2.3.1 Datensicherheit in 4.0-Prozessen

Stichwörter: Cybersicherheit, IT-Sicherheit, Vernetzung, Virtualisierung, IT-Infrastrukturen

› Warum ist das Thema wichtig?

Mit zunehmender Vernetzung von Arbeitsmitteln durch intelligente Software[1] mit ihren Modellen der künstlichen Intelligenz (KI) in und außerhalb des Betriebes wächst die Bedeutung der Datensicherheit. Mittels cyber-physischer-Systeme (CPS)[2] können nicht nur Daten beinahe in Echtzeit zwischen einzelnen Systemen ausgetauscht werden, mit zunehmender Datenvernetzung smarter Geräte (wie zum Beispiel Arbeitsmittel, Anlagen, Arbeitsstoffe, Fahrzeuge, Einrichtungen) wächst auch die Angriffsfläche bei Betrieben und den dort tätigen Menschen.[3] Durch das autonome Agieren der 4.0-Technologie[4] beinahe in Echtzeit können sich Fehlfunktionen schneller auf das Gesamtsystem der Arbeit auswirken als unter Nutzung bisheriger Technologien. Eine erfolgreiche Nutzung von 4.0-Technologien in Betrieben setzt eine den Anforderungen angepasste systematisch umgesetzte Datensicherheit voraus.[5]

› Worum geht es bei dem Thema?

Begriffe: Datensicherheit – Cybersicherheit

Datensicherheit beinhaltet im Folgenden alle technischen, organisatorischen und rechtlichen Aspekte, die zur Sicherheit im Umgang mit sämtlichen Daten dienen, die im Betrieb generiert und verarbeitet werden. Erreicht wird dies durch die Beachtung der Schutzgüter der IT-Sicherheit.[6]

- **Vertraulichkeit:** Nur befugte Personen und autonome technische Systeme (intelligente Software [inkl. KI]), können auf bestimmte Daten zugreifen.
- **Integrität:** Unversehrtheit sowohl vor Manipulation als auch technischen Defekten (der Zustand der Daten kann nicht unbefugt verändert, beschädigt oder gelöscht werden).
- **Verfügbarkeit:** Verwendbarkeit von Daten im Bedarfsfall (inklusive Verhinderung von Systemausfällen).
- **Authentizität:** Echtheit und Glaubwürdigkeit der Daten.

Datensicherheit umfasst somit die sichere Übermittlung sowie Speicherung und die Sicherstellung, dass keine unbefugte Person oder intelligente Software (inkl. KI) Zugang zu den Daten erhält.

Das IT-Sicherheitsgesetz[7] und die Datenschutz-Grundverordnung (DSGVO) verpflichtet Unternehmen,[8] organisatorische und technische Vorkehrungen zur Vermeidung von Störungen ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen.

Cybersicherheit befasst sich mit allen Aspekten der Sicherheit in der Informations- und Kommunikationstechnik. Das Aktionsfeld der Informationssicherheit wird dabei auf den gesamten Cyberraum ausgeweitet. Dieser umfasst sämtliche mit dem Internet und vergleichbaren Netzen verbundene Informationstechnik und schließt darauf basierende Kommunikation, Anwendungen, Prozesse und verarbeitete Informationen mit ein.[9]

Viele Betriebe haben smarte Arbeitsmittel wie Assistenzsysteme, Smartphones, Tablets oder Werkzeuge im Einsatz. Diese smarten Arbeitsmittel können untereinander vernetzt sein. › *Siehe Umsetzungshilfe 3.1.4 Sicherheit von verketteten Arbeitsmitteln mit 4.0-Technologie.*

Bisher physikalisch voneinander abgegrenzte Systeme (wie Arbeitsmittel, Produkte, Räume, Prozesse und Menschen) vernetzen sich mit dem Einsatz von 4.0-Technologien mit ihren Modellen der künstlichen Intelligenz (KI) zu intelligenten, autonomen Systemen.

Dabei kann eine ununterbrochene Erfassung von Daten innerhalb von Geschäfts- und Arbeitsprozessen stattfinden.[10] Im Unternehmen vorhandene Daten beinhalten enormes Wissen über Märkte, Beschäftigte, Kunden und Anlagen. Mit dem Einsatz von intelligenter Software (inkl. KI) weitet sich

Diese Umsetzungshilfe gibt Experten und Interessierten Anregungen, wie Arbeit 4.0 zu gestalten ist. Die Empfehlungen sollten an die jeweilige konkrete betriebliche Situation angepasst werden.

