Industrie 4.0 und IT-Sicherheit der Dinge

Das Risiko zur Chance machen!

Grundsätzlich werden im Internet der Dinge (kurz IoT – für den englischen Ausdruck „Internet of Things") reale, physische Objekte wie zum Beispiel Heizungsanlagen, Kühlschränke, Kleidung, Waschmaschinen, Sonsoren etc. mit virtuellen Repräsentationen wie etwa RFID-Chips verknüpft und in einer globalen Infrastruktur miteinander vernetzt. Mehr Komfort oder/und mehr Effizienz, so die Verheißung. Dem steht jedoch auch eine massive Vergrößerung der Angriffsfläche gegenüber, denn wie überall in der IT und im Internet besteht auch im IoT das Risiko, dass Kriminelle die verbaute Intelligenz und Kommunikationsmittel für ihre Zwecke missbrauchen. Um sich auf dem Weg ins IoT nicht wegen Sicherheitsmängeln auf sehr lange Zeit auszubremsen, ist bereits jetzt ein auf die Sicherheitsaspekte im IoT gerichtetes Handeln nötig. Gerade in Deutschland bestehen dafür sehr gute Voraussetzungen.

Prädestiniert für eine Einleitung zu dem Thema: „IT-Sicherheit in der Industrie" ist die Herleitung des Unterschiedes zwischen den beiden Begriffen: „Safety" und „Security". Safety ist in der Industrie eindeutig definiert und mit gesetzlichen Anforderungen fixiert. Durch spezielle Arbeitsrichtlinien soll der störungsfreie und anwendungssichere Betrieb von Geräten oder Fahrzeugen sichergestellt werden. Ein wesentliches Ergebnis der gesetzlichen Verordnungen ist die Tatsache, dass bei einer Einhaltung der Richtlinien keine Gefahren für den Anwender ausgehen. Die Umsetzung und Einhaltung der gesetzlichen Anforderungen wird von den Industrieunternehmen schon lange befolgt.

Anders sieht es jedoch im Umfeld des Begriffes Security aus. In der Theorie verfolgen Wissenschaft, Politik und Industrie ein gemeinsames (eindeutiges) Ziel, nämlich den Schutz der IT-Systeme vor dem unbefugten Zugriff Dritter. Hierzu existieren ebenfalls zahlreiche Richtlinien, die gesetzlichen Rahmenbedingungen sind aber entweder nicht existent oder werfen mehr Fragen auf als sie Antworten liefern. Stellvertretend hierfür lassen sich die mit dem IT-Sicherheitsgesetz der Bundesregierung einhergehenden Ungewissheiten nennen. Folglich wird das Thema Security in vielen Unternehmen nur rudimentär behandelt. Dieser Umstand stellt eine große Gefahr dar, denn die Ausprägungen des IoT sind vielseitig.

Die Motivation für die Vernetzung von Dingen und deren Mehrwert hängen vom jeweiligen Anwendungsfall ab. In Bezug auf die Industrie ist die Veränderung der Nachfrageseite und der Angebotsseite ein Treiber für den Einsatz von sogenannten Cyber Physical Systems (CPS). Das aktuelle Dilemma der Industrieunternehmen lässt sich wie folgt zusammenfassen: Auf der einen Seite wächst die Nachfrage nach individualisierten Produkten mit Losgröße 1. Auf der anderen Seite sind die aktuellen Wertschöpfungssysteme der Industrieunternehmen nicht in der Lage, diese wachsende Nachfrage zu decken. Zwangsläufig muss es in der Industrie also zu einem Paradigmenwechsel im Umgang mit den Produktionsfaktoren kommen [1]. Ein grundlegendes Ziel für Industrie 4.0 ist somit die Steigerung der Effektivität in allen Wertschöpfungsprozessen. Dazu müssen die eingebetteten Systeme der Industrie, in Anlehnung an die Konzepte des IoT, modernisiert und somit „smarter" gemacht werden. Konkrete Beispiele aus der Praxis haben bereits die Effektivität von CPS in der Industrie bewiesen. Insbesondere im Bereich der Lagerlogistik kann durch den Einsatz von RFID-Chips und Real Time Locating Systems bereits heute ein enormer Mehrwert erzielt werden (vgl. [2]). Aus Sicht der IT-Sicherheit wird dieser Mehrwert jedoch durch ein enormes Gefahrenpotenzial überschattet, wie nachfolgend anhand einer besonderen Ausprägung des IoT dargestellt wird.

