Digitalisierung in der Industrie: die Erfolgsfaktoren

Die besondere Wichtigkeit von IT-Sicherheit für die Industrie 4.0 und Wege diese zu gewährleisten

Von Liliana Preuß

Industrie 4.0, Internet of Things, Big Data und Cloud Computing sind nur einige Schlagworte einer weltweiten Entwicklung, die dieser Tage die Industrie revolutionieren. Moderne Informations- und Kommunikationstechniken vernetzen die industrielle Fertigung. Anlagen, Systeme und Komponenten tauschen eigenständig relevante Daten aus. Sogenannte „Smart Factories" wollen die Produktivität der gesamten Wertschöpfungskette erhöhen. Alltagsgegenstände werden zu „Smart Things". Haushaltsmaschinen, Sportequipment, Spielzeug oder medizintechnische Geräte werden mit Prozessoren, Sensoren und Netzwerktechnik ausgestattet. Und man verspricht sich Großes von diesen Entwicklungen: Die Digitalisierung soll die Arbeitsproduktivität der deutschen Industrie nach Jahren der Stagnation wieder deutlich steigern.

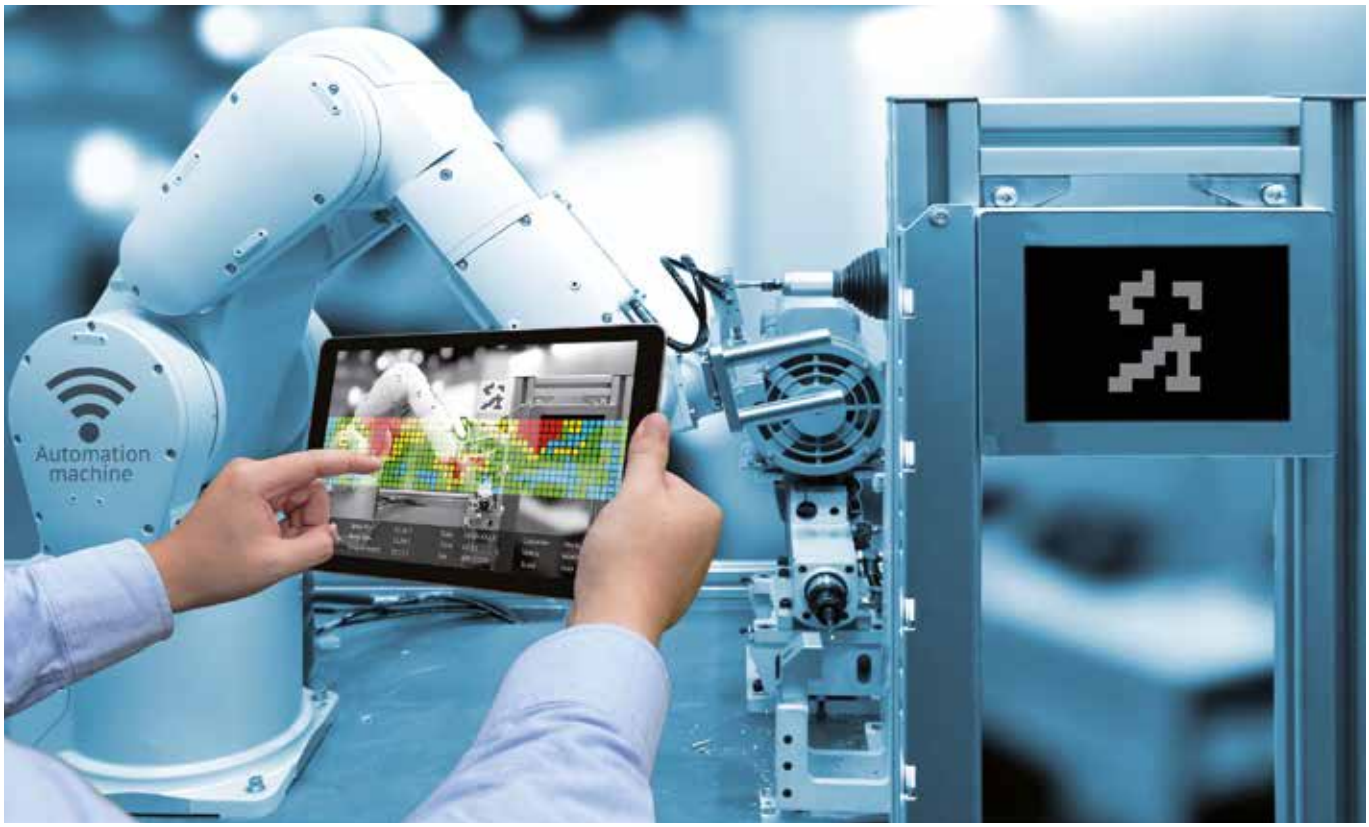
Bei aller Euphorie ist jedoch ein wesentlicher Teil der industriellen Digitalisierung bislang schwer vernachlässigt worden: Ihre Sicherheitsstandards sind stark ausbaufähig. So liegt die IT-Sicherheit noch innerhalb vieler Branchen im Ermessen der Betreiber von Industrieanlagen oder der Hersteller von „Smart Things", denen vielfach das Spezialwissen fehlt, um Sicherheitslücken zu identifizieren und somit Cyber-Angriffe zu vermeiden. Stete Verfügbarkeit und Integrität, Know-how-Schutz, Vertraulichkeit, Datenschutz und Authentizität sind unbedingte Schutzziele im Sinne der Industrie 4.0. Die wichtigsten Sicherheitsmechanismen sind entsprechend die Authentifizierung der Komponenten eines Systems, der Integritätsschutz der auszutauschenden Daten und die Berücksichtigung ihrer Vertraulichkeit. Dabei gilt es, insbesondere die Schnittstellen im Außen- und im Innenverhältnis sowie die Kommunikationssysteme einer Anlage zu schützen. Leider ist dieser Schutz aber nicht immer gewährleistet.

