OT- und IoT-Sicherheit bis zum einzelnen Gerät

Know-how Mit der Digitalisierung von Produktionsabläufen und dem Aufkommen des IoT verwischen die Grenzen zwischen Internet, IT und Industrieanlagen zunehmend. Damit wird der Schutz der betroffenen Geräte und Anlagen zur unabdingbaren Sicherheitsmassnahme.

Von Ruedi Kubli

Dass Cyberangriffe geradezu explosionsartig zunehmen, dürfte mittlerweile allgemein bekannt sein. Cyberkriminelle zielen jedoch nicht nur auf klassische IT-Umgebungen, sondern zunehmend auch auf Anlagen und Geräte in industriellen Betrieben sowie auf kritische Infrastrukturen. In diesen Bereichen spricht man von Operational Technology (OT) respektive vom Internet of Things (IoT). Dabei geht es um sämtliche Technologien und Geräte, die den Betrieb von Maschinen und Produktionsanlagen kontrollieren oder – wie beispielsweise Sensoren – aus der jeweiligen Umgebung Daten gewinnen, um die Steuerung überhaupt zu ermöglichen.

IT, OT und IoT

Auch Produktionsstätten, Versorgungsbetriebe, Verkehrsinfrastrukturen und Einrichtungen des Gesundheitswesens basieren vermehrt auf digital gesteuerten Prozessen und sind immer mehr mit der IT der jeweiligen Organisation vernetzt. Für Cyberkriminelle entstehen dadurch neue Möglichkeiten für Angriffe, die den betroffenen Unternehmen ganz direkt ans Lebendige gehen – und dies sogar im wörtlichen Sinn –, weil bei Fehlfunktionen der Betrieb völlig zum Erliegen kommen kann oder sogar Menschenleben gefährdet werden. Es liegt also auf der Hand, dass industrielle Steuerungssysteme, OT-Systeme im Allgemeinen sowie IoT-Geräte mindestens ebenso wie IT-Systeme geschützt werden müssen. Dies umso mehr, als neue Regularien wie die EU-Richtlinie NIS2 oder der vom Bund lancierte IKT-Minimalstandard Massnahmen zur Absicherung vorschreiben – aber auch, weil ein Cybervorfall, egal ob in IT, IoT oder OT, praktisch immer mehr Kosten und Aufwand verursacht als eine sinnvolle Vorbeugung.

IoT-Geräte sind schon vom Prinzip her grundsätzlich mit dem Internet verbunden, verfügen jedoch meist nicht über einen auch nur ansatzweise hinreichenden Schutz vor Angriffen und Manipulation. So können Cyberkriminelle bei manchen Geräten relativ unkompliziert zum Beispiel die Firmware auslesen, den eigenen Bedürfnissen anpassen und wieder zurück auf das Gerät spielen. Es ist schon vorgekommen, dass eine Vielzahl solcher Geräte für ein Botnetz missbraucht wurde, um damit Denial-of-Service-Attacken zu fahren. IoT-Geräte bieten dafür geradezu ideale Voraussetzungen, denn sie sind üblicherweise 24/7 in Betrieb.

