Bundesministerium
für Wirtschaft
und Energie

Studie im Auftrag des Bundesministeriums für Wirtschaft und Energie

IT-Sicherheit für Industrie 4.0

Produktion, Produkte, Dienste von morgen im Zeichen globalisierter Wertschöpfungsketten

Abschlussbericht – Kurzfassung

Impressum

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

Gestaltung und Produktion
PRpetuum GmbH, München

Stand
04. Januar 2016

Druck
Silber Druck oHG, Niestetal

Zertifikat seit 2002
audit berufundfamilie

Das Bundesministerium für Wirtschaft und Energie ist mit dem audit berufundfamilie® für seine familienfreundliche Personalpolitik ausgezeichnet worden. Das Zertifikat wird von der berufundfamilie gGmbH, einer Initiative der Gemeinnützigen Hertie-Stiftung, verliehen.

FSC
www.fsc.org
MIX
Papier aus verantwortungsvollen Quellen
FSC® C044084

Diese und weitere Broschüren erhalten Sie bei:
Bundesministerium für Wirtschaft und Energie
Referat Öffentlichkeitsarbeit
E-Mail: publikationen@bundesregierung.de
www.bmwi.de

Zentraler Bestellservice:
Telefon: 030 182722721
Bestellfax: 030 18102722721

Inhalt

Tabellen- und Abbildungsverzeichnis

Autoren

Autoren-Kernteam

Dr. Daniel Bachlechner, Fraunhofer ISI

Dr. Thorsten Behling, WTS Legal Rechtsanwaltsgesellschaft mbH

Esther Bollhöfer, Fraunhofer ISI

Thomas Dexheimer, Fraunhofer SIT

Prof Dr. Georg Borges, Universität des Saarlands

Michael Gröne, Sirrix AG

Peter Handel, Fraunhofer ESK

Dr. Thorsten Henkel, Fraunhofer SIT

Jana Post, WTS Legal Rechtsanwaltsgesellschaft mbH

Michael Stiller, Fraunhofer ESK

Gerhard Sutschet, Fraunhofer IOSB

Dr. Thomas Usländer, Fraunhofer IOSB

Michael Voeth, Robert Bosch GmbH

Heiko Weber, Software AG

Andreas Wigger, WTS Legal Rechtsanwaltsgesellschaft mbH

Review-Beteiligte

Dr. Detlef Hühnlein, ecsec GmbH

Jens Mehrfeld, Bundesamt für Sicherheit in der Informationstechnik

Dr. Norbert Schirmer, Sirrix AG

Prof. Dr. Jörg Schwenk, Ruhr-Universität Bochum / Horst Görtz Institut für IT-Sicherheit (HGI)

Christian Stüble, Sirrix AG

Expertenbeirat

Stefan Bauer, WITRON Logistik + Informatik GmbH
Klaus Bauer, TRUMPF Werkzeugmaschinen GmbH + Co. KG
Alfons Botthof, VDI/VDE Innovation + Technik GmbH
Wolfgang Dorst, BITKOM
Andreas Dümmler, ARBURG GmbH + Co KG
Tobias Gschwend, Otto Bihler Maschinenfabrik GmbH & Co. KG
Andreas Harner, DKE/VDE
Karl Haug, Felss Systems GmbH
Steffen Heyde, TeleTrusT – Bundesverband IT-Sicherheit e.V.
Stefan Hoppe, OPC Foundation
Dr. Detlef Houdeau, Infineon Technologies AG
Dr. Lutz Jänicke, Innominate Security Technologies AG
Benjamin Jurke, DMG Mori GmbH
Dr. Wolfgang Klasen, Siemens AG
Lukas Klotz, DMG Mori GmbH
Markus Preisinger, Felss Systems GmbH
Siegfried Schülein, infoteam Software AG
Martin Schwibach, BASF SE
Dr. Inessa Seifert, VDI/VDE Innovation + Technik GmbH
Dr. Walter Speth, Bayer Technology Services GmbH
Christian von Rützen, Dachser GmbH & Co. KG
Richard Wagner, Otto Bihler Maschinenfabrik GmbH & Co. KG

Vorbemerkungen

Die Verwendung des Begriffes „Sicherheit“ meint im Kontext der Studie immer IT-Sicherheit (englisch (IT-)„security“) und nicht die deutsche Übersetzung des englischen Wortes „safety“.

Die vorliegende Kurzfassung stellt die zentralen Ergebnisse des Abschlussberichtes der Studie dar.

Das Abkürzungsverzeichnis sowie der Glossar finden sich im Abschlussbericht.

Alle Personenbezeichnungen in der vorliegenden Studie beziehen sich ungeachtet ihrer grammatikalischen Form in gleicher Weise auf Frauen und Männer.

1 Motivation und Zielsetzung der Studie

Die Vision von Industrie 4.0 (kurz I4.0) beschreibt eine neue Art der wirtschaftlichen Produktion, die durch eine durchgängige Digitalisierung und die stärkere innerbetriebliche sowie überbetriebliche Vernetzung geprägt ist. Schon heute bestimmen IT-Infrastrukturen in zunehmendem Maße die industriellen Prozesse und sind in fast allen Bereichen unverzichtbar. Zukünftig werden komplexe IT-Infrastrukturen – bestehend aus mobilen und stationären Komponenten – die gesamte industrielle Wertschöpfungskette durchdringen und heute kaum vorstellbare Flexibilitäts- und Effizienzsteigerungen ermöglichen. Für die Zuverlässigkeit solcher Systeme und zum Schutz betriebs- und personengebundener Daten ist ein hohes Maß an IT-Sicherheit unabdingbar. Der Schutz vor Cyberattacken zur illegalen Aneignung von Daten oder zur Sabotage IT-basierter industrieller Prozesse betrifft neben einzelnen Teilnehmern ganze Wertschöpfungsketten bzw. -netzwerke, die vielfach global organisiert sind. Die heute weitgehend noch fehlende IT-Sicherheit wird laut VDE-Trendreport 2015[1] derzeit als das weitaus größte Hindernis für den Einzug von I4.0 in die produzierenden Betriebe Deutschlands gesehen. An gleicher Stelle wird auch zu Recht darauf hingewiesen, dass insbesondere IT-Sicherheit, als eine Dimension der Produktqualität und Alleinstellungsmerkmal der in Deutschland produzierenden Unternehmen, eine wichtige technologische Voraussetzung und der entscheidende „enabling" Faktor für die Umsetzung der Vision „Industrie 4.0" sein wird.

I4.0 entsprechend der Vision der acatech-Studie[2] und der Plattform Industrie 4.0[3] ist heute noch in keinem Unternehmen voll verwirklicht. Zukünftige Vorgänge, die in der derzeitigen Situation von vernetzten industriellen Prozessen tatsächlich stattfinden, können jedoch auf Basis existierender Publikationen zu I4.0 „extrapoliert" werden. Dies kann sowohl in Richtung weiter zunehmender Vernetzung über Länder-, Standort-, und Unternehmensgrenzen, als auch in Richtung zunehmender autonomer Abläufe in Produktion und Logistik und zunehmender Verfügbarkeit von großen und teils sensitiven Datenbeständen geschehen. Eine zentrale Herausforderung für die Industrie von morgen, insbesondere durch zunehmende Digitalisierung, Dynamik und Komplexität, ist die Fähigkeit der I4.0-IT-Architektur, sich an Änderungen anzupassen – sei es, dass neue Anlagen oder Produktionsprozesse in das System und dessen Netzwerk eingebracht werden oder dass bestehende Produktionssysteme und zugehörige Netzwerke verändert und nach außen geöffnet werden.[4] Eine wesentliche Veränderung durch I4.0 ist die Entstehung von dynamischen, echtzeitoptimierten und sich selbst organisierenden, unternehmensübergreifenden Ad-hoc-Wertschöpfungsnetzwerken.

Hauptcharakteristika der I4.0-Wertschöpfungsketten sind hierbei die

- Ab- bzw. Auflösung der klassischen Automatisierungspyramide[5]
- Verteilung der Wertschöpfungsprozesse auf verschiedene Akteure
- Hohe Dynamik der Kooperationsdauer der im Wertschöpfungsprozess beteiligten Partner
- Unterschiedliche technologische, betrieblich-organisatorische wie auch rechtliche Ausstattung der Partner: Sehr kleine Unternehmen (wie z. B. ein zwei bis fünf Mitarbeiter Ingenieurbüro) und international agierende Großkonzerne

Die Ablösung der klassischen Automatisierungspyramide und Verteilung des Wertschöpfungsprozesses auf verschiedene Akteure führen zu neuen Herausforderungen hinsichtlich IT-Sicherheit und bedingen neue IT-Sicherheitsmanagementprozesse, die nun über die Unternehmensgrenzen hinweg etabliert werden müssen. Unternehmensübergreifende Bedrohungsanalysen und Vertrauensbeziehungen werden notwendig.

1 Zusammenfassung der Studienergebnisse des VDE-Trendreports Elektro- und Informationstechnik 2015, https://www.vde.com/de/Verband/Pressecenter/Pressemeldungen/Fach-und-Wirtschaftspresse/2015/Documents/25-15_Hannover%20Messe_lang.pdf, abgerufen am 10.07.2015; VDE-Trendreport 2015 Elektro- und Informationstechnik, https://www.vde.com/de/InfoCenter/Seiten/Details.aspx?eslShopItemID=9ecf52cb-c85b-4a46-af0e-599367756c76, abgerufen am 10.07.2015.

2 Forschungsunion/acatech, Umsetzungsempfehlungen für das Zukunftsprojekt Industrie 4.0, April 2013.

3 Umsetzungsstrategie Industrie 4.0 – Ergebnisbericht der Plattform Industrie 4.0, April 2015, Seite 8.

4 Vgl. Secure Plug and Work – Ein Beitrag zum Zukunftsprojekt Industrie 4.0, Fraunhofer IOSB, http://www.iosb.fraunhofer.de/servlet/is/47385/, abgerufen am 10.07.2015.

5 Vgl. Kapitel 3.1.1 des Abschlussberichtes, Abbildung 3-1.

Zielsetzung der Studie

Vor dem Hintergrund dieser Herausforderungen hinsichtlich IT-Sicherheit für die I4.0 stellt sich die Frage was zu berücksichtigen ist: Welche Bedrohungen sind absehbar? Welche proaktiven IT-Security-Maßnahmen sind zum Schutz vor diesen Bedrohungen zu ergreifen? Welche reaktiven Maßnahmen sind nach einem IT-Security-Vorfall bzw. Schadensfall zu ergreifen? Und sind diese Maßnahmen über heutige Best-Practice-Ansätze abdeckbar oder existieren Hindernisse? Welche IT-Sicherheitskonzepte existieren und welche Ansätze für neue IT-Sicherheitskonzepte, die einen Rahmen vorgeben können, müssen durch Unternehmen und die Politik verfolgt werden?

Das Hauptziel dieser Studie ist daher die Ableitung von rechtlichen, organisatorischen und technischen Handlungsvorschlägen für Unternehmen und insb. KMU sowie Wirtschafts-, Technologie- und Förderpolitik sowie Aufsichts- und Regulierungsbehörden hinsichtlich der IT-Sicherheit von zukünftigen Wertschöpfungsnetzwerken. Diese Handlungsvorschläge werden hauptsächlich abgeleitet aus vier ausgewählten, praxisrelevanten I4.0-Fallbeispielen aus der Industrie (siehe Kapitel 4).

Im Gegensatz zu anderen Werken, insbesondere IT-Sicherheitsstandards und Technischen Richtlinien oder z. B. dem Grundschutzhandbuch des Bundesamtes für Sicherheit in der Informationstechnik (BSI), verzichtet die vorliegende Studie nach Möglichkeit auf die Darstellung technischer Details. Vielmehr stehen neben technologischen Herausforderungen in dieser Studie die organisatorischen und rechtlichen Fragestellungen sowie die Handlungsvorschläge im Vordergrund.

Der für ein sicheres Zusammenspiel von I4.0-Komponenten unerlässliche Informationsaustausch zwischen den unterschiedlichen Disziplinen (Technik, Organisation, Recht) ist ein wichtiges Ziel. Eine interdisziplinäre Betrachtung wird insbesondere benötigt, um I4.0 überhaupt in der Praxis einsetzen zu können, da Unternehmen sonst auf Grund von rechtlichen (oder nur psychologischen) Unsicherheiten und (gefühlten) Risiken auf den praktischen Einsatz von I4.0 verzichten würden.

Ein weiteres Ziel dieser Studie ist es, die Grenzen und Regeln hinsichtlich IT-Sicherheit zu definieren.

Die Vorgehensweise und die Methodik der Studie sowie die Abgrenzung zu anderen Arbeiten werden in den Kapiteln 1.4 und 1.5 des Abschlussberichtes ausführlich erläutert.

Die Studie wurde im Auftrag des Bundesministeriums für Wirtschaft und Energie (BMWi) von August 2014 bis Juli 2015 erstellt. Der Inhalt und die Empfehlungen wurden unabhängig durch die Auftragnehmer erarbeitet und reflektieren nicht notwendigerweise die Meinung des BMWi.

2 Studienbeteiligte und Beirat

Angesichts der hohen Komplexität, der noch nicht vollständig absehbaren Ausgestaltung der zukünftigen I4.0 und der notwendigen IT-Sicherheit ist für die Erstellung dieser Studie ein interdisziplinäres Autorenteam gebildet worden, um Know-how aus den unterschiedlichen Wissensbereichen Recht, Organisation und Technik zusammenzuführen. Das Autorenteam hat sich unter Leitung der Sirrix AG aus folgenden Organisationen und Schwerpunkten zusammengesetzt:

Angewandte Forschung sowie Normung und Standardisierung: **Fraunhofer Gesellschaft e.V.** mit Experten aus vier Instituten (ESK, IOSB, ISI, SIT).

IT-Sicherheitsindustrie: **Sirrix AG security technologies**.

Anbieter von Produkten im Umfeld I4.0 sowie Experten bei der Modellierung von Industrieprozessen: **Software AG**.

Integrator und Betreiber von Produkten im Umfeld I4.0: **Robert Bosch GmbH**.

Rechtliche Implikationen: **WTS Legal Rechtsanwaltsgesellschaft mbH** und **Prof. Dr. Georg Borges (Universität des Saarlands)**.

Reviews: **ecsec GmbH** und **Prof. Dr. Jörg Schwenk (Ruhr-Universität Bochum / Horst Görtz Institut für IT-Sicherheit (HGI))**.

Unterstützt wurde dieses Autorenteam durch einen umfangreichen Expertenbeirat[6] und insbesondere durch zwei assoziierte Partner:

IT-Sicherheitsbehörde: **Bundesamt für Sicherheit in der Informationstechnik (BSI)**.

IT-Sicherheitsverband: **TeleTrusT – Bundesverband IT-Sicherheit e.V.**

Einbindung des Beirates

Der im Zuge der Studie zusammengestellte Beirat aus namhaften Experten aus der Industrie wurde im Zuge eines Initialworkshops im November 2014 zur Vorstellung und Diskussion des Studiendesigns als auch im Zuge eines Expertenworkshops zur Hannover Messe 2015 zur Vorstellung und Diskussion der zentralen Handlungsvorschläge eingebunden. Die genutzten Fallbeispiele stammen von über den Beirat eingebundenen Industrieunternehmen. Erste Schlussfolgerungen wurden dem Beirat zur Kommentierung übersendet, die Rückmeldungen flossen in die Studie ein. Der Beirat wurde zudem um Stellungnahme zur finalen Entwurfsfassung gebeten. Die im Beirat vertretene Begleitforschung des BMWi-Forschungsprogramms „AUTONOMIK Industrie 4.0“, das Institut für Innovation und Technik (iit) in der VDI/VDE-Innovation + Technik GmbH, führte zudem im Januar 2015 einen Workshop – „Softwarearchitekturen für die Industrie 4.0“, durch, in welchem die Studie vorgestellt und Hinweise auf Herausforderungen aus weiteren konkreten Fallbeispielen aus den Autonomik-Projekten aufgenommen wurden.

6 Siehe Seite 11 „Expertenbeirat“ des Abschlussberichtes.

3 Zielgruppe

Die Studie richtet sich an alle interessierten Personen aus dem Bereich der industriellen Produktion, sie wurde auf besonderen Wunsch des Auftraggebers so verfasst, dass insbesondere Personen außerhalb des Fachexpertenkreises alle Informationen verstehen können. Als Zieladressatenkreis werden Entscheider in Unternehmen und Branchenverbänden, in Wirtschafts-, Technologie- und Förderpolitik, beim Gesetzgeber und in Aufsichts- und Regulierungsbehörden sowie in Standardisierungs- und Normierungsorganisationen erachtet. Für die Politik hinsichtlich ihrer Rolle in der notwendigen Moderation von Verhandlungsprozessen, bei der Förderung und der Gesetzgebung. Die Studie verfolgt das Ziel, diesem primären Zieladressatenkreis gerecht zu werden. Technische Detailanalysen treten daher gegenüber der Darstellung der übergreifenden technisch-organisatorisch-rechtlichen Zusammenhänge zurück.

4 Fallbeispiele, identifizierte Risiken und Herausforderungen

Ausgangspunkt der Studie sind vier praxisnahe Fallbeispiele aus ausgewählten unterschiedlichen Branchen, basierend auf Zulieferungen aus der Industrie (siehe Tabelle 4-1). Anhand dieser Fallbeispiele wurden die Situation der IT-Sicherheit und die zukünftigen Handlungsoptionen festgemacht. Eine umfassende wissenschaftliche Analyse der gesamten Industrie ist nicht erfolgt, weshalb keine allgemeingültigen Aussagen getroffen werden. Siehe hierzu auch Kapitel 4.1 des Abschlussberichtes.

