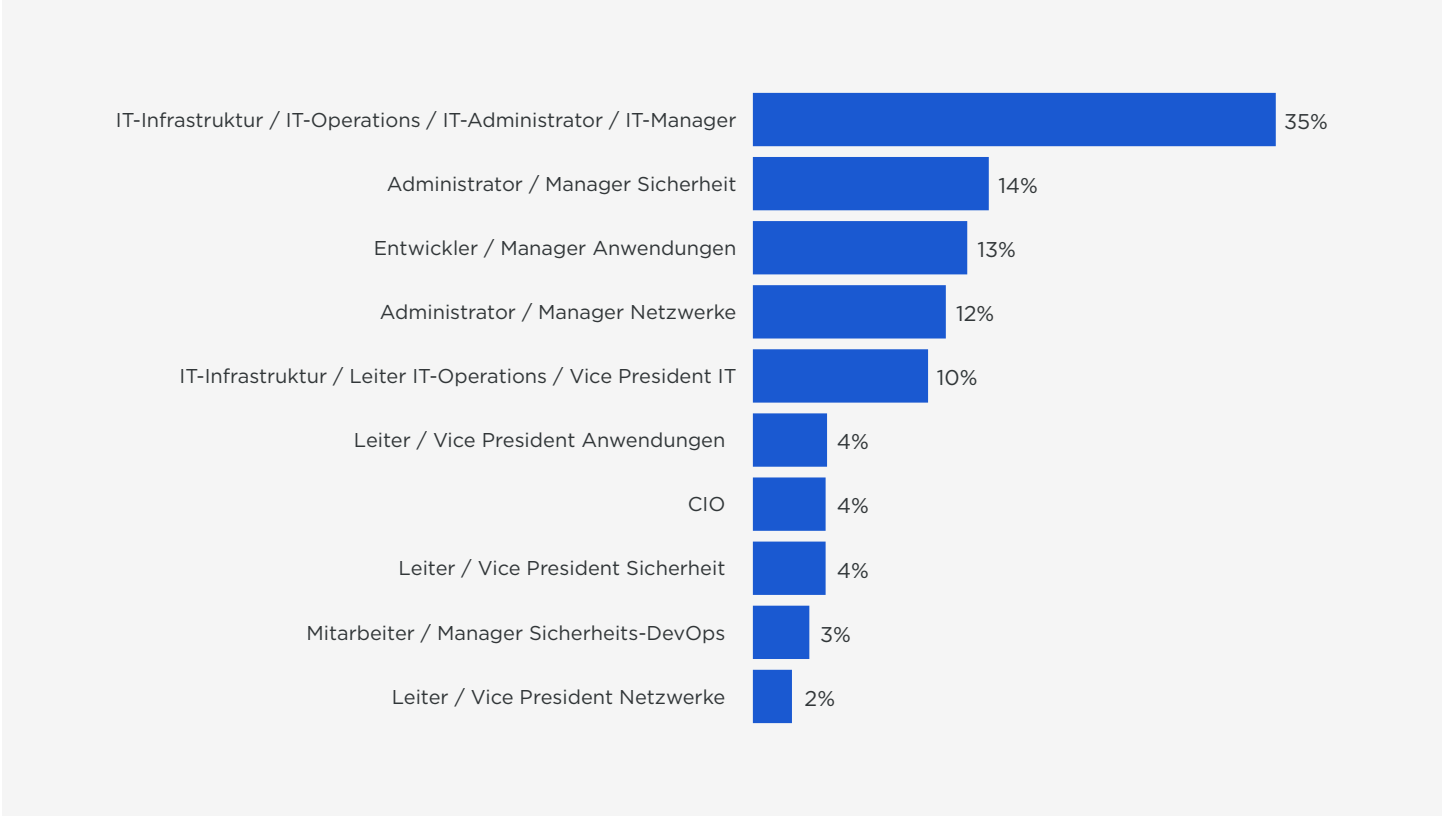
Was ist Segmentierung?