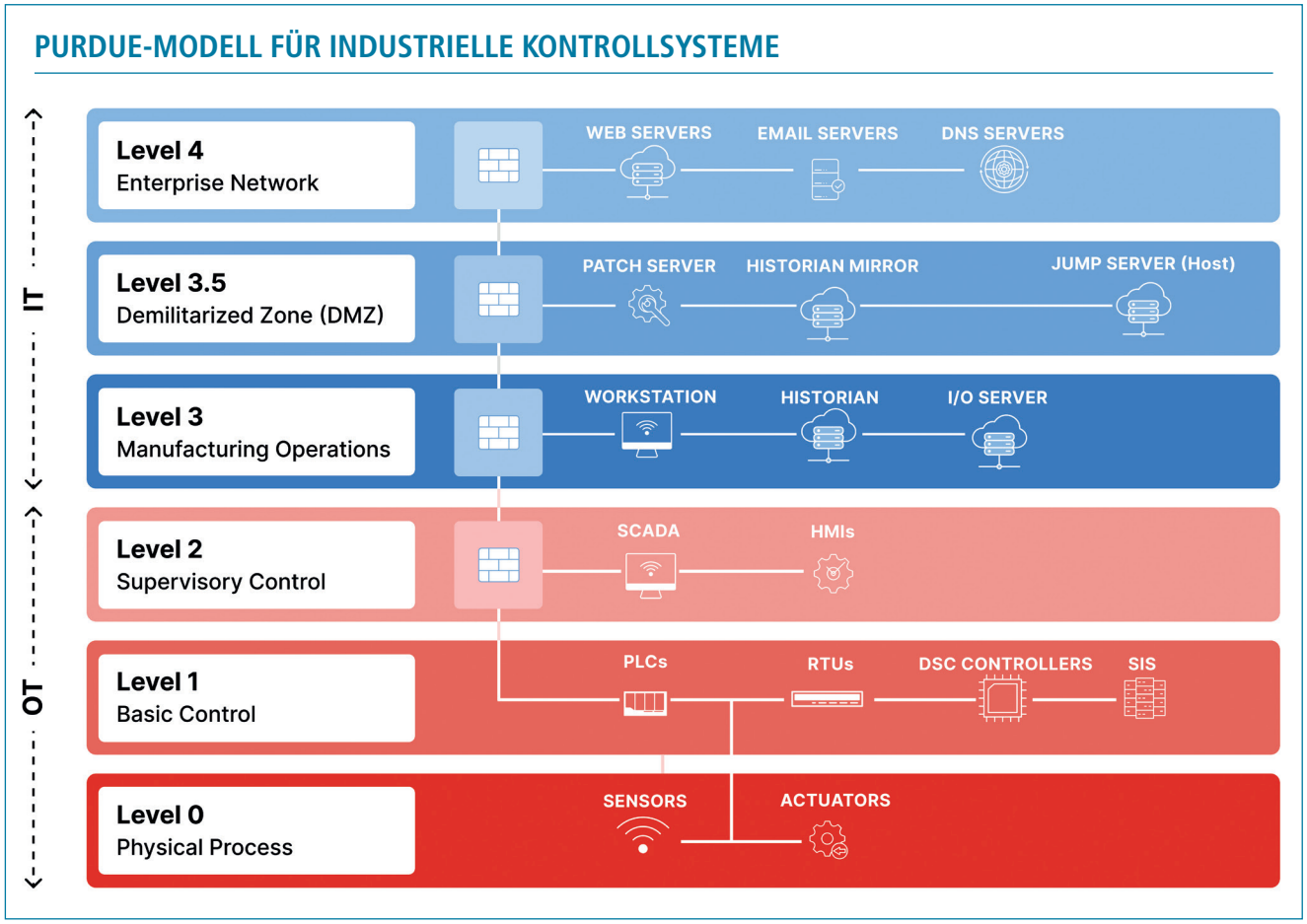
Wohlgemerkt: Unter dem Begriff IoT ist hier nicht primär die Rede von vernetzten Geräten für den Privatgebrauch (von der Smartwatch über die per App steuerbare Lampe bis zum kompletten Smarthome), sondern von Sensoren und Aktoren im industriellen Umfeld (Industrial IoT, IIoT) sowie im Gesundheitswesen (Medical IoT).

OT-Systeme sind im Gegensatz zur IoT-Welt traditionell vom Internet abgeschottet, aber die zunehmende Digitalisierung der industriellen Prozesse und die dafür erforderliche Verknüpfung der OT mit höheren Ebenen des Purdue-Modells – siehe Grafik –, in denen IT-Systeme bis hin zum ERP zum Einsatz kommen, hat die Grenze in den letzten Jahren zunehmend aufgeweicht und die Angriffsfläche dementsprechend ausgeweitet. Dazu kommt, dass Industrial IoT die streng hierarchische Struktur des Purdue-Modells teilweise auflöst. So kommen bereits in den unteren zwei Ebenen (Sensoren/Aktoren und Steuerungen) zunehmend Funktionen zum Einsatz, die eine Kommunikation mit anderen Systemen erfordern, was die ohnehin schon vergrösserte Angriffsfläche zusätzlich ausweitet.

