SOLUTION BRIEF

Security für OT-Netzwerke mit Mikro-Segmentierung

Lokalen VLAN-Traffic mit Firewalls überprüfen

Zusammenfassung

Früher genügten LAN-Lösungen wie ein auf einem Switch bereitgestelltes VLAN (virtuelles LAN), um Netzwerke für Betriebstechnologie (OT) vor einer lateralen Malware-Verbreitung im Netzwerk zu schützen. Solche VLAN-Lösungen bieten zwar größere Flexibilität bei der Segmentierung, doch für den Schutz von OT-Netzwerken ist dieser Segmentierungsgrad nicht ausreichend.

Mit der Mikro-Segmentierung von Fortinet lässt sich eine Zero-Trust-Security implementieren und der gesamte VLAN-Datenverkehr mit einer Next Generation Firewall (NGFW) überprüfen. Das Risiko, dass sich Malware quer im Netzwerk verbreitet, sinkt so erheblich. Zudem bietet eine Mikro-Segmentierung eine hohe Sicherheit für das OT-Netzwerk, ohne die Netzwerk-Performance zu beeinträchtigen.

Ein VLAN arbeitet auf Layer 2 des Kommunikationsnetzwerks und unterteilt dieses in mehrere virtuelle Netzwerke. Dadurch wird eine Broadcast-Domain in mehrere kleinere Domains gegliedert, was die Netzwerk-Leistung verbessert. VLANs ermöglichen zudem die logische Gruppierung von Netzwerk-Elementen, die innerhalb eines Kommunikationsnetzwerks physisch verteilt sind.

ICS/OT-Netzwerke kurz erklärt

Bei Steuerungstechnik (ICS) und Betriebstechnologie (OT) wird das Kommunikationsnetzwerk als Prozesssteuerungsnetzwerk (PCN, Process Control Network) bezeichnet. Dieses Netzwerk ermöglicht die Kommunikation zwischen verschiedenen Automatisierungsprozessen einzelner ICS-Komponenten, einschließlich der speicherprogrammierbaren Steuerung (SPS), externer Steuereinheiten (RTU, Remote Terminal Unit), verteilter Steuersysteme (DCS, Distributed Control System) sowie der Überwachungs- und Datenerfassungssysteme (SCADA, Supervisory Control And Data Acquisition).

Das PCN überträgt Anweisungen und Daten zwischen Steuer- und Messtechnik und verbindet verschiedene Komponenten innerhalb einer ICS/OT-Umgebung. Es handelt sich um ein leistungsstarkes, robustes und deterministisches LAN, das eine ständige Verfügbarkeit, schnelle Reaktionen sowie zuverlässige Fehlerprüfungen und -behebungen gewährleisten muss. Nur dann lassen sich Ausfallzeiten vermeiden sowie der deterministische, fehlerfreie und kontinuierliche ICS-Betrieb sicherstellen.

Um die Determinismus- und Robustheitsanforderungen von Steuerungstechnik zu erfüllen, werden PCNs häufig in flachen Netzwerk-Strukturen mit geringer oder keiner Abgrenzung der ICS-Komponenten konfiguriert (Abbildung 1). Durch diese flache PCN-Struktur wird das Netzwerk schneller und lässt sich einfacher verwalten.

