www.fir.rwth-aachen.de

WHITEPAPER

Cybersicherheit und Schwachstellen in produzierenden Unternehmen

Jacques Engländer · Lars Kaminski · Anna Majchrzak · Martin Bülskämper
Jan Hicking · Frederik Buchwald · Joel Mahns · Carina Popov

fir an der RWTH Aachen

25 YEARS OF EXCELLENCE | MHP A PORSCHE COMPANY

Impressum

Autoren:
Jacques Engländer · FIR e. V. an der RWTH Aachen
Lars Kaminski · FIR e. V. an der RWTH Aachen
Anna Majchrzak · FIR e. V. an der RWTH Aachen
Martin Bülskämper · FIR e. V. an der RWTH Aachen
Dr.-Ing. Jan Hicking · FIR e. V. an der RWTH Aachen
Frederik Buchwald · MHP Management- und IT-Beratung
Joel Mahns · MHP Management- und IT-Beratung
Carina Popov · MHP Management- und IT-Beratung

Bildnachweise:
Titelbild: © Tierney – stock.adobe.com; Grafiken: © FIR e. V. an der RWTH Aachen

Gender

Aus Gründen der besseren Lesbarkeit wird auf die gleichzeitige Verwendung der Sprachformen männlich, weiblich und divers (m/w/d) verzichtet. Sämtliche Personenbezeichnungen gelten gleichermaßen für alle Geschlechter.

Lizenzbestimmungen/Copyright

FIR e. V. an der RWTH Aachen
Campus-Boulevard 55
52074 Aachen
Tel.: +49 241 47705-0
E-Mail: info@fir.rwth-aachen.de
www.fir.rwth-aachen.de

MHP Management- und IT-Beratung
Film- und Medienzentrum
Königsallee 49
71638 Ludwigsburg
E-Mail: info@mhp.com
www.mhp.com

Inhaltsverzeichnis

Management-Summary

Durch die steigende Vernetzung in produzierenden Unternehmen nimmt die potenzielle Gefahr durch Cyberangriffe zu. Die meisten kleinen und mittleren Unternehmen (KMU) sind sich heute bewusst, dass hierbei nicht mehr ausschließlich Großkonzerne ein beliebtes Angriffsziel darstellen. Durch automatisierte Malware-Kampagnen und die wachsende Anzahl von Cyberangriffen rücken alle Akteure der Wertschöpfungskette produzierender Unternehmen zunehmend in das Visier von Angreifern – dabei können KMU direkt oder indirekt, zur Schädigung ihrer Partner, angegriffen werden.

Die steigende Bedrohungslandschaft ist allerdings nicht die einzige Herausforderung, mit der sich KMU konfrontiert sehen. Besonders schwerwiegend und besorgniserregend ist ihr Umgang mit Cybersicherheit: Viele KMU setzen sich trotz zunehmender Digitalisierung bislang nur unzureichend mit ihrer Cybersicherheit auseinander. Durch die Verschmelzung unterschiedlicher Domänen steigt nicht nur die Komplexität der Technologien, sondern auch die der Prozesse sowie der Organisation in Unternehmen. Die Sicherheit von Systemen definiert sich nicht mehr nur über einzelne Komponenten, sondern durch die Sicherheit des unternehmensübergreifenden Gesamtsystems. Klassische Lösungsansätze zur Absicherung einzelner Komponenten decken die gestiegenen Schutzanforderungen nicht mehr ausreichend ab.

Um KMU einen selbständigen und pragmatischen Einstieg in die Thematik zu ermöglichen, muss diese Komplexität beherrschbar gemacht werden. Aus Sicht der Cybersicherheit darf die Komplexität jedoch nicht dadurch reduziert werden, relevante Aspekte zu ignorieren. Es bedarf neuer und angepasster Sichtweisen, die KMU den Einstieg erleichtern. Der Ansatz, der durch eine Zusammenarbeit von *MHP* und *FIR* entstanden ist, steht hiermit künftig Geschäftsführungen und Entscheidern in KMU zur Verfügung, um den Nutzen ihrer schützenswerten Assets ihrem Cyberrisiko gegenüberzustellen. Durch die Skalierbarkeit des Ansatzes lassen sich einfach, schnell und sicher Verbesserungspotenziale aufdecken und Investitionen nachvollziehbar rechtfertigen.

1 Einleitung

Digitalisierung fördert nicht nur die Steigerung von Effizienz und Agilität, sondern fungiert als Triebfeder für Innovationen und ist damit Garant für Wettbewerbsfähigkeit und Performanz in Unternehmen jeder Branche. Durch die zunehmende Vernetzung und Digitalisierung vormals analoger, entkoppelter Systeme nimmt die Komplexität der IT durch vertikale und horizontale Integration in der Wertschöpfung erheblich zu. Mit Blick auf die zunehmende digitale Transformation und Vernetzung produzierender Unternehmen gewinnt das Thema Cybersicherheit immer mehr an Bedeutung. Besonders deutlich wird dies an der zunehmend datengetriebenen Produktion: Maschinen produzieren heute große Mengen von Daten und kommunizieren diese über diverse Schnittstellen zur weiteren Datenverarbeitung. So produziert beispielsweise jede der 2.000 Druckmaschinen der Heidelberger Druckmaschinen AG am Tag 4 Millionen Datensätze, was insgesamt circa 600 Gigabyte entspricht[1]. Damit einhergehend bekommen auch die Themen **Datensicherheit** sowie **-integrität** eine stärkere Bedeutung, weil die Wertschöpfungsfähigkeit des Unternehmens vermehrt davon abhängt[2]. Daher muss Cybersicherheit in produzierenden Unternehmen völlig neu gedacht werden – denn je höher das Aufkommen an Daten und Schnittstellen ist, desto mehr Schwachstellen entstehen und desto größer werden auch die Angriffsflächen für potenzielle Angreifer[3].

Potenzielle Schwachstellen liegen allerdings nicht nur innerhalb des Unternehmens, sondern können auch durch die vermehrte Vernetzung im Sinne einer Öffnung der Unternehmensgrenzen für Drittanbieter wie externe Dienstleister, Berater, Zulieferer, Forschungs- und Kooperationspartner oder auch durch den Kunden selbst entstehen. Hier ist es entscheidend, abzuwägen, inwieweit die Unternehmensgrenzen geöffnet werden sollten, sodass ein wertstiftender Austausch möglich ist, ohne aber das Kerngeschäft des Unternehmens zu gefährden. Gerade KMU stehen vor der Herausforderung, den Status quo ihrer Cybersicherheit korrekt einzuschätzen und adäquate Sicherheitslösungen umzusetzen. Oftmals wird Cybersicherheit noch nicht als geschäftskritischer Baustein im Unternehmen wahrgenommen, da sich in dieser Hinsicht noch keine ausreichende Sicherheitskultur etabliert hat[4]. Um adäquate technische und organisatorische Maßnahmen umsetzen zu können, bedarf es neben einem langfristigen Investment auch entsprechenden Fachpersonals, dessen Akquise sich als schwer erweisen kann[5].

Alleine durch die COVID-19-Pandemie konnte im Zeitraum von März bis Mai 2020 **eine Steigerung** von Scam- und Malware-Angriffen **um 600 %** festgestellt werden. Angreifer nutzen dazu die Unsicherheit der betroffenen Personen aus.[6] Google bestätigte, im April 2020 **täglich schätzungsweise rund 18 Millionen Malware- und Phishing-E-Mails an Unternehmen mit Bezug zu COVID-19 geblockt** zu haben[7]. Dies untermauert, wie wichtig es ist, die Kontrolle über Informationen und die **Absicherung wichtiger Infrastruktur sicherzustellen**[8].

Vor diesem Hintergrund wird deutlich, dass Resilienz und Performanz von KMU mit der Implementierung eines ganzheitlichen Ansatzes für Cybersicherheit einhergehen. Wie können sich nun KMU, die über geringe personelle wie finanzielle Kapazitäten verfügen, den Herausforderungen ihrer internen Datensicherheit adäquat stellen? Dazu gibt es bereits zahlreiche Rahmenwerke, die sich mit Fragestellungen der Cybersicherheit in Kombination mit Sicherheitslösungen und umzusetzenden Maßnahmen beschäftigen. Gängige Rahmenwerke wie die BSI-Standards, das IT-Grundschutz-Kompendium 2021, die DSGVO, IEC 62443 und RAMI4.0 bieten wissenschaftlich fundierte und ganzheitliche Vorgehensweisen an. Allerdings sind diese Rahmenwerke äußerst umfangreich und vielfach zu komplex, um es KMU zu ermöglichen, ein wirksames Management der Cybersicherheit zu betreiben[9]. Sie sind häufig wenig anwenderfreundlich konzipiert, bieten wenig Raum für nutzerzentrierte Anpassungen und richten sich eher an Großkonzerne oder Institute, die beispielsweise bereits über eine Abteilung für IT-Sicherheit verfügen. Gerade KMU fehlt es überwiegend an Kenntnissen über ihre

[1] s. Beigl et al. 2015, S. 12
[2] s. Niehues et al. 2017, S. 151f.
[3] s. Pohlmann 2020, S. 61 f.
[4] s. Henseler-Unger u. Hillebrand 2018, S. 689
[5] s. Müller 2014, S. 73 f. und S. 701
[6] s. Gallagher u. Brandt 2020
[7] s. Kumaran u. Lugani 2020
[8] s. Lallie et al. 2021, S. 13 f.
[9] s. Engländer u. Heimes 2020, S. 51

eigene Ausgangssituation bei der digitalen Transformation. Dadurch fällt es ihnen schwer, die eigenen Cybersicherheitsschwachstellen zu identifizieren oder auch den Umfang eingeholter Beratungsdienstleistungen zu bewerten. Die mangelhafte Informationslage über die eigene aktuelle Situation führt darüber hinaus dazu, dass Empfehlungen externer Dienstleister sehr allgemeine und konservative Lösungen beinhalten. Diese Verbesserungsvorschläge sind nicht auf die individuellen Sicherheitsanforderungen von KMU zugeschnitten und stehen somit in einem schlechten Kosten-Nutzen-Verhältnis für die betreffenden Unternehmen.