Dabei geht es um die Unterteilung eines Netzwerks in kleinere Zonen, sodass jede zu einem eigenen Segment wird. Dadurch wird Sicherheit insgesamt verbessert. Gleichzeitig werden Angreifer daran gehindert, sich lateral innerhalb von Netzwerken, Rechenzentren und Cloud-Umgebungen zu bewegen.

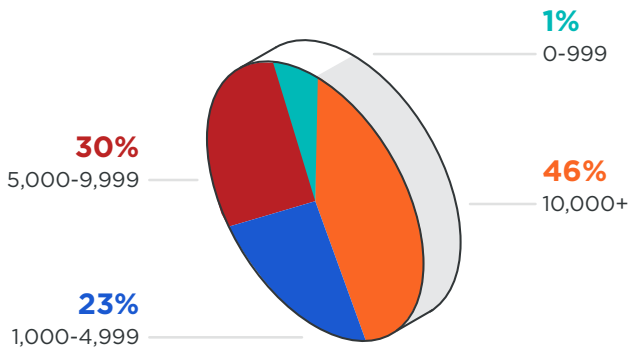
Mit wem haben wir gesprochen?

Wir sprachen mit mehr als 300 IT-Experten aus einem Querschnitt mittlerer bis großer Unternehmen, wobei die meisten Unternehmen über 1.000 Mitarbeiter hatten.

TÄTIGKEITSBEREICH



UNTERNEHMENSGRÖSSE



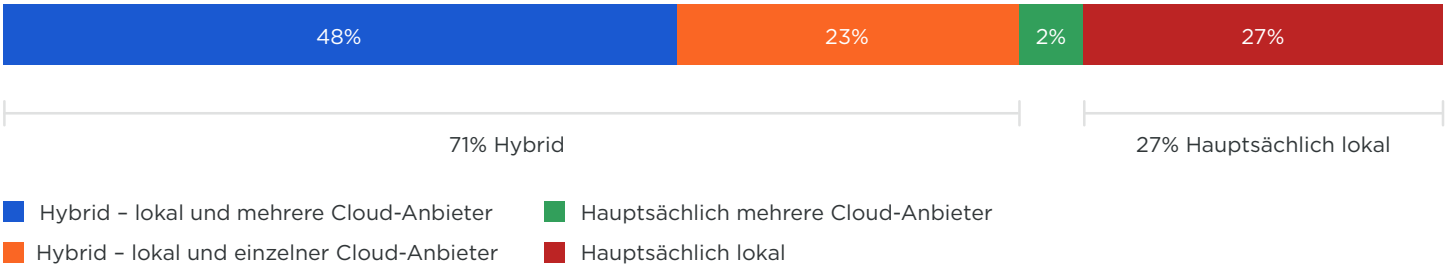
illumio

Schutz hybrider Umgebungen

Wir wollten wissen, welche Umgebungen in Unternehmen geschützt werden müssen. 71 % der Umfrageteilnehmer verwenden „hybride lokale Umgebungen“, d. h. sie nutzen sowohl Rechenzentren als auch Cloud-Umgebungen. 48 % gaben an, dass sie mehrere Cloud-Anbieter einsetzen..

Eine anwendungszentrierte Welt

Wir setzen zahlreiche Micro-Services ein, die uns meist verborgen bleiben. Wir fragten nach Anwendungen, die über Infrastrukturgrenzen hinweg verteilt sind. So lauteten die Antworten: Nur 3 % gaben an, dass Anwendungen bei ihnen nicht über mehrere Infrastrukturen hinweg betrieben werden. Allerdings sagten 30 %, dass mehr als die Hälfte ihrer Anwendungen verteilt sind, während dies bei 37 % auf 21 bis 50 % der Anwendungen zutrifft.