DIE 10 KRITISCHSTEN SICHERHEITSRISIKEN IM IOT-UMFELD

1 Schwache, leicht zu erratende oder fest eingebaute Passwörter
2 Unsichere Netzwerkdienste
3 Unsichere Schnittstellen im Ökosystem
4 Fehlender sicherer Update-Mechanismus
5 Verwendung unsicherer oder veralteter Komponenten
6 Fehlender angemessener Datenschutz
7 Unsichere Datenübertragung und -speicherung
8 Fehlendes Gerätemanagement
9 Unsichere Standardeinstellungen
10 Fehlende physische Härtung

Quelle: OWASP



IoT löst die strenge Hierarchie im Purdue-Modell teilweise auf, da damit auch Geräte in den untersten Ebenen mit anderen Systemen kommunizieren müssen. Quelle: Fortinet

Grundprobleme vieler IoT-Geräte

Manche IoT-Geräte verfügen kaum über Schutzfunktionen – nur schon hinsichtlich Zugriff. Ist ein Passwortschutz vorhanden, wird dieser oft schon deshalb obsolet, weil die vorgegebenen Standardpasswörter von den Anwendern nicht abgeändert werden. In einigen Fällen ist das Passwort sogar in der Firmware hardkodiert – aus Security-Sicht ein absolutes No-Go. So haben Angreifer praktisch beliebigen Zugriff auf die Geräte. Und in vielen Fällen werden die übertragenen Daten nicht verschlüsselt an einen Cloud-Dienst übermittelt, was das Risiko weiter steigert und sensible Daten exponiert.

Ein zweischneidiges Schwert ist dabei die spezialisierte Suchmaschine namens Shodan (shodan.io), mit der sich IoT-Geräte weltweit auffinden lassen. Einerseits erhalten Firmen, Cloud-Provider und die Forschung nützliche Einblicke ins Internet of Things, andererseits können natürlich auch Cyberkriminelle von der IoT-Suche profitieren und damit verwundbare Geräte identifizieren. Dabei lässt sich die Suche gezielt eingrenzen. So ist es zum Beispiel möglich, alle Geräte eines bestimmten Typs in der Schweiz zu finden.

OT auf Langlebigkeit ausgerichtet

OT-Systeme sind grundsätzlich auf möglichst hohe Langlebigkeit ausgerichtet und oft jahrzehntelang im Einsatz. Ältere Anlagen sind meist nicht mit umfangreichen Schutzfunktionen ausgestattet, was den externen Zugang betrifft.

Wenn Sicherheitsfunktionen bestehen, lassen sich diese oft nicht oder nur durch eine Intervention des Herstellers mit Sicherheitsupdates aktualisieren. Ein Austausch durch neuere Anlagen ist kaum möglich – dadurch wäre die Produktion oder die Versorgungsleistung unterbrochen, was besonders, aber nicht nur im Fall kritischer Infrastrukturen breitflächige Konsequenzen hätte.

Angriffe auf OT und IoT sind real

Dass Cyberattacken auf OT- und IoT-Systeme keine blosse Theorie, sondern harte Realität sind, zeigen zahlreiche Beispiele aus den vergangenen Jahren. Aus der Schweiz hört man bislang vergleichsweise wenig von solchen Angriffen, da es hierzulande bis jetzt keine umfassende Meldepflicht gibt, ausser für Betreiber kritischer Infrastrukturen, welche seit dem 1. April 2025 gegenüber dem Bundesamt für Cybersicherheit (BACS) meldepflichtig sind. Einige Beispiele aus der ganzen Welt zeigen aber, dass die Risiken durchaus ernst zu nehmen sind.