Mit diesem Whitepaper wird eine Grundlage geschaffen, um KMU zu befähigen, ihre Cybersicherheit eigenständig und möglichst kostennutzeneffizient zu gestalten. Im Vordergrund stehen dabei die Schwachstellen der zu schützenden Betriebsgüter (Assets). Nachfolgend sind unter diesen Assets all diejenigen IT-getriebenen Elemente zu verstehen, die entweder durch eigene Wertschöpfung oder unterstützende Funktionalitäten zur Wertschöpfung des Unternehmens beitragen. Dazu zählen physische Ressourcen wie Maschinen und Anlagen, digitale Ressourcen wie IT-Systeme und Anwendungen, Netzwerke sowie ferner Prozesse, Produkte und Dienstleistungen. Das eigentliche Angriffsziel stellt dabei nicht etwa die Maschine als solche dar, sondern ihre anfälligen IoT-fähigen Komponenten wie Gateways oder IIoT-Devices[10]. Im Gegensatz zu Assets, als Primärziel von Cyberkriminalität, sind Bedrohungen sehr dynamisch und ändern sich stetig (beispielsweise Viren, Trojaner, Phishing-Attacken oder Angriffe mit Ransomware). Dagegen bleiben die Ziele eines Angriffs meist gleich – wie etwa das Verschlüsseln von Daten oder die Störung der Kommunikation in der Produktion, was zu kostspieligen Maschinenstillständen führen kann. In den meisten Fällen zwingen die Erpresser die Opfer zu Lösegeldzahlungen.

Ein Trojaner war im Juli 2020 in das Firmennetzwerk des Maschinenbauers *Netzsch* eingedrungen und verschlüsselte nach und nach alle Daten des Unternehmens. Im Zuge dessen musste das Netzwerk komplett heruntergefahren werden, was die Produktion zum Stillstand brachte.[11]

Das von *MHP* und *FIR* entwickelte Konzept lenkt den Blick weg von der Vermeidung einzelner Bedrohungen und stellt den ganzheitlichen Schutz sensibler Daten in den Mittelpunkt des Vorgehens. Welche Folgen Nachlässigkeiten in Bezug auf Cybersicherheit haben können, kann anhand des folgenden Beispielszenarios nachvollzogen werden:

> *In der Buchhaltung wird ein vermeintlich harmloser E-Mail-Anhang geöffnet. Dieser beinhaltet einen Trojaner und infiziert das Computersystem mit Ransomware (dt. Erpressungstrojaner). Aufgrund eines nicht aktuellen Anti-Virenprogramms bleibt der Virus hierdurch unerkannt und verschafft sich umfangreichen Zugriff auf diverse Daten und Software. Von diesem infizierten Computersystem breitet sich der Virus auf das Unternehmensnetzwerk aus und befällt über ungeschützte Kommunikationsschnittstellen eine Maschinensteuerung. Durch ein elektromagnetisches Störsignal manipuliert der Virus eine Anlage, sodass es zum Produktionsstillstand und finanziellem Schaden im mehrstelligen Bereich kommt.*

Zwar hat in diesem Beispiel das Öffnen des E-Mail-Anhangs zu einem Produktionsstillstand geführt, aber letztlich ausgelöst wurde dieser nicht allein durch ein unzureichend geschütztes E-Mail-Postfach. Dieses Beispiel zeigt anschaulich, warum es nicht ratsam ist, das Hauptaugenmerk nur auf einzelne Bedrohungen zu legen, sondern dass erst die Asset-Fokussierung eine ganzheitliche Betrachtung des Themas Cybersicherheit, eine Wahrnehmung des Gesamtbildes aller Gefahren und so letztlich eine zielführende Vorgehensweise gegen vielerlei Bedrohungen ermöglicht.

Um den Herausforderungen der digitalen Transformation für ihre Produktion angemessen begegnen zu können, benötigen KMU einen ganzheitlichen Ansatz, der a) individuell auf ihre spezifische Sicherheitsaffinität bzgl. ihrer Assets ausgerichtet ist, b) dabei möglichst intuitiv, anwenderfreundlich und autonomiestiftend ist sowie c) langfristige, kostennutzeneffiziente Lösungen offeriert. Die dazugehörige Methodik stützt sich auf eine Asset-Taxonomie, die KMU dabei unterstützt, ihre Assets und die damit verbundenen Schwachstellen klar zu definieren sowie passende Maßnahmenempfehlungen herzuleiten.

[10] s. European Union Agency for Network and Information Security (ENISA) 2018, S. 16 f.

[11] s. Völker 2020

2 Cybersicherheit und Schwachstellenstruktur

Für die Entwicklung eines fundierten und individuell einsetzbaren Vorgehens (mit dem Ziel der Verbesserung der Cybersicherheit im jeweiligen Unternehmen) ist es essenziell, zunächst die unternehmenseigenen Assets zu identifizieren, zu strukturieren und zu analysieren. Die Bedrohungen für Unternehmen sind sehr dynamisch und individuell unterschiedlich, weswegen es äußerst schwierig ist, allein darauf basierend ein Schutzkonzept zu entwerfen. Dies gilt insbesondere für KMU, die im Bereich Cybersicherheit über vergleichsweise limitierte Ressourcen verfügen. Da bislang quasi abgeschlossene IT- und Produktionssysteme zunehmend von vernetzten cyber-physischen Systemen abgelöst werden bzw. sich dazu weiterentwickeln, rücken die einzelnen Assets umso mehr in den Vordergrund. Es ist essenziell für ein Unternehmen, jedes einzelne seiner Assets zu kennen und im Gesamtzusammenhang zu verstehen, um Schwachstellen zu erkennen und somit ein individualisiertes Schutzkonzept ableiten zu können. Denn jedes einzelne Asset kann bei einem Cyberangriff als Einfallstor dienen.

Im Folgenden wird die Rolle der Assets im Gesamtdatenfluss eines Unternehmens genauer analysiert und eingeordnet. Als Ausgangspunkt dient hierbei die von der *European Union Agency for Network and Information Security (ENISA)* ausgearbeitete Asset-Taxonomie[12]. Diese Asset-Taxonomie stellt eine Übersicht der relevantesten Assets im Bereich Industrie 4.0 und Smart Manufacturing vor dem Hintergrund der Cybersicherheit dar. Insbesondere berücksichtigt diese Übersicht neben Assets wie zum Beispiel Sensoren, Switches und Software auch Algorithmen und den Menschen als wertschöpfendes Element.

Die horizontale bzw. vertikale Vernetzung von Assets und ihre zunehmenden Funktionalitäten erschweren deren Strukturierung. Um dieses Problem zu lösen, wird basierend auf der ENISA-Asset-Taxonomie eine Asset-Struktur in Form eines „Schwachstellenmodells" entworfen. Dieses setzt sich aus vier Layern (dt. Ebenen) zusammen: Resource-Layer, System-Layer, Application-Layer und Integration-Layer (s. Bild 1). Die Verortung der Assets orientiert sich vor allem an der Funktionsweise der Assets in Bezug auf Daten. Um einen detaillierteren Einblick zu erhalten, werden im Folgenden die genannten Layer inhaltlich definiert sowie einige Beispiele potenzieller Schwachstellen vorgestellt.

[12] S. European Union Agency for Network and Information Security (ENISA) 2018

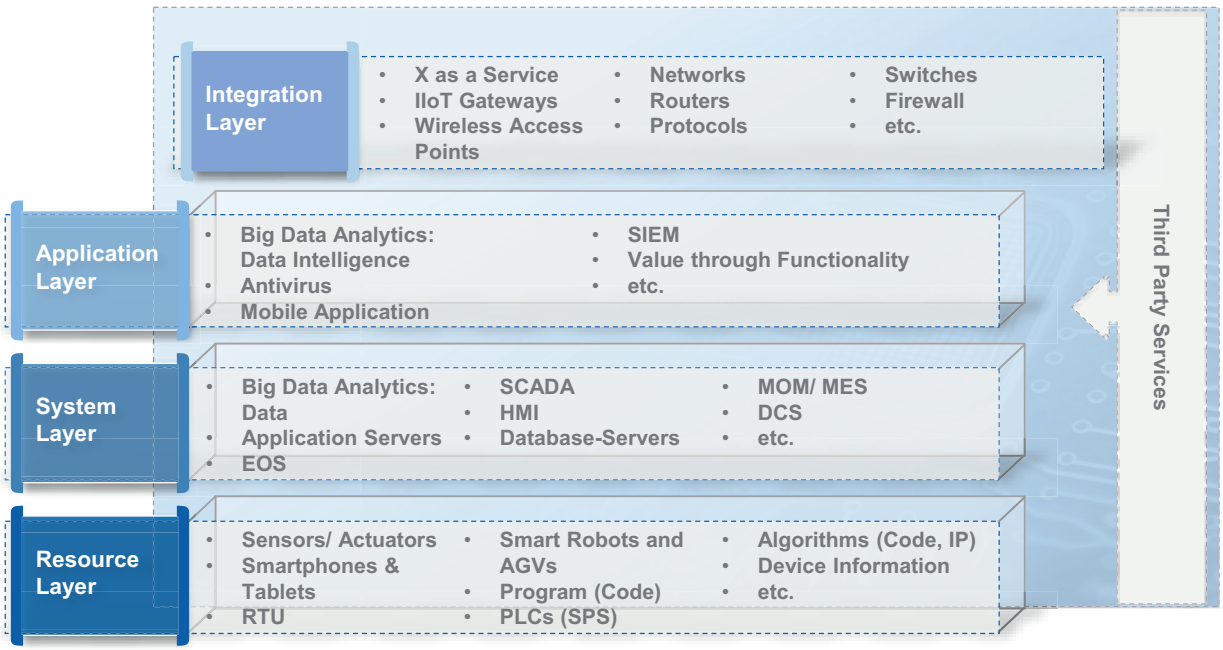

Bild 1: MHP- und FIR-Schwachstellenstruktur zur Einordnung von Assets (eigene Darstellung)

2.1. Resource-Layer

Der **Resource-Layer** beinhaltet produktionsnahe IT-Komponenten von Maschinen, Anlagen und Mitarbeitern inklusive deren Fähigkeiten und Kompetenzen sowie Intelligente Produkte im Feld und Hardware-Infrastruktur für den IT-Betrieb. Integrativ betrachtet, liefern die Ressourcen die physische Basis zum Aufbau eines ganzheitlichen und nachhaltigen Lösungssystems. Die Assets in diesem Layer dienen zur Datenaggregation bzw. als Datenquelle und zur Datenerfassung. Aufgaben von Sensoren und Aktoren innerhalb der Asset-Struktur sind beispielsweise die Erfassung und Weiterleitung von Informationen.