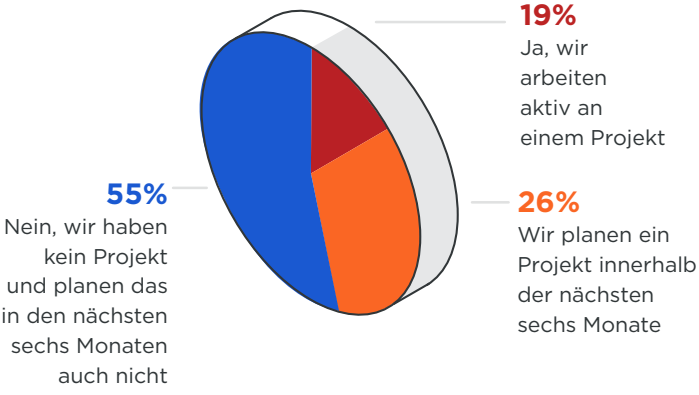
Massive Datenschutzverletzung – kein großes Problem?

Wer segmentiert heute, um das Risiko von Daten-Lecks zu verringern? Leider nur erschreckend wenige Unternehmen! Nur 19 % der befragten Unternehmen schützen sich mithilfe von Segmentierung vor Sicherheits-Vorfällen. Etwa 25 % planen aktiv ein Projekt, doch mehr als die Hälfte nutzt für den Schutz keine Segmentierung und hat das in den nächsten sechs Monaten auch nicht vor.

Erstaunliche 86 % der Teilnehmer nutzen noch Firewalls zur Segmentierung ihrer Anwendungen.

Die Firewall wurde immer noch nicht gefeuert

Wie wird Segmentierung heute eigentlich umgesetzt? Meist kommen dazu Firewalls zum Einsatz. Etwa 46 % versuchen, Segmentierung mithilfe von Software-defined Networks (SDN) zu erreichen, während 44 % auf Host-basierte Segmentierung entweder mit individuellen Host-IP-Adressen oder mithilfe der Firewalls in den Host-Betriebssystemen setzen.



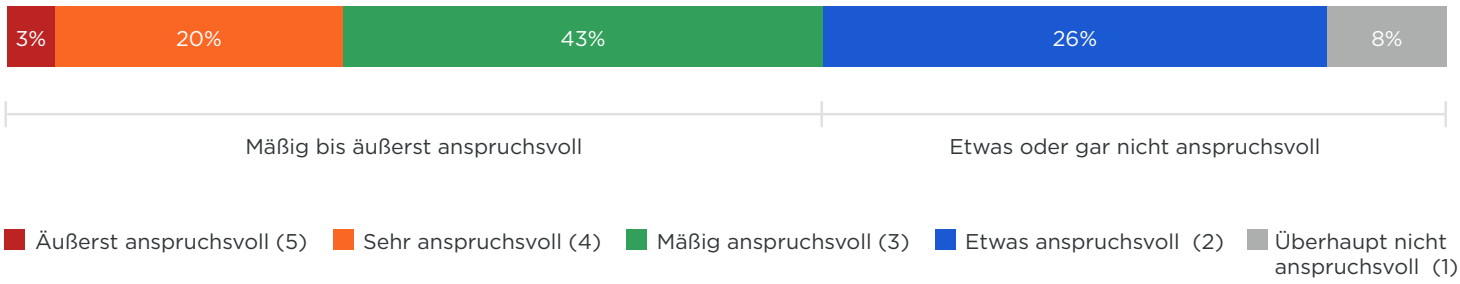
45 % arbeiten aktiv an einem Projekt oder sind in der Planungsphase

illumio

Wie anspruchsvoll ist die Verwaltung von Firewalls?

Kurz gesagt: sehr anspruchsvoll. Zwei Drittel der Umfrageteilnehmer stufen die Pflege ihrer Firewalls als äußerst anspruchsvoll ein. Zu den drängendsten Problempunkten gehörten Kosten, Fehlerbehebung, Bereitstellung und die Durchführung von Änderungen.

