Cyber-Sicherheit für Produktionsprozesse

Sicherheit im industriellen „Internet of Things“

Das „Internet of Things“ (IoT) ermöglicht der produzierenden Industrie einen riesigen Innovationssprung. Soll IoT ein Erfolg werden, müssen Cyber-Angriffe und Netzwerkprobleme allerdings rechtzeitig erkannt und konsequent abgeblockt werden – und zwar ohne, dass sich die Produktionsprozesse dadurch verzögern. Benötigt werden dafür speziell auf die Industrie ausgerichtete IT-Sicherheitslösungen….

Im Zeitalter des IoT werden Maschinen, Werkzeuge und Steuerungsgeräte zu Trägern digitaler Informationen. Sie sind „smart“ und können Daten verarbeiten und Befehle selbstständig weitergeben. Für die produzierende Industrie entstehen mit der Entwicklung des IoT neue Chancen. Produktionsprozesse werden beispielsweise dynamischer und effizienter. Gleichzeitig gehen mit der wachsenden Anzahl der mit dem Internet verbundenen Geräte jedoch auch Sicherheitsrisiken einher. Cyber-Kriminelle können die Schnittstellen mit dem Netz als Angriffspunkt nutzen – mit gravierenden Folgen. Diese reichen vom Verlust sensibler Unternehmensinformationen über die Sabotage einzelner Maschinen bis hin zu Produktionsausfällen.

Tatsache ist:

IT-Sicherheit gilt bei Unternehmen inzwischen als wichtigste Hemmnis beim Thema Industrie 4.0. Das ist das Ergebnis einer Studie der IDG Communications Media AG. Die Studienergebnisse wurden jüngst auf der Hannover Messe vorgestellt. Die Umfrage zeigt, dass die größte Sorge von Unternehmen Hackerangriffen oder DDoS-Attacken gilt, gefolgt von Industriespionage und dem daraus resultierenden Verlust der Wettbewerbsfähigkeit. Gleichzeitig gehen zwei Drittel (65 Prozent) der Unternehmen davon aus, dass Industrie 4.0 innerhalb der nächsten drei Jahre für sie wichtig oder sehr wichtig wird. Die Aussagen unterstreichen das Ergebnis der Studie „IT-Sicherheit für Industrie 4.0“ des Bundeswirtschaftsministeriums aus dem vergangenen Jahr. Dieses lautete: Die IT-Sicherheit ist zunehmend technische Voraussetzung und entscheidender Enabling-Faktor für die Industrie 4.0.

Netzwerk wird zur Blackbox

Vor allem dort, wo Maschinen und Anlagen für den Fernzugriff mit Herstellern und Wartungstechnikern vernetzt sind, entstehen hohe Sicherheitsrisiken. Über Fernwartungszugänge und Update-Interfaces an den Maschinen entstehen Schlupflöcher, durch die Daten unerwünscht nach außen dringen oder schädliche Daten ins Unternehmen gelangen können. Diesen Gefahren haben die in den Produktionsnetzwerken eingesetzten industriellen Leit- und Steuerungskomponenten kaum etwas entgegenzusetzen. Denn die meisten Komponenten der Steuerungs- und Regelungstechnik wurden in der Vergangenheit mit Blick auf deren Verfügbarkeit und nicht auf deren Sicherheit

Autorin:

Anja Dienelt,
Solution Manager IoT,
Rohde & Schwarz
Cybersecurity

entwickelt. Solange die Produktionsnetze von der übrigen IT-Infrastruktur getrennt waren, gab es deutlich weniger Angriffsmöglichkeiten. Mit dem Aufkommen des „Internet der Dinge“ und der Industrie 4.0 ändert sich dies.

Durch die Industrienetzwerke fließen immer mehr Daten, was daran liegt, dass diese enorm schnell anwachsen und im Gegensatz zum homogenen Office-Netz eher heterogen sind und geprägt von unterschiedlichen Anlagenlieferanten, die die Hoheit über ihre Maschinen haben. Das Netzwerk wird zur Blackbox, in der Informationen und Befehle unbeobachtet ausgetauscht werden – etwa für die Fernwartung von Anlagen, um Produktinformationen an Produktionssysteme weiterzugeben, eine permanente Zustandsüberwachung von Anlagen zu erlangen (Condition Monitoring) und um Logistikprozesse zu synchronisieren. Externe Partner haben zunehmend Zugriff auf dieses Netzwerk. Denn Maschinenbauer integrieren ihre eigenen IoT-Lösungen in ihre Geräte, sodass der Anlagenbetreiber letztlich kaum noch weiß, was auf seinem Netz läuft. Gleichzeitig ist er darauf angewiesen, dass die Produktion kontinuierlich und ohne Unterbrechungen arbeitet. Jegliche Latenzzeit muss vermieden werden. Nur dann wird Industrie 4.0 für die Industrie tatsächlich zur Chance.

Mehrstufiges Sicherheitskonzept

Um sich vor Angriffen und Netzwerkproblemen zu schützen, müssen Industrieunternehmen daher Gefahren aufdecken, Anomalien visualisieren und das Netzwerk vor Angriffen schützen – und zwar sehr schnell, sodass es innerhalb der Produktionsprozesse zu keinerlei Verzögerungen kommt.