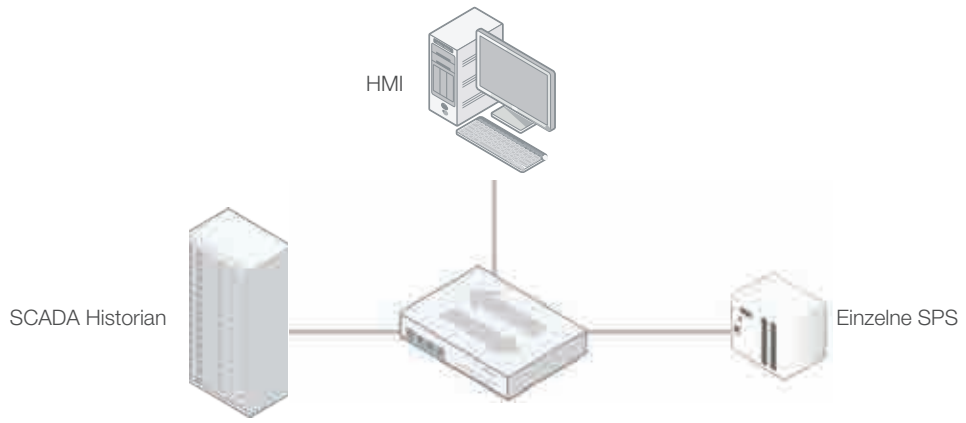

Abbildung 1: Beispiel einer flachen PCN-Topologie

Bei einer flachen PCN-Netzwerk-Struktur steigt jedoch die Anfälligkeit für Sicherheitsbedrohungen, z. B. durch Netzwerk-Flood-Angriffe oder die seitliche Verbreitung von Malware innerhalb des PCN. Diese Bedrohungen können sogar die PCN-Kommunikation stören und das gesamte ICS blockieren. Zudem erschwert eine flache Netzwerk-Struktur die PCN-Integration in andere Kommunikationsnetze außerhalb der Steuerungstechnik.

Automatisierungen wurden bislang mit LAN-Lösungen wie Netzwerk-Bridges und Gateways realisiert, um verschiedene Komponenten zu trennen und Netzwerk-Broadcasts oder -Floods innerhalb des PCN möglichst in Grenzen zu halten. Die Implementierung von VLANs kann diesen Segmentierungsprozess flexibler gestalten und eine Netzwerk-Trennung unabhängig vom physischen Layout schaffen. Mit VLANs allein lassen sich jedoch nicht die Sicherheitsprobleme lösen, die einem PCN weiterhin erheblichen Schaden zufügen können. Zudem funktioniert die VLAN-basierte Segmentierung innerhalb eines PCN langsamer als bei einem Unternehmensnetzwerk.

Die Purdue Enterprise Reference Architecture (PERA), die ursprünglich in den 1990er Jahren für die computerintegrierte Fertigung entwickelt wurde, bietet Systemintegratoren und Netzwerk-Verantwortlichen Anleitungen zur mehrstufigen Segmentierung eines Großsystems. Dies verbessert die Kontrolle über die Integration verschiedener Komponenten und Subsysteme. ISA-99 hat dieses Modell zur mehrstufigen ICS-Segmentierung und zur Implementierung von Sicherheitskontrollen übernommen. Aus ISA-99 wurde später die IEC-Norm ISA/IEC 62443.

Zonen und Kanäle in ICS/OT-Netzwerken

Um Sicherheitsprobleme in Netzwerken mit Steuerungstechnik (ICS) und Betriebstechnologie (OT) anzugehen, entwickelte die Automatisierungsbranche das Zone-Conduit-Konzept. Dieses unterteilt das PCN in mehrere Zonen und isoliert die verschiedenen Komponenten in einem ICS. Innerhalb eines ICS gruppiert eine Zone logische oder physische Ressourcen mit identischen Sicherheitsanforderungen und definiert Sicherheitsgrenzen für Informationen, die in eine Zone gelangen und diese verlassen. Zwischen den verschiedenen Zonen werden Kanäle (Conduits) angelegt, um die Kommunikation zwischen den Zonen zu regeln und Sicherheitskontrollen zu implementieren. Diese Kanäle fungieren als Kontrollmechanismen (Gatekeeper) zwischen den verschiedenen Zonengrenzen.

Das Zone-Conduit-Modell wurde mit den Normen IEC 62443-1-1 und IEC 62443-3-2 der International Society of Automation (ISA)/International Electrotechnical Commission (IEC) eingeführt und bietet detaillierte Anleitungen zum Definieren von Zonen und Kanälen. Darüber hinaus kann das PERA-Framework (Purdue Enterprise Reference Architecture) zur mehrstufigen Segmentierung verschiedener ICS-Zonen und -Kanäle dienen.

Disruption in der Industrie – OT, IIoT, IT, IoT und Konvergenz

Das Zukunftsmodell „Industrie 4.0“ und disruptive Technologien wie das Internet der Dinge (IoT) oder das industrielle Internet der Dinge (IIoT) haben ICS/OT-Netzwerke in konvergierte Netzwerke verwandelt. Steuerungstechnik und Betriebstechnologie befinden sich heute nicht mehr in einer isolierten Umgebung. Beide sind mit internen IT-Netzwerken und dem externen Internet verbunden und liefern wichtige geschäftliche Informationen – Stichwort „Business Intelligence“ –, die in Geschäftsentscheidungen einfließen.