Fallbeispiel Anlagen-/Maschinenbau

Dieses Beispiel betrifft den Anwendungsfall der Fernwartung im Anlagen- und Maschinenbau unter dem Gesichtspunkt der IT-Sicherheit. Derzeit existiert hier keine durchgängige oder standardisierte Lösung, was insbesondere kleinen und mittleren Unternehmen zunehmend Probleme bereitet. Diese Probleme werden sich im Rahmen von I4.0 aufgrund der zunehmenden Komplexität drastisch verschärfen.

Tabelle 4-1: Übersicht der ausgewählten Fallbeispiele aus der Industrie mir Verweisen auf Detailbeschreibungen im Abschlussbericht

Branche	Fallbeispiel	Details
Automobilbau	Inbetriebnahme produktionsrelevanter Echtzeitsysteme unter Zeitdruck	Kapitel 4.1.1
Anlagen-/Maschinenbau	Fernwartung	Kapitel 4.1.2
Chemische Industrie	Netzwerksegmentierung in der Produktion	Kapitel 4.1.3
Logistik	Integration von Logistikprozessen	Kapitel 4.1.4

Es folgen Kurzbeschreibungen der Fallbeispiele, ausführliche Details finden sich im Text des Abschlussberichtes, siehe Tabelle 4-1.

Fallbeispiel Automobilbau

Inbetriebnahmen einzelner Anlagen oder produktionsrelevanter Systeme (Echtzeitsysteme) unter Zeitdruck gefährden die IT-Sicherheit ganzer Produktionsnetze. Denn bei steigendem Zeitdruck sind Produktionsverantwortliche eher bereit IT-Sicherheitsrichtlinien zu vernachlässigen als eine Verzögerung des Produktionsanlaufs – und damit Einbußen in produzierten Stückzahlen – in Kauf zu nehmen.

Diese „lokalen" Verletzungen der IT-Sicherheitsrichtlinien führen typischerweise zu „global" unsicheren Situationen, weil die Ausnutzung lokaler IT-Sicherheitslücken üblicherweise die gesamte IT-Sicherheitsinfrastruktur kompromittiert.

Dieser Anwendungsfall verdient in Rahmen dieser Studie vor allem deshalb besondere Beachtung, weil hier typischerweise viele kleine und mittlere Unternehmen oft mit Großunternehmen zu einer für beide Seiten zufriedenstellenden und auch praktikablen Lösung finden müssen. Große Unternehmen müssen heute viele Lösungen akzeptieren, da sonst die Produkte teurer werden, (wenn diese nicht ihre Standard-IT-Sicherheitslösung einsetzen dürfen). KMU müssen dagegen oft auch Szenarien akzeptieren, die große Unternehmen vorgeben.

Des Weiteren spielt bei diesem Anwendungsfall auch das Schutzziel der Unabstreitbarkeit eine wichtige Rolle, da hier zeitweilig die faktische Kontrolle und damit die Verantwortung für schützenswerte Daten von einem Akteur auf einen anderen übergehen. Die hierfür erforderliche Vertrauensbasis ist, da mit verfügbaren Methoden nicht quantifizierbar, heute nicht gegeben.

I4.0-Komponenten zeichnen sich unter anderem dadurch aus, dass große Datenmengen gesammelt und über Netz-

werke (in Gegensatz zu heute auch dauerhaft) ausgetauscht und ausgewertet werden. Die Fernwartung von Maschinen, die zwar bereits heute vielfach praktiziert wird, wird damit aus Sicht der IT-Sicherheit vielschichtiger und kritischer.

Fallbeispiel aus der chemischen Industrie

In den Produktionsprozessen der chemischen Industrie sind heute schon häufig Anlagen über verschiedene Ebenen der Wertschöpfungskette miteinander verbunden. Als Schutzmechanismus ist das Netzwerk, über welches die Anlagen miteinander kommunizieren, in verschiedene IT-Sicherheitszellen unterteilt mit Regeln, welche Komponenten aus welchem Netzsegment mit welchen anderen Komponenten in einem anderen Netzsegment kommunizieren dürfen.

Die Regelung der Netzwerksegmentierung erfordert neue Technologien, wenn im Rahmen von I4.0 die Systeme unternehmensübergreifend und über alle Schritte der Produktion hinweg miteinander vernetzt werden sollen. Zudem wird der „Defense In Depth"-Ansatz, also, dass Schutzmechanismen auf verschiedenen Ebenen, rund um die Produktionssysteme diese absichern, vermutlich nicht mehr ausreichen. Stattdessen werden neue IT-Sicherheitsmechanismen und -konzepte direkt in den Produktions-/Automatisierungssystemen notwendig.

Fallbeispiel grenzüberschreitende Logistik-Prozesse

In der Verpackungsindustrie (hier konkret: Wellpappenherstellung und -verarbeitung) herrscht ein extrem hoher Kostendruck, der dazu führt, dass Produktion und Logistik in hohem Maße durchautomatisiert sind.

I4.0-Relevanz: Diese Querschnittsindustrie nimmt für Unternehmen von der Lebensmittelindustrie bis zum Maschinenbau eine wichtige Rolle bei der Optimierung von deren Logistikprozessen ein.

Bei den hierbei zwischen Unternehmen auch grenzüberschreitend ausgetauschten Daten lassen sich bei Verletzung der Vertraulichkeit sensitive Informationen z. B. über die geschäftliche Situation der Kunden (Auslastung), Kostenstrukturen, geplante Marketing-Kampagnen oder Kunden gewinnen. Zudem kann bei Verletzung der Datenintegrität ein hoher Schaden bei Hersteller oder beim Kunden z. B. durch verfälschte Stückzahlen oder verfälschtes Timing (Folgen wäre z. B. Blockierungen des Produktionsprozesses durch leere Verpackungsmateriallager bzw. Vergeudung von Ressourcen durch Überproduktion), irreführende Auszeichnung beim Bedrucken der Verpackungen oder unnötige Transportkosten entstehen.

Identifizierte Risiken und Herausforderungen

Obwohl die Vision I4.0 bisher in noch keinem Unternehmen voll verwirklicht ist, können zukünftige Szenarien basierend auf existierenden Publikationen zu I4.0 in Richtung weiter zunehmender Vernetzung über Länder-, Standort-, und Unternehmensgrenzen, zunehmender autonomer Abläufe in Produktion und Logistik und zunehmender Verfügbarkeit von großen und teils sensitiven Datenbeständen „extrapoliert" werden.

Schon die Ausgangssituation für I4.0, der aktuelle Zustand der Industrie 3.x, weist erhebliche Defizite in der IT-Sicherheit auf. Es muss daher bei allen weiteren Betrachtungen immer im Auge behalten werden, dass für die Lösung von durch I4.0 neu entstehenden Herausforderungen, Bedrohungen und Risiken zunächst ein sicheres Fundament durch die Adressierung dieser bereits existierenden Probleme erforderlich ist.

Für I4.0 werden sich nun aber, wie in den Fallbeispielen in der Langfassung der Studie illustriert wird, zusätzliche Herausforderungen ergeben, die in der gegenwärtigen Situation noch gänzlich unbekannt sind.

Es sind im Wesentlichen drei Eigenschaften der I4.0, aus denen neue, zentrale Herausforderungen im Kontext der IT-Sicherheit entstehen:

1. Die Vernetzung von Industrieanlagen und deren Komponenten wird künftig nicht nur organisations- und jurisdiktionsübergreifender, sondern vor allem auch dynamischer stattfinden als bisher. Die konkreten Teilnehmer an einem IT-Prozess in einer I4.0-Wertschöpfungskette sind nicht mehr im Voraus fest planbar. Um die IT-Sicherheit in einem solchen Szenario zu gewährleisten, muss eine belastbare Grundlage von Vertrauen und Verlässlichkeit geschaffen werden, die sich über alle Teilnehmer der Wertschöpfungskette erstreckt. Die Herstellung solcher Vertrauensbeziehungen kann nicht erst in dem Moment in Angriff genommen werden, indem sich aufgrund dynamischer Abläufe eine neue Kommu-

nikationsbeziehung über Unternehmens- und Ländergrenzen hinweg ergibt. Die Herausforderung besteht hier vor allem in der Definition von Mindestsicherheitsstandards, denen alle potentiellen Teilnehmer an den I4.0-Prozessen genügen müssen, beziehungsweise zu deren Einhaltung diese sich verbindlich verpflichten. Da diese Standards für Teilnehmer jeder Größe, also auch für KMU, mit zumutbarem Aufwand umsetzbar sein müssen und ihre Einhaltung nachweisbar sein muss, ergibt sich als weitere Herausforderung, hier auf internationaler Ebene ein schlankes, auf das Wesentliche beschränkte Rahmenwerk aus technischen und organisatorischen Maßnahmen zu konzipieren, das diesen Zweck erfüllt.

2. Die Menge an Daten, die von einem Teilnehmer einem anderen Teilnehmer aus funktionalen Gründen absichtlich mitgeteilt oder zugänglich gemacht werden, nimmt zu. Darunter befinden sich insbesondere auch solche Daten, die nicht nur aus Sicht eines einzelnen Unternehmens als Geschäftsgeheimnis gelten, sondern an die aufgrund staatlicher Gesetze eine besonders hohe Anforderung an die Vertraulichkeit besteht (z. B. Schutz von Personendaten). Verschärfend kommt hinzu, dass derjenige, der solche Daten anderen bereitstellt, oft nicht wissen kann, wer die Teilnehmer im weiteren Verlauf der Wertschöpfungskette genau sein werden, denen diese Daten bekannt gegeben werden müssen, um ihre Funktion in einem I4.0-Prozess zu erfüllen. Jeder Teilnehmer trägt damit nicht nur eine Verantwortung für die Sicherheit seiner eigenen Daten, sondern auch für die Sicherheit der Daten seiner Prozesspartner. Umgekehrt muss jeder Teilnehmer darauf vertrauen können, dass Daten, die er im Verlauf von I4.0-Prozessen im Rahmen eines Wertschöpfungsnetzwerkes seinen Kommunikationspartnern überlässt, von diesen angemessen geschützt werden.

3. Entscheidungen werden bei I4.0 zunehmend autonom von Maschinen (das heißt von Software-Programmen) getroffen. Diese Entscheidungen und die daraus resultierenden Änderungen von Abläufen und Teilnehmer-Konfigurationen können sich aufgrund von Ereignissen aus unterschiedlichsten Domänen und Partnersystemen ergeben sowie aus der Analyse von Daten aus unterschiedlichsten Quellen. Erfolgsentscheidend für diesen Aspekt von I4.0 ist sowohl die Integrität als auch die Authentizität der verwendeten Daten und Datenquellen.

Eine detaillierte Diskussion der identifizierten Risiken und Herausforderungen findet sich in den Kapiteln 4.3 bis 4.5 des Abschlussberichtes.

5 Handlungsmöglichkeiten heute und zentrale Hemmnisse

Die Analyse des Standes der Technik hinsichtlich der betrachteten technischen Sicherheitsmaßnahmenpakete[7] hat ergeben, dass diese grundsätzlich einen guten Basisschutz im Kontext von I4.0 bilden können. Dieser Basisschutz ist jedoch nach entsprechender Risikoanalyse immer in Abhängigkeit von der jeweiligen Sicherheitsarchitektur zu betrachten und umzusetzen. Die Analyse hat auch ergeben, dass viele Hindernisse bei der Umsetzung einzelner Maßnahmen auftreten können, die eine Eignung in bestimmten Teilaspekten in Frage stellen. Die Gründe für diese Hindernisse sind vielfältig. Sie beginnen bei einer durch etablierte Vorgehens- und Denkweisen schwierigen Einführung von Patchmanagement und dem Management von digitalen Identitäten und deren Authentifizierung und enden bei einer gewollten Höherpriorisierung von Verfügbarkeitsanforderungen aufgrund von Safety-Gesichtspunkten, da integrierte Ansätze hinsichtlich Safety und Security fehlen. Spezifische Produkte sind für bestimmte Maßnahmen wie bspw. Firewalls und Whitelisting vorhanden. Für einige Maßnahmen gibt es jedoch derzeit weder entsprechende am Markt verfügbaren Produkte noch vollumfängliche Konzepte, sondern oft nur in Projekten für bestimmte Umgebungen und Kunden geschaffene Speziallösungen. Es wurden die entsprechenden Aspekte und Felder identifiziert in denen Bedarf an der Förderung von Produktisierung vorhandener Konzepte oder Erarbeitung neuer Konzepte besteht. Details zu den Analysen finden sich in Kapitel 5.1 des Abschlussberichtes.

Es hat sich auch gezeigt, dass viele der organisatorischen Sicherheitsmaßnahmen, die heute für das industrielle Umfeld empfohlen und dort auch vielfach bereits umgesetzt sind, sich auch für I4.0 eignen. Es ist allerdings zu beachten, dass durch die Überwindung von Unternehmensgrenzen zahlreiche neue Schnittstellen entstehen und neue Prozesse benötigt werden. Diese müssen jeweils einzeln für sich und für ihre Auswirkungen auf andere Prozesse hin untersucht werden, um geeignete organisatorische Maßnahmen vornehmen zu können. Die Gefahren, die von einer fehlenden oder mangelhaften Umsetzung der Maßnahmen ausgehen, sind im I4.0-Kontext allerdings als deutlich größer einzuschätzen, zumal es mehr Akteure im Wertschöpfungsnetzwerk gibt und zwischen diesen eine wesentlich größeren Menge an sensiblen Daten ausgetauscht wird. Siehe hierzu auch die Kapitel 5.2.1 und 5.3 des Abschlussberichtes.

Aus der rechtlichen Perspektive ist deutlich geworden, dass die Fragestellungen, die derzeit in der juristischen Literatur vermehrt betrachtet werden (v. a. Datenschutz), nur teilweise die faktischen Probleme der KMU bei der Umsetzung von I4.0 betreffen: Vordringlich sind hier strukturelle Maßnahmen im Rechtsraum nötig, um Unsicherheiten über konkrete Anforderungen zu beseitigen, wirksame Durchsetzungsmechanismen zu schaffen, zu einer einheitlichen Vertragspraxis zu gelangen und Standards und Zertifikate zu etablieren auf deren Basis die Unternehmen ihre Leistungen anbieten und weiterentwickeln können. Detailanalysen finden sich in den Kapiteln 5.2.2 und 5.4 des Abschlussberichtes.

7 Aufgrund der Bedrohungssituation als relevant eingeschätzte Sicherheitsmaßnahmenpakete, basierend auf relevanten Standards und Rahmenwerken: Inbetriebnahme in sicherer Konfiguration, Fernwartung, Absicherung von Feldgeräten und Netzen, Datensicherung, Schutz vor Schadsoftware, Härtung, Patchmanagement, Authentisierung, Zugriffskontrolle, Protokollierung/Auswertung und mobile Datenträger.

6 Vorhandene und neue Konzepte und Standards

Technische Aspekte

Bezüglich der Anforderungen an den Schutz der Konstruktions- und Fabrikationsdaten sind die notwendigen Basistechnologien verfügbar. Allerdings stehen der Übertragung auf die Produktion einige bisher ungelöste Fragestellungen entgegen. Beispielsweise ist noch ungeklärt, wie Verfügbarkeitsansprüche der Produktion mit den bestehenden IT-Sicherheitskonzepten verbunden werden können. Hier besteht dringender Forschungs- und Entwicklungsbedarf. Darüber hinaus gestalten sich der Aufbau und der Betrieb z. B. einer PKI auch in der Verwaltungs-IT nicht immer einfach. Hier müssen Konzepte und Lösungen erarbeitet werden, wie diese Methoden auf Produktionsumgebungen abgebildet werden können.

Ähnlich sieht es im Bereich der hardware-basierten Vertrauensanker für Produktionssysteme – digitale Identitäten – aus. Auch hier existieren bereits Produkte, die prinzipiell Lösungsansätze zur Verfügung stellen. Allerdings müssen auch noch Fragestellungen der Skalierbarkeit solcher Systeme und der Kosten für die zusätzliche Hardware beantwortet werden. Möglicherweise bieten Weiterentwicklungen, wie z. B. TPM 2.0[8], mehr Freiheitsgrade in Bezug auf die Integration der Funktionen auf bestehende digitale Bausteine der Maschine. Diese Entwicklungen sollten gefördert und als Ziel entsprechend in mögliche Forschungsprogramme aufgenommen werden.

Die Fragestellung nach einer Methode zur kontinuierlichen Sicherheitsüberwachung von Produktionssystemen steht allerdings eher am Anfang. Zurzeit sind keine anwendbaren Konzepte bekannt. Erfahrungen aus dem Bereich der Intrusion Detection im Zusammenhang mit Big Data Analytics Know-how lassen es denkbar erscheinen, dass die Erkennung von IT-Sicherheitsvorfällen durch Auswertung von Aktuatorik- und Sensorik-Daten möglich sein könnte. Allerdings fehlen hier zzt. sowohl der wissenschaftliche Beweis, als auch die technische Erprobung im Produktionsumfeld.

Bezüglich der fortschreitenden Konvergenz von Safety und Security liegen die Notwendigkeiten auf der Hand. Hier ist allerdings festzustellen, dass Safety ein bereits gut erfasster und entsprechend regulierter Bereich ist, bei dem allen Akteuren die Sicherheitsableitungen nicht schwer fallen. Die IT-Sicherheit zählt – im Gegensatz zu z. B. Safety – momentan zu den deregulierten Bereichen. Es gibt kaum gesetzliche Vorgaben oder verbindliche Standards für die Industrie, nach denen man sich ausrichten kann. Daher fällt es allen Akteuren sehr schwer angemessene IT-Sicherheitsmaßnahmen zu identifizieren. Dies wird im Kapitel 6.3 des Abschlussberichtes entsprechend beleuchtet und bewertet. Zudem ist Stand heute noch nicht in vollem Umfang erkennbar, welche Wechselwirkungen Safety auf Security und umgekehrt erzeugen wird. Klar ist, dass Probleme in einem Bereich mit hoher Wahrscheinlichkeit Auswirkungen im anderen Bereich generieren werden. Daher besteht auch hier erhöhter Forschungsbedarf für die Integrationskonzepte und das Management der möglichen Wechselwirkungen. Siehe Kapitel 6.1 des Abschlussberichtes.

