Fraunhofer
IPT

FRAUNHOFER-INSTITUT FÜR PRODUKTIONSTECHNOLOGIE IPT

WHITEPAPER **CYBERSECURITY IN DER VERNETZTEN PRODUKTION**

INHALT

Einleitung **2**

Was gilt es zu schützen? **3**

Industrielle Produktion aus Perspektive der IT **4**
- Risiken und Herausforderungen in der Produktion 5
- Schwachstellen im Umfeld der Produktion 6
- Angriffsmethoden und -mittel 6

Studiendesign **8**
- Stichprobe und Erhebungsmethode 9
- Auswertungsmethode 9

Ergebnisse **11**
- Detailbetrachtung am Beispiel der Asset-, Change- und Konfigurationsmanagement-Domäne 11
- Zusammenfassung der Ergebnisse der weiteren IT-Sicherheits-Domänen 15

Ausblick **18**

Autoren **19**

Referenzen **20**

EINLEITUNG

Digitalisierung und Vernetzung bringen für Unternehmen ein enormes Wachstumspotenzial mit sich und werden in den kommenden Jahren stark an Bedeutung für den Wirtschaftsstandort Deutschland gewinnen [1, 2]. Die Unternehmens- und Strategieberatung McKinsey & Company schätzt, dass deutsche Unternehmen bis 2025 durch konsequente Digitalisierung 126 Milliarden Euro zusätzlich an Wertschöpfung erzielen können [3]. Im Gesamtkontext betrachtet erbrachte das produzierende Gewerbe im Jahr 2018 mehr als ein Viertel des gesamten deutschen Bruttoinlandsprodukts [4]. Trotz des großen Wachstumspotenzials liegt die Digitalisierungsrate in der Produktion deutscher Großunternehmen erst bei knapp 30 Prozent – bei kleinen und mittleren Unternehmen sogar nur bei 20 Prozent [5]. Eines der größten Hemmnisse bei der Vernetzung ist die Cybersicherheit [6]: Ging es bisher in erster Linie um die funktionale Sicherheit von Produktionsanlagen, so rückt nun die Cybersicherheit – bedingt durch den Wandel von geschlossenen zu offenen cyberphysischen Systemen (CPS) – immer mehr in den Vordergrund [7]. Lange Lebenszyklen führen jedoch dazu, dass für Anlagen keine Updates mehr angeboten werden, Patch-Policies veralten und damit unzureichend sind und dass die verfügbaren Netzwerk-Protokolle nicht mehr sicher sind [8].

Aufgrund der weltweiten Vernetzung ist Cyberkriminalität zudem nicht nur ein lokales, sondern ein globales Problem aller Industrienationen. Besonders Angriffe auf industrielle Automatisierungssysteme sowie die Anzahl der publik gewordenen Cyber-Vorfälle nehmen rasant zu [9, 10]. Cyberkriminalität reicht beispielhaft von schwerer Erpressung der Automobilhersteller mittels Ransomware bis hin zur physischen Beschädigung eines Hochofens in einem deutschen Stahlwerk [11, 12].

Das Fraunhofer-Institut für Produktionstechnologie IPT hat deshalb einen ganzheitlichen Production Security Readiness Check (PSRC) auf Basis aktueller Normen, Standards und Guidelines entwickelt, der produzierenden Unternehmen aufzeigt, auf welchem Sicherheitsniveau sie sich gerade befinden und welchen Risiken sie ausgesetzt sind. Basierend auf dem Sicherheitsniveau des Unternehmens zeigt der Production Security Readiness Check Handlungsoptionen auf, anhand derer Unternehmen die Lücke zwischen dem bereits erreichten und dem gewünschten Sicherheitsniveau schließen können.

WAS GILT ES ZU SCHÜTZEN?

Elektronische Informationen sind zu schützende Güter. Um den notwendigen Schutz zu gewährleisten, werden bestimmte Anforderungen an IT-Systeme gestellt. Diese Anforderungen werden als Schutzziele der IT-Sicherheit bezeichnet [13, 14]. Ziel ist es daher, zu verhindern, dass vertrauliche Informationen an unbefugte Personen gelangen (Vertraulichkeit) oder durch unautorisierte Dritte verändert werden können (Integrität) [15,16]. Parallel dazu soll der Zugang zu Informationen im besten Fall dauerhaft gewährleistet sein (Verfügbarkeit) [17]. Basierend auf diesen Anforderungen ergeben sich drei zentrale Ziele, die zu schützen sind: Vertraulichkeit, Integrität und Verfügbarkeit von Daten und Systemen [12, 16]. Neben diesen zentralen Zielen existieren weitere Schutzziele, unter anderem Authentizität, Zurechenbarkeit, Transparenz und Kontingenz [18]. Die Anforderungen an IT-Systeme in Form von Schutzzielen werden entweder vom Unternehmen bestimmt, wenn beispielsweise kritische Fertigungsdaten vertraulich gespeichert und verarbeitet werden sollen, oder sie werden in Gesetzen und Normen definiert.

Ein zusammenhängendes und allgemeingültiges IT-Sicherheitsrecht existiert in Deutschland derzeit nicht. Vielmehr sind rechtliche Vorgaben mit Bezug zur IT-Sicherheit auf eine Vielzahl unterschiedlicher Gesetze verteilt [19]. Das Inkrafttreten des IT-Sicherheitsgesetzes im Jahr 2015 sollte deshalb gezielter zur Verbesserung der Sicherheit von IT-Systemen in Unternehmen beitragen [20]. Zu den Hauptadressaten des Gesetzes gehören auch Betreiber kritischer Infrastrukturen (BSIG) sowie Telekommunikations- und Telemedienanbieter (TKG & TMG) [19, 21]. Die deutsche Industrieproduktion und die damit verbundenen Wertschöpfungsketten werden nicht explizit als Adressat genannt. Für diesen Sektor existieren außerhalb der Regelungen für kritische Infrastrukturen keine gesetzlichen Grundlagen, die die IT-Sicherheit betreffen [12]. In der IT gibt es eine Vielzahl verschiedener Standards und Normen unterschiedlicher Gremien, die die Sicherheit betreffen [12]. Abbildung 1 stellt die wichtigsten Gesetze, Normen und Gremien zur Förderung der IT-Sicherheit dar.

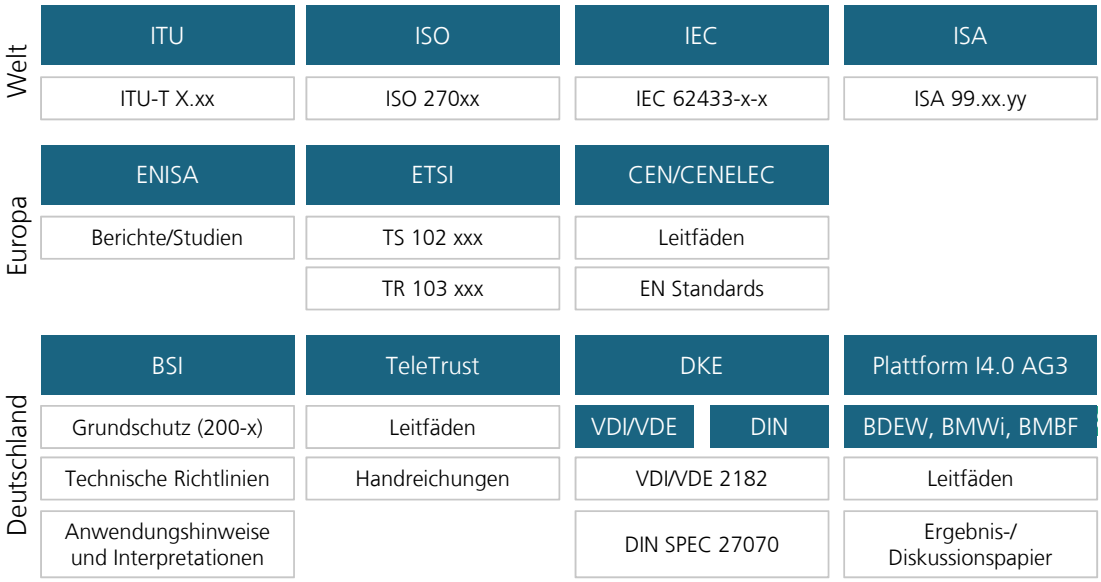

Abbildung 1: Übersicht der wichtigsten internationalen und nationalen IT-Sicherheitsgesetze, -normen und -gremien [28]

INDUSTRIELLE PRODUKTION AUS PERSPEKTIVE DER IT

Die heutige industrielle Produktion hat das Ziel, ihre Produktivität zu steigern und gleichzeitig Kosten zu senken. Um dieses Ziel zu erreichen, werden innerhalb der Produktion automatisierte Produktionsanlagen eingesetzt. Die einzelnen Bereiche der heutigen industriellen Automatisierung veranschaulicht die sogenannte Automatisierungspyramide (vgl. Abbildung 2, links) [23].

