SOLUTION BRIEF

Maximale Automatisierung, minimale Komplexität: Integrierte OT-Sicherheit mit der Fortinet Security Fabric

Zusammenfassung

Betriebstechnologie (OT) und Informationstechnologie (IT) wachsen immer stärker zusammen, wodurch CISOs plötzlich auch für die Sicherheit der Betriebstechnologie zuständig sind. Je weniger komplex die konvergierten IT- und OT-Infrastrukturen sind, desto besser können CISOs die Ausfallsicherheit und Verfügbarkeit von OT-Systemen gewährleisten. Die Fortinet Security Fabric ist eine bewährte Lösung für alle CISOs, die bei Sicherheitsfragen Wert auf Klarheit, Kosteneffizienz und Rechenschaftspflicht legen. CISOs erhalten damit ein umfassendes, integriertes und automatisiertes Framework mit End-to-End-Transparenz und einem zentralen Management, um OT-Umgebungen ohne Störung kritischer Betriebsabläufe zu schützen. Darüber hinaus erleichtern automatisierte Sicherheitsanalysen und -berichte den Nachweis, dass OT-Systeme neuen und künftigen Vorschriften und Sicherheitsanforderungen entsprechen.

Kostensenkungen durch eine effektivere Security-Abdeckung

Schätzungen zufolge nutzen Unternehmen durchschnittlich 75 verschiedene Sicherheitsprodukte,[1] von denen 77 % nicht vollständig integrierte Einzellösungen sind.[2] Eine wirksame Security lässt sich so nicht erreichen.

Die Fortinet Security Fabric unterstützt CISOs beim Schließen von Sicherheitslücken und vereinfacht Security-Abläufe mit einem einheitlichen Framework, das alles abdeckt: Netzwerke, Anwendungen, Geräte und Endpunkte. Geschützt wird das gesamte Unternehmensnetzwerk, einschließlich Clouds, WAN sowie sämtliche Randbereiche mit kabelbasierten und drahtlosen OT-Geräten. Die Security Fabric bietet vorkonfigurierte API-Verbindungen für über 70 Fabric-Ready-Partner und REST-APIs, mit denen Security-Teams auch Sicherheitslösungen von Drittanbietern einfach und schnell in die Architektur der Fortinet Security Fabric integrieren können.

Die komplexe Zusammenstellung und Abstimmung mehrerer Threat-Feeds mit Bedrohungsdaten stellt eine enorme Belastung für CISOs und ihre Teams dar. Dies kostet nicht nur wertvolle Arbeitszeit, sondern verlangsamt auch die Reaktion auf Schwachstellen und Angriffe. Mit der Fortinet Security Fabric wird diese Komplexität beseitigt. CISOs erhalten einen integrierten, kontinuierlichen Feed mit Bedrohungsinformationen, der vertrauenswürdige Signaturen weitverbreiteter ICS- und SCADA-Protokolle automatisch aktualisiert.

Die gesamte Fortinet Security Fabric lässt sich über eine einzige „Schaltzentrale“ transparent überwachen und steuern. Es handelt sich dabei um keine „Hub-and-Spoke“-Plattform, sondern um eine echte vernetzte Architektur. Jedes Element der Fortinet Security Fabric kommuniziert mit den anderen Elementen, wodurch sich Workflows automatisieren und Bedrohungsdaten gemeinsam nutzen lassen. Dies minimiert zeitaufwendige manuelle Arbeiten für überlastete Security-Teams und ermöglicht zugleich koordinierte Reaktionen auf Bedrohungen, illegale Zugriffe und Sicherheitsverletzungen.