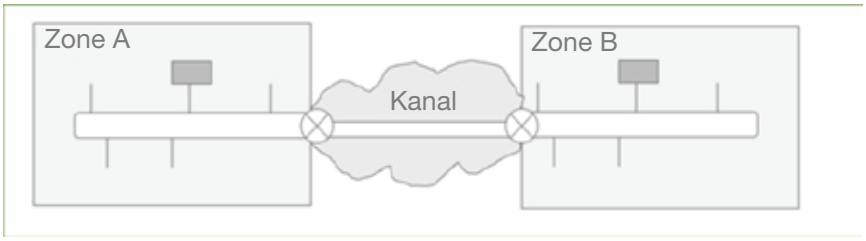

Abbildung 2: Zone-Conduit-Konzept

In einer konvergierten ICS/OT- und IT-Infrastruktur basiert die Kommunikation nicht mehr auf proprietären Netzwerk-Kommunikationsprotokollen oder einfach nur auf speziellen ICS/OT-Kommunikationsprotokollen. Stattdessen verwendet ein konvergiertes ICS/OT-IT-Netzwerk eine Kombination aus komplexen proprietären und offenen Standard-Kommunikationsprotokollen, die anfällig für verschiedene Angriffe sind. Dies erweitert die Angriffsfläche und herkömmliche Sicherheitskontrollen wie VLANs reichen für Steuerungstechnik nicht mehr aus. Das gilt umso mehr, je stärker OT- und IT-Netzwerke zusammenwachsen.

Das Definieren von Zonen und Kanälen sowie die mehrstufige Netzwerk-Segmentierung sind für das Zusammenspiel von ICS/OT und IT zwar notwendig, lösen aber nicht alle Sicherheitsprobleme einer konvergierten Netzwerk-Infrastruktur. Fakt ist: Komplexe Angriffsformen lassen sich mit VLANs allein nicht verhindern.

In einem VLAN werden Netzwerk-Pakete unkontrolliert an Geräte weitergeleitet, die zur gleichen Broadcast-Domain gehören. Jedes Paket, das über die Broadcast-Domain-Grenze hinausgehen muss, erfordert einen Netzwerk-Routing-Mechanismus. Dieser fungiert meistens als virtueller oder physischer Kanal, manchmal dient er auch für Sicherheitskontrollen, z. B. zur Traffic-Inspektion

zwischen beiden Broadcast-Domains. VLAN-Routing-Mechanismen bieten zwar einige Sicherheitsvorteile, die jedoch für moderne, konvergierte ICS/OT- und IT-Infrastrukturen nicht genügen.

Mit einem VLANs lässt sich zudem nicht die interne Netzwerk-Kommunikation einer Broadcast-Domain überprüfen. Innerhalb einer Broadcast-Domain können die Geräte, die Teil eines VLAN sind, uneingeschränkt miteinander kommunizieren, ohne dass diese Kommunikation überprüft oder überwacht wird.

In einer typischen ICS/OT-Netzwerk-Implementierung sind Dutzende von Komponenten in einem einzigen VLAN zusammengefasst. Diese Komponenten können frei miteinander kommunizieren, ohne einen Routing-Kanal zu durchlaufen – wodurch sich jede anomale Netzwerk-Kommunikation quer im PCN verbreiten kann.

Werden diese Netzwerke mit anderen Netzwerken zusammengelegt (normalerweise außerhalb der ICS/OT-Grenzen), muss jeder einzelne Kommunikationskanal überprüft werden können. Ansonsten besteht die Gefahr, dass Angriffe aufgrund komplexer Netzwerk-Integrationen unentdeckt bleiben. Zudem werden offene Kommunikationsprotokolle für den Informationsaustausch zwischen ICS/OT- und IT-Netzwerken zum Risiko, da Schwachstellen im Kommunikationsprotokoll und andere Sicherheitslücken einen Angriffsvektor für ICS/OT-Umgebungen darstellen können.

Die Zero-Trust-Architektur ist ein Netzwerk-Modell, das 2010 von Forrester Research entwickelt wurde.[1] Beim Zero-Trust-Modell werden alle Verbindungsversuche mit dem Unternehmensnetzwerk überprüft, bevor der Zugriff gewährt wird – unabhängig davon, ob Anfragen von innerhalb oder außerhalb des Unternehmensnetzwerks stammen.

In der ICS/OT-Infrastruktur dient dasselbe Zero-Trust-Security-Konzept dazu, die Netzwerk-Kommunikation zwischen ICS-Komponenten mit einer Whitelist zu erlauben.