Organisatorische Aspekte

Mit dem Konzept von I4.0 entstehen vielfältige Herausforderungen gerade für KMU. Nicht wenige davon betreffen die IT-Sicherheit und fast alle erfordern den Aufbau spezieller Kompetenzen. Da es für KMU weder möglich noch sinnvoll ist, alle geforderten Kompetenzen selbst aufzubauen, werden sie in einigen Bereichen auf Dienstleister zurückgreifen müssen. Da diese vor allem im Bereich der IT-Sicherheit nur unterstützen, nicht aber die Verantwortung abnehmen können sind KMU gefordert, sich selbst eine umfassende Strategie zu erarbeiten und das Unternehmen auf allen Ebenen auf die I4.0-Herausforderungen vorzubereiten.

Wie in Kapitel 6.2 des Abschlussberichtes erläutert ist ein guter Ansatzpunkt dazu der Rückgriff auf Erfahrungsberichte, Best-Practice-Sammlungen und Handlungsleitfäden. Diese sind nicht nur für Betreiber von Produktionsanlagen relevant, sondern auch für Dienstleister die Unternehmen auf dem Weg zu einer hochgradig vernetzten und automatisierten industriellen Produktion begleiten möchten.

Ein weiterer zentraler Punkt aus organisatorischer Sicht ist das Vorantreiben der Standardisierung. Bei einer in die Zukunft gerichteten Initiative wie I4.0 ist die Standardisierung keine Festschreibung von Technologien, die sich in

8 Trusted Platform Module Library Specification, Family „2.0“, https://www.trustedcomputinggroup.org/resources/tpm_library_specification, abgerufen am 14.12.2015.

der Praxis bewährt und am Markt durchgesetzt haben, sondern eine kooperative und durchaus konzeptionelle Arbeit zwischen Industrie, Forschungseinrichtungen und Verbänden. Dabei sollten, insbesondere beim Thema IT-Sicherheit, auch die Belange der KMU explizit einbezogen werden, um die Anwendbarkeit der Standards auch für diesen Kreis zu gewährleisten.

In die Zukunft gerichtete Standardisierung sollte als Kooperationsprojekt verstanden und strukturiert werden. Förderpolitische Anreize sind notwendig, um

- der einseitigen Durchsetzung von proprietären Technologien zu begegnen,
- KMUs zu motivieren, sich auch an der Standardisierung zu beteiligen,
- eine Vertretung auf internationaler Ebene gewährleisten zu können, auch durch Vertreter von Forschungseinrichtungen.

Zu beachten ist, dass die IT-Sicherheits-Standards umsetzbar und mit verhältnismäßigem Aufwand überprüfbar bleiben müssen – nur so kann vermieden werden, dass bestimmte Unternehmen von der Teilnahme an der I4.0 ausgeschlossen werden. Darüber hinaus ist eine Abstimmung auf internationaler Ebene wichtig. Der Einsatz von Standardprodukten, wie auch die Umsetzung von standardisierten Strukturen und Prozessen, bietet ein höheres Maß an Sicherheit für strategische Entscheidungen. Im Zusammenhang mit Mindeststandards geht es in erster Linie um die zweckmäßige Integration und Anwendung bestehender Standards. Die Analyse und Bewertung der vorhandenen und in Entwicklung befindlichen Normen und Standards in Kapitel 6.4 des Abschlussberichtes hat ergeben, dass

- Im Rahmen der Arbeiten zu einem I4.0-Referenzmodell eine Strukturierung des Themas IT-Sicherheit vorgenommen werden und damit die Klassifikation der notwendigen IT-Sicherheits-Standardisierungsarbeiten erfolgen sollte. Eine erste Übersicht dazu kann aus der Deutschen Normungs-Roadmap IT-Sicherheit[9] des DKE entnommen werden.
- Zahlreiche IT-Sicherheits-Standards sind auch auf den Bereich der industriellen Produktion übertragbar, bedürfen allerdings der Fokussierung auf das Zusammenspiel von IT-Sicherheitsanforderungen und Schutzzielen mit anderen nicht-funktionalen Anforderungen wie Ausfallsicherheit, Echtzeit und Verfügbarkeit.
- Eine belastbare Bewertung der Relevanz bestehender technischer IT-Sicherheitsstandards für den Bereich industrielle Produktion/I4.0 ist erst möglich anhand der Struktur und den ausgewählten Technologien von I4.0-Referenzarchitekturen.
- Eine mögliche I4.0-Referenzarchitektur auf der Basis von IEC/TR 62541-2 OPC Unified Architecture (OPC UA)[10] bringt auf der technischen Ebene eine Reihe von bestehenden IT-Sicherheitsstandards aus den Internet-Standardisierungsgremien (OASIS, IETF, W3C) mit sich. Deren Angemessenheit für die industrielle Produktion ist individuell abzuprüfen hinsichtlich der jeweiligen Sicherheitsanforderungen und Schutzziele aus einem Informationssicherheits-Managementsystem (ISMS)-Prozess. Eine allgemeine Bewertung des möglichen Schutzniveaus von OPC UA wird seit Januar 2015 vom BSI untersucht. Die Spezifikationsanalyse wurde abgeschlossen und es wurden keine systematischen Fehler in der Spezifikation gefunden. Es handelt sich daher um ein gutes Beispiel für „Security by Design“. Offene Punkte (z. B. im Bereich der Kryptographischen Verfahren), die sich durch die lange Lebensdauer der Spezifikationen ergeben werden, sollen in Zukunft verbessert werden. Zusätzlich sollen Vorgaben und Empfehlungen für Nutzer von OPC UA im Rahmen des Projektes erarbeitet und veröffentlicht werden.

Um die wesentliche Rolle des Menschen im Konzept von I4.0 und vor allem die damit einhergehende Verantwortung für Informationen und Prozesse zu gestalten, bedarf es multidisziplinärer Schulungsmaßnahmen, geeigneter Assistenzsysteme und sinnvollerweise auch des Einsatzes von Promotoren, die die Änderungen im Unternehmen begleiten und positiv verstärken.

9 Koordinierungsstelle IT-Sicherheit im DIN (KITS): Normungsroadmap IT Sicherheit, Version 2.0, 12/2014, https://www.dke.de/de/std/documents/rm%20it%20sec%20-v2.pdf, abgerufen am 16.07.2015.

10 IEC TR 62541-2:2010 OPC Unified Architecture - Part 2: Security Model, https://webstore.iec.ch/publication/7174, abgerufen am 16.07.2015.

Begleitend können positive Erfahrungsberichte aus anderen Unternehmen und Branchen den Prozess der Vertrauensbildung unterstützen. Eine schrittweise Einführung innerhalb des Unternehmens macht die Entwicklung besser nachvollziehbar und hilft Hemmschwellen und Widerstände abzubauen.

Zusammenfassend lässt sich festhalten, dass IT-Sicherheit im Umfeld von I4.0 auch organisatorischer Maßnahmen bedarf, die in ihrer Gesamtheit am ehesten zu erfassen sind, wenn der bevorstehende Wandel als zentrales Innovationsthema im Unternehmen betrachtet und aus allen Perspektiven gleichrangig angegangen wird.

Rechtliche Aspekte

Wie in Kapitel 6.3 des Abschlussberichtes erläutert wurden zwei aktuelle Ansätze zur Weiterentwicklung des rechtlichen Rahmens für IT-Sicherheit untersucht. Das IT-Sicherheitsgesetz gibt Impulse für die Entwicklung der IT-Sicherheitsregulierung, indem etwa eine breitflächige gesetzliche Pflicht zur IT-Sicherheit ausgesprochen wird (§ 13 Abs. 7 TMG neu) und indem im Teilbereich „kritische Infrastrukturen“ Instrumente wie Aufsichtsbefugnisse für IT-Sicherheit und die Entwicklung von Branchenstandards für IT-Sicherheit erprobt werden können. Die allgemeine Norm (§ 13 TMG) ist jedoch sehr unbestimmt, die übrigen Regeln gelten nur für wenige Unternehmen. Nicht zuletzt wegen der Lückenhaftigkeit und Unbestimmtheit zeigt das IT-Sicherheitsgesetz im Bereich I4.0 den Bedarf an einer Weiterentwicklung des rechtlichen Rahmens für IT-Sicherheit deutlich auf.

Im Bereich der Zertifizierung zeigt sich derzeit im Bereich des Datenschutzes eine hochinteressante Entwicklung, die Potenzial auch für die allgemeine IT-Sicherheit besitzt: Die auf einer gesetzlichen Regelung beruhende Zertifizierung von IT-Sicherheit und insbesondere die Herausbildung von transparenten, öffentlichen Standards für IT-Sicherheit sind geeignet, eine Verbesserung von IT-Sicherheit in der Fläche zu erreichen. Auch insoweit fehlt es derzeit aber an einem tragfähigen Konzept, sodass auch hier erhebliche Anstrengungen erforderlich sind. Die Nutzung der Erkenntnisse aus der Datenschutz-Zertifizierung könnte hier aber einen guten Einstieg bilden.

Feststellung: Dringender Handlungsbedarf

All diese Fragestellungen müssen dringend adressiert werden und bedürfen unmittelbarer Unterstützung seitens der politischen Entscheider, sei es durch weitere FuE-Förderungen, gesetzliche Regelungen oder flankierenden Maßnahmen zur Akzeptanz in der Wirtschaft und Bevölkerung.

7 Regulatorische Maßnahmen und erforderliche Diskurse

Die Untersuchung des gegenwärtigen Zustands der rechtlichen Regulierung von IT-Sicherheitsanforderungen hat Defizite gezeigt, die für I4.0 besonders relevant sind:

- Die Konkretisierung allgemeiner rechtlicher Anforderungen (§ 823 BGB, ProdHaftG etc.) durch die Rechtsprechung ist in Bezug auf technische Sicherheitsanforderungen nur eingeschränkt geeignet und vor allem wegen der Verfahrensdauer bis zu höchstrichterlichen Entscheidungen angesichts der rasanten technischen Entwicklung zu schwerfällig.

- Behördliche Aufsichts- und Konkretisierungsbefugnisse bestehen für einen Großteil der I4.0 nicht.

- Eine allgemein anerkannte Vertragspraxis (Musterklauseln und -verträge) hat sich in Bezug auf Sicherheitsanforderungen in der I4.0 noch nicht entwickelt.

- Die rechtliche Bedeutung technischer Standards ist unklar. Insbesondere fehlt es an einer klaren Bezugnahme rechtlicher Anforderungen zu konkretisierenden Standards.

Die bestehenden Defizite sollten durch regulatorische Maßnahmen des Gesetzgebers, aber auch durch Eigeninitiative der Wirtschaft, beseitigt werden. Dies setzt jedoch hinreichende Kenntnis und übereinstimmende Auffassung über die geeigneten Instrumente voraus, die derzeit nicht gegeben ist. Daher sind fachliche Vorarbeiten zum Thema „rechtliche Regulierung von IT-Sicherheit“ und ein Diskurs zwischen Wissenschaft, Praxis und Gesetzgeber erforderlich.

Ein wesentlicher Aspekt betrifft das Mittel der Regulierung. IT-Sicherheitsanforderungen können durch zahlreiche rechtliche Mittel adressiert werden. Im Vordergrund stehen behördliche Aufsicht einerseits, Haftung und Selbstregulierung andererseits. Insbesondere besteht Unklarheit, wie technische Standards mit rechtlichen Anforderungen verbunden werden können. Diese Aspekte müssen vor einem Eingreifen des Gesetzgebers fachlich diskutiert werden.

In dem notwendigen Diskurs sind die divergierenden Interessen abzuwägen. Ein beachtliches Interesse ist dabei die Erhaltung von Flexibilität und Fortschritt. Soweit rechtliche Regulierung von IT-Sicherheit abgelehnt wird, besteht oft die Befürchtung, starre Vorgaben könnten technischen Fortschritt verhindern. Dies muss verhindert werden.

Besonderes Gewicht muss dabei aber dem Interesse an Rechtsklarheit zukommen. Rechtsklarheit auch hinsichtlich der gebotenen IT-Sicherheit ist insbesondere für KMU eine vitale Notwendigkeit, da ansonsten Rechtsberatungskosten entstehen, die zwar von großen Unternehmen getragen werden können, für KMU aber erdrückend wären.

Gesetzgeberische Maßnahmen betreffen insbesondere die flächendeckende Einführung verbindlicher Pflichten zu IT-Sicherheit mit einer klaren Bezugnahme zu technischen Standards sowie ggf. Aufsichtsbefugnisse des BSI. Neue Modelle wie Anreize, etwa Haftungsprivilegierung bei Einhaltung von Standards, sind zu erwägen. Geeignete Verfahren zur Verbindlichkeit technischer Standards sind zu etablieren.

Auf der Ebene der Praxis sind breitflächig Standards, ggf. mit branchenspezifischen Besonderheiten, mit Bezug zur Sicherheit in der I4.0 zu etablieren. Es sollten Musterverträge und -klauseln zur Kooperation in der I4.0 und den IT-sicherheitsbezogenen Pflichten der Beteiligten entwickelt werden.

8 Interessenslagen, Positionen und Konflikte

Interessenslagen und Konflikte hinsichtlich Normierung, Standardisierung und Regulierung von IT-Sicherheit

Bei der Normierung und Standardisierung von Vorgehensweisen und Technologien ist auch die Frage der Vermittlung und Akzeptanz von IT-Sicherheit von Bedeutung. Umfrageergebnisse (wie z. B. der jährlich im Auftrag der Freudenberg IT erhobene IT Innovation Readiness Index von Pierre Audoin Consultants (PAC), vgl. http://www.freudenberg-it.com/de/it-innovation-readiness-index-2015) zeichnen hierzu ein etwas widersprüchliches Bild. Während beim Mittelstand die Skepsis gegenüber Datensicherheit mit sieben bis acht Prozent eher gering ausgeprägt ist und mit 25 Prozent eher Rechtsunsicherheiten im Vordergrund stehen, sind für 94 Prozent der Automotive-Unternehmen Cloud-Lösungen wegen der befürchteten Datenunsicherheit und Spionagerisiken nicht einsetzbar. Allerdings sind solche Erhebungen mit Vorsicht zu genießen, da nur allgemeine Begriffe ohne Bezug zu Anwendungsfällen abgefragt werden. Normen und Regulierung der IT-Sicherheit können daher als Unterstützung oder Gängelung betrachtet werden. Sie sollten daher als konstruktiver Beitrag zu einer Risikomanagement-Strategie eines Unternehmens angesehen und „vermarktet" werden, wobei ein Grundschutz als Mindestbeitrag sichergestellt werden muss. Hier sollte auf die Unternehmensgröße, auch bezüglich Zertifizierung, Rücksicht genommen werden. Während KMUs IT-Sicherheitsstandards (und sei es auch nur ein standardisierter Prozess) als hilfreich ansehen, da dadurch die zusätzlichen Investitions- und Personalkosten gesenkt und „Standard-Lösungen" eingesetzt werden können, haben größere Unternehmen das finanzielle und personelle Potenzial, um unternehmensspezifische IT-Sicherheitslösungen eigenständig nach definierten Standard-Rahmenbedingungen zu erarbeiten.

Unterschiedliche Positionen involvierter Unternehmen

Die über den Beirat beteiligten Unternehmen haben sowohl Unterstützung als auch Kritik an den erarbeiteten Handlungsvorschlägen[11] eingebracht. Dies hat insbesondere deutlich gemacht, dass die Interessenslagen im Themenbereich IT-Sicherheit besonders zwischen KMU und Großunternehmen oftmals unterschiedlich sind, da unterschiedliche Positionen insbesondere bei den Punkten Standardisierung/Normierung und Regulierung eingenommen werden, woraus sich zukünftig Konflikte bei der Umsetzung von Handlungsvorschlägen ergeben werden. Da der „Enabler" IT-Sicherheit jedoch nur dann zum Tragen kommt, wenn die damit verbundenen Ziele gemeinsam von allen Partnern eines Wertschöpfungsnetzwerkes, egal ob groß oder klein, verfolgt werden, wird sich kein von I4.0 zukünftig partizipieren wollendes Unternehmen dem notwendigen Diskurs entziehen können. Große Industrieunternehmen bestätigten auf der einen Seite, dass die zusammengestellten Handlungsmöglichkeiten und -vorschläge im Bereich der IT-Sicherheitsregulierung (vgl. Kapitel 7.2 des Abschlussberichtes) durchaus sinnvoll sind. Auf der anderen Seite existiert gleichzeitig die Kritik, dass mehr Regulierung („IT-Sicherheitsgesetz II", vgl. Kapitel 7.4.1.2.1 des Abschlussberichtes) nicht erwünscht ist.

Von Seiten der involvierten KMU wurde keinerlei derartige Kritik laut und die erarbeiteten Handlungsvorschläge ernteten durchweg positives Feedback.

Mehrheiten lassen sich durch die geringe Anzahl beteiligter Organisationen nicht direkt ableiten. Wie bereits in Kapitel 7 beschrieben, sind im notwendigen Diskurs die divergierenden Interessen der Betroffenen abzuwägen. Diese können im Hinblick auf Großunternehmen und KMU durchaus sehr stark voneinander abweichen, z. B. im Punkt Rechtsklarheit und den damit verbundenen Kosten.

11 In einer früheren Entwurfsfassung des Abschlussberichtes. Anregungen und Kritikpunkte wurden in die vorliegende Endfassung des Abschlussberichtes einbezogen.

