PLATTFORM INDUSTRIE 4.0

WEGWEISER

IT-Security in der Industrie 4.0

Erste Schritte zu einer sicheren Produktion

Industrie 4.0 – Welche Leitgedanken stehen hinter diesem Schlagwort? Zum einen werden in der Industrie 4.0 Produktionsabläufe zunehmend digital vernetzt, zum anderen unternehmensübergreifende Kooperations- und Wertschöpfungsnetzwerke gebildet. Eine (voll) automatisierte Kommunikation über unterschiedlichste Schnittstellen hinweg ermöglicht es, schneller und dynamischer zu handeln, effizienter zu fertigen und konventionelle Geschäftsfelder durch neue, plattformgestützte Geschäftsmodelle zu erweitern.

Unverzichtbare Grundvoraussetzung, Industrie 4.0 erfolgreich umzusetzen, ist der **sichere** und **vertrauensvolle Umgang mit Daten** sowie der verlässliche Schutz der unternehmensübergreifenden Kommunikation vor Angriffen von außen. Übergreifende Wertschöpfungsnetzwerke werden erst dann etabliert und gewinnbringend genutzt, wenn die notwendigen Datenströme eindeutigen und sicheren Identitäten zugeordnet sind.

Sicher in die digitale und vernetzte Produktion einsteigen

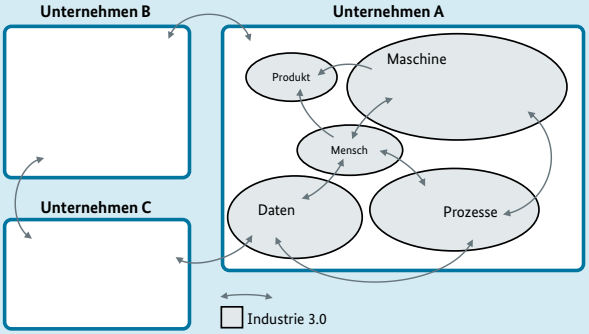
Auf ihrem Weg in die Wertschöpfungsnetzwerke der Zukunft bietet die Arbeitsgruppe 3 der Plattform Industrie 4.0 „Sicherheit vernetzter Systeme“ insbesondere kleinen und mittleren Unternehmen (KMU) eine Orientierungshilfe, um sicher in die digitale und vernetzte Produktion einzusteigen.

Nicht jedes KMU wird in Zukunft eigene Wertschöpfungsnetzwerke etablieren oder gar initiieren müssen. Damit Geschäftsanteile zukünftig nicht verloren gehen, sollten mittelständische Unternehmen aber in der Lage sein, in zukünftigen Kooperationsnetzwerken ihrer Partner oder Kunden mitzuwirken und eigenständig zu agieren. Eine der wesentlichen Herausforderungen dabei wird sein, **digitale Kompetenzen** aufzubauen, um auch in der Industrie 4.0 die eigene **digitale Souveränität** und **Handlungsfreiheit** sowie den **Schutz der Unternehmenswerte** zu wahren.

Ein Zukunftsszenario: Auftragsgesteuerte Produktion in dynamischen Wertschöpfungsnetzwerken

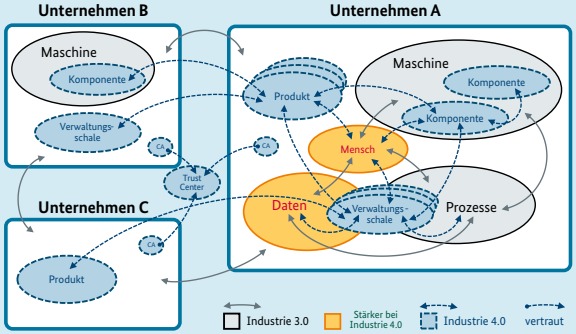
Durch den verstärkten Einsatz von Informations- und Kommunikationstechnologien werden in den kommenden Jahren **flexible Wertschöpfungsnetzwerke** in der Industrie 4.0 zunehmend klassische Produktionsketten mit ihren überwiegend hierarchischen Strukturen ablösen: Unternehmen bieten freie Fertigungskapazitäten über eine digitale Plattform an und steigern die Auslastung des eigenen Maschinenparks.

Informationsflüsse in klassischen Geschäftsmodellen der Industrie 3.0



Vernetzung innerhalb eines Unternehmens ist schon gegeben.