Fragile Sicherheitslage in der Sensorik

In der Sensorik beispielsweise ist IT-Sicherheit unerlässlich und doch nicht allzeit garantiert. Sensoren wandeln physische Zustände in Daten um und versenden sie zur Auswertung an Computer. Diese kleinsten vernetzten Bauteile kommen in Autos, Maschinenanlagen, Fitness-Armbändern, Mülleimern, Thermostaten, Kühlschränken, aber auch in Aufzügen zum Einsatz. TÜV NORD entwickelt derzeit eine spezielle Applikation für die Inspektion von Aufzügen: Vernetzte Sensoren sollen Messdaten aus den Aufzügen direkt via WLAN weitergeben, sodass der Prüfer seine Messergebnisse direkt vor Ort via Smartphone oder Tablet auswerten kann. Unbedingte Voraussetzung für solche Prozesse ist ein ausreichendes Maß an IT-Sicherheit, denn Sensoren stellen die Datenquellen und damit die Basis für jede weitere Informationsverarbeitung bei industriellen Systemen dar. Die Realität zeigt jedoch, dass die Sicherheit auf Ebene der Sensoren noch stark ausbaufähig ist. Je mehr Sensoren in der Industrie zum Einsatz kommen, desto mehr Fernwartungszugänge entstehen, die zwar Wartungsprozesse erleichtern, aber auch ein ernst zu nehmendes Sicherheitsrisiko darstellen können. Vielfach sind sie über öffentliche Zugänge wie GSM oder UMTS erreichbar – seltener sogar über ein lokales WLAN – und ermöglichen so von außen einen Zugriff auf Daten. Viele Unternehmen wissen gar nicht, dass und wo offene Zugänge zu ihren Produktionsanlagen frei liegen.

IT-Unsicherheit in Clouds

Aber nicht nur im Rahmen der Sensorik ist IT-Sicherheit unerlässlich. Eine zentrale Rolle in der Industrie 4.0 spielt auch das



Cloud Computing. In Clouds werden vielfach die gesamten Betriebsdaten eines industriellen Prozesses verarbeitet. Maschinen kommunizieren quasi direkt über die Cloud. Aufzüge senden beispielsweise in Echtzeit Informationen über erforderliche Reparaturen oder den Austausch von Komponenten und ermöglichen eine proaktive Systemwartung. Somit bekommen Servicetechniker eine Übersicht über den aktuellen Zustand des Aufzugs, Wartungsarbeiten werden planbarer und Ausfälle können vermieden werden. Aufgrund dieser besonderen Rolle der Cloud als Datenaustauschmedium ist besondere Sorgfalt bei der Auswahl eines Cloud Providers geboten. Unternehmen sollten sehr genau wissen, wie ihr Dienstleister mit Daten umgeht: Sind vertrauenswürdige Daten beispielsweise für jeden zugänglich? Laufen im Hintergrund der eigenen Daten Big-Data-Analysen? Welche Sicherheitsmaßnahmen führen Cloud Provider durch?

