CyOne Security AG
Hinterbergstrasse 18
6312 Steinhausen

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

WISSENS-UPDATE

Industrie 4.0 – Revolution stellt Sicherheit auf den Prüfstand

Mit der Industrie 4.0 sollen aus Daten künftig schneller Produkte werden. Dies gelingt, wenn Menschen, Maschinen, Anlagen und Produkte automatisch Informationen austauschen und so eine Produktionsstrasse bilden, die sich selbst organisiert: die Smart Factory. Damit der Brückenschlag zwischen physischer und virtueller Welt nicht zum Sicherheitsrisiko wird, ist der sichere und vertrauensvolle Umgang mit Daten sowie der Schutz der Kommunikationsnetzwerke und IoT-Ökosysteme gegen Cyber-Angriffe unverzichtbar.

Nach den drei industriellen Revolutionen durch die Mechanisierung, die Massenfertigung sowie die Automatisierung wird die zunehmende digitale Vernetzung die Industrie ein viertes Mal grundlegend verändern. Drei Beispiele:

- Maschinen bestellen Werkstoffe automatisch in time und nach voraussichtlichem Bedarf.
- Kundenspezifische Produkte bis hin zu Losgrössen 1 Stück werden auf einem einzigen Fliessband hergestellt – die Anweisungen für die Fertigung erhalten die Maschinen direkt vom Onlineshop oder aus dem Kundenportal.
- Unternehmen bieten freie Fertigungskapazitäten über digitale Plattformen an und steigern so die Auslastung des eigenen Maschinenparks.

Die Möglichkeiten, die sich aus der Digitalisierung und Vernetzung in der Industrie ergeben, sind verheissungsvoll. Durch sie wird die Industrie flexibler und effizienter produzieren können, die Individualisierung der Produktion bis hin zur Fertigung von Einzelstücken wird kostengünstiger und damit rentabler, neue Geschäftsmodelle und neue Möglichkeiten für das Kundenerlebnis entwickeln sich.

Zwei Welten, eine Sicherheit

Im Zentrum der Industrie 4.0 steht die Smart Factory. Die intelligente (smarte) Fabrik ist eine Produktionsanlage, die sich zu Teilen selbst organisiert. Menschen, Maschinen, Anlagen und Produkte kommunizieren automatisch miteinander, um eine autonome Produktion zu ermöglichen. Die vernetzte Smart Factory entwickelt sich zu einem technologischen Ökoystem, das dem Hersteller die Möglichkeit gibt, Daten zu nutzen, Prozesse zu optimieren und smarte Produkte und Services zu liefern.

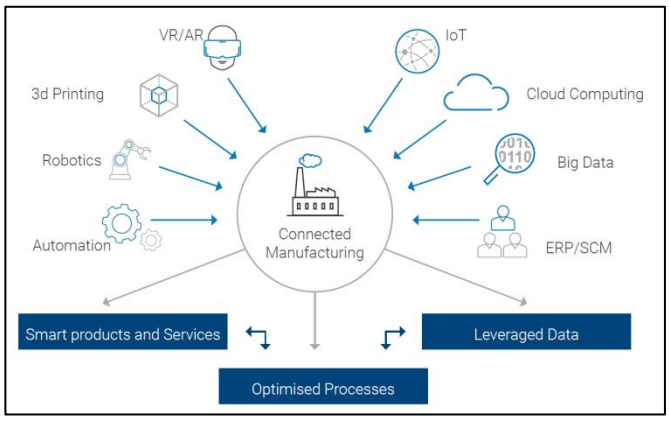

Abbildung 1: technologisches Ökosystem in der vernetzten Smart Factory

Grundlage der Smart Factory ist die Integration der Daten entlang der Kommunikation vom Auftraggeber bis hin zur Logistik und Spedition. Eine Möglichkeit ist, dass das Produkt seine Fertigungsinformationen in maschinell lesbarer Form selbst mitbringt. So kann ein RFID-Chip auf dem Produkt angebracht werden. Anhand dieser Daten wird der Weg des Produkts durch die Fertigungsanlage und die einzelnen Fertigungsschritte gesteuert. 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. Qualitätsprozesse können mit den Daten hinterlegt werden und der Kunde sieht den Status und die voraussichtliche Lieferung in Echtzeit.