Gefahren entstehen hierbei durch die Interaktion von IoT-Geräten mit ihrer Umgebung. Die Ausrüstung von Fertigungssystemen kann beispielsweise manipuliert werden, indem sich Angreifer physischen Zugriff zu Anlagen verschaffen oder physische Manipulationen vornehmen (z. B. das Ziehen von Steckern), sodass Sensoren und Aktuatoren gestört werden. Dies kann wiederum zu Fehlfunktionen im Regelkreis und dem ganzen angeschlossenen Prozess führen. Ebenfalls sind hochkomplexe Angriffsszenarien denkbar, bei denen die Zeitmessung oder die Stromversorgung eines Chips verändert wird, um den Betrieb des Systems zu manipulieren. Wenn nun Sensoren und Aktoren noch über IP-Adressen und die damit verbundenen Funktionen verfügen, steigt das cyberbezogene Risiko. Schwachstellen in diesen Assets könnten Hackern die Möglichkeit geben, Daten zu verändern bzw. die Datenerfassungsmuster so zu modifizieren, dass der Endverbraucher – sei es ein Mensch oder eine Maschine – getäuscht wird. Im Falle eines „Man-in-the-Middle-Angriffs" sitzt der Angreifer zwischen den kommunizierenden Geräten und leitet die Kommunikation zwischen ihnen weiter. So könnte er z. B. das Schlüsselaustauschprotokoll (viele industrielle Steuerungen tun dies unverschlüsselt) zwischen einem Steuerungssystem und einem Aktuator sabotieren. Demzufolge erweist sich das industrielle Internet der Dinge (kurz aus dem Englischen IIoT) als zweischneidiges Schwert für Sensoren sowie Aktuatoren, da es Hackern leicht gemacht wird, diese zu manipulieren, um in industrielle Netzwerke einzudringen und Chaos zu verursachen. Darüber hinaus beinhaltet der Resource-Layer ein weiteres wichtiges Asset innerhalb der Unternehmensumgebung – die eigenen Mitarbeiter. Insbesondere sie werden von Dritten dazu verleitet, unbewusst Risiken einzugehen und schützenswerte Informationen preiszugeben. Einer der häufigsten Angriffspfade ist das Social Engineering, die soziale Manipulation mit dem Ziel, bestimmte Verhaltensweisen hervorzurufen. Hierdurch können geistiges Eigentum des Unternehmens, der Ruf, die Kunden und die Kollegen geschädigt werden. Datenlecks, durch die Projektnamen, Telefonnummern, E-Mails und Lieferadressen zugänglich gemacht werden, mögen zunächst harmlos erscheinen. Sobald sie jedoch miteinander verknüpft und/oder mit weiteren Informationen kombiniert werden, stellen sie ein hohes Risiko für das Unternehmen, seine Mitarbeiter und seine Kunden dar.

2.2. System-Layer

Mit statischen, sich langsam ändernden betrieblichen Kernsystemen, die das informationstechnologische Rückgrat eines Unternehmens und die digitale Repräsentanz aller betrieblichen Abläufe abbilden, ist der **System-Layer** über dem Resource-Layer verortet. Neben den betrieblichen Kernsystemen sind weitere, singulär datenhaltende Lösungen, wie beispielsweise Datenbanken, auf dem Shopfloor enthalten. Die im System-Layer eingeordneten Assets, wie beispielsweise *Mensch-Maschine-Schnittstelle (HMI), Asset Supervisory Control and Data Acquisition (SCADA)* sowie *Distributed Control System (DCS)* oder auch *Prozessleitsystem (PLS)*, können als Backend verstanden werden.

Zum besseren Verständnis wird im Folgenden eine Schwachstelle im System-Layer anhand von SCADA sowie HMI verdeutlicht:

Eine der vielen Möglichkeiten, über die Angreifer in SCADA-Systeme eindringen können, ist die HMI. Sie stellt somit eine vielschichtige Herausforderung dar. Eine HMI zeigt Maschinendaten an und übermittelt Befehle eines Operators an eine Maschine. Über diese Schnittstelle überwacht ein Operator die auf einem SCADA-System angezeigten Informationen und reagiert auf diese. Da sich die HMI/SCADA-Software im Zeitalter von Industrie 4.0 und IIoT weiterhin in Entwicklung befindet, werden Schwachstellen in der Software bis heute noch ausgenutzt. Regelmäßig kommt es so zu Speicherbeschädigungen, sogenannten klassischen Code-Sicherheitsproblemen. Ebenfalls treten Schwachstellen bei der Verwaltung von Anmeldeinformationen auf, z. B. bei der Verwendung von hartkodierten Passwörtern, deren Speicherung in einem wiederherstellbaren Format (z. B. Klartext) und dem unzureichenden Schutz von Anmeldeinformationen. Fehlende Authentifizierung oder auch Autorisierung und unsichere Standardeinstellungen sowie Code-Injektion-Probleme komplementieren gängige HMI/SCADA-Schwachstellen.

2.3. Application-Layer

Oberhalb des System-Layers ist der **Application-Layer** angeordnet. Hier sind alle nutzerzentrierten Anwendungen verortet, die es einem Benutzer erlauben, auf einfache und intuitive Art mit der Unternehmensressource „Information" wertstiftend zu agieren. Der Application-Layer kann als Frontend bzw. Schnittstelle für den Datennutzer verstanden werden. Darüber hinaus sind die dem Application-Layer zugeordneten Assets durch Software sehr flexibel und verändern sich schnell. Als praxisbezogene Assets können *Mobile Applications, AntiVirus* wie auch *Security Information and Event Management (SIEM)* genannt werden.

Da ein SIEM mittlerweile zur Grundausstattung in den meisten produzierenden Unternehmen gehört, wird es nachfolgend als Praxisbeispiel herangezogen. SIEM als System aggregiert täglich unzählige Sicherheitslogs/ Protokolldaten, die in der gesamten technologischen Infrastruktur des Unternehmens erzeugt werden. Das System identifiziert und kategorisiert daraufhin alle Ereignisse, erkennt effektiv Angriffe und kann diesbezüglich aussagekräftige Informationen liefern. Potenzielle Sicherheitsprobleme und mögliche, bösartige Aktivitäten, die gegen vorgegebene Regelsätze verstoßen, können somit dargestellt werden. Wird ein SIEM gehackt, kann unter Umständen die Arbeitsfähigkeit eines Unternehmens gefährdet sein. Unumgehbare Schwachstellen, wie beispielweise der E-Mail-Server, könnten nicht mehr kontinuierlich unter Berücksichtigung ihrer potenziellen Ausnutzbarkeit überwacht werden. Dies betrifft insbesondere Systeme, die häufig mit dem Internet kommunizieren. An dieser Stelle ist anzumerken, dass sich die beiden zuvor beschriebenen Layer zwar inhaltlich voneinander abgrenzen, sie aber bezogen auf ihre Funktionalitäten vermehrt zusammen betrachtet werden müssen, da mittlerweile viele Assets des System-Layers und des Application-Layers vereint sind.

2.4. Integration-Layer

Als vierter Layer befähigt der **Integration-Layer** ein Unternehmen dazu, interdependente, lose Kopplungen von Systemen herzustellen, die Anwendungs- und weitere Daten bereitstellen. Der Layer stellt die Verfügbarkeit aller relevanten Daten sicher und orchestriert die Verteilung der Daten zwischen den einzelnen Layern. Zudem verankert der Integration-Layer Third-Party-Services in der Asset-Struktur des Unternehmens. In diesem Layer werden unter anderem IoT-Gateways und -Protokolle verortet. Protokoll-Gateways sind Geräte, die sicherstellen, dass verschiedene Arten von IT- und OT-Geräten miteinander kommunizieren können, auch wenn sie unterschiedliche Protokolle verwenden.

Ein Protokoll legt fest, wie Daten zwischen verschiedenen Geräten in demselben Netzwerk übertragen werden. Allerdings werden die für diesen Schritt verwendeten Kommunikationsprotokolle zur Unterstützung der Assets in der Regel nicht mit Blick auf die Cybersicherheit konzipiert und es können nötige Mechanismen fehlen, wie zum Beispiel die Authentifizierung zur Erkennung von Fehlern und abnormalem Verhalten, welches Sicherheitsangriffe begünstigt. Es gibt zwei Arten von Protokoll-Gateways: solche, die den Datenverkehr in Echtzeit übersetzen und Datenstationen, die den übersetzten Datenverkehr speichern und ihn auf Anfrage bereitstellen. Schwachstellen in Protokoll-Gateway-Geräten können heimliche Angriffe auf industrielle Systeme ermöglichen, wodurch Angreifer unter Umständen wertvolle Informationen erhalten und dadurch kritische Prozesse sabotieren können. So können zum Beispiel ernsthafte Störungen verursacht werden, wenn das Gerät den Datenverkehr nicht richtig übersetzt. Daher müssen Protokoll-Gateways von Sicherheitsprodukten überwacht werden, damit ein Angriff schnellstmöglich entdeckt wird. Durch das rasche Diagnostizieren von Übersetzungsproblemen kann ein heimlich erfolgter Angriff behoben und gravierende Auswirkungen auf produzierende Unternehmen minimiert werden.

An dieser Stelle ist abschließend hervorzuheben, dass jedes verwendete Asset auch eine Schwachstelle darstellt, welche einem Unternehmen schaden kann. Daher bietet es sich an, die Kritikalität einer Schwachstelle anhand ihres Risikos für das Unternehmen zu bewerten. Anhand dieser Schwachstellenanalyse können Risiken priorisiert und Gegenmaßnahmen eingeleitet werden. Hierzu wird im nachfolgenden Kapitel 3 eine detaillierte Vorgehensweise vorgestellt.

