Mittelstand-Digital

Gefördert durch:

Bundesministerium für Wirtschaft und Energie

aufgrund eines Beschlusses des Deutschen Bundestages

Sicherer Datenaustausch

Mittelstand-Digital Magazin
WISSENSCHAFT TRIFFT PRAXIS
Ausgabe 16

Impressum

Herausgeber/Redaktion:
Begleitforschung Mittelstand-Digital
WIK-Consult GmbH
Rhöndorfer Straße 68
53604 Bad Honnef
HRB: Amtsgericht Siegburg, 7043
Tel. +49 (0)2224-9225-0, Fax +49 (0)2224-9225-68
E-Mail: *mittelstand-digital@wik.org*
www.mittelstand-digital.de

Verantwortlich: WIK-Consult, Martin Lundborg
Redaktion: WIK-Consult, Lisa Schrade-Grytsenko und Pirmin Puhl
Satz und Layout: WIK-Consult, Karin Wagner

Bildnachweis:
Titel: AdobeStock-peterschreiber.media
Seite 5: Ruslan Ropat/envato elements
Seite 10: Mittelstand 4.0 Kompetenzzentrum Kaiserslautern/A. Sell
Seite 11: AdobeStock-BillionPhotos.com
Seite 17: AdobeStock-Looker_Studio
Seite 23: Wichelhaus GmbH & Co KG.
Seite 27: Martinelle auf Pixabay
Seite 28/30: tti Technologietransfer und Innovationsförderung Magdeburg GmbH, Roland Hallau
Seite 31: Enginsight GmbH
Seite 33-38: WZL_der RWTH_Aachen
Seite 41: Markus Spiske on Unsplash

Stand: August 2021

Druck:
Plump Druck & Medien GmbH
Rolandsecker Weg 33, 53619 Rheinbreitbach

ISSN (Print) 2198-8544
ISSN (Online) 2198-9362

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

Mittelstand-Digital Magazin WISSENSCHAFT TRIFFT PRAXIS – Ausgabe 16

Sicherer Datenaustausch

Inhalt

Editorial

Liebe Leserinnen und Leser,

Daten sind die Grundlage der Digitalisierung und innovativer Unternehmen. Während der Pandemie ist der Datenverkehr deutlich gewachsen und wird auch in Zeiten nach der Pandemie zunehmen. Aus dem Home-Office, in der Cloud, auf der Produktionsfläche und über die gesamte Wertschöpfungskette hinweg. Einer Studie des Fraunhofer ISST zufolge sind 50 – 80 % der großen Unternehmen an unternehmensübergreifendem Datenaustausch beteiligt. Bei den kleinen und mittleren Unternehmen sind das nur ca. 40 %. Dabei wird der Datenaustausch auch für kleine und mittlere Unternehmen immer wichtiger und ist heute schon möglich und nötig. Um die innovative und verantwortungsvolle Bereitstellung und Nutzung von Daten signifikant zu erhöhen, hat die Bundesregierung zu Beginn des Jahres 2021 ihre Datenstrategie verabschiedet. Die vertrauensvolle Nutzung datenbasierter Geschäftsmodelle benötigt aber auch die Gewährleistung von Daten- und IT-Sicherheit. Dies gilt nicht nur bei der Gewinnung und Nutzung von Daten, sondern auch bei deren Austausch, der notwendig ist um das volle Potenzial ausschöpfen zu können. Sicherer Datenaustausch – wie das für KMU funktioniert, zeigen die Zentren im Netzwerk Mittelstand-Digital anhand vieler anschaulicher Beispiele in dieser Ausgabe von WISSENSCHAFT TRIFFT PRAXIS.

Das Zentrum Kaiserslautern zeigt, wie das europäische Projekt Gaia-X unter Gewährleistung größtmöglicher Sicherheitsaspekte auch für kleine und mittlere Unternehmen den Austausch von Daten ermöglicht und welche Vorteile ein digitales Ökosystem bietet. Wie eine gemeinsame Nutzung bzw. ein Datenaustausch zwischen einer Vielzahl an Teilnehmenden ermöglicht werden soll, ohne dabei zu viele Informationen preiszugeben und Datenschutz, Datensicherheit und Vertraulichkeit gewährleisten zu können, zeigt das Kompetenzzentrum Stuttgart.

Im Beitrag der Transferstelle IT-Sicherheit im Mittelstand (TISiM) erfahren kleine und mittlere Unternehmen, welche Maßnahmen in ihrem Betrieb konkret umgesetzt werden müssen, um die Organisation IT-sicher zu gestalten. Mit Hilfe des Sec-O-Mat erhalten Unternehmen in Form eines Aktionsplans eine individuelle Analyse und konkrete Handlungsempfehlungen mit kuratierten Angeboten um Maßnahmen ergreifen zu können.

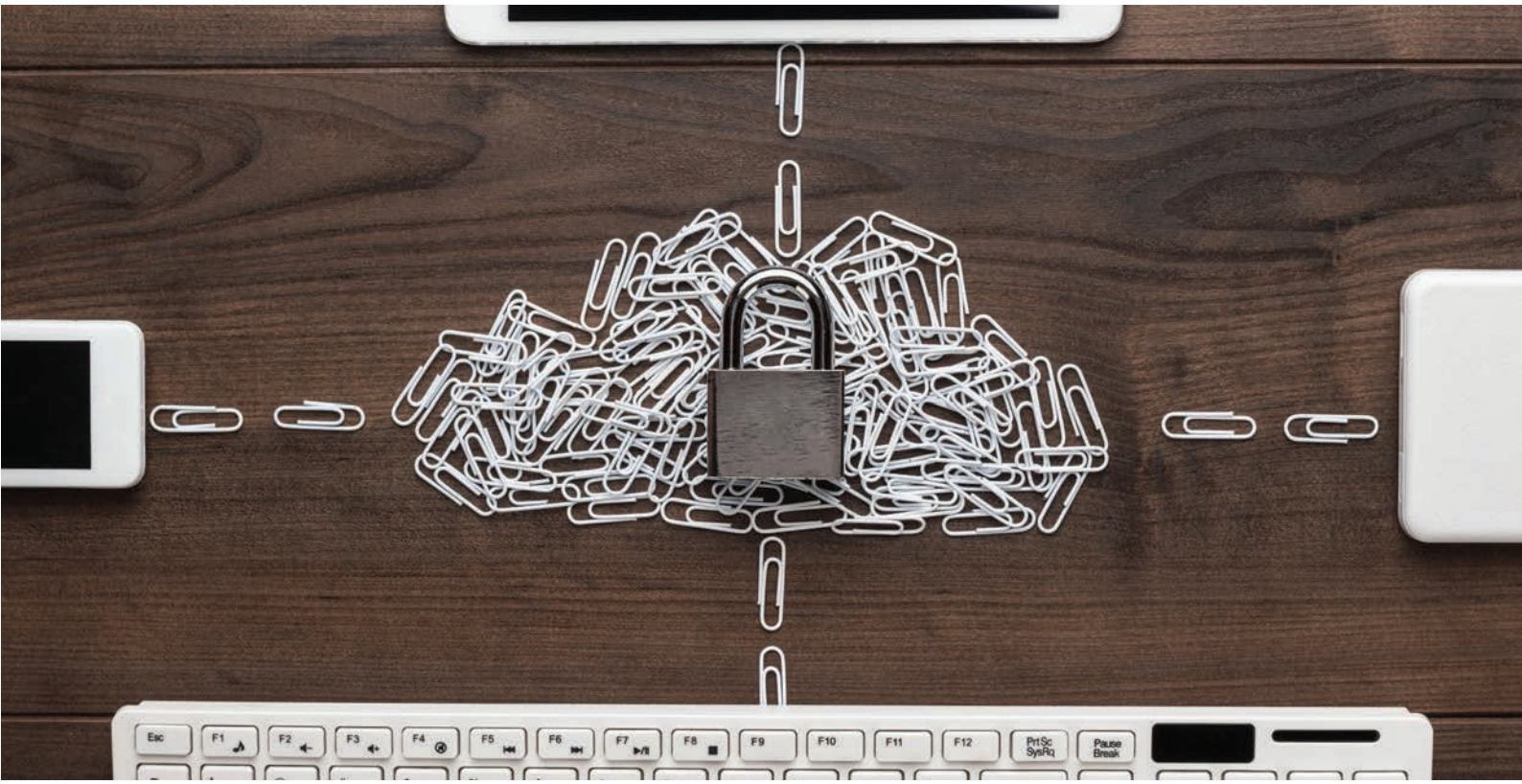
Im Beitrag des Kompetenzzentrums eStandards kommen die Unternehmen zu Wort. Anhand von vier KMU, die das Zentrum zusammen in einem Verbundumsetzungsprojekt zu „Sicherheitsstandards im multilateralen Datenaustausch“ begleitet, werden Erfahrungen aufgezeigt, wie sicherer Datenaustausch in der Praxis gelingt und welche Vorteile Unternehmen aus verschiedenen Branchen daraus gezogen haben.

Wie können Unternehmen erfahren, ob in ihrem Betrieb ein sicherer Datenaustausch stattfindet oder ob es Sicherheitslücken gibt? Das Zentrum Chemnitz stellt verschiedene Herangehensweisen vor, wie Schwachstellen aufgedeckt werden können und wie KMU ihre bestehenden Netzwerke sichern können. Um Vorteile und praxisgerechte Erprobung geht es im Beitrag des Zentrums Dortmund. Tobias Kaufmann, Johannes Mayer und Philipp Niemietz stellen die Plattform myDataEconomy vor, mit der auch kleine und mittelständische Unternehmen eine sichere Nutzung und Monetarisierung der eigenen Daten erproben um umsetzen können. Wie Unternehmen sich den Herausforderungen stellen können, die im Rahmen von Kooperationen bei der Informations- und Datensicherheit auftauchen können, zeigt abschließend das Zentrum IT-Wirtschaft. Vorgestellt werden verschiedene Vorgehensweisen, die Unternehmen beachten sollten, wenn sie sich diesem Thema widmen.

Die 7 Beiträge dieser Ausgabe stehen für die Themenvielfalt der 26 Zentren im Netzwerk Mittelstand-Digital in ganz Deutschland. Betrachten Sie sie als Vorgeschmack auf ihre diversen Informations- und Qualifizierungsangebote zu diesen und weiteren Digitalisierungsthemen. Informationen über die mehr als 130 Anlaufstellen und einen umfassenderen Einblick in die Expertise des Mittelstand-Digital-Netzwerks erhalten Sie auf www.mittelstand-digital.de.

Wir wünschen Ihnen eine interessante und inspirierende Lektüre.

Lisa Schrade-Grytsenko und *Pirmin Puhl*
Begleitforschung Mittelstand-Digital



Keran Sivalingam, Larissa Theis

Datensicherheit im Gaia-X Ökosystem

Eine sichere und vernetzte Dateninfrastruktur, die den höchsten Ansprüchen an digitaler Souveränität gerecht wird - dieses Ziel hat sich die europäische Initiative Gaia-X gesetzt, um einen gemeinsamen europäischen Datenraum für Unternehmen zu schaffen. Dabei sind die Themen Datensicherheit, Datensouveränität und digitale Souveränität von zentraler Bedeutung. Wie kann der Austausch von Daten durch Gaia-X unter Gewährleistung größtmöglicher Sicherheitsaspekte bewerkstelligt werden? Welche Möglichkeiten bietet Gaia-X gerade für kleine und mittlere Unternehmen (KMU)? Das Mittelstand-Digital Zentrum Kaiserslautern ist mit dem Schulungsdemonstrator PAUL Teil der Gaia-X Testumgebung an der SmartFactory Kaiserslautern und unterstützt KMU unter anderem mit Expertise im Bereich der Industrie 4.0 und der Produktion der Zukunft. Dieser Beitrag zeigt die Relevanz von sicherem Datenaustausch und die Potenziale von Gaia-X als digitalem Ökosystem für KMU auf.

Datenaustausch ist eine Herausforderung

Der Austausch von Daten spielt für Unternehmen eine immer größere Rolle im Arbeitsalltag. Dies gilt insbesondere bei der Zusammenarbeit eines Unternehmens mit einem anderen, unabhängig von der Branche. Im Zuge der voranschreitenden Digitalisierung findet auch der Datenaustausch immer öfter im virtuellen Raum statt. In den letzten Jahren hat die digitale Transformation auch in zahlreichen mittelständischen Unternehmen Einzug erhalten, sodass viele KMU mittlerweile eine Vielzahl an Daten vorliegen haben, auf die sie zurückgreifen können. Auch in der Produktions- und Fertigungsindustrie, welche die deutsche KMU-Landschaft entscheidend prägt, hat sich dieser Trend als Teilbereich der Industrie 4.0 durchgesetzt.[1]

Der Austausch von Daten zwischen zwei Unternehmen sieht auf den ersten Blick eher einfach aus. Allerdings stellt die Umsetzung schon viele Unternehmen vor nicht unerhebliche Herausforderungen, wie zum Beispiel Datenschutz und Compliance. Der Homeoffice-Trend durch die Corona-Krise hat die Anforderungen an einen

1 Bundesministerium für Wirtschaft und Energie (2019).

Ziele von Gaia-X

1. die technische und wirtschaftliche Konzeption einer sicheren Dateninfrastruktur zu konkretisieren,
2. auf dieser Basis ein gemeinsames Ökosystem von Anwendern und Anbietern aus Organisationen der öffentlichen Verwaltung, des Gesundheitswesens, Unternehmen und wissenschaftichen Einrichtungen zu schaffen,
3. sowie unterstützende Rahmenbedingungen und Strukturen zu etablieren

sicheren Datenaustausch zudem noch erhöht. Hinzu kommt, dass ein Unternehmen häufig nicht nur bilaterale Geschäftsbeziehungen in Deutschland pflegt, sondern auch auf weltweit vernetzte Geschäfts- und Produktionsbeziehungen mit Zulieferern angewiesen ist. Die Akteure innerhalb des Netzwerks bringen oft unterschiedliche technische Voraussetzungen mit; Sie miteinander zu vernetzen ist eine hochkomplexe Angelegenheit. Gerade der Austausch von Daten über Unternehmensgrenzen hinweg geschieht abteilungsübergreifend und entlang der gesamten Wertschöpfungskette des Unternehmens von der Auftragserstellung bis hin zur finalen Logistik. Daten in einem Netzwerk dieser Art auszutauschen, ist daher äußerst anspruchsvoll.[2]

Ein solch umfassender Datenaustausch über die gesamte Wertschöpfungskette erfordert eine multilaterale Zusammenarbeit, die nur durch eine Standardisierung und einen einheitlichen Zugang aller Beteiligten zu den Daten effizient zu gestalten ist. Ermöglicht wird das durch ein interoperables und datenorientiertes Netzwerk. Denn nur in einem harmonisierten, offenen und transparenten digitalen Ökosystem können Daten vertrauensvoll und sicher verfügbar gemacht, zusammengeführt und miteinander geteilt werden - eines der Hauptziele von Gaia-X. Bei Gaia-X handelt es sich um eine europäische Initiative, um eine sichere und föderierte Dateninfrastruktur bereitzustellen.

Das Netzwerk aus Infrastruktur, Daten und Interaktionsmöglichkeiten untereinander bildet das Gaia-X Ökosystem. Dieses Ökosystem soll gerade für Mittelständler die Einstiegshürden in die Cloud minimieren und einen breiten Zugang zu einer sicheren Dateninfrastruktur ermöglichen, in der die Unternehmen entscheiden können, welche Daten sie wann und mit wem teilen möchten – ganz im Sinne der Datensouveränität.[3]

2 DVZ (2021).
3 Bundesministerium für Wirtschaft und Energie (2019).

Datensicherheit in Ökosystemen

Digitale Ökosysteme haben sich mittlerweile in vielen Bereichen der Industrie durchgesetzt. Teilweise wickeln Unternehmen sogar ihre gesamte Interaktion über ein solches Ökosystem ab. Ihr Geschäftsmodell ist dann plattformbasiert und man spricht von Plattformökonomie. Auf einer solchen Plattform können verschiedene Ökosystemteilnehmer direkte Beziehungen miteinander eingehen (siehe Hotelbuchungsplattformen, Car-Sharing-Angebote, etc.). Auch für KMU wird es immer wichtiger, an solchen Ökosystemen teilzunehmen, da sie neue Chancen und Möglichkeiten bieten und Disruption ermöglichen. Durch innovative Ideen können Unternehmen so neue Märkte erschließen oder eine ganze Branche verändern. In der Fertigungsindustrie gewinnt zum Beispiel Manufacturing-as-a-Service immer mehr an Bedeutung. Hier werden Fertigungsaufträge über eine digitale Plattform vergeben. Unternehmen, die auf der Plattform sind, wird damit ein neuer Kundenkreis zugänglich. In der Automobilindustrie haben sich zum Beispiel Plattformen und Ökosysteme wie das SupplyOn oder Catena-X etabliert .[4]

Dabei ist es wichtig zu verstehen, dass die Begriffe digitales Ökosystem und digitale Plattform nicht synonym verwendet werden können. Die digitale Plattform ist ein IT-System, welches durch ein Unternehmen betrieben wird. Sie ist eine technische Umsetzung für das Ökosystem. Das Ökosystem als Ganzes besteht aber aus weiteren Komponenten: den Teilnehmenden (Anbietende und Kund:innen), den angebotenen Diensten (Services) und nicht zuletzt auch aus der IT-Infrastruktur, die genutzt wird. Die Datensicherheit in einem solchen Ökosystem betrifft somit alle Beteiligten und muss über alle Ebenen gewährleistet sein. Einen besonderen Aspekt, den es hier zu betrachten gilt, ist der sichere und vertrauensvolle Umgang mit Daten, welcher oft als Datensouveränität bezeichnet wird .[5]

Datensouveränität und digitale Souveränität

Eine offizielle Definition des Begriffs Datensouveränität existiert nicht. Wir verstehen darunter die größtmögliche Kontrolle, Einflussnahme und Einsicht des Datenanbieters über die Verwendung seiner Daten. Der Datengebende soll befähigt werden, Transparenz bezüglich der Nutzung seiner Daten zu erhalten. Die Datensouveränität wird in diesem Kontext als der wichtigste Sicherheitsaspekt des Datenaustauschs gesehen und zugleich auch als die Kernherausforderung, welche es zu lösen gilt.

4 Titze et al. (2021).
5 Jung/Naab (2020).

Im gleichen Zug wird oft auch die digitale Souveränität genannt, wobei die beiden Begriffe häufig miteinander verwechselt werden. Der Austausch von Daten im industriellen sowie im privaten Kontext erfolgt in der Regel über große Cloud- und IT-Infrastrukturanbieter. Oft handelt es sich hierbei um große Unternehmen, die ihre Marktmacht ausnutzen können um die Kund:innen auf verschiedenen Ebenen abhängig zu machen oder die außerhalb des europäischen Rechtsrahmens ihren Sitz haben. Diese Abhängigkeit wird für die Nutzer:innen der Clouds zunehmend zu einer existenziellen Frage. Dabei sind Clouds und digitale Plattformen wichtige Elemente der Digitalisierung. Sie bilden die Basis und Lebensadern aktueller und künftiger Geschäftsmodelle, da neue innovative Technologien wie Künstliche Intelligenz auf große Datenmengen angewiesen sind (Big Data). Die Unabhängigkeit der Nutzer:innen von Anbietern wird als digitale Souveränität bezeichnet .[6]

Um die hier in Europa vorherrschenden Werte wie Souveränität, Sicherheit, Offenheit und Transparenz, sowie die geltenden Datenschutzbestimmungen zu gewährleisten, ist sowohl Datensouveränität als auch digitale Souveränität notwendig. Hierfür müssen die Cloud-Infrastrukturen herstellerunabhängig und frei nutzbar sein. Das bedeutet auch, ein Wechsel zwischen verschiedenen Infrastrukturanbietern muss ohne weiteres möglich sein. Um dieses Ziel zu erreichen haben sich mehr als 200 Unternehmen, Verbände und Forschungsinstitute unter Führung des BMWi zusammengeschlossen und arbeiten gemeinsam an der nächsten Generation der europäischen Dateninfrastruktur – Gaia-X.

Gaia-X – ein europäisches Datenökosystem

Das europäische Projekt Gaia-X hat es sich zur Aufgabe gemacht, die Herausforderungen der digitalen und der Datensouveränität zu lösen. Hierzu wird aktuell ein Vorschlag erarbeitet, der es Unternehmen ermöglichen soll, geschlossene Datenräume zu schaffen, in denen Daten nach den Leitprinzipen von Gaia-X ausgetauscht werden können. Durch Harmonisierung und Vereinheitlichung sollen zudem die Einstiegshürden in die digitale Welt und das Ökosystem deutlich verringert werden. Eine solche Hürde ist zum Beispiel der Wechsel zwischen verschiedenen Cloudanbietenden.

Leitprinzipien von Gaia-X

1. Europäischer Datenschutz
2. Offenheit und Transparenz
3. Authentizität und Vertrauen
4. Souveränität und Selbstbestimmtheit
5. Freier Marktzugang und europäische Wertschöpfung
6. Modularität und Interoperabilität
7. Nutzerfreundlichkeit

BMWi (2019)

Wie ist Gaia-X aufgebaut?

Das Gaia-X Ökosystem besteht aus drei Teilen: dem Datenökosystem, dem Infrastrukturökosystem und den föderierten Diensten. Das Datenökosystem stellt Datenräume bereit, die auf gemeinsamen Regeln basieren. Daten und Serviceangebote können so transparent und branchenübergreifend ausgetauscht und genutzt werden. Das Infrastrukturökosystem stellt Infrastrukturangebote von verschiedenen Anbietern interoperabel zur Verfügung. Anbieter können so gemeinsam ihre Angebote miteinander verknüpfen oder ausbauen. Anwender:innen haben die Möglichkeit, im Ökosystem aus einem Pool von Anbietern zu wählen und jederzeit zu wechseln. Das Risiko einer Abhängigkeit wird so stark reduziert. Die föderierten Dienste (Services) sind Datendienste, die im sicheren Datenraum genutzt werden können. Föderiert heißt in diesem Fall, dass bestimmte Voraussetzungen erfüllt sein müssen, um seine Dienste im Gaia-X Ökosystem anbieten zu dürfen. Damit wird ein hohes Maß an Sicherheitsanforderungen garantiert und die Datensouveränität gewahrt. Grundlage der Regeln und des Systems bilden die Leitprinzipien (siehe Infobox). Unternehmen, die sich nicht an diese halten, können nicht Teil des Ökosystems werden.[7]

Datenraum *Industrie 4.0/KMU*

Im Gaia-X Ökosystem werden alle drei Komponenten zu einem Datenraum vereint. Unterschiedliche Branchen benötigen unterschiedliche Datenräume. Hierzu gibt es im Gaia-X Ökosystem die sogenannten Domänen. Aktuell existieren sechs Domänen, die an individuellen Datenräumen arbeiten: Industrie4.0/KMU, Gesundheitswesen, Energie, Mobilität, Finanz- und Versicherungswesen sowie Raumfahrt.

6 Jung/Naab (2020).

7 Bundesministerium für Wirtschaft und Energie (2019).

Wie sieht ein Datenraum konkret aus und welchen Mehrwert bietet er? Das möchten wir am Beispiel der SmartFactory-KL aufzeigen, Konsortialführer des Mittelstand-Digital Zentrums Kaiserslautern und Demonstrator eines Anwendungsfalls im Gaia-X Konsortium. Im Projekt „Modular Smart Manufacturing Gaia-X Testumgebung" (SmartMA-X) prüfen die Forscher:innen, ob die definierten Anforderungen im Datenraum *Industrie4.0/KMU* der Realität standhalten können.