Smart sind in Zukunft neben den Fabriken auch die Dienstleistungen (Smart Services) sowie die Produkte (Smart Products). Als Smart Services gelten Angebote, die virtuelle und physische Dienstleistungen kombinieren. Ein Beispiel hierfür ist die Fernüberwachung einer Anlage für einen automatischen Nachtschichtbetrieb eines Konfigurationsservices für eine komplexe Fertigungsinsel, welcher direkt vom Hersteller angeboten wird. Für den Hersteller bedeutet dies Kundennähe, Expertise und letztendlich auch die Möglichkeit, sein Serviceportfolio zu erweitern. Bei den Produkten sind es hauptsächlich zwei Eigenschaften, die sie smart machen: Das Produkt verfügt über Informationen aus dem eigenen Herstellungsprozess und wurde so besser an individuelle Kundenwünsche angepasst, und das Produkt verfügt über die Fähigkeit, während der Nutzungsphase Daten zu sammeln und mit einem Netzwerk zu kommunizieren.

Vernetzung ermöglicht neue Netzwerke

Die intelligente Vernetzung geht in Zukunft weit über eine Smart Factory hinaus. Sind erst einmal alle relevanten Unternehmensbereiche einer Firma – von der Produktion und Planung über die Logistik bis hin zum Lieferantenmanagement – intern und unternehmensübergreifend vernetzt, können flexible Wertschöpfungsnetzwerke gebildet werden. Dies ermöglicht zum Beispiel, dass ein Unternehmen sein Fertigungsspektrum temporär und auftragsgerecht erweitern kann, indem die Fertigungsanlage eines Netzwerkpartners beansprucht wird.

Eingeschränkt verwendbar © CyOne Security AG. Alle Rechte vorbehalten

Solch flexible Wertschöpfungsnetzwerke, welche die Produktionskapazitäten bei Bedarf bereitstellen, zu realisieren, wird noch Jahre dauern. Die Grundlagen dafür bestehen aber bereits heute oder sind im Aufbau begriffen. So treiben viele Betriebe die automatisierte Kommunikation in ihren Fertigungshallen intensiv voran. Digitale Anwendungen, MIS (Management Information Systeme), welche Brücken schlagen zwischen der physischen und virtuellen Welt, gehören inzwischen vielerorts bereits zum Inventar und werden ausgebaut. Von der reinen Information geht es in Richtung automatisierter Auftragssteuerung. Das Internet der Dinge im industriellen Kontext ist auf dem Vormarsch und mit der Vernetzung steigen auch die Cyber-Risiken, die mit den vielfältigen digitalen Schnittstellen einhergehen.

Intelligent ist, was sicher ist – die sechs Schlüsselfaktoren

Unverzichtbare Grundvoraussetzung, um Industrie 4.0 erfolgreich umzusetzen, ist der sichere und vertrauensvolle Umgang mit Daten sowie der verlässliche Schutz der unternehmensübergreifenden Kommunikation gegen Angriffe. Die Sicherheit muss deshalb von Beginn an in jeden Produktentwicklungsprozess mit einfliessen («Security by Design»). Unternehmen, die ihre Maschinen, Mitarbeitenden und Anwendungen intelligent vernetzen wollen, ohne dabei die IT-Sicherheit zu gefährden, sollten folgende sechs Punkte beachten:

1. **Netzwerksegmentierung mittels Gateways**
   IoT-Gateways mit kombinierten Sicherheitsfunktionen schützen Maschinen und Anlagen, die mit dem Internet verbunden sind, vor Cyber-Attacken. Sie ermöglichen die Integration der Daten in die übergeordneten Leitsysteme und sichern gleichzeitig die Maschinen und Anlagen sowie die Kommunikation ab. Mit Hilfe der Gateways lassen sich Netzwerkbereiche mit unterschiedlichen Schutzstufen voneinander trennen (Netzwerksegmentierung) und in Zonen einteilen. So werden z.B. Maschinendaten (z.B. Safety) kontrolliert nur in der Anlagensteuerung gehalten, wobei die Produktionsdaten zwecks Logistikinformation und Qualitätsdaten und über kontrollierte Gateways an einen Rechner im ERP-System gesendet werden. Mittels VPN können räumlich getrennte Netze über Maschinenstandorte hinaus zusammengefasst werden. Die VPN-Verschlüsselung schützt die Daten während der Übertragung vor Manipulation und Diebstahl.