Wenn heutzutage ein Unternehmen erfolgreich angegriffen wird, dann gehen damit direkte, finanzielle Schäden einher oder es kommt zu einem Imageverlust. Im Zuge der bevorstehenden Innovationen in den Bereichen IoT oder Industrie 4.0 werden auch kritische Infrastrukturen (KRITIS) mit dem Internet verschmelzen. Es ist daher sehr wahrscheinlich, dass die gängigen Angriffsvektoren aus dem Internet zukünftig auch für die KRITIS eine Gefahr darstellen. Die damit einhergehenden Folgen sind weitreichend. Parallel zu dem Begriff Safety muss zukünftig auch im Umfeld des Begriffs Security mit dem Wohl von Menschenleben umgegangen werden. Das ist aber noch nicht alles, denn erfolgreiche Angriffe auf die KRITIS eines Landes betreffen nicht nur ein Smart Home oder eine spezielle Firma, sondern vielmehr eine ganze Gesellschaft. Spätestens wenn es um das Wohl von Menschenleben und den Erhalt der öffentlichen Sicherheit geht, wird die Relevanz von gesetzlichen Verordnungen deutlich und die Forderung nach mehr Verantwortung verständlich. Diesbezüglich haben die Industrieunternehmen für Industrie 4.0 bereits ein höheres Schutzniveau im Internet gefordert. Wie steht diese Forderung jedoch im Verhältnis zu der eigenen Sensibilisierung für Security?

IT-Sicherheit in der Industrie muss sich drastisch wandeln

Bedingt durch die heutigen Medien gewinnt der Begriff IT-Sicherheit immer mehr an Relevanz. Fast täglich wird in den Nachrichten über Datenpannen oder Schwachstellen in IT-Systemen und den daraus resultierenden Folgen für die Kunden berichtet. Ausgelöst von kleinen oder großen IT-Sicherheitsvorfällen und Datenschutzpannen wird in der Bevölkerung das Interesse an IT-Sicherheit immer größer. Die Unternehmen sind zunehmend daran interessiert, nicht in den Fokus der Medien zu geraten. Der mit einer Daten-Panne verbundene Imageverlust hat in der Regel höhere Auswirkungen als die möglichen direkten finanziellen Schäden durch den Angriff an sich. Diese Tatsache wird sich wahrscheinlich im Rahmen von Industrie 4.0 drastisch ändern, denn ein Angriff auf die Produktionsanlagen eines Industrieunternehmens kann ungeahnte finanzielle Schäden mit sich bringen. Darüber hinaus können Cyber-Angriffe auf die kritischen Infrastrukturen eines Landes die öffentliche Sicherheit gefährden oder sogar Menschenleben kosten. Der Imageschaden wirkt in einem derartigen Szenario nur als Randerscheinung. Die Industrieunternehmen sind sich dieser Problematik bewusst. Deshalb wird die IT-Sicherheit im Laufe der nächsten Jahre immer mehr an Relevanz gewinnen

und fester Bestandteil der Sicherheitspolitik von Unternehmen werden. Diese Aussage lässt sowohl hoffen als auch auf eine schlechte Ausgangslage schließen.

Viele Unternehmen haben über eine lange Zeit hinweg das Thema Sicherheit von Informationssystemen vernachlässigt. Die Gründe hierfür lassen sich häufig auf die besonderen Rahmenbedingungen für Informationssysteme in der Industrie zurückführen. Nennenswert ist in diesem Zusammenhang vor allem die fehlende Schnittstelle zum Internet. Gängige Angriffsvektoren spielten per se keine Rolle bei der Konzeptionierung von Schutzvorkehrungen. Bis heute gibt es viele Unternehmen, die ihre Produkte in Form von „Insellösungen" absichern. Diese sind in der Regel proprietär und folgen dem Designprinzip der Verdunkelung – auch als „Security by Obscurity" bekannt. Mit Blick auf den heutigen Stand der Technik kann bei derartigen Lösungen nicht von Mechanismen zur Steigerung der Sicherheit gesprochen werden. Grundsätzlich gilt: Die Sicherheit eines Informationssystems darf niemals von der Geheimhaltung der Schutzmechanismen abhängen. Selbst mit dem Wissen über die verwendeten Schutzmechanismen muss die verwendete Technologie sicher sein. Es muss also Wert auf ganzheitliche Sicherheitskonzepte gelegt werden, die nicht auf proprietären Lösungen beruhen, sondern vielmehr Standard-Lösungen verwenden. Hierbei kann es sich um Lösungen handeln, die im Vorfeld von Behörden oder wissenschaftlichen Institutionen als sicher eingestuft beziehungsweise zertifiziert wurden (vgl. [3]).