9 Handlungsvorschläge

Zusammen mit der abschließenden Bewertung von Standards und Normen komplettieren die vorgestellten technischen, organisatorischen und rechtlichen Konzepte die notwendige Basis für die Entwicklung von Handlungsvorschlägen. Aufbauend auf den identifizierten Herausforderungen, den Risiken und Bedrohungen sowie den verfügbaren IT-Sicherheitskonzepten wurden konkrete Handlungsvorschläge formuliert. Diese Vorschläge sollen den Anwendern und der Politik dabei helfen, für konkrete Szenarien zu erkennen, an welchen Stellen Handlungsbedarf besteht. Zudem sollen sie bei der Identifizierung und Etablierung von Maßnahmen unterstützen, um vorhandenen Risiken und Bedrohungen sowie rechtlichen und organisatorischen Hemmnissen zu begegnen (vgl. auch Kapitel 7.4 des Abschlussberichtes).

Eine Vielzahl von Handlungsvorschlägen muss kurzfristig[12] im Zeitraum von wenigen Jahren angegangen werden. Hier sind sowohl die Wirtschafts-, Technologie- und Förderpolitik, Standardisierungsorganisationen als auch die Unternehmen selbst gefragt, welche in vielen Bereichen eng zusammenarbeiten müssen oder voneinander abhängig sind. Aus diesem Grund sind die nun folgenden Handlungsempfehlungen gemäß ihrer primären Zielgruppe sortiert, d. h. für Entscheider in

- Unternehmen und Branchenverbänden (Kapitel 9.1),
- Politik / Gesetzgeber und Aufsichts- und Regulierungsbehörden (Wirtschafts-, Technologie- und Förderpolitik) (Kapitel 9.2)
- und Standardisierungs- und Normierungsorganisationen (Kapitel 9.3).

Innerhalb der Zielgruppe wird unterschieden zwischen betrieblich-organisatorischen, rechtlichen und technischen Handlungsempfehlungen. Zudem findet eine Kategorisierung statt, die in den jeweiligen Unterabschnitten erläutert wird.

9.1 Unternehmen und Branchenverbände

Ausgehend von den vorliegenden Erkenntnissen werden nachfolgend entsprechende Handlungsvorschläge formuliert die sich an Unternehmen richten und primär Industrieunternehmen/KMU als Anwender von I4.0 betreffen. Diese teilen sich auf in betrieblich-organisatorische, rechtliche und technische Handlungsvorschläge.

Es erfolgt eine Zuordnung der betrieblich-organisatorischen Vorschläge zu den Kategorien Technikintegration, Rolle des Menschen und Vertrauen in die Technik, Kooperationspartner und Potenzial der Vision von I4.0. Die rechtlichen Handlungsvorschläge fallen unter die Kategorien Rechtsgestaltung und Vertragsmuster. Ausgehend von den vorgestellten technischen Konzepten (s. Kap. 6) werden die technischen Handlungsvorschläge in den Kategorien Safety & Security, Industrial Rights Management, Integritätsprüfungen und hardwarebasierte Sicherheitsanker, Maintenance und Management von Industriekomponenten, Schlüsselverwaltung für digitale Verschlüsselung sowie Production Line IT-Security Monitoring formuliert.

Im Hinblick auf die betroffenen Unternehmen und Branchenverbände gilt, dass die Umsetzung aller organisatorischen und technischen Handlungsvorschläge sofort angegangen werden sollte. Einige der rechtlichen Handlungsvorschläge können von KMU bereits umgesetzt werden, andere sollten umgesetzt werden, sobald entsprechende Muster durch Branchenverbände unter Beteiligung der Aufsichtsbehörden entwickelt worden sind.

Diese Kategorisierungen der Handlungsvorschläge spiegeln sich in der folgenden Tabelle 9-1:

12 Die vorgeschlagenen Umsetzungszeithorizonte der Handlungsvorschläge unterscheiden sich nach kurzfristig (ein bis zwei Jahre), mittelfristig (drei bis fünf Jahre) und langfristig (sechs bis zehn Jahre).

Tabelle 9-1: Priorisierte Handlungsvorschläge für Unternehmen und Branchenverbände mit Zuordnung zu Disziplinen und Kategorien

Handlungsvorschlag	Disziplin	Kategorie
Top-down-Förderung von Vertrauen in das Konzept und die Vision von I4.0	betrieblich-organisatorisch	Vertrauen
Musterverträge zur Kooperation und Sicherheitsanforderungen	rechtlich	Rechtsgestaltung
Integrierte Methodik für Safety & Security	technisch	Safety & Security
Verschlüsselung sensibler Daten	technisch	Industrial Rights Management
Hinterfragen etablierter Strukturen und Prozesse im Rahmen des Risikomanagements	betrieblich-organisatorisch	Technikintegration
Musterdatenschutzklauseln und -einwilligungen	rechtlich	Rechtsgestaltung
Integritätsprüfungen	technisch	Integritätsprüfungen und hardwarebasierte Sicherheitsanker
Orientierung an Erfahrungsberichten, Best-Practices und Handlungsleitfäden	betrieblich-organisatorisch	Technikintegration
Muster-Non-Disclosure-Agreements	rechtlich	Rechtsgestaltung
Verwendung hardware-basierter Sicherheitsanker	technisch	Integritätsprüfungen und hardwarebasierte Sicherheitsanker
Umsetzung bewährter organisatorischer IT-Sicherheitsmaßnahmen	betrieblich-organisatorisch	Technikintegration
Entwicklung von Komponenten mit Secure Plug & Work Fähigkeiten	technisch	Safety & Security
Einsatz von Assistenzsystemen zur Entlastung von Mitarbeitern	betrieblich-organisatorisch	Rolle des Menschen
Aufbau von Public-Key-Infrastrukturen oder Single-Sign-On	technisch	Schlüsselverwaltung für digitale Verschlüsselung
Einsatz von Promotoren zur Förderung von Änderungsprozessen	betrieblich-organisatorisch	Rolle des Menschen
Entwicklung von Anomalie-Erkennungssystemen	technisch	Production Line IT-Security Monitoring
Durchführung einer gezielten Personalentwicklung	betrieblich-organisatorisch	Rolle des Menschen
Durchführung von Pilotprojekten in einem etablierten Umfeld	betrieblich-organisatorisch	Vertrauen

9.1.1 Betrieblich-organisatorisch

Technikintegration

Wie bereits erwähnt, stehen Unternehmen bisher weitestgehend alleine auf ihrem Weg zu einer vernetzten und automatisierten industriellen Produktion da und agieren demensprechend zögerlich. Mangelnde Erfahrung und fehlende Vorhersehbarkeit von Entwicklungen hat häufig Ad-hoc-Maßnahmen und Improvisation zur Folge, wie im Fallbeispiel Automobilbau (s. Kap. 4.1.1) beschrieben. Dies macht die Entwicklung und Einhaltung von Richtlinien und Verfahren, die zur Gewährleistung der IT-Sicherheit notwendig sind, schwierig. Prozesse auf Basis von Versuch und Irrtum lassen sich nur schwer mit der Gewährleistung eines bestimmten IT-Sicherheitsniveaus vereinbaren.

1) HINTERFRAGEN ETABLIERTER STRUKTUREN UND PROZESSE IM RAHMEN DES RISIKOMANAGEMENTS

Vorschlag: Die Bedeutung der integrierten Abschätzung von technischen, rechtlichen und organisatorischen Folgen der Integration neuer Techniken in bestehende Prozesse kann von Unternehmen nicht hoch genug eingeschätzt werden. Einerseits müssen in der industriellen Produktion etablierte Praktiken auf ihre Eignung für die I4.0 und andererseits neue technische Entwicklungen auf ihr Nutzen-Risiko-Verhältnis hin überprüft werden. Es muss klar sein, dass die I4.0 nicht nur mit Vorteilen verbunden sein kann, sondern an einigen Stellen auch Nachteile in Kauf genommen werden müssen.

Begründung: Bei der zunehmenden Vernetzung und Automatisierung der industriellen Produktion kommt das Bewusstsein für die sich durch Technikintegration verändernde Bedrohungslage leicht zu kurz. Einerseits werden etablierte Praktiken nur selten auf ihre Angemessenheit hin überprüft und andererseits werden neue technische Entwicklungen ohne eingehende Prüfung des Nutzen-Risiko-Verhältnisses in bestehende Prozesse integriert. Eine Sensibilisierung der Unternehmen und der einzelnen Mitarbeiter muss kurzfristig realisiert werden, da das Potenzial für Angriffe bereits besteht. Der Prozess zur Analyse und Anpassung gefährdeter Strukturen und Datenflüsse muss unverzüglich angestoßen werden (s. Kap. 6.2.1).

Details: Kapitel 7.4.2.1.1 des Abschlussberichtes.

2) ORIENTIERUNG AN ERFAHRUNGSBERICHTEN, BEST PRACTICES UND HANDLUNGSLEITFÄDEN

Vorschlag: Nutzung von Erfahrungsberichten (Success-Stories), Best-Practices und Handlungsleitfäden anderer Unternehmen, Forschungseinrichtungen und/oder Verbände.

Begründung: Während einige Unternehmen oder Industriezweige bereits auf eine lange Erfahrung mit einer überdurchschnittlich stark vernetzten und automatisierten industriellen Produktion zurückblicken können, stehen andere noch am Anfang. Von einem intensiven Erfahrungsaustausch, vor allem im Bereich der IT-Sicherheit, würden alle Beteiligten profitieren, da die Wahrscheinlichkeit von Zwischenfällen reduziert und das Vertrauen in die Industrie insgesamt gesteigert werden würde (s. Kap. 5.2.1). Im Hinblick auf IT-Sicherheit können diese Mittel Hilfestellungen zu Richtlinien und Verfahren, Methoden und Werkzeugen sowie zu Schulungen und Sensibilisierungsmaßnahmen geben. Unternehmen können bereits kurzfristig mithilfe von Erfahrungsberichten, Best-Practice-Sammlungen und Handlungsleitfäden in ihrer schrittweisen aber kontinuierlichen Annäherung an das Konzept I4.0 bestärkt werden und von Entwicklungen in anderen Unternehmen oder Industriezweigen profitieren. Eine Sammlung und Aufbereitung von Erfahrungsberichten, Best-Practice-Sammlungen und Handlungsleitfäden und eine zentrale Bereitstellung muss unmittelbar begonnen werden, damit die Unternehmen eine konkrete Vorstellung von den Chancen und Risiken bekommen und damit eine fundierte Investitionsentscheidung hinsichtlich verschiedener Technologien treffen können. Andernfalls ist zu befürchten, dass das Interesse an I4.0 mangels verfügbarer Erfahrungswerte abschwächt und die Unternehmen den technologischen Anschluss verpassen.

Details: Kapitel 7.4.2.1.2 des Abschlussberichtes.

3) UMSETZUNG BEWÄHRTER ORGANISATORISCHER IT-SICHERHEITSMAßNAHMEN

Vorschlag: Orientierung an vorhandenen, teils auf die industrielle Produktion spezialisierten Leitfäden und Standards für die IT-Sicherheit.

Begründung: Die Grundprinzipien der IT-Sicherheit aus organisatorischer Sicht haben auch in der industriellen Produktion der Zukunft ihre Gültigkeit. Aufgrund der

zunehmenden Komplexität und Dynamik im Kontext von I4.0 nimmt die Bedeutung einer umfassenden Planung und transparenten Umsetzung von organisatorischen IT-Sicherheitsmaßnahmen allerdings zu. Solange noch keine I4.0-spezifischen Best-Practice-Sammlungen, Leitfäden und Standards existieren, die Fragen der IT-Sicherheit umfassend behandeln, sollten sich Unternehmen bei der Planung und Umsetzung organisatorischer IT-Sicherheitsmaßnahmen an vorhandenen, teils auf die industrielle Produktion spezialisierten Leitfäden und Standards für die IT-Sicherheit orientieren. Zusätzlich ist vor allem im Hinblick auf Richtlinien und Verfahren das Ergreifen von Maßnahmen ratsam, die die Einhaltung derselben sicherstellen. Angesichts der aktuell bestehenden Sicherheitslücken sollte dies unverzüglich geschehen. Die verfügbaren und dokumentierten Maßnahmen sollten mindestens so lange eingesetzt werden, bis die aktuell diskutierten Anpassungen umgesetzt werden. Eine iterative und kontinuierliche Übernahme der aktuellen Sicherheitsmaßnahmen muss eingeplant werden. Aktuell sollte z. B. unbedingt der IT-Grundschutzkatalog des BSI umgesetzt werden, selbst wenn dieser (noch) nicht auf I4.0-Spezifika eingeht. Da dieser kontinuierlich weiterentwickelt wird, haben die Unternehmen hier einen guten Anhaltspunkt.

Details: Kapitel 7.4.2.1.3 des Abschlussberichtes.

Rolle des Menschen

Die digitale Integration und Echtzeitsteuerung von Produktionsprozessen durch dezentrale Rechnereinheiten ermöglicht es zum einen, zukünftig auch mit An- und Ungelernten komplexere Tätigkeiten in der Produktion auszuführen (z. B. durch „geführte“ Arbeit mithilfe von Motion-Capture-Anzügen und Datenbrillen). Zum anderen wird der Bedarf an hoch qualifizierten Beschäftigten vor allem im IT-Bereich steigen, um das digitale Produktionssystem zu steuern, überwachen und anzupassen. Allerdings beruht ein Großteil der Innovationsstärke und Wettbewerbsfähigkeit deutscher Unternehmen auf der herausragenden Beherrschung technischer Herstellungsverfahren und Produktionsprozesse (z. B. Qualität, Flexibilität, Liefertreue) – s. Kap. 6.2.2 des Abschlussberichtes. Daher ist es dringend erforderlich, eine gezielte Personalentwicklung zu betreiben, so dass spezifische Kompetenzen und Erfahrungen auch im Rahmen von I4.0-Produktionssystemen zukünftig weiter genutzt und strategisch weiterentwickelt werden können.

4) EINSATZ VON PROMOTOREN ZUR FÖRDERUNG VON ÄNDERUNGSPROZESSEN

Vorschlag: Unternehmen sollten die Neuausrichtung als Chance sehen und den Mitarbeitern auch so vermitteln. In der Praxis hat sich dazu in anderen Bereichen der Einsatz von Promotoren bewährt, die den Änderungsprozess aktiv und intensiv fördern. Auch ein Einsatz von Projektteams und gegebenenfalls einer Pilotumgebung bieten sich zur Überwindung möglicher Hemmnisse an.

Begründung: Es ist verständlich, wenn Menschen mit Unbehagen auf Veränderungen reagieren, weil diese mit dem Aufbrechen vertrauter Routinen und dadurch mit Unsicherheiten verbunden sind. Im Hinblick auf die IT-Sicherheit kann dieses Unbehagen zu menschlichem Fehlverhalten, vor allem bei der Umsetzung von Richtlinien und Verfahren, führen – in Extremfällen ist sogar denkbar, dass sich Mitarbeiter gegen das eigene Unternehmen wenden. Ein wichtiges Beispiel ist der Einsatz von Projektteams und gegebenenfalls einer Pilotumgebung, um möglichen Hemmnissen auf der Ebene der täglichen Routine praxisnah zu begegnen. Mittel- bis langfristig muss es Ziel sein, eine Innovationskultur im Unternehmen zu schaffen und zu fördern. Dieser langwierige Prozess muss so schnell wie möglich eingeleitet und dann weiterentwickelt werden. Der Zielzustand kann jedoch erst langfristig erreicht werden, s. Kap. 6.2.2.

Details: Kapitel 7.4.2.1.4 des Abschlussberichtes.

5) DURCHFÜHRUNG EINER GEZIELTEN PERSONALENTWICKLUNG

Vorschlag: Im Hinblick auf Schulungen sollten sich Unternehmen an multidisziplinären Maßnahmen auf Verbandsebene beteiligen. Diese könnten eine gute Möglichkeit bieten auch über Unternehmensgrenzen hinweg zu lernen – was vor allem für KMU hilfreich wäre.

Begründung: Der mit I4.0 einhergehende Wandel erfordert immer mehr Interdisziplinarität sowie die Arbeit in interprofessionellen Teams. Doch auch die zunehmenden Qualifizierungsbedarfe auf der fachlichen und methodischen Ebene dürfen nicht außer Acht gelassen werden (s. Kap 6.2.2). In solchen Maßnahmen sollte auch ein Bewusstsein für das notwendige Zusammenwirken von Recht, Organisation und Technik zur Gewährleistung eines angemessenen IT-Sicherheitsniveaus im Kontext von I4.0 vermittelt

werden. Ein Beispiel ist die gezielte Weiterbildung eines Maschinenführers hinsichtlich der IT-Einbindung und IT-gestützten Anlageneinrichtung sowie hinsichtlich der Vernetzungsmöglichkeiten mit Fremdanlagen oder -Systemen. Nur mit entsprechenden Kenntnissen kann der Mitarbeiter die Funktionsweise verstehen und sich im Falle von Displaymeldungen richtig verhalten. Unternehmen sind aktuell gefragt, Bedarfe zu definieren, so dass sich ein multidisziplinäres Qualifizierungsangebot am Markt entwickeln kann. Darauf aufbauend können Unternehmen dann gezielt Qualifizierungsmaßnahmen planen.

Details: Kapitel 7.4.2.1.5 des Abschlussberichtes.

6) EINSATZ VON ASSISTENZSYSTEMEN ZUR ENTLASTUNG VON MITARBEITERN

Vorschlag: Unternehmen sollten Assistenzsysteme einsetzen. Entsprechende Systeme können vor allem auch im Kontext der Umsetzung von organisatorischen IT-Sicherheitsmaßnahmen hilfreich sein. Gezielte Auswertungen von Ereignissen und kontinuierliche Verbesserungen führen im Idealfall zu lernenden Systemen, die im Zeitverlauf immer besser darin werden, den Menschen zu unterstützen.

Begründung: Der Wandel hin zu einer industriellen Produktion der Zukunft reduziert die monotonen Tätigkeiten für Mitarbeiter und erhöht damit die Anforderungen. Gleichzeitig steigt die Komplexität und Dynamik der Produktion im Allgemeinen. Noch existieren nur wenige Assistenzsysteme, die die Bediener von Maschinen und Anlagen sinnvoll unterstützen. Systeme wie z. B. interaktive 3D-Brillen (Stichwort google glasses) befinden sich im Produktionsumfeld in der Erprobungsphase. Diese Anforderung ist mittelfristig zu verstehen, da Assistenzsysteme erst entwickelt werden können, wenn die Prozesse ausgestaltet und umgesetzt sind.

