FORTINET

Netzwerk-Betrieb vereinfachen und automatisieren

Inhaltsverzeichnis

Zusammenfassung

Die rasche Einführung neuer digitaler Innovationen wie Cloud-Dienste und IoT-Geräte (Internet der Dinge) führt zu immer komplexeren, fragmentierteren Netzwerk-Infrastrukturen. Gleichzeitig sind die meisten Unternehmen mit einem Fachkräftemangel und zunehmend strengeren Compliance-Anforderungen konfrontiert. Diese wachsende betriebliche Komplexität lässt sich nur mit der Einfachheit und Effizienz einer integrierten Architektur bewältigen. Eine Integration der Security ermöglicht ein zentrales Management, Echtzeit-Analysen, die Automatisierung manueller Arbeitsabläufe und des Netzwerk-Betriebs und vereinfacht zudem die Bereitstellung sowie Auditing- und Reporting-Prozesse, um behördliche Vorgaben zu erfüllen.

Durch Netzwerk-Integration die Komplexität meistern

Netzwerk-Verantwortliche kennen das Problem: Der Schutz der Infrastruktur wird durch die steigende Komplexität zunehmend erschwert. Die Fülle isolierter Netzwerk- und Security-Einzelprodukte geht zu Lasten der Transparenz und einer koordinierten Bedrohungsabwehr. Dazu kommt der weltweit anhaltende Fachkräftemangel im Security-Bereich – dem Unternehmen fehlen die Mitarbeiter und die Fachkompetenz, um die verschiedenen Security-Tools richtig einzusetzen. Außerdem erfordern immer strengere Compliance-Anforderungen oft manuelle Zusammenstellungen für Berichte und Audits, was bereits am Limit arbeitende Teams zunehmend belastet.

Die Einführung einer integrierten Netzwerk-Security-Infrastruktur ist der erste Schritt zur Lösung dieser kritischen Probleme. Eine solche Architektur, die alle im Unternehmen implementierten Lösungen miteinander verbindet, bildet die Grundlage für wichtige Funktionen wie eine einfachere Bereitstellung, ein zentrales Management, Analysen für die gesamte Sicherheitsstruktur, nahtlose Compliance-Berichte und automatisierte Betriebsabläufe.

Über ein Viertel (27 %) der Netzwerk-Verantwortlichen beklagen die mangelnde Transparenz über die gesamte Angriffsfläche.[1]

Einfachere Bereitstellung

Mit einer integrierten Security-Architektur erhalten Unternehmen erweiterte Funktionen für eine koordinierte Sicherheit bei Bereitstellungen und Konfigurationen. Das verringert viele Komplexitätsprobleme wachsender Unternehmen – und verbessert zugleich die Effizienz bzw. Betriebsabläufe und entlastet personell begrenzte IT-Teams. Insbesondere beim Zusammenlegen von Netzwerken nach Fusionen und Übernahmen oder der Eröffnung neuer Standorte lässt sich die Security mit automatisierten Onboarding-Funktionen schnell und nahtlos für alle Bereiche des erweiterten Unternehmensnetzwerks skalieren.

Eine effektive Security-Architektur sollte Funktionen wie eine Zero-Touch-Bereitstellung unterstützen, damit Unternehmen neue Standorte schneller und einfacher in das Netzwerk einbinden können. Mit einer Zero-Touch-Bereitstellung kann ein Security-Gerät – z. B. eine Next-Generation-Firewall (NGFW) – einfach in einer Filiale oder einem entfernten Standort angeschlossen und dann automatisch von der Zentrale aus über eine Breitbandverbindung konfiguriert werden, ohne dass extra ein IT-Team vor Ort sein muss. Auch können vorhandene Konfigurationen als Vorlage verwendet werden, um umfassende Implementierungen in neuen Filialen und Remote-Standorten zu beschleunigen.

Zentrales Management

Für den Netzwerk-Betrieb müssen Datenbewegungen überwacht und anomale Aktivitäten identifiziert werden können. Das wird jedoch durch eine komplexe Security erschwert. Unternehmen nutzen durchschnittlich 47 verschiedene Security-Lösungen und -Technologien, von denen viele nur für einen einzigen Angriffsvektor oder eine Compliance-Anforderung angeschafft wurden.[2] Isolierte Geräte in einer disaggregierten Security-Architektur kommunizieren nicht miteinander und können keine Bedrohungsinformationen austauschen.
Die Folge: Netzwerk-Teams müssen ständig zwischen den Management-Konsolen verschiedener Anbieter hin- und herwechseln. Ein klarer, einheitlicher und rechtzeitiger Einblick in die Vorgänge im gesamten Unternehmen lässt sich so unmöglich gewinnen.

