WHITEPAPER

Reduzieren des OT-Cyber-Risikos mit der Fortinet Security Fabric

Strategien für den CISO

Zusammenfassung

Die digitale Transformation (DX) beschleunigt die Konvergenz von Betriebstechnik (OT)* und Informationstechnologie (IT) und führt Unternehmen in die Zukunft. Unternehmen nutzen digitale Technologien wie Internet of Things (IoT), Cloud Computing und künstliche Intelligenz (KI), um ihren Betrieb zu optimieren, Sicherheit und Zuverlässigkeit zu verbessern und einen Wettbewerbsvorteil zu erlangen. Trotz der vielen Vorteile haben jedoch sowohl die Konvergenz von OT und IT als auch die zunehmende Implementierung digitaler Technologien die OT-Angriffsfläche erweitert und ihre Anfälligkeit für Cyber-Bedrohungen erhöht.

Wie können Unternehmen dann das OT-Cyber-Risiko minimieren? Die Antwort ist die Fortinet Security Fabric, eine transformative und einzigartige Security-Architektur. Die Security Fabric integriert erstklassige Sicherheitslösungen, um breite Transparenz sowohl der OT- als auch der IT-Angriffsfläche bereitzustellen und gleichzeitig die operativen Abläufe zu automatisieren und kontinuierliche Gefahrenbewertungen durchzuführen. Dieses Whitepaper behandelt fünf Best Practices zur Cyber-Sicherheit, die das OT-Cyber-Sicherheitsprofil stärken, und ordnet sie jeweils verschiedenen Komponenten der Security Fabric zu. Die Gesamtlösung von Fortinet dient als Grundlage für die Konvergenz von IT- und OT-Umgebungen und die Erzielung eines neuen Mehrwerts für das Unternehmen.

Von Fortinet entwickelte Cyber-Sicherheit für konvergierende OT/IT-Netzwerke

Wenn Unternehmen ihre IT- und OT-Infrastruktur zielgerichtet für Konvergenz und DX anpassen, müssen sie auch eine Security-Transformation durchlaufen, um sich vor sich entwickelnden Cyber-Bedrohungen zu schützen. Fortinet bietet einen proaktiven und transformativen Ansatz für die Cyber-Sicherheit: die Fortinet Security Fabric (siehe Abbildung 1), die folgende Vorteile liefert:

- Breite Sichtbarkeit der gesamten OT- und IT-Angriffsfläche
- Integrierter Schutz über alle Geräte, Netzwerke und Anwendungen hinweg
- Automatisierte Abläufe und Reaktionen durch KI und maschinelles Lernen (ML)

* OT ist ein Synonym für **industrielle Steuerungssysteme (Industrial Control Systems, ICS)**. OT wurde als Begriff im Gegensatz zur IT geschaffen, da OT-Protokolle, Anbieter und Anwendungsfälle unterschiedlich sind. **SCADA-(Supervisory Control and Data Acquisition-)Systeme** sind ein Bestandteil von OT. SCADA-Systeme verwenden grafische Benutzeroberflächen für das übergeordnete Management von OT/ICS-Prozessen.

Die Bereitstellung der Security Fabric ist der Übergang in einen gewünschten Zustand, der Transparenz, Integration, Automatisierung und Stabilität in einer Security-Umgebung bietet. Die Security Fabric kann in Stufen erreicht werden, die sich an den unternehmerischen Sicherheitsprioritäten orientieren. Bei der Planung dieser Phasen sollten Unternehmen die folgenden Best Practices befolgen:

