Bildquelle: pozitivstudija /iStock.com

Sicherheit für kritische Infrastrukturen

Mit der Digitalisierung öffnen sich bisher von der Aussenwelt abgeschottete Steuersysteme und kritische Infrastrukturen (Operational Technology, OT) der Aussenwelt – und werden somit auch «empfänglich» für Cyberangriffe. Eine wirksame OT-Security ist demzufolge ein Gebot der Stunde.

Kritische technische Infrastrukturen – unabhängig davon, ob sie für das Funktionieren eines Landes oder eines Unternehmens unerlässlich sind – haben eine über 150-jährige Geschichte hinter sich. Zu Beginn der Industrialisierung wurden Anlagen wie Produktionsmaschinen oder Kraftwerke manuell mithilfe rein mechanisch arbeitender Komponenten wie Schalter und Regler gesteuert. Im fortgeschrittenen 20. Jahrhundert kamen elektrische und elektronische Überwachungs- und Steuersysteme hinzu, die dann immer mehr auch softwarebasiert arbeiteten: Man spricht dabei von Operational Technology, kurz OT.

OT funktionierte lange Zeit im Rahmen geschlossener Systeme: Maschinen, Sensoren, Aktoren und Kontrollsysteme stammten jeweils von einem bestimmten Hersteller, nutzten dedizierte Kommunikationswege und Bedienoberflächen, waren gegenüber anderen Anlagen und der Aussenwelt abgeschottet und konnten ohne physisches Eindringen kaum «gehackt» werden – die Sicherheit von Infrastrukturen wie Produktionsanlagen, Energieversorgung, medizinischen Systemen, Verkehrssystemen und Gebäudetechnik ergab sich aus dem «Air Gap» zum Rest der Welt.

Digitalisierung verändert OT und OT-Sicherheit

Mit der Digitalisierung hat sich dies radikal geändert. OT-Systeme – von der einzelnen PLC-Komponente (Programmable Logic Controller) zur Abfrage und Steuerung von Sensoren und Aktoren über industrielle Kontrollsysteme (ICS) bis hin zum übergreifenden SCADA-System (Supervisory Control and Data Acquisition) für das Management der kompletten OT-Umgebung – sind heute vernetzt, arbeiten mit IT-Systemen zusammen, lassen sich per Fernzugriff kontrollieren und setzen dabei neben herstellereigenen Standards zunehmend auf zwar nach wie vor OT-spezifische, aber standardisierte Protokolle wie etwa Modbus, BACnet, IEC-104DNP3, MQTT und OPC bis hin zu TCP/IP.

Kurz gesagt: Der sicherheitstechnisch traditionell hochgeschätzte Air Gap ist Geschichte, vor allem auch wegen der zunehmenden Nutzung von Remote-Access-Tools für den Umgang mit den OT-Systemen. Durch die vermehrte Offenheit der OT-Systeme wächst die Angriffsfläche gegenüber Cyberattacken. Demzufolge müssen OT-Systeme mindestens ebenso sorgfältig geschützt werden wie IT-Systeme – aber OT ist nicht IT, und es bedarf teils unterschiedlicher Sicherheitsmassnahmen auf verschiedenen Ebenen des für industrielle Kontrollsysteme nach wie vor relevanten Purdue-Modells.

Auf den ersten zwei Ebenen, der Feldebene mit den einzelnen Aktoren und Sensoren wie Ventilen, Pumpen oder Druck-, Temperatursensoren und der Steuerungsebene mit Komponenten wie PLCs, RTUs und IPCs, geht es um die direkte Überwachung und Steuerung der physikalischen Prozesse, die teils manuell über Bedienboards und teils via M2M-Kommunikation (Machine-to-Machine) über spezielle Protokolle erfolgt. Erst ab der dritten, der Prozessleitebene, kommt die Verknüpfung mit IT-basierten Systemen wie SCADA-Servern ins Spiel. Diese wiederum kooperieren mit den IT-Systemen auf den höheren Levels, von der Betriebsleitebene mit MES (Manufacturing Execution Systems) für die Industrie und vergleichbaren Systemen für andere Infrastrukturen bis zur Unternehmensebene mit den bekannten IT-Systemen wie ERP und CRM.

Herausforderungen der OT-Sicherheit

IT- und OT-Sicherheit sind ähnlich herausgefordert: Um die Risiken überhaupt beurteilen zu können,

INTERVIEW MIT ROLF BAMERT, OT-SPEZIALIST, BOLL ENGINEERING

Wie unterscheiden sich OT und IT punkto Sicherheitsrisiken?
Rolf Bamert: Sicherheitsvorfälle in kritischen Infrastrukturen haben eine potenziell viel grössere Tragweite. Bei einem IT-Vorfall verliert eine Firma Geld, Reputation und allenfalls Kunden. Bei einem Ereignis zum Beispiel in einer Versorgungsinfrastruktur können Menschen zu Schaden kommen oder sogar sterben, oder es kommt zu Umweltschäden. Wenn etwa die Wasserversorgung von Zürich kontaminiert ist, ist die Gesundheit von Hunderttausenden Menschen in Gefahr.