ALLGEMEINE SCHWIERIGKEITEN BEI DER VERWALTUNG VON FIREWALLS

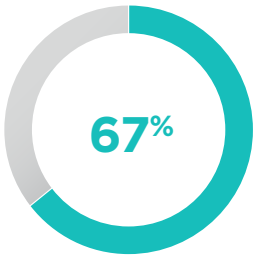


Schon gewusst?

Security Segmentierung wird 4–6 mal schneller bereitgestellt als Firewalls und Anwendungs-Updates können innerhalb weniger Stunden abgeschlossen werden.

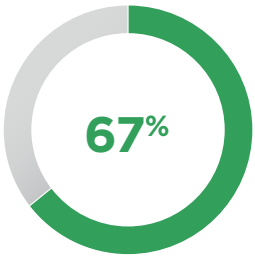
Worin liegt das Problem bei Firewalls?

Die Schwierigkeiten der Umfrageteilnehmer mit ihren Firewalls reichten von der Bereitstellung über die Budgetierung bis hin zur Implementierung von Änderungen und deren Überprüfung. So kommentierten sie ihre Probleme:



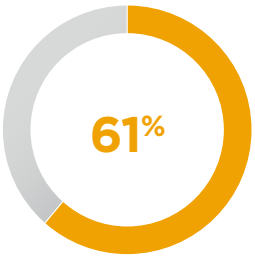
Erstimplementierung und Optimierung

67 % gaben an, dass die Erstimplementierung und Optimierung von Firewalls äußerst bis etwas anspruchsvoll ist.



Implementierung von Änderungen

67 % gaben an, dass die Implementierung von Änderungen in Firewalls äußerst bis etwas anspruchsvoll ist.