Die SmartFactory Kaiserslautern ist als Verein mit dem Namen „Technologie-Initiative SmartFactory-KL e.V." registriert. Die knapp 50 Mitglieder stammen aus Forschung und Industrie. In verschiedenen Arbeitsgruppen erarbeiten Expert:innen aus Unternehmen und wissenschaftlichen Einrichtungen Lösungen anhand realer Aufgabenstellungen aus der Industrie. Die SmartFactory Kaiserslautern (SF-KL) veröffentlichte 2019 ein Update zu Industrie 4.0, dass sie *Production Level 4* (PL4) nannte. In diese Vision zur Produktion der Zukunft flossen die praktischen Erfahrungen mit Industrie 4.0 ein, sowie neue technologische Möglichkeiten, wie beispielsweise neue KI-Methoden. Sie denkt die Architektur der Produktion in einem großen Maßstab neu, um eine flexible, stabile, nachhaltige und ökonomische Fertigung für individuelle Waren zu ermöglichen. Kernidee ist das Anbieten von Fertigungsfähigkeiten (Skills) unterschiedlicher Unternehmen auf einer digitalen Plattform, die von anderen Unternehmen für ihre Produktion genutzt werden können: Manufacturing-as-a-service (MaaS).[8]

Die Voraussetzung für dieses Produktionsmodell ist ein vertrauenswürdiges Datenökosystem, an das alle beteiligten Akteure standardisiert eingebunden werden können, um eine vertrauliche und sichere Kommunikation zu garantieren. Gaia-X ist solch ein Datenökosystem, welches den sicheren Datenraum *Industrie 4.0/KMU* zur Verfügung stellt. Die SF-KL wurde von der Bundesregierung als die zentrale Gaia-X Testumgebung für die Domäne „Industrie 4.0" und den Use Case ‚Produktion' ausgewählt.[9]

Use Case der SmartFactory-KL

Im dem von der SF-KL vorgestellten Szenario sind verschiedene Unternehmen der Fertigungsindustrie im Datenraum *Industrie4.0/KMU* aktiv und bieten Produktionskapazitäten als Service in Gaia-X an. Zusätzlich zu den Produktionsservices werden auch Datenservices angeboten, welche von Produktionsmaschinen genutzt werden können (z. B. Services der Künstlichen Intelligenz wie

8 Technologie-Initiative SmartFactory KL e.V. (2020).
9 Bundesministerium für Wirtschaft und Energie (2021).

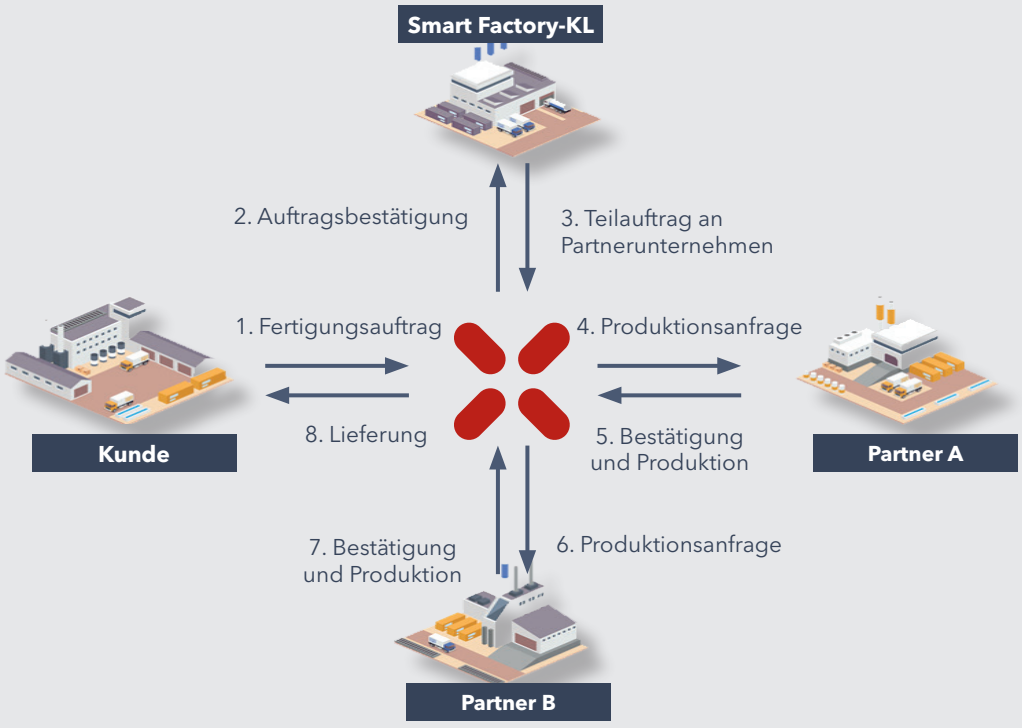


Abbildung 1: Szenario des Use Cases der SmartFactory-KL (Quelle: SmartFactory-KL)

vorausschauende Wartung – Predictive Maintenance). Das Szenario sieht so aus: Im Ökosystem soll ein Produktionsauftrag von einem Unternehmen (Kunde) vergeben werden. Hierzu ist es notwendig, vertrauliche Daten auszutauschen, wie zum Beispiel computergestützte 3D-Zeichnungen, Verträge oder ähnliches. Um die Daten sicher zu übermitteln, werden diese im Datenraum *Industrie4.0/KMU* zwischen dem Kunden und der SmartFactory-KL ausgetauscht.

Bei der Validierung der Bestellung stellt das System fest, dass der Auftrag nicht vollständig von der SmartFactory-KL hergestellt werden kann. Die Produktion erfordert zwei Teilprozessschritte, die von Partnerunternehmen im Ökosystem erfüllt werden können. Hierfür müssen eng abgestimmte Produktionsdaten zwischen der SmartFactory-KL und den Partnerunternehmen A und B ausgetauscht werden. Das geschieht wieder im Datenraum *Industrie4.0/KMU*. Vor, während und nach der Produktion werden kontinuierlich Daten zwischen diesen Unternehmen ausgetauscht und das immer nach den Regeln des Gaia-X Ökosystems im Datenraum. Dadurch wird die Datensouveränität gewahrt und wichtige sicherheitskritische Aspekte stets mit einbezogen.

Dieser Use-Case zielt zusätzlich in Richtung resilienter Produktion, denn er zeigt, dass im Falle eines Lieferengpasses oder Modulausfalls die Produktionsplanung schnell auf die Störung reagieren kann, ohne dass es zu einem Produktionsstillstand kommen muss. Die Produktionsprozesse, die in der eigenen Fabrik ausfallen oder fehlen, können schnell an eine andere Produktionsstätte ausgelagert werden. Auf diese Weise wird erprobt, wie in Zukunft Wertschöpfungsnetzwerke innerhalb kürzester Zeit unkompliziert auf- und umgebaut werden können (ad-hoc-Netzwerke).

Potentiale für KMU

Die Unternehmenslandschaft in Europa besteht zu 99,8 % aus kleinen und mittleren Unternehmen (KMU) (in Deutschland sind es 99,5 %)[10], weshalb das Thema Datensicherheit insbesondere für KMU immer mehr an Bedeutung gewinnt. Im Zusammenhang mit Gaia-X ergeben sich so neue Potentiale für KMU.

Datensicherheit

Gerade die Datensouveränität und Datensicherheit, die mit den Gaia-X Datenräumen einherkommen, sind hier nicht von der Hand zu weisen. Die Einigung auf ein Regelwerk, welches von einer unabhängigen Gesellschaft herausgegeben wird, vereinfacht den Einstieg in die Cloud für viele Unternehmen. In den Datenräumen können zudem Daten durchgängig erfasst und sicher geteilt werden. Das stellt einen großen Vorteil bei der Nutzung von Datenservices dar. Die Teilnahme an einem solchen Datenraum erleichtert KMU den Einstieg in neue, innovative Technologien. Solche Services, wie z. B. Anwendungen Künstlicher Intelligenz, benötigen bekanntlich eine große Menge an Daten, um zu funktionieren und auch die Nutzung der Technologien selbst erfordert wieder einen Datentransfer. Über einen Datenraum können diese Daten sicher und einfach geteilt werden.

Potentiale für KMU

- Regionale Ecoparks
- Wertschöpfungsnetzwerk
- Durchgängige Datenerfassung
- Nutzung von KI-Services
- Resiliente Produktion

Wertschöpfungsnetzwerke und regionale Ecoparks

Ein weiterer Vorteil ergibt sich aus der Bereitstellung von Produktion- und Datenservices im Ökosystem selbst. Für die Fertigungsindustrie entsteht die Möglichkeit, ad-hoc-Wertschöpfungsnetzwerke schnell und einfach zu bilden. Dies führt zu neuen Produktionsmöglichkeiten für Unternehmen. Vorher nicht bekannte Lieferketten sind so leicht zu identifizieren und neue Geschäftsmöglichkeiten entstehen. Im Beispiel der SmartFactory-KL können unternehmensübergreifende Lieferketten gebildet werden. Die digitale Anbindung wird durch die Nutzung des Ökosystems stark vereinfacht und ein Wertschöpfungsnetzwerk entsteht. Wenn man nun einen Schritt weiterdenkt, können hierdurch regionale Wertschöpfungsnetzwerke gebildet werden. Diese regionalen Ecoparks stellen Produkte vor Ort her – ein im Sinne der Nachhaltigkeit und Klimabilanz überaus erfreulicher Nebeneffekt.

Teilnehmen an Gaia-X

In unserem Beitrag haben wir aufgezeigt, wie das Gaia-X Ökosystem den Datenaustausch zwischen Unternehmen verändern wird. Datensicherheit und Datensouveränität als zentrale Qualitätseigenschaft von Digitalen Ökosystemen werden in Gaia-X ganzheitlich in die Gestaltung miteinbezogen. Aktuell befindet sich die

10 Braun (2021).

Entwicklung des Gaia-X Ökosystems noch im Aufbau. Für KMU besteht somit noch die Möglichkeit, gestaltend am Ökosystem teilzunehmen. Notwendige Informationen finden Sie auf der offiziellen Homepage von Gaia-X: *https://gaia-x.eu/how-to-join*.

Falls Sie Interesse am Use-Case der SmartFactory-KL haben, kommen Sie gerne auf uns zu. Im Rahmen des Projektes smartMA-X werden zwei Demonstratoren gebaut beziehungsweise weiterentwickelt, die veranschaulichen, wie Gaia-X, Industrie 4.0 und die Fertigungsindustrie gemeinsam funktionieren. Auch der Demonstrator PAUL (Produktion und Automatisierung Erleben) des Mittelstand-Digital Zentrums Kaiserslautern wird im Rahmen von smartMA-X ausgebaut werden. Der Schulungsdemonstrator zeigt auf spielerische Weise, wie Digitalisierung in der Fertigung aussehen kann. Im Zuge der Weiterentwicklung wird PAUL als Fertigungsstätte in das Gaia-X Netzwerk integriert werden, um gerade kleinen und mittleren Unternehmen den inhaltlichen Zugang zum Thema Datensicherheit im digitalen Ökosystem Gaia-X zu erleichtern.

Literatur

DVZ - Deutsche Verkehrs-Zeitung (2021) Datenaustausch über ganze Lieferketten: Autobranche baut Netzwerk aus.

Bundesministerium für Wirtschaft und Energie (2019) Das Projekt GAIA-X. Eine vernetzte Dateninfrastruktur als Wiege eines vitalen, europäischen Ökosystems, Berlin

Bundesministerium für Wirtschaft und Energie (2021) Der Datenraum Industrie 4.0. Die Plattform Industrie 4.0 lädt ein, die digitalen Ökosysteme von morgen zu gestalten, Berlin

Titze, Christian; McNeill, William; Johns, Brock; De Muynck, Bart (2021) Magic Quadrant for Multienterprise Supply Chain Business Networks

Jung, Christian; Naab, Matthias (2020) Security in Digitalen Ökosystemen: Eine sichere Plattform und viel mehr. *https://www.iese.fraunhofer.de/blog/security-in-digitalen-oekosystemen-die-sichere-digitale-plattform-ist-nur-die-halbe-miete/*. Zugegriffen: 22. Juni 2021

Braun, Simone (2021) KMU im EU-Vergleich. *https://www.ifm-bonn.org/statistiken/mittelstand-im-einzelnen/kmu-im-eu-vergleich*. Zugegriffen: 22. Juni 2021

Technologie-Initiative SmartFactory-KL e.V. (2020) Fortschritt im Netzwerk. Die Demonstratorbauer 2020, Kaiserslautern

Autoren

Keran Sivalingam, M.Sc., ist Researcher bei der Technologie-Initiative SmartFactory-KL e.V. und Projektleiter von SmartMA-X, einem Use Case im Gaia-X Ökosystem. Im Projekt wird ein Demonstrator entwickelt, welcher den praktischen Nutzen von Gaia-X aufzeigen wird. Im Mittelstand 4.0-Kompetenzzentrum Kaiserslautern war er vorher lange als KI-Trainer tätig und hat kleine und mittlere Unternehmen beim Einsatz von Künstlicher Intelligenz unterstützt.

Larissa Theis, M.A., ist Content Marketing Managerin bei der Technologie-Initiative SmartFactory-KL e.V. und für die Öffentlichkeitsarbeit des Mittelstand-Digital Zentrums Kaiserslautern zuständig. Sie ist unter anderem für die Pressearbeit und Kommunikation des Zentrums nach außen über die Webseite und Social-Media-Kanäle verantwortlich und erstellt Text-, Bild- und Videomaterial über das Zentrum.

Roland Gröll, Julian Herr, Thomas Batz, David Ruge

Vom sicheren Datenaustausch zur kollaborativen Nutzung von Daten

Der sichere Datenaustausch ist vor allem durch die klassische Verschlüsselung (Kryptographie) geprägt. Dabei entwickeln sich das Thema und die Anforderungen immer weiter. Lag der Schwerpunkt früher auf der Verschlüsselung von Daten zwischen zwei Personen oder Unternehmen, besteht heute die Herausforderung darin, dass eine gemeinsame Nutzung bzw. ein Datenaustausch zwischen einer Vielzahl an Nutzern (Usern) ermöglicht werden soll, ohne dabei zu viele Informationen preiszugeben und Datenschutz, Datensicherheit und Vertraulichkeit gewährleisten zu können. Diese Evolution innerhalb des sicheren Datenaustausches wird in diesem Artikel näher beleuchtet.

Daten werden für Unternehmen immer wichtiger. Für die interne Arbeit, bei der Kommunikation mit den Kunden, aber auch für die Interaktion mit anderen Unternehmen und Behörden. Dabei ist zu unterscheiden zwischen geschlossenen und offenen Kommunikationsbeziehungen: Bei geschlossenen Kommunikationsbeziehungen, wie zwischen einem Unternehmen und seinen Zulieferern, sind die beteiligten Partner, die Systeme, die zu übertragenden Daten, die Schnittstellen und die Sicherheitsmechanismen bekannt. Ein Vertrag zwischen den Beteiligten bestimmt, was mit den Daten des jeweils anderen zulässig ist und was nicht. Der Datenaustausch ist hier meist weitreichend, es werden häufig auch Echtzeitdaten, wie produzierte Menge, Qualitätseigenschaften, Liefermengen und Termine, übertragen. Charakteristisch für die geschlossenen Kommunikationsbeziehungen ist, dass sich die Partner kennen (und meist vertrauen) und eine vertragliche Regelung zwischen ihnen besteht. In offenen Kommunikationsbeziehungen oder Plattformen (Plattformökonomie) können sich Unternehmen anmelden und mit anderen, auch unbekannten Unternehmen, interagieren und beispielsweise Bestellungen aufgeben oder Daten kaufen. In einem ersten Schritt haben sie nur eine Vertragsbeziehung mit dem Plattformbetreiber. Derartige offene Plattformen bieten die

Möglichkeit, sich breiter zu präsentieren und auch mit bisher unbekannten Unternehmen in Geschäftsbeziehung zu treten sowie eine effizientere, digitale Abwicklung der Geschäftsvorgänge zu erreichen.

Bei einer derartigen Plattform ist Datenschutz ein wesentlicher Aspekt, damit andere nicht unbefugt Daten lesen und missbrauchen können. Ein weiterer, mindestens genau so wichtiger Aspekt ist, dass potentielle Geschäftspartner dazu berechtigt werden müssen, zumindest zeitweise auf vertrauliche Daten zugreifen zu können, um den Geschäftsvorgang zu initiieren und durchzuführen.

Im Folgenden zeigen wir dies genauer am Beispiel eines offenen, internetbasierten Marktplatzes für die industrielle Produktion und vertiefen anschließend die Themen Vertraulichkeit und Integrität.

Marktplatz für die industrielle Produktion (Smart Factory Web)[1]

Eine derartige Plattform ist der vom Fraunhofer IOSB betriebene, offene und internetbasierte Marktplatz für die industrielle Produktion Smart Factory Web (SFW), der als Labordemonstrator zusätzlich die Möglichkeit bietet, verschiedene Ausgestaltungen einer solchen Plattform zu entdecken.

Im SFW können sich Teilnehmer registrieren und entweder ihre Fähigkeiten oder Produkte beschreiben und diese mittels „Plug and Work" einfach integrieren (Anbieter) oder ihren Bedarf (Kunde) an solchen spezifizieren (siehe Abbildung 1). Das System gleicht Nachfrage und Angebot miteinander ab und erstellt eine Liste der passenden Angebote. Es ist auch möglich, komplexe Fertigungsaufträge zu spezifizieren, bei denen verschiedene Anbieter jeweils Teile der Gesamtaufgabe übernehmen, wodurch eine zusammengesetzte Lieferkette entsteht.

Der Nutzen einer Plattform steigt, wenn neben der reinen Fähigkeit ein Produkt zu erzeugen weitere Informationen, wie die verfügbare Menge, die mögliche Lieferzeit, der Preis oder Eigenschaften des Produktionsprozesses (faire Produktion, keine Kinderarbeit, keine Konfliktmineralien verwendet, Produktionsländer etc.), verfügbar sind. Dieses Wissen ist für einen potenziellen Kunden unerlässlich und für einen potenziellen Mitbewerber sehr hilfreich. Daher muss die Plattform zwischen diesen Arten der Nutzer differenzieren können und dafür sorgen, dass nur der potenzielle Kunde diese Daten zweckgebunden innerhalb des Vertragskontextes nutzen kann. Dies kann mittels der Mandantenfähigkeit innerhalb der Plattform und während der Nutzung über den Industrial Data Space sichergestellt werden.

1 Links zu Smart Factory Web:
https://www.smartfactoryweb.de/servlet/is/94960/
https://www.iosb.fraunhofer.de/de/projekte-produkte/smart-factory-web.html

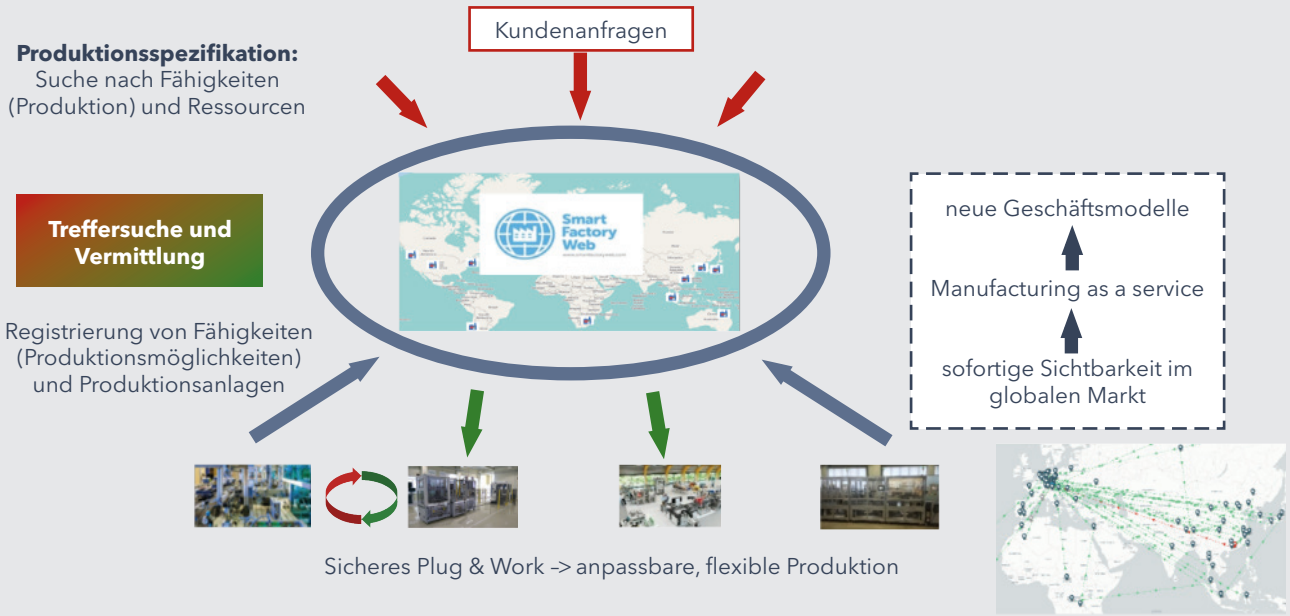


Abbildung 1: Produzenten und Kunden im Smart Factory Web

Mandantenfähigkeit bedeutet, dass innerhalb eines zentralen Systems bestimmte eigene Daten zusätzlich nur von demjenigen gesehen werden können, für den sie explizit freigegeben wurden. Andere Unternehmen (Mandanten) sehen diese zunächst nicht.

Nach der Suche geeigneter Lieferanten erfolgt üblicherweise das Aushandeln des Lieferkontraktes, was wiederum auch ein Bestandteil der Plattform sein kann. Je nach Plattformgestaltung wird der Vertrag direkt mit den Lieferanten oder mit der Plattform geschlossen, die dann auch für die Abwicklung des Lieferkontraktes verantwortlich ist. Während der Produktion kann der Besteller zusätzlich Informationen über die Produktion, wie aktuell produzierte Menge, voraussichtliches Lieferdatum oder Qualitätsinformation, erhalten. Alle diese Informationen sind wiederum sinnvoll für den Kunden, dürfen jedoch nicht von unbefugten Nutzern wie potenziellen Konkurrenten gesehen werden. Der Schutz kann wiederum durch die Mechanismen des Industrial Data Spaces sichergestellt werden.

Ein weiterer Sicherheitsaspekt ist der Schutz vor dem Betreiber der Plattform. Falls dieser auch als Produzent innerhalb der Plattform auftritt, hat er möglicherweise ein Interesse daran, sehr attraktive Produkte zu identifizieren und unter eigener Regie anzubieten. Hier ist ein technischer Schutz schwierig zu realisieren; vertragliche Regelungen oder ein neutraler Plattformbetreiber sind hier die Mittel der Wahl.

Insgesamt ist zu sehen, dass im Rahmen der Plattformökonomie vielfältige Chancen erwachsen, aber auch erhebliche organisatorische und technische Sicherheitsmaßnahmen notwendig sind. Zum beiderseitigen Nutzen muss ein Datenökosystem entstehen, in dem berechtigte Partner zeitweise sehr individuelle und vertrauliche Daten sehen und austauschen können.

Vertraulichkeit und Integrität

Auf technischer Ebene lässt sich eine Übertragung von individuellen und vertraulichen Daten dann als gesichert beschreiben, wenn mindestens die beiden Schutzziele „Vertraulichkeit" und „Integrität" durch die Methoden des Datenaustausches garantiert werden. Obwohl in der Praxis Verfahren genutzt werden können, die beide Schutzziele gleichzeitig realisieren, ist es ebenso denkbar, auf eine Vertraulichkeit der Daten zu verzichten, sofern lediglich die Unverfälschtheit der übertragenen Daten nachvollziehbar sein muss.

Erreicht wird das Schutzziel der Vertraulichkeit i.d.R. über sogenannte Verschlüsselungsverfahren. Dabei wird ein Datensatz unter Zuhilfenahme eines kryptographischen Schlüssels chiffriert. Ein daraufhin erhaltenes Chiffrat kann nun über einen **potenziell nicht vertrauenswürdigen Kanal** (wie zum Beispiel das Internet, welches erst durch die hier beschriebenen Maßnahmen vertrauenswürdig wird) dem Empfänger zugeschickt werden. Sofern ein geeignetes Verschlüsselungsverfahren korrekt eingesetzt und das zugehörige Schlüsselmaterial geheim gehalten wurde, ist es für eine dritte Partei mit Zugriff auf dieses Chiffrat unmöglich, die darin enthaltenen Daten sichtbar zu machen.

In vielen Fällen bietet allerdings das verwendete Verschlüsselungsverfahren allein noch keinen Schutz vor Manipulation der Daten durch Dritte. So könnte beispielsweise ein potenzieller Angreifer, welcher den Kommunikationskanal des Senders und Empfängers kontrolliert, beginnen, die verschlüsselten Daten zu verändern. Diese Veränderungen können bei der Dechiffrierung wiederum zu einem anderen ursprünglichen Datensatz führen, welcher nicht dem des Absenders entspricht. Somit kann es einem Angreifer trotzdem gelingen die übertragenen Daten ohne deren genaue Kenntnis zu manipulieren.

Um derartige Manipulationen auf dem Transport auf Empfängerseite zu erkennen, ist es notwendig, die Daten zusätzlich auf einem sogenannten authentifizierten Kanal zu übertragen. Dies kann beispielsweise durch die Verwendung von digitalen Signaturen oder auch einem authentifiziertem Verschlüsselungsverfahren erreicht werden. Authentifizierte Verschlüsselung ist ein grundlegender kryptographischer Baustein für sichere Systeme und Anwendungen. Das Ziel ist, sowohl Vertraulichkeit als auch Authentifizierung in einer Kommunikation zweier Parteien über einen unsicheren Kanal zu gewährleisten um einen **sicheren Kanal** herzustellen. Wichtig ist hierbei zu betonen, dass eine Manipulation der Daten auf dem Übertragungsweg nicht verhindert, vom Empfänger jedoch erkannt werden kann, bevor weitere Datenverarbeitungsprozesse gestartet werden.

Eine weit verbreitete Verwendung von authentifizierten und vertraulichen Datenkanälen findet sich beispielsweise in der alltäglichen Benutzung des Web Browsers. Dieser kann sensible Daten per „Transport Layer Security" (TLS) mit einer Website teilen, sofern die Website dieses Verfahren unterstützt.

Bei der reinen Verwendung von Signaturen/Verschlüsselungsverfahren lässt sich allerdings lediglich feststellen, dass man mit dem Besitzer eines bestimmten Schlüssels kommuniziert. Um diesen Besitzer eindeutig einer Partei zuzuordnen (Rückschluss vom kryptographischen Schlüsselmaterial auf die Identität der Partei), bietet sich die Verwendung einer Public Key Infrastruktur (PKI) an. Diese erlaubt es den Parteien, sich bei der PKI

zu registrieren. Hierbei stellt die PKI einer Partei ein Zertifikat über deren eigene Identität und ihr registriertes, kryptographisches Schlüsselmaterial aus.