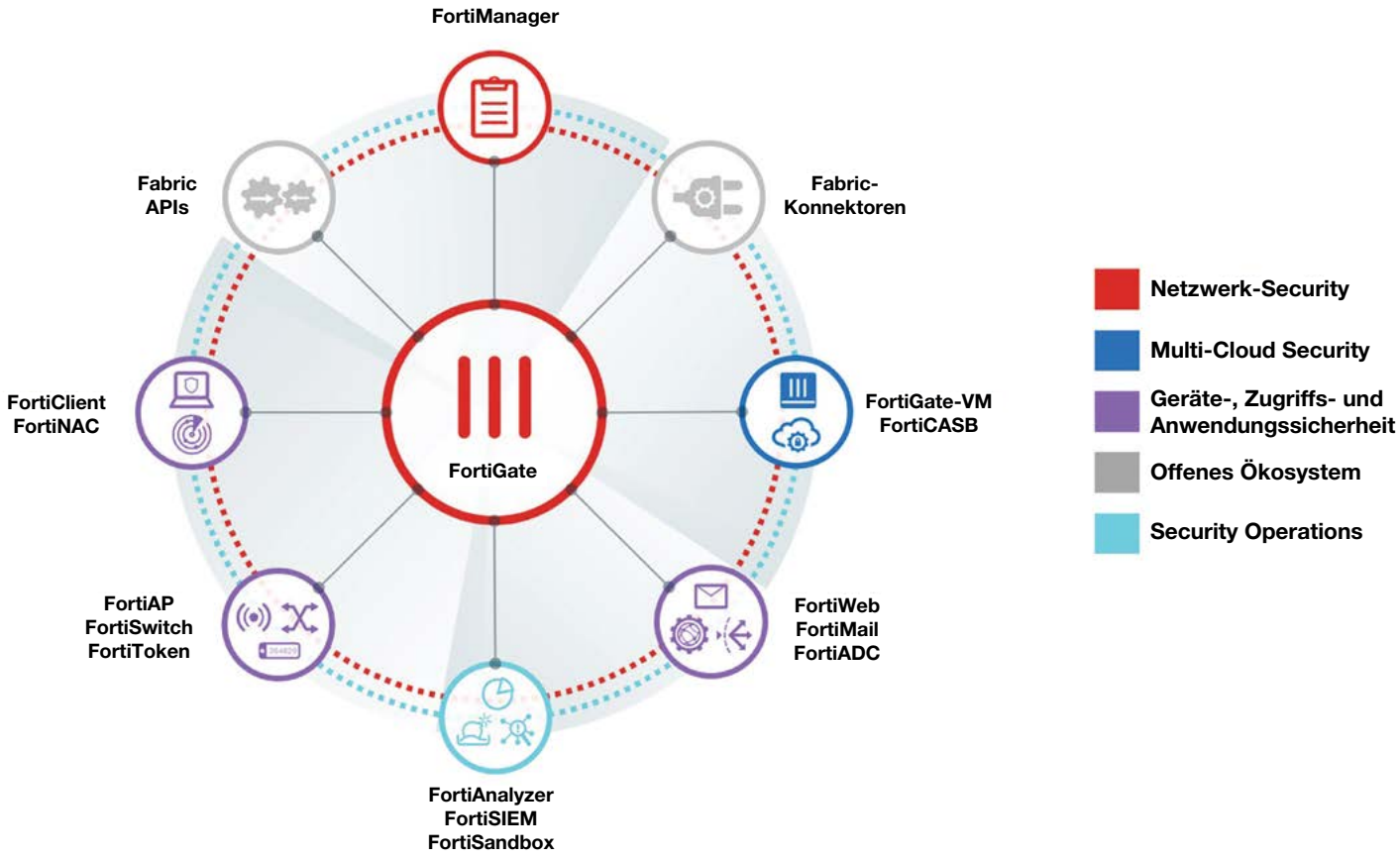

Abbildung 1: Die Fortinet Security Fabric ermöglicht die Zusammenarbeit mehrerer Technologien über OT- und IT-Umgebungen hinweg, die alle von einer einzigen Threat Intelligence-Quelle unterstützt werden, um Sicherheitslücken im Netzwerk zu schließen und auf jeden Angriffsvektor zu reagieren.

Empfohlene Best Practices für die OT-Cyber-Sicherheit

Eine kostenlose Bedrohungsanalyse hilft bei der Identifizierung und Priorisierung von Risiken.

Einschränkung der Bewegungsfreiheit eines Angreifers innerhalb und zwischen Netzwerken.

