# Sicherheit für industrielle Kontrollsysteme

Die sogenannte Operational Technology, kurz OT, gerät immer mehr ins Visier von Cyberkriminellen. Dies ist umso gefährlicher, als OT-Netzwerke in der Regel nicht auf Cybersicherheit ausgelegt sind. Ruedi Kubli, Sales Engineer und Leiter des Fortinet-Teams bei BOLL, erklärt im Interview, was es mit OT Security auf sich hat.

**Was bedeutet Operational Technology?**
Ruedi Kubli: OT umfasst alle elektronischen Systeme wie Sensoren, Aktoren, SCADA-Server (Supervisory Control and Data Acquisition) oder industrielle Kontrollsysteme (ICS), die direkt mit industriellen Anlagen von der Produktionsstrasse bis zur Kraftwerksturbine zusammenhängen. In diesem Umfeld laufen Prozesse ab, die bei fehlerhafter Steuerung physische Gefahren nach sich ziehen können – bis hin zur Gefährdung menschlichen Lebens. Der Sicherheit solcher Systeme kommt eine besonders grosse Bedeutung zu. Dies übrigens durchaus auch in KMUs: Für Angreifer ist es nicht viel aufwändiger, 1000 KMUs zu attackieren als einen Grosskonzern.

**Wodurch unterscheiden sich OT- von IT-Systemen?**
OT-Systeme sind auf eine lange Lebensdauer von zehn oder mehr Jahren ausgelegt. Sie sind oft nicht für regelmässige Updates konzipiert und verfügen nicht über Sicherheitsmechanismen wie Authentifizierung oder die Möglichkeit, Agenten zu installieren, wie es im IT-Endpunktschutz gang und gäbe ist. Es ist schwierig, in einem solchen Umfeld Sicherheitslücken auszuräumen oder neue Sicherheitsstandards zu etablieren.

**Sind OT-Netzwerke grundsätzlich unsicher?**
Dies muss nicht so sein. Aber OT-Netzwerke sind traditionell wenig segmentiert – jedes System kann mit jedem kommunizieren –, und es ist keine Zugangskontrolle auf dem Niveau von IT-Netzwerken üblich. Ausserdem sind im OT-Umfeld neben IP auch industrielle Protokolle gängig, wie etwa Modbus, MQTT und Profibus. Herkömmliche Sicherheitslösungen und IT-Sicherheitsexperten verstehen sich meist nicht auf diese Protokolle.

**Wer kümmert sich um die Sicherheit von OT-Umgebungen?**
Traditionell sind Hersteller wie Siemens oder ABB für die Sicherheit der Anlagen zuständig. Erst in den letzten Jahren wurde dabei zunehmend auch die Cybersecurity berücksichtigt. Doch es gibt weiterhin problematische Aspekte. So ist etwa beim Umgang mit Daten, zum Beispiel Smart-Metering-Messdaten, oft nicht klar, wie und wo diese verarbeitet und abgelegt werden. Eine Datenklassifizierung wie in der IT ist nicht üblich. Auf der anderen Seite ist die OT gerade deswegen ein immer beliebteres Angriffsziel – die Anlagen sind nicht so gut geschützt, und Cyberkriminelle können gewissermassen unter dem Radar agieren.

***Ruedi Kubli ist Fortinet-Team-Leader beim IT-Security-Distributor BOLL.***

**Was muss eine OT-Sicherheitslösung leisten?**
Etwas vom Wichtigsten sind die Visibilität und die Transparenz über die Infrastruktur. Alle Assets müssen bekannt und ihre Risiken identifiziert sein. Des Weiteren braucht es eine stringente Zugangskontrolle, was Zugriffe aus der IT-Umgebung und zwischen den OT-Systemen betrifft. Dabei hilft auch eine funktionsgemässe, konsequente Segmentierung im OT-Netzwerk. Und noch etwas: OT-Systeme arbeiten oft in rauen Umgebungen bezüglich Temperatur, Luftfeuchtigkeit oder Staub – die Geräte, bis hin zum Netzwerkswitch, müssen robust sein und harsche Umweltbedingungen aushalten.

**Wer liefert solche Lösungen?**
Es gibt diverse Netzwerk- und Security-Hersteller, die sich vermehrt auf OT spezialisiert haben oder ihre Lösungen OT-tauglich machen. Ein Generalist mit einem gesamtheitlichen Ansatz ist Fortinet, der seine Security Fabric auf die OT-Welt erweitert, ergänzt um eine Datenbank mit Sicherheitsinformationen zu zahlreichen OT-Systemen und -Geräten. Und für den Healthcare-Sektor arbeitet Fortinet mit dem Spezialisten Medigate zusammen und integriert dessen Lösung in die Security Fabric.

**Welche Produkte spielen hier eine Rolle?**
Für OT-Umgebungen kommen prinzipiell die gleichen Produkte wie in der IT zum Einsatz, zum Teil in angepassten Rugged-Versionen und ergänzt durch spezielle Services für Industrial Security. Zum Beispiel die Fortigate-Firewalls und Switches für die Segmentierung, FortiAuthenticator für Identitäts- und Zugangsverwaltung oder FortiSIEM für Transparenz und Security Management.

BOLL
IT Security Distribution

**BOLL Engineering AG**

Jurastrasse 58
5430 Wettingen
Tel. 056 437 60 60

info@boll.ch
www.boll.ch