2. **Absicherung und Remote-Zugriff**
   Die Maschinen und Anlagen sind mit einer zentralen IoT-Plattform verbunden, worüber sich die gesamte Infrastruktur verwalten und überwachen lässt. Remote-Zugriff zwecks Wartung oder Updates vom Hersteller stellen die Verfügbarkeit der Anlagen sicher. Wichtig dabei ist, dass die Anlage bei Zugriff über das Internet oder über Funktechnologien eine starke Authentisierung durchführt sowie sämtliche Interaktionen einer Sitzung protokolliert und dass der Fernzugriff nicht zum Einfallstor für Cyber-Attacken auf die IT-Infrastruktur dienen kann.

3. **Nicht jeder darf alles machen**
   Akteure benötigen individuelle Benutzerkonten. Dies betrifft Menschen, Maschinen und Anlagen gleichermassen. Durch die Verknüpfung der Zugangsdaten mit den Benutzerkonten wird die Authentisierung und Autorisierung sowie die Nachvollziehbarkeit sichergestellt. Jeder Anwender erhält nur auf die für seinen Arbeitsbereich relevanten Daten und Anwendungen Zugriff. Zwecks Qualitätssicherung werden Änderungen am Prozess und an den Parametern nachvollziehbar protokolliert.

Eingeschränkt verwendbar © CyOne Security AG. Alle Rechte vorbehalten

4. **Zentrale Verwaltung aller Anwendungen und Datenströme**
   Ein zentrales Management-Tool sollte eine umfassende Übersicht über sämtliche Anwendungen und Datenverbindungen aufzeigen. Auf einen Blick lässt sich so erkennen, auf welche Netzwerk-Komponenten zugegriffen wird und woher Zugriffe erfolgen. Ideal, wenn dabei sämtliche Zugriffe erfasst und gespeichert werden – als Grundlage, um eine spätere Auswertung, Analysen und Optimierung zu ermöglichen.

5. **Infrastruktur überwachen, Daten analysieren**
   Zentral verwaltet lassen sich die Daten visualisieren und analysieren. So kann etwa die Overall Equipment Effectiveness berechnet und können Optimierungspotenziale aufgedeckt werden. Beim Monitoring steht neben der Datensammlung insbesondere auch die Absicherung der verschiedenen Komponenten gegen Cyber-Attacken im Fokus. Zu sicherheitsrelevanten Ereignissen zählen etwa inkorrekte Passworteingaben, unbekannte Datenströme (Kopien) Ressourcenüberlastung, freigeschaltete Remote-Zugänge, unbefugte Zugriffe oder Änderungen in sicherheitsrelevanten Konfigurationsdateien.

6. **Fernwartung und Predictive Maintenance**
   Die Datenanalyse ermöglicht die frühzeitige Erkennung von Fehlerpotenzial, so dass bereits vor einem «Schadenfall» via Fernzugriff Massnahmen eingeleitet werden können. Dies heisst auch, Hersteller, Zulieferer und Partner effizient und einfach einbinden zu können, um das Potenzial zu nutzen. Geeignete Sicherheitskonzepte z.B. über einen Jumphost stellen sicher, dass Partner von definierten Rechnern aus nur auf die entsprechenden Anlagenteile zugreifen oder dass Zugriffe und Sitzungen zwecks Nachvollziehbarkeit aufgezeichnet werden.

