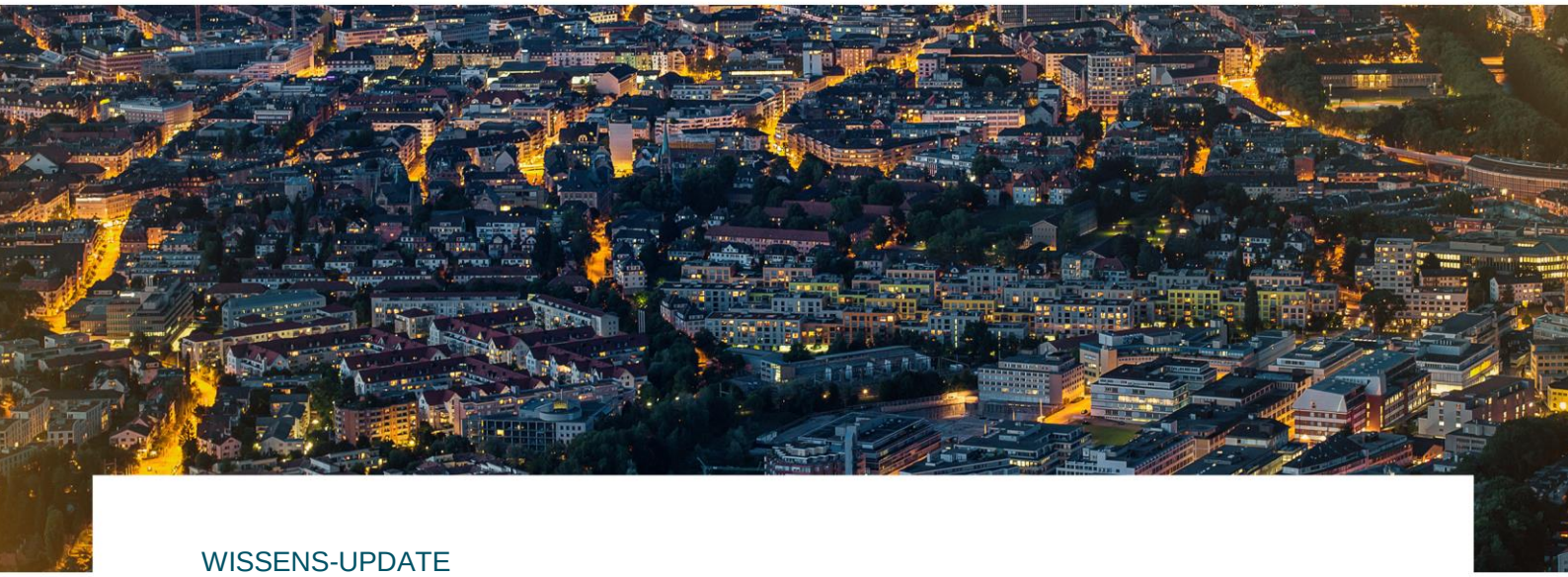
CyOne Security AG
Hinterbergstrasse 18
6312 Steinhausen

Telefon +41 41 748 85 00
info@cyone.ch
cyone.ch



WISSENS-UPDATE

IIoT Security in der Smart Factory – damit der technische Fortschritt nicht zum Bumerang wird

Reto Amstad | Senior Security Consultant | Steinhausen, 10. August 2021

Wenn Maschinen und Produkte miteinander kommunizieren, werden Produktionsprozesse flexibler, effizienter und autonomer. So die Vision der Smart Factory. Die durchgängig digitale Vernetzung schafft aber auch neue Cyber-Risiken. Diese unter Kontrolle zu bringen, gelingt ausschliesslich mit einer systemübergreifenden Sicherheitsarchitektur, welche bereits bei der Entwicklung des einzelnen Produkts beginnen soll.

Der Smart Factory gehört die Zukunft. Dank Digitalisierung und Vernetzung kommunizieren Menschen, Maschinen, Anlagen, Sensoren und Produkte in der intelligenten Fabrik automatisch miteinander und sorgen für eine flexiblere, effizientere und autonomere Produktion. Die verschiedenen Komponenten werden in Netzwerken zusammengeführt, sodass sie hochgradig komplexe Infrastrukturen selbständig steuern, regeln und kontrollieren können.