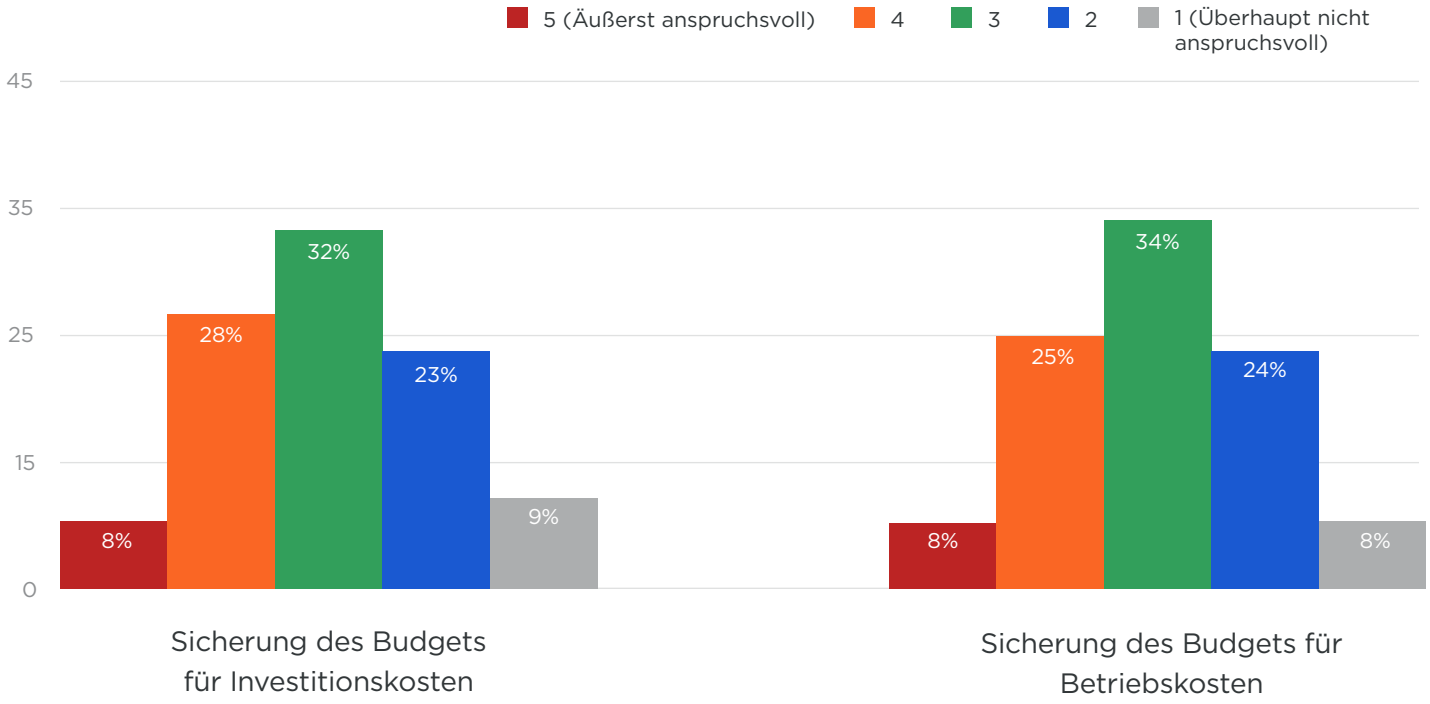
Überprüfung von Änderungen

61 % gaben an, dass die Überprüfung von Änderungen in Firewalls äußerst bis etwas anspruchsvoll ist.

illumio

„Vergoldete“ Firewalls

Eines der größten Probleme war das Loch, das die Firewall in das Budget gerissen hat. Firewalls sind teuer, und für 68 % der Umfrageteilnehmer ist es schwierig, sich die Investitionskosten zu sichern. Zudem ist ihre Pflege kostspielig: 66 % hatten auf die eine oder andere Art Schwierigkeiten, die Mittel für Betriebskosten bereitzustellen. Vielleicht ist das nicht überraschend, da Firewall-Anschaffungen im sechsstelligen Bereich liegen und ihre Implementierung und Verwaltung Millionen kostet.



Schon gewusst?

Security Segmentierung ist eine kostengünstigere und zuverlässige Option, die ins Betriebssystem integrierte Firewalls nutzt. Damit ist sie um mindestens 200% günstiger als traditionelle Segmentierung mit Firewalls.

illumio

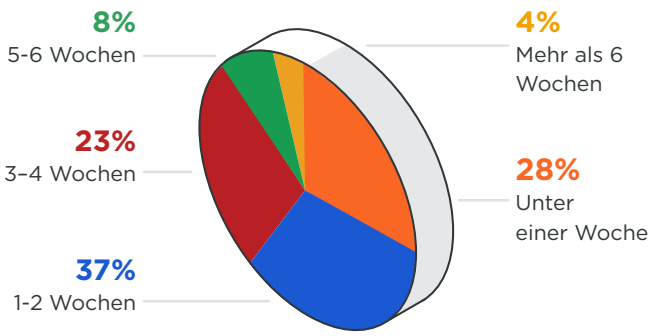
Kaputte App, zerstörte Karriere?

Es ist eine traurige Wahrheit, dass wir häufig versuchen, mit Firewall-Technologie der 90er Jahre mit DevOps Schritt zu halten. Mehr als zwei Drittel der Umfrageteilnehmer bestätigen, dass ihre Firewalls das Testen von Regeln vor der Bereitstellung erschweren, sodass es schneller zu versehentlichen Fehlkonfigurationen von Regeln und Anwendungsausfällen kommt.

Wir müssen wahrscheinlich nicht betonen, dass „mal eben“ eingeführte Code-Änderungen eilige Firewall-Regeländerungen im Rahmen des Änderungskontrollprozesses nach sich ziehen können. Allerdings dauert eine einzige Firewall-Aktualisierung zur Anpassung an eine neue Anwendung oder Anwendungsverhalten im Durchschnitt ein bis zwei Wochen.

Anpassung an neue Anwendungen

Mit einer Firewall ist es ganz einfach... den Geschäftsbetrieb zu verlangsamen, Anwendungen zu beeinträchtigen und Karrieren zu zerstören.