Vorteile der Fortinet Security Fabric für Betriebstechnologie (OT)

- Optimiert das Security-Management mit integrierten Sicherheitselementen
- Minimiert Zeitaufwand und Betriebsstörungen beim Aufrechterhalten der Sicherheit und Verfügbarkeit von Betriebstechnologie
- Erleichtert das Compliance-Reporting durch lückenlose Transparenz und umfassende Automatisierung
- Unterstützt CISOs bei der Einschätzung und Kommunikation des Sicherheitsprofils gegenüber Stakeholdern

Kundenerfahrung

Ein führendes nordamerikanisches Öl- und Gasunternehmen benötigte vollständige Transparenz, Kontrolle und Security beim Netzwerk-Zugriff, um 5000 ICS-Endpunkte an 200 Standorten zu schützen. Mit der Fortinet Security Fabric konnte das Unternehmen die Personalkosten vermeiden, die sonst für manuelle Wartungs- und Update-Aufgaben der dezentralen Systeme angefallen wären.

Automatisierte Erkennung und Zugriffskontrolle für Betriebstechnologie

Der erste Schritt beim Schutz von Betriebstechnologie besteht darin, zu wissen, welche Geräte mit dem Netzwerk verbunden sind, was auf ihnen ausgeführt wird und wer sie verwendet (falls es einen Benutzer gibt). Die Netzwerk-Zugangskontrolle FortiNAC automatisiert die Erkennung, Profilerstellung und Kennzeichnung von OT-Geräten. Dies spart Arbeitszeit und verringert manuelle Konfigurationsfehler. FortiNAC erfasst die Daten von über 2000 LAN- und WLAN-Gerätetypen aus unterschiedlichsten Protokollen – wie SNMP (Simple Network Management Protocol), CLI (Command Line Interface), Syslogs, RADIUS (Remote Authentication Dial-In User Service) – sowie von verschiedenen APIs.

Anhand der umfassenden Informationen, die FortiNAC während des Profilierungsprozesses sammelt, werden Tags erstellt. Diese Kennzeichnungen spiegeln die Geschäftslogik wider, beispielsweise den Gerätetyp (z. B. eine Kamera, ein BYOD-Gerät oder einen Drucker) und die Abteilung, in der ein Gerät verwendet wird. FortiNAC leitet diese Tags über die Fortinet Security Fabric an FortiGate Next Generation Firewalls (NGFWs) weiter, die anhand der Tags eine absichtsbasierte Segmentierung des internen Netzwerks anlegen und Zugriffsrichtlinien definieren. FortiNAC wendet diese Richtlinien dann an, um den Zugriff auf OT-Geräte zu steuern und gleichzeitig kontinuierlich neue Geräteverbindungen und abweichende Verhaltensweisen vorhandener Geräte zu überwachen. Werden Anomalien festgestellt, lassen sich die Zugriffsberechtigungen des Geräts bis zur weiteren Überprüfung sofort ändern.

Einfachere Compliance mit automatisierten Analysen und Berichten

Das Abrufen und Abgleichen von Protokollen für die Compliance und Audits stellen für ohnehin schon unter Zeitdruck stehende IT-Teams eine zusätzliche Belastung dar. In das Betriebssystem aller Security-Fabric-Elemente sind deshalb bereits Funktionen integriert, die die Compliance und das Reporting wesentlich effizienter gestalten. Diese Funktionen entsprechen dem PCI-DSS-Standard (Payment Card Industry Data Security Standard) und anderen Vorschriften wie FIPS 140-2 (Federal Information Processing Standard) oder EAL 4–7 (Common Criteria Evaluation Assurance Levels).

Die Fortinet Security Fabric umfasst auch Elemente für Sicherheitsanalysen und SIEM (Security Information Event Management). Diese arbeiten zusammen, um Daten von Sicherheitsgeräten in IT- und OT-Netzwerken zu sammeln, zu organisieren und zu korrelieren. Isolierte Betriebsbereiche werden dadurch aufgelöst. Da die Netzwerk-Topologie in Echtzeit abgebildet wird, erfasst die SIEM-Lösung neue Sicherheitsvorfälle ohne Zeitverzögerung. Die Logs sind so immer auf dem neuesten Stand – auch bei unterbesetzten IT-Teams.