Details: Kapitel 7.4.2.1.6 des Abschlussberichtes.

Vertrauen

Im Hinblick auf das Vertrauen in die I4.0 besteht vor allem bei KMU die Angst vor einem möglichen Kontrollverlust durch die zunehmende Vernetzung und Automatisierung der Produktion.

Beispiel: Der Teilezulieferer befürchtet z. B. als Lieferant ersetzbar zu werden, sobald er seine Baupläne und Fertigungskapazitäten offen legt. Zudem steht die Befürchtung im Raum, über die Informationsebene zusätzlich angreifbar im Rahmen der Industriespionage zu sein.

7) TOP-DOWN-FÖRDERUNG VON VERTRAUEN IN DAS KONZEPT UND DIE VISION VON I4.0

Vorschlag: Etablierung eines offenen top-down-Prozesses zur Vertrauensbildung unter den Mitarbeitern. Ein Ansatz Vertrauen zu schaffen besteht darin den Wandel als zentrales Innovationsthema im Unternehmen zu verstehen und auch so zu kommunizieren. Positive Erfahrungsberichte aus anderen Unternehmen und Industriezweigen können den Prozess der Vertrauensbildung unterstützen. Eine schrittweise Einführung innerhalb des Unternehmens macht die Entwicklung besser nachvollziehbar und hilft Hemmnisse und Widerstände abzubauen. Der Prozess kann durch den Aufbau von Systemvertrauen, zum Beispiel durch den Einsatz von zertifizierten Produkten und Prozessen, zusätzlich unterstützt werden.

Begründung: Unternehmen fällt es mitunter schwer, grundlegendes Vertrauen in das Konzept oder die Vision von I4.0 zu schaffen. Wie eine Veränderung wie der Wandel hin zur industriellen Produktion der Zukunft in einem Unternehmen wahrgenommen wird hängt unter anderem von der Geschwindigkeit der Veränderung und der Nachvollziehbarkeit der Maßnahmen ab. Im Hinblick auf die I4.0 ist wichtig, dass Möglichkeiten zum Aufbau von Systemvertrauen gefunden werden. Das Thema „Schaffen einer Innovationskultur in Unternehmen“ ist ein mittel- bis langfristig anzusetzendes, was jedoch nicht bedeutet, dass es nicht unmittelbar gestartet werden sollte, s. Kap. 6.2.3.

Details: Kapitel 7.4.2.1.7 des Abschlussberichtes.

8) DURCHFÜHRUNG VON PILOTPROJEKTEN IN EINEM ETABLIERTEN UMFELD

Vorschlag: Unternehmen sollten gezielt bestehende Kooperationen nutzen, um I4.0-Pilotprojekte in einem etablierten Umfeld zu testen und um die Kooperationen zu vertiefen.

Begründung: Häufig fehlt es Unternehmen an einem geeigneten Umfeld, um erste Erfahrungen mit einem neuen technischen Entwicklungen zu sammeln. Vor allem KMU sind auf unbekanntem Terrain sehr zögerlich, da der betriebliche Alltag kaum Raum für Versuch und Irrtum lässt. Ein Unternehmen wird die neuen Risiken offener

angehen, wenn es sie im bekannten Umfeld erproben kann, wie z. B. im Rahmen von bestehenden Kooperationen mit Entwicklungspartnern, Lieferanten oder Kunden, bestenfalls noch bei gleichgewichtigen Risikoanteilen bzw. in einer abgeschotteten Testumgebung. Diese Pilotprojekte sind kurzfristig anzugehen, da so die Unternehmen kurzfristig Erfahrungen sammeln können.

Details: Kapitel 7.4.2.1.8 des Abschlussberichtes.

9.1.2 Rechtlich

Rechtsgestaltung

Aufgrund unbestimmter oder nicht einschlägiger gesetzlicher Erlaubnisnormen stellen sich den Unternehmen Hindernisse bei der Erhebung und Weitergabe von personenbezogenen Daten in I4.0 Strukturen. Weder die derzeitige Gesetzeslage noch die geplante Datenschutzgrundverordnung in ihrer bislang erörterten Form schaffen in diesem Umfeld ausreichende Rechtsklarheit, sodass Unternehmen mit nicht unerheblichen Rechtswidrigkeitsrisiken konfrontiert sind.

Beispiel: Kundendaten. Entscheidet sich der Käufer eines PKW für eine Individuallackierung muss die die individuelle Farbcodierung zwischen den beteiligten Rechnern und intelligenten Lackierrobotern im I4.0-Umfeld des Automobilherstellers ausgetauscht werden. Eine Anonymisierung wird nur schwerlich zu erreichen sein, denn damit das Fahrzeug mit dem individuellen Farbcode mit dem Abschluss der Lackierung dem richtigen Kunden zugeordnet werden kann, müssen Farbcode und Kunde mit einem Zuordnungsmerkmal verknüpft werden. Besonders kritisch wird es, wenn diese Daten grenzüberschreitend an einen Standort oder Kooperationspartner außerhalb des Europäischen Wirtschaftsraumes übermittelt werden müssen.

Die Rechtsunsicherheiten können durch eigene rechtsgestaltende Instrumente wie Einwilligungen der Personen, auf die sich die Daten beziehen, und vertragliche Regelungen mit den Kooperationspartnern reduziert werden. Gerade KMU sind dabei jedoch auf entsprechende Vorlagen und Muster angewiesen, die auf die typische Ausgestaltung für I4.0 Strukturen zugeschnitten sein müssen. Diese können nur durch Branchenverbände in Abstimmung mit den Regulierungsbehörden ausgearbeitet werden.

Auch in Bezug auf den Schutz von Betriebs- und Geschäftsgeheimnissen können Rechtsunsicherheiten bei der Vertragsgestaltung durch entsprechende Muster von Verbänden reduziert werden.

9) MUSTERVERTRÄGE ZUR KOOPERATION UND SICHERHEITSANFORDERUNGEN

Vorschlag: KMU sollten – soweit möglich – auf Musterklauseln und -verträge zurückgreifen. Diese sollten durch Verbände, etwa durch Branchenverbände, erarbeitet werden. Ideal wäre ist, einen Grundbestand einheitlicher Regeln zu schaffen, der für alle Branchen gilt, und diese durch branchenspezifische Besonderheiten zu ergänzen

Begründung: Musterverträge oder -klauseln zur Kooperation in der I4.0 sind bisher kaum verbreitet. Dies hat zur Folge, dass keine einheitlichen Anforderungen an sicherheitsbezogene Pflichten der Beteiligten und technische Anforderungen bestehen. Insbesondere Betreiber von Produktionsanlagen und Dienstleister mit Fokus auf die I4.0 sollten diese innerhalb von Branchenverbänden erarbeiten. Eine Ausarbeitung von Mustern für KMU ist lediglich mittelfristig zu erwarten, da dies einen Abstimmungsprozess erfordert und divergierende Interessen zu berücksichtigen sind.

Details: Kapitel 7.4.2.2.1 des Abschlussberichtes.

10) MUSTERDATENSCHUTZKLAUSELN UND -EINWILLIGUNGEN

Vorschlag: KMU sollten – soweit möglich – auf Musterklauseln und -einwilligungen zurückgreifen. Insbesondere im Bereich des Datenschutzes müssten diese jedoch von Branchenverbänden in Kooperation mit den Datenschutzaufsichtsbehörden zunächst entwickelt werden. Auch sollten KMU von Zertifizierungen und Datenschutzsiegel Gebrauch machen, sobald die rechtlichen Grundlagen durch die Politik geschaffen worden sind.[13]

Begründung[14]: Datenschutzbezogene Musterklauseln und -einwilligungen finden kaum Anwendung, was jedoch

13 Vgl. Handlungsvorschlag in Ziffer 0. Dies ist eine notwendige Vorstufe, die zunächst umzusetzen wäre.

14 Vgl. insbesondere Kapitel 4.4.4 und 5.2.2.1.1 des Abschlussberichtes.

auch darin begründet liegt, dass derzeit keine auf I4.0 zugeschnittenen Muster existieren. Diese müssten zudem durch die Regulierungsbehörden auch anerkannt sein. Hierzu bedarf es Anstrengungen der Branchenverbände entsprechende Muster in Abstimmung mit den Regulierungsbehörden zu erarbeiten. Aufgrund des Abstimmungsprozesses ist hier jedoch von einem mittelfristigen Zeitrahmen auszugehen. Mit einer Umsetzung der rechtlichen Rahmenbedingungen zu Zertifizierungen und einem Datenschutzsiegel ist allenfalls langfristig zu rechnen.

Bei dieser Empfehlung besteht eine Abhängigkeit zum Handlungsvorschlag „Musterklauseln und Mustereinwilligungen für I4.0 hinsichtlich Datenschutz und Betriebs- und Geschäftsgeheimnisse“, sehen Sie hierzu Kapitel 7.4.1.2.5 des Abschlussberichtes.

Details: Die Thematik wird insgesamt in Kapitel 7.4.2.2.2 des Abschlussberichtes erörtert.

11) MUSTER-NON-DISCLOSURE-AGREEMENTS

Vorschlag: KMU sollten auf Non-Disclosure-Agreements zurückgreifen. Auch hier können Branchenverbände entsprechende Muster schaffen, auf die KMU sodann zurückgreifen sollten.

Begründung[15]: KMU machen nicht immer von der Möglichkeit von Non-Disclosure-Agreements Gebrauch. Auf spezifische I4.0-Anwendungen zugeschnittene Muster stehen, soweit ersichtlich, nicht zur Verfügung. Insbesondere Betreiber von Produktionsanlagen und Dienstleister mit Fokus auf die I4.0 sollten diese innerhalb von Branchenverbänden erarbeiten. Dies sollte kurzfristig möglich sein, da Muster-NDA für unterschiedliche I4.0-Anwendungen von den betroffenen Branchen zeitnah entwickelt werden können.

Details: Kapitel 7.4.2.2.3 des Abschlussberichtes.

9.1.3 Technisch

Safety & Security

Zukünftig müssen die Themenbereiche Safety und IT-Security gemeinsam betrachtet werden. Eine integrierte Methodik muss dabei die Sicherheit beider Bereiche gewährleisten. Diese Methodik muss zum einen sicherstellen, dass IT-Security Probleme nicht den Zugriff auf Produktionskomponenten eröffnen. Zum anderen muss der gewünschte und erlaubte Zugriff auf diese Komponenten so organisiert werden, dass hier keine Optionen eröffnet werden, die IT-Systeme zu manipulieren. Hier gibt es zzt. weder Aktivitäten, eine integrierte Sicht zu erzeugen, noch sind Best-Practice-Ansätze für diesen Einsatzzweck verfügbar. Allerdings können diese Ansätze möglicherweise mit vertretbaren Aufwenden aus den aktuellen Prozessen und Technologien abgeleitet werden.

Beispiel: Durch Beschädigung eines IT-Systems in der Produktion mit Schadsoftware verhält sich das System nicht mehr seiner Spezifikation entsprechend. Möglicherweise bewegen sich mechanische Komponenten wie Roboterarme schneller als zulässig. Hier erzeugt ein IT-Sicherheitsvorfall ein mögliches Safety-Risiko. Es könnte zu einer mechanischen Havarie kommen und Teile des Systems können Menschen gefährden.

Im Normalfall ist dieses Risiko jedoch durch weitere Maßnahmen beschränkt, wie z. B. die Absicherung solcher Systeme durch räumliche Abtrennung. Auch der Zugang zu diesen Räumen wird heute mit Aktuatorik und Sensorik organisiert, die an IT-Systeme angeschlossen sind. Daher kann diese Absicherung in I4.0 nicht mehr als ausreichend angesehen werden.

12) INTEGRIERTE METHODIK FÜR SAFETY & SECURITY

Vorschlag: Entwicklung einer integrierten Methodik (Prozesse und Standards) für den Entwurf flexibel vernetzter, zugleich Security- und Safety-kritischer Systeme.

Begründung[16]: Zukünftig müssen moderne, teiloffene Produktionssysteme (cyber-physische Produktionssysteme) umfassend abgesichert werden, um unbefugten Zugriff (im Sinne von Security) zu unterbinden und gefahrbringende

15 Vgl. insbesondere Kapitel 4.4.6 des Abschlussberichtes.

16 Vgl. insbesondere Kapitel 6.1.4 des Abschlussberichtes.

Betriebszustände (im Sinne von Safety) abzuwenden. In den Fallbeispielen Automobilbau und Chemische Industrie finden sich bereits Hinweise auf eine Sensibilisierung der Branchen für solche Wechselwirkungen. Unternehmen als Anwender von I4.0 können, unterstützt durch die Wissenschaft (Forschung/Entwicklung von Sicherheitstechnologie für I4.0), dies kurzfristig umsetzen, da Best Practice Guidelines im Gegensatz zur Standardisierung schnell erarbeitet werden können. Im Idealzustand liegen integrierte Standards (siehe 9.3) vor wenn die integrierte Methodik umgesetzt wird.

Details: Kapitel 7.4.2.3.1 des Abschlussberichtes.

Industrial Rights Management

Selbst wenn die Forderung nach Verschlüsselung sensibler Daten zunächst nicht industrie-4.0-spezifisch erscheint, ist es doch als absolutes Neuland für die industrielle Produktion einzustufen. Daher erscheint es dringend geboten, die zzt. verfügbaren Technologien auf ihren Einsatznutzen hin bezüglich I4.0 zu analysieren, zu bewerten und an entsprechenden Stellen auch einzusetzen.

Dies ist auch bis zu einem gewissen Grad schon heute technologisch umsetzbar, auch wenn die meisten Produktionskomponenten dafür jetzt noch nicht geeignet erscheinen. Zukünftig muss Verschlüsselung als Option wählbar sein und vorhandene Systeme müssen einer Prüfung in Bezug auf ihre optionale Ertüchtigung unterzogen werden.

Beispiel: Im I4.0 Szenario ist es durchaus denkbar, dass ein Produzent von Produkten selber gar nicht über die notwendige Produktionsinfrastruktur verfügt. Der Vision nach kann das Produkt mit bestehenden Produktionssystemen gefertigt werden, indem diese über die Web-Infrastruktur gesteuert werden. In diesem Fall würden alle Intellectual Property-Werte des Produzenten auf nicht firmeneigenen Produktionssystemen verarbeitet werden.

In diesem Fall ist es ganz besonders wichtig, dass diese Daten so gehalten und verarbeitet werden, dass nur die Eigentümer dieser Daten Zugriff haben oder Zugriff erlauben können.

13) VERSCHLÜSSELUNG SENSIBLER DATEN

Vorschlag: Bei der Planung und Entwicklung neuer Komponenten, Systeme und Anlagen sollte, wo immer möglich, eine Verschlüsselung von sensiblen Daten vorgesehen werden.

Begründung[17]**:** Durch die Auswahl und den Einsatz verschlüsselungsfähiger Protokolle oder auch Datenformate, die eine strukturerhaltende Verschlüsselung ermöglichen (z. B. XML Encryption), können sensible Daten, wie z. B. Produktions- und Fabrikationsdaten, mittels symmetrischer und asymmetrischer Kryptografie geschützt werden. Hersteller von Produktionsanlagen und Komponenten sollten dies kurzfristig umsetzen, da diese Maßnahmen unmittelbar in laufende Entwicklungen einfließen sollten. Hindernisse existieren in Form von harten Verfügbarkeits-, Echtzeit- und Safety-Anforderungen, welche es im Einzelfall abzuwägen gilt.

Details: Kapitel 7.4.2.3.2 des Abschlussberichtes.

Integritätsprüfungen und hardwarebasierte Sicherheitsanker

Jede Verschlüsselungstechnologie ist nur so gut wie die Organisation der Schlüssel es zulässt. Das beste Schloss in der sichersten Tür mit dem perfektesten Schlüssel bringt keine Sicherheit, wenn der Schlüssel erworben oder das Schloss ausgebaut werden kann. Hier müssen flankierende Maßnahmen die Integrität von „Schlüssel, Schloss und Tür“ gewährleisten.

Diese Möglichkeit der Prüfung der Integrität von Industriekomponenten ist daher unmittelbar empfehlenswert und wird auch die Integrität der Schlüssel ermöglichen, die im vorangegangenen Beispiel die Datensicherheit herbeiführen können. Im Produktionsumfeld können dies hardwarebasierte Sicherheitsanker sein. Diese lassen sich momentan bereits mittels sog. Trusted Computing Modulen (TPM) auf Produktionskomponenten aufbringen. Langfristig wird man hier technische Weiter- oder auch Neuentwicklungen benötigen.

Beispiel: In der I4.0 werden Maschinen viel autonomer miteinander interagieren als wir das heute erleben. Im Zusammenhang mit der bereits erwähnten Interaktion dieser Systeme auch über traditionelle Unternehmensgrenzen

17 Vgl. insbesondere die Kapitel 6.1.1 und 6.1.2 des Abschlussberichtes.

hinweg, entsteht durch die Verschränkung der Produktionsumgebungen eine als kritisch anzusehende Infrastruktur. Hier ist es daher besonders wichtig abzusichern, dass nur autorisierte und auch integre Produktionskomponenten miteinander interagieren. Daher ist eine kontinuierliche Integritätsprüfung aller am Produktionsprozess beteiligten Komponenten erforderlich. Diese Prüfung kann aber nur erfolgen, wenn die Identität und Integrität der Produktionskomponenten sichergestellt werden kann.