Allerdings reicht ein sicherer Datenaustausch allein nicht in allen Fällen aus. Im Folgenden wollen wir eine Herausforderung bei der Kollaboration mehrerer Unternehmen vorstellen, wie sie im Rahmen des Forschungsprojekts ReKoNet[2] untersucht werden. Neben der Notwendigkeit, die zur Kollaboration benötigten Eingabedaten vertraulich und authentifiziert zwischen allen Teilnehmern auszutauschen, soll zusätzlich sichergestellt sein, dass kein Unternehmen die Kenntnis von den Eingabedaten eines anderen Unternehmens erlangt. Es soll also lediglich das gemeinsame Ergebnis des Kollaborationsalgorithmus nach der Auswertung aller Eingabedaten an alle Teilnehmenden kommuniziert werden. In der folgenden Textbox legen wir unser Szenario genauer dar.

2 *http://projekt-rekonet.de/*

Szenario kollaborative Datennutzung

Die Produktion eines Hochpräzisionsbauteils setzt sich aus der Produktion mehrerer Einzelbauteile bei verschiedenen Zuliefererfirmen sowie der Endmontage der Einzelbauteile bei einer Abnehmerfirma zusammen. Da Produktionsprozesse immer mit einer gewissen Ungenauigkeit einhergehen, die sich beispielsweise in Abweichungen von Fertigungsmaßen widerspiegeln, ist es für die Abnehmerfirma beim Einkauf der Einzelteile entscheidend einschätzen zu können, inwieweit diese in der Endmontage noch zueinander passen werden.

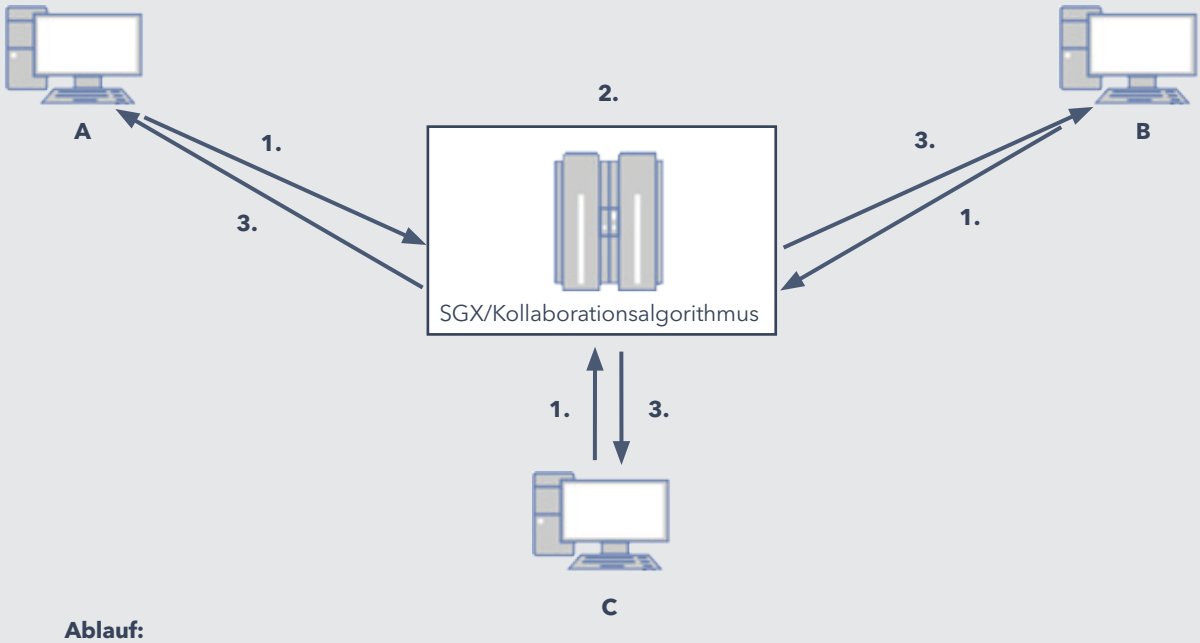
Sowohl der Zulieferer als auch der Kunde haben jedoch ein Interesse daran, möglichst wenige Daten auszutauschen. Einige der Daten könnten der jeweils anderen Partei einen Vorteil in der Verhandlung von zukünftigen Produkten oder Dienstleistungen bringen oder Details über einen geheimen Fertigungsprozess offenbaren.

Um möglichst wenige Daten preiszugeben, könnte man eine vertrauenswürdige, weitere Partei (z. B. einen Notar) hinzuziehen. Der Zulieferer und der Kunde könnten die Daten an die vertrauenswürdige Partei übermitteln. Diese berechnet anhand dieser Daten eine Kombination und Bepreisung der Bauteile und gibt dieses Ergebnis zurück an die Kunden und den Zulieferer. Wenn man nun davon ausgeht, dass die weitere Partei (also hier der Notar) tatsächlich vertrauenswürdig ist und die Eingabedaten nicht herausgibt, bleiben diese Daten vertraulich.

Um diese Herausforderung technisch zu lösen, kann man sogenannte Trusted Execution Environments (TEE) verwenden. Diese sind als Hardwarelösung Teil der Funktionalität der Ausführungseinheiten eines Rechners. Im Modell unseres Kollaborationsalgorithmus wird der Hersteller des Rechners notwendigerweise zu einer Drittpartei, deren Angaben zur Vertrauenswürdigkeit ihrer Lösung auf das Szenario passen müssen. Beispielsweise ist die TEE so konstruiert, dass keine anderen Prozesse auf dem Rechner auf die Daten des Codes innerhalb der TEE zugreifen können. Somit soll verhindert werden, dass ein anderer Benutzer des Systems die Eingabedaten oder Zwischenergebnisse der Berechnung erfährt. Dies gilt auch für das Betriebssystem.

Der Hersteller stellt zudem eine Infrastruktur zur Verfügung, die es allen Teilnehmern der Kollaboration erlaubt, die Integrität des in der TEE ausgeführten Codes vor dem Senden der Eingabedaten zu überprüfen.

Konkret entwickeln Zulieferer und Kunde zusammen den Code, der die Berechnung zur Paarung und Bepreisung durchführt. Eine der beteiligten Parteien (es spielt keine Rolle, welche) stellt einen Server zur Verfügung und liefert den Code darauf aus. Jetzt können alle Parteien über eine Funktionalität der TEE (die sogenannte Remote Attestation) überprüfen, ob der Code unverändert ausgeliefert wurde. Wenn das sichergestellt ist, können sie eine authentifizierte und verschlüsselte Verbindung zwischen sich selbst und der TEE aufbauen. Die Verschlüsselung stellt sicher, dass selbst der Betreiber des Servers die Daten nicht einsehen kann. Die Authentifizierung stellt sicher, dass der Betreiber des Servers die Daten nicht modifizieren kann. Da davon ausgegangen wird, dass alle Parteien geprüft haben, dass der richtige Code ausgeführt wird, können sie sicher sein, dass die Daten die TEE selbst nicht verlassen und die Berechnung ohne Manipulation durchgeführt wird. Eine Übersicht über den beispielhaften Ablauf findet sich in Abbildung 2.



Ablauf:

1. Teilnehmer A, B und C schicken ihre vertraulichen Eingabedaten an die TEE
2. Der Server/die TEE führt den Kollaborationsalgorithmus mit den vertraulichen Daten aus 1. aus
3. Die Teilnehmer A, B und C erhalten das Ergebnis des Kollaborationsalgorithmus ohne die Eingaben der jeweils anderen beiden Parteien zu lernen

Abbildung 2: Ablauf des Kollaborationsalgorithmus

Fazit

Klassische Kommunikationsvorgänge zwischen Unternehmen mit Kunden und Behörden haben im Alltagshandeln weiterhin einen hohen Stellenwert. Die dort bestehenden Anforderungen an Datenschutz, Datensicherheit und Vertraulichkeit müssen erfüllt werden. Dies kann durch die Entwicklung eines klassischen Kryptokonzepts[3] gut gewährleistet werden, wie es teilweise in Unternehmen bereits geschehen ist.

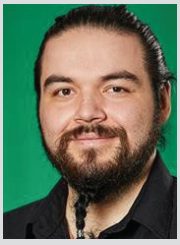
Der Aufwand bei der Umsetzung ist auch für kleine und mittlere Unternehmen (KMU) überschaubar. Die Anforderungen des digitalen Zeitalters gehen für viele Firmen deutlich weiter. Die Präsenz in offenen Marktplätzen – sei es als Anbieter von Produkten bzw. Dienstleistungen oder als Kunden – wird immer wichtiger. Damit einher geht auch eine stärkere Offenlegung des eigenen Angebots bzw. des nachgefragten Produkts bzw. der Dienstleistung, der dazugehörenden Spezifikation, der nachgefragten Menge, des Preises und weiterer sensitiver Firmendaten. Offenkundig ist, dass diese Informationen für einen Berechtigten zumindest zeitweise unabdingbar sind, aber vor potenziellen Konkurrenten verborgen bleiben sollen.

Daher entwickelt sich der klassische „Sichere Datenaustausch" weiter zu einer „Kollaborativen Datennutzung". Es wird für Unternehmen immer wichtiger, gemeinsame Vorgänge und Prozesse analytisch auszuwerten, ohne gleichzeitig andere wichtige Assets preiszugeben. Dieser Herausforderung begegnen die beiden vorgestellten Beispiele.

3 *https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium_Einzel_PDFs_2021/03_CON_Konzepte_und_Vorgehensweisen/CON_1_Kryptokonzept_Edition_2021.pdf?__blob=publicationFile&v=2.*

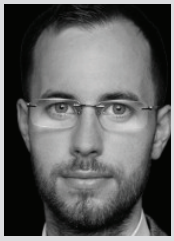
Autoren

Roland Gröll studierte Informatik am Karlsruher Institut für Technologie (KIT) mit den Schwerpunkten Algorithmentechnik und Kryptographie. Seit April 2017 ist Roland Gröll am Forschungszentrum Informatik als Wissenschaftlicher Mitarbeiter im Kompetenzzentrum IT-Sicherheit tätig. Hier ist sein Schwerpunkt Postquantenkryptographie.



Julian Herr studierte Mathematik und Informatik mit den Schwerpunkten Kryptographie und Sicherheit. Seit 2019 ist er als wissenschaftlicher Mitarbeiter am Kompetenzzentrum IT-Sicherheit am Forschungszentrum Informatik mit den Schwerpunkten Kryptographie und Penetration Testing tätig.

Thomas Batz arbeitet beim Fraunhofer IOSB (Fraunhofer Institut für Optronik, Systemtechnik und Bildauswertung) in Karlsruhe, welches am Mittelstandskompetenzzentrum Stuttgart beteiligt ist. Schwerpunkte seiner Arbeit sind Plattformökonomie, IT-Sicherheit und Anforderungsanalyse komplexer IT-Systeme.



David Ruge studierte Politikwissenschaften an der Universität Trier und der Freien Universität Berlin. Seit 2017 ist er als wissenschaftlicher Referent am Kompetenzzentrum IT-Sicherheit am Forschungszentrum Informatik mit den Schwerpunkten Informationssicherheit tätig.

Das Mittelstand 4.0-Kompetenzzentrum Stuttgart führt kleine und mittlere Unternehmen im Rahmen von Workshops und Projekten an Themen der Digitalisierung heran. Es informiert und unterstützt bei der Service- und Geschäftsmodellentwicklung innerhalb des Themenfelds Gebäude. Zudem werden die Bereiche Gesundheit, IT-Sicherheit, Mobilität und Produktion fokussiert.

www.digitales-kompetenzzentrum-stuttgart.de

Mittelstand 4.0
Kompetenzzentrum
Stuttgart

Sandra Balz

Mehr IT-Sicherheit für den Mittelstand mit dem Sec-O-Mat von TISiM

Der Praxisreport Mittelstand von Deutschland sicher im Netz e.V. 2020 hat gezeigt, dass jeder vierte Betrieb über keinerlei Datensicherung verfügt. Nur jedes fünfte Unternehmen achtet laut Report auf verschlüsselte E-Mails. Hier braucht es niedrigschwellige Unterstützungsangebote. TISiM – die Transferstelle IT-Sicherheit im Mittelstand bündelt und sortiert bestehende Angebote, um sie zielgerichtet an kleine und mittlere Unternehmen sowie Handwerksbetriebe und Selbstständige zu vermitteln.

Mit dem durch TISiM entwickelten onlinebasiertem Tool, dem Sec-O-Mat können Unternehmen, Freiberufliche und Handwerksbetriebe nach einer kurzen Unternehmensbefragung bedarfsgerechte Umsetzungsvorschläge zur Verbesserung der IT-Sicherheit erhalten.

Damit der Sec-O-Mat Empfehlungen aussprechen kann, benötigt er Informationen über die Unternehmen. Dabei ist das Ziel, den Aufwand für Anwendende so gering wie möglich zu halten.

Zunächst werden wenige Fragen beantwortet. Diese bestehen aus allgemeinen Angaben zum Unternehmen, den jeweiligen Bereichen im Unternehmen, in denen IT-Systeme eingesetzt werden, sowie den potenziellen Auswirkungen, die verschiedene Schadensszenarien in Unternehmensbereichen haben könnten.

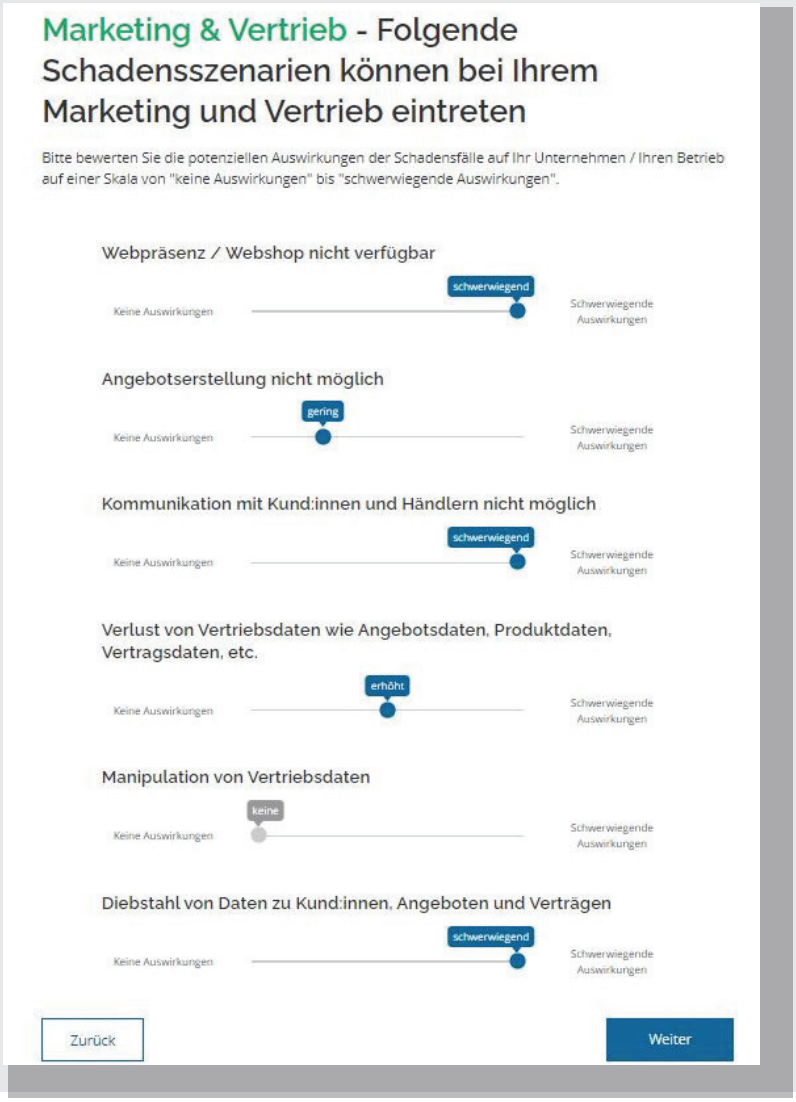
Möchte sich nun ein Unternehmen darüber informieren, welche Maßnahmen konkret umgesetzt werden müssen, um die Organisation IT-sicher zu gestalten, startet der Sec-O-Mat mit den Unternehmenseckdaten. Um den Weg von Befragung bis TISiM-Aktionsplan bestmöglich darzustellen, zeigen wir dies anhand eines fiktiven Unternehmens auf. Das Unternehmen hat 14 Mitarbeitende von denen elf einen Internetzugang für berufliche Zwecke nutzen. Das Unternehmen ist in der Handelsbranche mit einem eigenen Online-Shop tätig und nutzt weder externe Dienstleister noch eigene IT-Mitarbeitende. Computer und IT-Systeme werden in den Bereichen Ein- und Ausgangslogistik, Kundendienst, Personalmanagement, Beschaffung und Marketing und Vertrieb eingesetzt.

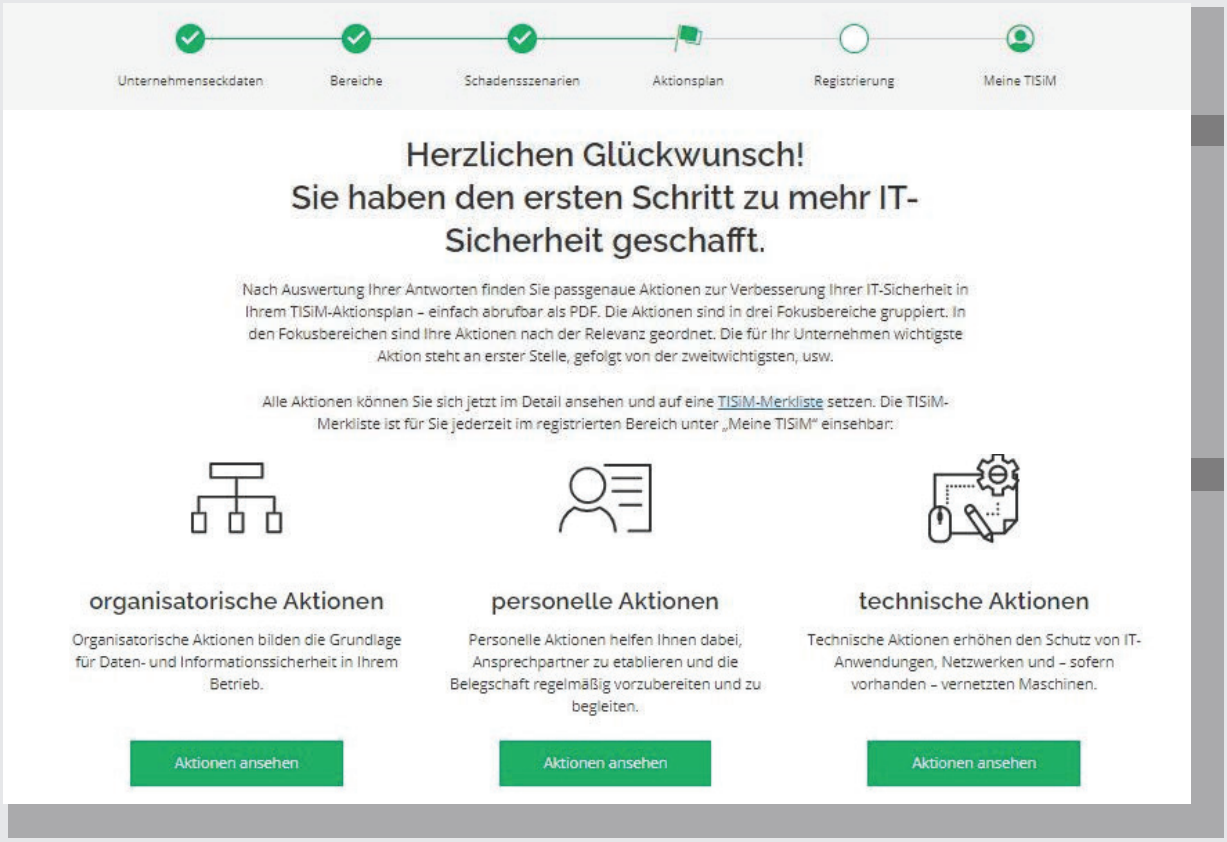
Im nächsten Schritt beurteilt das Unternehmen die potenziellen Auswirkungen der Schadensfälle auf das Unternehmen auf einer Skala von "keine Auswirkungen" bis "schwerwiegende Auswirkungen". Hierbei werden alle Bereiche abgefragt, die in der Befragung zuvor angegeben worden sind („Wo setzen Sie Computer und IT-Systeme ein?").

Besonders schwerwiegend wäre für unser fiktives Unternehmen, wenn Wareneinlagerung oder die Bestandsabfrage aufgrund eines IT-Sicherheitsvorfalls nicht möglich sind, da diese Informationen für die Verkäufe im Onlineshop unerlässlich sind. Zudem wäre es fatal für die Reputation des Unternehmens, wenn eine Kommunikation mit der Kundschaft nicht möglich ist, ebenso wie der Diebstahl von Daten zu ebendieser oder zu Aufträgen. Große finanzielle Einbußen müsste das Unternehmen auch verbuchen, wenn der Webshop nicht mehr verfügbar wäre oder die Leistungserbringung nur eingeschränkt möglich wäre.

Ist die Beurteilung der Schadensszenarien abgeschlossen, erhält das Unternehmen den TISiM-Aktionsplan und kann diesen abspeichern oder ausdrucken und sich zum Nachhalten der Maßnahmen registrieren. Nachgehalten werden die Maßnahmen zum Beispiel durch regelmäßige Erinnerungen, Newsletter mit aktuellen Informationen zu Sicherheitsverletzungen und Informationen zu Neuigkeiten im Projekt.

Der im Anschluss an die Befragung ausgespielte TISiM-Aktionsplan enthält am Bedarf des Unternehmens orientierte Umsetzungsvorschläge. Diese werden drei Fokusbereichen zugeordnet: Organisatorische, personelle und technische Aktionen. Organisatorische Aktionen (z. B.: Verbindungen mit externen Netzwerken regeln oder





Passwortregeln festlegen) bilden die Grundlage für Daten- und Informationssicherheit in Betrieben. Personelle Aktionen (z. B.: Sicherheitsbewusstsein steigern oder Schulungen durchführen) helfen dabei, Ansprechpersonen zu etablieren und die Belegschaft regelmäßig vorzubereiten und zu begleiten. Technische Aktionen (z. B.: Netzwerke trennen oder Verschlüsselung einsetzen) erhöhen den Schutz von IT-Anwendungen, Netzwerken und – sofern vorhanden – vernetzten Maschinen.

Die ausgespielten Umsetzungsvorschläge werden sorgfältig durch IT-Sicherheitsexpert:innen kuratiert. Neben einem Abgleich der eigenen Recherche mit den Selbstauskünften der Anbietenden werden insbesondere der Unternehmensstandort (auch mit Blick auf DSGVO), mögliche Abo-Fallen, stark werbende Angebote und die Passgenauigkeit für die Zielgruppe überprüft. Dadurch wird das Ziel verfolgt, möglichst zuverlässige, vertrauenswürdige und an Bedarfe der Zielgruppe ausgerichtete Umsetzungsvorschläge zu empfehlen.

Damit die Umsetzungsempfehlungen bedarfsorientiert ausgespielt werden können, arbeitet im Hintergrund des Sec-O-Maten das so genannte Smart Matching, ein intelligenter Algorithmus. Durch den Abgleich der Antworten auf die Unternehmensbefragung mittels Smart Matching werden passende Umsetzungsempfehlungen mit entsprechenden Aktionen ermittelt. Seine wesentliche Komponente ist ein Expertensystem, in dem IT-Sicherheitsexpert:innen sowohl die Schadensszenarien als auch die Aktionsbereiche vorgelegt bekommen. Sie ordnen den Schadensszenarien in feinen Abstufungen Handlungsempfehlungen zu.

Das Wissen der beteiligten Expert:innen wird aggregiert und kontinuierlich weiterentwickelt und das Tool lernt aus den Zuordnungen der Expert:innen. Je mehr TISiM-Anwendende eine Handlungsempfehlung zu einem Schadensszenario gleich zurechnen, desto höher wird die Handlungsempfehlung priorisiert. Die IT-Sicherheitsexpert:innen des Projektes haben zudem den Handlungsempfehlungen Aktionen zugeordnet, die an gängige Standards (z. B. BSI-Grundschutz, ISO 27001, VdS10000) anschlussfähig sind und haben eine zeitliche Reihenfolge für die Aktionen innerhalb einer Handlungsempfehlung festgelegt.

Als Ergebnis des Zusammenspiels aus Unternehmensbefragung, kuratierten Angeboten und Smart-Matching wird der TISiM-Aktionsplan ausgespielt.

Unser Unternehmen lädt sich nun nach Beantwortung der Unternehmensbefragung den vollständigen TISiM-Aktionsplan herunter, um einen ersten Überblick über die vorgeschlagenen Umsetzungsempfehlungen zu erhalten. Innerhalb der drei Fokusbereiche sind weitere Aktionen aufgeführt. Das fiktive Unternehmen interessiert sich vor allem für Maßnahmen zum sicheren Datenaustausch und legt auf diese ein besonderes Augenmerk. Unter organisatorischen Aktionen findet sich beispielsweise die Aktion „Verbindung mit externen Netzwerken regeln". Die hier ausgespielten Umsetzungsvorschläge können dann eingesehen und geprüft werden. Diese reichen von kostenfreien Informationsmaterialien hin zu kostenpflichtigen Dienstleistungen. Unternehmen haben hier die Wahl, das für sie passendste Angebot auszuwählen – unabhängig vom individuellen Budget.