Eine integrierte Security-Architektur mit zentralisierten Management-Funktionen vereinfacht die Transparenz und Kontrolle. Sie konsolidiert mehrere Management-Konsolen, die bislang zur Verwaltung der vielen Einzelgeräte in einer disaggregierten Architektur notwendig waren. Eine effektive Management-Lösung sollte daher eine zentrale Konsole für einen Überblick über alle implementierten Lösungen bieten. Nur so lässt sich das Netzwerk unternehmensweit schützen und eine richtlinienbasierte Kontrolle einfach, konsequent und einheitlich durchsetzen. Da über die Hälfte (52 %) aller Sicherheitsverletzungen auf Mitarbeiter- oder Systemfehler (und nicht auf bösartige oder kriminelle Absichten) zurückgehen,[3] trägt ein zentrales Management aller Unternehmensnetzwerke dazu bei, dass Netzwerk-Verantwortliche sicherheitsrelevante Konfigurationsfehler – und damit die Gefahr von Schwachstellen und Netzwerk-Ausfällen – drastisch reduzieren können.

Zwei Drittel der Unternehmen (66 %) konsolidieren aktiv die Anzahl ihrer Cyber-Security-Anbieter, um die betriebliche Effizienz zu steigern und Kosten zu senken.[4]

Analysen in Echtzeit

Steigt die Anzahl der Unternehmensfilialen, wächst auch die Angriffsfläche am Netzwerk-Rand. Netzwerk-Verantwortliche müssen sich daher zunehmend auf Echtzeit-Analysen verlassen, um Netzwerk- und Sicherheitsrisiken umgehend bewerten und identifizieren zu können. Erreichen lässt sich dies mit einer integrierten Security-Architektur, die Daten aus allen Teilen der implementierten Infrastruktur koordiniert, um umfassende Übersichten über den Netzwerkverkehr, Anwendungen und den allgemeinen Zustand des Netzwerks zu liefern.

Funktionen wie ein unternehmensweites Konfigurations-management und rollenbasierte Zugriffskontrollen (RBAC) können dem Operations-Team und Netzwerk-Verantwortlichen dabei helfen, Änderungen einfacher zu verfolgen und menschliche Fehler zu minimieren. Auch lassen sich eine SLA-Protokollierung für Service-Level-Vereinbarungen, eine rückblickende Vorgangsüberwachung (History Monitoring), anpassbare SLA-Warnungen, Monitoring-Berichte zur Netzwerk-Bandbreite und adaptive Response-Handler für Netzwerk-Ereignisse implementieren.

Compliance Reporting

Nahezu alle Compliance-Bestimmungen erfordern eine Dokumentation. Ein solider Audit-Trail, der jeden Vorfall, jede Aktion und jedes Ergebnis verfolgt, liefert dem Unternehmen die Daten, um die Einhaltung von Vorschriften nachzuweisen. Das Compliance-Management ist jedoch häufig ein stark manueller, arbeitsintensiver Prozess, der je nach Branche und Unternehmen oft mehrere Vollzeitkräfte über Monate beschäftigt.

In Unternehmen mit vielen Security-Einzelprodukten müssen für korrekte Compliance-Berichte die Daten pro Gerät zusammengestellt und anschließend normalisiert werden. Dafür müssen Operations-Teams die Sicherheitskontrollen mithilfe der Audit-Tools jedes einzelnen Anbieters über-wachen und diese Informationen anschließend korrelieren, um die Konformität nachzuweisen. Diese komplexen, umständlichen Auditing-Prozesse sind ineffizient und führen aufgrund menschlicher Fehler sehr häufig zu unbrauchbaren Ergebnissen.

Zwei Drittel (66 %) der Security-Experten geben an, dass Compliance-Vorgaben einer der Hauptgründe für Investitionen in die Sicherheit sind.[5]

Durch die Automatisierung des Compliance-Trackings und -Reportings im Rahmen des Netzwerk-Betriebs lassen sich diese Prozesse rationalisieren. Personell begrenzte Netzwerk- und Security-Teams können sich so auf kritischere Betriebsaktivitäten konzentrieren. Eine effektive Lösung für das Security-Management sollte Compliance-Vorlagen für Best Practices und bestimmte Vorschriften umfassen, um die Kosten und den Arbeitsaufwand aufgrund der Komplexität zu reduzieren. Insbesondere sollte die Lösung Echtzeit-Berichte für Branchenvorschriften wie PCI DSS (Payment Card Industry Data Security Standard) liefern können. Sicherheitsstandards wie NIST (National Institute of Standards and Technology) und CIS (Center for Internet Security) sollten ebenfalls unterstützt werden.