1–2 Wochen, im Durchschnitt 37 %

Nur 28 % der Umfrageteilnehmer konnten mit Sicherheit sagen, dass sie ihre Segmentierungs-Firewalls in weniger als einer Woche an neue Anwendungen oder Anwendungs-Updates anpassen können.

Was steckt dahinter?

Security Segmentierung erfolgt Software-basiert und ist nicht an das Netzwerk gekoppelt.

Was steckt dahinter? Dies sind einige der Vorteile:

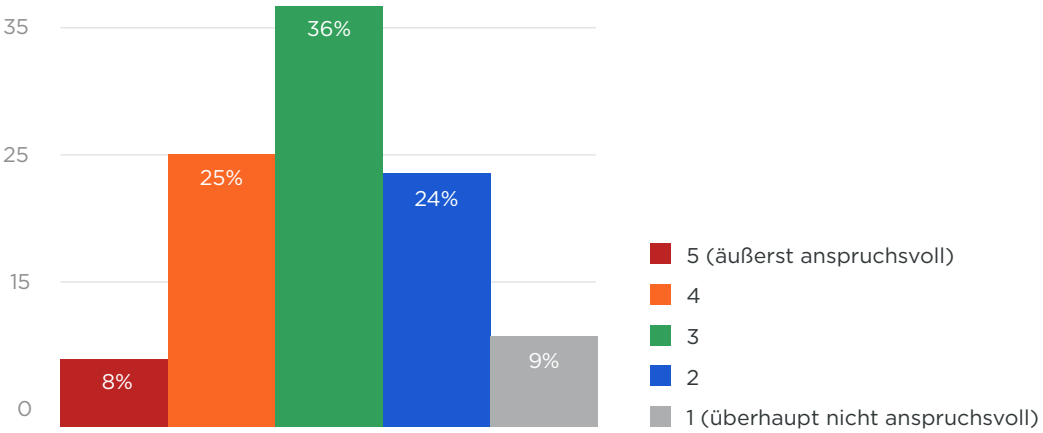
- Einfaches Testen vor der Bereitstellung, sodass keine Anwendungen beeinträchtigt werden
- 90 % weniger Regeln
- Kann innerhalb weniger Stunden aktualisiert werden

illumio

Wie lange ist zu lang?

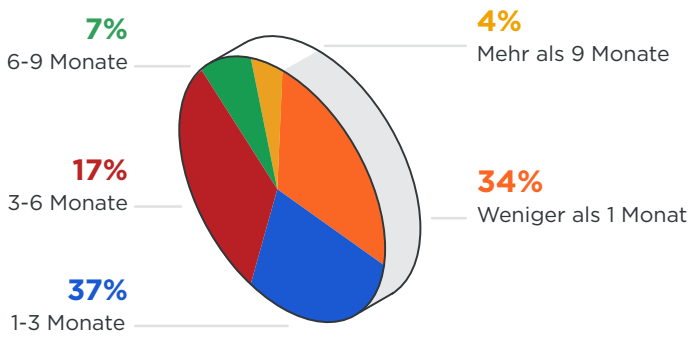
Im Schnitt dauert die Bereitstellung und Optimierung von Firewalls zur Segmentierung bei den Umfrageteilnehmern ein bis drei Monate. Warum dauert das bei Firewalls so lange? Zum einen hat es etwas mit ihrer Größe und Komplexität zu tun. Rechenzentrum-Firewalls sind riesige Systeme, die an der Laderampe abgestellt und anschließend im Rack aufgebaut und verkabelt werden. Anschließend müssen tausende komplizierte Richtlinienregeln eingerichtet, Netzwerksegmente geplant und Änderungskontrollprozesse implementiert werden. Diese gesamte Bereitstellung nimmt Monate in Anspruch.

AUFWAND BEI DER BEREITSTELLUNG UND OPTIMIERUNG



Erstimplementierung und Optimierung

DAUER DER IMPLEMENTIERUNG UND OPTIMIERUNG VON FIREWALLS



1–3 Monate, im Durchschnitt 37 %

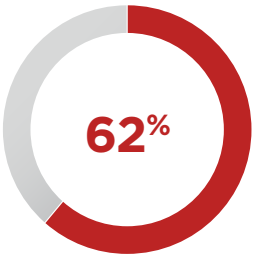
illumio

Wie viel ist zu viel?