Grundlage der Smart Factory ist der Echtzeit-Informationsaustausch zwischen Produkt und Fertigungsanlage: Das Produkt bringt seine Fertigungsdaten selbst in maschinell lesbarer Form mit, beispielsweise auf einem RFID-Chip. Anhand dieser Daten werden der Weg des Produkts durch die Fertigungsanlage und die einzelnen Fertigungsschritte gesteuert und bis zur Auslieferung zum Kunden verfolgt.

Die Produkte der Smart Factory wissen somit jederzeit, wo sie sind, kennen ihre Historie, ihren aktuellen Zustand und die Produktionsschritte, die ihnen zum fertigen Produkt noch fehlen. Das

ermöglicht neue Geschäftsmodelle wie beispielsweise die Individualisierung von Produkten bis hin zur rentablen Fertigung von Einzelstücken, oder aber die Abkehr vom klassischen Verkauf von Produkten hin zur Fokussierung auf Dienstleistungen und Services.

Auch wenn die Smart Factory vielerorts noch Zukunftsmusik ist, ist es absolut zentral, sich jetzt bereits umfangreiche Gedanken über die Implikationen dieses technologischen Wandels zu machen. Denn die ersten Schritte in Richtung digital vernetzte Produktion haben Industrieunternehmen bereits unternommen.

Digitale Durchdringung birgt Risiken

Das Potenzial von Smart Factories haben mittlerweile die meisten Industriebetriebe erkannt. Zahlreiche Unternehmen treiben Automatisierung und Kommunikation in ihren Fertigungshallen bereits intensiv voran. Digitale Anwendungen, die Brücken schlagen zwischen der physischen und der virtuellen Welt, sogenannte Cyber Physical Systems (CPS), gehören inzwischen vielerorts bereits zum Inventar. Das können beispielweise Lagerfahrzeuge sein, die ihre Ziele aufgrund von Produkt- und Logistikdaten ansteuern.

Das hat Konsequenzen: Das Internet der Dinge im industriellen Kontext (IIoT) führt zu einer verstärkten digitalen Durchdringung aller Systeme. Unmengen von Daten und Informationen werden produziert und müssen identifiziert, bewertet, gespeichert, übertragen und letztlich auch verarbeitet werden. Dabei verknüpft das IIoT Organisationsdaten – zum Beispiel Produktdefinitionen, Stücklisten und technische Spezifikationen – mit technischen Daten aus computergestützten Fertigungssystemen.

Drastische Folgen von Sicherheitslücken

Die Datenmengen können Optimierungspotenzial offenlegen, aber auch zum Risikofaktor werden. Denn durch die steigende Vernetzung der Operational Technology (OT) und die Integration der OT in das Internet der Dinge (IoT) unterliegt die einst abgeschottete Produktion plötzlich denselben Cyber-Gefahren wie klassische Datennetze, Rechenzentren oder die Office-IT. Allerdings sind in der Produktion die Folgen von Sicherheitsvorfällen deutlich drastischer. Bestehen Sicherheitslücken, ist die gesamte produktive Verfügbarkeit gefährdet; die wirtschaftlichen Schäden, die entstehen können, sind enorm.

Ein Beispiel eines Features, welches zur Systemschwachstelle wird, ist das Notfallsystem in der Automobilindustrie. Damit nach einem Unfall ein Notruf abgesetzt werden kann, wird eine Schnittstelle zwischen Motorsteuergerät und dem GPS-Datennetz verbaut. Genau diese Schnittstelle erlaubte es Hackern schlussendlich, den Wagen unbefugt zu steuern oder zu bremsen.