Die Automatisierungspyramide beschreibt sechs verschiedene Ebenen im Unternehmen, die in einem Kommunikationsverhältnis zueinander stehen. Die fortschreitende Vernetzung der Produktion führt dazu, dass IT- (Information Technology) und OT- (Operational Technology) Netzwerke langsam miteinander verschmelzen. Ein kompletter Air Gap, die physische Trennung der Systeme zwischen Prozess- und Betriebsleitebene, nimmt de facto in der heutigen Produktion kontinuierlich ab. Produktionsanlagen, die früher isoliert mit proprietären Protokollen in der IACS- (Industrial Automation and Control Systems) Umgebung betrieben wurden, übernehmen heute beispielsweise offene Netzwerkprotokolle der IT-Netzwerke [26]. Bedrohungen gegenüber Produktionsanlagen wurden bisher als beherrschbar betrachtet, da diese Anlagen – aus IT-Perspektive gesehen – Inseln bildeten, die nur begrenzt von außen angreifbar waren [12]. Bezogen auf die Automatisierungspyramide sorgt nun der Industrie-4.0-Ansatz dafür, dass alle Systemkomponenten durchgängig horizontal und vertikal miteinander vernetzt sind. Dies bedeutet jedoch, dass die klassische hierarchische Automatisierungspyramide aufgelöst wird und ein Automatisierungsnetzwerk entsteht (vgl. Abbildung 2, rechts). Für die Sensorik und Aktorik in der Feldebene heißt dies, dass sie nicht nur ausschließlich Daten mit der Steuerungsebene (SPS/SCADA) austauschen, sondern ebenenübergreifend [27]. Feldgeräte sind dann direkt an das Automatisierungsnetzwerk angebunden. Aus Sicht der IT-Sicherheit bedeutet das, dass Feldgeräte nun direkt aus dem Internet via Ethernet/WLAN erreichbar und damit auch angreifbar sind. Schützende Ebenen aus SPS- oder SCADA-Systemen existieren nicht mehr. Schnittstellen zu mobilen Datenträgern bieten zusätzliches Angriffspotenzial [28]. Sowohl aus der Automatisierungspyramide als auch aus dem dargestellten Automatisierungsnetzwerk lassen sich Risiken und Herausforderungen für die Produktion ableiten.

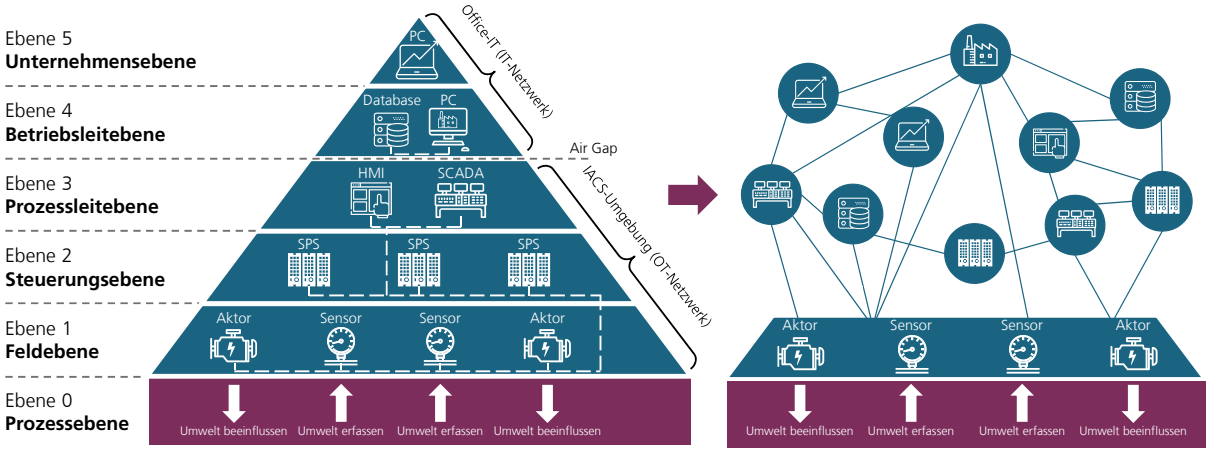

Abbildung 2: Automatisierungspyramide und -netzwerk in der Produktion [23] [24]

Risiken und Herausforderungen in der Produktion

Die Risiken und Herausforderungen in der Produktion lassen sich in drei Kategorien einordnen: Die Literatur unterscheidet zwischen der operativen, der technischen und der Management-Domäne [8]. So gilt es, eine Vielzahl von operativen Zielen, beispielsweise die Gewährleistung der Funktionsfähigkeit, bei einer gleichzeitig hohen Verfügbarkeit der Produktionsanlagen zu erreichen. Auf der technischen Seite begründen sich die Risiken und Herausforderungen im Einsatz eingebetteter Systeme und unsicherer Netzwerkprotokolle, aber auch in dem Anspruch, eine Performance in Echtzeit zu gewährleisten. Ein IACS muss in den meisten Fällen in Echtzeit operieren, um den Produktionsprozess zu managen. Die Kommunikationslatenz und der Jitter sind die entscheidenden Faktoren für eine Echtzeit-Kommunikation des OT-Netzwerks. Die Forderung nach einer geringen Latenz erschwert die Implementierung ressourcenhungriger Security-Mechanismen wie Verschlüsselungen.

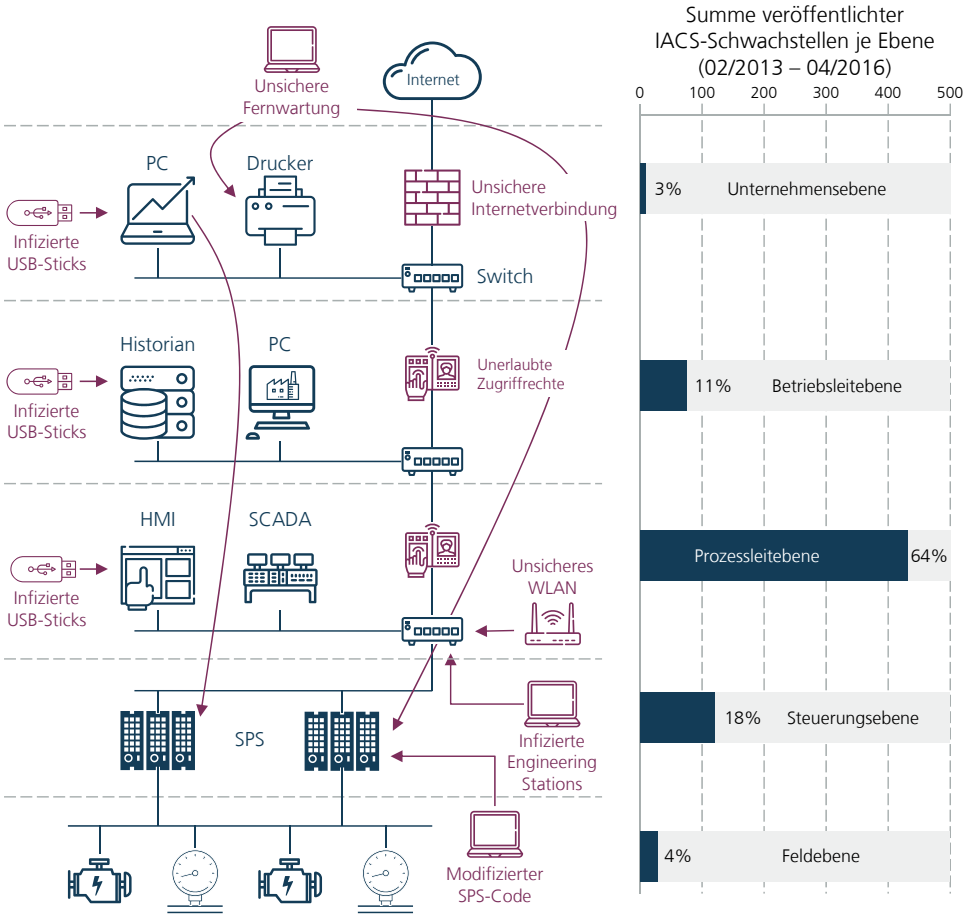

Abbildung 3: Kumulierte Anzahl und Darstellung möglicher Schwachstellen in der Automatisierungspyramide [30][31]

Aus der Management-Perspektive bergen die geringe Sensibilisierung der Benutzer und Anwender, die unzureichende Regelung der IT-Sicherheit in der Produktion sowie die langen Anlagenlebenszyklen zusätzliche Risiken [8]. Die Beschaffung einer neuen Industrieanlage zieht höhere Investitionen nach sich: Die Anlage muss über mehrere Jahrzehnte hinweg betrieben werden, damit sich die Investitionskosten bezahlt machen. Eine Anlagenlebensdauer bis zu 30 Jahren ist keine Seltenheit [29]. Diese langen Lebenszyklen führen im Sinne der Cybersecurity zu zwei Problemen: Es besteht kaum Schutz gegenüber der neuen Gefährdungen und die Sicherheit hängt gleichzeitig meist von nicht mehr unterstützten (Betriebs-) Systemen ab [8]. Wenn Unternehmen diesen beschriebenen Risiken und Herausforderungen nicht konsequent begegnen, können Schwachstellen in der Produktion entstehen.

Schwachstellen im Umfeld der Produktion

Schwachstellen existieren in jeder einzelnen Ebene der Automatisierungspyramide: Im linken Teil der Abbildung 3 sind exemplarisch Schwachstellen für jede einzelne Ebene dargestellt. Im rechten Teil ist die Anzahl der veröffentlichten IACS-bezogenen Schwachstellen von 2013 bis 2016 kumuliert abgebildet. Diese Zahl basiert auf öffentlichen Meldungen sowie der ICS-CERT-Datenbank. Mit 465 von 724 Fällen betrifft mehr als die Hälfte der veröffentlichten Schwachstellen die Prozessleitebene [30, 31].

IT-Sicherheitsexperten vermuten mehrere Ursachen, warum besonders in dieser Ebene viele Schwachstellen aufgedeckt werden. Mögliche Ursachen sind [30]:

1. Die eingesetzte industrielle Hard- und Software ähnelt der Office-Hard- und -Software (z.B. HMI) und ist deshalb den Schwachstellenforschern geläufig.
2. Eingesetzte Software kann einfach und günstig in Form von Demoversionen von Forschern beschafft werden.
3. Die Prozessleitebene ist von kritischer Natur, das heißt, der Zugang zur Prozessleitebene gewährt automatisch Zugang zur verbundenen Feldebene und zum physischen Prozess. Die Suche nach Schwachstellen innerhalb der Steuerungs- und Feldebene wird überflüssig.
4. Nichtauthentifizierte Protokolle erlauben direkten Zugang zum OT-Netzwerk.