Unserem fiktiven Unternehmen werden nun beispielsweise zur Aktion „Verbindung mit externen Netzwerken regeln" unter anderem verschiedene Checklisten und weitere Informationsmaterialen vorgeschlagen. Durch einen Klick auf den Link landet das Unternehmen so direkt beim jeweiligen Angebot und kann ohne Umwege in der Umsetzung gehen.

Im nächsten Schritt können die einzelnen Aktionsbereiche im Detail angesehen werden. Im Aktionsplan-PDF wurde nun die Aktion „Verbindung mit externen Netzwerken regeln" avisiert. In der Detailansicht kann nun eingesehen werden, dass diese Aktion drei Aktionsbereichen zugeordnet ist, die durch unterschiedliche Icons markiert sind: Absicherung des lokalen Netzwerks, Schutz vor schadhaften Webinhalten/Schadsoftware, Absicherung von Cloud-Zugängen.

Die Aktionen können zudem auf eine TISiM-Merkliste gesetzt und so zusätzlich priorisiert und sortiert werden. Unser fiktives Unternehmen hat nun folgende Aktionen auf die Merkliste gesetzt, um einen sicheren Datenaustausch sicherzustellen (s. Textbox).

Die Auswahl der Aktionen ermöglicht unserem Unternehmen, sich auf den ausgewählten Bereich, in diesem Fall sicheren Datenaustausch, zu fokussieren. Innerhalb der Aktionen können nun entsprechende Umsetzungsvorschläge ausgewählt werden. Zudem können nach Registrierung gemerkte Aktionen auch wieder von der TISiM-Merkliste entfernt werden und so Schritt für Schritt bearbeitet werden. Ändern sich Voraussetzungen im Unternehmen, kann die Befragung jederzeit wiederholt werden.

Der Sec-O-Mat bietet zudem über das Menü einen direkten Zugang zu weiteren TISiM-Leistungen. So können TISiM-Nutzende mit einem Klick ihren nächstgelegenen TISiM-Regional Standort finden, mit dem DsiN-Sicherheitsbarometer über aktuelle Sicherheitsbedrohungen informiert werden oder im FAQ-Bereich Hintergrundinformationen zum Sec-O-Mat erhalten.

Ermitteln Sie jetzt Ihren IT-Sicherheitsbedarf mit dem Sec-O-Mat unter: *www.sec-o-mat.de*

Organisatorische Aktionen

Verbindung mit externen Netzwerken regeln
Sind Sie oder Ihre Mitarbeitenden oft unterwegs und arbeiten dann mit Firmen-IT? Formulieren Sie klar verständliche Regeln zur sicheren Verbindung mit WLAN und anderen Netzwerken außerhalb Ihres Unternehmens. So sollte z. B. eine verschlüsselte VPN-Verbindung bei der Nutzung von WLANs an öffentlichen Plätzen wie Cafés, Flughäfen und Bahnhöfen eingesetzt werden.

Personelle Aktionen

Sicherheitsbewusstsein steigern
Nur wenn Mitarbeitende die Risiken auch wahrnehmen, können sie sich sicher verhalten. Steigern Sie das Bewusstsein für Informationssicherheit bereits beim Einstieg neuer Mitarbeitender. Sensibilisieren Sie zudem in regelmäßigen Abständen für einen sicheren Umgang mit IT-Systemen und Informationen. Dabei unterstützen Sie etwa Aushänge, Flyer oder Info-Mails.

Vorbildfunktion als Geschäftsführung leben
Die Geschäftsführung prägt in Ihrer Vorbildfunktion den Umgang mit Daten- und Informationssicherheit in ihrer Organisation. Informieren Sie sich daher selbst regelmäßig über die aktuelle Risikolage, passen Sie Ihre Gegenmaßnahmen der Risikolage an und lassen Sie sich den Umsetzungsstand sowie die Wirksamkeit Ihrer Maßnahmen berichten. Halten Sie sich gerade als Geschäftsführung an die selbst aufgestellten Regeln!

Technische Aktionen

Eigenes Netzwerk absichern
Ohne Schutzmaßnahmen können Unbefugte recht einfach auf Ihr Netzwerk zugreifen. Sichern Sie daher Ihr Netzwerk ab, z. B. indem Sie fremde Geräte im WLAN abweisen. Nutzen Sie zudem VPN-Lösungen, wenn Sie mit anderen Standorten bzw. mobilen Mitarbeitenden kommunizieren.

Starke Authentifizierung verwenden
Verarbeiten Sie geschäftskritische Informationen auf Ihren IT-Systemen? Dann nutzen Sie besonders sichere Lösungen zur Identitätsprüfung wie eine Mehr-Faktor-Authentifizierung. Dabei wird Ihre Identität anhand zweier physisch getrennter Merkmale geprüft, beispielsweise als Code per SMS und Passwort im Browser.

Schwachstellen finden und schließen
IT-Systeme werden mit der Zeit immer angreifbarer, da Hacker bisher noch nicht bekannte Schwachstellen finden und diese publik machen. Durch regelmäßige Überprüfungen Ihrer IT-Systeme und Software-Anwendungen können Sie bekannte Schwachstellen aufspüren. Automatisierte Verfahren unterstützen Sie dabei. Schließen Sie die gefundenen Schwachstellen dann schnellstmöglich.

Schadsoftware verhindern
In der Regel hilft es dem Angreifer am meisten, wenn er es schafft, Schadsoftware auf ein IT-System aufzuspielen. Schützen Sie Ihre IT-Systeme vor Schadprogrammen. Installieren Sie dafür bei Bedarf Antivirus-Software oder nutzen Sie die betriebseigenen Abwehrmechanismen.

Verschlüsselung einsetzen
Vertrauliche Informationen benötigen einen besonderen Schutz: Verschlüsseln Sie geschäftskritische Dokumente sowohl bei der digitalen Ablage als auch bei der Übertragung, etwa per E-Mail.

Datensicherung durchführen und testen
IT-Systeme können ausfallen, oder angegriffen werden – in beiden Fällen sind Ihre Daten möglicherweise weg. Schützen Sie sich vor ungewolltem Datenverlust. Führen Sie daher regelmäßige Datensicherungen durch und üben Sie regelmäßig, die Datensicherungen von wichtigen Systemen wiederherzustellen.

AutorIn

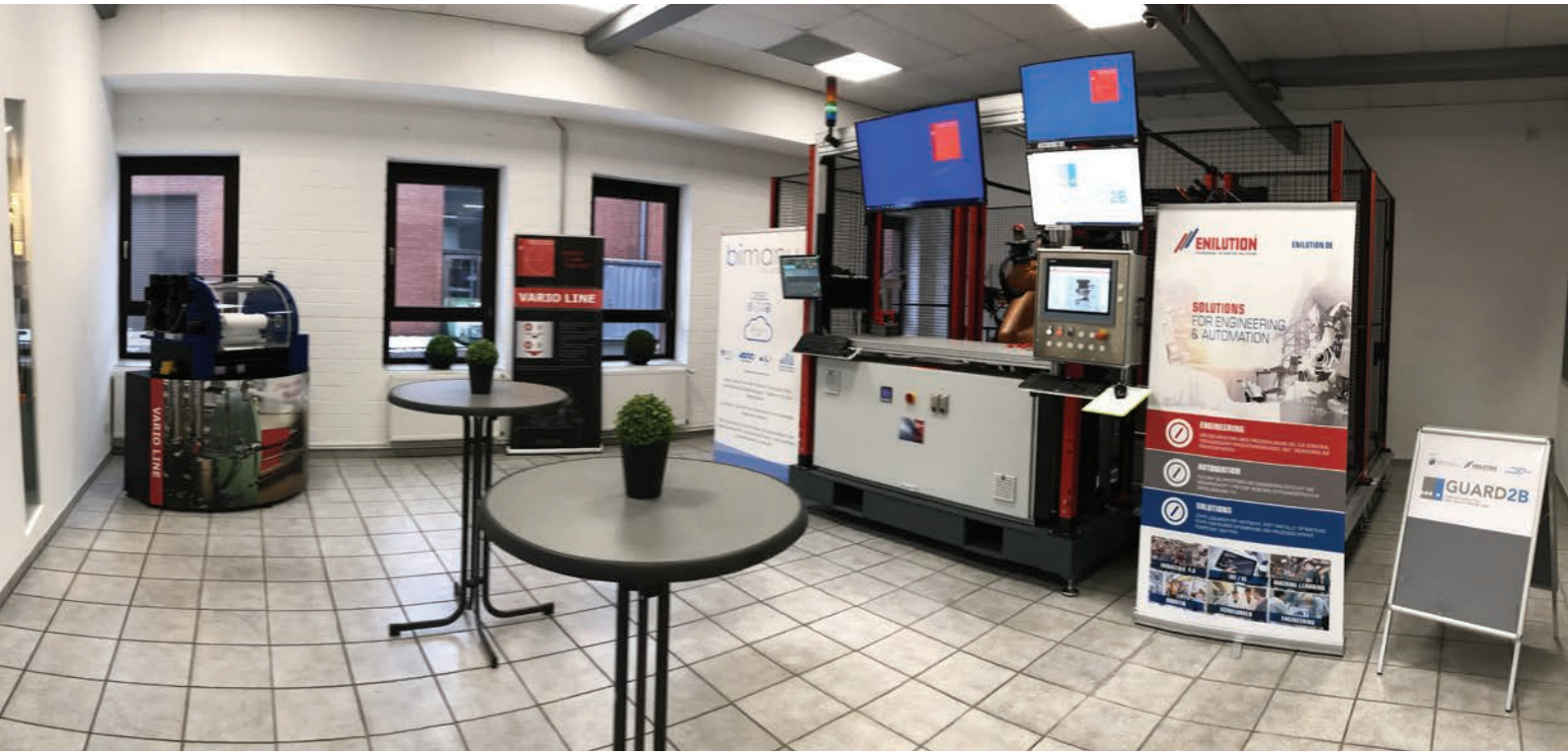
Sandra Balz hat Politik, Medienwissenschaften und Kunstgeschichte in Marburg mit Stationen in Florenz und Mailand studiert. Von 2002 bis 2020 war sie Referentin für Abgeordnete des Deutschen Bundestages, seit 2013 mit dem Schwerpunkt digitale Wirtschaftspolitik (Wettbewerbsrecht 4.0, KI, Start-up-Förderung, soziale Netzwerke,Innovationsförderung, IT-Sicherheit). Seit April 2020 ist sie Leiterin der Transferstelle IT-Sicherheit im Mittelstand (TISiM).

TISiM – die Transferstelle IT-Sicherheit im Mittelstand bietet passgenaue Informationen aus einer Hand. Sie bündelt, bereitet praxisnah auf und vermittelt Angebote zum Thema IT-Sicherheit. Darüber hinaus unterstützt sie kleine und mittlere Unternehmen, Handwerksbetriebe, Freiberufler und Selbstständige bei deren Umsetzung.

TISiM wird gefördert durch die Initiative IT-Sicherheit in der Wirtschaft des Bundesministeriums für Wirtschaft und Energie. Sie ist ein Konsortialprojekt renommierter Institutionen mit langjähriger Erfahrung in der IT-Sicherheit: Deutschland sicher im Netz e.V. (DsiN), DIHK, den Instituten FOKUS und IAO der Fraunhofer-Gesellschaft e. V. sowie der Hochschule Mannheim.

Weitere Informationen zu TISiM finden Sie unter: *https://www.tisim.de/*

Transferstelle
IT-Sicherheit im Mittelstand
Einfach. Sicher. Machen.



Erich Behrendt, Ralf Keuper, Werner Krause, Hannes Bauer, Jörg Demtröder

Sicherer Datenaustausch in der Produktion – Berichte aus der Praxis

Die Bereitschaft kleiner und mittelständischer Unternehmen, Maschinen-, Druck-, Fertigungs- und Sensordaten unternehmensübergreifend auszutauschen wird durch die Befürchtung, dass Mitbewerber oder Hacker in den Besitz wettbewerbsrelevanter Daten kommen können, stark gehemmt. Ebenso besteht die Sorge, in Abhängigkeit eines oder mehrerer Plattform-Betreiber zu geraten. Großen Wert legen die Unternehmen daher auf ihre Datensouveränität, d.h. sie wollen selber darüber entscheiden, wer Zugang für welche Daten für welchen Zweck bekommt. Überdies soll der Transaktionsverlauf manipulations- und rechtssicher dokumentiert werden. Weiteres wichtiges Kriterium ist die Möglichkeit, den Anbieter ohne allzu großen Aufwand wechseln zu können.

In dem Verbundumsetzungsprojekt (VPP) „Sicherheitsstandards im multilateralen Datenaustausch" begleitet das Mittelstand 4.0-Kompetenzzentrum eStandards seit Anfang 2021 Unternehmen bei der Entwicklung, Einführung und dem Test von offenen, freien Standards für den sicheren Datenaustausch. Der Sondermaschinenfertiger Wichelhaus, der 3D-Druck-Spezialist PROTOTEC, die Blockchain-Spezialisten von truzzt und die Verschlüsselungsprofis von WETOG werden durch Prozessbegleiter des Kompetenzzentrums unterstützt, übertragbare Modelle für den Mittelstand zu entwickeln, zu erproben und zu transferieren.

Sicherer Datenaustausch aus Sicht eines Maschinenbauers (von Jörg Demtröder)

In den meisten Produktionsbetrieben mit komplexem Industrieequipment wird beim Thema Maschinendaten oftmals in einem Atemzug die Frage nach der Datensicherheit genannt. Die Sorge, dass sensible Informationen, insbesondere beim Einsatz von modernen Cloud-Lösungen, potentiell von nicht autorisierten Dritten abgegriffen werden können, lässt so manche Produktionsleiter vor innovativen Lösungen im Rahmen von Remote Maintenance – also zum Beispiel dem Austausch der Daten mit dem Maschinenbauer zwecks Fernwartung – zurückschrecken. Daher ist es bei diesen sensiblen Lösungen von großer Bedeutung, die Digitalisierung der Produktion auf höchstem Datensicherheitsstandard zu realisieren und die Datensouveränität zu gewährleisten.

Das war für uns der entscheidende Anstoß für die Teilnahme an dem VPP „Sicherheitsstandards im multilateralen Datenaustausch". Uns ist es vor allem wichtig, dass allein der Kunde darüber entscheidet, wer auf die Daten für welchen Zweck, wie lange zugreifen darf. Die Zugriffe und Transaktionen müssen dabei rechts- und manipulationssicher protokolliert werden. Jegliche Daten werden nur dann ausgetauscht, wenn sie von vertrauenswürdigen, zertifizierten Partnern angefragt und freigegeben werden. Der Transaktionsverlauf wird durch den Einsatz einer Blockchain manipulations- und rechtssicher für alle Teilnehmer einsehbar dokumentiert. Ein lesbarer Zugriff auf die Daten während der Übertragung ist nicht möglich. Vorgesehen ist, dass der Endkunde die Analyse über einen Zugang zu der Cloud abrufen kann.

Für uns als Maschinenbauer bietet die Teilnahme an dem VPP die Möglichkeit, Erfahrungen zu sammeln, um unsere bereits bestehenden Lösungen verbessern und neue Services anbieten zu können. Das ist dann der Fall, wenn das System in der Lage ist, auch maschinenunabhängige Daten mit in die Analyse einzubinden und so einen digitalen 360°-Blick auf die Produktion zu ermöglichen. In diesem Zuge können zum Beispiel Daten des ERP-Systems und der Energieabrechnung mit aufgenommen werden.

Mit der Teilnahme an dem VPP sehen wir uns in unserer Zielsetzung bestärkt, unsere Kunden pragmatisch und effizient als Technologiepartner zu unterstützen, Stillstandzeiten zu verringern und digitale Lösungen für Wartung, Inbetriebnahme und Maschinenschulungen anzubieten.

Sicherer Datenaustausch aus Sicht des Anwenders im 3D-Druck

PROTOTEC ist ein 3D-Druck-Dienstleister und Prototypenbauer, welcher seit 1995 als einer der ersten 3D-Druck-Dienstleister in Deutschland an den Start ging. Schon damals war es nicht einfach, aus digitalen Daten ein reales Modell zu erzeugen. Das Problem damals lag jedoch eher darin, dass viele Daten noch gar nicht in digitaler Form zur Verfügung standen. Viele Zeichnungen waren noch auf Papier oder in digitaler Form nur in 2D, jedoch noch lange nicht in 3D-Modellen verfügbar. Mit der Zeit hat sich das Modell gewandelt und die digitalen Systeme haben sich mehr und mehr etabliert und sind zum Standard in der Produktentwicklung geworden.

Ohne die digitalen 3D-Datenmodelle ist heutzutage ein 3D-Druck nicht mehr denkbar und möglich. Demnach ist für jeden Auftrag und jedes Modell, welches gedruckt werden soll, der Austausch von sensiblen Informationen und Daten zwingend erforderlich. Dieser Austausch erfolgt heutzutage meist per E-Mail. Doch was passiert mit den Daten auf dem Weg vom Sender zum Empfänger?

Aufgrund der vielen digitalen Daten und dem weltweiten Internetverkehr stellt sich immer wieder die Frage, wie man diese Daten vor unbefugtem Zugriff schützen kann. Auch deshalb, weil Prototypen und Marktneuheiten (unter Umständen auch mit laufenden Patentanmeldungen) in fast jedem Fall einer Geheimhaltungsvereinbarung (GHV) unterliegen. In genau diesen GHVs sind oftmals Passagen enthalten, welche den folgenden Wortlaut besitzen: *„…die Daten dürfen nicht weitergegeben und müssen vor unbefugtem Zugriff geschützt werden…"*. Doch wer kontrolliert, was auf dem Weg des Datenaustausches mit den Daten geschieht?

Aufgrund der Vielzahl und der Sensibilität der Daten beschäftigt sich PROTOTEC mit dem Thema „sicherer Datenaustausch". Es ist zu einem Fokusthema der digitalen Geschäftsausrichtung des Unternehmens geworden. Schließlich ist der 3D-Druck eine digitale Fertigungsmethode, die sich immer größerer Beliebtheit erfreut. Und das nicht nur für Prototypen und Muster, sondern auch mehr und mehr für Kleinserien und Serienteile. Somit werden in Zukunft zunehmend mehr Daten über das „World Wide Web" ausgetauscht. Und die Spionage- und Hackerangriffe nehmen zu und der Nutzen wird für die Angreifer immer größer.

Interessant sind digitale Vernetzungslösungen, die nicht nur IT-Sicherheit auf hohem Niveau gewährleisten, sondern ökonomisch transparente Verwertungen von Datenmodellen mit verschiedenen Partnern auf einer Plattform ermöglichen.

Partner eindeutig identifizieren, Daten mit Nutzungsbedingungen versenden und den Austauschprozess rechtssicher dokumentieren

Eine entscheidende Voraussetzung für den sicheren Datenaustausch ist, dass nur Unternehmen und Personen, die zuvor eindeutig identifiziert wurden, teilnehmen können. Nicht minder wichtig ist, dass die Unternehmen selber die Nutzungsbedingungen für ihre Daten festlegen können. Für die rechts- und manipulationssichere Dokumentation des Datenaustauschs bietet sich der Einsatz einer Blockchain an. Insgesamt sollte die eingesetzte Technologie den Ansprüchen der Norm DIN SPEC 27070 genügen und nach dem Architekturmodell der International Data Spaces Association arbeiten. OpenSource und damit Quelltext offener Code ist erwünschenswert, um die interne Verarbeitung der Daten transparent zu halten.

Die Partner können innerhalb des Verbundpraxisprojektes des Kompetenzzentrums eStandards eine solche Blockchain-Lösung bei sich installieren oder als Software-as-a-Service nutzen. Jeder Transaktionspartner (Person, Unternehmen) legt zur Identifizierung ein Konto bei beim Lösungsanbieter an. Der Datenaustausch verläuft dann automatisch über die Blockchain-Lösung, die sowohl GAIA-X- wie auch IDSA-konform (International Data Spaces) ist. Das bedeutet, dass die Datenhoheit zu jedem Zeitpunkt bei den Transaktionspartnern liegt, die ihre Nutzungsbedingungen (wer darf die Daten für welchen Zweck verwenden) an die Daten anheften können. Über das angeschlossene Clearinghouse (Blockchain), zum Ausgleich gegenseitiger Forderungen und Verbindlichkeiten, wird der Transaktionsverlauf dokumentiert.

IT-Sicherheit

Bei der Informationssicherheit geht es um den Schutz der technischen Systeme eines Unternehmens. Das umfasst sowohl die Informationstechnologie (IT) wie auch die Operational Technology (OT), die Hard- und Software, mit denen die Leistungen physischer Geräte, Maschinen, Anlagen sowie deren Prozesse und Ereignisse überwacht, kontrolliert und gesteuert werden. Die Verschmelzung von IT und OT stellt die Unternehmen vor große Herausforderungen, da sich die Verfahren aus der IT nicht ohne weiteres auf die OT übertragen lassen. Während in den Büros die Erreichbarkeit von außen für zum Beispiel Kunden und Lieferanten im Vordergrund steht, geht es in der Fertigung vor allem darum, Produktionsausfälle zu verhindern. Der direkte Kontakt mit der Außenwelt auf Shopfloor-Ebene war bis vor kurzem nicht vorgesehen und auch nicht nötig. Heute kommunizieren jedoch immer mehr Maschinen direkt mit externen, nicht selten völlig unbekannten Akteuren, zum Beispiel über Cloudlösungen oder IIoT-Plattformen (Industrial Internet of Things). Für kleine und mittlere Unternehmen kommt es darauf an, einen Vendor-lock-in zu vermeiden, also die Abhängigkeit von Produkten oder Dienstleistungen eines Anbieters, sodass sich der Wechsel zu einem Mitbewerber wirtschaftlich nicht rechnet, ohne dabei auf die Datenhoheit und IT-Sicherheit verzichten zu müssen.

Ein wichtiger Teilaspekt der Informationssicherheit ist die Gewährleistung der Datenintegrität und -verfügbarkeit sowie die Bewertung der Vertrauenswürdigkeit der externen Kommunikations- und Geschäftspartner. Im Zentrum steht dabei stets die Frage, wie die Daten versendet und empfangen werden, zum Beispiel per E-Mail, FTP oder Cloud – und natürlich: Von wem stammen die Daten und wie wird die Datenintegrität sichergestellt? Die Klärung dieser Fragen versetzt uns in die Lage, den sichersten Weg für den Datenaustausch zu ermitteln.

Im VPP des Mittelstand 4.0-Kompetenzzentrums eStandards wird der Transaktionsverlauf über eine Blockchain rechts- und manipulationssicher dokumentiert. Die beteiligten Unternehmen verfügen zu jedem Zeitpunkt über einen vollständigen und einheitlichen Datenbestand. Die Daten werden dabei dezentral gespeichert – eine zentrale Instanz, welche die Daten verwaltet, existiert nicht. Der automatische Datenaustausch wird mit der Blockchain-Lösung abgewickelt, die sich an der IDSA-Referenzarchitektur orientiert. Die Lösung übernimmt dabei die eindeutige Identifizierung der externen Kommunikationspartner. Für den Austausch besonders sensibler Daten wird eine in dieser Form einmalige Verschlüsselungslösung eingesetzt, die eine sichere Datenübertragung gewährleistet und leicht zu implementieren ist.

Ein weiteres Ziel im VPP des Kompetenzzentrums ist die Erstellung eines IT-Sicherheitskonzepts, das die Themen Netzwerksegmentierung, Schwachstellenmanagement, Awareness-Schulung und die Netzwerk-Inventarisierung behandelt sowie allgemeingültige Regeln (Best Practices) für kleine und mittelständische Unternehmen formuliert.

Ausblick

Die Fähigkeit, vertrauenswürdige Daten aus verifizierten Quellen beziehen, versenden und veredeln zu können, ist für Wichelhaus und PROTOTEC überlebenswichtig. So müssen sich die Maschinenbetreiber darauf verlassen können, dass ihre Maschinendaten auf dem Weg zu Wichelhaus weder manipuliert noch von Unbefugten eingesehen werden können. Gleiches gilt für die Übertragung von 3D-Druckdaten, die von den Auftraggebern an PROTOTEC verschickt werden.

In dem VPP befindet sich das Kompetenzzentrum eStandards momentan noch in der Anfangsphase. Weitere Schritte sind die Installation der Blockchain-Lösung bei Wichelhaus in Solingen und danach erste Testläufe mit Testdaten. Bei PROTOTEC wird die Verschlüsselungstechnologie von WETOG in einem Testpiloten ausgewählten Kunden als Alternative angeboten. Während bei Wichelhaus der Schwerpunkt darauf liegt, den sicheren Datenaustausch als Basis für neue Services, wie Guard2B MDE, zu nutzen, fokussiert sich PROTOTEC auf den sicheren Austausch der 3D-Druckdaten.

Ergebnis des VPP wird eine prototypische Lösung sein, die auf etablierten und anerkannten Standards wie ISO/IEC 62443 und DIN SPEC 27020 und Referenzarchitekturen wie IDSA und GAIA-X aufsetzt. Die Verwendung von Open-Source-Komponenten, genannt seien der DataSpace Connector und die truzzt box, verhindert,

dass sich die am Datenaustausch beteiligten Unternehmen in Abhängigkeit von großen Plattformen begeben. Gerade für kleine und mittelständische Unternehmen aus dem Maschinenbau und dem 3D-Druck ist das ein Verkaufs- bzw. Kaufargument. Für spezielle Anforderungen können jederzeit kommerzielle Lösungen angebunden werden.