Je mehr, desto besser... galt bei Firewall-Regeln noch nie. 62 % der Unternehmen setzen bei jeder für Segmentierung verwendeten Firewall mehr als 1.000 Regeln ein. Da Unternehmen häufig über mehrere Standorte und Firewalls verfügen, überrascht es kaum, dass einige große Unternehmen hunderttausende Firewall-Regeln nutzen.

Es ist kaum möglich, diese gigantischen Regelsätze zur Segmentierung zu beherrschen. Viele Regeln existieren schon seit Jahren, sodass niemand Hand anlegen möchte – aus Angst, dass es zu Unterbrechungen kommt.

62 % der Unternehmen setzen bei jeder für Segmentierung verwendeten Firewall mehr als 1.000 Regeln ein.



62 % der Unternehmen setzen bei jeder für Segmentierung verwendeten Firewall mehr als 1.000 Regeln ein.

illumio

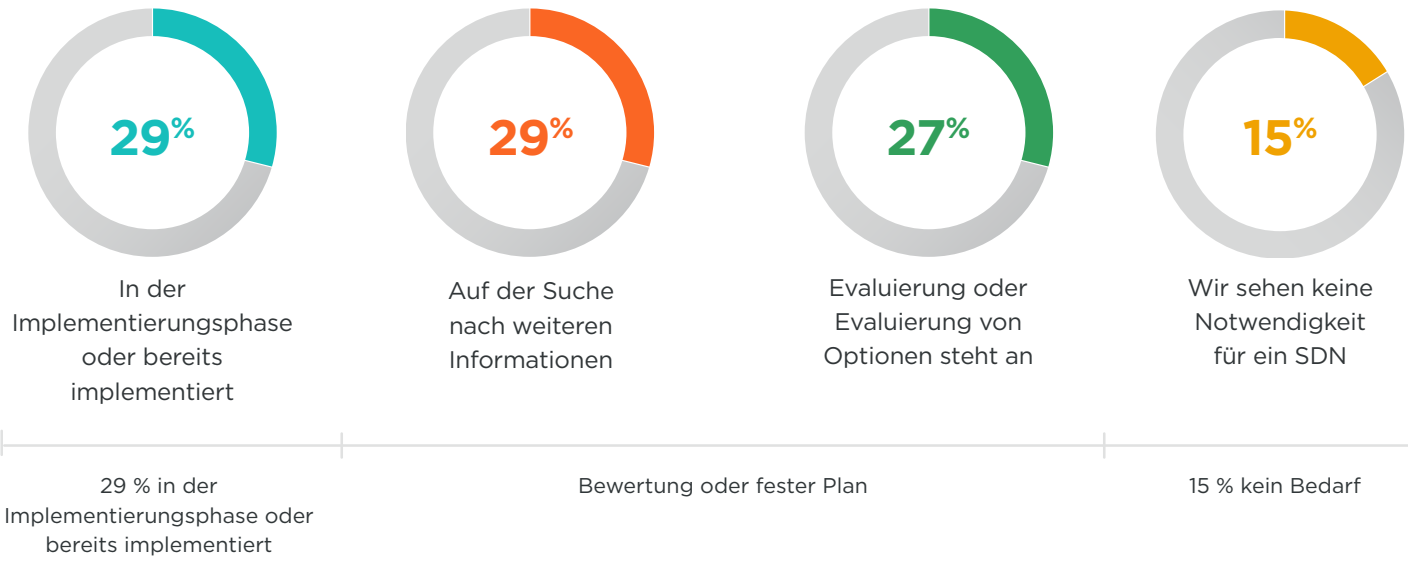
Warum dieses Festhalten an Firewalls?