Angriffsmethoden und -mittel

Um Sicherheitsmaßnahmen zu implementieren, ist es erforderlich, die Angriffsmethoden der Angreifer zu verstehen. Sie unterscheiden sich nicht von jenen, die Sicherheitsexperten anwenden, um ein System zu testen. Verschiedene Arten von Angriffen sind in Abbildung 4 dargestellt.

Unabhängig von der Art der Angriffe laufen diese in einem ähnlichen Muster ab [34]:
1. Ausspähen von Schwachstellen des Systems
2. Infiltration des Systems durch Ausnutzen der Schwachstelle
3. Ausführen der Schadsoftware

Die Darstellung basiert auf Experteninterviews der ENISA ICS Security Stakeholder Group (EICS) und der European SCADA and Control Systems Information Exchange (EuroSCSIE) im Rahmen einer ENISA-Studie. Weitere Experten stammten aus der Industrie, der Wissenschaft und der Politik [32].

Abbildung 4: Gängige Methoden und Mittel zum Angriff auf industrielle Produktionsanlagen [32][33][34]

STUDIENDESIGN

Zur Ermittlung des aktuellen Sicherheitsniveaus von Unternehmen hat das Fraunhofer IPT den »Production Security Readiness Check (PSRC)« entwickelt. Der PSRC ist ein Modell zur selbstständigen Messung des Cybersecurity-Status produzierender Unternehmen und hilft diesen, ihre Cybersecurity-Planung zu bewerten und zu verbessern. Besonders konzentriert sich der PSRC auf die Implementierung und das Management von Cybersecurity-Praktiken im Zusammenhang mit Assets der Informationstechnik (IT), der Betriebstechnik (OT) als auch mit Umgebungen, in denen sie betrieben werden. Das Modell des PSRC wurde in Form eines Excel-Sheets abgebildet.

Der Production Security Readiness Check unterstützt produzierende Unternehmen bei den folgenden Zielen:

1. Bewertung und Stärkung der Cybersecurity-Maßnahmen in der Produktion
2. Aufzeigen von Risikofaktoren im Unternehmen und in der Produktion
3. Priorisierung von Aktionen und Investitionen in Cybersecurity

Der PSRC wurde so entwickelt, dass er von produzierenden Unternehmen jeder Branche, Struktur und Größe genutzt werden kann [35]. Das Tool basiert primär auf dem Cybersecurity Capability Maturity Model (C2M2) sowie aus einer Kombination gängiger Cybersecurity-Standards wie der ISO 27001, der IEC 62443, dem NIST CSF und dem BSI IT-Grundschutz. Die Anwendung der bestehenden Security-Normen und Standards ist im IT- und OT-Bereich essenziell, um einen holistischen Sicherheitsansatz zu gewährleisten [36][37][38]. Der PSRC besteht aus neun Domänen, die jene Themen abbilden, die für einen ganzheitlichen Sicherheitsansatz betrachtet werden müssen. Diese sind in Abbildung 5 dargestellt [35].

- Risikomanagement (RM)
- Asset-, Change- und Konfigurationsmanagement (ACKM)
- Identitäts- und Zugangsmanagement (IZM)
- Bedrohungs- und Schwachstellenmanagement (BSM)
- Situationsbewusstsein (SB)
- Informationsaustausch und Kommunikation (IAK)
- Reaktion auf Ereignisse und Vorfälle sowie Kontinuität der Produktion (EVKP)
- Supply-Chain-Management (SCM)
- Risikofaktor Mensch (RFM)

Abbildung 5: Die neun Domänen des PSRC

Stichprobe und Erhebungsmethode

Die Stichprobenauswahl basierte auf der »Klassifikation der Wirtschaftszweige, Ausgabe 2008 (WZ 2008)« des Statistischen Bundesamts. Für diese Studie war besonders der Wirtschaftszweig »C Verarbeitendes Gewerbe« relevant. Zur Ansprache der Unternehmen wurde mithilfe des Wirtschaftsinformationsdienstleisters »Nexis« auf die Creditreform-Datenbank zurückgegriffen. Es wurden Unternehmen mit einer Mindestmitarbeiterzahl von 20 aus dem produzierenden Gewerbe ausgewählt, die über eine E-Mail-Kontaktadresse verfügten.

Aus dem gegebenen Unternehmenspool nahmen schließlich 28 Unternehmen verschiedener Industriezweige an der detaillierten Studie teil. Ihre Zuordnung zu den jeweiligen Industriesektoren ist Abbildung 6 zu entnehmen. Diese Unternehmen bewerteten im ersten Schritt ihren Sicherheitsstatus mithilfe des PSRC. Der Zeitaufwand für die Selbsteinschätzung war auf mindestens drei Stunden je Unternehmen ausgelegt. Basierend auf den ausgefüllten Ergebnissen wurden im zweiten Schritt mit ausgewählten Unternehmen Telefon-Interviews im Umfang von je 30 bis 60 Minuten durchgeführt. Ziel der Interviews war es, die erhaltenen Ergebnisse zu verifizieren und die Gründe für einen möglicherweise geringen Umsetzungsstand qualitativ zu erforschen.

Auswertungsmethode

Um die zuvor definierten Domänen besser miteinander vergleichen zu können, erfolgte die Auswertung für jede Domäne identisch: Die Auswertung begann stets allgemein und endete in einer Detailbetrachtung. Um die beschriebenen Cybersecurity-Praktiken – die die Grundlage des PSRC bilden – ein einem angemessenen Abstraktionsgrad darstellen zu können, wurden diese im Excel-Sheet als unabhängige, eindeutig differenzierbare Bausteine abgebildet. Diese Bausteine beziehen sich hier-

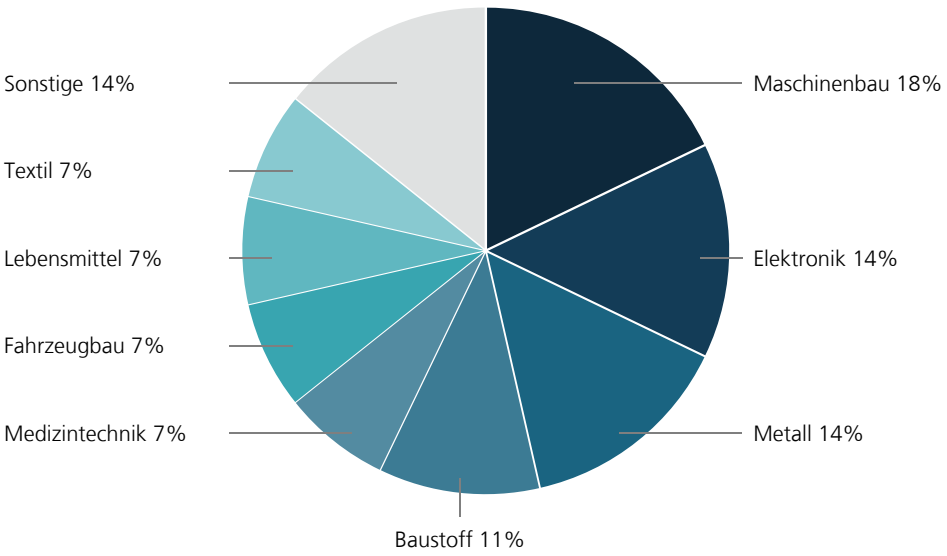

Abbildung 6: Beteiligte Industriesektoren an der IT-Sicherheitsstudie

für jeweils auf eine möglichst feingranulare Fragestellung und besitzen dabei zwar eine identische Nomenklatur, sind jedoch domänenübergreifend inhaltlich unterschiedlich. Beispielsweise bewertet das Unternehmen in der Asset- Change- und Konfigurationsmanagement (ACKM)-Domäne auf einer vierstufigen Skala, ob es den Baustein »ACKM-1.1a: Es existiert ein Inventar an OT- und IT-Assets, die für die Produktion relevant sind« nicht, teilweise, weitgehend oder vollständig umgesetzt hat [35]. Basierend auf den Einzelwertungen der jeweiligen Bausteine wird der zusammengefasste Umsetzungsstand aller Praktiken einer Domäne für die teilnehmenden kleinen und mittleren Unternehmen (KMU) sowie Großunternehmen in Form eines Boxplot-Diagramms dargestellt. Konkret bedeutet es, dass über alle Praktiken hinweg für jedes einzelne Unternehmen der Mittelwert des Umsetzungsstands bestimmt wurde. Die einzelnen Mittelwerte der Unternehmen wurden dann im Boxplot-Diagramm dargestellt. Als Zusatzinformation zeigt das Boxplot-Diagramm sowohl den – gegen Ausreißer robusten – Median als auch den Mittelwert der zuvor berechneten Einzelwerte. Die Vorteile des Boxplot-Diagramms liegen in der übersichtlichen Darstellung der Verteilung und der Spannweite der Ergebnisse.

Im nächsten Schritt fand eine detaillierte Betrachtung der Methoden- und Managementziele innerhalb der Domäne ebenfalls in Form eines Boxplot-Diagramms statt. Die Methoden- und Managementziele dienen als Kategorien für die einzelnen Cybersecurity-Praktiken (z.B. »ACKM-1.1b: Es existiert ein Inventar an Informationsbeständen, die für die Produktion relevant sind«, etc.) in übergeordnete Ziele wie z.B. »Ziel: 1. Managen des Asset-Inventars« der ACKM-Domäne [35]. Vergleiche dazu den Auszug aus der ACKM-Domäne in der Abbildung 7.

In der Detailbetrachtung wurde schließlich der IST- mit dem SOLL-Umsetzungsstand der einzelnen Bausteine innerhalb einer Domäne von KMU sowie Großunternehmen in einem Netzdiagramm verglichen. Dazu wurde für jeden einzelnen Baustein für alle KMU und Großunternehmen zusammenfassend der IST-Umsetzungsdurchschnitt ermittelt und dem empfohlenen SOLL-Umsetzungsstand gegenübergestellt. Diese Darstellung ermöglicht es, den Optimierungsbedarf jedes einzelnen Bausteins zu erfassen.