Besonders im Rahmen von eingebetteten Systemen ist ein geeignetes Sicherheits-Management von besonderer Bedeutung, denn bei diesen Systemen muss die Sicherheit über verschiedene Produktlebenszyklen hinweg gewährleistet werden. Dies wird viele Unternehmen vor eine besondere Herausforderung stellen. In vielen Fällen existiert nicht einmal eine Richtlinie für die Löschung eines ausgeschiedenen Mitarbeiters. Die Forderung der Industrie nach einem höheren Schutzniveau im Internet ist zwar legitim, dennoch darf die eigene Verantwortung nicht vernachlässigt werden.

Zukünftiges Sicherheitsniveau wird bereits heute beeinflusst

Viele der aktuellen Sicherheitsmaßnahmen im Internet lassen sich infolge der besonderen Rahmenbedingungen nicht auf die zukünftigen Systeme übertragen. Für eine Sicherheitsbetrachtung ist es also zunächst wichtig, diese speziellen Anforderungen zu identifizieren. In Abbildung 1 sind die einzelnen Rahmenbedingungen und deren Beziehung zueinander dargestellt.

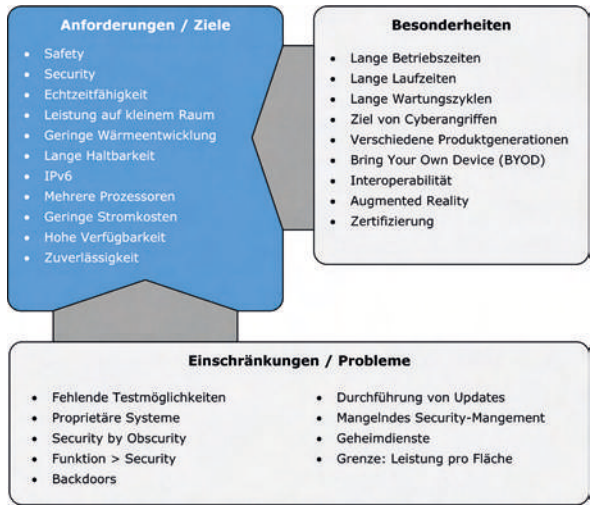

Abbildung 1: Rahmenbedingungen für Informationssysteme in der Industrie

Nicht alle aufgeführten Rahmenbedingungen werden langfristig eine Rolle spielen. Da die Entwicklung hin zu Industrie 4.0 aber ein fließender Prozess ist und heute immer noch Systeme ausgerollt werden, die diesen Rahmenbedingungen unterliegen, müssen sie bei heutigen Sicherheitsbetrachtungen dennoch berücksichtigt werden. Dieser Umstand ist der Tatsache geschuldet, dass die Systeme in der Industrie längere Produktlebenszyklen aufweisen müssen. Eine störungsfreie Produktion wirkt sich direkt auf die Wirtschaftlichkeit eines Industrieunternehmens aus. Die Systeme werden dementsprechend für lange Laufzeiten konstruiert. Diese Besonderheit kann bereits heute Auswirkungen auf die Sicherheit in Industrie 4.0 haben. Werden weiterhin Komponenten ohne geeignete IT-Sicherheitsmechanismen ausgerollt, wird es langfristig zu schwer auffindbaren Schwachstellen in den Systemen der Industrie kommen. Der Aufwand für das Nachrüsten von IT-Sicherheitsmechanismen kann enorm sein. Zusätzlich besteht auch die Wahrscheinlichkeit, dass keine IT-Sicherheitsmechanismen nachgerüstet werden können. Schließlich werden die heutigen eingebetteten Systeme für besondere Anforderungen gefertigt. Es gilt: Leistung muss auf kleinem Raum, mit geringer Wärmeentwicklung und geringem Stromverbrauch erzielt werden. In vielen Fällen ist schlichtweg kein Platz für weitere IT-Sicherheitsmechanismen vorhanden.