3 Vorgehen zur Anwendung

Ziel der hier vorgestellten Methodik ist es, das (Cyber-) Sicherheitslevel in einer Produktion ganzheitlich anzuheben, indem alle am Wertschöpfungsprozess beteiligten, sicherheitskritischen Assets identifiziert und individuelle Lösungen gesamtheitlich aufeinander abgestimmt werden. Jedes Asset wird dabei im Hinblick auf seinen Nutzen (Business-Impact) sowie sein Cyberrisiko entlang der Wertschöpfung analysiert. Aufbauend darauf werden sicherheitsfördernde Maßnahmen abgeleitet. Gemäß der vorgestellten Schwachstellenstruktur (s. Bild 2) werden die Schwachstellen der Objekte in die Layer *Resource, Application, System* und *Integration* eingeordnet. Anhand der Betriebsabläufe wird die Auswirkung eines Sicherheitsvorfalls durch jedes Asset auf weitere Betriebsgüter transparent gemacht. Im Ergebnis entsteht ein konkreter Implementierungsplan von Sicherheitsmaßnahmen, durch den die Kombination einzelner Handlungsfelder das gesamtheitliche Sicherheitsniveau steigert.

3.1. Analyse der Asset-Landschaft (Phase 1)

Die Methodik ist in drei Phasen aufgeteilt, deren Ausgangsbasis die assetorientierte Schwachstellenstruktur (s. Kapitel 2) bildet. Zunächst wird der Betrachtungsbereich definiert, alle relevanten Assets in ihm werden identifiziert und in die entsprechenden Layer eingeordnet (Phase 1). Hierbei gilt es, den Betrachtungsbereich so konkret wie möglich zu fassen, um eine Vergleichbarkeit der späteren Verbesserungsmaßnahmen sicherzustellen und zugleich die Anzahl der Vergleichspaare überschaubar zu halten. Im Anschluss wird eine Business-Impact-Analyse durchgeführt (Phase 2), um den Nutzen der Assets für die Wertschöpfung transparent zu machen. Ihr Ergebnis dient als Basis zur späteren Maßnahmenpriorisierung (Phase 3), welche den Einfluss des Assets im Falle eines Ausfalls auf die Geschäftsfähigkeit bewertet. Die Herausforderung einer Business-Impact-Analyse besteht darin, das subjektive Empfinden der Bewertenden zu quantifizieren. Dadurch kann es zwischen Unternehmen zu unterschiedlichen Kriterien und deren Gewichtungen kommen. Das passende Vorgehen zur Durchführung einer Business-Impact-Analyse muss daher in jedem Betrachtungsfall individuell an die Bedürfnisse des Unternehmens angepasst werden, z. B. Risikoaffinität, Branche oder Geschäftsmodell. Im Rahmen der vorgestellten Methodik wird empfohlen, den Einfluss eines ausfallenden Assets in vorher gewichtete Schadensarten und Schadenskategorien einzuordnen. Dabei sollte eine Ordinalskala verwendet werden, um das Nutzenprofil zu beschreiben.

Der ausbleibende Nutzen im Falle eines Ausfalls wird durch die Anbindung eines Assets an vor- und nachge-

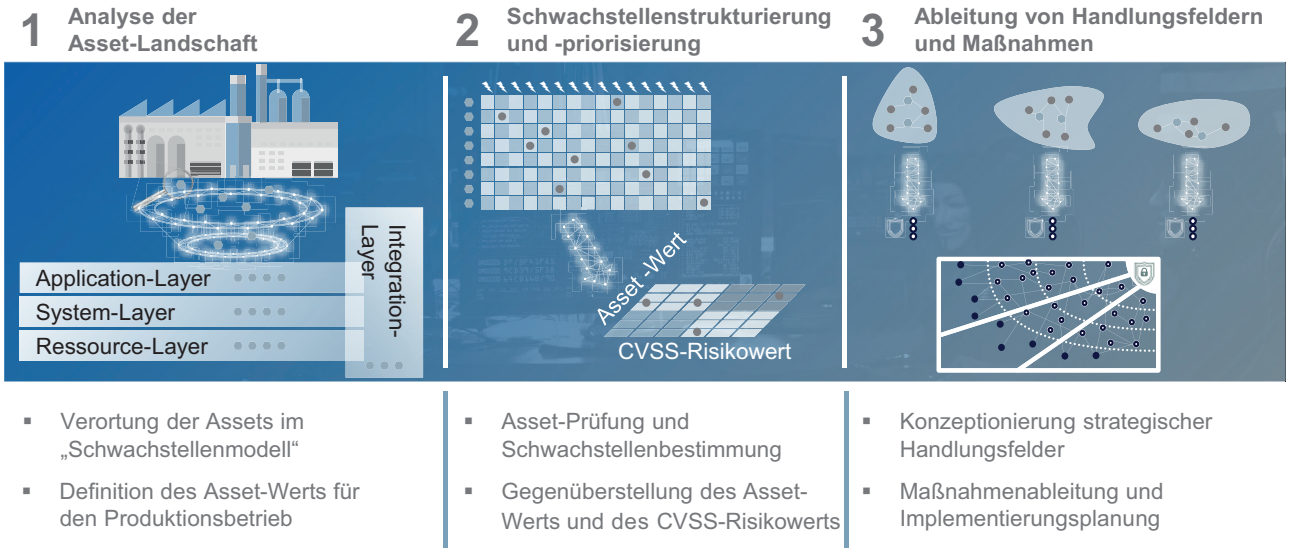

Bild 2: MHP- und FIR-Methodik zur Identifikation von Cybersicherheitsschwachstellen in der Produktion (eigene Darstellung)

lagerte Assets verstärkt. Bei der Business-Impact-Analyse ist daher unbedingt auch ein Einfluss an die angrenzenden Assets (Cross-Impact) zu berücksichtigen.

Laut einer Studie von *Palo Alto Networks* sind 98 Prozent des IoT-Datenverkehrs unverschlüsselt. Insbesondere altbekannte Schwachstellen in älteren OT-Protokollen, wie MODBUS, Profinet, IPPC und OPC, werden von Hackern genutzt, um Daten aus dem industriellen Netzwerk im Klartext (!) auszulesen oder Zugriff auf Maschinen zu erlangen. Einmal hinter die Firewall eines Netzwerks gelangt und im Besitz der Kontrolle, richten sie eine Command-and-Control-Struktur ein, mit der weitere Maschinen innerhalb des Netzwerks kontrolliert werden sollen[13].

Nicht zuletzt aus diesem Grund hat seit geraumer Zeit ein Umdenken stattgefunden, bei dem im Cyberraum nicht alles miteinander verbunden sein sollte. Stattdessen gilt es, nur jene Datenflüsse zu erlauben, die zwingend erforderlich sind. Falls möglich, sollten diese zudem zeitlich begrenzt und automatisch geschlossen werden[14]. Dieses Sicherheitskonzept des „Zero Trust" wird in der beschriebenen Methodik betrachtet. Der einzelne Geschäftseinfluss eines Assets ist immer in Kombination mit dem Cross-Impact zu betrachten. Aus den beiden Leitgedanken der Nutzenorientierung und des „Zero Trust" geht hervor, dass diejenigen Funktionen, die nicht zur direkten Wertschöpfung beitragen, mögliche Sicherheitsrisiken beinhalten können.

Die erste Phase schließt mit der Erstellung von Nutzenprofilen (s. Bild 3) für alle zu untersuchenden Assets des Betrachtungsbereichs. Diese Profile enthalten eine Dokumentation zum Nutzen der Assets sowie ihren Einfluss auf vor- und nachgelagerten Assets. Angeschlossen an die Identifikation und Bewertung der relevanten Assets erfolgt in der zweiten Phase zunächst die Erstellung einer Risikobewertung zur anschließenden Gegenüberstellung mit den Nutzenprofilen.

Voraussetzung für die Erstellung eines derartigen Nutzenprofils ist, sich mithilfe eines Fragenkatalogs einen umfangreichen Überblick hinsichtlich der zu schützenden Assets zu verschaffen. Eine klare Aufstellung darüber, welche Konsequenzen der Ausfall bestimmter Assets hat, ermöglicht es, die Schutzbedarfe der Assets ihrer Priorität nach zu ordnen. Dadurch ergibt sich eine

[13] s. Palo Alto Networks 2020, S. 3

[14] s. Pistorius 2020, S. 69

Auswirkung	1 - niedrig	2 - normal	3 - hoch	4 - sehr hoch
Finanzielle Auswirkung	keine nennenswerten Auswirkungen (z. B. Verlust geringer als 5 % des Umsatzes)	finanzieller Schaden bleibt für die Institution tolerabel (z. B. Verlust weniger als 5 – 20 % des Umsatzes)	Schaden bewirkt beachtliche finanzielle Verluste; Schaden nicht existenzbedrohend (z. B. Verlust unter 20 – 30 % des Umsatzes)	finanzieller Schaden ist für die Institution existenzgefährdend (z. B. wenn der Verlust 30 % des Umsatzes überschreitet)
Rechtliche Auswirkung	keine nennenswerten Auswirkungen	Verstöße gegen Gesetze und Bestimmungen mit geringen Konsequenzen; Verstöße werden nur intern bemerkt	Verstoß gegen Gesetze und Bestimmungen mit tolerierbaren Konsequenzen; Verstöße werden auch außerhalb der Institution bemerkt	Verstoß gegen Gesetze mit Konsequenzen für den Geschäftsbetrieb und einzelne Mitarbeiter
Auswirkung auf Reputation	keine nennenswerten Auswirkungen	Vertrauen ist nicht beeinträchtigt; kaum Verluste von Marktanteil; Störungen nicht bemerkt bzw. als bedeutungslos eingeschätzt	Image und Vertrauen sind beeinträchtigt; merkliche Verluste von Marktanteilen; hoher Aufwand zum Wiederausgleich	starke Image- und Vertrauensverluste; starke Verluste von Marktanteilen; Wiederausgleich von Image und Vertrauen nicht möglich

Bild 3: Beispiel für ein Nutzenprofil eines Assets (eigene Darstellung)

individuelle Rangfolge, die klärt, welche Assets im jeweiligen Unternehmen schützenswerter sind als andere. Eine solche Assetpriorisierung kann von der Geschäftsführung in Zusammenarbeit mit Ansprechpartnern aus den entsprechenden Fachbereichen durchgeführt werden. Es gilt beispielsweise abzuschätzen, welchen finanziellen Schaden der Ausfall einer bestimmten Maschine und ein damit verbundener Produktionstopp für das Unternehmen haben werden. Ein derartiger Produktionsstopp kann zudem auch Imageschäden und Vertrauensverluste beim Kunden zur Folge haben, wenn etwa Verträge und Liefertermine nicht mehr eingehalten werden können. Bei Einschätzungen, die sich mit rechtlichen Fragen beschäftigen, empfiehlt es sich, Unterstützung aus den jeweiligen Ressorts oder durch externe Berater einzuholen.