Asset-, Change- und Konfigurationsmanagement – Selbstbewertung

Ziel: 1. Managen des Asset-Inventars	Baustein	IST	SOLL	GAP
ACKM-1.1a: Es gibt ein Inventar an OT- und IT-Assets, die für die Produktion r	**ACKM-1.1a**	3	3	
ACKM-1.1b: Es gibt ein Inventar an Informationsbeständen, die für die Produkt	**ACKM-1.1b**	2	2	
ACKM-1.2c: Das Inventar enthält Zusatzinformationen zur Unterstützung der ur	**ACKM-1.2c**	1	2	Moderat
ACKM-1.2d: Inventarisierte Assets werden anhand ihrer Wichtigkeit für die Pro	**ACKM-1.2d**	1	2	Moderat
ACKM-1.3e: Das Inventar beschreibt (physische und logische) Verbindungen, K	**ACKM-1.3e**	1	2	Niedrig
ACKM-1.3f: Das Asset-Inventar wird in einer festgelegten Häufigkeit überprüft	**ACKM-1.3f**	1	2	Niedrig
Ziel: 2. Managen der Asset-Konfiguration	**Baustein**	**IST**	**SOLL**	**GAP**
ACKM-2.1a: Basiskonfigurationen sind für inventarisierte Assets festgelegt, um	**ACKM-2.1a**	2	3	Kritisch
ACKM-2.1b: Basiskonfigurationen werden verwendet, um Assets vor Inbetriebr	**ACKM-2.1b**	2	3	Kritisch

Abbildung 7: Ein Auszug aus der ACKM-Domäne [35]

ERGEBNISSE

Domänenübergreifend ist der Umsetzungsstand aller Cybersecurity-Praktiken der befragten KMU und Großunternehmen in Abbildung 8 dargestellt.

Die befragten Großunternehmen weisen im Mittel einen höheren Cybersecurity-Umsetzungsstand auf als die KMU. Dies macht sich besonders im Median (Großunternehmen: 0,98; KMU: 0,66) bemerkbar. Diese Daten zeigen, dass das Thema Cybersecurity bei den befragten KMU insgesamt weniger präsent ist als bei den Großunternehmen. Beide Boxplots weisen große Streubreiten und somit eine hohe Varianz in der Umsetzung der Cybersecurity-Praktiken auf.

Detailbetrachtung am Beispiel der Asset-, Change- und Konfigurationsmanagement-Domäne

Die Asset-, Change- und Konfigurationsmanagement-Domäne beschreibt die Verwaltung, Konfiguration und Änderung von IT- und OT-Assets. Unter Assets werden alle Vermögenswerte eines Unternehmens verstanden, einschließlich der gesamten Hard- und Software in der Produktion [35]. In der Asset-, Change- und Konfigurationsmanagement-Domäne ergeben sich zusammenfassend folgende Ergebnisse, die in Abbildung 9 zu sehen sind: Im Vergleich zur Risikomanagement-Domäne weist die ACKM-Domäne einen höheren Umsetzungsstand auf – im Mittel und im Median sowohl für die teilnehmenden KMU (Mittelwert: 1,13; Median: 0,98) als auch für die Großunternehmen (Mittelwert: 1,47; Median: 1,55).

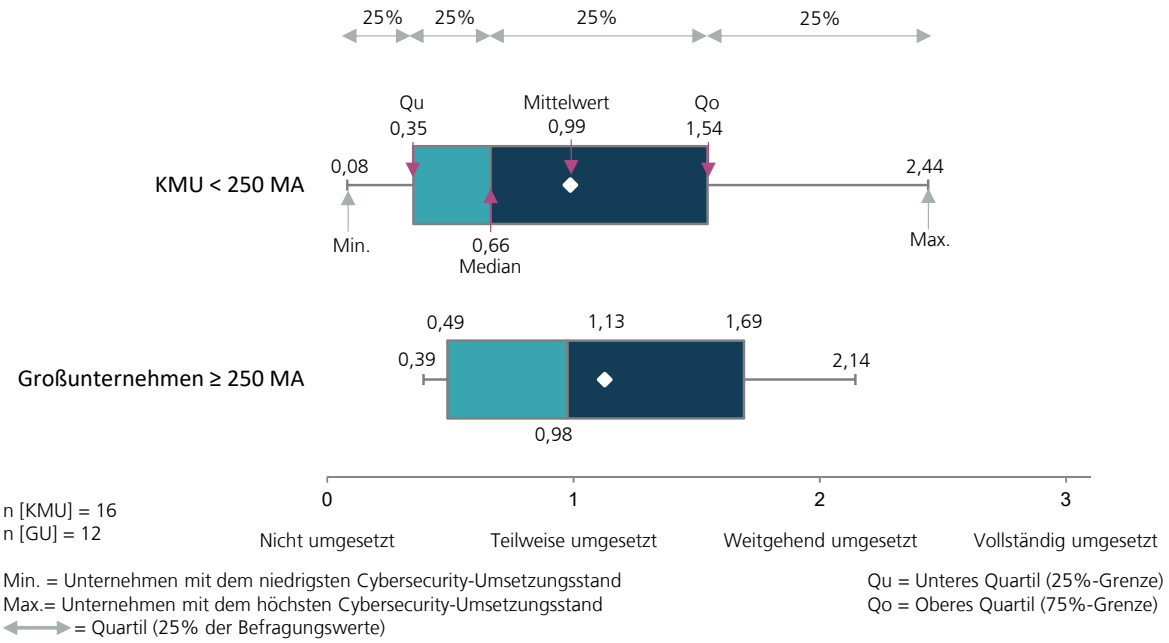

Abbildung 8: Umsetzungsstand aller Cybersecurity-Praktiken in allen Domänen

Dies lässt sich damit begründen, dass das Management von Unternehmensassets – unabhängig von der IT-Sicherheit – besonders in Großunternehmen ein geläufiger Prozess ist.

Ein Unternehmen aus der Printmedien-Industrie hat die im Mai 2018 eingeführte DSGVO als Chance genutzt, nicht nur im IT- sondern auch im OT-Netzwerk freiwillig die Asset-Dokumentation zu verbessern und so das Sicherheitsniveau anzuheben. Jedoch sehen die befragten Großunternehmen die Einmischung der Gesetzgebung in nicht-kritische Sektoren wie die Produktion als problematisch an. Befürchtet wird eine Überregulierung durch die Gesetzgebung.

In einer detaillierten Darstellung (Abbildung 10) ist zu erkennen, dass die teilnehmenden Unternehmen durchaus über ein Basisinventar an IT- und OT-Assets verfügen, die für die Produktion relevant sind. Alle weiteren das Inventar unterstützenden Zusatzinformationen wie das Mapping physischer und logischer Verbindungen zwischen Assets werden entweder nicht – in KMU – oder nur teilweise – in den Großunternehmen – umgesetzt, was sich im jeweiligen Mittelwert widerspiegelt. Ein Unternehmensbeispiel zeigt im Fall des Mappings ein historisch bedingtes Wachstum der Verbindungen innerhalb des Unternehmens, gepaart mit einer schlechten Dokumentation. Das hat zur Folge, dass nicht alle Verbindungen eindeutig nachzuverfolgen sind.

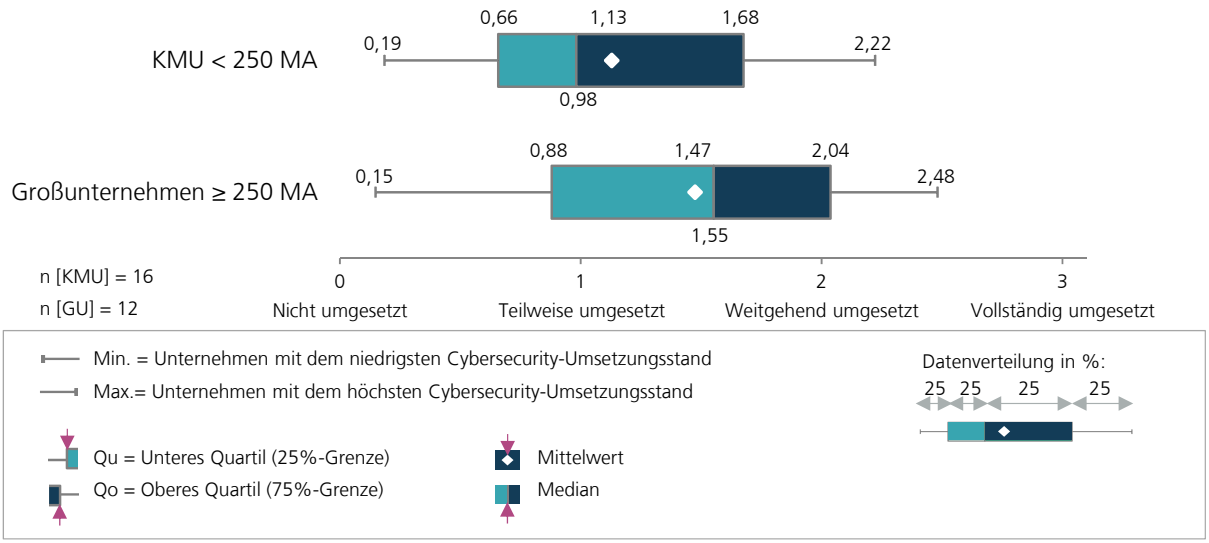

Abbildung 9: Umsetzungsstand aller Cybersecurity-Praktiken in der ACKM-Domäne

Besonders die Institutionalisierung der Aktivitäten, also ihre Verankerung in den ersten drei Methodenzielen, wurde von mehr als der Hälfte der teilnehmenden KMU nicht umgesetzt. Im Netzdiagramm (Abbildung 11) betrachtet konnten weder die teilnehmenden KMU noch die Großunternehmen den empfohlenen Umsetzungsstand vollständig erreichen. Die Großunternehmen schnitten in den meisten Bausteinen besser als die KMU ab. Basiskonfigurationen für inventarisierte Assets sind teilweise (KMU: 1,75) und weitgehend (Großunternehmen: 2,25) vorhanden, um dieselbe Konfiguration bei identischen Assets zu gewährleisten (vgl. Baustein ACKM-2.1a). Beim Einspielen von Basiskonfigurationen auf Produktionsanlagen werden die IT-Schutzziele nur zum Teil betrachtet. Produktionsanlagen von Fremdunternehmen wirken wie eine Art Blackbox für Unternehmen: Das heißt, dass ein Unternehmen darauf vertrauen muss, was der Hersteller vorkonfiguriert und vorinstalliert hat. Die Hersteller von Produktionsanlagen dokumentieren jedoch die eingestellten Parameter häufig nur unzureichend.