Im Juli 2024 erfolgte ein Angriff auf das 2018 gegründete Mikromobilitätsunternehmen Ridemovi, das zum Beispiel in verschiedenen italienischen Städten E-Bikes und klassische Fahrräder zur Miete bereitstellt, die sich über eine App buchen lassen. Cyberkriminelle verbreiteten eine Fake-App, mit der sich die Fahrräder kostenlos nutzen liessen. Dies hatte etwa zur Folge, dass in Bologna 80 Prozent der Fahrräder ausser Betrieb gesetzt werden mussten. Das Beispiel zeigt die Verwundbarkeit IoT-basierter digitaler Infrastrukturen, wobei auch die Lieferkette eine Rolle spielt.

In Moskau gab es eine Attacke auf das Versorgungsunternehmen Moscollector. Das Ziel der Angreifer waren IoT-Sensoren für Abwasser und Fernwärme. Im Rahmen des Angriffs wurde mithilfe einer Malware namens Fuxnet das Dateisystem beschädigt und die Firmware umprogrammiert. Dies hatte zur Folge, dass NAND-Speicherchips physisch beschädigt und die Kommunikationskanäle mit Zufallsdaten überschwemmt wurden.

Ein weiteres Beispiel zeigt, dass auch persönliche Daten von Kunden betroffen sein können. Die Hotelkette Omni litt unter einer elf Tage langen Betriebsstörung, weil Cyberkriminelle den Keycard-Zugang zu den Zimmern und das Reservierungssystem manipulierten. Für das Unternehmen resultierte ein geschätzter Umsatzverlust von 40 Millionen US-Dollar, und die Angreifer erlangten Zugang zu 3,5 Millionen Datensätzen von Hotelgästen.

Der US-amerikanische Traubensafthersteller Welch Foods wurde Opfer eines Ransomware-Angriffs, bei dem nicht die Daten auf IT-Systemen, sondern die Systeme der Produktionsanlage verschlüsselt wurden. Der Herstellbetrieb des Unternehmens, das im Besitz einer Kooperative von Traubenanbauern ist, war drei Wochen lang unterbrochen.

Ein weiterer Ransomware-Fall wurde mithilfe von Ransomware as a Service möglich: Der Allergiemedikamentenhersteller HAL Allergy wurde exakt in der Nachfragespitze vor der Frühlingssaison von einer Gruppe attackiert, die die Doppelerpressungs-Ransomware Ransomhouse nutzte. Aus dem Angriff auf die Auftragsbearbeitung und die Produktlieferung resultierte eine 32-tägige Störung.

Security by Design ist Pflicht

Bei all diesen Angriffen stellt sich die Frage, wie Hersteller oder Entwickler ihre Lösungen vor entsprechenden Attacken schützen können. Das wichtigste Prinzip dabei heisst Security by Design. Sicherheit muss von Anfang an in die Herstellung oder Entwicklung eines Produkts einbezogen werden. Es ist darauf zu achten, dass die Lösungen keine Schwachstellen enthalten. Dem kann man sich unter anderem damit annähern, dass die Firmware möglichst minimalistisch gestaltet wird, was die Angriffsfläche implizit reduziert.

Auf der Anwenderseite ist es wichtig, sämtliche Funktionen zu deaktivieren, die nicht wirklich genutzt werden. Dazu kommen weiter die Netzwerkarchitektur und der Umgang mit den Zugängen aufs Netzwerk. Ein probates Mittel ist die Isolierung potenziell betroffener Geräte und Anlagen durch Mikrosegmentierung, die mit modernen Firewall-Systemen kein Problem darstellen sollte und die OT-Anlagen und IoT-Geräte von den IT-Systemen wirkungsvoll abschottet.