Ein effektives Security-Management sollte auch Tools bieten, mit denen Netzwerk-Verantwortliche ihre Umgebung anhand von branchenüblichen Best Practices bewerten können. Dieser Prozess umfasst u. a. die Aggregation und Abstimmung von Bedrohungsdaten aus mehreren Quellen. Für Operations-Teams sind solche Empfehlungen hilfreich, um einen effektiven Bedrohungsschutz zu realisieren.

Datenschutzbestimmungen haben den Schutz personenbezogener Daten stärker in den Fokus gerückt: 59 % der Security-Experten geben an, dass dies jetzt höchste Priorität hat.[6]

Netzwerk-Automatisierung

Laut einer aktuellen Studie fehlen weltweit 4,07 Millionen Cyber-Security-Experten. 65 % der Unternehmen berichten von einem Fachkräftemangel in kritischen Bereichen.[7] Infolgedessen benötigen Analysten mehr Zeit für Untersuchungen, Fehlerbehebungen bleiben aus und Vorfälle werden uneinheitlich ohne langfristige Strategie angegangen.

Weltweit muss der Fachkräfte-Pool im Bereich Cyber-Security um 145 % wachsen, um den aktuellen Bedarf an Cyber-Sicherheitsexperten zu decken.[8]

Mit einer integrierten Security profitieren Sie von einer leistungsstarken Automatisierung für das gesamte Netzwerk. Sie erhalten eine koordinierte Bedrohungsabwehr, die selbst mit personell begrenzten Teams einen effektiven Schutz gewährleistet. Automatisierte Workflow-Optimierungen eliminieren manuelle Schritte, die das Eingreifen von Mitarbeitern erfordern (wie die Alarmkorrelationen und Untersuchungen) und verringern so das Zeitfenster zwischen der Erkennung und Abwehr von Bedrohungen. So lassen sich auch Betriebsanomalien vermeiden, die auf menschliche Fehler zurückgehen. Funktionen zur gemeinsamen Nutzung und Automatisierung von Bedrohungsdaten sind heutzutage für den Schutz von Daten und Vorgängen von entscheidender Bedeutung.

Nach einer vierjährigen Studie zu Einsparungen bei den Sicherheitskosten eröffnet die Automatisierung die zweithöchste Nettoeinsparung bei den befragten Unternehmen.[9]

Weiterentwicklung zum automationsgesteuerten Netzwerk-Management

Eine integrierte Architektur kann zur Lösung von Komplexitätsproblemen beitragen und durch ein stärker automatisiertes Netzwerk-Management den Hauptursachen von Cyber-Sicherheitsverletzungen (wie Systemstörungen, Fehlkonfigurationen und menschliche Fehler) proaktiv entgegenwirken.

Dazu gehören auch einfachere Bereitstellungsfunktionen, ein zentrales Management, Analysen, erweiterte Tools für Compliance-Berichte und eine netzwerkfähige schnellere Bedrohungsabwehr – und zwar in allen Teilen des Netzwerks (On-Premises, in der Cloud und in Hybrid-Umgebungen). Das Fabric Management Center von Fortinet, das den FortiManager und FortiAnalyzer umfasst, bietet diese Funktionalität. Netzwerk-Administratoren profitieren hiermit – dank der zentralen Monitoring-Übersicht über die gesamte Fortinet Security-Fabric-Infrastruktur – von effizienteren Betriebsabläufen.

Bei der Bewertung von Lösungen sollten alle Teams prüfen, welche Investitionen die größten Vorteile hinsichtlich Effizienzsteigerung, Risikominimierung und Kostensenkungen – Stichwort „TCO“ – bringen. Mit einer integrierten Netzwerk-Security-Architektur, die Automatisierungsfunktionen priorisiert, lassen sich „Dauerprobleme“ infolge einer komplexen Infrastruktur erfolgreich lösen.

[1] „Cybersecurity and the Network Engineering and Operations Leader: A Report on Current Priorities and Challenges“. Fortinet, 4. September 2019.

[2] „53% of enterprises have no idea if their security tools are working“. Help Net Security, 31. Juli 2019.

[3] „2019 Cost of a Data Breach Study“. Ponemon Institute und IBM Security, Juli 2019.

[4] Jon Oltsik: „The cybersecurity technology consolidation conundrum“. CSO, 26. März 2019.

[5] Michael Nadeau: „Compliance mandates, cybersecurity best practices dominate 2019 security priorities“. CSO, 23. Oktober 2019.

[6] Ebd.

[7] „Strategies for Building and Growing Strong Cybersecurity Teams: (ISC)² Cybersecurity Workforce Study 2019“. (ISC)², November 2019.

[8] Ebd.

[9] Kelly Bissell, et al.: „The Cost of Cybercrime: Ninth Annual Cost of Cybercrime Study“. Accenture und Ponemon Institute, 6. März 2019.

www.fortinet.com/de

667870-0-0-DE

31. August 2020, 8:42 Uhr