Falls Parameter-Änderungen an Produktionsanlagen durchgeführt werden, dokumentieren Unternehmen diese Änderungen zwar regelmäßig, testen sie jedoch nicht hinsichtlich der Schutzziele (Vertraulichkeit, Integrität und Verfügbarkeit), sondern schätzen sie in einem Best-Practice-Verfahren nur ab (vgl. Bausteine ACKM-3.1a-3.3g). Der Grund für dieses

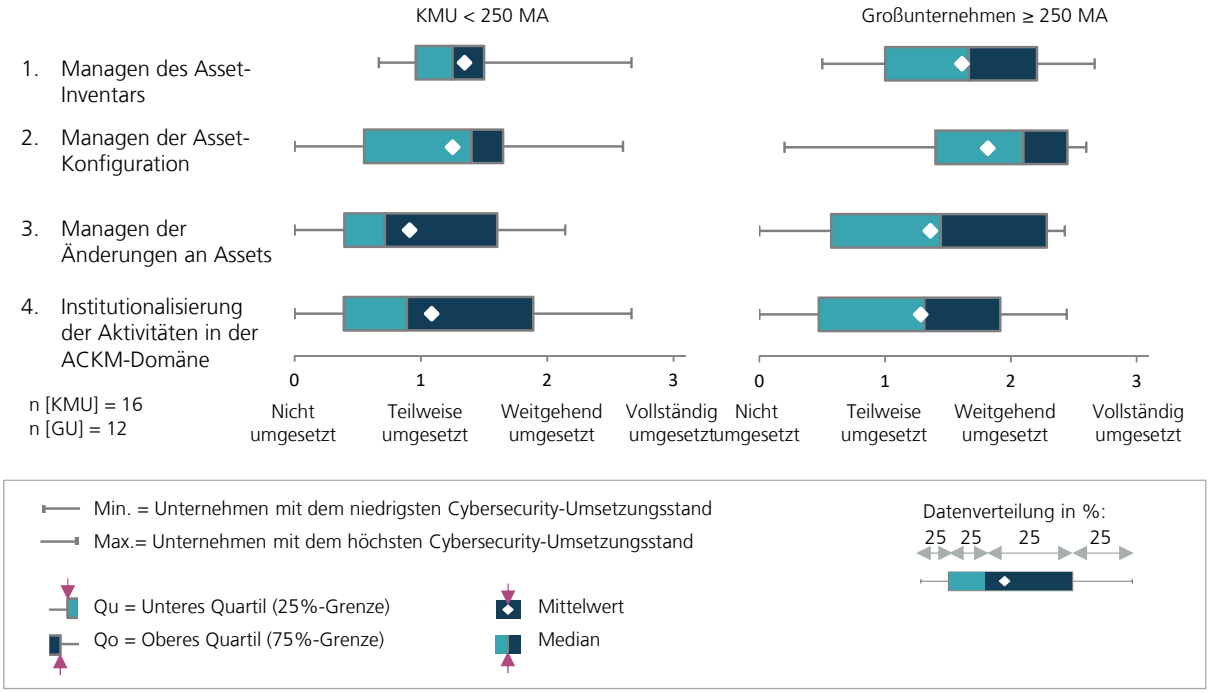

Abbildung 10: Umsetzungsstand der Methoden- und Managementziele in der ACKM-Domäne [35]

Vorgehen liegt in der Vermeidung von Produktionsstillständen. Ein weiterer Grund für die fehlenden Tests von Änderungen liegt darin, dass die Wahl für Anlagen in der Produktion nach dem Best-of-Breed-Prinzip erfolgt. Das bedeutet, es werden individuelle Lösungen je Anwendungsbereich identifiziert und in die bestehende Infrastruktur integriert. Dadurch entsteht ein sehr heterogenes Maschinenbild, das es nicht erlaubt, mit jedem Maschinenhersteller eine eigene Testumgebung (»Sandbox«) zu entwickeln. Ebenfalls wird der Nutzen einer alleinigen Konzentration auf die Verfügbarkeit einer Anlage von einem Experten eines teilnehmenden Maschinenbauunternehmens kritisch bewertet.

Die Segmentierung und Isolierung von IT- und OT-Netzwerken sowie deren Assets ist allen befragten Unternehmen zwar ein Begriff, wird jedoch besonders von KMU nicht durchgängig angewendet. So sehen diese vielfach noch keine Notwendigkeit, da ihre Produktion keine direkte Verbindung zum Internet aufweist und daher nicht gesondert segmentiert werden muss. Die Herstellung eines vertikalen, ebenenübergreifenden Zugriffs in der Automatisierungspyramide in beide Richtungen – bei gleichzeitiger Trennung der Produktionssysteme – stellt besonders die KMU vor eine Herausforderung.

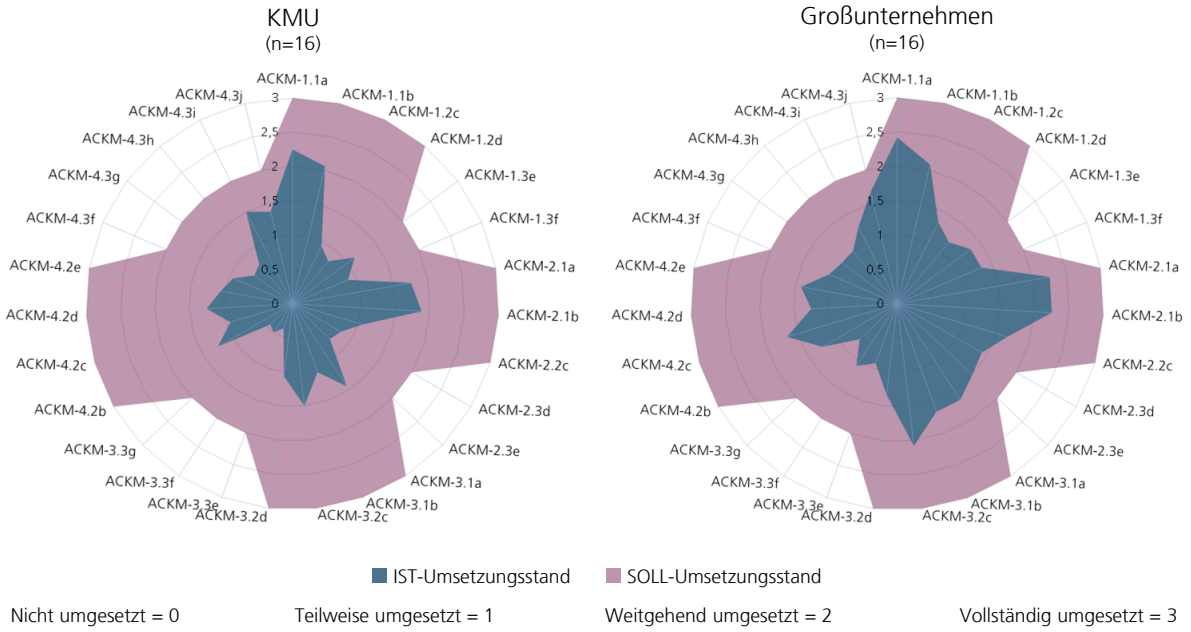

Abbildung 11: IST- und SOLL-Umsetzungsstand der einzelnen Bausteine in der ACKM-Domäne

Zusammenfassung der Ergebnisse der weiteren IT-Sicherheits-Domänen

Großunternehmen, vor allem börsennotierte, verfügen über ein allgemeines Risikomanagement mit gut dokumentierten Handbüchern. Innerhalb des Risikomanagements wird Cybersecurity überwiegend aktiv im Office-Netzwerk angegangen. In der Produktion wurde das Risiko durch Cyberangriffe zwar erkannt, aber nur in wenigen Fällen aktiv ins Visier genommen. Bei den teilnehmenden KMU verhält es sich ähnlich, allerdings fällt hier die Umsetzung der Sicherheitsmaßnahmen im Mittel noch geringer aus. Sowohl die Großunternehmen als auch die KMU haben Schwierigkeiten, die Bedrohungslandschaft durch Cyberangriffe ganzheitlich zu erfassen. Zitat eines Befragten: »Man kann überall ansetzen sozusagen.« – es wird gescheut, in einen Initialaufwand zu investieren. Der Umgang mit dem Risiko von Cyberangriffen hat eher eine reaktive als eine proaktive Natur.

