SOLUTION BRIEF

Einfachere, einheitlichere OT-Security mit Fortinet

Zusammenfassung

Sowohl Umgebungen mit Betriebstechnologie (OT) als auch mit Informationstechnologie (IT) müssen mit Cyber-Security-Lösungen geschützt werden. OT-Umgebungen haben jedoch einige Besonderheiten, die andere Herangehensweisen bei der Sicherheit erfordern. Die Fortinet Security Fabric berücksichtigt diese einzigartigen Anforderungen von Betriebstechnologie und zentralisiert zugleich das Management der OT- und IT-Cyber-Sicherheit mit einer einzigen Konsole. Zudem bietet die Security Fabric eine echte Integration und Automatisierung für die gesamte Sicherheitsinfrastruktur eines Unternehmens. Das gewährleistet einen einzigartigen Schutz und vollkommene Transparenz über jedes einzelne Netzwerk-Element wie Segmente, Geräte, Appliances – unabhängig davon, ob virtuell, in der Cloud oder On-Premises bereitgestellt. Unternehmen profitieren mit diesem Ansatz von einer geringeren Komplexität, insbesondere gegenüber isolierten Mehrpunkt-Sicherheitslösungen, die oft nicht zusammenarbeiten.

Betriebstechnologie (OT) erfordert eine spezielle Cyber-Security

Beim Schutz von OT-Umgebungen müssen Unternehmen einzigartige Herausforderungen bewältigen:

- OT-Ausfallzeiten nach Sicherheitsvorfällen können zu Produktions- und Umsatzverlusten von Hunderttausenden oder sogar Millionen von Euro führen.
- Das Herunterfahren bestimmter OT-Systeme zum Patchen ist wegen des Umsatzrisikos praktisch unmöglich.
- Neue IoT-Geräte (Internet der Dinge) in OT-Umgebungen bringen neue Risiken sowie zusätzliche Compliance-Anforderungen mit sich, die nachverfolgt und in Berichten gemeldet werden müssen.
- Die Integration von künstlicher Intelligenz (KI), maschinellem Lernen (ML) und anderen IP-basierten Elementen der digitalen Transformation (DX) in OT-Umgebungen birgt ebenfalls neue Risiken in sich.

Im Vergleich zur IT-Security erfordert die OT-Security eine andere Herangehensweise mit Schwerpunkt auf Effizienz, Sicherheit und Verfügbarkeit. Anlagenbetreiber und Fertigungsleiter sollten daher darauf achten, dass ein Security-Ansatz für Betriebstechnologie die folgenden Anforderungen erfüllt:

Integrierte Lösungen, um das Management zu vereinfachen

Wird für jedes Sicherheitsproblem eine Einzellösung angeschafft, entsteht eine fragmentierte Security-Architektur – ein Problem, mit dem viele Unternehmen heute zu kämpfen haben. Dazu kommt die Fülle an Einzellösungen auf dem Markt, von denen nur wenige gut zusammenarbeiten (allein 57 OT-Sicherheitslösungen in sieben Kategorien wurden z. B. in einer Studie der National Laboratories des US-Energieministerium identifiziert).[1] Einzellösungen führen zu einer Komplexität, die kaum noch zu bewältigen ist: Unzählige Tools müssen mit mehreren Konsolen verwaltet werden und produzieren Sicherheitsdaten, die sich nur manuell korrelieren, abgleichen und analysieren lassen. Sicherheitslücken und häufigere Fehler durch Mitarbeiter sind die Folge.

Die Fortinet Security Fabric bringt im Durchschnitt Kostensenkungen und einen Produktivitätsgewinn von 11,5 % verglichen mit einem Architektur-Ansatz, der auf Security-Einzellösungen basiert.

Die Fortinet Security Fabric vereinfacht die Cyber-Sicherheit durch die Integration von Security-Lösungen in eine koordinierte, offene Sicherheitsplattform (siehe Abbildung 1). Die Security Fabric erstreckt sich über IT- und OT-Umgebungen und ermöglicht die Zusammenarbeit von Sicherheitselementen und den Austausch von Bedrohungsinformationen, um erweiterte Risiken zu erkennen und zu verhindern. Die Security Fabric arbeitet mit integrierten Bedrohungsdaten der FortiGuard Labs, die alles abdecken – von neu erkannten Zero-Day-Angriffen und hochkomplexen Bedrohungen bis hin zu Botnetzen und Indicators of Compromise (IOCs).[2] Mit der FortiSandbox ist zudem eine komplette Sandboxing-Lösung bereits integriert, um unbekannte Bedrohungen und Zero-Day-Threats zu erkennen und zu verhindern.