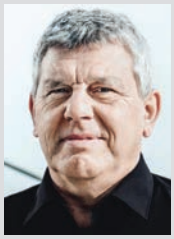
Damit folgen wir in dem VPP der GAIA-X-Philosophie. So wie GAIA-X soll das VPP ein Rahmenwerk für Unternehmen wie Wichelhaus und PROTOTEC schaffen. Welche Technologie (Blockchain, „normale" Datenbank oder Kryptografie) sich hinter den Lösungen verbirgt, ist zweitrangig.

Autoren

Erich Behrendt: Honorarprofessor für Digitale Transformation & Leadership an der University of Europe for Applied Sciences, Fachreferent und Evaluator des Mittelstand 4.0-Kompetenzzentrums eStandards.

Ralf Keuper: Berater, Blogger und Autor u. a. zu Daten Souveränität und Identity Economy, Prozessbegleiter des Mittelstand 4.0-Kompetenzzentrums eStandards.

Werner Krause: Inhaber Krause IT Consulting, Fachreferent des Mittelstand 4.0-Kompetenzzentrums eStandards.



Hannes Bauer: Internetpionier, Gründer von Kolibri, der ersten Suchmaschine in Deutschland, Geschäftsführer der orbiter.de GmbH und Gründer von Idento.one.

Jörg Demtröder: CEO der Wichelhaus Gruppe, welche aus zwei Sondermaschinenbauern und einer Engineering Gesellschaft besteht.

Titelbild:
Demonstrator und Versuchsanlage für den Blockchain-Einsatz bei der Firma Wichelhaus in Solingen.

Das Mittelstand 4.0- Kompetenzzentrum eStandards unterstützt kleine und mittlere Unternehmen bei der Entwicklung und Umsetzung von nachhaltigen und digitalen Geschäftsideen mit Hilfe von Standards für den elektronischen Geschäftsverkehr in allen Unternehmensbereichen, kurz eStandards.

Weitere Informationen zum Kompetenzzentrum finden Sie unter
https://www.estandards-mittelstand.de/

Mittelstand 4.0
Kompetenzzentrum
eStandards

Andreas Neuenfels

Sichere Netzwerke – Grundlage für einen sicheren Datenaustausch

Kleine und mittlere Unternehmen sind aus Zeit- und Kostengründen zunehmend mit dem Aufbau sowie dem Betrieb eines sicheren Netzwerkes überfordert. Häufig fehlt dabei der entscheidende Überblick über das gesamte Netzwerk, so dass es zu Problemen innerhalb der Architektur oder Konfiguration der Netzwerkkomponenten kommt. Ein sicherer Datenaustausch wird dadurch gefährdet. Das Mittelstand 4.0-Kompetenzzentrum Chemnitz stellt mit dem Demonstrator „Schwachstellen-Scanner" eine innovative und einfache Lösung für dieses Problem vor.

Eine wichtige Aufgabe im Unternehmensalltag ist sowohl die interne Kommunikation, z. B. zwischen Mitarbeitern oder Organisationseinheiten, als auch die externe Kommunikation, z. B. mit Kunden oder Behörden. Diese findet über verschiedenste Geräte statt und soll den Informations- und Datenaustausch ermöglichen. In typischen kleinen und mittelgroßen Unternehmen (KMU) stehen hierfür, insbesondere im Office-Bereich, üblicherweise Computer, Laptops, (Mobil-)Telefone oder Drucker zur Verfügung.

Aufgrund der Digitalisierung und der immer stärkeren Vernetzung einzelner Unternehmensbereiche kommunizieren immer mehr Geräte miteinander. Steuergeräte von Werkzeugmaschinen, Sensoren auf der Produktionsstrecke oder mobile Logistikeinheiten sind nur einige Beispiele für in KMU befindliche Netzwerkteilnehmer. Diese Geräte sind, ebenso wie diese aus dem Office, mögliche Angriffspunkte für Angreifer – denn überall dort, wo Kommunikation stattfindet, bieten sich Möglichkeiten Daten abzufangen oder zu manipulieren

Überblick über eigene Systeme und deren Konfiguration fehlt

Die Netzwerke typischer KMU sind in kurzen Zeiträumen oft sehr stark gewachsen, so dass viele mögliche Sicherheitsaspekte nicht beachtet werden oder Unsicherheit herrscht, welche Geräte überhaupt miteinander Daten austauschen. Netzwerkkomponenten sind häufig nicht korrekt konfiguriert oder es fehlen kritische Sicherheitsupdates, wodurch Schwachstellen durch Angreifer ausnutzbar sind. Zusätzlich können diese

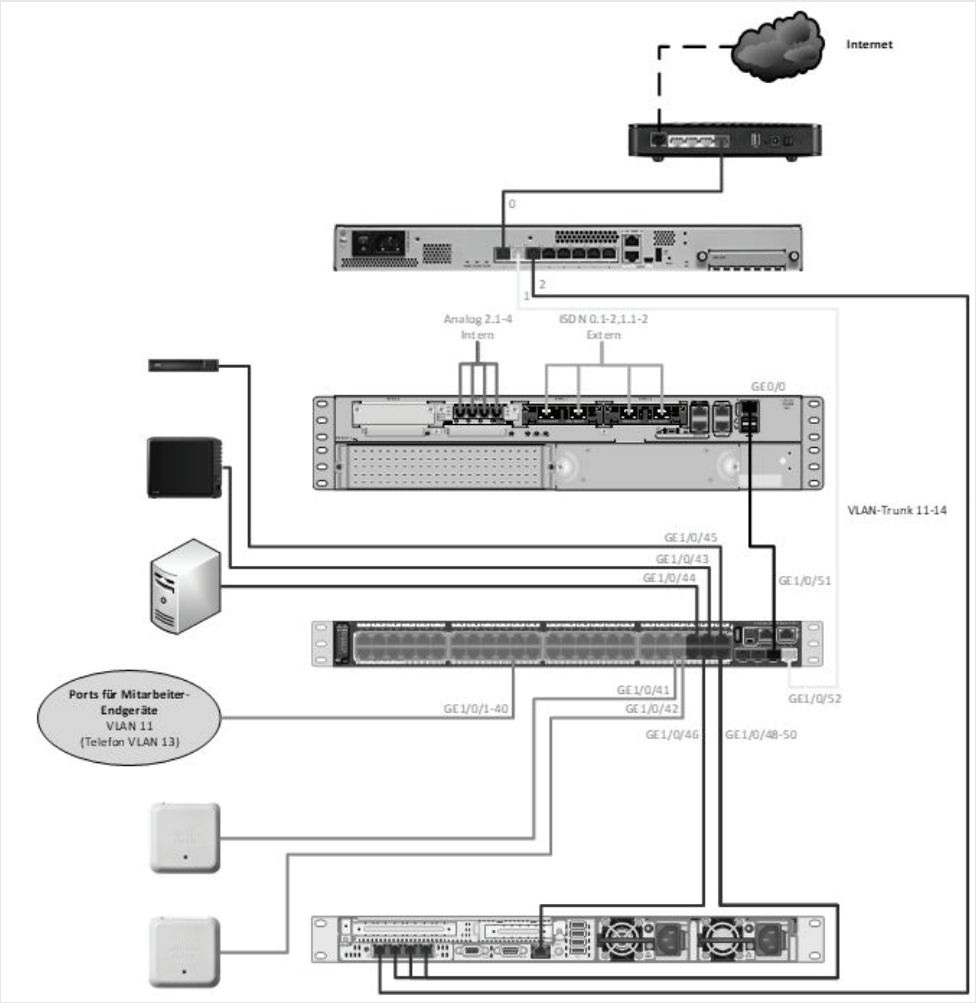


Abbildung 1: Typischer Netzwerkplan eines kleinen Unternehmens

Netzwerkteilnehmer auch einfach von Externen gefunden werden, sollten sie ungeschützt mit dem Internet verbunden sein.

Suchmaschinen wie z. B. „shodan.io" oder „censys.io" ermöglichen es, diese über das Internet erreichbaren Komponenten zu finden. Hierbei können bei falscher Konfiguration auch Daten wie IP- oder MAC-Adressen, freie Ports und Dienste oder sogar Angaben zu Seriennummern oder Firmware-Versionen gefunden werden. Solche Angaben werden von angreifenden Dritten genutzt, um geeignete Schwachstellen und Schadsoftware zu finden, die gezielt den Datenaustausch im Unternehmen negativ beeinflussen.

Somit ist es essentiell, eine sichere Netzwerkkonfiguration für alle Komponenten in der Unternehmens-IT zu realisieren – und das unabhängig davon, wo diese lokalisiert sind (Office- vs. Produktions-IT).

Netzwerke als Ausgangspunkt zur sicheren Kommunikation analysieren

Zunächst ist es wichtig herauszufinden, welche Gerätschaften, unabhängig von der Internetanbindung, in der Unternehmens-IT vorhanden sind und Daten austauschen. Dies kann manuell durchgeführt werden. Es bietet sich dabei ausgehend von der Unternehmensinfrastruktur an, sowohl Organisationseinheiten, Standorte, räumliche bzw. strukturelle Trennungen sowie die Verbindungen untereinander zu betrachten. Hierzu sind alle Geräte sowie die dazugehörigen Adressen bzw. Protokolle zu analysieren und sämtliche Abzweigungen sowie Verbindungen zu dokumentieren. Elementar sind zudem Informationen über einzelne Server (inklusive Services) und den Clients. Dazu gehören auch eingesetzte Software, Lizenzen, Konfigurationen, Firmware-Versionen etc. Solche Informationen können auch im Netzwerkplan zusammengefasst werden.

Schwachstellen erkennen und schließen

Anhand der zuvor dokumentierten Geräte sollten nun Abgleiche mit Datenbanken erfolgen, die über Informationen zu den sogenannten „Common Vulnerabilities and Exposures (CVE)" – also den Schwachstellen und Anfälligkeiten von Systemen – enthalten. Beispiele für solche Datenbanken sind:

- Datenbank für IT-Angriffsanalysen des Hasso-Plattner-Instituts *https://hpi-vdb.de/vulndb*
- Computer Emergency Response Team der Bundesverwaltung (CERT-Bund) *https://www.cert-bund.de/*
- National Vulnerability Database – NIST *https://web.nvd.nist.gov/view/vuln/search*
- CVE Details – MITRE *http://www.cvedetails.com*
- Exploit-Database *https://www.exploit-db.com*
- ICS-CERT ICS-Cyber Emergency Response Team (NCCIC) *https://ics-cert.us-cert.gov*

Teilweise sind in diesen Datenbanken der Schweregrad der Schwachstellen, die potenziellen Angriffstechniken und wie man sich dagegen schützen kann, hinterlegt.

Die häufigsten Schutzmaßnahmen basieren auf Sicherheitsupdates der eingesetzten Soft- bzw. Firmware sowie dem Schließen ungenutzter Dienste und Ports im Netzwerk.

Netzwerkkommunikation überprüfen

Neben dem Schließen offensichtlicher Schwachstellen sollten die Netzwerke von KMU regelmäßig hinsichtlich des Datenaustausches geprüft werden. Zentrale Fragestellungen sind dabei, wer miteinander kommuniziert und was der jeweilige Inhalt ist. Hintergrund dieser Fragestellung ist, dass nicht ausgeschlossen werden kann, dass Unbefugte bereits (intern oder extern) Zugriff auf das Unternehmensnetzwerk haben oder sich diesen, aufgrund nicht geschlossener Schwachstellen, in Zukunft verschaffen können.

Zur Überprüfung können unterschiedliche Netzwerk-Monitoring-Tools eingesetzt werden. Teilweise verfolgen diese den Ansatz, Datenzugriffe zu protokollieren. Andere Tools setzen auf die Analyse und Dokumentation von versendeten Datenpaketen in- und außerhalb des Netzwerkes. Die bekanntesten Vertreter solcher Tools sind Wireshark, Teamshark, Ettercap und PRTG Network Monitor.

Das Problem bei diesen Tools ist, dass man nur die Datenpakete und deren Ursprung bzw. Ziele kennt, aber nicht ob diese ggf. Schadcode enthalten oder diese Zugriffe untypisch sind. Diese Beurteilung obliegt den Verantwortlichen für IT-Sicherheit und ihren Fertigkeiten. Deshalb etablieren sich zurzeit immer mehr sogenannte „Intrusion Detection Systeme (IDS)", welche es ermöglichen, Attacken in Netzwerken automatisiert aufzuspüren oder ungewöhnliche Datenverbindungen (Anomalien) zu erkennen. Häufig werden IDS mit einer so genannten „Deep Packet Inspection (DPI)" ausgestattet, um ungewollte Inhalte in Datenpaketen zu registrieren. DPI sind Netzwerktechnikverfahren um übertragene Datenpakete zu analysieren und u.a. Schadcode zu identifizieren.

Administrativen Aufwand für KMU senken

Eine manuelle und kontinuierliche Analyse des eigenen Netzwerkes sowie der dort ablaufenden Kommunikation erfordert viel Zeit. Kleinere und mittlere Unternehmen besitzen häufig nicht die Ressourcen oder das Know-how, um sich mit den eingangs vorgestellten Themen umfassend auseinander zu setzen.

Dies hat das Mittelstand 4.0-Kompetenzzentrum Chemnitz erkannt und bietet mit dem „Schwachstellen-Scanner" eine kompakte Lösungsmöglichkeit als Demonstrator an. Dieser ermöglicht die vollständige Analyse einer Netzwerkumgebung, findet und bewertet Schwachstellen und überwacht die ablaufenden Kommunikationsprozesse. Gleichzeitig dient der Demonstrator zur Sensibilisierung und Wissenserweiterung von IT-Verantwortlichen. Der Schwachstellen-Scanner stellt eine Erweiterung des Demonstrators „IT-Sicherheit von Produktionsanlagen" dar und wurde in Zusammenarbeit mit einem deutschen Softwarespezialisten entwickelt. Eingesetzt wird der Demonstrator im Rahmen von Workshops, aber auch für Modellprojekte in Unternehmen.

Lösungswege für Administratoren aufzeigen

Die Basis des Demonstrators stellt eine beispielhafte industrielle Netzwerkumgebung dar. Diese besteht aus zwei baugleichen, aber unterschiedlich konfigurierten speicherprogrammierbaren Steuerungen, einem HMI (Human Machine Interface, also eine Mensch-Maschine-Verbindung) sowie der notwendigen Verkabelung und Netzwerkinfrastruktur (Switch), welche in einem Koffer untergebracht sind. Der Demonstrator wurde mit dem neuentwickelten Schwachstellen-Scanner erweitert und verfügt durch einen zusätzlichen LTE-Router über eine Anbindung zum Internet. Diese ist erforderlich, um die Software des Scanners aktuell zu halten, aktuelle Datenbankabfragen (z. B. der CVE) zu ermöglichen und externe Angriffe über das Internet zu simulieren.

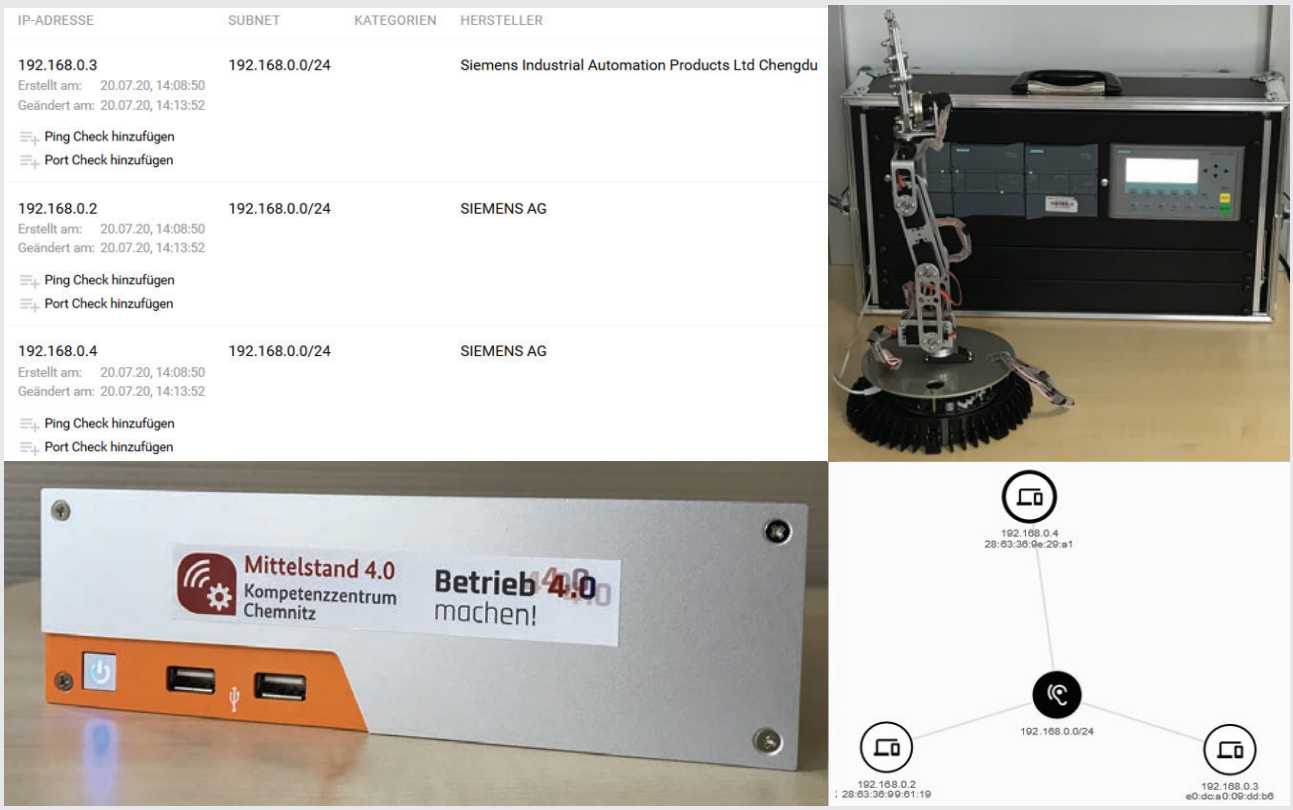


Abbildung 2: Aufbau des Schwachstellen-Scanners sowie der industriellen Testumgebung

Der Schwachstellen-Scanner verfügt über verschiedene Werkzeuge, die IT-Sicherheitsverantwortliche der KMU sensibilisieren und unterstützen sollen. Die grundlegende Funktion des Schwachstellen-Scanners ist zunächst die Analyse des Netzwerkes. Hierbei inventarisiert der Demonstrator die zuvor angesprochenen Netzwerkkomponenten und dokumentiert alle wesentlichen Informationen (IP-Adressen, Herstellerinformationen, etc.). In einem weiteren Schritt nutzt der Schwachstellen-Scanner diese Informationen und sucht in verschiedenen Datenbanken bekannte Schwachstellen zu diesen Geräten.

Zusätzlich können verschiedene Penetrationstests[1] sowie Brute-Force-Angriffe[2] durchgeführt werden. Dadurch ist eine Erkennung weiterer Schwachstellen und Fehlkonfigurationen (z. B. Standardanmeldedaten) möglich.

In Ergänzung dazu werden durch weitere Analysen innerhalb und von außerhalb des Netzwerkes die Netzwerkkonfigurationen im Rahmen eines Web- und Port-Monitorings durchgeführt. Hierdurch wird ersichtlich, welche Dienste und Komponenten für externe Dritte erreichbar sind. Weiterhin erfolgt eine Eingruppierung und Bewertung der gesammelten Schwachstellen, so dass kritische Hindernisse, die einem sicheren Datenaustausch entgegenstehen, sehr schnell erkannt und gelöst werden können. Zudem können die Ergebnisse als PDF-Dateien exportiert werden, um ggf. Anspruchsgruppen wie Dienstleister darüber zu informieren. Zusätzlich ermöglicht der Scanner eine kontinuierliche Überwachung der Netzwerkkommunikation und kann entsprechende Anomalien aufdecken. Weiterhin lässt der Demonstrator automatische Sicherheitsprozesse wie beispielsweise das Patch-Management zu.

1 Penetrationstest: Umfassende Prüfung von IT-Systemen, welche die Angriffsempfindlichkeit bestimmen soll. Genutzt werden dabei Angriffsmethoden und –techniken, die der Herangehensweise von Hackern ähneln. Ziel ist es, Schwachstellen und Angriffsvektoren in Netzwerken und Geräten aufzudecken.

2 Brute-Force-Angriff: Angriffsmethode, bei der durch „Trial-and-Error" versucht wird, Anmeldedaten oder Schlüssel (bzw. Passwörter) herauszufinden.

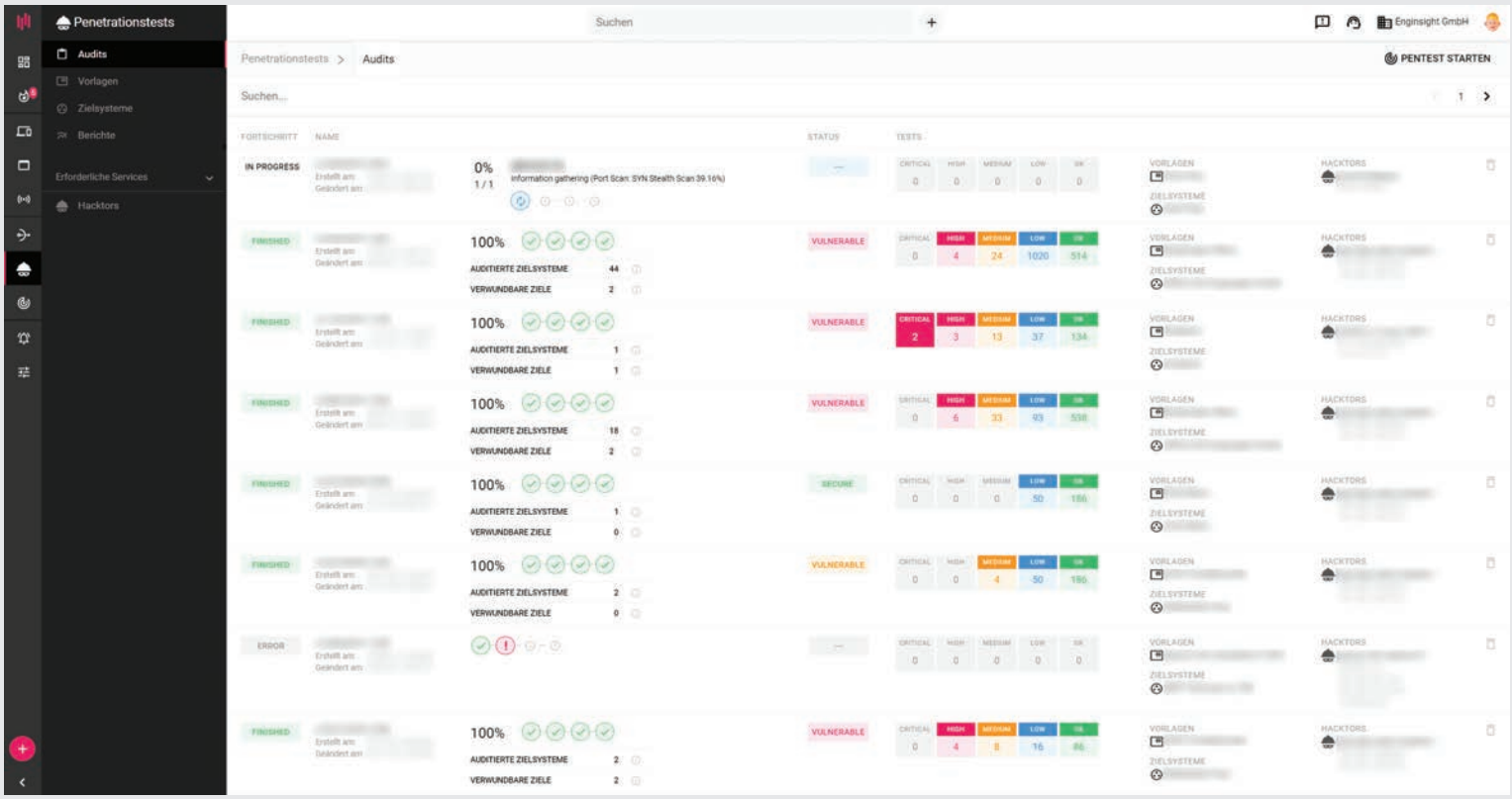


Abbildung 3: Auszug aus einem Auditreport des Schwachstellen-Scanners

Netzwerkeinstellungen für den sicheren Datenverkehr optimieren und Personal sensibilisieren

Der Schwachstellen-Scanner wurde in Verbindung mit der dargestellten industriellen Netzwerkumgebung bereits in zahlreichen Veranstaltungs- und Workshop-Formaten präsentiert. Hierbei ist es gelungen, stellvertretend für viele am Markt erhältliche Lösungen, die Vorzüge von automatisierten Schwachstellen-Scannern bzw. Sicherheitschecks aufzuzeigen und somit einen Einblick in innovative Technologien für IT-Verantwortliche in KMU zu gewähren.