Informationsflüsse in digital vernetzten Wertschöpfungsnetzwerken der zukünftigen Industrie 4.0



Die automatisierte Kommunikation zwischen den Unternehmen wird zugunsten einer höheren Agilität durch direkte Kommunikation zwischen den Entitäten (u. a. Menschen, Maschinen und Produkte) der beteiligten Unternehmen erweitert.

Andere Unternehmen greifen auf das Angebot zu und erweitern temporär und auftragsgerecht ihr eigenes Fertigungsspektrum.

Gerade für kleine und mittelständische Unternehmen bieten solche Netzwerke verteilter Produktionen die Möglichkeit, spezifische Produkte und Dienstleistungen in nahezu beliebiger Menge und hoher Qualität am Markt konkurrenzfähig anzubieten. Dieses Konzept basiert darauf, dass **alle relevanten Unternehmensbereiche** – von der Produktion und Planung über die Logistik bis hin zum Lieferantenmanagement – intern und unternehmensübergreifend **digital vernetzt** sind.

Das Zukunftsszenario einer solchen „Auftragsgesteuerten Produktion" geht deutlich darüber hinaus, einen Auftrag durch die eigene Produktion zu steuern. Vielmehr bilden sich in der Industrie 4.0 Kooperationsnetzwerke zwischen Unternehmen. Die Initiierung dieser Zusammenarbeit wird voll automatisiert erfolgen, ebenso wie die dazu notwendige vertikale und horizontale Vernetzung der Produktionssysteme der Netzwerkpartner.

Technische Grundvoraussetzung, um solche Netzwerke zu realisieren, ist der **Schutz der Kommunikationskette vor Dritten**. Wertschöpfungsnetzwerke werden dann erfolgreich etabliert und handlungsfähig, wenn sie auf validierten, verifizierbaren und damit **sicheren Identitäten** basieren. Erst dadurch können Kommunikationspartner eindeutig und vertrauenswürdig identifiziert und übertragene Daten validiert werden.

Kooperationsnetzwerke der Zukunft: Herausforderungen für die IT-Sicherheit

Unternehmen können sich an den zukünftigen Wertschöpfungsnetzwerken beteiligen, wenn sie die **Basis-Anforderungen an eine sichere und vertrauensvolle Kommunikation** erfüllen: Aufträge, Produktions- und Prozessdaten müssen innerhalb des Netzwerkes sicher und ohne Zugriffe durch Unbefugte zwischen den beteiligten Unternehmen ausgetauscht werden können.

Grundlegend für eine unternehmensübergreifende Zusammenarbeit sind unternehmenseigene Prozesse, die **relevante Unternehmenswerte** und deren Schutzbedarfe erkennen. Welche Daten und Informationen sind für das eigene Unternehmen innerhalb komplexer Wertschöpfungsketten besonders schützenswert? Die Ausrichtung des eigenen Unternehmens, um in einer prosperierenden Industrie 4.0 mitzuwirken,

erfordert daher zunächst Offenheit – für neue Informationstechnologien, die es beispielsweise ermöglichen, Auftragsdaten mit dem Fertigungsinformationssystem (MES) des Unternehmens direkt auszutauschen.

Aus Sicht der IT-Sicherheit kommt der **Authentifizierung der Kommunikationspartner und -systeme** in der Industrie 4.0 besondere Bedeutung zu. Es gilt sicherzustellen, dass der Absender derjenige ist, der er vorgibt zu sein, und dass die Informationen den gewünschten Empfänger erreichen: Lassen sich die erhaltenen Informationen eindeutig dem ursprünglichen Urheber zuordnen, und das auch in den voll automatisierten Kommunikationskaskaden der Industrie 4.0? Ebenso sind die Autorisierung der Anfrage und die Integritätsprüfung der Auftragsdaten relevante Aufgaben, auf deren Basis eine kapazitive Bewertung der Produktionsressourcen erfolgt und in Abhängigkeit des Ergebnisses eine automatisierte Bestellung für Vorprodukte sowie Roh- und Hilfsstoffe ausgelöst wird.