[1] Intelligente Software steuert cyber-physische Systeme (CPS) und andere autonome technische Systeme (wie Messenger-Programme). Intelligente Software nutzt Modelle künstlicher Intelligenz zusammen mit anderen Basistechnologien wie zum Beispiel Algorithmen, semantischen Technologien, Data-Mining. Intelligente Software ist autonom und selbstlernend.

[2] Cyber-physische Systeme (CPS) verbinden und steuern als autonome technische Systeme Arbeitsmittel, Produkte, Räume, Prozesse und Menschen beinahe in Echtzeit. Die komplette oder teilweise Steuerung übernimmt intelligente Software auf Grundlage von Modellen der künstlichen Intelligenz. Genutzt werden dazu unter anderem auch Sensoren/Aktoren, Verwaltungsschalen, Plattformen/Clouds.

[3] BSI 2016a, S. 3

[4] 4.0-Technologie bezeichnet hier Hardware und technologische Produkte (wie Assistenzmittel/Smartphones, Sensoren/Aktoren in smarten Arbeitsmitteln, Fahrzeugen, Produkten, Räumen usw., smarte Dienstleistungen, Apps), die von intelligenter Software (inkl. KI) ganz oder teilweise gesteuert werden.

[5] BSI 2016a, S. 3

[6] Schutzziele auf Basis der Schutzgüter werden zum Erreichen/Einhalten der Datensicherheit vor beabsichtigten Angriffen auf IT-Systeme definiert, BMWi 2016.

[7] Im Juli 2015 ist das Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) in Kraft getreten, BSI 2016b.

[8] Organisationen, die der Telekommunikationsbranche angehören oder zu den sogenannten Kritischen Infrastrukturen (KRITIS) zählen, unterliegen dem IT-Sicherheitsgesetz. Das sind Anlagen oder Systeme, die für die Erfüllung wichtiger gesellschaftlicher Funktionen unverzichtbar sind. Betriebe müssen eigenständig prüfen, ob sie dazuzählen. Ausgenommen sind lediglich Kleinstunternehmen, das heißt Firmen mit weniger als zehn Beschäftigten und weniger als zwei Mio. € Jahresumsatz.

[9] BSI 2018

[10] Fallenbeck & Eckert 2014, S. 397

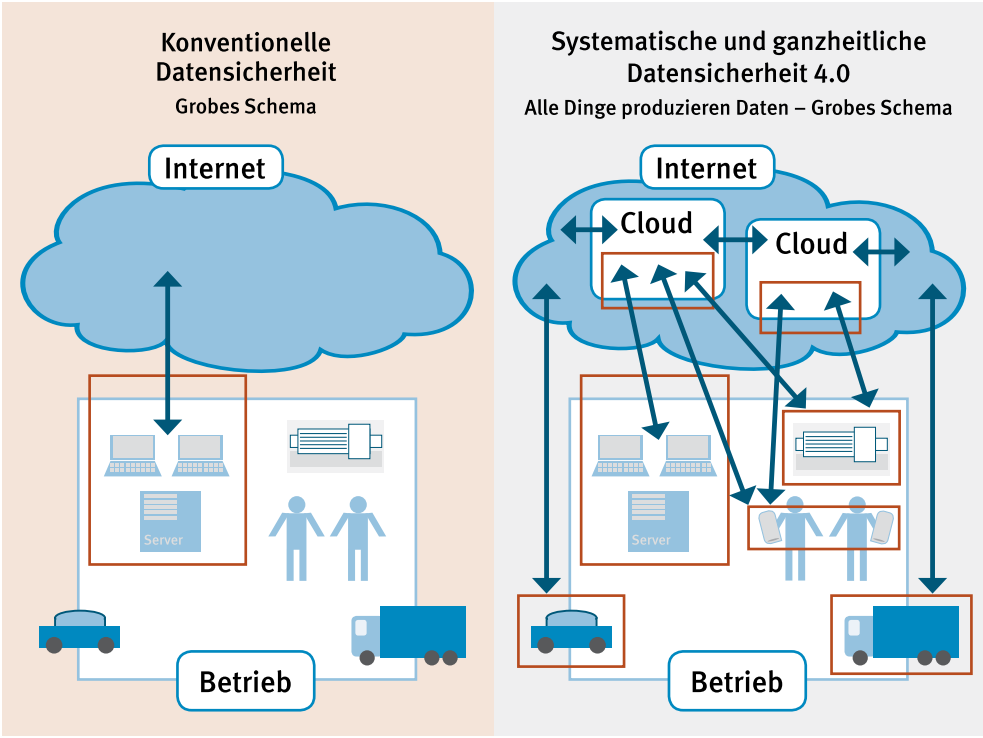

Abbildung 1: Konventionelle versus ganzheitliche Datensicherheit (eigene Darstellung)