14) INTEGRITÄTSPRÜFUNGEN

Vorschlag: Hersteller sollten bei der Planung und Entwicklung neuer Komponenten, Systeme und Anlagen entsprechende Möglichkeiten zur Integritätsprüfung während der Boot- und Laufzeit sowie bei Instandhaltungsmaßnahmen vorsehen, so dass neue Komponenten bereits ab Werk die rudimentäre Fähigkeit besitzen, die Integrität ihrer eigenen Firmware, Anwendungen und Konfigurationsparameter zu prüfen.

Begründung: Die Integrität von Hard- und Softwarekomponenten ist eine wichtige Voraussetzung für eine sinnvolle Verwendung von Verschlüsselungstechnologien. Ein entsprechender Schutz könnte schon kurzfristig in Produkte integriert werden, da entsprechende Chips und Softwarelösungen bereits am Markt erhältlich sind.[18] Im Fallbeispiel „grenzüberschreitende Logistikprozesse“ wird als Folge einer Verletzung der Datenintegrität ein hoher Schaden bei Hersteller oder Kunden angeführt. Hindernisse bei der Einführung solcher Integritätsprüfungen existieren, wie auch bei der Verschlüsselung sensibler Daten, in Form von harten Verfügbarkeits-, Echtzeit- und Safety-Anforderungen, welche es im Einzelfall abzuwägen gilt.

Details: Kapitel 7.4.2.3.3 des Abschlussberichtes.

15) VERWENDUNG HARDWAREBASIERTER SICHERHEITSANKER

Vorschlag: Hersteller sollten bei der Planung und Entwicklung neuer Komponenten nach Möglichkeit immer ‚hardwarebasierte Sicherheitsanker‘ vorsehen, wie z. B. das in der Office-IT etablierte Trusted Platform Module (TPM). Neue Komponenten würden dann bereits mit geeigneten hardwarebasierten Sicherheitsankern ausgeliefert, so dass diese für zukünftige Software-Erweiterungen vorbereitet sind. Diese Sicherheitsanker müssen in ein sinnvolles Schlüsselmanagement integriert werden.

Begründung[19]: Hardware-Sicherheitsanker in allen Endgeräten stellen eine sinnvolle Basis für zukünftige Sicherheitskonzepte für Automatisierungskomponenten und Produktionsanlagen dar - ein sinnvolles Schlüsselmanagement vorausgesetzt. Da entsprechende Chips und Softwarelösungen bereits am Markt erhältlich sind, könnten Hardware-Sicherheitsanker schon kurzfristig in Produkte integriert werden. Hindernisse existieren lediglich seitens der Komponentenhersteller in Form von Kostendruck bei der Produktion.

Details: Kapitel 7.4.2.3.4 des Abschlussberichtes.

Maintenance und Management von Industriekomponenten

Im Kontext der zu erwartenden zunehmenden räumlichen Verteilung der Produktion in I4.0 kommt der sicheren Inbetriebnahme und auch dem sicheren Betrieb von Systemen und Komponenten in der Fläche eine viel größere Bedeutung zu als es gegenwärtig vorstellbar ist. Allein die Verteilung der Produktion wird eine Maintenance durch Personal vor Ort kaum umsetzbar erscheinen lassen. Hinzu kommt, dass die Anpassung der Systeme wesentlich agiler stattfinden wird. Hier ist eine Anpassung der digitalen Systeme an Plug-and-Play-Paradigmen, wie sie bereits aus der klassischen IT bekannt sind, direkt empfehlenswert.

Beispiel: Bereits heute kennt man das Paradigma, dass sog. Apps auf Systeme geladen werden können, die dann bestimmte Funktionalitäten der Hardware operationalisieren. Bestes Beispiel sind die Navigationsfunktionen vieler Mobilfunksysteme. Das Kartenmaterial, aktuelle Verkehrsdaten und die Routenlogik werden durch Daten aus dem Cloud-Umfeld dargestellt. Die Berechnungen der Routen erfolgt in der Cloud während deren Darstellung auf dem Gerät erfolgt.

Analog kann man den Secure-Plug-and-Work-Aspekt von Industriekomponenten organisieren. Die Hardware vor Ort wird durch webgestützte Systeme kontinuierlich aktualisiert. Neue Komponenten werden durch entsprechende Technologien schnell und sicher in Produktionsumgebungen eingeführt.

18 Vgl. insbesondere die Kapitel 6.1.1 und 6.1.2 des Abschlussberichtes.

19 Vgl. insbesondere die Kapitel 6.1.1 und 6.1.2 des Abschlussberichtes.

16) SECURE PLUG & WORK

Vorschlag: Entwicklung geeigneter Hardware- und Softwarekomponenten zur Umsetzung des Szenarios „Secure Plug & Work“ für Safety-kritische Systeme in der I4.0. Neu entwickelte Hard- und Softwarekomponenten sollen ein Höchstmaß an automatischer Konfigurations- und Rekonfigurations-Funktionalität im Sinne von Secure Plug & Work bieten.

Begründung: Eine flexible Automatisierung erfordert die Fähigkeit zur autonomen Rekonfiguration und Optimierung der Produktionsumgebung, ohne dabei Safety oder Security zu gefährden. Dies betrifft gleichermaßen KMU und Industrie als Anwender von I4.0. Mechanismen zur Selbstbeschreibung von Komponenten in Bezug auf Funktionalität, Identifizierung, sowie die Fähigkeit zum Selbstaufbau der Kommunikation und geregeltem Datenaustausch sind zwingende Voraussetzung, um zukünftig neue Komponenten, Maschinen oder Anlagen in komplexe Produktionssysteme effizient und sicher einbringen zu können. Entsprechende Umsetzungen sollten kurzfristig möglich sein, da nur Änderungen an der Software erforderlich sind.[20] Als Hindernisse bei der Umsetzung sind Widerstände seitens der Hersteller zu befürchten, hier auf herstellerübergreifende Standards zu setzen.

Details: Kapitel 7.4.2.3.5 des Abschlussberichtes.

Schlüsselverwaltung für digitale Verschlüsselung

Wie in dem Abschnitt Industrial Rights Management bereits erwähnt wurde, kommt der Verschlüsselung von Industriedaten immer größere Bedeutung zu. Hierzu werden nicht nur entsprechend sichere Schlüssel (z. B. hinreichende Schlüssellänge) auf integren (z. B. Tamper Resistance) Komponenten benötigt. Vielmehr muss insbesondere bei Verwendung kryptographischer Verfahren, wie z. B. asymmetrischer Verschlüsselungsmethoden mit zwei unterschiedlichen Schlüsseln, die Schlüsselverteilung und -verwaltung entsprechend sichergestellt werden.

Dazu gibt es bereits Best-Practice-Ansätze aus dem PKI-Umfeld. Auch wenn diese Technologie nicht I4.0-spezifisch ist, sollte es möglich sein, eine Zertifikatsinfrastruktur zur Verschlüsselung analog dieser Methode zu etablieren.

Beispiel: Maschinen bekommen, wie in Abschnitt hardwarebasierte Sicherheitsanker bereits beschrieben wurde, zukünftig digitale Identitäten. Damit erfüllen sie alle Voraussetzungen, um mittels der verfügbaren Technologie PKI Identitäts- und Verschlüsselungszertifikate zu verarbeiten. Die Verwaltung und Organisation dieser Schlüssel kann als Best-Practice-Ansatz aus der klassischen IT übernommen werden.

17) AUFBAU VON PUBLIC-KEY-INFRASTRUKTUR ODER SINGLE-SIGN-ON

Vorschlag: Ein möglicher Ansatz wäre die Bereitstellung entsprechender Infrastrukturen durch die Hersteller von Maschinen und Komponenten als Mehrwertdienst zu ihren Produkten. Diese würden dann bereits mit digitalen Identitäten ausgeliefert werden und so den Anwendern mittels geeigneter sicherer Verfahren Zugriff auf entsprechende Schlüssel und Zertifikate ermöglichen.

Begründung: Der Aufbau einer zukunftsfähigen Infrastruktur, wie z. B. einer Public-Key-Infrastruktur (PKI) oder eines M2M-fähigen Single-Sign-On (SSO) Systems, dient der Ausstellung von Zertifikaten/ Sicherheitstokens und Schlüsseln für Komponenten, Maschinen, Dienste und Personen. Mittelfristig kann eine solche Infrastruktur grundsätzlich eine mögliche und sinnvolle Basis für den sicheren Betrieb und Austausch von Daten zwischen Komponenten, Systemen und Anlagen auch über Unternehmensgrenzen hinweg darstellen.[21] Hindernisse können zum einen die Notwendigkeit sein, auch umfassende Änderungen an den bisherigen Prozessen vornehmen zu müssen. Zum anderen können mit dem Aufbau einer PKI je nach Größe und Zweck hohe Aufwände und Kosten verbunden sein. So müssen alle Parteien, die miteinander kommunizieren möchten, von derselben Zertifizierungsstelle erfasst oder die zertifizierenden Instanzen über eine Zertifikatskette verbunden sein.

Details: Kapitel 7.4.2.3.6 des Abschlussberichtes.

Production Line IT-Security Monitoring

Auch in einer Produktionsumgebung mit integren Komponenten, die verschlüsselte Daten halten und mittels eindeutiger Hardwareidentitäten sicher organsiert werden

20 Siehe auch Kapitel 3.1.5 des Abschlussberichtes.

21 Siehe auch Kapitel 6.1.1 des Abschlussberichtes.

können sind dennoch IT-Sicherheitsprobleme denkbar. Diese müssen zeitnah erkannt werden und auf ihre Ursachen zurückverfolgt werden können. Insbesondere an der Produktionslinie ist dabei ein Monitoring der gesamten Infrastruktur wünschenswert, die so organisiert ist, dass die Produktion nicht gestört oder verlangsamt wird. Hier ist zu empfehlen, auf der Basis von Datenauswertung und Mustererkennung IT-Sicherheitsvorfälle so früh wie möglich zu erfassen und Abwehrmaßnahmen zu ergreifen.

Beispiel: I4.0 fokussiert sehr auf die Auswertung aller Daten, die im und um den Produktionsprozess erzeugt werden. Hier werden schon jetzt Auswerteverfahren herangezogen, um die Performance zu steigern und die Störanfälligkeit zu verringern. Diese Daten können ebenfalls dahin gehend ausgewertet werden, dass die Erkennung auf IT-Sicherheitsaspekte hin ausgeweitet wird.

18) ENTWICKLUNG VON ANOMALIE-ERKENNUNGSSYSTEMEN

Vorschlag: Die Forschung und Entwicklung an intelligenten, kombinierten und adaptiven Anomalie-Erkennungssystemen, wie z. B. zur Erkennung von Eindringlingen (Intrusion Detection), sollte intensiviert werden. Neue Komponenten sollen mindestens alle sicherheitsrelevanten Ereignisse protokollieren und zum Zwecke einer späteren Auswertung bereitstellen. Intelligente, kombinierte und adaptive Anomalie-Erkennungssysteme sollen in Produktionsanlagen integrierbar und einsetzbar sein.

Begründung[22]: Um auch zukünftigen Sicherheitsrisiken nachhaltig zu entgegnen, sind neue, adaptive Verfahren notwendig, welche die IT-Systeme nicht isoliert betrachten, sondern zielgerichtet den Produktionsprozess selbst schützen. Es müssen neue Methoden gefunden werden, um die IT-Landschaft der Produktion im laufenden Betrieb einer Analyse und Absicherung zu unterziehen, ohne Ziele wie Echtzeitfähigkeit und Verfügbarkeit zu gefährden. Dazu müssen allerdings erst noch Forschung und anschließende Produktentwicklung sowie Evaluierung der Ergebnisse notwendig stattfinden. Mittelfristig aber könnten Hersteller und Betreiber von Produktionsanlagen und Komponenten schon mit derartigen Systemen einer Vielzahl heutiger und häufiger Probleme der Industrie begegnen, u. a.:

- Analyse und Bewertung von IT-Sicherheit in Produktionsanlagen bereits in der Planungsphase
- Kontinuierliche Überwachung einer Anlage im Betrieb, ohne direkt auf die Systeme physikalisch zugreifen zu müssen
- Berücksichtigung von Kontextinformationen und semantischem Bezug auf den IST-Zustand
- Bereitstellung eines Tools bspw. als Cloud-Dienst ermöglicht die dezentrale und zeitgleiche Überwachung mehrerer Standorte
- Protokollierung aller Ereignisse für die Einhaltung der ges. Compliance Auflagen

Details: Kapitel 7.4.2.3.7 des Abschlussberichtes.

9.2 Politik / Gesetzgeber und Aufsichts- und Regulierungsbehörden

Ausgehend von den vorliegenden Erkenntnissen werden nachfolgend entsprechende Handlungsvorschläge formuliert die sich primär an die Politik / den Gesetzgeber und somit vorrangig an die Förderpolitik, die Wirtschaftspolitik und Aufsichts- und Regulierungsbehörden richten.

Im Folgenden werden die in dieser Studie offenkundig gewordenen Feststellungen und Empfehlungen in den Bereichen betrieblich/organisatorisch (vgl. Kap. 7.2.2 des Abschlussberichtes) und Recht (vgl. Kap. 7.2.3 des Abschlussberichtes) mit den wesentlichsten Handlungsvorschlägen noch einmal verkürzt strukturiert dargestellt. Dies betrifft insbesondere Handlungsfelder zur Implementierung rechtlicher Rahmenbedingungen zur Technikintegration, Rolle des Menschen und Vertrauen (betrieblich-organisatorisch) sowie Zertifizierung von IT-Sicherheit, datenschutzrechtlicher Erlaubnisnormen, Vertragsmuster und sonstige Standardisierungsmöglichkeiten zur Schaffung von Rechtssicherheit und Gestaltungsunterstützung insbesondere für KMU (rechtlich).

Diese Kategorisierungen der Handlungsvorschläge spiegeln sich in der folgenden Tabelle 9-2:

22 Vgl. auch Kapitel 6.1.3 des Abschlussberichtes.

Tabelle 9-2: Priorisierte Handlungsvorschläge für Politik / Gesetzgeber und Regulierungsbehörden mit Zuordnung zu Disziplinen und Kategorien

Handlungsvorschlag	Disziplin	Kategorie
Einigung auf sinnvolle Vorgaben im Hinblick auf Strukturen und Prozesse (Mindeststandards)	betrieblich-organisatorisch	Technikintegration
Einheitliche rechtliche Pflichten zur IT-Sicherheit und prüffähige Standards	rechtlich	Rechtssicherheit
Förderung der Entwicklung von Bewertungs- und Entscheidungsunterstützungsmodellen	betrieblich-organisatorisch	Technikintegration
Rechtssicherheit durch datenschutzrechtliche Rechtsgrundlagen für Datenströme bei I4.0	rechtlich	Rechtssicherheit
Rechtlicher Rahmen für IT-Sicherheitszertifizierung	rechtlich	Rechtssicherheit
Konzeption geeigneter Aus- und Weiterbildungsangebote	betrieblich-organisatorisch	Rolle des Menschen
Ausbau behördlicher Kompetenzen und Kooperation im Bereich IT-Sicherheit	rechtlich	Rechtssicherheit
Bereitstellung einer Kommunikationsplattform zur Diskussion und Aufklärung mit Fokus auf KMU	betrieblich-organisatorisch	Vertrauen
Musterklauseln und Mustereinwilligungen für I4.0 hinsichtlich Haftung sowie Datenschutz und Betriebs- und Geschäftsgeheimnisse	rechtlich	Rechtsgestaltung
Erforschung von Maßnahmen zur Vermeidung von menschlichem Fehlverhalten im Kontext von Angriffen	betrieblich-organisatorisch	Rolle des Menschen
Orientierungsrahmen für angemessene technisch-organisatorische Maßnahmen durch Datenschutzsiegel	rechtlich	Rechtssicherheit
Herausarbeitung von Hindernissen, die durch (internationales) Exportrecht bei I4.0 gemeinhin entstehen können	rechtlich	Ermittlung von Hindernissen
Forschung und Konzeption zum Rechtsrahmen für IT-Sicherheit	rechtlich	Rechtssicherheit
Länderübergreifende einheitliche Schutzstandards in Bezug auf Geheimnisschutz[23]	rechtlich	Rechtssicherheit

23 Schutz von Betriebs- und Geschäftsgeheimnissen.

9.2.1 Betrieblich-organisatorisch

Technikintegration

Die Vision von I4.0 erweist sich als stark technologiegetrieben. Technische Entwicklungen der letzten Jahre haben die heutige Vision von I4.0 überhaupt erst entstehen lassen. Noch gibt es aber weder Standards noch „die I4.0-Technologie", so dass Unternehmen bisher weitestgehend alleine auf ihrem Weg zu einer vernetzten und automatisierten industriellen Produktion sind (s. Kap. 6.2).

19) EINIGUNG AUF SINNVOLLE VORGABEN IM HINBLICK AUF STRUKTUREN UND PROZESSE (MINDESTSTANDARDS)

Vorschlag: In Abstimmung mit der Industrie sollte die Entwicklung von I4.0-Mindeststandards durch entsprechende gesetzliche Rahmenbedingungen gefördert werden (Kapitel 7.1.1.1). Zu beachten ist bei der Festlegung der Mindeststandards, dass die Standards auch von KMU umsetzbar und mit verhältnismäßigem Aufwand überprüfbar sind. Darüber hinaus erscheint eine Abstimmung auf internationaler Ebene sinnvoll. Der Einsatz von Standardprodukten, wie auch die Umsetzung von standardisierten Strukturen und Prozessen, bietet ein höheres Maß an Sicherheit für strategische Entscheidungen.