Zusätzlich wurde der Demonstrator auch in realen Netzwerkumgebungen erprobt und im Rahmen eines Digitalisierungsprojektes bei einem Unternehmen vor Ort eingesetzt. Ziel war es, das IT-Sicherheitsniveau im Ingenieurbüro Reimann zu steigern. Das Unternehmen ist ein modernes Elektronikunternehmen und bietet Dienstleistungen für die Soft- und Hardwareentwicklung an. Entsprechend des Leistungsportfolios des Ingenieurbüros Reimann spielen Fragen im Zusammenhang mit der IT-Sicherheit eine große Rolle. Insbesondere werden zunehmend Dienstleistungen durch einen internetbasierten Fernzugriff auf die Systeme und Anlagen der Kunden erbracht. Service, Wartung und Monitoring sind dafür nur einige Beispiele.

Somit ist ein sicherer Datenaustausch für das Unternehmen unerlässlich. Der Schwachstellen-Scanner ermöglichte eine detaillierte Inventarisierung und Analyse des Unternehmensnetzwerkes des Ingenieurbüros. Diese Ergebnisse wurden anschließend ausgewertet und in geeignete Maßnahmen überführt.

Das Mittelstand 4.0-Kompetenzzentrum Chemnitz bietet diese Leistung auch anderen KMU an. Gern stellen wir Ihnen den Demonstrator im Rahmen eines Workshops oder weiterer Qualifikationsformate vor.

Autor

Andreas Neuenfels absolvierte ein Masterstudium als Wirtschaftsingenieur im Bereich Maschinenbau mit dem Schwerpunkt Produktionstechnik an der Otto-von-Guericke Universität Magdeburg. Er ist seit 2015 bei der tti Magdeburg angestellt und ist für verschiedene Digitalisierungs- und Managementsystemprojekte zuständig. Mit diesem angesammelten Wissen unterstützt er das Mittelstand 4.0-Kompetenzzentrum Chemnitz insbesondere auf den Gebieten der Informationssicherheitsmanagementsysteme und der allgemeinen IT-Sicherheit in der Produktion.

Das Mittelstand 4.0-Kompetenzzentrum Chemnitz unterstützt kleine und mittlere Unternehmen, sowie das Handwerk, bei der digitalen Transformation. Neben der Begleitung zur technischen Veränderung der Produktions- und Arbeitswelt, liegt der Fokus auf der Wissensvermittlung für die Themen Datensicherheit, Datenschutz und Recht. Das Zentrum pflegt hierzu das Sicherheitstool Mittelstand (SiToM) zur Einschätzung des vorhandenen IT-Sicherheitsniveaus und die „Wissensbox Recht 4.0". Hier finden sich wichtige Rechtsvorschriften und Literatur in der Übersicht und es werden aktuelle Urteile zum Thema des digitalen Rechts mittelstandsgerecht aufbereitet. Beide Onlineangebote sind auf der Website *www.betrieb-machen.de* für jeden Interessierten zugänglich.

Schwerpunkte des Zentrums sind u. a.:

- Sicherheitstest & -analysen
- IT-Sicherheitskonzepte
- IT-Sicherheitsmanagement
- Datensicherheit
- Datenschutz

www.betrieb-machen.de

Mittelstand 4.0
Kompetenzzentrum
Chemnitz

Tobias Kaufmann, Johannes Mayer, Philipp Niemietz

Datenökonomie – Wie eine geteilte Datenbasis den Nutzen für alle Stakeholder maximieren kann

Der Einsatz von Machine-Learning (ML) in Unternehmen wird künftig unausweichlich. Die Aussagefähigkeit der Ergebnisse verwendeter ML-Methoden ist aber abhängig von der zu Grunde liegenden Datenbasis. Die heute oftmals kleine, homogene Datenbasis beschränkt daher die Ergebnisse der Methoden entscheidend. Die externe Anreicherung durch den Austausch von Daten schafft die Grundlage für hochwertige und effiziente Modelle. Es fehlt aber an einer standardisierten Lösung – einem Datenmarktplatz –, die den Austausch sicher und mit Vertrauen ermöglicht. Die in diesem Beitrag vorgestellte Plattform funktioniert als as-a-Service-Lösung für jede Datenquelle in jeder Unternehmensgröße und ist daher auch für kleine und mittlere Unternehmen (KMU) eine interessante Variante zur Nutzung vieler und Monetarisierung eigener Daten.

Die digitale Transformation in der Produktionstechnik

Wandelnde Anforderungen unterschiedlicher Stakeholder an Güter und Services, deren Qualität, Verfügbarkeit und Variantenvielfalt fordern zunehmend Transparenz zur Herkunft, bei Fertigungsprozessen und von Aufträgen sowie eine Bewertung der Nachhaltigkeit. Diese Transparenz verschmilzt zunehmend mit dem expliziten Wissen, welches in den Daten der Unternehmen verankert ist. Daten aus Entwicklung, Fertigung, Montage und Nutzung werden daher auch gerne als das „Öl von morgen" bezeichnet und einem Rohstoff gleichgestellt, der für Unternehmen und Endverbraucher rasch an Bedeutung gewinnt[1]. Dabei können Daten unterschiedliche Formen annehmen und sich in ihrer Größe, Anzahl und Varianz unterscheiden. Die wachsende Datenmenge, die Vielzahl paralleler und latenzkritischer Abrufe zur Analyse und Auswertung sowie dynamische Prozesse und

1 The economist (2017).

kurzfristige Entscheidungen erfordern neue, leistungsfähige Methoden und eine Edge-/Cloud-Infrastruktur zur Datenverarbeitung, -speicherung, -analyse und -bereitstellung. Methoden des maschinellen Lernens (engl.: Machine Learning) als Teilgebiet der künstlichen Intelligenz (KI) ermöglichen die Identifikation von Mustern, Gesetzmäßigkeiten und Lösungen in der Datenbasis.

Insbesondere KMU fehlt es jedoch an Leitlinien, Strategien und der benötigten Infrastruktur für den Einsatz von KI-Lösungen, so dass ihnen der Zugang zu diesen Technologien verwehrt bleibt. Das Retrofitting, also das nachträgliche Ausrüsten von Bestandsmaschinen (oftmals in KMU 15-20 Jahre alt) mit bspw. Sensorik, erscheint mit ungewissen Kosten und Aufwänden verbunden, der Nutzen ist nicht quantifizierbar, Potenziale bleiben unentdeckt. Eine Studie der PricewaterhouseCoopers GmbH zeigte 2019, dass von 500 befragten KMU 51 % offen für den Einsatz von KI sind, allerdings bislang nur 4 % KI einsetzen. Gleichzeitig erachten 70 % der Unternehmen den Einsatz von KI-Services für Entscheidungsprozesse als sinnvoll. Hier besteht ein großes Defizit hinsichtlich der Verfügbarkeit und Nutzung von digitalen Services in Unternehmen[2].

Leitlinien, Potenzialanalysen und Qualifikationsmaßnahmen hinsichtlich der Digitalisierung und auch speziell für KI bieten die Zentren des Mittelstand-Digital Netzwerks. Zusätzliche Beratungs- und Erprobungsformate für KMU speziell zur Einführung und Anwendung von (menschzentrierter) KI bieten die in diesem Jahr durch das Bundesministerium für Arbeit und Soziales (BMAS) geförderten KI-Zukunftszentren. Anlehnend daran gründet der Einsatz von KI auf einer transparenten Fertigung, in der Daten aus Prozessen für ein Data-Mining und den digitalen Zwilling der Produktion erhoben werden. Das sogenannte Condition-Monitoring (I) stellt den ersten Schritt auf dem Weg der digitalen Transformation dar, entlang welcher, über vorausschauende Wartung und -Qualität (II und III) hinaus, Daten als Ressource in einer Datenökonomie (IV) mit dem Kernbaustein eines Datenmarktplatzes gehandelt werden. Neben der initialen Hürde der internen Datenerhebung ist es für den strategischen, erfolgreichen Einsatz und Nutzen von Daten im Unternehmen erforderlich, über die Grenzen des eigenen Datensilos zu blicken und die eigene Datenbasis extern anzureichern. Wie dies gelingt, wird im Folgenden erläutert.

Potenziale und Anforderungen für den Einsatz von datengetriebenen Analysemethoden

Methoden des maschinellen Lernens ermöglichen tiefgreifende Analysen in einem Bruchteil der Zeit konventioneller Methoden mit einer wesentlich erhöhten Präzision zur Erlangung von wettbewerblichen Alleinstellungsmerkmalen. Weiterhin wird es möglich bislang unentdeckte Muster und Anomalien in den Daten explorativ zu identifizieren und den Verlauf von Merkmalen dieser Muster zu prognostizieren. Somit entsteht die Möglichkeit aus Prozessdaten entscheidungsrelevante Informationen für Mitarbeitende und Prozesse zu gewinnen[3]. Hier kommen Methoden wie Data-Mining und neuronale Netze zum Einsatz. Sie ermöglichen im Zusammenspiel mit einer hinreichenden Datenbasis 1) eine ganzheitliche Anlagenoptimierung hinsichtlich Qualität, aber auch hinsichtlich Resilienz, Verfügbarkeit und Nachhaltigkeit sowie 2) eine echtzeitfähige und präzise Produkt- und Prozessüberwachung.

2 Hoffmann et al. (2019).

3 Whitaker et al. (2018).

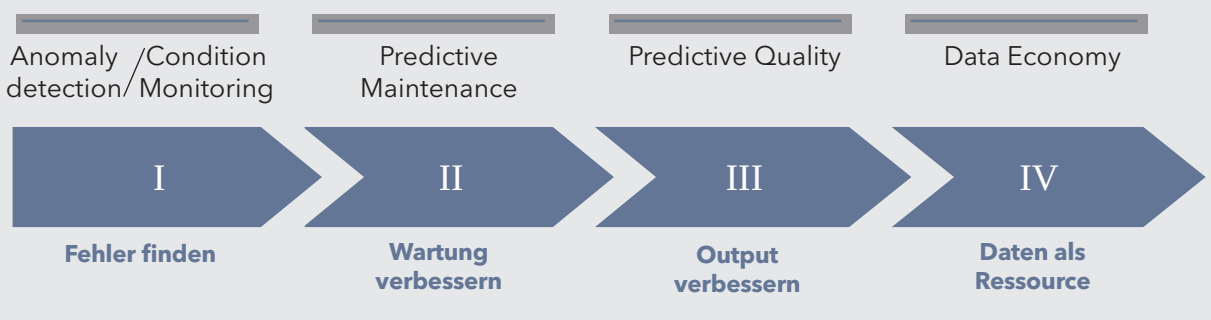


Abbildung 1: Stufen der Nutzengenerierung mit Hilfe von Daten entlang der digitalen Transformation

Die überwiegende Mehrheit der Industrieunternehmen ist bei der Umsetzung dieser neuen Analysemethoden bislang noch nicht erfolgreich. Die Anforderungen der Methoden an die Datenbasis hinsichtlich Größe, Heterogenität und Qualität der Daten sind oftmals nicht erfüllt, weswegen die Aussagefähigkeit der Ergebnisse sowie deren Präzision und Güte beschränkt ist. Die heute oftmals kleine, homogene Datenbasis einer Fertigungslinie liefert dann nicht die erhofften Ergebnisse und hemmt damit die unternehmensseitige Bereitschaft zur Investition in Infrastruktur und weitere Datenquellen. Der derzeitige Umgang mit Daten aus dem Prozess und der Anlagenperipherie zeigt, dass erhobene Daten zum Großteil lediglich innerhalb des eigenen Unternehmens, einer Abteilung oder einer Fertigungslinie eingesetzt werden. 61 % der Unternehmen scheiterten laut WORLD ECONOMIC FORUM (WEF) an der anspruchsvollen Realisierung von datengetriebenen Anwendungsfällen über einen einzelnen Wertstrom des Unternehmens hinaus[4]. Die vollständige Vernetzung nach dem bisherigen Prinzip führt zur Entstehung von vielen, kleinen und homogenen Datensilos[5]. Aufgrund dieses eingeschränkten Nutzungserlebnisses für einen Großteil der Unternehmen konnten bislang Bedarf und Mehrwert, die oftmals mit hohen Investitionskosten verbunden sind, nur selten gerechtfertigt werden. Dies führt mitunter dazu, dass der Anteil der vernetzten KMU bei weniger als 1 % liegt, die interne Produktionsvernetzung von KMU bei weniger als 10 % und die Digitalisierungsrate bei KMU bei ca. 20 % liegen[6].

Nutzenmaximierung durch Data-Sharing

Daten außerhalb der eigenen Bilanzhülle bringen gleichwohl vielseitige Anwendungsmöglichkeiten und Nutzen für weitere Stakeholder mit sich (Wissen, Optimierungspotenziale und Handlungsempfehlungen), die veredelt in Form von digitalen Services zurückgespielt werden können. Ein Unternehmen allein ist oftmals nicht in der Lage, die Anforderungen der datengetriebenen Modelle an die Datenvielfalt und -menge zu erfüllen. Mehrere dieser Datenströme gleicher oder ähnlicher Prozesse besitzen jedoch einen hohen, bislang nicht systematisch definierbaren Wert für diese Unternehmen. Damit stellt der Handel von Daten eine notwendige Bedingung für den erfolgreichen Einsatz von Methoden des maschinellen Lernens dar. Die Diskrepanz dieser beiden Perspektiven stellt ein Hindernis beim Fortschritt der digitalen Transformation dar und unterstreicht den Bedarf nach der Zugänglichkeit zu weiteren Datenquellen sowie der Möglichkeit des Handelns (engl.: Data-Sharing) zu einem monetären Gegenwert. Der Handel induziert einen Marktplatz, der die Schlagworte Datensicherheit, -integrität und -unveränderlichkeit mit Vertrauen, Verfügbarkeit, Zugänglichkeit und einem Preis adressiert. Wird die Möglichkeit des Data-Sharings bei der Bewertung der Potenziale mitbetrachtet, so bieten Daten neben 1) und 2) (Verweis auf S. 2, oben) auch die Möglichkeit, 3) den Austausch von Produkteigenschaften, wie bspw. Werkstoff und Geometrie, und 4) die Verifikation der Herkunft ausgewählter Güter zu realisieren.

Neben den technologischen Anforderungen an einen Datenaustausch ist es für Unternehmen wichtig, den Wert ihrer Daten systematisch und vergleichbar zu erfassen. Dieser Vorgang wird auch als Datenmonetarisierung bezeichnet. Klassischerweise bestimmen Angebot und Nachfrage den Preis. Bislang existiert noch kein einheitliches Vorgehen, den Wert von Daten vor oder nach der Generierung des Datensatzes zu ermitteln oder zu definieren. Eine Möglichkeit, erzeugte Daten im Nachhinein zu monetarisieren, schildern TRAUTH et al.[7]. Dieser Ansatz umgeht den Aufwand, den Preis eines ausgewählten Datensatzes vor dem Eigentumsübergang zu bestimmen. Gleichzeitig sinkt aber die Kaufbereitschaft vieler Kunden, da der Wert nicht bekannt und daher psychologisch oftmals gering eingeschätzt wird.

Eine notwendige Bedingung für die Teilnahme von Unternehmen an einem Datenmarktplatz ist, dass firmeneigenes und persönliches Know-how bei der Nutzung dennoch nicht die Unternehmensgrenzen verlässt. Als Grundlage für den Austausch von Daten bedarf es einer Vertrauensbasis. Die Gründung der GAIA-X Initiative[8] unterstreicht hier den Bedarf der Gesellschaft nach einer solchen Lösung. Für die Unternehmen bedeutet das eine standardisierte, skalierbare und sicher zugängliche Lösung, die in Form einer Plattform verfügbar ist.

Technologiegetriebene Sicherheit und Vertrauen beim Datenaustausch

Die hohen Sicherheitsanforderungen beim Austausch und Handel sensibler Daten, die im Konzept eines Datenmarktplatzes durch den Einsatz von sogenannten Distributed-Ledger-Technologien (DLT) – zu denen auch die Blockchain-Technologie gehört – erfüllt werden, bilden die Grundlage, auf der das notwendige Vertrauen in die Methode entstehen kann. Eine DLT ist prädestiniert für Anwendungen, bei denen Vertrauen bzgl. potenzieller nachträglicher Manipulationen oder Abweichungen von dargebotenen Datensätzen innerhalb eines (dezentralen) Netzwerks von Bedeutung ist. Die DLT sichert via Dezentralität und digitaler Identität die

4 Betti et al.(2021).
5 Aioma (o. D.).
6 PricewaterhouseCoopers GmbH (2019).
7 Trauth et al. (2020).
8 BMWi (o. D.).

Integrität aller Datenpunkte, bietet ein medienbruchfreies Bezahlmöglichkeiten und gestattet die Automatisierung von Handelsvorgängen in Echtzeit. Das Fehlen von Intermediären (vgl. Banken im klassischen Bezahlsystem) ermöglicht fälschungssichere, digitale Transaktionen und die Dokumentation von Eigentumsverhältnissen. Das Hauptmerkmal der DLT ist die geografisch dezentrale Verteilung von Datensätzen innerhalb des Netzwerks. DLT schaffen eine identische Datenbasis unter den Teilnehmern und verhindern durch erhöhte Transparenz und Nachvollziehbarkeit von Transaktionen unbemerkte Datenmanipulationen. Eine DLT ist demnach besitzerlos und wird durch das gesamte Netzwerk verwaltet.

Bei der Auswahl der DLT ist darauf zu achten, dass die benötigte Rechenzeit für die notwendige Transaktionsvalidierung und der Speicherbedarf nicht mit der Anzahl der Transaktionen und Teilnehmer ansteigt. Andernfalls wird der Einsatz von DLT z. B. in der Produktionstechnik hinderlich. So ist es bspw. bei der bekannten Bitcoin-Blockchain der Fall[9]. Demgegenüber weisen die für die Produktionstechnik optimierten DLTs, wie z. B. das IOTA-Protokoll, die Eigenschaft auf, dass die benötigte Validierungsgeschwindigkeit mit der Anzahl der Teilnehmer und Transaktionen ansteigt. Der darin verwendete IOTA-Tangle (siehe Abbildung 2; Pendant zur Blockchain), basiert auf einem gerichteten azyklischen Graphen (engl: DAG) und weist eine wesentlich gesteigerte Skalierbarkeit vor. Im Gegensatz zu verketteten Listen, die Blöcke mehrerer Transaktionen beinhalten (vgl. Blockchain), stellen beim DAG die Transaktionen selbst die Knoten des Graphens dar[10]. Bei dem IOTA-Protokoll wird zudem bewusst auf Transaktionsgebühren verzichtet, wodurch der Einsatz für das IoT attraktiv wird. Damit ein Nutzer eine Transaktion senden kann, müssen zwei andere Transaktionen überprüft werden[11]. Um im Netzwerk als bestätigt zu gelten, muss eine gesendete Transaktion über ein bestimmtes Verifizierungsniveau verfügen, also ausreichend oft von anderen Teilnehmern überprüft worden sein, wodurch die gesteigerte Leistung mit steigender Anzahl an Transaktionen bzw. Knoten erklärt wird[12]. Ein Datenmarktplatz, dessen Funktionalität in DLT umgesetzt ist, erscheint ebenfalls besitzerlos. Lediglich der Zugriff kann durch Anbieter vereinfachend bereitgestellt werden.

9 Schlatt et al. (2016).

10 Makhdoom et al. (2019).
11 Popov et al. (2016).
12 Wellington/Roderval (2020).

Abbildung 2: Visualisierung von Transaktionen und gespeicherten Informationen im IOTA-Tangle, der wegweisenden digitalen Technologie zur verfälschungssicheren Dokumentation für den Handel mit Daten

Wie funktioniert eine Transaktion im IOTA-Tangle?

Im IOTA-Protokoll sind Transaktionen, im Gegensatz zur bekannten Bitcoin-Blockchain, nicht mit Gebühren versehen. Die Kryptowährung MIOTA basiert also nicht wie der Bitcoin auf einer Blockchain, sondern auf einem Tangle (Gewirr). Dieser ist ein gerichteter, azyklischer und skalierbarer Graph. Er verwaltet sich durch alle Teilnehmer dezentral und speichert alle im Netzwerk getätigten Transaktionen. Konsens im Tangle entsteht durch das gegenseitige Bestätigen von Transaktionen. Das Konsensverfahren verhindert die Manipulation von außen und stellt Vertrauen im Netzwerk her. Um eine neue Transaktion durchführen zu dürfen, muss der Teilnehmer zwei weitere bestätigen. Mit hinreichender Anzahl an Bestätigungen gilt die Transaktion als validiert. Konsens entsteht nun, wenn von der Transaktion aus Verifizierungspfade zu sämtlichen (unbestätigten) Transaktionen führen. Jede Transaktion enthält die wesentlichen Informationen wie Absender, Empfänger und Menge der IOTA Token. Jeder Transaktionsprozess wickelt sich in vier aufeinanderfolgenden Schritten ab. Zunächst erfolgt die Signierung neuer Transaktionen mit einem privaten Schlüssel des i. d. R. pseudonymisierten Nutzers. Die Signierung speichert die nötigen Informationen einer Transaktion. Im zweiten Schritt wählt eine Node (Netzwerkteilnehmer/ -knoten) zwei unbestätigte Transaktionen aus, die in der neuen Transaktion bestätigt werden. Diese Knoten werden nach einem komplizierten Zufallsalgorithmus ausgewählt, der mitunter Spam im Netzwerk vermeidet. Die Validierung prüft ebenso, ob die Signaturen korrekt sind und ob die beiden zu validierenden Transaktionen widersprüchliche Informationen erhalten, bevor die Transaktion schließlich im letzten Schritt veröffentlicht wird. Die Transaktion wird dann an einen Node gesendet, der diese im Netzwerk verteilt. Diese Transaktion selbst wartet dann auf die Validierung durch andere Netzwerkteilnehmer. Dieses Verfahren verdeutlicht, wie sich Knotenpunkte umso schneller miteinander verknüpfen, je größer das Tangle-Netzwerk wird. Umso zügiger bestätigen sich demnach auch neue Transaktionen. Dies stellt im Gegensatz zur Blockchain einen bedeutenden Vorteil bei der Anwendung von DLTs in der Produktionstechnik dar.

Quellen:
https://www.bmvi.de/SharedDocs/DE/Anlage/DG/blockchain-gutachten.pdf?__blob=publicationFile , S. 30f und 41ff
https://www.btc-echo.de/news/wie-funktionieren-transaktionen-im-iota-tangle-80187/
https://www.bosch.com/de/stories/blockchain-einfach-erklaert/

Lösungsmöglichkeiten und Szenarien in der Fertigungstechnik

Eine Pionierlösung in dem Gebiet der Plattform- und Datenökonomien ist die myDataEconomy. Sie entstammt dem RWTH-Spin-Off-Unternehmen senseering GmbH und stellt eine Software-as-a-Service (SaaS)-Lösung dar. Das Werkzeugmaschinenlabor WZL der RWTH Aachen (WZL) erprobt diese Lösung und Plattform derzeit mit diversen produzierenden Unternehmen in Deutschland und innerhalb mehrerer Forschungsvorhaben. Die SaaS-Plattform adressiert die weltweit wichtige Fragestellung, wie der Austausch vertraulicher Daten mit Geschäftspartnern sicher gestaltet werden kann und verwendet dabei die IOTA-Technologie zur Sicherstellung des erforderlichen Vertrauens. In einem kostenlosen Probezeitraum kann die auf einem OpenSource-Ansatz beruhende Plattform von jedem Unternehmen genutzt und erprobt werden. In der myDataEconomy liegen die digitalen Assets einerseits lokal im Unternehmen bei maximaler Souveränität der Daten, andererseits unterliegen sie einem granularen Berechtigungsmechanismus, welcher es ermöglicht, Daten für selektierte Teilnehmer freizugeben und direkt untereinander zu transferieren. Auf diese Weise können Daten gezielt für bspw. kooperierende Partner zugänglich gemacht und mit individuellen Preisen bestückt werden. Eine dezentrale Verwaltung der verfügbaren Daten durch die Teilnehmerinnen und Teilnehmer fördert das eingeforderte Vertrauen und ermöglicht gleichzeitig die Bildung digitaler Allianzen, wie sie Abbildung 3 zeigt.

Unternehmensinterne Projekte oder -übergreifende Allianzen können innerhalb eines globalen Marktes beispielsweise zwischen Zulieferer und Produzenten entstehen. Die Plattform funktioniert als Service-Lösung für jede Datenquelle in jeder Unternehmensgröße und ist daher auch für KMU eine Lösung mit besonders niedrigschwelligem Zugang.

Im Exzellenzcluster Internet of Production der RWTH Aachen forschen Wissenschaftler:innen aus fünf verschiedenen Fakultäten, darunter auch Mitarbeiter:innen der Kompetenzzentren, gemeinsam an der Realisation des Austauschs von Daten zwischen der Entwicklungs-, Produktions- und Nutzungsphase[13]. Dazu wurden drei

13 Niemietz et al. (2020).

reale Szenarien aus der Produktionstechnik identifiziert, die durch eine Datenökonomie möglich werden: a) Verkauf von Sekundärdaten für z. B. ein Produktbenchmark oder die Verbesserung eigener Produkte durch Feedbackdaten, b) Kauf von Daten Dritter zur eigenen adaptiven Prozessauslegung, indem z. B. chargenindividuelle Werkstoffinformationen aus der Zuliefererkette vorliegen und c) Anreichern datengestützter Systeme, die eine Entscheidungsunterstützung für Bedien- und Instandhaltungspersonal liefern.

