Advertorial

OT-Sicherheit erfordert Umdenken

Operational Technology (OT) ist heute ein prioritäres Angriffsziel von Cyberkriminellen. Doch viele OT-Umgebungen sind nur unzureichend auf Cybersicherheit ausgerichtet. Was die Herausforderungen sind und was es für die OT-Sicherheit braucht, lesen Sie hier.

Operational Technology umfasst elektronische Komponenten wie Sensoren und Aktoren, SCADA-Server (Supervisory Control and Data Acquisition) sowie industrielle Kontrollsysteme (ICS), die in industriellen Anlagen und kritischen Infrastrukturen für die Steuerung und Überwachung zuständig sind. Fehler, wie sie etwa durch Cyberangriffe ausgelöst werden können, haben oft physische Konsequenzen – vom Ausfall einer Produktionsstrasse über den Zusammenbruch der Energieversorgung bis hin zur direkten Gefahr für Menschenleben. Es ist klar: OT-Umgebungen müssen besonders gut abgesichert werden, was in der Praxis leider allzu oft nicht der Fall ist.

OT versus IT

OT unterscheidet sich in verschiedener Hinsicht von IT. So bestehen OT-Netzwerke aus einer Vielzahl von Hardwarekomponenten mit integrierter Firmware, proprietären Betriebssystemen sowie OT-spezifischen oder gar herstellereigenen Protokollen, die schwieriger zu katalogisieren und zu überwachen respektive zu aktualisieren sind als IT-Systeme. OT-Systeme sind auch mit grösseren Risiken behaftet als IT-Systeme, weil sie auf eine lange Lebensdauer (bis hin zu Jahrzehnten) ausgelegt sind.

OT-Netzwerke sind zudem weniger stark segmentiert, da sie ursprünglich für einen eigenständigen Betrieb konzipiert und nicht für die Integration in eine umfassendere Umgebung geplant wurden. Dementsprechend wurde auch der Zugangskontrolle traditionell eher wenig Aufmerksamkeit geschenkt. Und bei den Steuerungssystemen legten Hersteller von OT-Anlagen wie Siemens oder ABB in der Vergangenheit wenig Wert auf Cybersicherheit.

IT-Systeme auf der anderen Seite arbeiten heute durchwegs IP-basiert. Es existiert ein riesiger Markt von Cybersecurity-Lösungen für IT-Netzwerke. In der IT ist man sich strikte Zugangskontrolle und Segmentierung, Bedrohungsschutz auf Basis global gewonnener Threat Intelligence, verschlüsselte Kommunikation und umfassende Transparenz mithilfe systemübergreifender Inventarisierungs-, Monitoring- und Administrationslösungen längst gewohnt. Doch auf OT-spezifische Anforderungen waren gängige Cybersecurity-Lösungen für die IT bisher nicht vorbereitet.

Anforderungen an die OT-Sicherheit

OT-Sicherheitslösungen müssen eine vergleichbare Funktionalität bieten wie IT-Sicherheitslösungen, ergänzt um die Spezifika von OT-Umgebungen. So müssen sie OT-spezifische Protokolle beherrschen und bei der Inventarisierung und Überwachung OT-Komponenten samt Firmwarestand und Schwachstellen erfassen können. Die volle Transparenz und Visibilität über die gesamte Infrastruktur ist matchentscheidend, ebenso eine wasserdichte Zugangskontrolle für die Kommunikation zwischen der IT- und der OT-Umgebung.

Wie das IT-Netzwerk sollte auch das OT-Netzwerk im Hinblick auf Sicherheit sinnvoll segmentiert werden. Zur Absicherung einzelner OT-Komponenten eignet sich die individuelle Mikrosegmentierung, mit der genau festgelegt werden kann, mit welchen anderen Systemen und Geräten eine Komponente überhaupt kommunizieren darf.

IT-Security-Hersteller auf OT-Kurs

Immer mehr Netzwerk- und Security-Hersteller haben die Bedeutung der OT erkannt und ihre Lösungen in unterschiedlichem Umfang OT-tauglich gemacht. Fast alle bekannten Cybersecurity-Anbieter, darunter etwa Fortinet, Palo Alto Networks oder Kaspersky, haben mittlerweile ihre Lösungen durch OT-spezifische Funktionalität ergänzt oder zusätzliche Lösungen auf den Markt gebracht. Dazu kommen weitere, ganz auf OT fokussierte Hersteller wie Claroty.

Vom Prinzip her kommen in der OT meist die gleichen Produkte wie in der IT zum Einsatz: Firewalls, Switches, Access Points und Softwarelösungen für die Verwaltung und Überwachung der Netzwerke sowie zur Bedrohungsabwehr. Und punkto Hardware bieten einige Hersteller neben den in der IT gebräuchlichen Geräten auch «Rugged»-Varianten für harsche Umgebungen mit erweitertem Temperaturbereich und zur Montage in industriespezifischen Szenarien (Hutschiene) an.

Kontakt

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