der virtuelle Raum nun auch in die physische Welt aus: Intelligente Produkte steuern ganz oder teilweise die Prozesse oder die Kommunikation in Unternehmen.[11] Die Daten und die intelligente Software der CPS (inkl. KI) liegen oftmals nicht auf betriebseigenen Servern, sondern auf externen Servern einer Cloud, und weitere Systeme können gegebenenfalls auf die Daten zugreifen (Cybersicherheit).

Dabei sind drei Aspekte für die Datensicherheit von Bedeutung:

- Durch die steigende Anzahl von genutzten Geräten, die Verbindung mit dem Internet haben, steigen die Datenmengen, die in Betrieben erhoben und gespeichert werden, drastisch an.
- Wenn Geräte, Anlagen oder ganze Herstellungsprozesse durch 4.0-Technologie (teilweise oder vollständig) autonom gesteuert und vernetzt werden, macht sie das anfälliger für Beeinträchtigungen.[12]
- Durch den Austausch von Daten beinahe in Echtzeit, auch über Unternehmensgrenzen hinaus, steigen die Verletzlichkeit (Vulnerabilität) von Daten und die Gefahr ihrer Korruption.

Dadurch dehnt sich Datensicherheit auf neue Handlungsbereiche aus und erfordert deswegen eine systematische und ganzheitliche Betrachtung – *siehe Abbildung 1*.

Wenn ein sicherer Umgang mit den Daten nicht gewährleistet wird, können diese Manipulationen, Diebstahl oder anderen Angriffen ausgesetzt sein. Oft sind es keine Cyberkriminellen, die die Datensicherheit bedrohen, sondern unabsichtliche oder unachtsame Veränderungen durch Führungskräfte und Beschäftigte, beispielsweise das Löschen einer Datei auf einer geteilten Cloud. Bei Beeinträchtigung der Datensicherheit können auch Schäden an den Maschinen und Produkten sowie Beeinträchtigungen von Prozessen und Gefährdungen von Personen auftreten. Es können vertrauliche Informationen offengelegt und missbraucht werden oder Schäden an wichtigen Systemen und Dokumenten entstehen.

Die geänderten Anforderungen für Datensicherheit zeigen folgendes Szenario beispielhaft auf: Ein Formenbauer stellt für einen Architekten Modelle und Formen her. Die von dem Architekten erhaltene Datei mit den Vorlagen, die gleichzeitig die Fräsmaschine des Formenbauers konfiguriert, weist jedoch ein Schadprogramm auf. Dieses breitet sich auf das autonome Steuerungssystem und dadurch auf die Fräs-/Druckmaschinen aus. Die Suche nach der Ursache ist langwierig und die Aufträge können nicht oder nur fehlerhaft ausgeführt werden.[13] Das Szenario zeigt, dass auch Kundendaten die Datensicherheit beeinträchtigen können. Unternehmen müssen gewährleisten, dass sie jederzeit sicher auf Daten zurückgreifen können beziehungsweise schadhafte Daten abwehren. Gleichzeitig dürfen die eigenen Daten die Datensicherheit bei Kunden und Lieferanten nicht gefährden.

Schadensbehaftete Daten können nicht nur von außerhalb des Unternehmens kommen. Neben Angriffen durch Außen- oder Innentäter dürfen bei der Betrachtung von 4.0-Prozessen zur IT-Sicherheit sonstige Schäden, die durch technisches oder menschliches Fehlverhalten oder sonstige Ereignisse hervorgerufen werden, nicht vernachlässigt werden.[14] In vielen Unternehmen werden private mobile Geräte (BYOD, Bring Your Own Device) auch im Arbeitskontext eingesetzt und erhalten Zugriff auf Ressourcen des Unternehmens. In den meisten Betrieben ist es gelebte Praxis, smarte Geräte und Arbeitsmittel sowie IT-Systeme mit ganz unterschiedlichen Sicherheitsanforderungen miteinander zu verbinden. Schadensbehaftete Daten von außen dringen

