Checkliste: Wie Fortinet CIOs beim Vereinfachen der Security unterstützt

CIOs werden an der Schnelligkeit ihres Handelns gemessen. Dinge wie Cloud-Anwendungen und intelligente Entwicklungsabläufe (DevOps) beschleunigen Geschäftszyklen und ermöglichen vollkommen neue Funktionen.

Aber schnelles Handeln ohne die richtige Cyber-Security gefährdet das Unternehmen: Durch dieselben digitalen Innovationen, die die Produktivität steigern, können Risiken entstehen, die der CIO in den Griff bekommen muss. Denn Datenpannen können weitreichende Folgen haben: 1) Datendiebstahl oder Zahlung von Lösegeld, um Daten freizugeben, 2) Ausfallzeiten, 3) Image-Schäden, 4) Rechtskosten sowie 5) Bußgelder und Strafen.

7 Wege, wie Fortinet die Security vereinfacht

Fortinet unterstützt CIOs dabei, die Komplexität der Netzwerk-Security zu verringern und zugleich die Kosten zu senken, die mit dem ständigen Hinzufügen isolierter Einzelprodukte bei neuen Bedrohungen oder Risiken einhergehen.

☑ Integrierte Sicherheit

Die Fortinet Security Fabric integriert Sicherheitslösungen in die gesamte Sicherheitsinfrastruktur, um die Komplexität zu verringern und Reaktionen auf Bedrohungen in nahezu Echtzeit zu ermöglichen. Die Grundlage bildet ein offenes Ecosystem. Dieses umfasst auch Drittlösungen, um den Schutz zu verstärken und gleichzeitig bisherige Investitionen in die Security zu maximieren.

☑ Transparenz und Kontrolle

Fortinet bietet eine integrierte Security, die auf die jeweilige Angriffsfläche abgestimmt ist – vom Rechenzentrum über die Cloud bis hin zum Netzwerk-Rand. Dies ermöglicht Transparenz und Kontrolle über die gesamte Angriffsfläche und jedes einzelne Sicherheitselement. Das Security-Management erfolgt über eine zentrale Konsole.

☑ Threat Intelligence in Maschinengeschwindigkeit

Die Security Fabric bietet den Rahmen für den schnellen Informationsaustausch zur Abwehr komplexer polymorpher Bedrohungen und Multivektor-Angriffe. Auch automatische Erkennungs-, Schutz- und Korrekturmaßnahmen werden unterstützt.

☑ Absichtsbasierte Segmentierung

Da wichtige Informationen heutzutage in immer größeren Netzwerken verfügbar sind, müssen Unternehmen den Zugriff auf Daten anhand der Geschäftsabsicht regeln. Eine absichtsbasierte Segmentierung ermöglicht eine engmaschige Zugriffskontrolle (Wer? Was? Wo?), eine kontinuierliche Gefahrenbewertung und eine automatisierte Bedrohungsabwehr. Auch erhalten IT-Teams damit Kontrolle über den Netzwerk-Traffic in „Ost-West“- und „Nord-Süd“-Richtung.

☑ Automatisierte Workflows

Dank der integrierten Security lässt sich die gesamte „Kill-Chain“ automatisieren – einschließlich Management von Sicherheitsinformationen und -ereignissen, Zero-Touch-Bereitstellung und der Netzwerk-Zugriffskontrolle. Die Automatisierung von Sicherheitsprozessen entlastet das IT-Team von täglichen Log-Überprüfungen und anderen manuellen Aufgaben. Mitarbeiter können sich so stärker auf geschäftskritische Aktivitäten konzentrieren. Zudem ermöglichen automatisierte Workflows das Erkennen, Verhindern und Abwehren von Bedrohungen in Echtzeit.

☑ Risiko-Management

Nicht alle Schwachstellen können in Echtzeit gepatcht werden. CIOs benötigen ein proaktives Risiko-Management mit dynamischen Dashboards, die die Gefährdung durch jede Schwachstelle aufzeigen. Fortinet bietet genau das – gemeinsam mit Prozessen zur Verhinderung, Erkennung und Reaktion auf Sicherheitsvorfälle. Diese Prozesse tragen dazu bei, das Risiko zu minimieren, Probleme schneller zu lösen und Sicherheitsstandards einzuhalten.

☑ Automatisiertes Tracking und Reporting

Fortinet bietet integrierte Kontrollfunktionen für Regulierungs- und Sicherheitsstandards sowie Tools für die Nachverfolgung, Berichterstellung und Audits, mit denen CIOs einen proaktiven Ansatz zur Compliance-Einhaltung verfolgen können. Das automatisierte Reporting umfasst Branchenvorschriften wie PCI DSS (Payment Card Industry Data Security Standard), das Regelwerk im Zahlungsverkehr, sowie Sicherheitsstandards des National Institute of Standards and Technology (NIST) und des Center for Internet Security (CIS).

Vereinfachen und Stärken der Schutzmechanismen des Netzwerks

Die Fortinet Security Fabric integriert alle Elemente einer Sicherheitsinfrastruktur und automatisiert gleichzeitig Security-Workflows und die gemeinsame Nutzung von Bedrohungsinformationen. CIOs erhalten damit eine leistungsstarke Lösung, um Komplexität und Kosten zu reduzieren.

FORTINET®

www.fortinet.com/de

3. Dezember 2019

323490-0-0-DE