1. Identifizieren von Assets, Klassifizieren und Priorisieren von Werten

Der erste Schritt für einen CISO, der versucht, das OT-Sicherheitsprofil seines Unternehmens zu verbessern, ist die Erstellung eines aktuellen Inventars der in seinem Netzwerk laufenden Geräte und Anwendungen. Fortinet kann dies mit einem kostenlosen Fortinet Cyber Threat Assessment bereitstellen, das bestimmten Kunden zur Verfügung steht.[1] Der Vorgang beginnt mit der Verwendung einer FortiGate Next-Generation Firewall (NGFW) oder FortiNAC (Network Access Control) zur passiven Überwachung des Netzwerkverkehrs. Diese passive Datenverkehrsanalyse wird dann verwendet, um Geräte basierend auf ihren Eigenschaften und ihrem Verhalten zu identifizieren und ein Profil zu erstellen. Der resultierende Bericht liefert folgende Informationen:

- Hinweise auf risikoreiche Anwendungen
- Identifikation der am stärksten ausgenutzten Schwachstellen von Anwendungen
- Bewertung des Risikowerts jedes einzelnen Assets
- Identifikation von Hinweisen auf Malware, Botnets und möglicherweise gefährdete Geräten
- Kategorisierung von Anwendungen und Analyse ihrer Netzwerknutzung

CISOs können mit Fortinet zusammenarbeiten, um diese Informationen als Grundlage für die Optimierung eines Sicherheitsplans zu nutzen.

2. Segmentieren des Netzwerks

Bei allen vier oben beschriebenen OT-Datenschutzverletzungen konnten sich die Angreifer quer durch die IT- und OT-Netzwerke und zwischen ihnen bewegen. Die Netzwerksegmentierung schränkt diese Bewegung ein. Es handelt sich um eine grundlegende Best Practice zum Schutz von OT-Systemen, wie sie in den Sicherheitsstandards ISA/IEC-62443 (ehemals ISA-99) beschrieben ist.[2]

Die Segmentierung unterteilt das Netzwerk in eine Reihe funktionaler Segmenten oder „Zonen“ (die Unterzonen oder Mikrosegmente beinhalten können) und „Conduits“ (Kanäle zwischen den Zonen). Die **FortiGate Internal Segmentation Firewall (ISFW)** definiert und verstärkt die Zonen und Kanäle.[3] Dies geschieht mit Hilfe der Fortinet **absichtsbasierten Segmentierung**, einem Ansatz, der das Vertrauensniveau von Benutzern, Geräten und Anwendungen kontinuierlich überwacht und deren Zugriff dynamisch basierend auf Geschäftsabsicht, Verhalten und Risiko steuert. Dadurch wird die Angriffsfläche drastisch verkleinert, da es Eindringlingen erschwert wird, Schwachstellen zu finden und auszunutzen.

3. Analysieren und Schützen des Datenverkehrs vor Bedrohungen und Schwachstellen

Es ist unerlässlich, den Netzwerkverkehr zu analysieren, um Bedrohungen zu identifizieren und zu blockieren. Fortinet Management and Analytics bietet diese Fähigkeit durch die Integration von Informationen aus den folgenden Quellen:

FortiSIEM (Security Information and Event Management) erkennt automatisch alles, was mit einem Netzwerk verbunden ist, und erstellt eine Configuration Management Database (CMDB). Darüber hinaus wird eine prüffähige Datenverkehrsaufstellung erstellt, die für die proaktive Risikoabwehr und den Nachweis der Compliance mit Regulierungs- und Sicherheitsstandards verwendet wird.

FortiManager bietet eine Dashboard-Ansicht, die den aktuellen Status der Security Fabric anzeigt, sowie eine einheitliche Perspektive, die sowohl den Teams des Security Operations Center (SOC) als auch des Network Operations Center (NOC) bereitgestellt wird. SOC-Teams können den Umfang von Sicherheitswarnungen und -problemen einsehen, und das NOC-Team kann sehen, ob Leistungseinbußen das Ergebnis eines Sicherheitsvorfalls sind. Basierend auf diesen Erkenntnissen kann das Operations-Team die Anforderungen des Security-Teams besser verstehen und dessen Anforderungen zur Neukonfiguration oder Quarantäne leichter zustimmen.

FortiAnalyzer automatisiert die Protokollverwaltung und die Echtzeit-Bedrohungsanalyse. FortiAnalyzer nutzt den IOC-(Indicators of Compromise-)Dienst von FortiGuard Labs, der aus einem täglichen Paket von etwa 500 000 IOCs besteht, die aus verschiedenen weltweiten Quellen stammen. Dies hilft bei der Identifizierung von Kommunikationen mit Servern, die sich als bösartig erwiesen haben. FortiAnalyzer kann über den FortiGuard Security Rating Service auch eine quantifizierte Risikobewertung sowohl intern über einen gewissen Zeitraum als auch für ähnlichen Unternehmen bereitstellen.