3.2 Schwachstellenstrukturierung und -priorisierung (Phase 2)

Die zweite Phase schafft einen Überblick über die Gefährdungslagen der einzelnen Assets durch Sicherheitsrisiken. Aus den Ergebnissen der ersten Phase werden insbesondere solche Assets priorisiert und tiefergehend untersucht, die einen hohen Geschäftswert bzw. hohen Geschäftsschaden bei Ausfall erzeugen. Durch diese vorgreifende Fokussierung wird der Untersuchungsaufwand reduziert und geschäftskritische Assets werden in den Vordergrund gerückt. Im Fokus der Sicherheitsprüfung steht der von *MHP* und *FIR* erarbeitete IT-Prüfkatalog. Dieser wurde auf Basis von Handlungsempfehlungen des Bundesamts für Sicherheit in der Informationstechnik (BSI) gemeinschaftlich erarbeitet und in der *Digital Experience Factory GmbH auf dem RWTH Aachen Campus* verprobt. Anhand des Katalogs werden standardisierte Prüfungen auf die im individuellen Fall betroffenen Assets angewendet. Auf diese Weise werden offene Schwachstellen detektiert. Dieser Katalog fasst insgesamt 89 Prüfkriterien, die auf die jeweils relevanten Assets angewendet werden.

Die erkannten Gefahrenpotenziale gilt es im darauffolgenden Schritt auf ihr Risiko hin zu bewerten. Hierbei fließt die individuelle Risikoaffinität der Prüfer mit in die Risikoquantifizierung ein. Ein etabliertes Verfahren zur Bewertung der Verwundbarkeit eines Assets ist das Common-Vulnerability-Scoring-System, kurz CVSS. Mittels standardisierter Faktoren wird das Risiko quantifiziert und in einem Score zwischen 0 und 10 festgehalten. Der

[15] Das 2014 veröffentlichte BSI LARS wird in regelmäßigen Abständen aktualisiert.

Prüfkategorie	Maßnahme	Beschreibung
Personelle Aspekte	Training des Personals	Das Personal muss regelmäßig an Qualifizierungs- und Fortbildungsprogrammen teilnehmen. Zusätzlich zu den Qualifizierungsprogrammen muss das Personal in regelmäßigen Awareness-Schulungen über denkbare Bedrohungen und Schwachstellen informiert und hierfür sensibilisiert werden. Das Service- und Wartungspersonal sowie Administratoren müssen durch Schulungen in die Lage versetzt werden, mögliche Schwachstellen zu identifizieren und zu bewerten sowie diesen durch angemessene Gegenmaßnahmen zu begegnen.
Prozesse	Benutzer- und Rechtemanagement	Soweit möglich sollten auf allen ICS in Abhängigkeit von dem angemeldeten Benutzer nur die jeweils erforderlichen Zugriffsrechte vergeben sein. Die Benutzer und die an sie vergebenen Rechte müssen ICS-weit verwaltet werden können. Die Berechtigungsvergabe muss dem Prinzip der geringsten Privilegien folgen und es muss ein rollenbasiertes Berechtigungskonzept umgesetzt werden. Ein Lebenszyklus der Benutzer, Rollen und Rechte muss etabliert werden.
Log-Monitoring & -Management	Monitoring von Industrial-Control-Systems (ICS)	Durch das Überwachen (engl. *Monitoring*) der ICS können Fehler und Engpässe wie beispielsweise Netzabbrüche, Verfügbarkeitsverluste oder eine Zunahme der Last und Abnahme der Performance frühzeitig identifiziert werden. Typische, für die Produktion notwendige ICS sind beispielsweise HMI, SPS und Netzkopplungselemente wie Switches und Router.

Bild 4: Beispiele für die Prüfkategorien (eigene Darstellung, basierend auf den Inhalten von Wichmann 2014, S. 9 f.)[15]

Score trennt dabei zwischen kleinen (0,0 bis 0,1), niedrigen (0,1 bis 3,9), mittleren (4,0 bis 6,9), hohen (7,0 bis 8,9) und kritischen Verwundbarkeiten (9,0 bis 10,0). Durch die Gegenüberstellung der individuellen Nutzen-(Ergebnis aus Business-Impact-Analyse)- und Risikoprofile (Ergebnis der Risikoquantifizierung) eines jeden Assets entsteht eine Matrix mit vier Quadranten. In dem Quadranten mit den beiderseits stärksten Ausprägungen sammeln sich die hochpriorisierten Assets und diejenigen Assets, deren Sicherheitsniveaus schnellstmöglich angehoben werden sollten. Die Assets werden hierbei alleinstehend priorisiert. Mit dem Ziel, das Sicherheitsniveau gesamtheitlich anzuheben, gilt es, die einzelnen Maßnahmen in Einklang zu bringen. Wie in der ersten Phase definiert, müssen zu Beginn der Folgephase die Abhängigkeiten zwischen den Assets herangezogen und sowohl Zielsetzung als auch Aufwand der Maßnahmen gegeneinander abgewogen werden.

3.3 Ableitung von Handlungsfeldern und Maßnahmen (Phase 3)

In der dritten und letzten Phase beginnt die Ableitung angemessener Sicherheitsmaßnahmen. Hierfür wird der *MHP*- und *FIR*-IT-Prüfkatalog genutzt (s. Bild 5), welcher jeder Schwachstelle bereits mögliche Maßnahmen zuordnet.

Darüber hinaus werden die erstellten Risikoprofile genutzt, um eine Maßnahme auf mehrere Schwachstellen anzuwenden und somit Synergieeffekte zwischen den Schutzmaßnahmen der Assets zu heben. Dabei werden die Sicherheitsmaßnahmen den jeweiligen Risikoprofilen zugeordnet und mit dem Nutzenprofil abgeglichen. Der Abgleich adressiert dabei nicht nur den Nutzen für die Geschäftsprozesse eines einzelnen Assets, sondern prüft auch, ob Wechselwirkungen mit anderen Maßnahmen bestehen. Diese Wechselwirkungen gilt es in Einklang zu bringen (+ ergänzend, 0 neutral, - beeinträchtigend) und sich gegenseitig ausschließende Maßnahmen gegeneinander abgewogen hinsichtlich ihres Gesamtnutzens zu bewerten. Sollten zwei oder mehr sich ausschließende Maßnahmen zwingend notwendig sein, müssen ggf. Sonderlösungen implementiert werden. Die vorgestellte Methodik dient insbesondere dazu, genau diese Zielkonflikte in der komplexen Themenstellung des Cyberraums aufzuspannen. Durch die klare Priorisierung der Nutzen, der Abstimmung von Sicherheitsmaßnahmen und des Aufzeigens zwingender Zielkonflikte entstehen thematische Handlungsfelder, die es gilt, sukzessive in den jeweiligen Ebenen des Schwachstellenmodell zu implementieren.

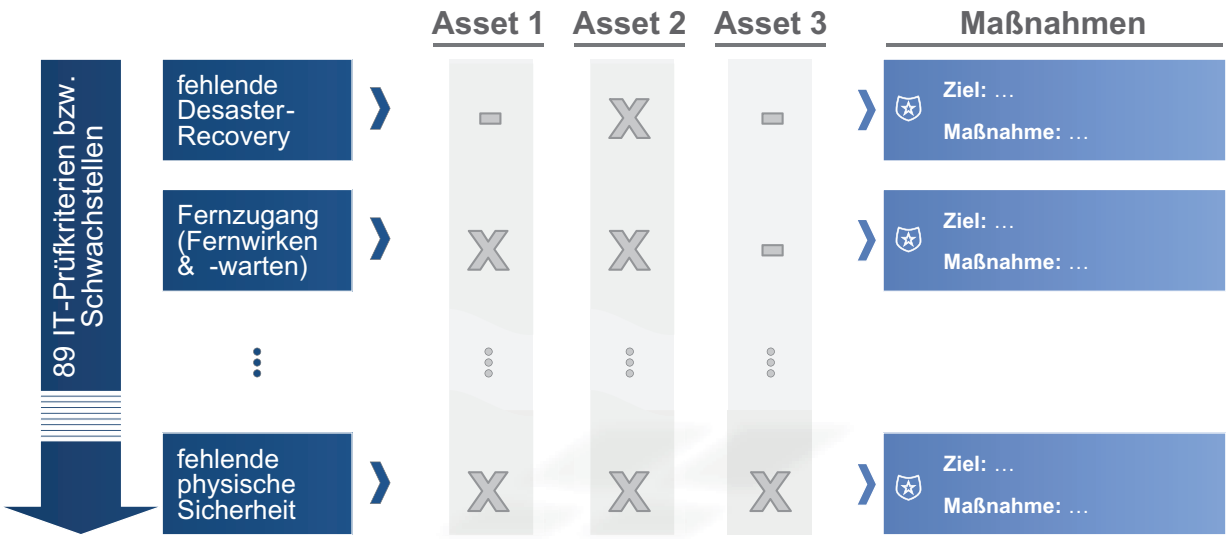

Bild 5: Ableitung von Maßnahmen auf die Handlungsfelder gemäß Prüfkatalog (eigene Darstellung)

4 Szenarien aus der Praxis (Usecases)

Im Folgenden werden anhand zweier Usecases, „Betriebsmittel als Schwachstelle in der Produktion“ und „Kompromittierte Datenverfügbarkeit (Ransomware)“, die möglichen Auswirkungen von Cyberangriffen auf die Produktion aufgezeigt. Dies dient dem Ziel, ein grundlegenderes Bewusstsein hinsichtlich der Vielschichtigkeit von Cybersicherheit in vernetzten Produktionsumgebungen zu schaffen. Im ersten Usecase wird dabei exemplarisch die zuvor vorgestellte Methodik bei einem Unternehmen angewendet. Der zweite Usecase stellt einen üblichen Angriff durch Ransomware auf Produktionsanlagen dar.