Viele und inhaltlich variierende Anfragen sind zu erwarten. Daher wird es auch in der Produktion notwendig sein, insbesondere **Standards in IT-Verfahren** für Identifikation, Authentifizierung und Autorisierung zu nutzen. Der Austausch von (Produktions-)Daten in immer größeren Mengen erfordert die Nutzung beziehungsweise Bereitstellung von Cloud-basierten Diensten und Daten-Plattformen. Das ist dann möglich, wenn standardisierte und sichere Methoden existieren, die die Schutzziele der Verfügbarkeit, Integrität und Vertraulichkeit durchgängig sicherstellen.

Die Vielzahl der beteiligten Akteure, Maschinen und Werkstücke erfordert zudem, dass **Benutzerkonten und Berechtigungen** verwaltet werden – weit über die Grenzen der eigenen Organisation hinaus. Einfache, sichere und standardisierte Verfahren, um sogenannte Identity Provider in das eigene Usermanagement zu integrieren, sind daher unerlässlich. Denn sie bilden diese Aufgabe auch in komplexen Strukturen und Hierarchien zuverlässig ab.

Analyse: Wo steht mein eigenes Unternehmen aus Sicht der IT-Security?

Um das eigene Unternehmen und zugehörige Produkte auf den Einsatz von Industrie 4.0 vorzubereiten, ist es für den Mittelstand zwingend erforderlich, bereits heute eine mögliche Einbindung und jeweilige Position des eigenen Unternehmens innerhalb der Industrie 4.0-Wertschöpfungsnetzwerke zu bestimmen. Daraus sollten dann der Schutzbedarf der Unternehmenswerte sowie notwendige Sicherungsmaßnahmen abgeleitet werden.

Dabei liegt der Fokus auf den einzuhaltenden **„VIV"-Schutzzielen** des Datenaustauschs: **V**erfügbarkeit, **I**ntegrität und **V**ertraulichkeit. Darüber hinaus gewinnt auch die Authentizität (Identifikation und Autorisierung eines Kommunikationspartners) in der Industrie 4.0 zunehmend an Bedeutung.

Bei folgender Auswahl an Sicherheitsmaßnahmen haben erfolgskritische Prozesse hohe Priorität. Dazu gehört der Schutz vor Sabotage und von Geschäftsgeheimnissen, wie beispielsweise des Fertigungs-Know-hows.

Um den **Einstieg in die eigene Risikoanalys**e zu erleichtern, empfiehlt die Arbeitsgruppe „Sicherheit vernetzter Systeme", folgende, zentrale Fragestellungen zu beantworten:

- Welche Fertigungskompetenzen und -kapazitäten können angeboten bzw. sollten eingebunden werden?
- Welche Daten müssen innerhalb einer unternehmensübergreifenden Prozesskette wann, wem, wie bereitgestellt werden bzw. werden wann, von wem, wie benötigt?
- Wie kritisch sind diese Daten in Bezug auf deren Vertraulichkeit und Integrität für das eigene Unternehmen?
- Wie kann insbesondere ein datenschutzkonformer Umgang mit Kundendaten gewährleistet werden?

- Welche Kooperationspartner zur Ressourcen-Teilung stehen in verteilten Produktions- und Wertschöpfungsnetzwerken bereit und in welchem Maß müssen vertrauenswürdige Daten mit diesen Partnern ausgetauscht werden?

- Welche Verträge müssen ggf. mit den Kooperationspartnern zum Beispiel hinsichtlich der Zurechnung und Haftung durch Leistungsstörungen oder der Eigentumsrechte an den bereitgestellten bzw. verarbeiteten Daten geschlossen werden?

- Welche Maschinen, Komponenten und Produkte sollen in einer Industrie 4.0 aus der eigenen Produktion nach außen kommunizieren und benötigen eine Identität mit entsprechenden Eigenschaften?

- Wie kann in der Produktion eine gesicherte Kommunikation nach außen realisiert werden, um die Integrität und Vertraulichkeit der übermittelten Informationen sicherzustellen?

- Welche Mitarbeiter sind für IT-Sicherheit in der Produktion und der Verwaltung im eigenen Unternehmen zuständig?

Jetzt handeln: Was kann im eigenen Unternehmen heute getan werden, um sicher in die Industrie 4.0 einzusteigen?

Welche Schritte eingeleitet werden sollten, um das eigene Unternehmen und insbesondere die eigene Produktion aus Sicht von IT-Security weiterzuentwickeln, hängt zunächst von der individuellen Situation des jeweiligen Unternehmens ab. Die obigen Fragen helfen bei einer ersten Selbsteinschätzung.