Im Vergleich zu allen anderen Domänen erreichte die Identitäts- und Zugangsmanagement-Domäne sowohl bei den KMU als auch bei den Großunternehmen den höchsten Umsetzungsstand. In dieser Domäne existieren bereits ausgereifte Verzeichnisdienste wie Windows Active Directory (AD) und Standard-Software wie SAP, die den Unternehmen helfen, den gesamten Lifecycle – von der Erstellung bis zur Deaktivierung – eines logischen und physischen Zugangs zu managen. Ähnlich der ACKM-Domäne und der Verwaltung von Assets haben sich Prozesse zur Verwaltung von Zugängen und Identitäten in den Unternehmen etabliert. Einige wenige Unternehmen wenden zusätzlich das Need-to-Know-Prinzip bei der Zugangsvergabe an. Ein Großunternehmen zeigte Probleme bei der Vergabe von Zugängen an Produktionsstandorten außerhalb Deutschlands oder Europas auf. Aufgrund des mangelnden Bewusstseins für Security – vor allem im asiatischen und arabischen Raum – werden laut dem IT-Administrator Sicherheitsrisiken bei schlecht administrierten Zugängen falsch eingeschätzt. Das Verständnis für Security ist seiner Meinung nach in Europa, den USA und auch in Indien auf einem ähnlichen Level.

Eine weitere Herausforderung besteht in dem »Spagat« zwischen Security und der Nutzerfreundlichkeit der IT-Netzinfrastruktur. Konkret bedeutet das bereits, etwa den Umgang mit USB-Sticks zu regeln: Einerseits würde das generelle Verbot aller USB-Sticks im Unternehmen die Nutzerfreundlichkeit drastisch senken, andererseits würde die Zulassung eines unkontrollierten Einsatzes von USB-Sticks die Sicherheit deutlich gefährden.

Die Ergebnisse der Bedrohungs- und Schwachstellenmanagement-Domäne ähneln denen der Risikomanagement-Domäne: Während die Großunternehmen über eine strukturierte Vorgehensweise zur Eliminierung von Schwachstellen und Bedrohungen verfügen, wenden die KMU diese Tätigkeiten ad hoc an. Beide überfordert jedoch die Beschleunigung der Update-Zyklen der Assets. Der Umgang mit Schwachstellen an verschiedenen Komponenten weist enorme Unterschiede auf: Während Windows-Komponenten einem aktiven Patch Management unterzogen werden, betreiben die Unternehmen für SPS-Steuerungen de facto kein aktives patchen. Falls dennoch getestet wird, nehmen vor allem die Großunternehmen zum Zeitpunkt des Patchens Support der jeweiligen Hersteller in Anspruch. Jedoch lassen sich die exakten Auswirkungen eines Patches auf eine Anlage nicht vorhersagen. Dies liegt an der bereits in der ACKM-Domäne beschriebenen Schwierigkeit, dass die Unternehmen Testsysteme und Geräte nicht in mehrfacher Ausführung vor Ort haben.

In der Domäne Situationsbewusstsein mussten Unternehmen ihre Aktivitäten rund um das Thema Logging und Monitoring bewerten. Logging und Monitoring werden durchgeführt, aber in keinem umfassenden oder zielführenden Rahmen: Die Produktion wird nicht gesondert betrachtet, sondern es wird unternehmensweit im IT- und OT-Netzwerk protokolliert. Besonders die Großunternehmen setzen sogenannte Security-

Information-and-Event-Management- Systeme ein, die das Unternehmen bei der Überwachung unterstützen. KMU wählen, bedingt durch geringere Ressourcen, einen Alternativweg: Sie sourcen zum Teil die Logging- und Monitoring-Aktivitäten an Dienstleister aus, die periodisch die protokollierten Daten auswerten. Großunternehmen mit einem hohen Datenaufkommen nutzen zwar gängige Logfile-Analyse-Tools, haben jedoch Schwierigkeiten, Schwellwerte für Alarme und Warnungen zu konfigurieren, die das Unternehmen vor Cyberangriffen schützen sollen. Das Normalverhalten eines Netzwerkes zu definieren und Fehlalarme von echten Alarmen zu unterscheiden, muss größtenteils von Hand erledigt werden. Viele Hersteller von Produktionsanlagen kommunizieren den betreibenden Unternehmen nicht klar, was diese überwachen müssen, sollen oder können.

Der Informationsaustausch und die Kommunikation bezüglich Cybersecurity-Themen können insgesamt als nicht ausreichend beschrieben werden: Diese Domäne weist den zweitniedrigsten Umsetzungsstand aller Domänen auf und birgt besonderes Verbesserungspotenzial. Die meisten teilnehmenden Unternehmen, sowohl die Großunternehmen als auch die KMU, vertrauen ausschließlich auf ihre eigenen Ressourcen und informieren sich selbstständig, ohne in einem Austauschnetzwerk aktiv zu sein.

Die Reaktionen auf Cyber-Ereignisse und -Vorfälle und auch die Aktivitäten rund um die Kontinuität der Produktion werden ebenfalls nicht ausreichend umgesetzt. Aufgrund hochentwickelter Angriffsmethoden befürchten die teilnehmenden Unternehmen, dass sie eine Vielzahl an Angriffen nicht erkennen. Ein vorausschauendes Denken, das Vorfälle generell verhindern soll, etabliert sich nur langsam. Präventive Maßnahmen zur Gewährleistung einer kontinuierlichen Produktion werden bei Großunternehmen zunehmend mithilfe eines Business Continuity Managements entwickelt. Obwohl dies von immer mehr Kunden der Großunternehmen gefordert wird, spielen Cybersecurity-Events dabei eine untergeordnete Rolle. Es existieren zwar pro forma Notfallpläne, diese werden jedoch nur in den seltenen Fällen mit Blick auf den Ernstfall getestet. Bei einem Cyberangriff oder Vorfall bevorzugen die Unternehmen intern eine offene Kommunikation. So wird beispielsweise ein CEO-Fraud-Angriff intern via E-Mail kommuniziert. Die IT-Leiter motivieren Mitarbeitende, jedes verdächtige Ereignis zu melden. Die Unternehmen sind bestrebt eine »No-Blame-Culture« zu etablieren, um den Mitarbeitenden die Angst vor möglichen Konsequenzen zu nehmen.

Der Umgang mit Cybersecurity-Praktiken in Bezug auf die komplette Lieferkette ist weder den befragten KMU noch den Großunternehmen vertraut. Bei der Beschaffung neuer Anlagen werden Security-Anforderungen im Lastenheft nur in den seltenen Fällen aufgeführt. Ebenfalls wird die IT-Abteilung selten in Beschaffungsprozesse involviert. Verantwortlichkeiten, wer für die Sicherheit der Anlage nach der Auslieferung zuständig ist, sind zwischen dem Hersteller und dem Betreiber einer Anlage nur unzureichend geregelt. Darüber hinaus vertrauen die Betreiber der Anlagen zurzeit auf die Versprechen der Hersteller, dass die ausgelieferte Anlage sicher ist. Es werden keine die Security betreffenden Abnahmeprüfungen oder Security-Audits durchgeführt. Die befragten Großunternehmen weisen in dieser Domäne den niedrigsten Umsetzungsstand aller Domänen auf.

Trotz des geringen Umsetzungsstands der Domäne Risikofaktor Mensch sind Schulungen zur Cybersecurity ein Thema bei den befragten Unternehmen. Häufig scheitert es jedoch an der konsequenten Durchführung: Es wird lediglich im Intranet auf die Existenz von Schadsoftware hingewiesen, aber eine aktive, sich wiederholende Schulung findet entweder gar nicht oder nur selten statt. Viele Mitarbeitende wiegen sich in einer trügerischen Sicherheit, dass die IT-Abteilung sie vor Risiken schützen wird. Bei der Einstellung neuer Mitarbeiterinnen und MItarbeiter verfügen besonders die befragten Großunternehmen über schriftliche Einweisungen in die IT, die von den Arbeitnehmenden unterzeichnet werden müssen. Jedoch wird in dieser Einweisung, falls überhaupt, Security nur

am Rand erwähnt. Eine besondere Herausforderung ist, dass bei der Einführung technischer Sicherheitsmaßnahmen die organisatorischen Maßnahmen in Form von Schulungen nicht zu vernachlässigen sind. Die Wahrscheinlichkeit ist sonst sehr hoch, dass Mitarbeitende den Sinn einer neu eingeführten technischen Maßnahme nicht verstehen und diese daher nicht akzeptieren oder sogar umgehen.

In Abbildung 12 sind die übrigen Domänen zusammenfassend quantitativ dargestellt.