Für den Zugang auf das Netzwerk und die darin eingebundenen Geräte sollte eine Zero-Trust-Architektur zum Zug kommen. Diese basiert auf dem Grundprinzip, dass alle Zugänge und Zugriffe prinzipiell unterbunden werden, wenn sie nicht explizit erlaubt sind. Zugriff heisst dabei nicht nur der Zugriff durch menschliche Akteure, sondern auch durch Aktivitäten von Software und Geräten. Zur Absicherung des gerade bei OT-Anlagen oft erforderlichen Remote-Zugangs, zum Beispiel durch Techniker des Herstellers, setzt man am besten auf eine PAM-Lösung (Privileged Access Management) respektive auf eine SRA-Lösung (Secure Remote Access).

Ganz allgemein ist es naturgemäss unerlässlich, zu wissen, welche Geräte im Netzwerk überhaupt vorhanden sind. Dies ist erstaunlicherweise in manchen Umgebungen nicht gegeben. Hier hilft nur eine Inventarisierungslösung, die idealerweise weiter geht, als nur das Vorhandensein von Geräten zu erkennen. Genauso wichtig ist es, dass der exakte Typ des Geräts, die Firmware-Version, bekannte Schwachstellen sowie die Kommunikation eines Geräts mit anderen Geräten und Systemen aufgezeigt werden. Eine Basis für die Inventarisierung kann Device Fingerprinting sein, um zu erkennen, welche Geräte überhaupt im Spiel sind. Auf dieser Grundlage lässt sich zum Beispiel die genannte Mikrosegmentierung sinnvoll planen und umsetzen. Und ganz allgemein: Ein Inventar hilft, Risiken zu erkennen – eine unabdingbare Voraussetzung, um diese Risiken anzugehen und zu minimieren.

Patch-Management, wie es in der IT üblich ist, ist zumindest bei gewissen Geräten und bei älteren Anlagen in der OT oft nicht möglich. Falls es keine Sicherheitsupdates gibt, lässt sich die Sicherheit durch Virtual Patching verbessern. Dabei wird der betreffenden Anlage als Abschirmung ein System vorgeschaltet, das sicherheitstechnisch auf den neuesten Stand gebracht werden kann und das nur legitime Zugriffe auf die Anlage weiterleitet.

Doch sogar wenn es für ein System regelmässige Aktualisierungen gibt, endet der Support des Herstellers üblicherweise nach einer gewissen Zeit. In der IT ist das sattsam bekannt. So endet etwa der Support für Windows 10 im Oktober 2025. Im Fall von Anlagen und Geräten lässt sich nicht einfach ein neues Betriebssystem installieren. Die Geräte müssen vielmehr nach einem festgelegten Prozess ausser Betrieb genommen und, falls nötig, durch neue ersetzt werden. Sonst können Schwachstellen, die nicht mehr gepatcht werden, ernsthafte Risiken mit sich bringen.

Cybersecurity-Hersteller auf OT-Pfaden

Auf dem Markt sind verschiedene Hersteller, die sich spezifisch mit OT- und IoT-Sicherheit beschäftigen, teils sogar spezialisiert auf bestimmte Sektoren wie Medical IoT. Aber auch Security-Anbieter, die traditionell auf IT-Security fokussiert sind, haben die Zeichen der Zeit erkannt und statten ihre Lösungen zunehmend mit Funktionen aus, die auf OT- und IoT-Umgebungen zugeschnitten sind. Dazu gehören die bekanntesten Hersteller fortschrittlicher Firewalls, aber auch Softwareanbieter mit Lösungen in Disziplinen wie Vulnerability-Management und Attack-Surface-Management. ■

DER AUTOR

Ruedi Kubli ist als Business Development Manager für OT und IoT beim auf IT-Security spezialisierten Distributor Boll Engineering in Wettingen tätig. Er verfügt über mehrere Zertifizierungen von Herstellern wie Claroty und Fortinet sowie weitere Security-Zertifizierungen wie CISSP Certified Information Systems Security Professional und CISA Certified Information Systems Auditor