Die Relevanz für eine Betrachtung der konkreten Rahmenbedingungen kann durch ein weiteres Beispiel verdeutlicht werden. Wie in Abbildung 1 bereits dargestellt, unterliegen die zukünftigen Systeme einer Reihe von Anforderungen. Für die Industrie sind die folgenden Anforderungen von besonderer Bedeutung: hohe Verfügbarkeit, hohe Sicherheit, Zuverlässigkeit und Echtzeitfähigkeit. Im Gegensatz zu den Anforderungen in einem Heim-Netz (große Datenmengen, niedrige Kosten, niedrige Verzögerung) hat die Datenrate geringe Priorität. Dienste, wie zum Beispiel IP-TV oder Streaming, verursachen im Heim-Netz Datenmengen im GByte-Bereich. Das Versenden von Sensordaten oder Steuernachrichten verursacht im normalen Betrieb lediglich Datenmengen in Höhe von einigen KByte (vgl. [4]). Durch die unterschiedlichen Anforderungen können auch unterschiedliche IT-Sicherheitsmechanismen zum Einsatz kommen, wie im weiteren Verlauf noch erläutert wird.

Handlungsbedarf lässt sich aus den Anwendungsszenarien ableiten

Durch die Vernetzung von Produktions-IT und Business-IT entstehen mit Industrie 4.0 viele neue Kommunikationswege, die aus Sicht der IT-Sicherheit von entscheidender Bedeutung sind. Viele Gefahren und Schutzbedarfe lassen sich direkt aus den Kommunikationswegen ableiten. Neben der Sicherung von Kommunikationskanälen muss auch an jedem Knotenpunkt selbst über IT-Sicherheitsmechanismen nachgedacht werden. Einige interessante Kommunikationsszenarien sind in den Abbildungen 2 bis 4 dargestellt. Als Ausgangspunkt für die neuen Kommunikationswege wird in jeder Abbildung das Schichtenmodell nach DIN ISO 62264 verwendet. Dieses Schichtenmodell eignet sich ideal für die Beschreibung der aktuellen Kommunikationswege im klassischen Produktionsumfeld.

Jedes Kommunikationsszenario demonstriert die Erweiterung des klassischen Produktionsumfeldes um neue innovative Anwendungsszenarien. Allen Szenarien ist gemeinsam, dass eine Fülle an neuen Schnittstellen zum Internet entsteht. Die neuen Schnittstellen sind potenzielle Einfallstore für die Angreifer und müssen deshalb bei jeder IT-Sicherheitsbetrachtung besonders berücksichtig werden.