Und was zeichnet OT-Sicherheit im Vergleich zur IT-Security aus?
Im Vergleich zur IT, die man als wendiges Motorboot sehen kann, kommt die OT eher als grosser Tanker daher. Jede Kursänderung erfordert Aufwand und Zeit und will sorgfältig geplant sein. OT-Systeme sind auf Langlebigkeit und höchste Zuverlässigkeit ausgelegt und werden oft jahrelang unverändert betrieben. Darauf müssen auch die Sicherheitsmassnahmen Rücksicht nehmen.

Was heisst das konkret?
OT-Systeme mit Schwachstellen lassen sich nicht einfach so auf eine neue Version aktualisieren oder ausmustern und Geräte nicht wie IT-Systeme regelmässig patchen, ohne möglicherweise deren Funktion zu stören – beispielsweise ein Weichen-Stellwerk der Bahninfrastruktur oder Verkehrsleitsysteme. Jede Unterbrechung ist unerwünscht und könnte negative Folgen haben. Stattdessen empfehlen sich Workarounds wie «Virtual Patching» mithilfe vorgeschalteter Schutzsysteme, damit Bedrohungen gar nicht erst zum Gerät gelangen.

In der IT wird oft automatisiert mit Bedrohungen und Schwachstellen umgegangen. Wie steht es damit in der OT?
Ein automatisches Enforcement ist in der OT-Welt nicht zielführend, denn zur Bestimmung der erforderlichen Massnahmen ist detailliertes Prozesswissen nötig: Wenn Ventil X aufgrund eines Sicherheitsalarms plötzlich geschlossen wird, könnte dies den ganzen Prozess zu Fall bringen – in einem anderen Prozess hätte es vielleicht keine Auswirkungen. Ein anderes Beispiel: Eventuell ist die Firmware-Aktualisierung eines Elements gar nicht nötig, weil es zwar vorhanden, aber für den Betrieb nur wenig relevant ist.

Fernzugriff für Wartung und Verwaltung ist in der OT zunehmend gang und gäbe. Was gilt es hier zu beachten?
Vor allem eines: Die Zugriffskontrolle und die Überwachung müssen so streng gehandhabt werden wie beim physischen Zutritt zu einem Rechenzentrum oder einem Kraftwerk, das heisst starke Authentifizierung mit mehreren Faktoren und Biometrie sowie Monitoring und Aufzeichnung aller Remote-Sitzungen – beim Besuch vor Ort wird man ja auch strikt kontrolliert und begleitet.

muss zuerst bis ins Detail bekannt sein, wie die Infrastruktur aufgebaut ist. Danach geht es darum, die Angriffsfläche und mögliche Angriffswege zu verstehen. Nur so lässt sich die Infrastruktur in einem weiteren Schritt adäquat schützen.

Dabei fällt auf, dass eine Reihe von IT-Security-Themen auch in der OT-Security höchst relevant sind. So etwa ein umfassendes Inventar aller Systeme und Geräte, die Analyse anfallender Log-Informationen und stets zu wissen, welche Systeme und Geräte auf welche Weise mit anderen kommunizieren. Ebenfalls dazu gehören die Absicherung einzelner Systeme und Bereiche durch Netzwerksegmentierung, starke Authentifizierung sowie Verschlüsselung der Kommunikation. Und hier findet sich schon die erste OT-spezifische Herausforderung: Traditionell wurde in der OT kaum segmentiert, allenfalls einfach authentifiziert, und kaum verschlüsselt. Mehr zu den Unterschieden zwischen OT- und IT-Security findet sich im Interview mit Rolf Bamert, OT-Spezialist bei BOLL Engineering.

Optionen für die OT-Security

Sowohl bekannte Anbieter von IT-Security-Lösungen als auch Spezialisten für OT-Security bieten OT-orientierte Sicherheitslösungen in verschiedenen Funktionsbereichen an, die BOLL im Distributionsprogramm führt. Für die Segmentierung, aber auch für Malwareschutz und Bedrohungserkennung bieten sich Firewall-Hersteller wie Fortinet und Palo Alto Networks an, die teils mit spezieller Hardware für harsche Umgebungen aufwarten. Ein zuverlässiges Inventar erstellen Lösungen von Palo Alto (cloudbasiert) und Claroty (Cloud oder On-Premises). Den besten Schutz für den Fernzugriff und die Nachvollziehbarkeit aller Vorgänge ermöglichen Privileged-Access-Management-Plattformen (PAM) wie diejenige von Fudo Security oder Claroty, abgesicherten Remote Access bieten indes auch Fortinet und Palo Alto Networks.

BOLL
IT Security Distribution

BOLL Engineering AG

Jurastrasse 58
5430 Wettingen
Tel. 056 437 60 60

info@boll.ch,
www.boll.ch