Darüber hinaus nutzt Fortinet Management and Analytics **FortiGate** NGFWs für die Prüfung des Datenverkehrs und den Schutz vor bösartigen Dateien, Anwendungen und Exploits.

FortiGate NGFWs nutzen **FortiGuard Industrial Security Services**[4], die Teil der Abonnementdienste FortiGate Enterprise Bundle[5] und 360 Bundle[6] sind, für aktualisierte Signaturen, die es ihnen ermöglichen, die gängigsten OT-Protokolle zu identifizieren und zu überwachen sowie versuchte Exploits bekannter OT-Schwachstellen zu erkennen und zu blockieren (siehe Tabelle 1). Das Blockieren bekannter Exploits ist besonders kritisch in OT-Umgebungen, in denen die Geräte gewöhnlich ohne Patches oder Firmware-Updates betrieben werden.

Um Bedrohungen zu erkennen und Richtlinien durchzusetzen, scannen FortiGate NGFWs den verschlüsselten SSL-(Secure Sockets Layer-) / TLS-(Transport Layer Security-)Datenverkehr. Da verschlüsselter Datenverkehr heute 72 % des gesamten Netzwerkverkehrs ausmacht und 50 % der Cyber-Angriffe verbirgt, ist die Überprüfung des verschlüsselten Datenverkehrs unabdingbar.[7,8] Im Gegensatz zu anderen Firewall-Lösungen, die dramatische Leistungseinbußen verzeichnen, verwenden FortiGate NGFWs speziell entwickelte Sicherheitsprozessoren (SPUs), um negative Auswirkungen auf die Leistung zu minimieren. Auf diese Weise können Unternehmen vermeiden, ihre Firewall-Infrastruktur nachzurüsten und um weitere Appliances zu erweitern – egal ob im Rechenzentrum oder am Netzwerkrand. Das Ergebnis ist, dass FortiGate NGFWs beim Scannen von verschlüsseltem Datenverkehr in Vergleichstests das beste Preis-Leistungs-Verhältnis erzielen. Dies umfasst auch die Blockierung von 100 % der Umgehungen.[9]

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

Die Security Fabric stellt außerdem noch folgende weitere Elemente bereit, die den Datenverkehr analysieren und vor Bedrohungen schützen:

Das **FortiMail**-E-Mail-Gateway wehrt Bedrohungen wie Spear-Phishing ab, eine Taktik, die häufig bei OT-Datenschutzverletzungen zum Stehlen von Anmeldeinformationen eingesetzt wird. Spear-Phishing und andere E-Mail-basierte Angriffe sind heute für zwei Drittel der installierten Malware verantwortlich.[10] FortiMail kann auch so eingestellt werden, dass vermutete, aber unbekannte Bedrohungen an **FortiSandbox** weitergeleitet werden, das Aktionen analysiert und Bedrohungen identifizieren kann, bevor sie an den Endbenutzer übertragen werden. FortiSandbox kann auch potenzielle Bedrohungen von anderen Zugangspunkten wie Endgeräten, dem Netzwerk, Cloud-Implementierungen und Dateifreigaben analysieren. Da FortiSandbox vollständig in die Security Fabric integriert ist, teilt es automatisch Threat Intelligence-Daten in Echtzeit über alle Security-Elemente hinweg.

FortiDeceptor[11] verwendet Köder, sogenannte „Decoys“, um Bedrohungsaktivitäten umzuleiten und zu analysieren und Informationen über die gesamte Security Fabric auszutauschen. **FortiIsolator**[12] ist eine Browser-Isolationslösung, die einen visuellen „Luftspalt“ zwischen Benutzer-Browsern und Websites erzeugt. Es zeigt Web-Inhalte in einem entfernten Einwegbehälter an und isoliert so jede Bedrohung durch Malware.

Verschlüsselter Datenverkehr verbirgt 50 % der Cyber-Angriffe.[13]

Die Multi-Faktor-Authentifizierung erschwert die Verwendung gestohlener Anmeldeinformationen, eine häufige Taktik zur Datenschutzverletzung in OT-Systemen, erheblich.