Zur Veranschaulichung wird ein Use-Case-Szenario vorgestellt, welches vier Stakeholder am Markt adressiert, deren Geschäftsmodell durch den Einsatz eines Datenmarktplatzes signifikant erweitert werden kann. Darunter fallen zwei produzierende Unternehmen, die in einer Kunden-Lieferanten-Beziehung stehen, eine Forschungseinrichtung sowie ein Plattform- und IoT-Serviceanbieter.

Persona 1 ist Stahlproduzent und kann auf eine langjährige Branchenexpertise zurückblicken und erwirtschaftet mit 280 Mitarbeitenden einen Jahresumsatz von 100 Mio. Euro. Das Kaltwalzwerk des Unternehmens erhält jedoch bis heute i. d. R. keinerlei Kundenfeedback über die Leistungsfähigkeit oder In-Toleranz-Schwankungen des Materials, sodass eine datenbasierte Verbesserung des eigenen Produktes mit Hilfe digitaler Services nicht möglich ist. Weiterhin gelingt es nicht, den digitalen Zwilling des Produktes zu monetarisieren und bereitzustellen, sodass Kunden ihre Prozesse entsprechend der Chargenschwankungen optimieren könnten.

Persona 2 ist Stahlkunde, seit knapp 60 Jahren am Markt aktiv und spezialisiert auf die Weiterverarbeitung von hochfesten und sicherheitskritischen Stahlcoils durch den Fertigungsprozess Feinschneiden. Das mittelständische Unternehmen produziert je Anlage bis zu 5 Mio. Bauteile pro Jahr, verfügt jedoch über keinerlei vorgelagerte Werkstoffinformationen. Die Anlagenverfügbarkeit, die teils unerwarteten Verschleißszenarien am Werkzeug- oder Peripheriekomponenten unterliegt, hängt somit ausschließlich vom Personal ab. Verschleiß geht einher mit Einbußen in der Qualität und einer Ausschussrate bis hin zum Ausfall der Produktion. Aufgrund der hohen Kosten, Ressourcenverschwendung und Aufwände ist es daher für Unternehmen von großer Bedeutung, den optimalen und vorausschauenden Zeitpunkt für einen Werkzeugtausch zu ermitteln. Aufgrund fehlender Daten und Analysen beruht der Wechsel bislang jedoch auf Basis von Erfahrungswerten. Der Stahlkunde erhebt ebenfalls keine IoT-Daten seiner Fertigung hinsichtlich Predictive-Maintenance/-Quality, da digitale Services für den gewinnbringenden Nutzen fehlen.

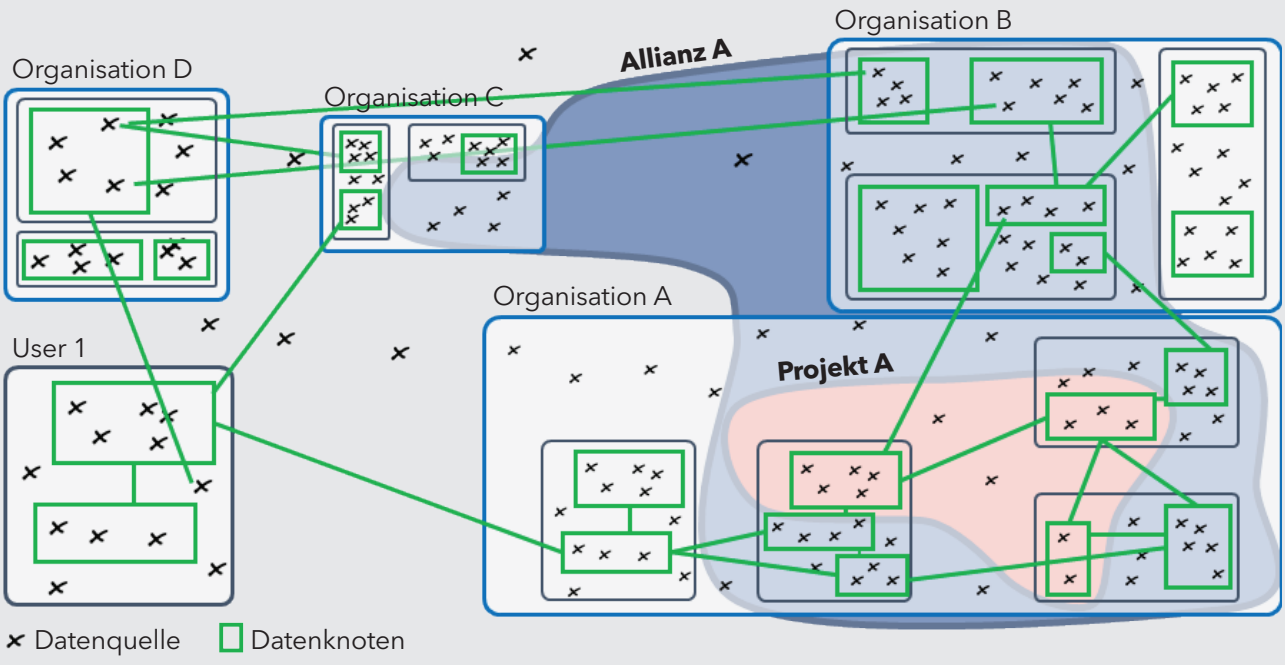


Abbildung 3: Architektur für Datenräume und Allianzen in einer Datenökonomie zum sicheren Handel mit Daten

Persona 3 stellt mit dem WZL der RWTH Aachen eine Forschungseinrichtung mit über 100 Jahren Domänenwissen in den Bereichen Stahl und umformenden Fertigungsverfahren dar. Hier wird der Transfer von Methoden des maschinellen Lernens in die Produktion fokussiert. Fehlende industrielle Datensätze hemmen das WZL jedoch in der Erforschung von KI-Algorithmen und Monetarisierung von Fertigungsdaten.

Persona 4 wird durch einen Anbieter für Data-Sharing-Plattformen verkörpert, der diese zum souveränen, sicheren und hoheitlichen IoT-Datenaustausch zwischen Stakeholdern und Partnern betreibt.

Die myDataEconomy gewährt allen 3 Stakeholdern entscheidende Vorteile: Der Stahlhersteller hat zu jeder Zeit latenzminimierten Zugriff auf weltweites Produktfeedback in der Weiterverarbeitung. Dies erlaubt die kontinuierliche Verbesserung seiner Produkte, eine engere Kundenbindung und letztendlich die Steigerung des Absatzes durch garantierte und gleichbleibend hohe Qualität. Dem Stahlkunden erlaubt die detaillierte Information über den metallurgischen und geometrischen Zustand sowohl die Anlagen zwecks Wartung als auch die Prozesse hinsichtlich der Eingangsgrößen zu optimieren. Die gesteigerte Produktivität, die auch reduzierten Ausschuss umfasst, ist dabei nachhaltig. Für Forschungseinrichtungen mit Data-Scientists und Technologieexpert:innen wird durch die Verfügbarkeit von IoT-Daten die Entwicklung von datengetriebenen Modellen ermöglicht, die die Produktivität des Stahlkunden weiter steigern können. In einem Großserien-prozess, wie dem Feinschneiden, können so Stillstandszeiten und damit Kosten um 20 bis 40 Prozent reduziert werden[14]. Zusätzlich besteht für die drei genannten Stakeholder die Möglichkeit, die eigenen IoT-Daten respektive die Modellentwicklung als digitaler Service über die Plattform für Wettbewerber und potenzielle Kunden zu monetarisieren.

Das Potenzial von Datenräumen entfaltet sich jedoch erst, wenn eine entsprechend große und qualitativ hochwertige Datenbasis respektive Teilnehmerschaft eingebunden ist. Der derzeit noch unbekannten und jungen Vision der Datenmarktplätze fehlt es derweil an Akzeptanz hinsichtlich des potenziellen Nutzens bzw. auch an Bekanntheit, insbesondere im mittelständischen Unternehmerumfeld, für das die Plattform einen niedrigschwelligen Zugang zum Datenmarktplatz bietet und von großem Nutzen sein kann. Daher wurde durch die senseering GmbH in Kooperation mit dem WZL der RWTH Aachen mit dem Datenmarktplatz.nrw[15] ein öffentlich zugängliches Projekt initiiert, welches den digitalen Zwilling der digitalen Wirtschaft in NRW repräsentiert. Die myDataEconomy wird hier nah am Mittelstand mit dem Ziel erprobt, Datenräumen für eine Datenökonomie zu schaffen, in denen durch Datenaustausch neue Geschäftsmodelle und Dienstleistungen entstehen können. Beginnend mit der Einbindung von Datenproduzenten, die technische Unterstützung erfahren, werden in einem nächsten Schritt IoT-Data-Scientists unternehmensunabhängig integriert, sodass künftig Datenkonsumenten und Service-Anbieter vom Datenmarktplatz profitieren können. Für Sicherheit, Vertrauen und Integrität sorgt bereits ab Beginn des Vorhabens die zertifizierte GAIA-X-Konformität dank DLT für alle Teilnehmer. Das Vorhaben ist in einer ersten Phase offen zugänglich für Unternehmen aus NRW und später auch deutschlandweit. Neben produzierenden Unternehmen eignen sich solche Datenräume bspw. auch für Smart-City- und Smart-Weather-Projekte, die Lebensmittelindustrie und allgemeine Zertifizierungsvorhaben oder Auditierungen und ist somit branchenübergreifend relevant.

14 Bousdekis et al. (2020).
15 https://datenmarktplatz.nrw/#IDwhy ; Zugegriffen: 29. Juni 2021.

Literatur

Aioma (o. D.) Das größte Risiko der Digitalisierung: Datensilos. URL: *https://hub.aioma.com/de/marketing-automation-software/marketing-automation/datensilos-digitalisierung*. Zugegriffen: 29. Januar 2021

Betti, F.; Bezamat, F.; Bloempott, S.; Fendri, M. (2021): Data Excellence: Transforming manufacturing and supply systems

BMWi (o. D.) GAIA-X: URL: *https://www.bmwi.de/Redaktion/DE/Dossier/gaia-x.html*. Zugegriffen: 29. Januar 2021

Hoffmann, J. B; Heimes, P; Senel, S: (2019) IoT Platforms for the Internet of Production. IEEE Internet Things J. Vol. 6(3):4098–4105. doi:10.1109/jiot.2018.2875594

Makhdoom, I.; Abolhasan, M.; Abbas, H.; Ni, W. (2019): Blockchain's adoption in IoT: The challenges, and a way forward. In: J. Netw. Comput. Appl., Volume 125, S. 251-279, DOI: 10.1016/j.jnca.2018.10.019

Niemietz, P; Pennekamp, J; Kunze, I; Trauth, D; Wehrle, K; Bergs, T. (2020): Stamping Process Modelling in an Internet of Production. In: Procedia Manufacturing, Vol 49, S. 61-68. DOI: 10.1016/j.promfg.2020.06.012

Popov, S.; Saa, O.; Finardi, P. (2019): Equilibria in the tangle. In: Comput. Ind. Eng., 136, S. 160-172, DOI: 10.1016/j.cie.2019.07.025

PricewaterhouseCoopers GmbH (2019): Künstliche Intelligenz in Unternehmen, Studie an 500 KMU, URL: *https://www.pwc.de/de/digitale-transformation/kuenstliche-intelligenz/kuenstliche-intelligenz-in- unternehmen.html*, Abruf: März 2021

Schlatt, V.; Schweizer, A.; Urbach, N.; Fridgen, G. (2016): Blockchain: Grundlagen, Anwendungen und Potenziale. Projektgruppe Wirtschaftsinformatik des Fraunhofer-Instituts für Angewandte Informationstechnik FIT, WhitePaper, S. 9 ff, URL: *https://www.fit.fraunhofer.de/content/dam/fit/de/documents/Blockchain_WhitePaper_Grundlagen-Anwendungen-Potentiale.pdf*

Autoren

Tobias Kaufmann, M. Sc.; wiss. Mitarbeiter (WZL der RWTH Aachen), studierte Produktionstechnik im Maschinenbau mit der Vertiefung Fertigung und Montage. Seit Ende 2017 ist er wissenschaftlicher Mitarbeiter am Lehrstuhl für Technologie der Fertigungsverfahren am WZL der RWTH Aachen und beschäftigt sich seit Anfang 2019 intensiv mit dem Transfer von datengetriebener Modellierung und Machine-Learning-Modellen in den Produktionsalltag. In seiner Promotion legt er den Fokus auf Prozessketten und die Steigerung der Nachhaltigkeit durch datengetriebene Entscheidungsunterstützung in der Betriebsmittversorgung produzierender Anlagen. Seit 2018 war er zudem im Mittelstand 4.0-Kompetenzzentrum Digital in NRW aktiv.

Johannes Mayer, M. Sc.; wiss. Mitarbeiter (WZL der RWTH Aachen), studierte Maschinenbau und Management an der TU München und ist seit 2019 wissenschaftlicher Mitarbeiter in der Forschungsgruppe Digitale Transformation am Werkzeugmaschinenlabor WZL der RWTH Aachen. Sein Forschungsgebiet betrifft die Entwicklung von datengetriebenen Geschäftsmodellen, die Identifikation und Untersuchung von industriellen Anwendungsfällen der Blockchain-Technologie sowie die Monetarisierung von Fertigungsdaten in einer Datenökonomie. Inhaltlich befasst sich seine Promotion mit IoT-Daten und föderierten IoT-Services in einem Datenmarktplatz für die Fertigungstechnik.

Philipp Niemietz, M. Sc.; Forschungsgruppenleiter (WZL der RWTH Aachen), studierte Informatik und ist seit 2018 wissenschaftlicher Mitarbeiter in der Forschungsgruppe Digitale Transformation am Werkzeugmaschinenlabor WZL der RWTH Aachen. Seit 2019 leitet er die Forschungsgruppe mit 8 wiss. Mitarbeiterinnen und Mitarbeitern. Sein thematischer Schwerpunkt liegt in der datengetriebenen Analyse von situativen und kontinuierlichen Veränderungen im Großserienprozess Feinschneiden.

The economist (2017): The world's most valuable resource is no longer oil, but data. URL: *https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data*

Trauth, D.; Bergs, T.; Gülpen, C.; Maaß, W.; Mayer, J.; Musa, H.; Niemietz, P.; Rohnfelder, A.; Schaltegger, M.; Seutter, S.; Starke, J.; Szych, E.; Unterberg, M. (2020): Internet of Production: Turning Data into Value – Monetarisierung von Fertigungsdaten. DOI: 10.24406/ipt-n-589615, S. 342 – 362

Bousdekis, A; Apostolou. D. and Mentzas, G. (2020): Predictive Maintenance in the 4th Industrial Revolution: Benefits, Business Opportunities, and Managerial Implications. In IEEE Engineering Management Review, Vol 48,1, S. 57-62., DOI: 10.1109/EMR.2019.2958037

Wellington F.-S.; Roderval, M. (2020): Iota Tangle: A cryptocurrency to communicate Internet-of-Things data. In: Future Generation Computer Systems, Volume 112, S. 307-319, DOI: 10.1016/j.future.2020.05.047

Whitaker, D. A.; Egan, D.; OBrien, E. & Kinnear, D. (2018): Application of multivariate data analysis to machine power measurements as a means of tool life predictive maintenance for reducing product waste. arXiv preprint arXiv:1802.08338

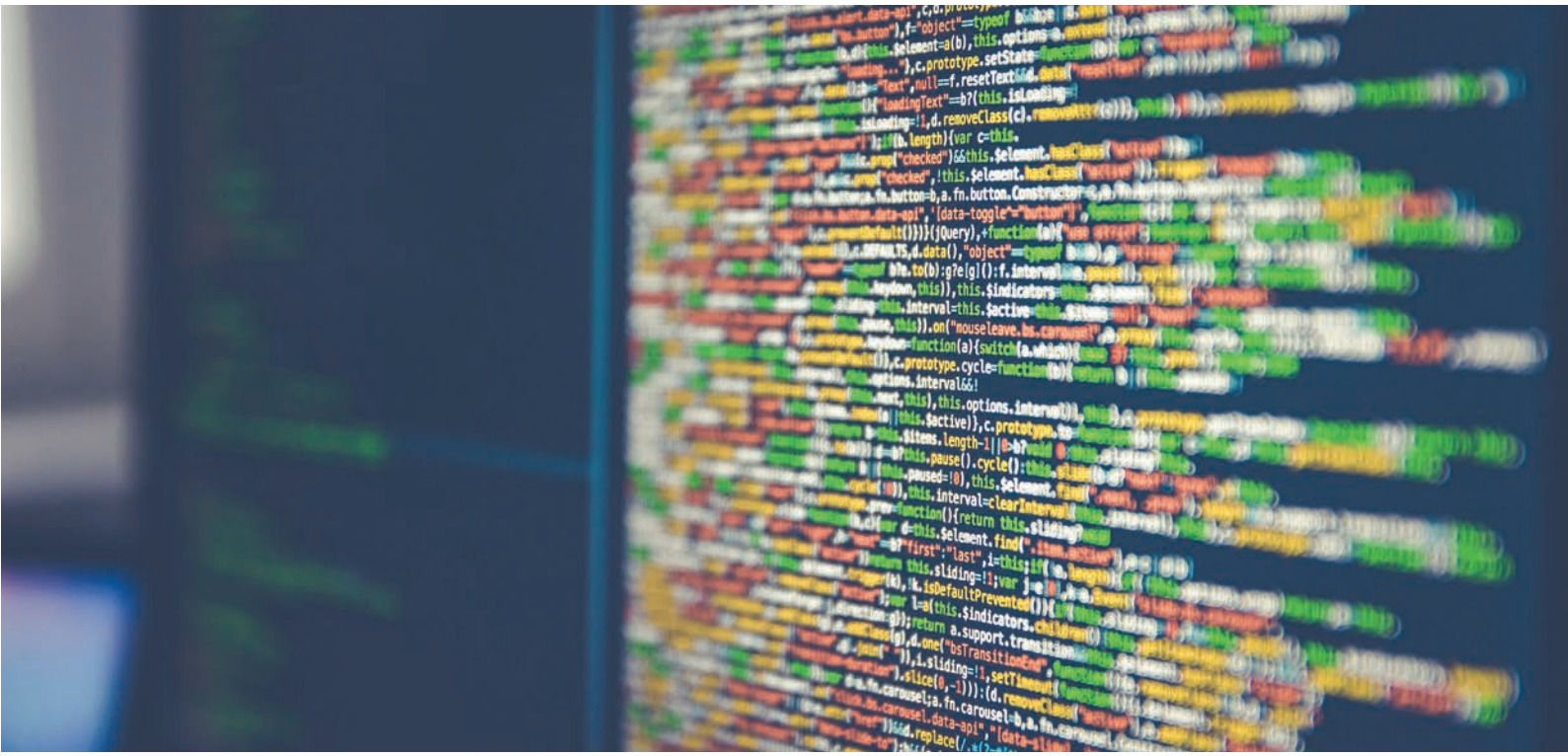
Das Mittelstand 4.0- Kompetenzzentrum Dortmund unterstützte kleine und mittlere Unternehmen von 2016-2021 bei der Digitalisierung und bündelte dafür die Expertise von Forschungseinrichtungen aus den Regionen Rheinland, Metropole Ruhr und OstWestfalenLippe.

Zu den Schwerpunkten des Kompetenzzentrums zählten u. a.:

- Agile und nutzerzentrierte Entwicklung digitaler Produkt- und Serviceangebote
- Blockchain-basierte Lösungen für Wertschöpfungsnetzwerke
- Maschinelles Lernen für Produktionssysteme und Produkte

https://www.digital-in-nrw.de

Mittelstand 4.0
Kompetenzzentrum
Dortmund



Daniel Kant, Andreas Johannsen

Sicherer Datenaustausch in Kooperationen – „Kooperation first – Sicherheit second?“

Das Mittelstand 4.0 Kompetenzzentrum IT-Wirtschaft unterstützt mit seinen Angeboten strategische Kooperationen in der IT-Branche. Dabei müssen IT-Schnittstellen und Daten in den unterstützten IT-Konsortien adäquat abgesichert werden, nicht zuletzt deshalb, weil IT-Dienstleister ihre IT-Produkte an Kunden lizenzieren oder Daten im Auftrag von Kunden verarbeiten. Der Artikel befasst sich allgemein mit den Herausforderungen, welche im Rahmen von Kooperationen bezüglich der Informations- und IT-Sicherheit bestehen, insbesondere im Hinblick auf den sicheren Datenaustausch. Des Weiteren wird die Wichtigkeit einer ganzheitlichen Sicht von IT-Governance-, Risiko- und Compliance-Management in KMU-Verbünden hervorgehoben sowie aufgezeigt, was bei der informationstechnischen Absicherung von Kooperationen und Konsortien beachtet werden sollte.

Wachsende Bedeutung des sicheren Datenaustausches

Kleine und mittlere Unternehmen (KMU) sehen sich zunehmend den Herausforderungen der digitalen Transformation gegenübergestellt, insbesondere was die Absicherung der heute vermehrt auf digitalem Datenaustausch basierenden Geschäftsmodelle betrifft. Im Fall von IT-Sicherheitsvorfällen können Daten verändert, veröffentlicht oder sogar von Angreifern verschlüsselt werden. Um Geschäftsprozesse logisch sowie physisch bestmöglich aufrecht zu erhalten, gilt es schon vor einem ungewollten Datenabfluss jegliche Veränderung oder unberechtigte Dateneinsicht zu verhindern. Allein der Schaden für Unternehmen in Deutschland durch Datendiebstahl sowie Wirtschaftsspionage und -sabotage beläuft sich jährlich auf über 100 Milliarden Euro[1]. Angriffe können heute bereits bequem über das Darknet eingekauft werden – das BKA spricht dabei von Cybercrime-as-a-Service[2]. Für viele Unternehmen kann ein IT-Sicherheitsvorfall existenzbedrohend sein. Neben dem

1 Cyber Security Cluster Bonn e.V. (2020).
2 Bundeskriminalamt (2021).

wirtschaftlichen Schaden sehen sich gerade IT-Unternehmen einem erheblichen Reputationsschaden ausgesetzt, wenn erfolgte Angriffe öffentlich werden. Viele KMU kennen dabei weder ihre Bedrohungslage noch ihr konkretes Risikoprofil und unterschätzen folglich die Wahrscheinlichkeit, Opfer eines Angriffs zu werden[3]. In der Domäne der Cyber-Sicherheit gilt es aus Sicht der Unternehmen, Künstliche Intelligenz (KI) aufgrund der Potentiale und Chancen unbedingt auf dem Schirm zu haben. Auch wenn KI zur Erhöhung des IT-Schutzniveaus beitragen kann, stehen jedoch kleine und mittlere Unternehmen der KI-Nutzung in Sachen IT-Sicherheit noch eher skeptisch gegenüber[4]. Generell ist es oft so, dass gerade in den KMU die IT-Sicherheit allgemein noch sehr stark als Kostenfaktor gesehen wird. Neben der rein technischen Absicherung stellt für kleine und mittlere Unternehmen der IT-Wirtschaft (IT-KMU) auch die Compliance im Rahmen von Kooperationen und Konsortien eine besondere Herausforderung dar.

Herausforderungen bezüglich der IT-Sicherheit in Kooperationen

Jede Kooperation ist einzigartig hinsichtlich der genutzten Kommunikationskanäle und der verwendeten Anwendungen. Datensicherheit sollte in diesem Kontext als kritisches Element für das Gelingen einer Kooperation verstanden werden. In Kooperationen von kleinen und mittleren IT-Unternehmen erhöht sich die Wahrscheinlichkeit für IT-Sicherheitsvorfälle, denn die Verknüpfung von Softwarelösungen bedingt die Nutzung gemeinsamer Schnittstellen, Systeme, Plattformen, Dienste, Quelltexte, IT-Ressourcen und Daten. Eine Kompromittierung dieser kann unmittelbare Auswirkungen auf jedes einzelne kooperierende Unternehmen haben - bis hin zu monetären Schäden und Reputations- oder Imageschäden (insbesondere, wenn personenbezogene Daten betroffen sind). Im Rahmen von Kooperationen und Konsortien von IT-Mittelständlern muss deshalb ein Fokus darauf liegen, Schäden von allen Kooperationspartnern bestmöglich abzuwenden. Herausfordernd hierbei ist auch, dass die einzelnen Unternehmen z. T. ein sehr unterschiedliches Schutzniveau ausweisen sowie üblicherweise über eigene, individuelle IT- und Sicherheitsrichtlinien verfügen.

Gemeinsame IT-Sicherheitsrichtlinie unerlässlich

Für eine sichere und vertrauensvolle Zusammenarbeit zwischen IT-Unternehmen braucht es daher besonders klare Rahmenbedingungen und Regeln, um die entsprechenden Kommunikationskanäle und -plattformen informationstechnisch adäquat abzusichern. Bei der Bildung von Konsortien zwischen Unternehmen kennen sich die Akteure untereinander oft noch nicht. Schon deshalb sollte zu Beginn einer solchen Kooperation eine Vertraulichkeitsvereinbarung (Non-Disclosure-Agreement)[5] geschlossen werden. Diese sichert den kooperierenden Unternehmen zu, dass alle Informationen, die im weiteren Verlauf der Zusammenarbeit ausgetauscht werden, vertraulich behandelt und damit nicht offengelegt werden. Des Weiteren sollte sich auf eine Informationssicherheitsrichtlinie verständigt werden. Dabei handelt es sich um eine Sicherheitsrichtlinie (*engl.*: Information Security Policy) im Rahmen von Kooperationen zwischen KMU im IT-Umfeld, welche eine einheitliche Sicherheitsausrichtung gewährleisten soll[6].