Mikro-Segmentierung von ICS/OT-Netzwerken

Ein VLAN ermöglicht zwar eine flexible logische Segmentierung, doch die Mikro-Segmentierung bietet eine präzisere Kontrolle über den Netzwerk-Verkehr. Das liegt daran, dass die Mikro-Segmentierung das VLAN stärker partitioniert und Sicherheitsrichtlinien für jede Partition implementiert. Diese Sicherheitsrichtlinien lassen sich auf verschiedene Arten von Datenverkehr abstimmen, um den Netzwerk- und Anwendungsfluss zwischen ICS-Komponenten zu begrenzen. Mit der Mikro-Segmentierung können ICS-Verantwortliche eine Zero-Trust-Security implementieren, damit z. B. eine bestimmte SPS selbst innerhalb des gleichen VLAN nicht mit einer anderen SPS kommunizieren kann – es sei denn, die Sicherheitsrichtlinie erlaubt dies ausdrücklich.

In einem mikrosegmentierten Netzwerk werden VLANs normalerweise mit NGFWs kombiniert, um Sicherheitsrichtlinien zu implementieren sowie die Netzwerk-Kommunikation zu überprüfen und zu filtern. Der Fortinet FortiSwitch und FortiGate NGFWs bieten einen integrierten Ansatz für die Mikro-Segmentierung. Diese integrierte Lösung erweitert die VLAN-Funktionen von Layer 1 (Netzwerk-Kommunikation) auf Layer 3 (Routing) und Layer 7 (Transparenz), wodurch sich der Netzwerk-Traffic überprüfen lässt. Der FortiSwitch arbeitet auf Layer 2 und definiert die VLANs, während die FortiGate NGFW auf Layer 3 das Routing der gesamten Kommunikation

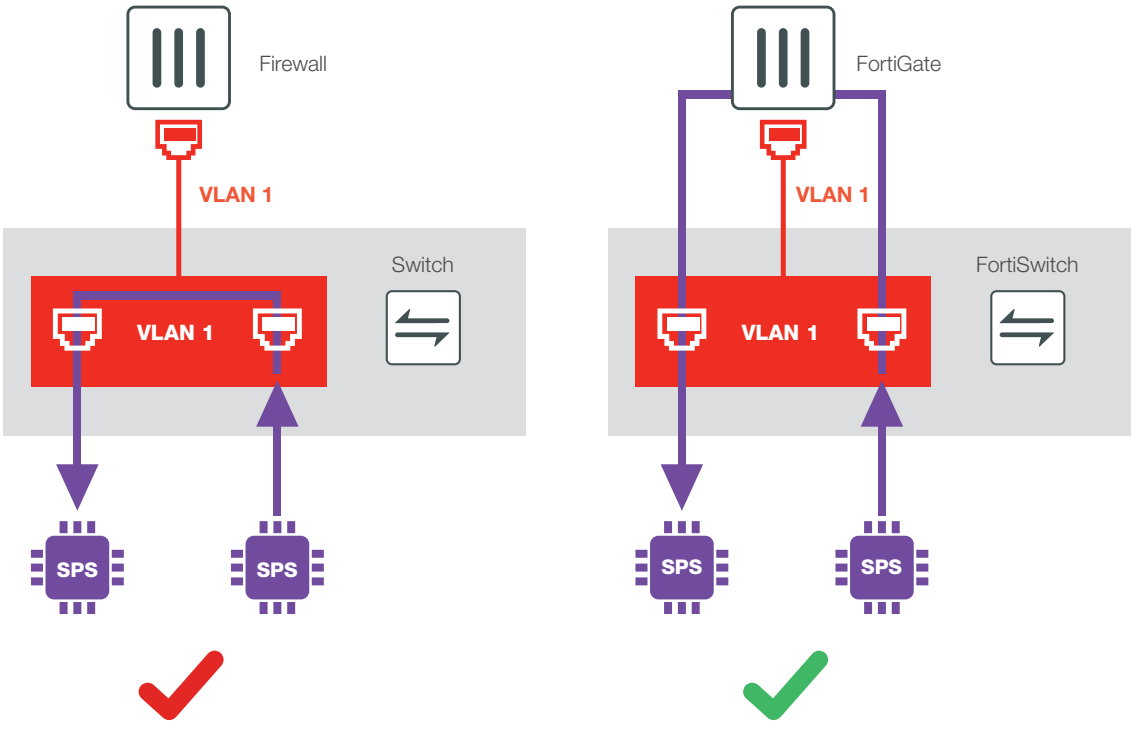

Abbildung 3: Normales VLAN-Routing im Vergleich zur Mikro-Segmentierung mit Fortinet FortiSwitch und FortiGate

zwischen sowie innerhalb von VLANs übernimmt. Der Netzwerk-Verkehr lässt sich so mit granular abgestimmten Sicherheitsrichtlinien überprüfen und für alle Netzwerk-Protokolle und -Daten, die über die NGFW laufen, wird eine Layer-7-Inspektion möglich.