Aufgrund der extrem hohen Zahl und Dichte digitaler Schnittstellen ist die Vorstellung, die Anlage komplett absichern zu können, unrealistisch. Deshalb sind Funktionen zur Erkennung von Angriffen und anderen sicherheitsrelevanten Ereignissen ebenso zentral wie auch ein Wiederherstellungsplan, der im Fall eines Angriffs die Anlage in einen Zustand der Vertrauenswürdigkeit, den Normalzustand, zurückversetzt. Kommt hinzu: die Unternehmensnetzwerke befinden sich in laufender Veränderung. Kontinuierlich werden Anpassungen vorgenommen.

Für Hersteller von IIoT- und OT-Devices gilt es, diesem Umstand bereits bei der Entwicklung Rechnung zu tragen, indem der Faktor Security im Entwicklungsprozess von Beginn an eine zentrale Rolle einnimmt.

Erfolgsfaktor Sicherheit

Die Informations- und Datensicherheit ist ein substanzieller Bestandteil bei der Entwicklung von Systemkomponenten für die Industrie 4.0. Unsere Experten unterstützen Sie umfassend:

Dienstleistungen für Betreiber

- Sicherheitsreview existierender IIoT-Architekturen und Aufzeigen allfällig vorhandener Lücken
- Design einer geeigneten Sicherheitsarchitektur bei Digitalisierungsvorhaben für die sichere Vernetzung von Anlageteilen
- Durchführen einer Schwachstellenanalyse der neu vernetzten Industrieanlage mit Fokus auf die IT-Infrastruktur / ERP-System (Innensicht)
- Durchführen einer Schwachstellenanalyse aus dem Internet mit Blick auf das gesamte IIoT-Ökosystem (Aussensicht)

Eingeschränkt verwendbar © CyOne Security AG. Alle Rechte vorbehalten

- Durchführen eines Sicherheitsscans und Dokumentieren der gefundenen Sicherheitslücken für existierende Anlageteile oder für einzelne integrierte Gerätekomponenten
- Design und Implementation von sicheren Fernzugriffskonzepten und den dazugehörigen Berechtigungsmodellen

Dienstleistungen für Hersteller

- Überprüfung und Analyse von Sicherheitsarchitekturen
- Design der optimalen Sicherheitsarchitektur und Update-Fähigkeiten
- Design und Implementation kryptologischer Funktionen
- Datenseparation von klassifizierten Daten und Geräte-relevanten Systemdaten
- Design der richtigen IT-Sicherheitsarchitektur für die optimale Integration vernetzter OT-Devices
- Betreiben einer sicheren Update-Plattform

Die Lebensdauer industrieller Anlagen oder einzelner Systeme ist in der Regel hoch. Dies führt dazu, dass ihr Aus- oder Umbau zu einem Mix von Komponenten verschiedener Generationen führt. Insofern wird von IoT- und OT-Devices verlangt, dass sie ein hohes Mass an Flexibilität aufweisen, was ihre Integration ins Netz betrifft. Diese Flexibilität darf hingegen keinesfalls bedeuten, dass bei der Sicherheit Abstriche gemacht werden. Denn Verfügbarkeit, Verhinderung von Zweckentfremdung und Wahrung der Datensicherheit sind essentiell für eine erfolgreiche Transformation hin zur Industrie 4.0.

CyOne Security: kompetenter Partner für die Umsetzung von OT-Schutzzielen

Informations- und Datensicherheit muss ein substanzieller Bestandteil in der Entwicklung und der Implementierung von OT sein. Da in OT-Systemen nicht nur Security (Sicherheit), sondern auch Safety (Schutz) eine entscheidende Rolle spielt, sollte zwingend sichergestellt werden, dass selbst bei einem Cyber-Vorfall keine Gefahr für Menschen und Umgebung besteht.

Die CyOne Security bringt tiefes Expertenwissen in Cipher- und Cyber Security in die Sicherheitskonzepte und -lösungen vernetzter Produktionsanlagen und IIoT ein. Mit dem Dreigespann Product Security, System Security und Operational Security bieten wir 360°-Sicherheitskompetenz.

Beginnen Sie heute und schützen Sie Ihre vernetzte Smart Factory vor Cyber-Risiken für eine sichere Industrie 4.0.

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

Kontaktieren Sie uns für ein kostenloses Expertengespräch.

Eingeschränkt verwendbar © CyOne Security AG. Alle Rechte vorbehalten