Dafür ist ein mehrstufiges Sicherheitskonzept notwendig, bestehend aus:

1. Netzwerk-Sensor
2. Reporting-Tool
3. Industrie-Firewall

1. Der Netzwerk-Sensor

– auch als Probe bezeichnet – wird an mehreren Stellen in das Netzwerk eingefügt. Dort schneidet er den Netzwerkverkehr mit und analysiert ihn. Auf diese Weise lässt sich zum einen erkennen, was in

der Leitung passiert – gleichzeitig lassen sich Angriffe finden.

Kern einer solchen Netzwerkanalyse ist eine sogenannte Deep Packet Inspection (DPI)-Engine. Anstatt den Datenverkehr über den genutzten „Port“ zu klassifizieren, werden mit dem DPI-Verfahren die Daten inhaltlich dekodiert. Erst das ermöglicht detaillierte Einblicke in den Datenverkehr. Auf diese Weise werden auch versteckte Angriffe auch in erlaubten Protokollen gefunden.

2. Reporting-Tool

Das Reporting-System trifft auf Basis dieser Daten Aussagen zum Zustand des Netzes, wie etwa die Kommunikationsbeziehungen im Netz oder das Kommunikationsverhalten einzelner Maschinen. Die gewonnenen Daten verschaffen Unternehmen die entscheidende Grundlage zur Sicherung eines kontinuierlichen Betriebs und ermöglichen darüber hinaus eine genauere Planbarkeit hinsichtlich Netzwerkauslastung und -dimensionierung.

Es gibt sogar die Möglichkeit, dass das Reporting Anomalien in dem Moment visualisiert, in dem sie im Netzwerk auftreten. Ein solches Event-Monitoring weist Administratoren und Betreiber industrieller Netze sofort auf mögliche Probleme im Netz hin. Probleme, die aus infizierten Maschinensteuerungen, Fehlkonfigurationen oder potenziellen Cyber-Angriffen resultieren können, lassen sich auf diese Weise schnell erkennen. Ein zeitnahes „Troubleshooting“ ist möglich, noch bevor die Produktion vom Angriff beeinflusst wird und hohe Kosten entstehen.

3. Die Industrie-Firewall

Neue Abwehrtechnologien werden benötigt. Bislang wurden Prozess- und Steuerungsnetze hauptsächlich durch klassische Firewalls geschützt, die das Firmennetzwerk im Ganzen vor Angriffen von außen sichern (First Line of Defense). Solche Perimeter-Firewalls reichen als Schutzkonzept in komplexen Industrienetzwerken nicht mehr aus. Benötigt werden stattdessen zusätzlich Firewalls, die im Inneren des Netzes arbeiten und dieses in mehrere Zonen segmentieren. Solche „Brandabschnitte“ sorgen dafür, dass im Falle eines Angriffs, der Schaden nicht auf das gesamte Netzwerk übertreten kann.

Um auch unbekannte Angreifer fernzuhalten, braucht die Industrie zudem Firewalls mit einer integrierten DPI-Engine. Diese ermöglicht einen sogenannten proaktiven Schutz mittels Whitelisting. Dieses Konzept stellt sicher, dass Industrienetzwerke nur von autorisierten Personen mit definierten Befehlen angesteuert werden. Auf diese Weise wird auch ein Schutz vor „Zero-Day-Exploits“ möglich, also vor Cyber-Angriffen die Sicherheitslücken ausnutzen, die noch unbekannt sind und deshalb nicht geschlossen wurden.

Hohe Performance

Neben der Genauigkeit bei der Datenerkennung, spielt die Zuverlässigkeit der Performance in der Industrie eine entscheidende Rolle. Latenzzeiten gilt es zu vermeiden, denn Produktionsprozesse dulden keine Unterbrechung. Die Datenübertragung in einem Produktionsnetzwerk muss stets sofort erfolgen, deshalb sollte eine Industrie-Firewall mit der sogenannten „Single-Pass-Technologie“ arbeiten, bei der der Netzverkehr parallel statt sequentiell bearbeitet wird. Das steigert die Performance erheblich.

Und schließlich sollte eine Firewall für Industrienetzwerke auch verschiedene Industrieprotokolle, wie SCADA, Modbus TCP oder DNP 3 unterstützen, damit sie diese auch erkennen und dekodieren kann. Die Hardware muss zudem so konzipiert sein, dass sie auch für anspruchsvolle Einsatzorte wie Produktionshallen, Windparks, Werkstätten oder für das Verkehrswesen (bspw. Schifffahrtsindustrie) geeignet ist. Mit einer gehärteten Hardware schützt die Firewall auch unter extremen Temperaturverhältnissen oder unter EMV-Einflüssen – also ungewollten elektrischen oder elektromagnetischen Effekten – verlässlich das Netzwerk.

■ *Rohde & Schwarz Cybersecurity GmbH & Co. KG.*
cybersecurity.rohde-schwarz.com