Die IT hat diese Problematik vielerorts erkannt und Massnahmen getroffen, um die Konnektivität und die Integration von Fertigungsmaschinen zu schützen. Nur die Kommunikationsnetze hochverfügbar, echtzeitfähig und ausfallsicher zu designen, reicht allerdings nicht aus. Es braucht mehr: Die Fertigungsmaschinen selbst müssen von Anfang an eine solide Sicherheitsarchitektur aufweisen, sodass sie nicht zu einem Einfallstor für Cyber-Kriminelle und einem Risiko für die gesamte Infrastruktur werden.

Was Industrieunternehmen und Hersteller tun müssen

Das bringt Herausforderungen mit sich – für Anwender ebenso wie für Hersteller vernetzter Maschinen. Industrieunternehmen müssen bereits bei der Beschaffung neuer, vernetzter Fertigungsmaschinen zwingend sicherstellen, dass sie ausschliesslich Hersteller berücksichtigen,

welche die relevanten Sicherheitsdesigns pflichtbewusst umsetzen: Datentrennung, Datensicherheit, Datentransfer-Schnittstellen in Hardware und Software. Nur so kann gewährleistet werden, dass die neu zu integrierenden Anlagen zu keinem Einfallstor in die eigene IT-Infrastruktur werden.

Hersteller wiederum müssen sich bewusst sein, dass vernetzte Fertigungsmaschinen während ihres gesamten Lebenszyklus mit drei zentralen Herausforderungen konfrontiert sind. Sie müssen:

1. mit den kontinuierlichen Veränderungen der Sicherheit in Unternehmensnetzwerken Schritt halten;
2. sich innerhalb eines operativen und regulatorisch geprägten Prozessumfeldes behaupten;
3. sich gegen die sich dauernd weiterentwickelnden Cyber-Bedrohungen schützen lassen.

Dies heisst ebenfalls, dass die Systeme bewusst und bereits bei der Entwicklung updatefähig entwickelt werden und auf der anderen Seite, dass eine Härtung des Systems schon in der Entwicklung erfolgt und nicht benötigte Interfaces und Schnittstellen deaktiviert sind. Um als Hersteller nachhaltigen Mehrwert zu schaffen, darf die Sicherheit folglich nicht nur auf einzelne Geräte beschränkt werden. Es reicht auch nicht aus, nur die Vernetzung einzelner Produktlösungen im Auge zu behalten. Denn durch das Zusammenspiel aller Komponenten entsteht ein IoT-Ökosystem, in welchem die Sicherheit ein integraler Bestandteil sein muss. Die IIoT Security muss also systemübergreifend konzipiert und wirksam werden.

Sicherheitsüberlegungen bereits bei der Produktentwicklung

Sicherheitsanforderungen und die Implementierung müssen bereits bei der Produktentwicklung berücksichtigt werden. Nur wenn alle drei Sicherheitsaspekte Konnektivität, Produkt und Integration aufeinander abgestimmt sind, ist eine optimale Cyber Security für alle am IoT-Ökosystem beteiligten Parteien gewährleistet. So können Anwender einerseits sicher produzieren und Hersteller andererseits einen erfolgreichen, sicheren Betrieb gewährleisten, Kosten minimieren und fatale Reputations- und Kundenverluste verhindern.

Um vernetzte Produkte und Systeme vor den Gefahren aus dem Cyberspace zu schützen, bringt CyOne Security jahrzehntelange Erfahrung und tiefes Expertenwissen in Cyber Security in die Sicherheitskonzepte und -lösungen ein. Das gilt sowohl für Hersteller von vernetzten Fertigungsanlagen als auch für deren Anwender: CyOne Security unterstützt Hersteller und Industriebetriebe bei der Umsetzung ihrer Schutzziele und setzt dabei auf die 360°-Sicherheitskompetenz von Product Security, System Security und Operational Security.

Beginnen Sie heute, Ihre Smart Factory vor Cyber-Risiken zu schützen.

Machen Sie den ersten Schritt: Analysieren Sie gemeinsam mit unseren Experten Ihre aktuellen und zukünftigen Cyber-Sicherheitsbedürfnisse, damit wir mit Ihnen über zielgerichtete Sicherheitslösungen diskutieren können.

Kontaktieren Sie uns für ein kostenloses Expertengespräch.