[11] Kagermann 2017, S. 235
[12] vgl. Kagermann 2017, S. 235; Röcher 2013
[13] Röcher 2013
[14] BMWi 2016, S. 25

größtenteils über das Internet ein. Bisher war daran „nur“ die IT-Infrastruktur einzelner Arbeitsplätze angebunden. Nun können Schäden über jedes smarte Arbeitsmittel, das in einem Unternehmen genutzt wird, auf die damit vernetzten Steuerungssysteme weiterverbreitet werden und so Funktionen und Einstellungen zum Beispiel der Maschinen ändern. Im Rahmen der Internetanbindung setzen viele Betriebe Sicherheitslösungen wie Firewalls, Anti-Virus-Programme oder Intrusion-Prevention-Systeme ein, die den 4.0-Anforderungen aber nicht mehr genügen. So wird es beispielsweise Viren – die zuvor eher von Desktop-PCs bekannt waren – durch die vernetzten Systeme ermöglicht, sich in verschiedenen Prozessen, die mit einer firmeninternen Software ausgestattet sind, auszubreiten.[15] Unternehmen können zwar von den Erfahrungen klassischer IT-Lösungen profitieren, doch sollten bestehende Technologien und Prozesse auf den eigenen

Datensicherheit von 4.0-Prozessen als systematisches ganzheitliches Konzept | **Tabelle 1**

	Beispiele für organisatorische Aspekte von Datensicherheit von CPS	Beispiele für technische Aspekte von Datensicherheit von CPS
Arbeitsplatz/ -plätze	› Was müssen Führungskräfte und Beschäftigte bei der Nutzung smarter Arbeitsmittel beachten?	› Wie kann die sichere Datenübertragung von und zu smarten Arbeitsmitteln technisch sichergestellt werden?
Betrieb	› Haben wir die Sicherheitsrisiken für unseren Betrieb durch den Einsatz von 4.0-Technologien (inkl. KI) analysiert und haben wir auf dieser Grundlage ein Konzept, das die Datensicherheit gewährleistet, sowohl gegenüber Angriffen und Zugriffen von außen als auch Bedienfehlern? › Welche Daten sollten wann, wem und wie verfügbar sein oder werden wann, von wem und wie benötigt? › Welche Steuerungsprozesse soll intelligente Software (inkl. KI) ganz oder teilweise übernehmen und welche Sicherheitsaspekte sind dabei zu berücksichtigen? › Wird ein zusätzlicher Datensicherheitsbeauftragter für den Umgang mit autonomen Systemen benötigt?	› Wie können die vernetzten Systeme und Prozesse gegen Angriffe und Zugriffe von außen geschützt werden? (technische Umsetzung) › Wie können Steuerungsprozesse durch intelligente Software (inkl. KI) technisch abgesichert werden, damit die Daten nicht gefährdet sind? › Welche technischen Komponenten werden für den sicheren Datenaustausch beinahe in Echtzeit benötigt? › Wie können die benötigten Daten den legitimierten Personen zur passenden Zeit in der passenden Form sicher verfügbar gemacht werden?
Überbetriebliche Prozesse zum Beispiel zwischen Betrieben, Crowdworkern, Zulieferern, Vernetzung von CPS über die Cloud	› Welche Anforderungen an Datensicherheit sollen die genutzten Clouds erfüllen? › Welche Daten aus unserem Betrieb werden durch die 4.0-Technologien erzeugt und wissen wir, wie sie zum Beispiel über Plattformen genutzt werden? (Cybersicherheit) › Welche konkreten Sicherheitsrisiken gibt es? Welche Daten und Prozesse sollen nur intern verfügbar sein und welche sollen für Dritte freigegeben werden? › Welche Verträge sollten mit den Kooperationspartnern geschlossen werden? (zum Beispiel Eigentumsrechte an bereitgestellten/verarbeiteten Daten oder zur Haftung durch Leistungsstörungen)	› Erfüllen die genutzten Clouds die technischen Anforderungen an die Datensicherheit? › Welche smarten Arbeitsmittel, Geräte, Anwendungen und Produkte kommunizieren aus den eigenen Geschäftsprozessen welche Informationen in welcher Form wohin? › Wie können die vernetzten Systeme und Prozesse gegen Angriffe und Zugriffe von außen geschützt werden? (technische Umsetzung) › Erfüllen die autonomen technischen Systeme die vertraglich festgelegten technischen Bedingungen oder können sie angepasst werden, um diese zu erfüllen?
Kunden	› Wie kritisch sind welche Kundendaten in Bezug auf Vertraulichkeit und Integrität? Wie kann ein sicherer Umgang mit Kundendaten gewährleistet werden?	› Sind die Schnittstellen zum Kunden sicher und gehen die autonomen technischen Systeme sicher mit den Kundendaten um?