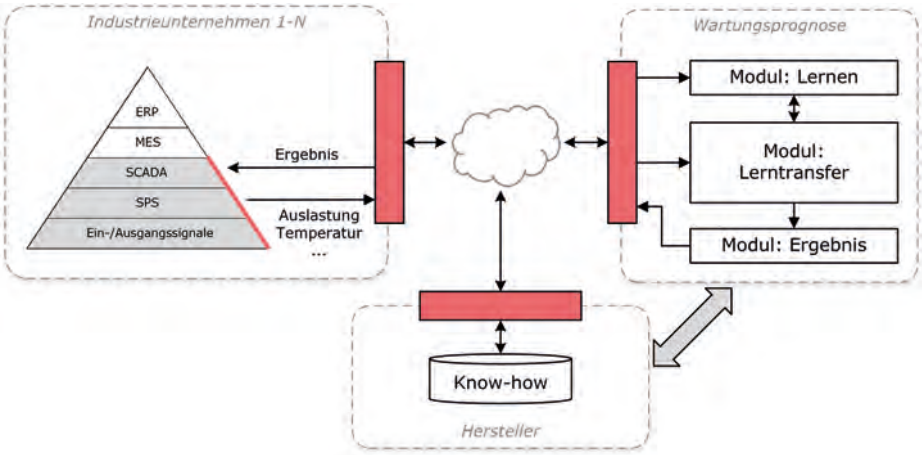

Abbildung 2: Wartungszyklen in Industrie 4.0 prognostizieren

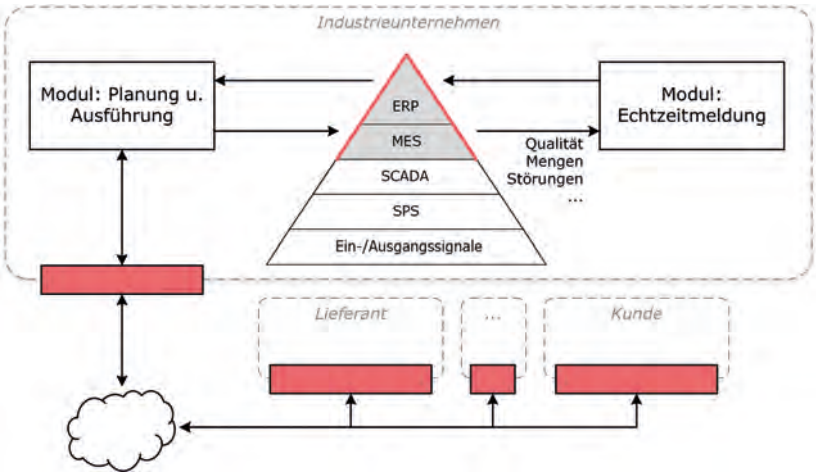

Abbildung 3: Synergien während der Planung, Steuerung und Ausführung von Aufträgen erzielen

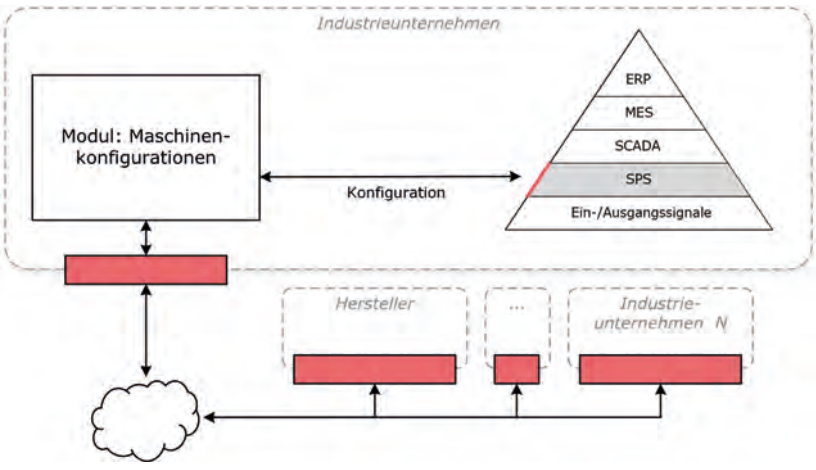

Abbildung 4: Austausch von Maschinenkonfigurationen bei Industrie 4.0

Das in Abbildung 2 dargestellte Anwendungsszenario lässt das große Potential von Cloud Computing und Big Data in der Industrie erahnen. Der konkrete Einsatz dieser Technologien ist in der klassischen IT bereits gang und gäbe. Der daraus resultierende Mehrwert ist unumstritten. In vielen Strategiepapieren zu Industrie 4.0 ist der Einsatz dieser Technologien bereits fester Bestandteil. Entgegen aller Euphorie sei aber darauf hingewiesen, dass das Einsatzgebiet von Cloud Computing ebenfalls von den zuvor geschilderten Rahmenbedingungen abhängt. Insbesondere die Anforderungen an die Echtzeitfähigkeit könnten vielen Anwendungsszenarien einen Strich durch die Rechnung machen (vgl. [5]).

Rahmenbedingungen ermöglichen effektive IT-Sicherheitsmechanismen

Im Umfeld von Industrie 4.0 kommt es zur Verschmelzung von IT-Systemen mit unterschiedlichen Sicherheitsanforderungen. Aus diesem Grund muss für jeden einzelnen Anwendungsfall und für jedes einzelne Zielsystem abgewogen werden, welche IT-Sicherheitsmechanismen benötigt werden und welche überhaupt realisierbar sind. Wie bereits im Vorfeld erläutert wurde, hängt die konkrete Auswahl von geeigneten Schutzmaßnahmen direkt von den zugrundeliegenden Rahmenbedingungen ab.