Die Fortinet Security Fabric bietet außerdem einen Security Rating Service. Dieser ermittelt die Sicherheitsleistung, bewertet das Sicherheitsprofil anhand von Branchen-Benchmarks und empfiehlt Verbesserungen, die auf Best Practices der Branche basieren.[4] Der Security Rating Service wird in einem Dashboard der zentralen Management-Konsole angezeigt. CISOs erhalten damit eine wertvolle Unterstützung, um Stakeholder mit Graphiken und Zahlen über wichtige Sicherheitsaspekte zu informieren. Zum Beispiel können CISOs anhand neuer Informationen aus der Security Fabric nachweisen, ob OT-Geräte die Sicherheitsrichtlinien des Unternehmens erfüllen. Auch der aktuelle Compliance-Status für Industriestandards und gesetzliche Vorgaben lässt sich einfach präsentieren.

Fast zwei Drittel der CISOs geben an, dass ihre Bedrohungsinformationen und -prozesse schwer zu verwalten sind.[3]

FortiNAC kann mehr als 2000 kabelgebundene und kabellose Netzwerkgeräte steuern. Fortinet entwickelt derzeit APIs für weitere Produkte.

„Für die Verwaltung und Kontrolle kritischer Ressourcen benötigten wir detaillierten Zugriff auf Firewalls und andere Security-Tools, um ein einheitliches Sicherheitsprofil zu schaffen und aufrechtzuerhalten. Deshalb haben wir uns für Fortinet entschieden.“

– Richard Hannah,
Vice President Information Services bei Gibson Energy

Fortinet bietet bewährte OT-Security

Seit über einem Jahrzehnt schützen Cyber-Security-Lösungen von Fortinet zahlreiche OT-Umgebungen in Sektoren wie Energie, Verteidigung, Fertigung, Lebensmittel und Transport. Die Fortinet Security Fabric integriert OT-Sicherheitslösungen mit einem erstklassigen Bedrohungsschutz für IT-Umgebungen im Unternehmen – vom Rechenzentrum über die Cloud bis hin zum Netzwerk-Rand. Diese Integration, gepaart mit Automatisierung und integrierter Unterstützung von Industriestandards, minimiert die Komplexität und reduziert die Betriebskosten des OT-Security-Managements im Vergleich zu isolierten IT-OT-Sicherheitslösungen. Mit der Fortinet Security Fabric können CISOs ohne Störung der Betriebsabläufe auf einfache Weise sicherstellen, dass die OT-Umgebung geschützt und regelkonform ist.

NSS Labs und Gartner bestätigen führende Fortinet-Security

- Die NSS Labs haben Fortinet-Lösungen in neun verschiedenen Security-Produktgruppen als „Empfehlenswert“ bewertet.[5]
- Fortinet wurde im Magic Quadrant 2018 von Gartner im Bereich Netzwerk-Firewalls für Unternehmen[6] und im Gartner Magic Quadrant für Unified Threat Management (SMB Multifunction Firewalls) als Leader eingestuft.[7]

[1] Kacy Zurkus: „Defense in depth: Stop spending, start consolidating“. CSO Online, 14. März 2016.

[2] Patrick E. Spencer: „Cyber Resilience Rises to the Forefront in 2019, According to New Scalar Security Study“. Scalar Security Blog Post, 20. Februar 2019.

[3] Sam Friedman: „Taking cyber risk management to the next level: Lessons learned from the front lines at financial institutions“. Deloitte, abgerufen am 20. Mai 2019.

[4] „Proactive, Actionable Risk Management with the Fortinet Security Rating Service“. Fortinet, Donnerstag, 14. Februar 2019.

[5] „Independent Validation of Fortinet Solutions, NSS Labs Real-World Group Tests“. Fortinet, April 2019.

[6] „2018 Gartner Magic Quadrant Reports“. Fortinet, abgerufen am 10. Mai 2019.

[7] Ebd.

FORTINET

www.fortinet.com/de

14. Dezember 2020, 16:40 Uhr

391455-0-0-DE