[15] Fallenbeck & Eckert 2014, S. 397

Sicherheitsbedarf hin reflektiert und angepasst werden. Bei 4.0-Technologien ist es notwendig, nicht nur die einzelnen Teile der Prozesskette sicher zu gestalten (zum Beispiel den Kundenkontakt), vielmehr sollte der gesamte Prozess den Kriterien des sicheren Umgangs mit Daten genügen. Besonders an Schnittstellen, wie zum Beispiel bei Zugriff mehrerer Anwendungen auf dieselben Datensätze, können potenzielle Risiken entstehen.[16]

Auch die Nutzung von Cloud-Diensten für betriebliche Daten erweitert und verändert das Feld der Datensicherheit. Während klassische Softwareprodukte meist vom Nutzer selbst auf eigenen Rechnern installiert und betrieben werden, wird beim Cloud Computing Software in Form von Cloud-Services wie zum Beispiel SaaS (Software as a Service) über das Internet bereitgestellt – Installation, Betrieb und Wartung werden vom Service-Anbieter übernommen. Das Rechenzentrum des Service-Anbieters kann durchaus ein höheres Sicherheitsniveau als der Serverraum eines kleinen und mittleren Unternehmens aufweisen, auch reduziert sich der Aufwand für Back-ups und erfolgt geräteunabhängig.[17] › *Siehe Umsetzungshilfen 2.5.1 Anforderungen an eine Cloud und 2.5.2 Cloud-Modelle der Bereitstellung und Dienstleistung*.

Zur Gewährleistung der Datensicherheit bei 4.0-Prozessen werden Konzepte immer wichtiger, die neben technischen auch organisatorische Maßnahmen vorsehen.[18] Dabei sind Fragestellungen relevant, wie sie beispielhaft in Tabelle 1 aufgeführt sind.

› Welche Chancen und Gefahren gibt es?

Chancen einer solide gebauten Datensicherheit sind:

- Hohe Funktionalität der smarten Arbeitsmittel
- Störungsfreie und sichere Arbeitsprozesse
- Höhere Akzeptanz von Führungskräften und Beschäftigten gegenüber der Nutzung von 4.0-Technologien aufgrund von sicherem Umgang mit Daten
- Sicherer Umgang mit Daten ist wesentliches zukunftsträchtiges Qualitäts- und Unterscheidungsmerkmal und bildet einen positiven Wettbewerbsfaktor[19]
- Gute und verlässliche Datensicherheit stärkt das in das Unternehmen gesetzte Vertrauen von Geschäftspartnern. Datensicherheit unterstützt einen kontinuierlichen Geschäftsbetrieb und den gewissenhaften Umgang mit Informationen
- Mögliche Gefährdungen der Systeme werden prospektiv erkannt und können reduziert werden

Eine nicht hergestellte Sicherheit der Daten kann beispielsweise folgende **Gefahren** mit sich bringen:

- Unberechtigte Informationsweitergabe, Datenverlust, Informationsabfluss,
- Verlust der Kontrolle über Daten und Anwendungen
- Sabotage oder Manipulation von Informationen oder Arbeitsmitteln
- Gefährdung von Beschäftigten durch gestörte/manipulierte Arbeitsprozesse auf Grundlage von fehlender Datensicherheit
- Verletzung geltender Vorgaben und Richtlinien (zum Beispiel an Datenschutz oder im Steuerrecht)
- Diebstahl von Informationen sowie geistigem Eigentum
- Mögliche Gefährdungen werden nicht oder zu spät erkannt und können nicht (mehr) reduziert werden
- Temporäre Beeinträchtigung von Arbeitsabläufen, Arbeitsmitteln, Assistenzsystemen oder Sicherheitsanlagen, zum Beispiel durch Ausfall von Cloud-Dienstleistungen (Denial of Service)

› Welche Maßnahmen sind zu empfehlen?