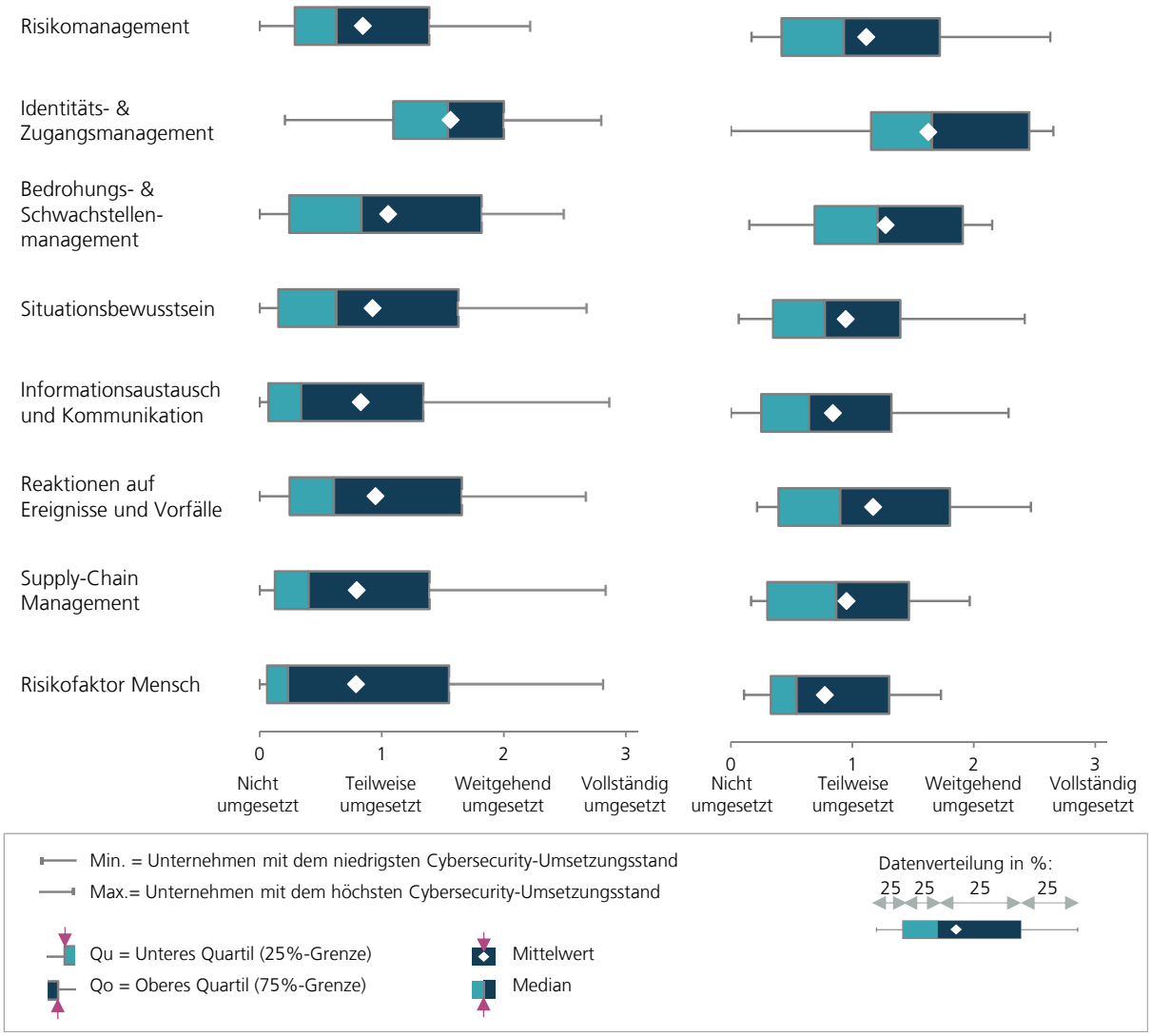

Abbildung 12: Umsetzungsstand der weiteren Domänen

AUSBLICK

Die Untersuchung hat gezeigt, dass mithilfe des Production Security Readiness Check das Sicherheitsniveau der einzelnen Unternehmen im produzierenden Gewerbe detailliert aufgenommen werden kann. Indem der PSRC eigene Schwachstellen aufzeigt, kann dieser somit zur Verbesserung des Sicherheitsniveaus beitragen. Hinsichtlich der Auswertung kann konstatiert werden, dass der Umsetzungsstand der Cybersecurity-Aktivitäten weder in KMU noch in Großunternehmen den geforderten Grad erfüllt. Diesbezüglich herrscht branchenübergreifend enormer Handlungsbedarf – obgleich sich einige Unternehmen in bestimmten Domänen bereits intensiv mit diesem Thema befasst.

In den Interviews erhielt der PSRC durchgängig positives Feedback. Besonders die Aufteilung in verschiedene Domänen gefiel den Unternehmen, da dadurch deutlich wird, auf welche Security-Bereiche sie zukünftig besonderes Augenmerk legen sollten. Ein KMU möchte mithilfe des PSRC der Geschäftsführung vermitteln, welche Maßnahmen für den Ausbau der Cybersecurity im Unternehmen festzulegen sind. Der hohe Detailgrad des Readiness Checks führte jedoch bei KMU ohne eigene IT-Abteilung teilweise bei der Beantwortung der Fragen zu Schwierigkeiten. Für diese Zielgruppe sollte der Umfang und die Komplexität reduziert werden. Eine weitere Möglichkeit besteht darin, den Readiness Check an verschiedene Industriesektoren und deren besondere Anforderungen anzupassen. Die gewählte Datenerhebungsmethode in Form eines Self-Assessments erwies sich grundsätzlich als geeignet.

Den einmalig dokumentierten IST-Umsetzungsstand können Unternehmen zukünftig als Benchmark-Referenz für die weitere Umsetzung von Cybersecurity-Praktiken nutzen. Der Readiness Check kann dafür als Arbeitshilfe in regelmäßigen Zeitabständen zu Rate gezogen werden, da er bei Aktualisierung den Fortschritt in der Etablierung und Verbesserung der eigenen Cybersecurity-Praktiken dokumentieren kann. Er ermöglicht den Unternehmen, jederzeit ihr aktuelles Sicherheitsniveau abzufragen und die weiterhin vorhandenen Schwachstellen zu erkennen.

Besonders der Wandel der klassischen Automatisierungspyramide zum Automatisierungsnetzwerk und darüber hinaus zum Cyberphysischen System wird weitere Herausforderungen an neue Technologien nach sich ziehen. So werden beispielswweise die Eigenschaften des neuen Mobilfunkstandards 5G – hohe Datenraten, geringe Latenz – von hoher Bedeutung sein und neue Möglichkeiten bieten, Feldgeräte aus kritischen Infrastrukturen drahtlos anzubinden. In diesem Zusammenhang wird Cybersecurity einen noch höheren Stellenwert einnehmen [39]. Dann wird sich zeigen, in welchem Umfang der PSRC weiterhin unterstützend eingesetzt werden kann. Insgesamt kann der Production Security Readiness Check schon heute einen wichtigen Beitrag zu einer sichereren IT- und OT-Umgebung in Unternehmen leisten – gerade im Zuge der zunehmenden Digitalisierung und der damit wachsenden Bedeutung der Cybersecurity.

AUTOREN

Raphael Kiesel, M.Sc. M.Sc.
Gruppenleiter, Abteilung Produktionsqualität

Timo Heutmann, M.Eng.
Wissenschaftlicher Mitarbeiter, Abteilung Produktionsqualität

Jan Dering, M.Sc.
Masterarbeiter in der Abteilung Produktionsqualität

Alexander Kies, M.Sc.
Wissenschaftlicher Mitarbeiter, Abteilung Produktionsqualität

Dr.-Ing. Dipl.-Wirt.-Ing. Thomas Vollmer
Leiter der Abteilung Produktionsqualität

Prof. Dr.-Ing. Robert H. Schmitt
Mitglied des Direktoriums des Fraunhofer-Instituts für Produktionstechnologie IPT und Inhaber des Lehrstuhls für Fertigungsmesstechnik und Qualitätsmanagement am WZL der RWTH Aachen.

Danksagung

Für die Unterstützung bei der Ausarbeitung der Studienergebnisse möchten wir insbesondere Prof. Dr. Thomas Russack von der FOM Hochschule für Oekonomie & Management unseren Dank aussprechen.

REFERENZEN

[1] Vereinigung der Bayerischen Wirtschaft e. V. (Hrsg.): Studie – Digitalisierung als Rahmenbedingung für Wachstum. 2017. URL: https://www.prognos.com/uploads/tx_atwpubdb/20170904_Pronos_vbw_Digitalisierungs_als_Rahmbedining_update.pdf [Stand: 19.11.2020].

[2] Presse- und Informationsamt der Bundesregierung (Hrsg.): Digitalisierung gestalten – Umsetzungsstrategie der Bundesregierung. 2018. URL: https://www.bundesfinanzministerium.de/Content/DE/Downloads/Digitalisierung/2018-11-15-Digitalisierung-gestalten.pdf?__blob=publicationFile&v=2 [Stand: 19.11.2020].

[3] McKinsey & Company (Hrsg.): Digitalisierung im Mittelstand erhöht Wachstum in Deutschland um 0,3 Prozentpunkte pro Jahr. 2017. URL: https://www.mckinsey.com/de/news/presse/digitalisierung-im-mittelstand-erhoht-wachstum-in-deutschland-um-03-prozentpunkte-pro-jahr [Stand: 15.01.2019].

[4] Statistisches Bundesamt (Hrsg.): Bruttoinlandsprodukt 2018 für Deutschland. Begleitmaterial zur Pressekonferenz am 15. Januar 2019 in Berlin. 2019. URL: https://www.destatis.de/DE/Presse/Pressekonferenzen/2019/BIP2018/pressebroschuere-bip.pdf?__blob=publicationFile [Stand: 19.11.2020].

[5] Lichtblau, K.; Schleiermacher, T.; Goecke, H.; Schützdeller, P.: Digitalisierung der KMU in Deutschland. Konzeption und empirische Befunde. 2018. URL: https://www.iwconsult.de/fileadmin/user_upload/projekte/2018/Digital_Atlas/Digitalisierung_von_KMU.pdf [Stand: 19.11.2020].

[6] Icks, A.; Schröder, C.; Brink, S.; Dienes, C.; Schneck, S.: Digitalisierungsprozesse von KMU im Verarbeitenden Gewerbe. Bonn: Institut für Mittelstandsforschung (IfM) Bonn, 2017. http://hdl.handle.net/10419/156246

[7] Deutsche Telekom AG (Hrsg.): Security on the Industrial Internet of Things. How companies can defend themselves against cyber attacks. 2016. URL: https://www.t-systems.com/blob/269626/1c7f8ae72c3e86714a4ffc47aeaef407/DL_WP_Security%20M2M.pdf [Stand: 19.11.2020].

[8] Hahn, A.: Operational Technology and Information Technology in Industrial Control Systems. In: Colbert, E. J. M.; Kott, A. (Hrsg.): Cyber-security of SCADA and Other Industrial Control Systems. Cham: Springer International Publishing, 2016, S. 51-68.

[9] Kaspersky Lab ICS CERT (Hrsg.): Threat Landscape for Industrial Automation Systems in H2 2017. 2018. URL: https://ics-cert.kaspersky.com/media/KL_ICS_REPORT_H2-2017_FINAL_EN_22032018.pdf [Stand: 19.11.2020].