4.1. Betriebsmittel als Schwachstelle in der Produktion

Automatisierung und Digitalisierung sind in vielerlei Hinsicht der Wegbereiter für neue Potenziale. Viele Unternehmen gehen aufgrund der technischen Machbarkeit und vorrangig, um die Bedürfnisse ihrer Kunden maximal zu bedienen, den Weg in die Massenindividualisierung. In einigen Branchen, wie beispielsweise der Automobilbranche, ist diese Komplexität nur schwer handhabbar. Um dennoch die unzähligen und unabhängigen Materialströme zu beherrschen, greifen Unternehmen insbesondere in der Endmontage vermehrt auf fahrerlose Transportsysteme (FTS) zurück. Hierdurch werden einzelne Bauteile und Komponenten zu Werker und Produkt geliefert. Da jedes Produkt in seiner spezifischen Zusammensetzung vermutlich nur selten hergestellt wird und sich der Losgröße 1 annähert, ist dies eine Möglichkeit, die Material- und Informationsströme effizient abzubilden. Neben dem großen Potenzial dieser Technologie stellt sie auch ein wichtiges Asset in produzierenden Unternehmen dar. Bereits während der Konzeptionierungsphase zur Implementierung eines FTS gilt es, die *MHP*- und *FIR*-Methodik auf das neue Asset anzuwenden, um Implikationen auf die Cybersicherheit zu validieren.

In Anbetracht des ausgearbeiteten Frameworks können FTS in der ersten Phase **Analyse der Asset-Landschaft** dem Resource-Layer zugeordnet werden. Sie zeigen eine hohe Abhängigkeit gegenüber Komponenten auf dem Shopfloor wie beispielsweise Robotern, die die Montagearbeiten unterstützen. Die starke Abhängigkeit und Vernetzung auf dem Shopfloor muss insbesondere bei der Schwachstellenanalyse und der späteren Umsetzung von Maßnahmen berücksichtigt werden.

Im Folgenden wird die Geschäftskritikalität dieses Szenarios durch die *MHP*- und *FIR*-Methodik näher beleuchtet. Der Anwendungsfall beschreibt ein einzelnes FTS, welches lokal manipuliert wird. Wie in der Methodik dargelegt, gilt es zunächst, den Einfluss dieser Manipulation anhand einer Business-Impact-Analyse zu bewerten und im Weiteren den Anfälligkeits-Score des Assets durch das CVSS-Modell zu ermitteln.

Der Einfluss der Manipulation kann auf mehrere Dimensionen aufgeteilt werden: Die gängigsten Dimensionen sind hierbei der finanzielle, der rechtliche sowie der Einfluss auf die Reputation (s. Bild 4.1). Mit der in Kapitel 3 dargelegten Business-Impact-Analyse können diese Dimension mit Zahlenwerten von 1 bis 4 bewertet werden, wobei 1 „kein Einfluss“ und 4 „hoher Einfluss“ bedeutet. Diese Bewertung wird für die Manipulation eines einzelnen fahrerlosen Transportsystem beispielhaft vorgenommen.

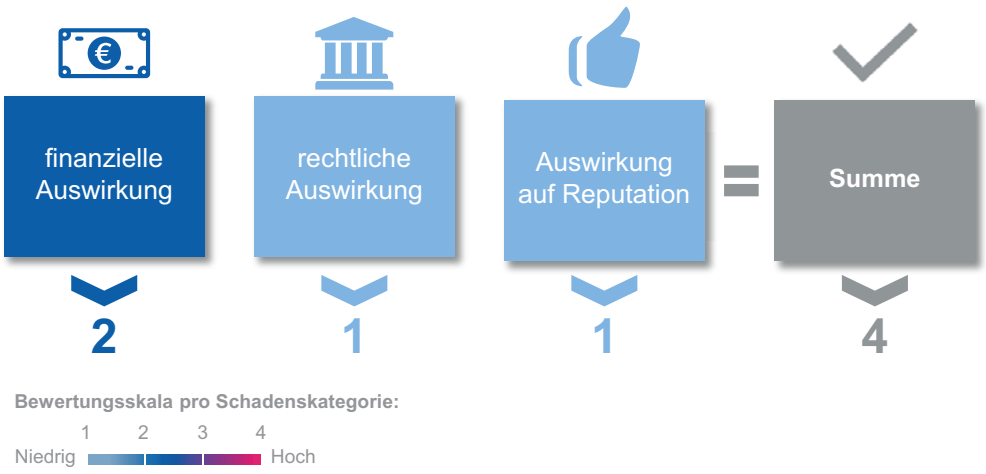

Bild 6: Business-Impact-Analyse eines FTS (eigene Darstellung)

Wird angenommen, dass das FTS durch die Manipulation die Produktionslinie nicht mehr bedienen kann, bedeutet dies gleichzeitig, dass das Produkt nicht gefertigt werden kann. Der finanzielle Schaden dieses Ausfalls wird daher mit 2 bewertet. Der einzelne Ausfall eines FTS würde zwar einen Umsatzverlust verursachen, jedoch nicht die ganze Produktion stoppen. Rechtlich gesehen muss beachtet werden, dass das Risiko verhältnismäßig gering ist. Ohne präventive Maßnahmen können historische Daten über Bauteil und Produkt veröffentlicht werden. Im unglücklichsten Fall kann es sogar durch die Verkettung einzelner Events zu kleinsten Personenschäden kommen. Entsprechend kann der rechtliche Schaden hier mit einer 1 bewertet werden. Abschließend muss der Einfluss auf die Reputation bewertet werden. Im Falle des Ausfalls eines einzelnen FTS liegt nahe, dass dieser Vorfall keine großen Auswirkungen hätte und von Externen gar nicht erst wahrgenommen wird. Daher wird dieser Faktor mit 1 bewertet. Aufsummiert ergibt dies einen niedrigen Einfluss (4 von 12) auf das Unternehmen.

In der zweiten Phase der *MHP*- und *FIR*-Methodik, der **Schwachstellenstrukturierung und -priorisierung**, gilt es, Schwachstellen aufzudecken und zu bewerten. Mögliche Schwachstellen können dem Prüfkatalog entnommen und im Anschluss durch das CVSS bewertet werden. Im CVSS-Basis-Score werden unter anderem der Angriffsvektor, die Einwirkung von Nutzern, die Vertraulichkeit, Integrität oder auch die Verfügbarkeit einbezogen. Werden diese Faktoren für das dargestellte Szenario bewertet, ergibt dies einen Score von 7.1 (hoch, s. Bild 7). Auf einer Skala bis zehn stellt 7.1 einen hohen Score dar.

Für das dargestellte Szenario eines einzelnen manipulierten FTS ergibt sich also ein geringer Einfluss auf den Nutzen für das Unternehmen. Die Anfälligkeit dieses Systems wird in Anbetracht der aufgezeigten Parameter jedoch als hoch eingeschätzt.

Nach der Priorisierung der Schwachstellen folgt die dritte Phase mit der **Ableitung von Handlungsfeldern und Maßnahmen**. Die Ergebnisse der zweiten Phase würden bedeuten, dass für diesen Anwendungsfall in einem kurz- bis mittelfristigen Horizont entsprechende Maßnahmen definiert werden müssen, um das System zu schützen. Diese Maßnahmen können wiederum dem *MHP*- und *FIR*-IT-Prüfkatalog entnommen werden. Was in dem Szenario nicht betrachtet wurde, ist der Fall, dass nicht nur ein einzelnes FTS zur Zielschiebe eines Angriffs werden kann, sondern auch die gesamte Flotte oder das Backendsystem, worüber diese gesteuert wird. Dadurch wäre ersichtlich, dass zusätzlich zu dem hohen CVSS-Wert auch ein äußerst hoher Einflusswert auf das Unternehmen gegeben ist. Hieraus wird deutlich, dass zum einen für die betrachteten Assets mehrere Szenarien erstellt werden müssen und zum anderen auch die Abhängigkeiten dieser Assets untereinander untersucht werden müssen. Aus der Betrachtung unterschiedlicher Szenarien und der Abhängigkeiten von Assets untereinander können Handlungsfelder definiert werden, um nicht nur einzelne Elemente zu schützen, sondern das System als Ganzes.

Darüber hinaus ist die Cybersicherheit ein Thema, welches kontinuierlich geprüft und verbessert werden muss. Daher hat es sich bewährt, die dargestellte Methodik mindestens jährlich durchzuführen, um Änderungen der Asset-Strukturen einzubeziehen.