Dieser ganzheitliche Security-Ansatz, bei dem alle Umgebungen über eine zentrale Konsole verwaltet werden, vereinfacht nicht nur Mitarbeiterschulungen, sondern senkt auch die Gesamtbetriebskosten (TCO). Das bestätigt auch eine unabhängige Studie: Verglichen mit modernen Security-Einzellösungen verschiedener Anbieter profitieren Unternehmen mit der Fortinet Security Fabric im Durchschnitt von Kostensenkungen und einem Produktivitätsgewinn von 11,5 % über einen Zeitraum von sechs Jahren.[3]

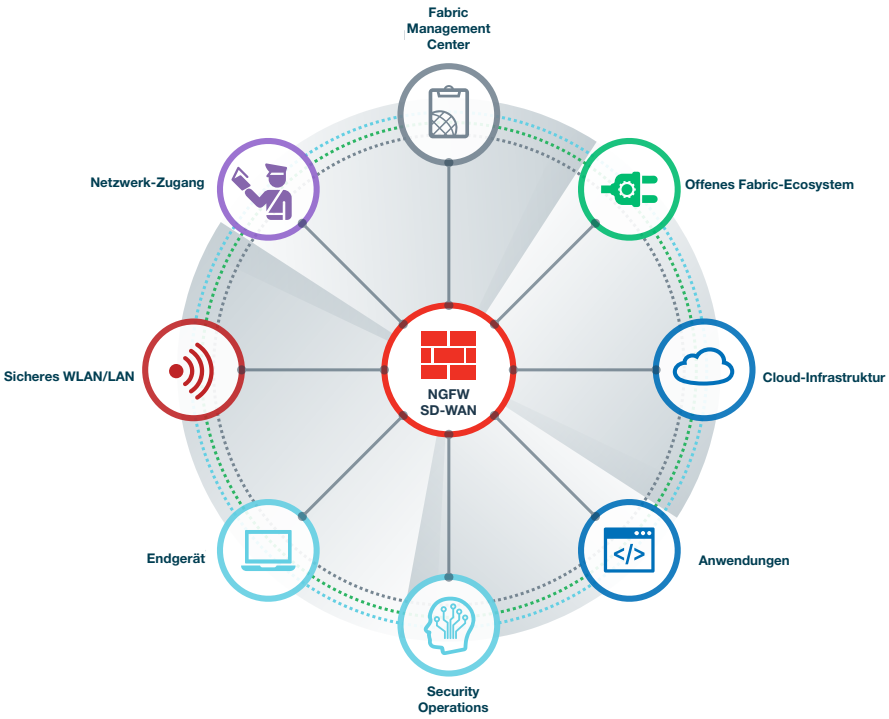

Abbildung 1: Mit der Fortinet Security Fabric können mehrere Security-Technologien nahtlos über alle Umgebungen hinweg zusammenarbeiten – unterstützt von einer einzigen Threat-Intelligence-Quelle und kontrolliert über eine gemeinsame „Schaltzentrale". So werden Sicherheitslücken im Netzwerk geschlossen und Reaktionen auf Angriffe und Datenschutzverletzungen beschleunigt.

Speziell für OT-Einschränkungen entwickelt

OT-Netzwerke enthalten häufig viele Altgeräte wie speicherprogrammierbare Steuerungen (SPS), die als vertrauenswürdig gelten, mit denen sich Teams gut auskennen und die sich seit vielen Jahren bewährt haben. Solche Legacy-Systeme haben jedoch einige Besonderheiten, die bei der Security zu berücksichtigen sind.

„Virtuelles Patching" schützt Betriebstechnologie, die sonst nicht gepatcht werden kann.