Im Gegensatz zu den klassischen IT-Systemen ist beispielsweise die Zahl der erwünschten Operationen in einer Produktionsumgebung überschaubar klein. Diese erwünschten Operationen könnten in sogenannten Whitelists festgelegt werden. Die Filterung von erwünschten oder unerwünschten Operationen könnte anschließend durch eine Application Layer Firewall realisiert werden. Der Einsatz dieser speziellen Firewalls ist in der klassischen IT nur bedingt möglich, da die Analyse von Daten aus der Anwendungsebene oft mit starken Performanz-Einbußen verbunden ist. Zum einen können die Protokolle auf Anwendungsebene große Datenmengen produzieren, zum anderen ist es aufgrund der hohen Komplexität der Protokolle nur sehr schwer zu entscheiden, welche Daten überhaupt gefiltert werden sollen. Dieser Sachverhalt

trifft höchstwahrscheinlich nicht auf die zukünftigen Systeme in der Industrie zu. Wie in dem zuvor geschildeten Beispiel erwähnt, sind die entstehenden Datenmengen mit einigen KByte weitaus geringer, als es in klassischen Anwendungen der Fall ist. Des Weiteren ist in der Regel im Vorfeld spezifiziert, welche Funktionen ein eingebettetes System auf Anwendungsebene realisieren muss. Daraus lassen sich direkt die erlaubten Parameter innerhalb der Kommunikation ableiten. Die Gefahr durch zusätzliche Software und damit einhergehende unberücksichtigte Protokolle stellt durch die genaue Spezifikation der benötigten Funktionalitäten keine Bedrohung dar. Im Gegensatz dazu besteht in der klassischen IT immer das Risiko, dass ein Anwender eine zusätzliche Software auf seinem Desktop-PC installiert, über die ein Angreifer in das System eindringen kann. In diesem Fall ist es eher hinderlich, jede erlaubte Operation erst in eine Liste aufnehmen zu müssen.

Die Sicherstellung der Authentizität der einzelnen Befehle bekommt bei diesem Ansatz jedoch eine besondere Bedeutung. Whitelisting bietet keinen Schutz, wenn gültige Befehle von einem Angreifer versendet werden. Dies kann beispielsweise der Fall sein, wenn der Computer eines Mitarbeiters kompromittiert wurde. Der Angreifer kann zwar nur vordefinierte Befehle nutzen, die Entstehung eines Schadens ist dennoch möglich. Des Weiteren ist die Sicherheit des Systems nur gewährleistet, wenn die Firewall ordnungsgemäß konfiguriert ist, was in der Praxis häufig ein Problem darstellt. Im Vergleich zu Antivirenprogrammen hat das Whitelisting jedoch einen entscheidenden Vorteil: Unbekannte Malware stellt keine Bedrohung dar, und zusätzliche Ressourcen werden auf der Hardware nicht beansprucht.

Die überschaubare Komplexität der eingebetteten Systeme in der Industrie bringt einen weiteren Vorteil mit sich. Alle diese Systeme werden speziell für die Erfüllung einer bestimmten Aufgabe konstruiert. Sowohl auf Hardware-Ebene als auch auf Software-Ebene sind die Anforderungen an eine flexible Einsatzmöglichkeit gering. Daraus folgt, dass die Komplexität der Betriebssysteme ebenfalls gering gehalten werden kann. Im Gegensatz zu den klassischen IT-Systemen können die einzelnen Komponenten eines CPS mit Mikro-Kernels ausgestattet werden. Hierbei handelt es sich um minimalistische Betriebssysteme, die nur mit den nötigsten Funktionen ausgestattet sind. Diese Mikro-Kernels können vereinfacht überprüft und zertifiziert werden. Das Risiko für Schwachstellen oder Backdoors ist somit deutlich geringer als bei herkömmlichen Betriebssystemen.