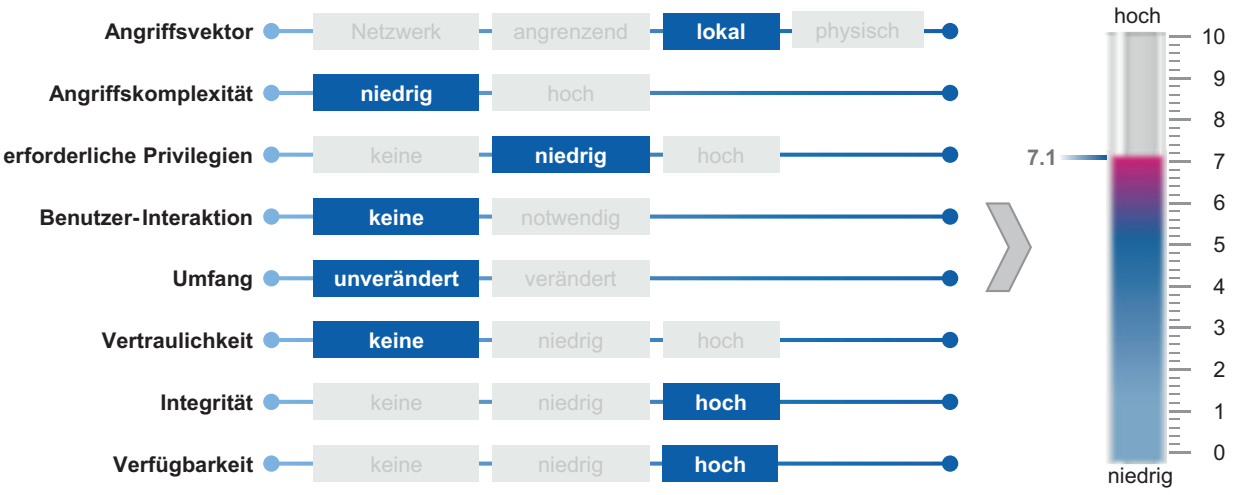

Bild 7: Schwachstellenbewertung nach dem Common-Vulnerability-Scoring-System (CVSS) (eigene Darstellung)

4.2. Kompromittierte Datenverfügbarkeit (Ransomware)

Die Verschmelzung der IT und OT (*Operational Technology*) schreitet unaufhaltsam voran. Die traditionelle Trennung der beiden isolierten Domänen, räumlich wie logisch, verschwindet zunehmend durch das Aufbrechen von Silos. Grund dafür sind die sich ändernden Paradigmen durch Industrie 4.0 wie eine horizontale und vertikale Vernetzung sowie digitale Durchgängigkeit. Um in Zukunft digitale Abbilder der Realität gestalten zu können, sogenannte Digital Twins, müssen Komponenten und Assets, aber auch Prozesse und Fähigkeiten in die digitale Welt überführt werden. Dabei ist stets entscheidend, welchen Granularitätsgrad die digitalen Abbilder aufweisen. Möchte der Produktionsleiter nur wissen, ob seine Maschine gerade läuft oder möchte er auf Basis des detaillierten Zustands die nächste Wartung planen und ggf. seine Produktionsplanung daran anpassen? Für Entwicklungsingenieure spielt der Digital Twin besonders vor dem Hintergrund von Simulationen eine entscheidende Rolle. Diese können deutlich vereinfacht und beschleunigt werden. In jedem Fall gilt es, dass Assets sowie Fertigungs- und Produktionsanlagen permanent und von überall erreichbar sind.

Im Zuge dieser steigenden Vernetzung sind Produktionsumgebungen (engl. *Industrial Control System*, kurz ICS) interessanter für Hacker geworden. Das Einschleusen von Schadprogrammen in Form von Malware erfolgte in der Vergangenheit typischerweise über physische Wechseldatenträger bzw. externe Hardware wie etwa USB-Sticks. Heute jedoch zeichnet sich ein anderes Bild ab: Über mit dem Internet verbundene Komponenten und Seitenkanalangriffe ohne entsprechende Netzwerksegmentierung ist es häufig ein Leichtes, dedizierte Malware in ICS einzubringen. Bekannte Beispiele wie Stuxnet aus dem Jahr 2010, bei dem ICS direkt adressiert wurden, oder WannaCry und Petya aus dem Jahr 2017, bei denen ICS nur indirekt infiziert worden sind, zeigen auf, wie bedrohlich die Situation auch heute noch ist. Dabei ist anzunehmen, dass die steigende Komplexität von ICS und Industrie-4.0-Umgebungen durch das Zusammenschalten verschiedener einzelner Komponenten eine Abnahme der Sicherheit des Gesamtsystems mit sich bringt, sofern nicht entsprechende Technologien wie NextGen-Firewalls eingesetzt und Sicherheitsprinzipien wie Security-by-Design berücksichtigt werden. Typische Angriffsszenarien auf ICS sind Zero-Day-Exploits oder Angriffe auf IIoT-Geräte, die in kostengünstiger Form zwar ihren Zweck erfüllen, jedoch nur in seltenen Fällen über Sicherheitsmechanismen verfügen. Die Tatsache, dass Unternehmen ihre Pilotprojekte im Industrie-4.0-Umfeld im Internet veröffentlichen und dabei häufig über die eingesetzten Komponenten berichten bzw. ganze Systemstrukturen preisgeben, erleichtert nur den Zugang über Social Engineering.

Letztlich schließt sich hier der Kreis zum Digital Twin. Wenn ein digitales Abbild von Assets und den umliegenden Strukturen gegeben ist, dann können Simulationen in Form verschiedener Angriffsszenarien durchgeführt werden, auf Basis dessen ein Risikowert abgeleitet werden kann. Das Stichwort ist hier Threat-Modelling. Ursprünglich aus der Softwareentwicklung stammend werden Systeme auf Basis verschiedener Referenzmodelle beschrieben und abgebildet. Im Anschluss werden mögliche Threats (Gefahren bzw. Schwachstellen), beispielsweise auf Basis von Datenflussdiagrammen, abgeleitet und bestimmten Assets zugeordnet. Es ergibt sich eine individuelle Matrix unterschiedlicher Gefahren in Bezug auf die Assets. Wichtig dafür ist jedoch, dass alle Zonen, Verbindungen, Komponenten, Assets, Versions- und Patchstände, Betriebssysteme und viele weitere Eigenschaften in Submodellen abgebildet sind, um eine umfassende, valide und effektive Simulation durchführen zu können. Bis Unternehmen so weit sind, wird noch viel Zeit vergehen. Daher bildet das vorgestellte Framework eine fundierte Ausgangslage, um Schwachstellen in Bezug auf Assets zu bestimmen, auch ohne tiefgreifendes Fachwissen und aufwendige Prozesse zur Entwicklung eines Threat-Models.

Ein Ransomwareangriff im Januar 2021 führte zum Ausfall zweier Produktionsanlagen eines europäischen Herstellers. Dabei verkaufte Fortinet VPNs mit bekannten Schwachstellen, für die es bereits seit langem Patches gab. Über die VPN-Schwachstellen verschaffte sich ein Verschlüsselungstrojaner Zugang zum Netzwerk des Unternehmens. Dort breitete er sich auf Servern aus, die zur Steuerung industrieller Prozesse des Herstellers benötigt wurden. Daraufhin wurden die Prozesse in zwei italienischen Produktionsstätten des Herstellers vorübergehend stillgelegt. Das Unternehmen konnte schließlich die meisten, aber nicht alle verschlüsselten Daten aus Backups wiederherstellen.[16]

[16] s. Goodin 2021

5 Zusammenfassung und Ausblick

Cybersicherheit stellt KMU aus dem produzierenden Gewerbe vor wesentlich größere Herausforderungen als marktbegleitende Großunternehmen. Die Vorteile der Digitalisierung wie zum Beispiel stärkere Transparenz beim Verbrauch von Ressourcen oder bei der Bemessung von Leistungen, lasten schwer auf der Marktposition von produzierenden KMU. Neben dem de facto etablierten Standard der digitalen Anbindung an ihr Ökosystem aus Lieferanten und Kunden führt die stetig steigende Zahl an Applikationen, Datenbanken und Schnittstellen zu mehr Cybersicherheit-Schwachstellen entlang der Lieferkette von KMU. Offensichtlich ist es keine langfristige Strategie, digitale Innovationen aus finanziellen und organisatorischen Gründen aufzuschieben. Insbesondere Großkunden können zur Risikominimierung und Steigerung der Planungssicherheit die höhere Transparenz, die digitale Kompetenz von Lieferanten weltweit einfordern. KMU, die sich diesem Drang entziehen möchten, laufen langfristig Gefahr, nicht mehr als *Preferred Supplier* gelistet zu werden.

KMU sind im Cyberraum den gleichen Bedrohungen ausgesetzt wie Großunternehmen. Dabei verfügen sie über deutlich weniger Ressourcen zur aktiven Verteidigung gegen Cyberangriffe. Dies spiegelt sich sowohl in Budgets als auch in der Anzahl und Qualifikation von Fachkräften für Cybersicherheit wider. KMU besitzen oftmals nicht die Mittel, um im gleichen Umfang auf Gesetze, Regularien und technische Speziallösungen einzugehen, wie Konzerne dies können. In der Regel werden Geschäftsprozesse durch wenige Personen verantwortet, wodurch sich diese oftmals zu Hauptsicherheitsverantwortlichen für ihren Bereich und die darin befindlichen Assets entwickeln. Eine adäquate Schulung oder gar tiefgreifende Fortbildung zur Sicherung dieser Assets kann meist nicht wahrgenommen werden.

Die am Markt beworbenen Rahmenwerke zum Aufbau einer Sicherheitsorganisation orientieren sich zumeist an theoretischen Konstrukten. Sie umfassen ausführlich alle relevanten Themenfelder der Cybersicherheit. Jedoch können die wenigsten Unternehmen all diesen Themenfeldern gerecht werden – insbesondere bei einer geringen Dichte an Führungskräften mit breitem Aufgabenspektrum, wie sie typisch für KMU sind. Cybersicherheit wird verstärkt zum Wettbewerbsvorteil für jene Unternehmen, die entsprechende Lösungen etablieren. Mehr denn je gilt daher für Unternehmen mit begrenzten Kapazitäten, die richtigen Sicherheitsvorkehrungen im richtigen Kosten-Nutzen-Verhältnis zur richtigen Zeit zu tätigen.

Zur Berücksichtigung der knappen Ressourcen müssen KMU sicherheitsstärkende Maßnahmen stark priorisieren und effizient handeln. Die *MHP*- und *FIR*-Methodik bietet dafür den idealen Rahmen. Sie identifiziert zunächst die wichtigsten und schützenswertesten Assets anhand der Analyse ihres Werts für das Unternehmen. Im darauffolgenden Schritt wird die Verwundbarkeit dieser Assets mithilfe des weltweiten Standards Common-Vulnerability-Scoring-System ermittelt. Durch die Kombination des erstgenannten Assetwerts und des Schwachstellen-Scores kann eine Priorisierung für den Aufbau von Sicherheitskonzepten vorgenommen werden.