Beispielsweise lassen sich SPS-Lösungen und andere OT-Elemente nicht aktiv mit Techniken aus der IT-Netzwerk-Security scannen. In solchen Fällen kann die Security Fabric den Netzwerk-Traffic passiv überprüfen und – basierend auf beobachteten Merkmalen und Verhaltensweisen – für jedes OT-Netzwerk-Element und dessen Status ein Profil anlegen. Dabei werden auch Sicherheitslücken festgestellt, die durch Software-Updates gepatcht werden müssen.

Das Problem ist nur: Viele OT-Elemente können nicht gepatcht werden. Aber auch hierfür bietet Fortinet eine Lösung. Mit den FortiGuard Industrial Security Services[4] (im FortiGate Enterprise Bundle[5] und 360 Bundle Subscription Services[6] inbegriffen) erhalten Fortinet Next Generation Firewalls (NGFWs) aktualisierte Signaturen, um die gängigsten OT-Protokolle zu identifizieren und zu überwachen. Anhand dieser Signaturen können Fortinet NGFWs Angriffsversuche auf bekannte OT-Schwachstellen erkennen und blockieren (siehe Tabelle 1). Das Ergebnis ist ein „virtuelles Patching", das ältere Betriebstechnologie schützt.

Eine weitere typische Einschränkung bei Betriebstechnologie ist, dass sich auf vielen OT-Geräten kein Security-Software-Client installieren lässt. Auch hier bieten FortiGate NGFWs einen effektiven Schutz: Für Betriebstechnologie ohne Security-Client wird eine Segmentierung angelegt, die diese Systeme von kritischen Daten und Anwendungen trennt. Das verhindert auch die laterale Verbreitung bösartiger Exploits. Zudem lassen sich gefährdete Geräte so schnell in Quarantäne setzen. Gleichzeitig verbessert dieser Ansatz die Zugangskontrolle über Geräte, um wichtige Compliance-Anforderungen und Standards wie die EU-Direktive zur Netz- und Informationssicherheit (NIS) oder NIST (National Institute of Standards and Technology) in den USA zu erfüllen.

Offene Sicherheitsplattform, die viele Legacy-Lösungen integriert

Die Fortinet Security Fabric umfasst vorkonfigurierte API-Verbindungen für über 70 Fabric-Ready-Partner. Diese große Auswahl an Drittlösungen gewährleistet eine tiefgehende Integration aller Security-Fabric-Elemente.[7]

Security-Produkte, die nicht vom Fabric-Ready-Partnernetz abgedeckt werden, lassen sich über REST-APIs und DevOps-Skripte schnell und einfach zur Security Fabric hinzufügen. Dies ermöglicht den Austausch von Telemetriedaten, die automatisierte Bereitstellung, Konfiguration und Reaktion der Security sowie andere Funktionen.

OT-Protokolle	
BACnet	HMI
DNP3	Modbus
Elcom	OPC
EtherCAT	PROFINET
EtherNet/IP	S7
HART	SafetyNET
IEC 60870-5-104	Synchrophasor
IEC 60870-6 (TASE.2)/ICCP	HMI
IEC 61850	
LonTalk	

OT-Anwendungen und -Anbieter		
7-Technologies/ Schneider Electric	Honeywell	RealFlex
ABB	ICONICS	Rockwell Automation
Advantech	InduSoft	RSLogix
Broadwin	Intellicom	Siemens
CitectSCADA	Measuresoft	Sunway
CODESYS	MicroSys	TeeChart
Cogent	Moxa	VxWorks
DATAC	PcVue	Wellintech
Eaton	Progea	Yokogawa
GE	QNX	

Tabelle 1: FortiGuard Industrial Security Services – Beispiele für die Unterstützung von Betriebstechnologie (OT)

Für eine einfachere Konnektivität kann die Security Fabric mit Switches und drahtlosen APs verschiedener Anbieter interagieren und diese steuern. Unterstützt werden 2000 verschiedene Modelle von über 170 Anbietern wie Cisco, HP und Ruckus.[8] In den meisten Fällen verbessert sich dadurch das Sicherheitsprofil des Unternehmens – bei gleichzeitig geringerem Management-Aufwand. Auch werden bestehende Investitionen geschützt, da Geräte erst später aufgerüstet oder ersetzt werden müssen.