4. Kontrolle des Zugriffs von Benutzern und Geräten

Die Security Fabric steuert die Möglichkeiten des Netzwerkzugriffs von Benutzern und Geräten, indem sie die Funktionen der folgenden Komponenten koordiniert:

FortiGate NGFWs können verwendet werden, um Benutzer- und Gerätegruppen zu erstellen und Sicherheitsrichtlinien für jede dieser Gruppen durchzusetzen. So können beispielsweise für lokale Benutzer im Vergleich zu Remote-Benutzern unterschiedliche Kontrollen eingestellt werden.

FortiAuthenticator validiert die Benutzeridentität und wendet auf jede Zone und jeden Kanal eine detaillierte Kontrolle des Benutzerzugriffs an. Die Anwendung identifiziert Benutzer, fragt Zugriffsberechtigungen von Drittsystemen ab und übermittelt diese Informationen an FortiGate-Geräte, sodass diese identitätsbasierte Richtlinien durchsetzen können.

FortiToken prüft die Identität weiter mit Multi-Faktor-Authentifizierung (MFA), bei der Benutzer-Anmeldeinformationen mit einem Hard- oder Software-Token, einem Fingerabdruck oder anderen biometrischen Daten kombiniert werden. MFA erschwert die Verwendung gestohlener Zugangsdaten erheblich.

FortiNAC authentifiziert Geräte, die an das Netzwerk angeschlossen sind, durch Beobachtung ihrer Eigenschaften. Einmal profiliert, kann FortiNAC Richtlinien auf Geräte anwenden, um zu steuern, ob und wie sie sich mit dem Netzwerk verbinden können und auf welche Segmente des Netzwerks sie Zugriff haben. FortiNAC kann auch Ports nach Bedarf sperren: Es sind keine Geräte oder Anwendungen erlaubt, bis sie explizit zugelassen sind. Ein Port bietet keine Netzwerkkonnektivität, bis das Verbindungsgerät autorisiert ist. Dadurch kann die Richtlinie durchgesetzt werden, dass jedes Gerät, das einem OT-Netzwerk hinzugefügt wird, zuerst von autorisierten Mitarbeitern genehmigt werden muss.

FortiClient lässt sich in FortiGate NGFWs integrieren, um Transparenz der Endgeräte in OT-Umgebungen zu erhalten und Schwachstellenalarme auszulösen.

5. Sichern von kabelgebundenem und drahtlosem Zugang

In vielen OT-Umgebungen nimmt die Belastung durch potenzielle Angriffe über kabelgebundene und drahtlose Access Points zu. Häufig wird dieses erhöhte Risiko von DX gesteigert. Einige Produktionsstätten und Lagerhäuser nutzen beispielsweise fahrerlose Transportfahrzeuge (FTF), die beim Transport von Waren und Materialien drahtlos miteinander verbunden sind.[14] Alle von Forrester in einer Studie befragten Unternehmen haben ihre Angriffsfläche vergrößert, indem sie entweder drahtlose oder IoT-Technologien einsetzen. Dazu gehören auch Verbindungen zu OT-Netzwerken.[15]

Alle befragten Unternehmen verfügen über WLAN- oder IoT-Geräte, wodurch das Risiko erheblich erhöht wird.

Um das Risiko zu minimieren, sollten Security-Teams den kabelgebundenen und drahtlosen Zugriff zentral über eine Schnittstelle verwalten. Durch eine FortiGate NGFW können sie Firewall-Funktionen und -Richtlinien auf Ports von **FortiSwitches** und **FortiAPs** im gesamten Unternehmen über proprietäre, sichere und verschlüsselte Tunnel übertragen.

Security-Teams können FortiNAC auch zur zentralen Konfiguration von Switches und drahtlosen APs von Drittanbietern verwenden – diese umfassen bis zu 2.000 Netzwerkgeräte von 170 Anbietern.

Robuste FortiSwitches, FortiAP Access Points und FortiGate NGFWs sind für Schock, Vibration, Staub, Feuchtigkeit und extreme Temperaturen in OT-Umgebungen ausgelegt – von Offshore-Ölplattformen über Schiffscontainer bis hin zu Fabrikhallen.[16,17,18]

Erhöhung der OT-Sicherheit

OT-Technologien wurden Anfang des 20. Jahrhunderts entwickelt, viele Jahrzehnte vor dem Aufstieg der IT. Traditionell waren OT- und IT-Netzwerke durch einen Luftspalt, die sogenannte „Air Gap“, getrennt. Jetzt werden beide integriert, um einen Mehrwert für das Unternehmen zu schaffen.