Ein Vorteil dieser Methodik ist die pragmatische Herangehensweise, die zugleich auf nationalen und internationalen Standards aufbaut. Dadurch ist sie universell und nicht nur in der Produktion einsetzbar. Ein weiterer Vorteil liegt darin, dass der Prüfkatalog langfristig um den BSI-IT-Grundschutz erweitert wird und somit auch die Methodik an die steigenden Bedürfnisse von wachsenden Unternehmen angepasst werden kann. Insbesondere durch ihre Skalierbarkeit wird die *MHP*- und *FIR*-Methodik der Anforderung von KMU nach einem leichten Einstieg in die komplexe Cybersicherheit gerecht. Denn Cybersicherheit umfasst nicht nur kurzfristig anfallende, technische Lösungen, sondern die langfristige Etablierung technischer, organisatorischer und kultureller Handlungsweisen.

Bild 8: Key-Takeaways

6 Literaturverzeichnis

Beigl, M.; Boden, C.; Heinz, C.; Lenk, A.; Markl, A.; Neumair, B.; Oppermann, H.; Riedel, T.; Schlitter, N.: Smart-Data-Technologien des BMWi-Technologieprogramms „Smart Data – Innovationen aus Daten". Hrsg.: Smart-Data-Begleitforschung. Berlin November 2015. https://www.digitale-technologien.de/DT/Redaktion/DE/Downloads/Publikation/Smart_Data_Technologien.pdf;jsessionid=20AEE0BCA3E4D13EDD25DDE89E8F5081?__blob=publicationFile&v=6 (Link zuletzt geprüft: 01.06.2021)

European Union Agency for Network and Information Security (ENISA) (Hrsg.): Good practices for Security of Internet of Things in the context of Smart Manufacturing. European Union Agency for Network and Information Security (ENISA), Heraklion, Greece, November 2018. https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot/at_download/fullReport (Link zuletzt geprüft: 01.06.2021)

Gallagher, S.; Brandt, A.: [Editor's note] Facing down the myriad threats tied to COVID-19. Sophos online, 14.04.2020. https://news.sophos.com/en-us/2020/04/14/covidmalware/ (Link zuletzt geprüft: 01.06.2021)

Goodin, D.: How a VPN vulnerability allowed ransomware to disrupt two manufacturing plants. Patching in industrial settings is hard. Ransomware shutting down production is harder. arstechnica online, 08.04.2021. https://arstechnica.com/information-technology/2021/04/ransomware-shuts-down-production-at-two-manufacturing-plants/ (Link zuletzt geprüft: 01.06.2021)

Henseler-Unger, I.; Hillebrand, A.: Aktuelle Lage der IT-Sicherheit in KMU. In: DuD – Datenschutz und Datensicherheit 42 (2018) 11, S. 686 – 690.

Kumaran, N.; Lugani, S.: Protecting businesses against cyber threats during COVID-19 and beyond. Google Cloud, 16.04.2020. https://cloud.google.com/blog/products/identity-security/protecting-against-cyber-threats-during-covid-19-and-beyond (Link zuletzt geprüft: 01.06.2021)

Lallie, H. S.; Shepherd, L. A.; Nurse, J. R. C.; Erola, A.; Epiphaniou, G.; Maple, C.; Bellekens, X.: Cyber Security in the Age of COVID-19: A Timeline and Analysis of Cyber-Crime and Cyber-Attacks during the Pandemic. In: Computers & Security 105 (2021) 1, S. 102248/ 20 S. https://www.researchgate.net/profile/Xavier_Bellekens/publication/342377769_Cyber_Security_in_the_Age_of_COVID-19_A_Timeline_and_Analysis_of_Cyber-Crime_and_Cyber-Attacks_during_the_Pandemic/links/5ef3264d458515ceb2081841/Cyber-Security-in-the-Age-of-COVID-19-A-Timeline-and-Analysis-of-Cyber-Crime-and-Cyber-Attacks-during-the-Pandemic.pdf (Link zuletzt geprüft: 01.06.2021)

Müller, K.-R.: IT-Sicherheit mit System. Integratives IT-Sicherheits-, Kontinuitäts- und Risikomanagement – Sicherheitspyramide – Standards und Practices – SOA und Softwareentwicklung. 5., neu bearb. u. erg. Auflage. Springer Vieweg, Wiesbaden 2014.

Niehues, M. et al.: Organisation, Qualität und IT-Systeme für Planung und Betrieb. In: Handbuch Industrie 4.0. Geschäftsmodelle, Prozesse, Technik. Hrsg.: G. Reinhart. Hanser, München [u. a.] 2017, S. 137 – 167.

Palo Alto Networks (Hrsg.): 2020 Unit 42 IoT Threat Report. Santa Clara (CA), Oktober 2020. [in Bibliothek des FIR e. V. an der RWTH Aachen verfügbar]

Pistorius, J.: Industrie 4.0 – Schlüsseltechnologien für die Produktion. Grundlagen – Potenziale – Anwendungen. Springer, Berlin [u. a.] 2020.

Pohlmann, N.: Wertschöpfung der Digitalisierung sichern. Vier Cybersicherheitsstrategien für den erfolgreichen Wandel in der IT. In: IT-Sicherheit – Mittelstandsmagazin für Informationssicherheit und Datenschutz (2020) 1, S. 60 – 65.

Völker, T.: [Pressemitteilung] Netzsch-Gruppe gehackt. Ransomware-Angriffe auf Maschinen- und Anlagenbau nehmen zu. Hrsg.: VSMA. Unternehmen Cybersicherheit online, 22.07.2020. https://unternehmen-cybersicherheit.de/netzsch-gruppe-gehackt-ransomware-angriffe-auf-maschinen-und-anlagenbauer-nehmen-zu/ (Link zuletzt geprüft: 01.06.2021)

Wichmann, A.: LARS ICS Version 1.0. Light and Right Security ICS – Ein Werkzeug für den leichtgewichtigen Einstieg in industrielle Cyber-Security. Bundesamt für Sicherheit in der Informationstechnik (BSI), Bonn 2014. Handbuch (PDF) in zip-Datei enthalten: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ICS/LARS.zip;jsessionid=337F07E5E836CAA6C84959AA525578F2.internet081?__blob=publicationFile&v=1 (Link zuletzt geprüft: 01.06.2021) [in Bibliothek des FIR e. V. an der RWTH Aachen verfügbar]

7 *MHP* und *FIR* als kompetente Partner in der Praxis

Um den Weg aus dem Forschungsbedarf bis in die Praxisanwendung zu ebnen, bedarf es der Zusammenarbeit von Experten aus beiden Bereichen. Als Bindeglied zwischen Anwendung und organisationaler Forschung hat das *FIR* eine prädestinierte Position, um Themen wie die Cybersicherheit aus einer nutzerzentrierten Perspektive gesamtheitlich zu erforschen. Themen wie industrielle und strategische Cybersicherheit liegen im Fokus der aktuellen Forschungsvorhaben des *FIR*, um insbesondere für KMU die Zugänglichkeit zu Cybersicherheitsmaßnahmen kosteneffizient anwendbar zu machen. *MHP* verfügt über langjährige Erfahrungswerte aus Mobility und Manufacturing. Mit dem Beratungsansatz der Symbiose aus Management- und IT-Beratung komplettieren sie das Expertenteam dieses Projekts. Ihre Expertise liegt hierbei in der effizienten Harmonisierung von cybersicheren, IT-getriebenen Geschäftsprozessen – von der Strategie bis hin zur Transformation – und den Kundenbedürfnissen.

Die ***MHP Management- und IT-Beratung GmbH*** entwickelt wegweisende Mobility- und Manufacturing-Lösungen für internationale Konzerne, gestandene Mittelständler und disruptive Start-ups. Als Premium-Business- und Technologiepartner gestaltet *MHP* bereits heute die digitale Zukunft von morgen. Der Beratungsansatz ist einzigartig: *MHP* verbindet ganzheitliche IT- und Technology-Expertise mit tiefgreifendem Management-Know-how. Damit ist sie der ideale Partner für einen erfolgreichen Digital-Turn. Als Digitalisierungsexperten liefern ihre Berater auf Basis von fundierten Analysen innovative Strategien, um Veränderungsprozesse in nachhaltigen Erfolg zu verwandeln. Mit über 2.800 Mitarbeitern treibt *MHP* weltweit an 19 Standorten den digitalen Fortschritt voran – gemeinsam mit über 300 Kunden. Und das mit Excellence auf allen Ebenen.

Der ***FIR e. V. an der RWTH Aachen*** verfügt über umfangreiche Forschungs- und Beratungserfahrungen in den Bereichen des Produktions-, Dienstleistungs- und Informationsmanagements sowie der Business-Transformation. Zudem ist er im *Cluster Smart Logistik auf dem RWTH Aachen Campus* angesiedelt und verfügt somit über eine entsprechende Branchenerfahrung durch diverse Projekte sowie durch den ständigen Kontakt zu Unternehmen dieser Branche. Im Kontext der zunehmenden Digitalisierung beschäftigt sich das *FIR* in verschiedenen Projekten und Gremien, wie der Allianz für Cybersicherheit, mit Anwendungsgebieten der IT-Komplexität, IT-Strategie oder Cloud-Transformation und prägt maßgeblich Initiativen wie Industrie 4.0. Aufgrund seiner umfangreichen Tätigkeiten, sowohl im Bereich Forschung als auch Realisierung, verfügt das *FIR* über Expertise in der anwendungsnahen und schnellen Verwirklichung von Innovationen. Insbesondere Themen wie industrielle und strategische Cybersicherheit liegen im Fokus der aktuellen Forschungsbemühungen des *FIR*, um Unternehmen von heute auf das Arbeiten von morgen vorzubereiten.

Kontakt

Jacques Engländer, M.Sc.
FIR e. V. an der RWTH Aachen
Tel.: +49 241 47705-517
E-Mail: Jacques.Englaeder@fir.rwth-aachen.de

Andreas Henkel, M.A.
MHP Management- und IT-Beratung GmbH
Tel.: +49 151 4066 7526
E-Mail: Andreas.Henkel@mhp.com

FIR e. V.
an der RWTH Aachen
Campus-Boulevard 55
52074 Aachen

Telefon: +49 241 47705-0
E-Mail: info@fir.rwth-aachen.de
www.fir.rwth-aachen.de