Automatisierte Prozesse für Intrusion Prevention, Detection und Incident Response

Die verschiedenen Elemente der Fortinet Security Fabric arbeiten wie ein einziges Sicherheitssystem zusammen. Firewalls, E-Mail, Endpunkt-Schutz, Sandboxing, Switche und drahtlose Access Points erkennen Malware automatisch, erstellen Signaturen und informieren andere Security-Elemente. Bedrohungen werden so effektiv abgewehrt und in Quarantäne isoliert oder es wird ein Alarm gesendet. Und da Angriffe heute ebenfalls künstliche Intelligenz (KI) und maschinelles Lernen (ML) nutzen und in Maschinengeschwindigkeit vorgehen, müssen Security-Lösungen sie in Maschinengeschwindigkeit bekämpfen können.

Wurde eine Bedrohung erkannt, automatisiert die Security Fabric Workflows, die zur schnellen Eindämmung richtlinienbasierte Ereignis-Trigger, Abwehrreaktionen und Genehmigungen kombinieren. Sicherheitsvorfälle lassen sich automatisch an eine ITSM-Lösung (Information Technology Service Management) weiterleiten. Security-Analysten erhalten mehrere Abwehroptionen zur Auswahl, die automatisch von zentraler Stelle aus umgesetzt werden können. Diese Funktionen reduzieren die Reaktionszeit von Tagen auf Minuten, damit sich personell begrenzte Security-Teams auf wichtige Entscheidungen – statt auf das reine Monitoring und Weiterleiten von Informationen – konzentrieren können.[9]

Automatisiertes Reporting mit Compliance- und Audit-Tracking

In den meisten Unternehmen werden bei der Audit-Vorbereitung Daten aus verschiedenen Sicherheitslösungen manuell korreliert und analysiert – ein mühsamer, aufwendiger Prozess, der in der Regel mehrere Mitglieder des Security-Teams von wichtigeren Aufgaben abhält. Mit dem FortiManager und FortiAnalyzer sparen Teams wertvolle Zeit, da sich das Compliance-Tracking und die Berichterstellung automatisieren lassen – alles im Einklang mit Branchenvorschriften und Sicherheitsstandards.

Die Security Fabric verkürzt Reaktionszeiten von Tagen – oder sogar Wochen – auf Minuten.

Der Security Rating Service bietet eine einzige Bewertung, die Aufschluss über das Gesamtsicherheitsprofil gibt sowie Bereiche mit akutem Handlungsbedarf aufzeigt.

Zu den erweiterten Compliance-Funktionen gehören Hunderte vorkonfigurierte, sofort verwendbare Berichte, deren Erstellung sich einfach planen lässt und die mit über 400 Diagrammen und 35 Vorlagen angepasst werden können. Zudem führt der FortiAnalyzer eine automatisierte, tiefgehende Analyse von Sicherheitsaktivitäten durch, um das Risiko der Angriffsfläche und den akuten Handlungsbedarf zu ermitteln. Diese Funktion informiert auch den Fortinet Security Rating Service, der ein Dashboard mit einer zentralen Übersicht über das Gesamtsicherheitsprofil des Unternehmens im Vergleich zu Marktbegleitern und anerkannten Sicherheitsstandards bietet. Der Fortinet Security Rating Service – bereits im FortiGate Enterprise Bundle[10] und 360° Protection Bundle[11] enthalten und als Abonnement erhältlich – ist eine einfache Möglichkeit, die Geschäftsleitung und den Aufsichtsrat über allgemeine Trends in einem gut verständlichen Format auf dem Laufenden zu halten (siehe Abbildung 2).[12]

