OT- und IoT-Sicherheit: Neue Herausforderungen für die Industrie

Cyberangriffe auf Operational Technology (OT) und Internet of Things (IoT) nehmen explosionsartig zu. Dabei geht es um Technologien und Geräte, die Maschinen und Produktionsanlagen kontrollieren oder mittels Sensoren Daten aus der Umgebung gewinnen.

Bild: © Getty Images

Ruedi Kubli

Akteure wie Produktionsstätten, Versorgungsbetriebe, kritische Infrastrukturen und das Gesundheitswesen basieren heute auf digital gesteuerten Prozessen und sind infolgedessen immer stärker mit der IT vernetzt.

Für Cyberkriminelle entstehen dadurch neue Angriffsmöglichkeiten, die den Betrieb zum Erliegen bringen oder sogar Menschenleben gefährden können.

Neue Regularien wie die EU-Richtlinie NIS2 oder der IKT-Minimalstandard des Bundes schreiben daher Schutzmassnahmen vor. IoT-Geräte sind grundsätzlich mit dem Internet verbunden, verfügen jedoch meist nicht über hinreichenden Schutz.

Im Austausch mit der IT

Dadurch können Cyberkriminelle oft unkompliziert die Firmware auslesen, manipulieren und zurückspielen.

Schon mehrfach vorgekommen ist der Missbrauch solcher Geräte für Botnetze und Denial-of-Service-Attacken – IoT-Geräte sind üblicherweise 24/7 in Betrieb und bieten eine ideale Plattform für derartige Angriffe. OT-Systeme waren traditionell vom Internet abgeschottet, aber die Digitalisierung industrieller Prozesse und die Verknüpfung mit höheren Ebenen des Purdue-Modells haben die Angriffsfläche ausgeweitet. Industrial IoT löst zusätzlich die hierarchische Struktur des Modells teilweise auf, indem Sensoren und Aktoren bereits auf der untersten Ebene mit dem Internet in Verbindung stehen.

Grundprobleme und reale Bedrohungen
Viele IoT-Geräte verfügen kaum über Schutzfunktionen. Standardpasswörter werden oft nicht geändert, manchmal sind Passwörter sogar in der Firmware hardkodiert. Zudem werden die zu übertragenden Daten häufig unverschlüsselt an Cloud-Dienste übermittelt.

Auch ältere OT-Anlagen verfügen meist nicht über umfangreiche Schutzmassnahmen und lassen sich nur schwer aktualisieren. Ein Austausch ist kaum möglich, da dies die Produktion unterbrechen würde. Dazu kommt, dass solche Anlagen auf jahre- bis jahrzehntelangen Betrieb ausgelegt sind und nicht dem neuesten sicherheitstechnischen Stand entsprechen.

Die Bedrohungen sind real. So wurde das Mikromobilitätsunternehmen Ridemovi durch eine Fake-App attackiert, wodurch sich Mietfahrräder gratis nutzen liessen und weswegen zum Beispiel in Bologna 80 Prozent der Fahrzeuge ausser Betrieb gesetzt werden mussten.

In Moskau beeinträchtigte die Malware Fuxnet IoT-Sensoren für Abwasser und Fernwärme, dies bis hin zur physischen Beschädigung von Speicherchips. Die Hotelkette Omni erlitt elf Tage Betriebsstörung und 40 Millionen Dollar Umsatzverlust, weil Angreifer die Keycard-Infrastruktur manipulierten.

Dazu kam ein Abfluss von Millionen Kundendatensätzen. Und der Traubensafthersteller Welch Foods war drei Wochen lang lahmgelegt, als Ransomware die Produktionsanlagen verschlüsselte.


Bild: BOLL Engineering

Der Autor: Ruedi Kubli, Business Development Manager für OT/IoT, BOLL Engineering, Wettingen

Security by Design ausschlaggebend
Das wichtigste Prinzip bei OT und IoT hinsichtlich Sicherheit heisst Security by Design: Sicherheit muss von Anfang an einbezogen werden.

Die Firmware ist minimalistisch zu gestalten, um die Angriffsfläche zu reduzieren. Nicht genutzte Funktionen müssen deaktiviert werden.

Bewährte Schutzmassnahmen umfassen Mikrosegmentierung zur Isolierung gefährdeter Geräte, Zero-Trust-Architekturen und PAM-Lösungen für den Remote-Zugang. Eine vollständige Inventarisierung aller Netzwerkgeräte ist unerlässlich, idealerweise mit Device Fingerprinting und Erkennung von Firmware-Versionen und Schwachstellen.

Bei älteren Anlagen ohne Update-Möglichkeit hilft das sogenannte Virtual Patching. Dabei handelt es sich um ein vorgeschaltetes System auf neuestem Stand, das nur legitime Zugriffe weiterleitet. Und nach Supportende müssen Geräte nach festgelegtem Prozess ausser Betrieb genommen werden, man darf sie nicht weiter einsetzen.

Umfangreiches Lösungsangebot
Der Markt reagiert: Spezialisierte OT- und IoT-Security-Anbieter wie Claroty, Asimily und Cyolo bieten Lösungen für OT-, IoT- und Medical-IoT-Umgebungen an. Aber auch traditionelle IT-Security-Hersteller wie Fortinet und Palo Alto Networks erweitern ihre bewährten Lösungen zunehmend mit entsprechenden Features. Einer ganzheitlichen OT- und IoT-Security sollte demzufolge nichts mehr im Wege stehen.

boll.ch