Die integrierte Fortinet-Lösung zur Mikro-Segmentierung von ICS/OT-Netzwerken bietet ICS-Verantwortlichen zahlreiche Vorteile.

- **Isolieren von Hosts und Geräten**: Durch die Isolierung jedes Geräts innerhalb des ICS-Netzwerks lässt sich die Netzwerk-Kommunikation präzise steuern. Der Netzwerk-Verkehr, der bei einem Gerät ankommt und das Gerät verlässt, muss durch die FortiGate NGFW fließen. Dies ermöglicht die Durchsetzung von Sicherheitsrichtlinien, die Überprüfung des Datenverkehrs, eine Anwendungskontrolle sowie die Intrusion Detection und Prevention (IDP).
- **Deep Packet Inspection (DPI) des ICS-Protokolls**: Die FortiGate NGFW unterstützt eine tiefgehende Überprüfung der übertragenen Pakete für über 32 ICS/OT-Protokolle mit mehr als 1500 sofort einsatzbereiten Application-Control-Signaturen zur Anwendungssteuerung.

Die FortiGate NGFW arbeitet mit Fortinets eigenem Betriebssystem FortiOS, das marktführende Netzwerk-Sicherheitsfunktionen wie DPI für ICS/OT-Protokolle, Unterstützung von speziellen ICS/OT-Netzwerk-Protokollen wie PRP (Parallel Redundancy Protocol), einen Malware-Schutz, ein Intrusion Prevention System (IPS) sowie softwaredefinierte SD-WAN-Funktionen für das Wide Area Networking bietet.

- **Verhindern seitlicher Angriffe**: Die Isolierung jeder einzelnen ICS-Komponente erschwert die Verbreitung von Malware innerhalb des ICS-Netzwerks. Der gesamte Datenverkehr im ICS-Netzwerk wird überprüft und kontrolliert.
- **Starke Performance**: FortiGate NGFWs sind bewährte marktführende Hochleistungs-Firewalls mit den geringsten Latenzzeiten[2] – ideal für die Überprüfung des Datenverkehrs in einem mikrosegmentierten ICS-Netzwerk.
- **Nahtlose Integration**: Logische und physische Netzwerk-Verbindungen müssen nicht geändert werden.
- **Zentrales Management**: Die gesamte Lösung wird über eine einzige integrierte Konsole verwaltet, um ICS-Verantwortliche bei der Security-Automatisierung zu unterstützen.

Die in Fortinet integrierte Mikro-Segmentierungslösung verwendet die PERA-Anleitung für die Lösungsimplementierung. Die Mikro-Segmentierung kann auf jeder Ebene innerhalb des ICS/OT-Netzwerks implementiert werden, solange eine Netzwerk-Verbindung zwischen den verschiedenen ICS-Komponenten besteht.