[10] Center for Strategic & International Studies (Hrsg.): Significant Cyber Incidents. o. J. URL: https://www.csis.org/programs/cybersecurity-and-governance/technology-policy-program/other-projects-cybersecurity [Stand: 15.01.2019].

[11] F-Secure GmbH (Hrsg.): Live Security Studie 2017/2018. Eine repräsentative Untersuchung von Bitkom Research im Auftrag von F-Secure. 2018. URL: https://blog.f-secure.com/wp-content/uploads/2018/05/f-secure-live-security-studie-2017_2018.pdf [Stand: 19.11.2020].

[12] Bundesministerium für Wirtschaft und Energie (Hrsg.): IT-Sicherheit für die Industrie 4.0. Produktion, Produkte, Dienste von morgen im Zeichen globalisierter Wertschöpfungsketten. Studie im Auftrag des Bundesministeriums für Wirtschaft und Energie. Abschlussbericht. 2016. URL: https://www.bmwi.de/Redaktion/DE/Publikationen/Studien/it-sicherheit-fuer-industrie-4-0.pdf?__blob=publicationFile&v=4 [Stand: 19.11.2020].

[13] Stobitzer, C.: Schutzziele der Informationssicherheit. 2017. URL: http://www.kryptowissen.de/schutzziele.php [Stand: 27.07.2018].

[14] Eckert, C.: IT-Sicherheit. Konzepte - Verfahren - Protokolle. 8. Aufl. München: De Gruyter, 2013.

[15] Holznagel, B.: Recht der IT-Sicherheit. München: Beck, 2003.

[16] Gadatsch, A.; Mangiapane, M.: IT-Sicherheit. Digitalisierung der Geschäftsprozesse und Informationssicherheit. Wiesbaden: Springer Vieweg, 2017.

[17] Dustdar, S.; Gall, H.; Hauswirth, M.: Software-Architekturen für Verteilte Systeme. Prinzipien, Bausteine und Standardarchitekturen für moderne Software. Berlin, Heidelberg: Springer, 2003.

[18] Bedner, M.; Ackermann, T.: Schutzziele der IT-Sicherheit. In: Datenschutz und Datensicherheit - DuD. 34. Jg., 2010, Nr. 5, S. 323–328. http://doi.org/10.1007/s11623-010-0096-1

[19] Schneider, F.: IT-Sicherheit 2018: Pflichten für Unternehmen. 2018. URL: https://www.cmshs-bloggt.de/tmc/it-recht/it-sicherheit-2018-sicherheit-fuer-unternehmen/ [Stand: 12.07.2018].

[20] TeleTrusT - Bundesverband IT-Sicherheit e.V. (Hrsg.): IT-Sicherheitsgesetz und Datenschutz-Grundverordnung: Handreichung zum "Stand der Technik" technischer und organisatorischer Maßnahmen. Revidierte und erweiterte Ausgabe 2018. 2018. URL: https://www.teletrust.de/fileadmin/docs/fachgruppen/ag-stand-der-technik/TeleTrusT-Handreichung_Stand_der_Technik_-_Ausgabe_2018.pdf [Stand: 17.07.2018].

[21] Bundesamt für Sicherheit in der Informationstechnik – BSI (Hrsg.): Schutz Kritischer Infrastrukturen durch IT-Sicherheitsgesetz und UP KRITIS. 2017. URL: https://www.bsi.bund.de/

SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Schutz-Kritischer-Infrastrukturen-ITSig-u-UP-KRITIS.pdf?__blob=publicationFile&v=7 [Stand: 19.11.2020].

[22] Bundesministerium für Wirtschaft und Energie (BMWi) (Hrsg.): IT-Security in der Industrie 4.0. Handlungsfelder für Betreiber. Leitfaden. 2016. URL: https://www.plattform-i40.de/PI40/Redaktion/DE/Downloads/Publikation/leitfaden-it-security-i40.pdf?__blob=publicationFile [Stand: 19.11.2020].

[23] Heinrich, B.; Linke, P.; Glöckler, M.: Grundlagen Automatisierung. Sensorik, Regelung, Steuerung. 2., überarbeitete und erweiterte Auflage. Wiesbaden: Springer Vieweg, 2017.

[24] INAUT Automation GmbH (Hrsg.): Ganzheitliche Lösung. o. J. URL: http://www.invilution.com/ganzheitliche-loesung [Stand: 12.08.2018].

[25] Wiesel, C.: Was ist wo los im Netz? Permanente und passive Analyse der Kommunikationsqualität in Profinet-Netzwerken. In: messtec drives Automation. 25. Jg., 2017, Nr. 10, S. 14-16.

[26] Stouffer, K.; Pillitteri, V.; Lightman, S.; Abrams, M.; Hahn, A.: Guide to Industrial Control Systems (ICS) Security. Supervisory Control and Data Acquisition (SCADA) systems, Distributed Control Systems (DCS), and other control system configurations such as Programmable Logic Controllers (PLC). 2015. http://dx.doi.org/10.6028/NIST.SP.800-82r2

[27] Vogt, M.; Sherman, A.: 3D-Snapshot-Kameradaten in der Industrie: Wie Edge-Computing die optimale Datenbereitstellung ermöglichen kann. Sick AG Whitepaper. 2018. URL: https://cdn.sick.com/media/docs/1/41/041/Whitepaper_3D_SNAPSHOT_CAMERA_DATA_IN_INDUSTRY_de_IM0077041.PDF [Stand: 19.11.2020].

[28] Niemann, K.-H.; Hoh, M.: Anforderungen an die IT-Sicherheit von Feldgeräten. Schutzlösungen für hoch vernetzte Produktionsanlagen In: atp edition. 59. Jg., 2017, Nr. 12, S. 42-53.

[29] Khondoker, R.; Larbig, P.; Scheuermann, D.; Weber, F.; Bayarou, K.: Addressing Industry 4.0 Security by Software-Defined Networking. In: Zhu, S.; Scott-Hayward, S.; Jacquin, L.; Hill, R. (Hrsg.): Guide to Security in SDN and NFV. Challenges, Opportunities, and Applications. Cham: Springer International Publishing, 2017, S. 229-251. https://doi.org/10.1007/978-3-319-64653-4_9

[30] Fireeye iSight Intelligence (Hrsg.): Overload. Critical lessons from 15 years of ICS Vulnerabilities. 2016 Industrial Control Systems (ICS) Vulnerability Trend Report. 2016. URL: https://www.tripwire.com/-/media/tripwiredotcom/files/solution-brief/ics-vulnerability-trend-report-final.pdf?rev=f9b8f49716224a10a1639d36582ec269 [Stand: 19.11.2020].

[31] Kaspersky Lab ICS CERT (Hrsg.): Threat Landscape for Industrial Automation Systems in the second half of 2016. 2017. URL: https://ics-cert.kaspersky.com/reports/2017/03/28/threat-landscape-for-industrial-automation-systems-in-the-second-half-of-2016/ [Stand: 19.11.2020].

[32] European Union Agency for Network and Information Security: Communication network dependencies for ICS/SCADA Systems. 2017. https://doi.org/10.2824/397676

[33] Bundesamt für Sicherheit in der Informationstechnik (BSI) (Hrsg.): Die Lage der IT-Sicherheit in Deutschland 2017. 2017. URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2017.pdf?__blob=publicationFile&v=4 [Stand: 19.11.2020].

[34] Department of Homeland Security (Hrsg.): Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies. Industrial Control Systems Cyber Emergency Response Team. 2016. URL: https://us-cert.cisa.gov/sites/default/files/recommended_practices/NCCIC_ICS-CERT_Defense_in_Depth_2016_S508C.pdf [Stand: 19.11.2020].

[35] U.S. Department of Energy (Hrsg.): Cybersecurity Capability Maturity Model (C2M2). Version 1.1. 2014. URL: https://www.energy.gov/sites/prod/files/2014/03/f13/C2M2-v1-1_cor.pdf [Stand: 19.11.2020].

[36] Norm DIN EN ISO/IEC 27001:2017-06. Informationstechnik - Sicherheitsverfahren - Informationssicherheitsmanagementsysteme - Anforderungen. https://dx.doi.org/10.31030/2634923

[37] National Institute of Standards and Technology (Hrsg.): Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. 2018. https://doi.org/10.6028/NIST.CSWP.04162018

[38] Bundesamt für Sicherheit in der Informationstechnik (Hrsg.): BSI-Standard 200-2. IT Grundschutz-Methodik. 2017. URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/standard_200_2.pdf?__blob=publicationFile&v=7 [Stand: 19.11.2020].

[39] Ahmad, I.; Kumar, T.; Liyanage, M.; Okwuibe, J.; Ylianttila, M.; Gurtov, A.: 5G security: Analysis of threats and solutions. In: Institute of Electrical and Electronics Engineers (Hrsg.): 2017 IEEE Conference on Standards for Communications and Networking (CSCN). 2017 IEEE Conference on Standards for Communications and Networking (CSCN) took place 18-20 September 2017 in Helsinki, Finland. Piscataway: IEEE, 2017, S. 193-199. https://doi.org./ 10.1109/CSCN.2017.8088621

Cybersecurity in der vernetzten Produktion
Whitepaper Fraunhofer IPT
Copyright © 2020

Autoren
Raphael Kiesel, Timo Heutmann,
Jan Dering, Alexander Kies,
Thomas Vollmer, Robert H. Schmitt

Fraunhofer-Institut für
Produktionstechnologie IPT
Steinbachstraße 17
52074 Aachen
Telefon +49 241 8904-0
info@ipt.fraunhofer.de
www.ipt.fraunhofer.de

Ihr Kontakt
Dr.-Ing. Dipl.-Wirt.-Ing. Thomas Vollmer
Abteilungsleiter Produktionsqualität
Telefon +49 241 8904-332
thomas.vollmer@ipt.fraunhofer.de

ISBN 978-3-00-067180-7
DOI: 10.24406/ipt-n-605817