Eine Chance, es von Anfang an richtig zu machen

Der Paradigmenwechsel im Umgang mit den Produktionsfaktoren ist ein möglicher Grund dafür, dass zwei Welten mit unterschiedlichen Rahmenbedingungen unaufhaltsam aufeinanderprallen werden. Skalierbarkeit, Flexibilität und unerschöpfliche Ressourcen in der klassischen IT treffen auf hohe Anforderungen an Formfaktor und Ressourceneffizienz in der Produktions-IT. Diese Rahmenbedingungen nehmen enormen Einfluss auf die Konzeptionierung und Entwicklung von geeigneten Sicherheitsmechanismen. Sie sind aber zeitgleich auch dafür verantwortlich, dass das Thema Security in der Industrie bisher vernachlässigt werden konnte. Die Ausgangslage für die IT-Sicherheit in Industrie 4.0 ist dementsprechend denkbar schlecht. Das gilt nicht nur für die eigenen Systeme in der Industrie, sondern auch für die produzierten Produkte, die Teil des IoT werden könnten. Auf der letzten IT-Sicherheitskonferenz „Black Hat" in Las Vegas wurde dieser Umstand erneut an praktischen Beispielen demonstriert. Dort wurden Autos gehackt, Scharfschützengewehre manipuliert und Angriffsszenarien auf Toaster geschildert. Die wichtigste Erkenntnis ist: Heute sind überwiegend keine geeigneten IT-Sicherheitsmechanismen verbaut oder Mechanismen zum nachträglichen Aufspielen oder Updaten vorhanden. Die daraus resultierende Gefahr ist groß, denn es werden immer weiter Systeme ausgerollt, die das zukünftige Schutzniveau bereits heute maßgeblich beeinflussen.
Es besteht nun die einmalige Chance, die bereits aus der Office-IT und dem allgemeinen Internet bekannten Fehler und Herausforderungen im Umfeld von Industrie 4.0 zu meistern. Die zahlreichen Angriffsszenarien und Gefahren sind Motivation genug, um die Kosten und Mühen auf sich zu nehmen. Zusammen mit einem starken Mittelstand besteht die Möglichkeit, eine Souveränität aus Deutschland heraus zu entwickeln. Diese Souveränität ist nicht nur auf Industrie 4.0 begrenzt, denn viele Ergebnisse werden sich ebenfalls positiv auf das gesamte Internet auswirken. Was Deutschland bisher im Internet verpasst hat, könnte mit Blick auf die gute Positionierung des Landes im Umfeld der Industrie wieder wettgemacht werden. ■

Literaturverzeichnis

- *[1] T. Bauernhansl, M. ten Hompel und B. Vogel-Heuser, Industrie 4.0 in Produktion, Automatisierung und Logistik, Wiesbaden: Springer Vieweg, 2014.*
- *[2] V. Stich, M. Deindl, F. Jordan, L. Maecker und F. Weber, „Studie – Cyber Physical Systems in der Produktionspraxis," April 2015. [Online]. Available: http://www.cps-hub-nrw.de/#Publikationen.*
- *[3] U. Bub und K. D. Wolfenstetter, Beherrschbarkeit von Cyber Security, Big Data und Cloud Computing – Tagungsband zur dritten EIT ICT Labs-Konferenz zur IT-Sicherheit, Springer Vieweg, 2014.*
- *[4] C. Wietfeld, „Kommunikationsnetze für Cyber Physical Systems," November 2013. [Online]. Available: http://www.cps-hub-nrw.de/#Publikationen.*
- *[5] B. Holtkamp, U. Springer und S. Steinbuß, „Cloud Computing und Cyber-Physical Systems," April 2014. [Online]. Available: http://www.cps-hub-nrw.de/#Publikationen.*

RENÉ RIEDEL,
wissenschaftlicher Mitarbeiter am Institut für Internet-Sicherheit – if(is) der Westfälischen Hochschule Gelsenkirchen, Forschungsbereich: Zahlungssysteme und Banktransaktionen

NORBERT POHLMANN,
Informatikprofessor für Verteilte Systeme und Informationssicherheit sowie Leiter des Instituts für Internet-Sicherheit – if(is) an der Westfälischen Hochschule Gelsenkirchen. Außerdem ist er Studienbeauftragter für den Master Internet-Sicherheit.