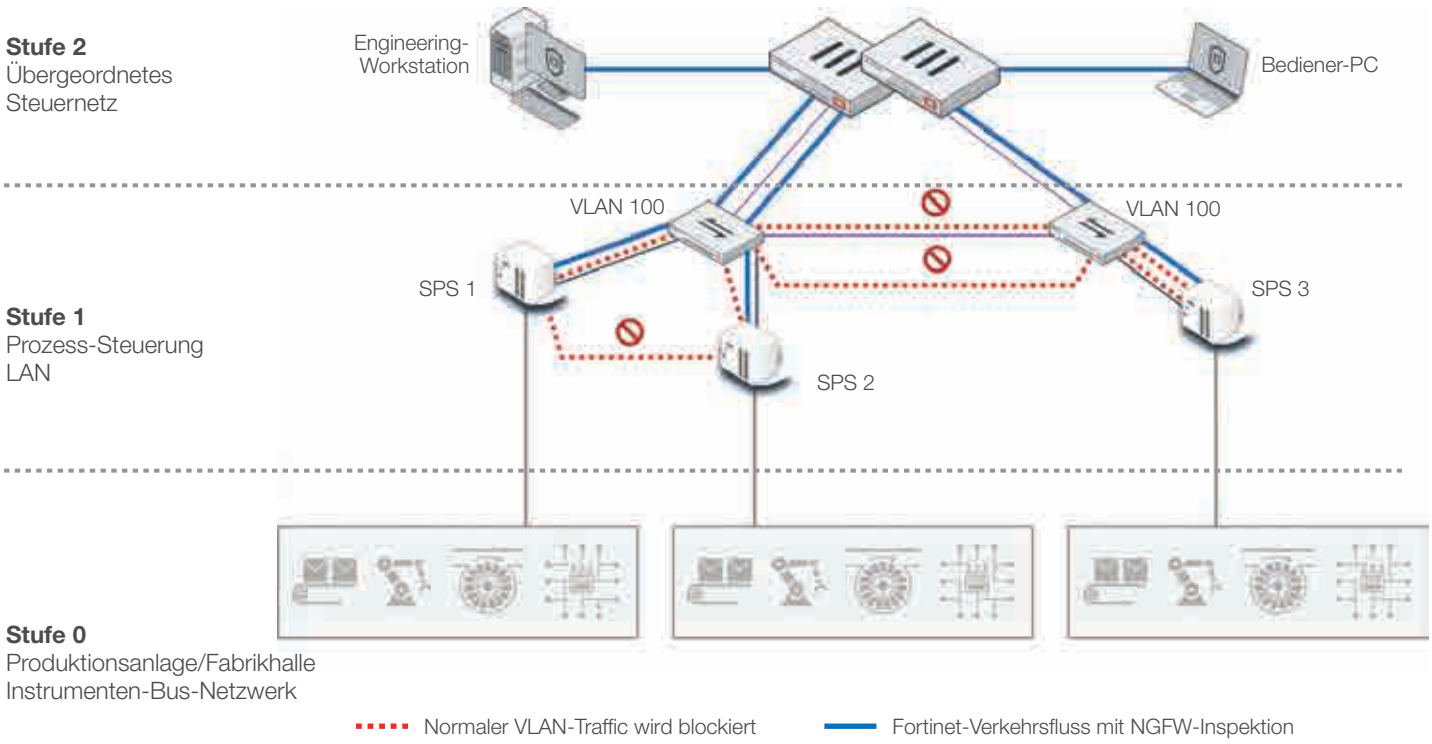

Abbildung 4: Beispiel für eine PERA-Implementierungsarchitektur mit Fortinet FortiSwitch und FortiGate

Fazit

Da ICS/OT-Netzwerke größtenteils aus langjährig genutzten Geräten mit besonderen Betriebsanforderungen bestehen, sollte die Security speziell für Betriebstechnologie abgestimmt sein.

Fortinet bietet einen einzigartigen, bewährten Ansatz für die Sicherheit von ICS/OT-Netzwerken. In 15 Jahren enger Zusammenarbeit mit OT-Unternehmen hat Fortinet viele wertvolle Einblicke in Steuerungstechnik und Betriebstechnologie gewonnen, die jetzt in den branchenweit ersten Bericht über Entwicklungen in der OT-Security eingeflossen sind.[3]

Aufbauend auf dieser Fachkompetenz und Erfahrung erfüllen Fortinet-Lösungen die speziellen Anforderungen von OT-Umgebungen auf einzigartige Weise. Mit der VLAN-basierten Mikro-Segmentierung lassen sich Geschäftsrisiken über ICS-Systeme kontrollieren, während die Steuerungstechnik gleichzeitig von einem logisch segmentierten Netzwerk profitiert. Gestützt wird dies von der Fortinet Security Fabric, die diese Lösungen kombiniert und dem Security-Team vollständige, zentralisierte Transparenz und Kontrolle über die gesamte Sicherheitsinfrastruktur bietet.

[1] Mary K. Pratt: „What is Zero Trust? A model for more effective security“. CSO, 16. Januar 2018.

[2] „Deterministic Communications for Secure High-speed Performance: Fortinet Protects Connections to Electronic Trading Platforms with the Industry's Lowest Latency and Jitter Rates“. Fortinet, 23. September 2019.

[3] „Fortinet 2019 Operational Technology Security Trends Report: An Update on the Threat Landscape for ICS and SCADA Systems“.Fortinet, 8. Mai 2019.

FORTINET

www.fortinet.com/de

14. Dezember 2020, 16:07 Uhr

562135-0-0-DE