Die erfolgreiche Teilnahme an vernetzten Wertschöpfungsnetzwerken der Industrie 4.0 erfordert IT-Security. In vielen Fällen lassen sich die Grundvoraussetzungen durch einfach umzusetzende Maßnahmen schaffen.

Für den Einstieg in die Schaffung der Voraussetzungen für Industrie 4.0 sind aus Sicht der Arbeitsgruppe häufig folgende Themen zu priorisieren:

1. Security-Verantwortlichen im Sinne eines Informationssicherheitsmanagementsystems (ISMS) benennen und qualifizieren.

2. Sensibilisierungsmaßnahmen für IT-Sicherheitsrisiken für die Mitarbeiter in der Produktion aufsetzen und durchführen.

3. Sicherheitskonzepte für Netzwerkzugänge (Fernwartung, WLAN, Cloud etc.) erarbeiten und umsetzen.

4. Regelungen zum Umgang mit Wechseldatenträgern (USB-Sticks etc.) und externer Hardware (Programmiergeräte und Diagnosesysteme etc.) treffen.

5. Bewusstsein für Risiken bei der Verwendung von Smartphones und Tablet-Systemen in der Produktion schaffen.

6. Sicherheitsvorkehrungen gegenüber Schadsoftware in der Produktion bei der Beschaffung neuer Maschinen und Anlagen fordern.

7. Aktuelle Betriebssysteme und Software in den Produktionsanlagen und Sicherheitsupdates von den Herstellern fordern.

FAZIT: Die Industrie 4.0 ist geprägt durch die vertrauensvolle Zusammenarbeit mit vielen Partnern. Damit Industrie 4.0 gelingt und ihr Potenzial für den deutschen Mittelstand gehoben werden kann, ist es heute notwendig, das eigene Unternehmen auf einen Stand zu bringen, von dem aus die zukünftigen Sicherheitsanforderungen erfüllt werden können.

Diese Publikation ist ein Ergebnis der AG Sicherheit vernetzter Systeme (Plattform Industrie 4.0).

Weiterführende Informationen sind unter anderem in folgenden Veröffentlichungen verfügbar:

- Auf dem Weg zur smarten Fabrik – Positionspapier Industrie 4.0, ZVEI – Zentralverband Elektrotechnik- und Elektronikindustrie e.V.
- Ausblick Security Industrie 4.0, ZVEI – Zentralverband Elektrotechnik- und Elektronikindustrie e.V.
- Fragenkatalog Industrial Security – Einfach anfangen, Verband Deutscher Maschinen- und Anlagenbau (VDMA)
- ICS Security Kompendium, Bundesamt für Sicherheit in der Informationstechnik (BSI)
- Light and Right Security ICS (LARS ICS), Bundesamt für Sicherheit in der Informationstechnik (BSI)
- VdS-Richtlinien 3473 – Cyber-Security für KMU, VdS Schadenverhütung GmbH
- Security in Automation – INS-Studie, DIN/NAM/VDMA
- Status Quo der Security in Produktion und Automation – Studie, Verband Deutscher Maschinen- und Anlagenbau (VDMA)

AUTOREN DER AG SICHERHEIT VERNETZTER SYSTEME:

Dr. Lutz Jänicke, PHOENIX CONTACT Cyber Security AG | Michael Jochem, Bosch Rexroth AG | Dr. Wolfgang Klasen, Siemens AG | Dr. Bernd Kosch, Fujitsu Technology Solutions GmbH | Michael Krammel, Koramis GmbH | Lukas Linke, ZVEI | Jens Mehrfeld, Bundesamt für Sicherheit in der Informationstechnik (BSI) | Michael Sandner, Volkswagen AG | Andreas Teuscher, Sick AG | Thomas Walloschke, Fujitsu Technology Solutions GmbH | Steffen Zimmermann, VDMA

Impressum

Herausgeber
Bundesministerium für Wirtschaft und Energie (BMWi)
Öffentlichkeitsarbeit
11019 Berlin
www.bmwi.de

Redaktionelle Verantwortung
Plattform Industrie 4.0
Bertolt-Brecht-Platz 3
10117 Berlin

Gestaltung und Produktion
PRpetuum GmbH, München

Bildnachweis
Kzenon/Fotolia (Titel); welcomia/istock (S. 2); cookiecutter/Fotolia (S. 4)

Stand
März 2016

Druck
Silber Druck oHG, Niestetal