Die Kooperationspartner einigen sich zusammen auf IT-Schutzziele inklusive gemeinsamer IT-Sicherheits-Mindeststandards. Hierbei ist es das übergeordnete Ziel, die funktionale sowie physische Sicherheit von Geschäftsprozessen sicherzustellen und Beeinträchtigungen von Informationsinfrastrukturen und deren Komponenten sowie den Datenverlust weitestgehend zu minimieren bzw. bestmöglich zu vermeiden. Des Weiteren führt die Richtlinie an, welche Sicherheitsanforderungen, -prinzipien und -konzepte bei kooperierenden Unternehmen vorhanden und umgesetzt sein müssen (z. B. Datensicherungskonzept).

Absicherung von IT-Schnittstellen ist essentiell

Eine gängige Möglichkeit Daten auszutauschen sind Programmierschnittstellen (*engl.*: Application Programming Interface, *abgek.*: API). Diese gilt es bestmöglich abzusichern. Weit verbreitet sind sie in Form sogenannter Web-APIs – diese haben den Vorteil, wichtige Ressourcen, Funktionen und Daten über das Internet zur Verfügung zu stellen. Insbesondere bei Web-APIs muss ein Mindestmaß an Kommunikationskanälen freigegeben werden, damit die Funktionalität überhaupt genutzt werden kann – ähnlich wie bei einem Webserver, bei dem üblicherweise zur Nutzung des Dienstes sogenannte Ports geöffnet sind.

In der Design- und Architekturphase von APIs werden Sicherheitsaspekte (*Security by Design*) leider immer noch nicht ausreichend berücksichtigt[7]. Deshalb sollte die Sicherheit von APIs ganzheitlich gedacht werden – dies erfordert eine API-Strategie, welche den gesamten

3 Köhler et al. (2021).
4 Begleitforschung Mittelstand-Digital (2019).
5 Vgl. *Non Disclosure Agreement* vom Mittelstand 4.0 Kompetenzzentrum IT-Wirtschaft (2019).
6 Vgl. *Information Security Policy* vom Mittelstand 4.0 Kompetenzzentrum IT-Wirtschaft (2019).
7 Siriwardena (2020).

Lebenszyklus einer API bereits in der Entwicklung berücksichtigt. Des Weiteren sollten Auswirkungen einer API für ein Unternehmen – beispielsweise für das Risikomanagement – miteinbezogen werden. Es wird davon ausgegangen, dass APIs bereits im Jahr 2022 der Angriffsvektor Nummer 1 bei Web-Applikationen sein werden[8]. Das Open Web Application Security Project (OWASP) hat sich zum Ziel gesetzt, Web-Anwendungen zu verbessern und deshalb u. a. 2019 eine Liste mit den zehn kritischsten API-Schwachstellen veröffentlicht[9]. Diese stellen eine gute Orientierung für eine erste Absicherung dar.

Die Exponierung dieser Schnittstellen im Internet kann für Unternehmen schwerwiegende Folgen haben, besonders dann, wenn eine Web-API unzureichend abgesichert ist. Ein lukratives Ziel stellen APIs für Cyber-Angreifer in jedem Fall dar. Aufgrund ihrer zunehmenden Verbreitung und der direkten Verbindung mit Anwendungs- oder Datenbankservern sind APIs buchstäblich die Schnittstelle zu personenbezogenen Daten. In schwerwiegenden Fällen kann eine Kompromittierung einer solchen Schnittstelle sogar ein Einfallstor in ein Unternehmensnetzwerk darstellen. Medial wurde in der Vergangenheit über diverse erhebliche IT-Sicherheitsvorfälle in Zusammenhang mit APIs berichtet, exemplarisch seien hier die Vorfälle bei T-Mobile (2017)[10], Uber (2016)[11], Instagram (2017)[12] und beim US Postal Service (2018)[13] genannt. Anhand eines kleinen Szenarios werden einige weit verbreitete API-Schwachstellen im Folgenden kurz vorgestellt.

8 Zumerle et al. (2019).
9 OWASP (2019).

10 *https://www.t-mobile.com/customers/6305378821* (abgerufen am 26.07.2021).
11 *https://www.bbc.com/news/technology-42075306* (abgerufen am 26.07.2021).
12 *https://www.heise.de/newsticker/meldung/Fehler-in-API-Moeglicherweise-Millionen-Kontaktdaten-von-Instagram-Usern-oeffentlich-3820497.html* (abgerufen am 26.07.2021).
13 *https://krebsonsecurity.com/2018/11/usps-site-exposed-data-on-60-million-users/* (abgerufen am 26.07.2021).

Szenario IoT-Kalender

Auf einen IoT-Kalender kann direkt im Internet über eine Web-API zugegriffen werden. Die Darstellung des entsprechenden Benutzerprofils erfolgt dabei über eine Smartphone-App bzw. in einem Webbrowser. Es konnten in diesem Beispiel über eine Web-API, welche wir mittels der Suchmaschine Shodan (www.shodan.io, abgerufen am 23.06.2021) gefunden haben, beliebige Benutzer-Profile ohne entsprechende Authentifizierung angefordert werden. Eine Modifikation der Benutzer-ID kann leicht über die Veränderung der URL erreicht werden – somit erhält man einfach die Termine eines anderen Benutzers. Die angeforderten Nutzungsdaten enthalten dann die jeweiligen Objekt-Attribute (Abbildung 1). Dies entspricht der von OWASP kategorisierten Schwachstelle API1: Broken Object Level Authorization, d. h. es können beliebige Objekte angefordert werden (auch solche anderer Benutzer), ohne dafür die entsprechenden Berechtigungen zu haben.

Abbildung 1: Beispieldarstellung eines IoT-Kalenders (angelehnt an die Darstellung von Yalon (2019))

Des Weiteren gab die API deutlich mehr Objekt-Attribute zurück, als von der Anwendung im jeweiligen Kontext benötigt werden – exemplarisch seien hier die Attribute „address", „phone", „mobile" und „email" genannt (vgl. Abbildung 2). Zur Erinnerung: Der Kalender soll eigentlich nur die Termine des heutigen Tages anzeigen – dafür wird ganz bestimmt keine Strasse oder Handynummer benötigt. Dies entspricht der Schwachstelle API3: Excessive Data Exposure und betrifft auch gleichermaßen den in der DSGVO festgeschriebenen Grundsatz der Datensparsamkeit. Darüber hinaus erfolgte der Zugriff auf die API über Port 80 und nicht Port 443 (und somit unverschlüsselt). Es kann resümiert werden, dass es möglich gewesen wäre, für dieses Szenario an (umfassende) personenbezogene Daten sämtlicher Benutzer zu gelangen.

Abbildung 2: Wiedergabe eines beliebigen Benutzer-Objektes nach Anfrage an einen konkreten IoT-Kalender (Quelle: Eigene Darstellung)

Empfehlungen zum sicheren Datenaustausch im IT-Mittelstand

Der sichere Datenaustausch sollte als kritisches Element für das Gelingen eines IT-Konsortiums verstanden werden – Infrastrukturen, Daten oder Ressourcen, welche die Kooperation betreffen, sind gegenüber Cyber-Angriffen angemessen abzusichern. Was die organisatorische IT-Sicherheit betrifft, sollte ein Informationssicherheitsmanagementsystem (ISMS) etabliert werden. Des Weiteren ist es ratsam, Risiko- und Sicherheitsanalysen durchzuführen, um potenzielle Schwachstellen zu detektieren und zu beheben. Authentifizierungs- und Verschlüsselungsmechanismen sollten außerdem für jegliche Art des Datenaustausches standardmäßig aktiviert sein. Im Folgenden (Checkliste IT-Sicherheit in IT-Konsortien) wurden Empfehlungen, die wir als besonders relevant betrachten, zur Absicherung von Kooperationen als Übersicht zusammengetragen.

IT-Risiken ganzheitlich sehen und managen

Jedoch können Daten nicht nur technisch gelöscht, eingesehen oder verändert werden. Natürlich ist auch folgende Frage erheblich: Wie schaut es mit der Datensouveränität aus? Wo werden die Daten (buchstäblich) gespeichert und gilt denn dort die DSGVO? Diese Fragestellung ist natürlich umso wichtiger, wenn bspw. in der Kooperation gemeinsam Kundendaten verarbeitet werden - wie z. B. in der Auftragsdatenverarbeitung. Die Dimension der Compliance und der Datensouveränität ist also mindestens genauso wichtig, wie die reine physische sowie technische Absicherung der Daten. Speziell in KMU-Verbünden ist es wichtig, eine ganzheitliche Sicht auf die IT- und Datensicherheit zu haben. Als kleines, anschauliches Beispiel sei hier die Corona-Pandemie genannt. Gerade die Home-Office-Situation war für viele IT-Admins eine Herausforderung im Hinblick auf die Informationssicherheit. Nicht nur der Fernzugriff

Checkliste IT-Sicherheit in IT-Konsortien

- *Gemeinsame IT-Sicherheitsrichtlinie*
  Die Kooperationspartner sollten eine einheitliche Sicherheitsstrategie entwickeln – hierfür eignet sich besonders eine Informationssicherheitsrichtlinie, auf die sich die kooperierenden Unternehmen einigen.
- *Mindeststandards setzen*
  Um ein hohes IT-Schutzniveau innerhalb der Kooperation zu erreichen, sollte sich auf verbindliche IT-Sicherheits-Mindeststandards verständigt werden. Diese können ebenfalls Bestandteil einer Informationssicherheitsrichtlinie sein.
- *Etablierung eines Informationssicherheitsmanagementsystems (ISMS)*
  Die Kooperationspartner müssen zwingend Regeln, Verfahren und Methoden etablieren, um den Umgang mit der Informationssicherheit klar zu regeln und zu kontrollieren.
- *Schutzmaßnahmen implementieren*
  Natürlich müssen neben den Management-Maßnahmen auch technische Schutzmaßnahmen wie z. B. Firewalls, Deep Packet Inspection* oder Malware-Erkennung zum Einsatz kommen.
- *Risiko- und Sicherheitsanalysen durchführen*
  Um Sicherheitslücken und Schwachstellen zu detektieren, eignen sich insbesondere Pentesting- und Vulnerabilitäts-Scans**.
- *Verschlüsselung nutzen*
  Um Vertraulichkeit zu gewährleisten, sollten sämtliche Verbindungen zu Plattformen, Ressourcen und Schnittstellen ausschließlich verschlüsselt nutzbar sein.
- *Logging und Monitoring*
  Vertrauen ist gut, Kontrolle ist besser: Netzwerkverkehr sollte überwacht und auf Unregelmäßigkeiten überprüft werden. Der Zugriff auf Systeme oder Ressourcen ist ebenfalls zu protokollieren.
- *Awareness-Bildung erhöhen*
  IT-Sicherheit ist ein proaktiver Prozess. Deshalb gilt es, die Beteiligten, einschließlich des Managements, bestmöglich für Informationssicherheit zu sensibilisieren und zu schulen.

* Verfahren, um Datenpakete in Netzwerken zu überwachen und zu filtern. Insbesondere werden Datenpakete hierbei auf unerwünschte Inhalte hin untersucht.
** Damit sind technische Sicherheitstests gemeint, um Schwachstellen bei IT-Systemen oder Netzwerken zu detektieren. Man bedient sich dabei ähnlicher Methoden wie ein Angreifer - jedoch finden diese Tests in einem vorher festgelegten Geltungsbereich und Rahmen statt.

auf Unternehmensressourcen musste sicher gewährleistet werden (Risiko), sondern auch sichergestellt werden, dass Informations- und IT-Sicherheitsvorgaben nach wie vor umgesetzt werden (Compliance). Was die die Compliance angeht, fehlt es gerade den kleinen und mittleren Unternehmen hier an Ressourcen und Expertise bezüglich der Umsetzung der z. T. weitreichenden sowie komplexen Gesetze, Verordnungen, Anforderungen und Regularien (siehe z. B. die DSGVO). Verletzungen diesbezüglich können zu ernsthaften juristischen Konsequenzen führen. Deshalb ist es natürlich im Interesse der Unternehmen zu überprüfen, ob die Richtlinien und dergleichen tatsächlich umgesetzt werden (Governance).

Dies ist ein gutes Beispiel, dass es einer ganzheitlichen Sicht für eine konforme Absicherung bedarf. Alle relevanten Informationen sollten optimalerweise auch an einem Ort zusammenlaufen. Leider existieren gerade bei schwergewichtigen Governance-Frameworks wie COBIT[14] Einführungsbarrieren in kleinen und mittleren Unternehmen[15]. Bestehende Ansätze, Lösungen und Frameworks des Governance-, Risiko- und Compliance-Managements (GRC) auf dem Markt richten sich überwiegend an Großunternehmen und sind noch zu wenig für KMU ausgestaltet. Deshalb veröffentlichte das Kompetenzzentrum IT-Wirtschaft einen KMU-freundlichen, kompetenzorientierten Ansatz zur Wahrnehmung und Messung der Kompetenzen im Bereich des IT-Governance-, Risiko- und Compliance-Managements in KMU[16]. Eine konkrete Umsetzung des Ansatzes wird in Form eines IT-GRC-Reifegrad-Werkzeugs im Kasten rechts vorgestellt.

IT-GRC Reifegrad Werkzeug

Basierend auf einem kompetenzorientierten IT-GRC-Ansatz entwickelt das Kompetenzzentrum IT-Wirtschaft ein prototypisches IT-GRC-Reifegrad-Werkzeug, mit dem Ziel, kleine und mittlere Unternehmen für IT-Governance-, Risiko- und Compliance-Management im Allgemeinen zu sensibilisieren und folglich einen niederschwelligen und anwenderfreundlichen Ein¬stieg in die Thematik zu ermöglichen. Zusätzlich zur technischen IT-Sicherheit und zu organisatorischen Fähigkeiten hebt das Werkzeug unter anderem auch die persönlich wahrgenommene Bedeutung von Sicherheitsthemen im Unternehmen hervor („Security Awareness"). Das Reifegrad-Werkzeug ermittelt dabei Handlungsbedarfe in den folgenden sechs Kompetenzbereichen:

1. IT-Compliance,
2. IT-Governance,
3. Security Awareness,
4. Information Security Management System (ISMS),
5. Cyber-Sicherheit und
6. Mobile Sicherheit

Das Werkzeug liefert nach einer abschließendem Bewertung Handlungsempfehlungen, z. B. in Form von unterstützenden Management-Maßnahmen. Des Weiteren werden mögliche Schutzmaßnahmen aufgezeigt, auf nützliche Anwendungen verwiesen sowie weiterführende Hilfestellungen in Form von Links, Dokumenten und Literatur gegeben.

Fazit und Ausblick

Datensicherheit ist ein Schlüsselfaktor für eine erfolgreiche Digitalisierung. Um diese gerade in Kooperationen und Konsortien, auch für KMU, gewährleisten zu können, ist eine gemeinsame Sicherheitsausrichtung unerlässlich. Nur so kann sichergestellt werden, dass sich die kooperierenden Unternehmen für einen Geltungsbereich auf verbindliche IT-Sicherheits-Mindeststandards verständigen. Dafür eignet sich insbesondere eine Sicherheitsrichtlinie im Rahmen von Kooperationen. Wenn es um die Verknüpfung von Software-Lösungen geht, sind APIs dabei von herausragender Bedeutung, da sie das Verbindungselement einer App-getriebenen Welt darstellen. Die Absicherung dieser Schnittstellen ist eine somit wichtige Voraussetzung für einen sicheren Datenaustausch. Hier sind sowohl Dienstleister als auch Entwickler in der Pflicht, bereitgestellte APIs adäquat zu schützen und Sicherheitsaspekte bereits in die Entwicklung einer API miteinzubeziehen (Security by Design). Des Weiteren muss der sichere Datenaustausch ganzheitlicher gedacht werden, da es neben einer reinen technischen Dimension auch immer die Compliance und weitere Dimensionen zu berücksichtigen gilt. Um diese unterschiedlichen Dimensionen und Sichtweisen zu vereinen, entwickelte das Kompetenzzentrum IT-Wirtschaft einen KMU-freundlichen Ansatz zur Wahrnehmung und Messung von IT-GRC-Management-Kompetenzen. Prototypisch wird dieser Ansatz in Form eines Reifegrad-Werkzeugs umgesetzt, welches den kooperierenden Unternehmen (aber auch KMU allgemein) neben der Bewertung des IT-GRC-Reifegrades zusätzlich nützliche Anwendungen, Hilfsmittel, Anlaufstellen sowie weiterführende Hilfestellungen in Form von Links und Literatur an die Hand gibt.

14 International sehr verbreitetes Framework für IT-Governance.
15 Guldentops (2014).
16 Johannsen und Kant (2020).

Literatur

Bundeskriminalamt (2021): Cybercrime Bundeslagebild 2020. Stand April 2021. *https://www.bka.de/SharedDocs/Kurzmeldungen/DE/Kurzmeldungen/210507_BLBCyber.html* (abgerufen am 23.06.2021)

Cyber Security Cluster Bonn e.V. (2020): Mehr Sicherheit für die digitale Transformation. Jahresbericht des Weisenrats für Cyber-Sicherheit 2020. Bonn, 15. Mai 2020. *https://cyber-security-cluster.eu/_Resources/Persistent/a/1/d/9/a1d95dca3a8642822f22eb1372cd2b66e271d4fe/Mehr%20Sicherheit%20f%C3%BCr%20die%20digitale%20Transformation%20-%20Jahresbericht%20des%20Weiserats%20f%C3%BCr%20Cyber-Sicherheit.pdf* (abgerufen am 23.06.2021)

Guldentops E. (2014) Governance of IT in small and medium sized enterprises. In: Devos J, van Landeghem H, Deschoolmeester D (Hrsg) Information systems for small and medium-sized enterprises. Springer, Berlin/Heidelberg, S 3–24

Begleitforschung Mittelstand-Digital (2019): Künstliche Intelligenz im Mittelstand. Relevanz, Anwendungen, Transfer. April 2019. *https://www.mittelstand-digital.de/MD/Redaktion/DE/Publikationen/kuenstliche-intelligenz-im-mittelstand.html* (abgerufen am 23.06.2021)

Johannsen, A.; Kant, D. (2020): IT-Governance, Risiko- und Compliance-Management (IT-GRC) – Ein Kompetenzorientierter Ansatz für KMU. HMD Praxis der Wirtschaftsinformatik 57. Springer. *https://link.springer.com/article/10.1365/s40702-020-00625-8* (abgerufen am 27.06.2021)

Köhler, C.; Rickerson, C.; Steinkrüger, P.; Wohlrab, O.; Kolb, S.; Kern, E.; Stuchtey, T.; Szanto, A. (2021): T-Dienstleister als Akteure zur Stärkung der IT-Sicherheit bei KMU in Deutschland". Studie im Auftrag des Bundesministeriums für Wirtschaft und Energie. Februar 2021. *https://www.bmwi.de/Redaktion/DE/Publikationen/Studien/it-dienstleister-als-akteure-zur-staerkung-der-it-sicherheit-bei-kmu-in-deutschland-anhang.html* (abgerufen am 27.06.2021)

Mittelstand 4.0 Kompetenzzentrum IT-Wirtschaft (2019): Information Security Policy. Informationssicherheitsrichtlinie für eine Kooperation. Version 1.7 . September 2019. *https://itwirtschaft.de/wp-content/uploads/2019/09/InfoSec-Policy-1_7.pdf* (abgerufen am 23.06.2021)

Mittelstand 4.0 Kompetenzzentrum IT-Wirtschaft (2019): Non Disclosure Agreement. Vertraulichkeitsvereinbarung. November 2019. *https://itwirtschaft.de/wp-content/uploads/2019/12/Muster_NDA.pdf* (abgerufen am 23.06.2021)

OWASP API Security Project (2019): OWASP API Security Top 10 2019. The Ten Most Critical API Security Risks. URL: *https://owasp.org/www-project-top-ten/* (abgerufen am 27.06.2021)

Siriwardena, P. (2020).: Advanced API Security – OAuth and Beyond, Apress, 2. Auflage, 2020

Yalon, E. (2019): API Security – From Therory to Practice. Checkmarx. November 2019. Seite 30. Folien: *https://de.slideshare.net/AdarWeidman/checkmarx-meetup-api-security-api-security-top-10-erez-yalon* (abgerufen am 23.06.2021). Video: https://www.youtube.com/watch?v=0ei3CdD7Ebk (abgerufen am 24.06.2021).

Zumerle, D; D'Hoinne, J.; O'Neill, M. (2019): API Security. What You Need to Do to Protect Your APIs [online], URL: *https://www.gartner.com/en/documents/3956746/api-security-what-you-need-to-do-to-protect-your-apis* (abgerufen am 27.06.2021)

Autoren

Daniel Kant M. Sc. studierte nach seiner Ausbildung an der Technischen Universität Berlin an der TH Brandenburg Informatik mit dem Schwerpunkt „Security and Forensics". Seine Masterarbeit schrieb er über Kritische Infrastrukturen und Cyber-Sicherheit. Derzeit ist er wissenschaftlicher Mitarbeiter und informiert im Rahmen des Mittelstand 4.0 Kompetenzzentrums IT-Wirtschaft kleine und mittlere IT-Unternehmen rund um die Themen IT-Sicherheit und Datenschutz. Sein Forschungsgebiet ist insbesondere die Schnittstelle zwischen IT-Sicherheit und der Künstlichen Intelligenz.

Prof. Dr. **Andreas Johannsen** studierte an den Universitäten Tübingen und Edinburgh, UK und promovierte bei Prof. Helmut Krcmar. Er ist geschäftsführender Direktor des Instituts für Betriebliche Integration und Digitalisierung (IBID). Weiterhin ist er Konsortialpartner im Mittelstand 4.0 Kompetenzzentrum IT-Wirtschaft und leitet dort die Arbeitspakete Schnittstellen & Datenschutz/-Sicherheit. Seit 2006 ist er Professor für Systementwicklung und -integration an der Technischen Hochschule Brandenburg. Zu seinen Arbeitsgebieten gehören die Themen sichere Systementwicklung und -Integration, Betriebliche Anwendungssysteme, und Agiles Projektmanagement.

Das Mittelstand 4.0-Kompetenzzentrum IT-Wirtschaft (KIW) informiert die mittelständisch geprägte IT-Wirtschaft und fördert die Vernetzung sowie die Realisierung kooperativer Geschäftsmodelle. Die Kernaufgabe des Kompetenzzentrums ist die Vernetzung von mittelständischen IT-Unternehmen und deren IT-Lösungen. Die TH Brandenburg unterstützt dabei als Konsortialpartner im Bereich IT-Sicherheit und Datenschutz mit Angeboten zur Selbstbefähigung sowie zur Erhöhung des Bewusstseins für die Informations- und IT-Sicherheit in Form von Werkzeugen, Webinaren, Veranstaltungen, Fachvorträgen, Workshops, Vorlagen und Leitfäden.

Weitere Informationen zum Kompetenzzentrum finden Sie unter *https://itwirtschaft.de/*

Mittelstand 4.0 Kompetenzzentrum IT-Wirtschaft

In der Reihe Mittelstand-Digital Magazin WISSENSCHAFT TRIFFT PRAXIS sind bisher erschienen:

Ausgabe 1:	Usability betrieblicher IT-Anwendungen
Ausgabe 2:	Digitale Standards im elektronischen Geschäftsverkehr
Ausgabe 3:	User Experience – Positives Erleben betrieblicher IT
Ausgabe 4:	Neue Formen des Home Experience Design
Ausgabe 5:	Digitale Bildung: Kompetenzen für die digital-unterstützte Wertschöpfung
Ausgabe 6:	Usability und User Experience in der Arbeitswelt von morgen
Ausgabe 7:	eBusiness-Standards als Wegbereiter für Industrie 4.0
Ausgabe 8:	Digitale Geschäftsmodelle: Erfolgsfaktoren und Praxisbeispiele
Ausgabe 9:	Digitale Produktionsmittel im Einsatz
Ausgabe 10:	Digitales Recht & Sicherheit
Ausgabe 11:	Arbeiten in der digital vernetzten Welt
Ausgabe 12:	Vernetzte Wertschöpfung
Ausgabe 13:	Digitale Daten
Ausgabe 14:	Nachhaltigkeit und Digitalisierung
Ausgabe 15:	Handel und Gastgewerbe

Mittelstand-Digital informiert kleine und mittlere Unternehmen über die Chancen und Herausforderungen der Digitalisierung. Kompetenzzentren helfen vor Ort dem kleinen Einzelhändler genauso wie dem größeren Produktionsbetrieb mit Expertenwissen, Demonstrationszentren, Netzwerken zum Erfahrungsaustausch und praktischen Beispielen. Das Bundesministerium für Wirtschaft und Energie ermöglicht die kostenlose Nutzung aller Angebote von Mittelstand-Digital.

Weitere Informationen finden Sie unter *www.mittelstand-digital.de*.

www.mittelstand-digital.de

ISSN (Print) 2198-8544
ISSN (Online) 2198-9362