Weil Änderungen, selbst wenn sie ein positives Ergebnis haben, unangenehm sind. 57 % der Umfrageteilnehmer nannten potenzielle Risiken aufgrund von Änderungen als Hauptgrund für das Festhalten an Firewalls. Viele sorgen sich auch um Widerstand gegen Änderungen im Unternehmen, mögliche Probleme sowie den dadurch verursachten Ärger mit der Fehlerbehebung.

Das unerfüllte Versprechen von SDN

Trotz der Bedenken in Bezug auf die Abkehr von Firewalls evaluieren die meisten Unternehmen gerade Software-definierte Netzwerke. Einige denken darüber nach, sie auch für einfache Segmentierung zu nutzen. Fast 30 % der Unternehmen sind gerade in der Implementierungsphase oder haben die Implementierung bereits abgeschlossen.

AKTUELLER STAND SOFTWARE-DEFINIERTER NETZWERKE (SDN)



Diese Anbieter-neutrale Umfrage wurde von Virtual Intelligence Briefing (ViB) unabhängig durchgeführt. ViB ist eine interaktive Online-Community, die sich auf neue und schnell wachsende Technologien konzentriert. Sie besteht aus mehr als 1,2 Millionen IT-Fachleuten und Entscheidungsträgern, die ihre Meinungen zu verschiedensten IT-Bereichen (einschließlich IT-Sicherheit) über komplexe Umfragen austauschen. Die verwendete Umfragemethode integriert umfangreiche Qualitätskontrollmechanismen auf drei Ebenen: Targeting, Verhalten innerhalb der Umfrage und A nalyse nach der Umfrage Die berechnete Fehlertoleranz liegt bei ca. 3,4 %. Die effektive Fehlertoleranz liegt aufgrund umfangreicher Qualitätskontrollen zur Gewährleistung einer hohen Datenqualität bei ca. 2,7 %. Weitere Informationen zu den Untersuchungsmöglichkeiten von ViB finden Sie unter https://vibriefing.news/research-services/.

illumio

Die letzte Grenze... für die Segmentierung

Trotz ihrer Unzulänglichkeiten bei der Segmentierung sind Firewalls immer noch eine bekannte Größe – wenn sich denn Unternehmen überhaupt für Segmentierung interessieren, um Schlagzeilen-trächtige Sicherheitsverletzungen zu vermeiden. Wie wir festgestellt haben, werden alternative Ansätze wie Host-basierte Sicherheitssegmentierung, die Firewalls in den Workload-Betriebssystemen zum besseren Schutz von Rechenzentren und Cloud-Umgebungen nutzt, durchaus ins Auge gefasst.

Der Vorteil dieses Ansatzes:

- Erstklassiger Schutz vor lateralen Datenschutzverletzungen in Rechenzentren und Cloud-Umgebungen
- Keine Bindung an das Netzwerk
- Einfache und schnelle Implementierung
- Möglichkeit zum Testen von Regeln vor der Bereitstellung
- Keine Gefahr der Beeinträchtigung von Anwendungen
- Kostengünstig
- Einfache Bedienung

Illumio bietet Unternehmen eine Zukunft ohne schlagzeilenträchtige Sicherheitsverletzungen – durch Transparenz, Segmentierung und Kontrolle der gesamten Netzwerkkommunikation für alle Rechenzentren sowie Cloud-Umgebungen. Illumio wurde 2013 gegründet und kann mit der Adaptive Security Platform® die laterale Bewegung der Angreifer innerhalb des Netzwerks zuverlässig stoppen. Dazu nutzt Illumio die Echtzeit-Zuordnung von Anwendungsabhängigkeiten zusammen mit Sicherheitssegmentierung für Container, virtuelle Maschinen und Bare-Metal-Umgebungen. Die weltweit größten Unternehmen wie Morgan Stanley, BNP Paribas, Salesforce und Oracle NetSuite vertrauen auf Illumio zur Reduzierung des Cyberrisikos. Weitere Informationen finden Sie unter www.illumio.com/what-we-do