Begründung: Neben technischen Standards ist Standardisierung auch im Zusammenhang mit organisatorischen Maßnahmen sinnvoll – vor allem auch im Kontext von organisatorischen IT-Sicherheitsmaßnahmen. Unternehmen müssen sich darauf verlassen können, dass nicht nur aus technischer Sicht von kooperierenden Unternehmen Mindeststandards eingehalten werden, sondern auch im Hinblick auf Strukturen und Prozesse. Bereits begonnene Standardisierungsprozesse sollten von den Unternehmen und von der Politik unterstützt werden. Darüber hinaus sind bestehende Standardisierungslücken zu schließen (s.o. Kap. 6.2.1 und 7.1.1.1). Es sollte eine kurzfristige Umsetzung erfolgen mit dem Ziel, dass Unternehmen auf bestehende Standards zurückgreifen und von Insellösungen abkehren. Im Rahmen von Kooperations- oder Austauschbeziehungen sollte eine Einigung hinsichtlich der anzuwendenden Mindeststandards erfolgen, wie z. B. auf eine passende ISO/IEC Norm, die ebenfalls organisatorische Maßnahmenvorgaben enthalten.

Details: Kapitel 7.4.1.1.1 des Abschlussberichtes.

Rolle des Menschen

Während der Wandel hin zur I4.0 im Hinblick auf die Technikintegration als Evolution verstanden werden kann, kommt es im Hinblick auf die Rolle des Menschen tatsächlich zu etwas, was als Revolution bezeichnet werden könnte. Es kommt zu einem Aufbrechen von Routinen, zum Einbüßen von Privilegien oder Machtempfinden, zu Einschränkungen der erlebten Freiräume und damit zu Unsicherheiten.

Beispiel: Durch eine auf Basis von Algorithmen weitgehend autonom agierende Anlage wird der Anlagenführer in seinem „Machtgefüge" und in den tatsächlichen Möglichkeiten, in die Prozesse einzugreifen beschränkt. Diese Einschränkung des Handlungs- und Entscheidungsspielraums kann durchaus negativ wahrgenommen werden, so dass durch Nutzung der Kompetenzen an anderer Stelle einem Informationsverlust entgegengewirkt werden muss.

20) FÖRDERUNG DER ENTWICKLUNG VON BEWERTUNGS- UND ENTSCHEIDUNGS-UNTERSTÜTZUNGSMODELLEN

Vorschlag: Im Rahmen eines fokussierten Forschungsprogramms sollte die Entwicklung von an die Anforderungen der I4.0 angepassten Bewertungs- und Entscheidungsunterstützungsmodellen vorangetrieben werden. Die Modelle sollen das Treffen von fundierten und rationalen Entscheidungen im Zusammenhang mit organisatorischen IT-Sicherheitsmaßnahmen erleichtern.

Begründung: Entscheidungsunterstützung wird aufgrund der zunehmenden Komplexität und Dynamik im Zusammenhang mit vernetzter und automatisierter industrieller Produktion immer wichtiger. Die konkreten Faktoren, die bei Entscheidungen im Zusammenhang mit organisatorischen IT-Sicherheitsmaßnahmen herangezogen werden sollten, sind heute noch weitgehend unbekannt. Die zentrale Herausforderung besteht darin, dass bei organisatorischen Entscheidungen nicht nur die monetär direkt abbildbaren Faktoren, sondern auch die sogenannten „weichen" Faktoren entscheidend sind. Langfristig muss es daher das Ziel sein, Modelle und Tools zur Entscheidungsunterstützung verfügbar zu haben, die die komplexen Prozesse abbilden können. Das Aufsetzen und insbesondere die Durchführung eines Forschungsprogramms können der Natur nach nicht kurz- oder mittelfristig erfolgen.

Details: Kapitel 7.4.1.1.2 des Abschlussberichtes.

21) KONZEPTION GEEIGNETER AUS- UND WEITERBILDUNGSANGEBOTE

Vorschlag: In Abstimmung mit der Industrie sollten zunächst die Anforderungen an Mitarbeiter in der I4.0 erhoben und anschließend passende Aus- und Weiterbildungsangebote konzipiert werden. Dabei sollten sowohl die Anforderungen an Mitarbeiter, die mit dem Aufbau und der Betreuung der Produktionsumgebung betraut sind, als auch jene an Mitarbeiter die Anlagen bedienen oder überwachen berücksichtigt werden. Ziel ist u.a. eine Bewusstseinsschärfung auch für die IT-Sicherheitsrisiken.

Begründung: Der mit I4.0 einhergehende Wandel erfordert nicht nur immer mehr Interdisziplinarität und Arbeit in interprofessionellen Teams, sondern auch umfassendes fachliches und methodisches Wissen. Es mangelt an Aus- und Weiterbildungsangeboten, die die umfassenden Anforderungen der I4.0, insbesondere auch im Hinblick auf IT-Sicherheit, abdecken. Zudem gibt es im Bereich der Industrie einen gravierenden Mangel an ausgebildeten Fachkräften im Bereich IT-Sicherheit. Ohne diese Fachkräfte in den größeren Unternehmen wird ein Know-How-Transfer nicht gelingen. Mittelfristig muss sich der Markt für Qualifizierungsangebote erst entwickeln. Lehreinrichtungen müssen gefunden werden, die Aus- und Weiterbildung anbieten können und wollen. Im Zielzustand existiert dann ein breites Angebot an interdisziplinären Qualifizierungsmaßnahmen.

Details: Kapitel 7.4.1.1.3 des Abschlussberichtes.

22) ERFORSCHUNG VON MAßNAHMEN ZUR VERMEIDUNG VON MENSCHLICHEM FEHLVERHALTEN IM KONTEXT VON ANGRIFFEN

Vorschlag: Im Rahmen eines Forschungsprogramms sollte der Faktor Mensch im Rahmen der IT-Sicherheit in der I4.0 gezielt untersucht werden. Dabei sollte der Fokus auf der Entwicklung von Maßnahmen zur Abwehr möglicher Angriffe, die menschliches Fehlverhalten ausnützen oder gezielt auf Social Engineering setzen, liegen.

Begründung: Wie in vielen anderen Bereichen auch scheitert IT-Sicherheit im Kontext der I4.0 häufig am Faktor Mensch. Angreifer nutzen heute nicht nur Systemschwachstellen aus, sie setzen ebenso auf menschliches Fehlverhalten. Beispiele sind vorgetäuschte Anrufe des Softwareherstellers (Stichwort: Microsoft Systemservice, es soll ein Update eingespielt werden) oder eines scheinbaren Kunden, der ganz dringend Daten benötigt, die er gerade verlegt hat. Besonders in KMU ist das Sicherheitsbewusstsein oft nicht ausreichend ausgeprägt, wie zahlreiche Studien beweisen. Es gilt daher, langfristig die Rolle des Menschen innerhalb des Konzepts zu festigen, so dass zumindest keine zusätzlichen Sicherheitsrisiken von den Mitarbeitern ausgehen.

Details: Kapitel 7.4.1.1.4 des Abschlussberichtes.

Vertrauen

Vertrauen hängt sehr eng mit der Überzeugung zusammen, dass ein angemessenes IT-Sicherheitsniveau gewährleistet werden kann. Für den Erfolg der I4.0 ist nicht nur Vertrauen in die Vision selbst eine zwingende Voraussetzung, sondern auch Vertrauen in die Technik und in mögliche Kooperationspartner. Im Alltagsbereich bedeutet dies z.B., dass der Nutzer den Einparkassistenten seines PKW nicht nutzen wird, wenn er es dem System nicht zutraut, den Einparkvorgang autonom zu erledigen.

23) BEREITSTELLUNG EINER KOMMUNIKATIONSPLATTFORM ZUR DISKUSSION UND AUFKLÄRUNG MIT FOKUS AUF KMU

Vorschlag: Die Politik sollte unter Einbeziehung von Vertretern der Industrie, der Wissenschaft und der Gesellschaft eine Kommunikationsplattform für die breite Diskussion der industriellen Produktion der Zukunft bereitstellen und damit zu einer umfassenden Aufklärung über Potenziale und Gefahren der I4.0 beitragen.

Begründung: Grundlegendes Vertrauen in das Konzept oder die Vision von I4.0 kann zu einem gewissen Grad durch eine breite Diskussion und Aufklärung erreicht werden. Eine frühzeitige Erörterung von Bedenken und die Klärung von offenen Fragen sind für den Erfolg der I4.0 unerlässlich. Die bestehende „Plattform Industrie 4.0“[24] enthält kaum Möglichkeiten für KMU für einen schnellen oder kurzfristigen Austausch. Das Engagement im Rahmen einer Arbeitsgruppe o.ä. ist für viele KMU jedoch zu zeitaufwändig. Da es oftmals um den Bedarf einer konkreten Problemlösung geht, ist die Nutzung der bestehenden Plattform Industrie 4.0 für KMU nicht zielführend. Es

24 http://www.plattform-i40.de/

besteht die Notwendigkeit, eine solche Plattform kurzfristig bereitzustellen, da gerade jetzt die Unsicherheit bei KMU am größten ist und daher ein großer Bedarf besteht, sich auszutauschen und von den Erfahrungen anderer zu profitieren.

Details: Kapitel 7.4.1.1.5 des Abschlussberichtes.

9.2.2 Rechtlich

Rechtssicherheit durch Gesetzgebung, behördlich anerkannte Muster und Beobachtung der weiteren Entwicklung

Klare rechtliche Vorgaben zur IT-Sicherheit in der I4.0, die für hohes Schutzniveau notwendig sind, stehen nicht flächendeckend zur Verfügung. Das fehlende Vertrauen und die Angst vor möglichem Kontrollverlust werden nicht ausreichend von einem Rechtsrahmen zur IT-Sicherheit aufgefangen. Rechtliche Unsicherheiten bestehen insbesondere auch bei grenzüberschreitenden I4.0 Strukturen mit Blick auf den Geheimnisschutz (Schutz von Betriebs- und Geschäftsgeheimnissen), das Exportrecht und mit Blick auf die datenschutzrechtliche Zulässigkeit der Übermittlung personenbezogener Daten. Dabei stellen sich den Unternehmen insbesondere Fragen der rechtssicheren Ausgestaltung von Verträgen mit Partnern und Dienstleistern in Bezug auf Datenschutz sowie Betriebs- und Geschäftsgeheimnissen. Hieraus resultiert etwa ein Bedürfnis an Mustern, Rechtsgrundlagen und Standards, die die Netzstrukturen von I4.0 hinreichend berücksichtigen. Auch besteht ein Bedürfnis zur Schaffung klarer gesetzlicher Rahmenbedingungen.

Beispiel: Rechtliche Anforderungen an IT-Sicherheit. Ein KMU, das in eine I4.0-Struktur eingebunden ist, möchte wissen, welche konkreten technischen Maßnahmen erforderlich sind, um die rechtlichen Anforderungen an IT-Sicherheit und Datensicherheit zu erfüllen. Dies ergibt sich bisher weder aus Musterverträgen noch aus verbindlichen Sicherheitsstandards für I4.0. Das KMU benötigt daher aufwendige Beratung oder verzichtet auf die Einhaltung der Anforderungen.

Beispiel: Beschäftigtendaten. Ein für seinen Kontrollbereich verantwortlicher Mitarbeiter wird elektronisch auf dem Bauteil vermerkt, da nachvollziehbar bleiben soll, welcher Mitarbeiter welches Partners für welches Bauteil pro Herstellungsschritt verantwortlich ist, damit dieser leicht und schnell ermittelt und angesprochen werden kann. Dieser Mitarbeiter ließe sich ebenso anhand des Schichtbuches bei dem Partner, bei dem dieser beschäftigt ist, ermitteln. Dies allerdings scheuen die Partner in der Produktionskette, da eine Ermittlung anhand des Schichtbuchs eine längere Identifizierungszeit mit sich brächte. Gerade im Falle des Vorliegens von Schwierigkeiten, die ohnehin zu Produktionsverzögerungen führen können, ist eine schnelle Identifikationsmöglichkeit des jeweiligen Mitarbeiters aber von großer Bedeutung.

Der Vermerk eines Identifikationsmerkmals des Mitarbeiters auf dem Bauteil führt aber auch dazu, dass diese Daten mit dem Bauteil an Standorte oder Kooperationspartner außerhalb des Europäischen Wirtschaftsraumes weitergegeben werden können. Rechtsunsicherheit besteht derzeit in der elektronischen Erfassung dieser Beschäftigtendaten und deren (internationaler) Weitergabe an dritte Stellen. Einige Rechtsunsicherheiten lassen sich durch Musterklauseln reduzieren (etwa zur Etablierung eines angemessenes Datenschutzniveaus bei der Übermittlung außerhalb des Europäischen Wirtschaftsraumes). In anderen Fällen bedarf es jedoch ausdrücklicher gesetzlicher datenschutzrechtlicher Regelungen, insbesondere dort, wo Einwilligungen zur Legitimierung der Erhebung, Verarbeitung und Nutzung der Daten zweifelhaft erscheinen.

24) EINHEITLICHE RECHTLICHE PFLICHTEN ZUR IT-SICHERHEIT UND PRÜFFÄHIGE STANDARDS

Vorschlag: Die Bundesregierung sollte den Rechtsrahmen für I4.0 insbesondere im Hinblick auf IT-Sicherheit evaluieren. Darauf aufbauend sollten gesetzliche Maßnahmen zur IT-Sicherheit ergriffen werden, die auch auf I4.0 anwendbar sind. Die Entwicklung von Standards zur IT-Sicherheit sollte gefördert werden.

Begründung: Das IT-Sicherheitsgesetz adressiert neben Anbietern von Telemediendiensten vor allem Betreiber von „kritische Infrastrukturen“ und erscheint insgesamt ausbaufähig. Zudem fehlt es derzeit an ausreichenden Entwicklungen an Standards für konkrete Themen und Bereiche der I4.0.

Der Staat kann die Entwicklung von Standards fördern, wie dies etwa im Bereich der Standards für Datenschutz-Zertifizierung geschehen ist. Hier wurde im Rahmen des Trusted Cloud-Programms des BMWi ein prüffähiger Datenschutz-Standard für Cloud-Dienste, das Trusted Cloud-Datenschutzprofil für Cloud-Dienste (TCDP) erarbeitet. Das TCDP

ist insoweit besonders interessant, als es gesetzliche Anforderungen – hier des BDSG – in prüffähige Anforderungen umsetzt und zugleich auf dem ISO/IEC 27018-Standard und dem ISO/IEC 27002-Standard aufsetzt, wodurch international anerkannte Standards genutzt werden.

Diese Ziele könnten kurz- und mittelfristig erreicht werden. Das IT-Sicherheitsgesetz ist in Kraft getreten. Weitere legislative Maßnahmen sind jedoch nicht ausgeschlossen und werden bereits erwogen. Entsprechend sollte auf der Grundlage des fachlichen Diskurses und der Erfahrung mit dem IT-Sicherheitsgesetz eine Fortentwicklung erfolgen („IT-Sicherheitsgesetz II").

Details: Kapitel 7.4.1.2.1 des Abschlussberichtes.

25) RECHTSSICHERHEIT DURCH DATENSCHUTZRECHTLICHE RECHTSGRUNDLAGEN FÜR DATENSTRÖME BEI I4.0

Vorschlag: Die Bundesregierung sollte sich bei den Verhandlungen zur Europäischen Datenschutzgrundverordnung für die Schaffung klarer und rechtssicherer Erlaubnistatbestände einsetzen, auf die sich Unternehmen auch bei I4.0 Anwendungen stützen können. Soweit dem nationalen Gesetzgeber Spielräume verbleiben sollten, etwa in Bezug auf das Beschäftigtendatenschutzrecht, sollte der deutsche Gesetzgeber verhältnismäßige Erlaubnistatbestände bei der Verarbeitung von Beschäftigtendaten bei I4.0 Anwendungen schaffen. Die Datenschutzaufsichtsbehörden sollten im Dialog mit Branchenverbänden Standardvertragsklauseln entwerfen, die die Strukturen und Bedürfnisse der einzelnen I4.0 Konstellationen flexibel berücksichtigen und den multilateralen Abschluss durch mehrere Unternehmen vorsehen. Entsprechende Standardvertragsklauseln dürften insbesondere für KMU eine Erleichterung darstellen. Dabei sollten auch Vertreter wichtiger Handelspartner, wie etwa die Federal Trade Commission der USA, in die Beratungen mit eingebunden werden.

Begründung[25]: Die bisher gängigen datenschutzrechtlichen Erlaubnistatbestände sind zur Legitimation des Datenumgangs von und -austauschs zwischen den Partnern im Rahmen von I4.0 nur bedingt geeignet und unterliegen erheblichen Rechtsunsicherheiten. Neben Fragen nach allgemeinen Rechtsgrundlagen für die Datenverarbeitungen im Rahmen von I4.0 bestehen insbesondere Rechtsunsicherheiten bei der Übermittlung von Daten in unsichere Drittstaaten. Die von der EU-Kommission bisher entwickelten Standardvertragsklauseln sind nicht auf die Besonderheiten der I4.0 zugeschnitten und sehen etwa keinen multilateralen Abschluss vor. Die Bundesregierung sollte sich mittelfristig im Rahmen der Verhandlungen über die EU-Datenschutzgrundverordnung für entsprechende Erlaubnistatbestände einsetzen. Im Falle eines nationalen Spielraums sollte der deutsche Gesetzgeber ein Beschäftigtendatenschutzgesetz erlassen, was gleichwohl aufgrund der Dauer von Gesetzgebungsverfahren nur mittelfristig umsetzbar ist. Parallel sollte die Ausarbeitung von Standardvertragsklauseln zwischen Datenschutzaufsicht und Branchenverbänden erörtert werden, wobei ein mittelfristiger Abstimmungszeitraum auch hier realistisch erscheint.

Details: Kapitel 7.4.1.2.2 des Abschlussberichtes.

26) RECHTLICHER RAHMEN FÜR IT-SICHERHEITSZERTIFIZIERUNG

Vorschlag: Es sollte eine gesetzliche Regelung zur IT-Sicherheits-Zertifizierung geschaffen werden, die Voraussetzungen, Verfahren und rechtliche Bedeutung der Zertifizierung regelt. Damit kann ein gesetzlicher Rahmen für anerkannte und bindende IT-Zertifizierungen geschaffen werden, auf die Unternehmen, insb. KMU, zurückgreifen können.

