

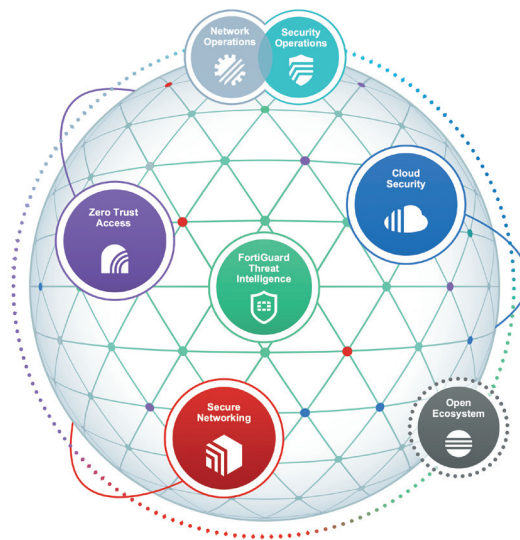
Umfassende Cybersicherheit für OT-Umgebungen

Industrielle Umgebungen und kritische Infrastrukturen stellen besondere Anforderungen an die Cybersicherheit. Mit Security Fabric for OT deckt Fortinet alle wichtigen Aspekte der Industrial Cybersecurity ab.

Das Bewusstsein, dass Cybersicherheit auch in den OT-Umgebungen (Operational Technologie) der Industrie und bei kritischen Infrastrukturen eine immens wichtige Rolle spielt, setzt sich immer mehr durch. Mit der Umsetzung wirksamer Sicherheitsmassnahmen in OT-Netzwerken hapert es aber vielerorts noch – dies unter anderem, weil traditionelle Cybersicherheitslösungen die Besonderheiten von OT-Umgebungen, darunter eine Vielzahl nicht oder schwierig zu patchender Komponenten sowie proprietäre und OT-spezifische Protokolle, nur ungenügend berücksichtigen. OT-spezifische Tools andererseits decken meist nur Teilaspekte ab und genügen somit nicht für eine umfassende OT-Security.

Einheitliche Plattform für ICS/OT und konvergente OT/IT

Der renommierte Cybersecurity-Anbieter Fortinet hat die OT-Problematik erkannt und seine bewährte IT-Sicherheitsplattform Security Fabric an allen Schlüsselstellen mit OT-Funktionalität ergänzt. So bietet der Hersteller für seine Netzwerk- und Security-Kernprodukte FortiGate-Appliances (Next-Generation Firewall) und FortiSwitch (Switching) neben den herkömmlichen FortiGuard-Sicherheitsdiensten spezifische OT-Services an. Dazu zählen beispielsweise dedizierte Industrial Security Services und der IoT



Detection Service, die zusammengenommen eine tiefgreifende Lösung für Inventarisierung und Visibilität, für Bedrohungsabwehr und Virtual Patching ergeben. Des Weiteren bieten die Fortinet-Firewalls die Möglichkeit der Mikrosegmentierung – dies bis auf Geräteebene. Damit lässt sich die Kommunikation zwischen (OT-)Anlagen und Systemen gezielt steuern und unerwünschter Traffic blockieren.

Vergleichbares gilt für die Administrations- und Analysetools FortiManager und FortiAnalyzer sowie für die Lösungen für Netzwerk- und Security-Operations (FortiSIEM, FortiSOAR). Darüber hinaus liefern die Fortinet-Produkte für Threat Intelligence & Response – es sind dies FortiEDR, FortiNDR und FortiSandbox – zusätzliche Sicherheit in OT-Netzwerken. Interessant ist auch die Honey-pot-Lösung FortiDeceptor. Mit ihr lässt sich zum Beispiel ein spezifisches OT-System wie ein SCADA-Server oder eine Steuerung eines bestimmten OT-Herstellers täuschend echt simulieren, um Erkenntnisse über das Verhalten von Angreifern zu gewinnen und mögliche Be-

drohungen zu erkennen und im Keim zu ersticken.

Von grosser Wichtigkeit ist zudem die Zugangskontrolle, bei der prinzipiell das Zero-Trust-Prinzip gelten sollte. Auch in diesem Bereich wartet Fortinet mit führenden Lösungen auf, darunter die speziell auf OT-Netzwerke hin erweiterte Network-Access-Control-Lösung FortiNAC, Produkte für starke Multifaktor-Authentifizierung (FortiAuthenticator, FortiToken), FortiVPN sowie die Privileged-Access-Managementplattform FortiPAM, die den sicheren und protokollierten Zugriff durch externe Dienstleister gewährleistet.

Hardwareseitig bietet die Fortinet-Produktpalette für industrielle Umgebungen gehärtete «Rugged»-Firewall-Appliances, Switches und Access Points sowie Kommunikations-Extender für 3G/4G/5G-Connectivity mit entfernten und mobilen Standorten.

Purdue-Modell perfekt abgedeckt

Das bekannte Purdue-Modell für industrielle Umgebungen teilt die Systeme in fünf Zonen für Sicherheit und Schutz, Prozesssteuerung, Betrieb und Kontrolle (ICS/OT) sowie die IT-orientierten Zonen Business & Enterprise und Cloud & External ein. Mit seinem breiten, auf OT hin erweiterten Sicherheitsportfolio stellt Fortinet eine komplette, integrierte und automatisierte Cybersecurity-Plattform bereit, die Visibilität, Kontrolle und direkt umsetzbare Erkenntnisse zu ICS/OT- und konvergenten IT/OT-Umgebungen liefert. Zudem deckt sie die Kerngebiete Secure Networking, Zero Trust, Security Operations und Security Services / Threat Intelligence ab und geht mit einer Vielzahl von gesetzlichen Vorschriften, industriellen Standards und Best Practices konform.

Kontakt

BOLL Engineering AG
Jurastrasse 58, 5430 Wettingen
Tel. 056 437 60 60, info@boll.ch,
www.boll.ch