Durch die Integration von IT und OT wächst die digitale Angriffsfläche. Mit den richtigen Kontrollen und Technologien schützen CISOs jedoch ihre OT-Umgebungen, da sie folgende Möglichkeiten erhalten:

1. Gewinn einer breiten Sichtbarkeit der Angriffsfläche
2. Segmentierung des Netzwerks, um die Auswirkungen von Eindringlingen zu begrenzen
3. Analyse des Datenverkehrs, einschließlich verschlüsselten Datenverkehrs und gängiger OT-Protokolle, zum Schutz vor Bedrohungen
4. Kontrolle des Zugriffs von Benutzern und Geräten, Durchsetzung identitätsbasierter Richtlinien mit kontinuierlicher Gefahrenbewertung
5. Sichern des kabelgebundenen und drahtlosen Zugangs durch eine zentrale Verwaltung der Kontrollen über eine einzige Konsole

Die Fortinet Security Fabric verbindet IT- und OT-Security-Lösungen über ein gemeinsames Betriebssystem: FortiOS. Sie bietet eine umfassende Transparenz der gesamten Angriffsfläche, integrierten KI-gesteuerten Schutz vor Datenschutzverletzungen sowie automatisierte Abläufe, Orchestrierung und Reaktionen. Die Bereitstellung der umfassenden Fähigkeiten und des vollen Nutzens kann in Phasen erfolgen, die sich nach den Prioritäten der Unternehmenssicherheit richten. Ein erster Schritt kann eine kostenlose Bedrohungsanalyse sein, die Risiken priorisiert.

[1] „Know Your Vulnerabilities—Get the Facts About Your Network Security“, Fortinet, letzter Zugriff 25. März 2019.

[2] „ISA Standards: Numerical Order“, International Society of Automation, letzter Zugriff 3. Januar 2018.

[3] „Protecting Your Network from the Inside-Out: Internal Segmentation Firewall (ISFW)“, Fortinet, Dezember 2016.

[4] „Industrial Control Systems“, Fortinet, letzter Zugriff 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] John Maddison, „Encrypted Traffic Reaches A New Threshold“, Network Computing, 28. November 2018.

[8] „Study Reveals Hackers Increasingly Use Encryption to Hide Criminal Activity“, Lifeline Data Centers, letzter Zugriff 21. März 2019.

[9] „Fortinet Receives Recommended Rating in Latest NSS Labs NGFW Report, Delivers High SSL Performance Suited for Encrypted Cloud Access“, Fortinet, 17. Juli 2018.

[10] David Finger, „Provide Customers with Advanced Threat Defense Against Email-Based Attacks“, Fortinet, 26. April 2018.

[11] „FortiDeceptor Enables a New Breach Protection Approach“, Fortinet, 21. März 2019.

[12] „FortiIsolator“, Fortinet, letzter Zugriff 27. März 2019.

[13] „Study Reveals Hackers Increasingly Use Encryption to Hide Criminal Activity“, Lifeline Data Centers, letzter Zugriff 21. März 2019.

[14] „Automated Guided Vehicle Market worth $2.74 billion by 2023“, MarketsandMarkets, letzter Zugriff 27. März 2019.

[15] „Independent Study Pinpoints Significant SCADA/ICS Cybersecurity Risks“, Fortinet, 7. Mai 2018.

[16] „FortiSwitch™ Rugged“, Fortinet, letzter Zugriff 7. Januar 2019.

[17] „Wireless Product Matrix“, Fortinet 222C Wireless AP, März 2019.

[18] „FortiGate® Rugged Series“, Fortinet, letzter Zugriff 14. Januar 2019.

September 30, 2019 7:28 vorm.

376629-0-1-DE

E:\PRACE\ARGOS\2019\09 2019\A-344888-982188\de-DE\OT\CISO\wp-ot-ciso-solution-selection-A4_de-DE\wp-ot-ciso-solution-selection-A4_de-DE