Begründung: Derzeit fehlt es an rechtlichen Grundlagen der IT-Sicherheit und von Verhaltensanforderungen. Dabei könnten IT-Sicherheits-Zertifizierungen Abhilfe schaffen. Zertifizierungen sind – im Zusammenspiel mit anerkannten Standards zur IT-Sicherheit – ein ideales Instrument, um auf breiter Fläche die Umsetzung von Sicherheitsmaßnahmen zu prüfen. Zugleich können Unternehmen durch Zertifikate die Einhaltung von Sicherheitsstandards nachweisen und damit Vertrauen schaffen.

Derartige gesetzliche Rahmenbedingungen können wegen der erforderlichen fachlichen Vorarbeiten und der Dauer von Gesetzgebungsverfahren nicht kurzfristig geschaffen werden. Eine mittelfristige Umsetzung erscheint jedoch denkbar. Anders als im Bereich des Datenschutzes kann der nationale Gesetzgeber hinsichtlich der Anforderungen an allgemeine IT-Sicherheitszertifizierungen selbst tätig werden.

Details: Kapitel 7.4.1.2.3 des Abschlussberichtes.

25 Vgl. insbesondere Kapitel 4.4.4, 5.2.2 und 5.4.2 des Abschlussberichtes.

27) AUSBAU BEHÖRDLICHER KOMPETENZEN UND KOOPERATIONEN IM BEREICH IT-SICHERHEIT

Vorschlag: Das System der behördlichen Aufsicht im Bereich IT-Sicherheit sollte weiterentwickelt werden und gezielt auch die Belange der I.40 einbeziehen. Dabei sind durch gesetzliche Maßnahmen neue, bisher nicht bestehende Kompetenzen zu schaffen.

Begründung: Das bisherige System behördlicher Aufsicht für IT-Sicherheit ist insbesondere in Bezug auf I4.0 unvollständig. Es bestehen institutionelle Defizite, etwa das Fehlen von zuständigen Behörden und Aufgaben.

Bei der Weiterentwicklung der behördlichen Aufsicht sollten die Möglichkeiten der Zusammenwirkung bestehender Aufsichtsbehörden ausgelöst werden. Eine Alleinzuständigkeit des BSI ist nicht sinnvoll. Vielmehr sollte eine Zusammenarbeit bei IT-Sicherheit und Datensicherheit im Sinne des Datenschutzes auch auf Ebene der Aufsichtsbehörden abgestimmt werden.

Aufgrund der Dauer von Gesetzgebungsvorhaben, ist mit einer kurzfristigen Umsetzung nicht zu rechnen. Auch der Ausbau der behördlichen Kooperation ist ein fortschreitender Prozess, der langfristig anzulegen ist.

Details: Kapitel 7.4.1.2.4 des Abschlussberichtes.

28) MUSTERKLAUSELN UND MUSTEREINWILLIGUNGEN FÜR I4.0 HINSICHTLICH HAFTUNG SOWIE DATENSCHUTZ UND BETRIEBS- UND GESCHÄFTSGEHEIMNISSE

Vorschlag: In Kooperation mit der Konferenz der Datenschutzbeauftragten des Bundes und der Länder, dem Düsseldorfer Kreis (informelle Beratungsgremien der deutschen Datenschutzaufsichtsbehörden) und der Artikel 29 Gruppe[26] (Beratungsgremium der nationalen Datenschutzaufsichtsbehörden, des europäischen Datenschutzbeauftragten und der Europäischen Kommission) sollten Branchenverbände Musterklauseln und Mustereinwilligungen für datenschutzrechtliche Verarbeitungen und Nutzungen speziell für häufige oder branchenübliche I4.0-Netzwerkstrukturen entwerfen. Zudem sollten Branchenverbände in Kooperation mit Experten aus der Praxis Musterklauseln zum Schutz vor Betriebs- und Geschäftsgeheimnissen entwerfen, die den besonderen Konstellationen bei I4.0-Anwendungen Rechnung tragen. Die Entwicklung von Musterverträgen oder -klauseln zur IT-Sicherheit verspricht nicht zuletzt im Hinblick auf die Internationalität der Informationstechnologie und der IT-Dienste große Chancen, wenn es gelingt, gemeinsame Positionen der Wirtschaft in diesem Aspekt zu entwickeln.

Feststellung[27]: Derzeit fehlt es an Mustern, die KMU den Umgang mit datenschutzrechtlichen Anforderungen bei I4.0-Netzwerkstrukturen erleichtern. Zudem fehlen Muster, die KMU verwenden können, um ihre Betriebs- und Geschäftsgeheimnisse gegenüber anderen Unternehmen bei Einbindung im Rahmen von Zusammenarbeiten bei I4.0 zu schützen. Diese müssten zudem durch die Regulierungsbehörden auch anerkannt sein. Hierzu müssten die Branchenverbände entsprechende Muster in Abstimmung mit den Regulierungsbehörden erarbeiten. Aufgrund des Abstimmungsprozesses ist hier jedoch von einem mittelfristigen Zeitrahmen auszugehen. Mit einer Umsetzung der rechtlichen Rahmenbedingungen zu Zertifizierungen und einem Datenschutzsiegel ist allenfalls langfristig zu rechnen.

Details: Kapitel 7.4.1.2.5 des Abschlussberichtes.

29) ORIENTIERUNGSRAHMEN FÜR ANGEMESSENE TECHNISCH-ORGANISATORISCHE MAßNAHMEN DURCH DATENSCHUTZSIEGEL

Vorschlag: Schaffung eines klaren Orientierungsrahmens für die wirtschaftliche Implementierung von hinreichenden technischen und organisatorischen Maßnahmen, z. B. durch das in dem Entwurf der Datenschutzgrundverordnung vorgesehene Datenschutzsiegel.

Begründung[28]: In der Praxis herrscht Unklarheit, ob die von den verantwortlichen Stellen implementierten technischen und organisatorischen Maßnahmen als angemessen zu qualifizieren sind, da es an einem ausreichenden Orientierungsrahmen für Anwendungen der I4.0 derzeit fehlt. Der Entwurf der EU-Datenschutzgrundverordnung

26 Vgl. Artikel 29 und 30 der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr.

27 Vgl. insbesondere Kapitel 4.4.4 und 5.2.2.1.1 des Abschlussberichtes.

28 Vgl. insbesondere Kapitel 5.4.2 des Abschlussberichtes.

sieht bereits jetzt die Einführung eines EU-Rechtsrahmens zur Vergabe von Datenschutzsiegeln vor. Die Bundesregierung kann sich daher bereits im Rahmen der laufenden Verhandlungen im europäischen Gesetzgebungsverfahren für diese Regelung einsetzen. Nach Ablauf der Umsetzungsfristen für die EU-Datenschutzgrundverordnung können Datenschutzsiegel dann zur Orientierung und Vereinheitlichung technisch-organisatorischer Maßnahmen beitragen. Mittelfristig sollte daher die Möglichkeit für Unternehmen zur Nutzung von Datenschutzsiegeln bestehen.

Details: Kapitel 7.4.1.2.6 des Abschlussberichtes.

30) HERAUSARBEITUNG VON HINDERNISSEN, DIE DURCH (INTERNATIONALES) EXPORTRECHT BEI I4.0 GEMEINHIN ENTSTEHEN KÖNNEN

Vorschlag: Die Bundesregierung sollte eine Arbeitsgruppe einrichten, die unter Beobachtung der weiteren Entwicklung der I4.0 dezidiert herausarbeitet, welche I4.0 Anwendungen in der Praxis gemeinhin Hindernissen durch (internationales) Exportrecht ausgesetzt sind.

Begründung[29]: Da die Entwicklung der I4.0 sich in der Praxis noch nicht hinreichend konturiert hat, lässt sich zurzeit nicht abschließend feststellen, welche Hindernisse durch das (internationale) Exportrecht entstehen könnten. Eine Beobachtung der weiteren Entwicklung der I4.0 durch eine Arbeitsgruppe müsste langfristig angelegt sein, um fundierte Feststellungen abschließend treffen zu können.

Details: Kapitel 7.4.1.2.7 des Abschlussberichtes.

31) FORSCHUNG UND KONZEPTION ZUM RECHTSRAHMEN FÜR IT-SICHERHEIT

Vorschlag: Es sollte ein Forschungsprogramm zur Förderung interdisziplinärer Forschung zu den Chancen und Anforderungen an IT-Sicherheits-Regulierung, insbesondere im Hinblick auf die Bedürfnisse der I4.0 eingerichtet und gefördert werden.

Begründung: Diese Studie hat gezeigt, dass die Regulierung von IT-Sicherheit generell noch am Anfang steht. Die Gefährdungen der vernetzten Entwicklung und Produktion im Hinblick auf I4.0 ist noch nicht ausreichend erforscht. Daher ist es notwendig, kurzfristig und möglichst schnell eine interdisziplinäre Forschung zur IT-Sicherheit mit Blick auf I4.0 zu etablieren, damit die Erkenntnisse für gesetzliche Maßnahmen genutzt werden können. Dies kann am besten durch Einrichtung und Förderung eines entsprechenden Forschungsprogramms erfolgen.

Details: Kapitel 7.4.1.2.8 des Abschlussberichtes.

32) LÄNDERÜBERGREIFENDE EINHEITLICHE SCHUTZSTANDARDS IN BEZUG AUF GEHEIMNISSCHUTZ

Vorschlag: Die Geheimnisschutzverordnung sollte regelmäßig evaluiert werden, um zu prüfen, ob sich in der Praxis Bedürfnisse zeigen, die durch die vorgesehene Regulierung noch nicht abgedeckt sind. Unabhängig davon sollten Branchenverbände Muster-Non-Disclosure-Agreements schaffen, auf die insbesondere KMU zurückgreifen könnten.

Begründung[30]: Eine umfassende Regulierung des Geheimnisschutzes (Schutz von Betriebs- und Geschäftsgeheimnissen) existiert noch nicht. Mit der neuen Geheimnisschutzverordnung[31] ist jedoch bereits ein Anfang geschaffen. Eine Evaluierung der Situation sollte langfristig erfolgen. Non-Disclosure-Agreements (NDA) sind bei KMU noch nicht ausreichend verbreitet, können den Schutz jedoch verbessern und wären bei Vorliegen entsprechender Muster kurzfristig umsetzbar.

Details: Kapitel 7.4.1.2.9 des Abschlussberichtes.

29 Vgl. insbesondere Kapitel 4.4.7 und 5.4.1 des Abschlussberichtes.

30 Vgl. Kapitel 3.3.5, 4.4.6 und 4.4.8 des Abschlussberichtes.

31 Vorschlag für eine RICHTLINIE DES EUROPÄISCHEN PARLAMENTS UND DES RATES über den Schutz vertraulichen Know-hows und vertraulicher Geschäftsinformationen (Geschäftsgeheimnisse) vor rechtswidrigem Erwerb sowie rechtswidriger Nutzung und Offenlegung /* COM/2013/0813 final - 2013/0402 (COD) */.

9.3 Normungs- und Standardisierungsorganisationen

Ausgehend von den vorgestellten technischen Konzepten (s. Kap. 6.1 des Abschlussberichtes) und der Bewertung der Normen und Standards (s. Kap. 6.4 des Abschlussberichtes), werden nachfolgend entsprechende Handlungsvorschläge formuliert die sich primär an Normungs- und Standardisierungsorganisationen richten und Industrieunternehmen als Anwender von I4.0 nur indirekt betreffen.

34) ERARBEITUNG EINER STRUKTUR FÜR IT-SICHERHEITSSTANDARDS

Vorschlag: Erarbeitung einer für I4.0 passenden Struktur und Klassifikation für IT-Sicherheitsstandards abgeleitet aus dem Referenzarchitekturmodell Industrie 4.0 (RAMI4.0) und den existierenden Referenzmodellen für ICS unter Einbindung wichtiger Unternehmen aus dem Bereich industrielle Produktion.

Tabelle 9-3: Priorisierte Handlungsvorschläge für Normungs- und Standardisierungsorganisationen

Handlungsvorschlag	Disziplin
Erarbeitung integrierter Standards für Safety & Security	Normung und Standardisierung
Erarbeitung einer Struktur für IT-Sicherheitsstandards	Normung und Standardisierung
Integration technischer Standards mit ISMS-Standards	Normung und Standardisierung
Engineering von sicheren IT-Systemen	Normung und Standardisierung

33) ERARBEITUNG INTEGRIERTER STANDARDS FÜR SAFETY & SECURITY

Vorschlag: Erarbeitung eines integrierten Sicherheitskonzepts im Sinne von Security und Safety durch Standardisierungsorganisationen mit dem Ziel einer gemeinsamen Zertifizierung.

Feststellung[32]: Für Safety gibt es eine Vielzahl branchenspezifischer Standards. In diese Standards sollen zukünftig die notwendigen Ergänzungen für IT-Security so eingebracht werden, dass Vernetzung über offene Netzwerke möglich wird. In Zukunft werden auch vermehrt Security-Zertifizierungen gefordert werden. Ziel ist es hier, eine integrierte Safety-Security-Zertifizierung vorzubereiten, die auch Systeme erfasst, welche sich zur Laufzeit autonom verändern. Standardisierungsorganisationen (Industrieunternehmen als Anwender von I4.0, aber auch als Mitglieder in Standardisierungsgremien) können hier nur mittelfristig etwas umsetzen, da die Erarbeitung von Standards zeitaufwändiger ist.

Details: Kapitel 7.4.3.1 des Abschlussberichtes.

Feststellung[33]: Es gibt keine allgemein akzeptierte Struktur von IT-Sicherheitsstandards, die für I4.0 unmittelbar einsetzbar wäre. Standardisierungsorganisationen sollten hier mittelfristig etwas umsetzen. Es ist unbedingt erforderlich ist diese Standardisierungsaufgabe schnellstmöglich unter Beachtung der laufenden internationalen Standardisierung und den Security-Arbeiten im IIC in Angriff zu nehmen.

Details: Kapitel 7.4.3.2 des Abschlussberichtes.

35) INTEGRATION TECHNISCHER STANDARDS MIT ISMS-STANDARDS

Vorschlag: Aufruf an die Standardisierungsgremien zur Erarbeitung von Richtlinien zur Umsetzung der Bewertungsstandards und Richtlinien auf die technischen Standards der Internet-Welt (W3C, IETF, OASIS) und der Serie von OPC Unified Architecture (OPC UA) Standards (konzeptionell und technisch). Dabei sollen die Spezifika von I4.0, insbesondere der nicht-funktionalen Anforderungen, in Form von Profilen/Ausprägungen der technischen Standards der

32 Vgl. auch Kapitel 6.1.4 des Abschlussberichtes.

33 Vgl. auch Kapitel 6.4 des Abschlussberichtes.

Internet-Welt berücksichtigt werden genauso wie die entstehenden I4.0-Referenzarchitekturen, abgeleitet aus dem RAMI 4.0 und den existierenden Referenzmodellen für ICS.

Feststellung: Standards im Bereich „Bewertung“ und „Richtlinien“ sind losgelöst von den technischen Standards. Standardisierungsgremien (wie z. B. DIN und DKE) und Branchenverbände (wie z. B. BITKOM) sollten hier mittelfristig etwas umsetzen und diese Lücke schließen. Hindernis ist hier lediglich die zeitaufwendige Standardisierung.

Details: Kapitel 7.4.3.3 des Abschlussberichtes.

36) ENGINEERING VON SICHEREN IT-SYSTEMEN

Vorschlag: Erarbeitung einer Richtlinie für eine IACS-bezogenen Analyse- und Design-Methode unter besonderer Berücksichtigung der IT-Sicherheitsmanagement-anforderungen nach ISO/IEC 27001 in Verbindung mit ISO/IEC 27002, VDI/VDE 2182, BDSG und BSI-Grundschutz sowie der Fähigkeiten der zu der jeweiligen Wertschöpfungskette passenden technischen Referenzarchitektur und deren IT-Sicherheitsstandards.

Feststellung[34]**:** IT-Sicherheitsstandards sollten einfließen in das Engineering von IT-Systemen („security and privacy by design“). Standardisierungsgremien wie z. B. DIN, DKE oder internationale Pendants sowie Verbände wie BITKOM, VDI/VDE, VDMA und ZVEI unter differentieller Berücksichtigung von Anforderungen verschiedener Branchen und Unternehmensgrößen sind hier gefragt. Wegen der Fülle von Anforderungen erscheint dieses Ziel nur langfristig erreichbar.

Details: Kapitel 7.4.3.4 des Abschlussberichtes.

9.4 Resümee

Die o. g. Handlungsvorschläge helfen den Anwendern von I4.0 und der Politik dabei, für konkrete Szenarien zu erkennen, an welchen kritischen Stellen Handlungsbedarf besteht. Zudem unterstützen die Handlungsvorschläge bei der Identifizierung und Etablierung von Maßnahmen, um vorhandenen Risiken und Bedrohungen sowie rechtlichen und organisatorischen Hemmnissen zu begegnen. Eine Vielzahl von Handlungsvorschlägen muss kurzfristig[35], d. h. im Zeitraum von wenigen Jahren, angegangen werden. Hier sind sowohl die Wirtschafts-, Technologie- und Förderpolitik, Standardisierungsorganisationen als auch die Unternehmen selbst, ungeachtet ihrer Betriebsgröße, sowie ihre jeweiligen Branchenverbände gefragt, welche in vielen Bereichen eng bzw. noch enger zusammenarbeiten müssen oder in vielen Fällen auch voneinander abhängig sind. Es besteht insbesondere seitens der Politik erheblicher regulatorischer Handlungsbedarf und die Auseinandersetzung der verschiedenen Interessenslagen muss vorangetrieben werden.

34 Vgl. auch Kapitel 6.4 des Abschlussberichtes.

35 Die vorgeschlagenen Umsetzungszeithorizonte der Handlungsvorschläge unterscheiden sich nach kurzfristig (ein bis zwei Jahre), mittelfristig (drei bis fünf Jahre) und langfristig (sechs bis zehn Jahre).

www.bmwi.de