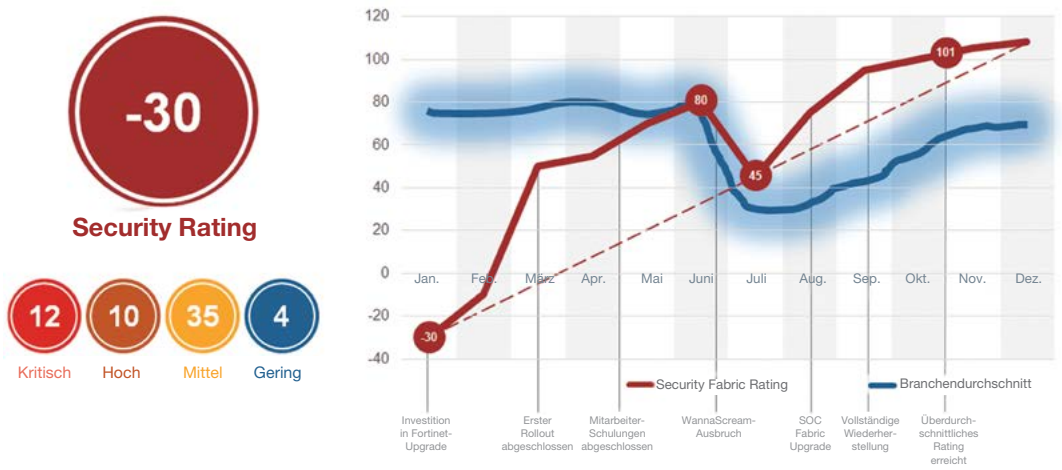

Abbildung 2: Mit dem Fortinet Security Rating Service lassen sich zeitbezogene und Trend-Analysen zum Sicherheitsprofil Ihrer Umgebung erstellen und mit dem Branchendurchschnitt vergleichen.

Einheitliche Cyber-Security, um Komplexität und Risiken zu minimieren

Mit der Fortinet Security Fabric können Unternehmen ihre OT- und IT-Cyber-Sicherheit mit einem Ansatz integrieren, der den einzigartigen Herausforderungen von OT-Netzwerken gerecht wird. Die Security Fabric basiert auf einem einheitlichen Betriebssystem, einer offenen API-gesteuerten Architektur und einem zentralisierten Management. Unternehmen können hiermit kritische Bedrohungsdaten effektiver erfassen, korrelieren, teilen und Bedrohungen abwehren. Dieser Sicherheitsansatz reduziert Risiken und ermöglicht Security-Teams, mit weniger Aufwand mehr zu erreichen.

Arbeiten Security-Elemente als integriertes Ecosystem zusammen, können Unternehmen betroffene Geräte sofort überall im Netzwerk identifizieren, isolieren und sanieren, Malware automatisch finden und entfernen sowie die Aktualisierung von Sicherheitsrichtlinien überall koordinieren. Alles lässt sich zentral abstimmen: OT, IT, IoT-Geräte und Clouds. Zugleich sinkt die Komplexität, während die Sicherheit und Compliance verbessert werden. Das ist ein wichtiger Punkt bei der digitalen Transformation von OT-Unternehmen. Denn mit einer solchen Security-Lösung können Sie sich darauf verlassen, dass wichtige Ressourcen wie IoT-Sensoren, KI, ML und Big Data geschützt sind.

1 Carl M. Hurd und Michael V. McCarty: „A Survey of Security Tools for the Industrial Control System Environment“. Idaho National Laboratory, U.S. Department of Energy, 12. Juni 2017.

2 „FortiGuard Labs“. Fortinet, abgerufen am 22. März 2019.

3 Zeus Kerravala: „How to Enable Digital Transformation and Improve ROI with Fortinet Security Fabric“. ZK Research, Februar 2018.

4 „Industrial Control Systems“. Fortinet, abgerufen am 25. März 2019.

5 „Comprehensive Security with the FortiGate Enterprise Protection Bundle“. Fortinet, 21. Januar 2019.

6 „360 Protection Bundle: Delivering Real-Time Network Management, Comprehensive Security and Operational Services, and Advanced Support“. Fortinet, 26. März 2019.

7 „Technology Alliances“. Fortinet, abgerufen am 21. April 2019.

8 „FortiNAC: Network Access Control“. Fortinet, abgerufen am 27. April 2019.

9 „Purpose-built Integrated NOC-SOC Management and Analytics“. Fortinet, 11. September 2018.

10 „Comprehensive Security with the FortiGate Enterprise Protection Bundle“. Fortinet, 21. Januar 2019.

11 „360 Protection Bundle: Delivering Real-Time Network Management, Comprehensive Security and Operational Services, and Advanced Support“. Fortinet, 26. März 2019.

12 „Proactive, Actionable Risk Management with the Fortinet Security Rating Service“. Fortinet, 5. April 2019.

FORTINET

www.fortinet.com/de

7. Dezember 2020, 14:08 Uhr

392073-A-1-DE