Datendiebstahl, Wirtschaftsspionage und Sabotage

Auch die Statistiken warnen vor den Gefahren mangelnder IT-Sicherheit: Laut Studien hat sich die Zahl der Schwachstellen innerhalb digitaler Steuerungssysteme in der Industrie (Industrial Control Systems-Komponenten) in den letzten fünf Jahren verzehnfacht. [1] Mit zunehmender Digitalisierung industrieller Prozesse steigt auch die Zahl der Störfälle im System. Insbesondere Social Engineering, also gezielte zwischenmenschliche Einflussnahme zum Zweck des Datenklaus und Identitätsdiebstahls via Phishing, wird eingesetzt, um Daten auszulesen und unautorisiert Zugriff zu erhalten. Aber auch das Einschleusen von Schadsoftware, der Einbruch über Fernwartungszugänge oder das Kompromittieren von Cloud-Komponenten sind ernst zu nehmende Gefahren für die IT-Sicherheit. [2] Eine Erhebung

des IT-Branchenverbands Bitkom ergab, dass in den vergangenen zwei Jahren gut die Hälfte der deutschen Unternehmen – in Industrieunternehmen sogar 69 Prozent – Opfer von Datendiebstahl, Wirtschaftsspionage oder Sabotage geworden ist. So verwundert es nicht, dass laut einer Studie von International Data Corporation (IDC) [3] 70 Prozent der CEOs in transnationalen Unternehmen angeben, IT-Sicherheit als eines der wichtigsten Themen überhaupt anzusehen.

Wege zu mehr IT-Sicherheit in der Industrie 4.0

Dieser alarmierende Befund macht deutlich, dass die derzeitigen Anstrengungen, Sicherheitslücken zu identifizieren und zu beheben, nicht ausreichen. Fast 150 Jahre lang haben die TÜV-Unternehmen den Menschen vor der Technik geschützt. Mit der zunehmenden Digitalisierung müssen wir die Technik vor dem Menschen schützen. Denn in einer immer stärker vernetzten Welt, in der Prozesse, Produktion und Produkte digital verknüpft sind und Maschinen automatisch Informationen austauschen, ist es unerlässlich, dass Daten nicht für jeden einsehbar sind oder verfälscht werden können. IT-Sicherheit muss zu jeder Zeit in allen Bereichen gewährleistet sein.

Aber vor allem bei Sicherheitsprüfungen auf der Netzinfrastruktur- und Anwendungsebene herrscht Nachholbedarf. Vielen Unternehmen ist noch nicht ausreichend bewusst, dass der Aufbau und die Zertifizierung eines eigenen Information Security Management Systems (ISMS) eine zwar wichtige, aber nicht ausreichende Grundlage für eine umfassende IT-Sicherheit im Unternehmen darstellt. Es gilt vielmehr, in einem zusätzlichen Schritt die im ISMS beschriebenen Prozesse, Systeme und Konfigurationen auf ihre tatsächliche Wirksamkeit hin zu überprüfen. Dies ist die Aufgabe gezielter Penetrationstests und Schwachstellenanalysen. Sie identifizieren organisatorische und technische Sicherheitslücken, um diese anschließend gezielt und wirksam zu schließen. Bei der Betrachtung der Organisation werden Schwachstellen wie unzureichende Dokumentationstiefe oder fehlende IT-Sicherheitsrichtlinien und -prozesse konkret untersucht. Auf der technischen Ebene sind es der Vernetzungsgrad, die Absicherung der ICS-Netze (ICS = Industrial Control System) sowie Fehlkonfigurationen und unzureichende Back-ups von Komponenten. Aber diese IT-Sicherheitstests sind bislang nicht verpflichtend.

Die Digitalisierung braucht länderübergreifende verlässliche Standards, die kontrolliert und zertifiziert werden müssten. Damit Interoperabilität zwischen verschiedenen Systemen funktioniert, werden international harmonisierte Normen und Standards dringend benötigt. Die Gruppe der zwanzig wichtigsten Industrie- und Schwellenländer – G20 – hat einen Prozess entwickelt, um die Digitalisierung unter anderem der Industrie voranzutreiben. Dabei sollen zu den Themen Industrie 4.0, Smart Cities, Smart Mobility und IT-Sicherheit Möglichkeiten und Potenziale der Zusammenarbeit in der internationalen Normung ausgelotet und verbindende Kernaussagen sowie Ziele entwickelt werden. Das Bundeswirtschaftsministerium war Gastgeber des ersten G20-Digitalministertreffens Anfang April 2017 in Düsseldorf (bei Redaktionsschluss lagen noch keine Ergebnisse des Treffens vor).

Quellen

[1] Kaspersky Labs: Industrial Control Systems Vulnerabilities Statistics, 2015, Seite 5.

[2] Bundesamt für Sicherheit in der Informationstechnologie, Industrial Control Systems Security, 2016.

[3] www.computerwoche.de: Die wichtigsten IT-Trends 2015 von IDC.

Dipl.-WiWi Liliana Preuß
TÜV Informationstechnik GmbH
lpreuss@tuev-nord.de