Maßnahmen zur Sicherung der Daten sollten möglichst zu den Sicherheitsanforderungen des jeweiligen Betriebes passen. Zu Beginn ist es sinnvoll, Geschäftsprozesse, in denen 4.0-Technologien mit ihren Modellen der künstlichen Intelligenz (KI) genutzt werden, auf deren Schutzbedarf zu untersuchen und die Risiken einzuschätzen. › *Siehe Umsetzungshilfe 2.2.1 Risikobetrachtung von 4.0-Prozessen*. Dabei kann die Erstellung realistischer Szenarien helfen, die einen vollständigen Geschäftsprozess umfassen (beispielsweise die Planung und Durchführung eines Auftrags auf einer Montagestelle). Dabei kann reflektiert werden …

- … welche personenbezogenen und Betriebsdaten erfasst werden (von den Arbeitsmitteln/Fahrzeugen/Räumen/Assistenzsystemen) und welche Daten für das eigene Unternehmen (auch innerhalb von Wertschöpfungsketten) besonders sensibel/schützenswert sind. Dazu gehört auch, zu beschreiben, wo überall im täglichen Ablauf Daten eingegeben, abgerufen, verarbeitet, mobil verwendet oder gespeichert werden.[20]
- … wer in welchem Ausmaß und zu welchem Zeitpunkt Zugriff auf die Daten, wer Lese- und Schreibrechte hat.[21] Dazu gehört auch zu reflektieren, bei wem die Verantwortung/Haftung für die Gewährleistung der IT-Sicherheit liegt, vor allem bei einem Wertschöpfungsnetzwerk oder bei der Kooperation mit anderen Partnern über BIM. › *Siehe Umsetzungshilfe 2.4.2 Building Information Modeling*.
- … wo diese Daten aus dem Betrieb lagern und was mit ihnen geschieht (Cybersicherheit), ob der Serverstandort im Betrieb oder extern ist und bei Nutzung einer Cloud, welche Rechtsprechung zugrunde liegt. Dazu gehört auch, ob es dabei physische Bedrohungen gibt, zum Beispiel durch Verschleiß der Datenträger, oder wie es um die Ausfallsicherheit der Produktionsanlagen bestellt ist. Dazu können

[16] BSI 2011
[17] vgl. Christmann et al. 2014, S. 3ff.; BSI 2016c, S. 6ff.
[18] Röcher 2013; § 9 des Bundesdatenschutzgesetzes, der die inner- und überbetriebliche Anwendung des Themas Datensicherheit regelt: Er sieht technische und organisatorische Maßnahmen als Wege einer betrieblichen Gestaltung vor.
[19] Schröter 2015, S. 1
[20] Schröter 2015
[21] Schröter 2015

Informationen beim Anbieter/Hersteller eingefordert werden.

- … wie Führungskräfte und Beschäftigte mit Daten, auch von Dritten, umgehen. Dazu gehört auch zu überprüfen, ob die Daten löschbar sind beziehungsweise nach welchem Zeitraum Daten gelöscht werden (müssen/dürfen).
- … welche Arbeitsmittel, Anlagen, Fahrzeuge, Gebäude, Assistenzsysteme oder Einrichtungen mit dem Internet verbunden sein sollten, ob und wie diese untereinander vernetzt werden.

Mithilfe dieser Hinweise lassen sich individuelle Sicherheitsmaßnahmen für den Betrieb ableiten.

Mögliche Sicherheitsmaßnahmen

Die Datensicherheit sollte über den gesamten Lebenszyklus der eingesetzten 4.0-Technologien (inkl. KI) gewährleistet werden können: Bereits bei der Planung sollten Sicherheitsaspekte in den Fokus gerückt werden. Auch in der Beschaffung, der individuellen Anpassung/Programmierung bis hin zur Nutzung und der Entsorgung sollten die Systeme hinsichtlich des sicheren Umgangs mit Daten betrachtet werden. Der Betrieb sollte ein Gesamtkonzept zur Datensicherheit aus organisatorischen und technischen Maßnahmen erstellen.

Beispiele für organisatorische Maßnahmen

- Die Benennung von einer oder mehreren Personen, die im Betrieb dieses Thema voranbringen, ist sinnvoll.[22] In kleineren Betrieben kann zum Beispiel eine Führungskraft diese Aufgabe übernehmen oder ein Digital-Berater. › *Siehe Umsetzungshilfe 2.1.8 Digital-Berater („Kümmerer“).* Zu den Aufgaben dieser Person gehören unter anderem eine Bestandsaufnahme bisheriger Aktivitäten zur Datensicherheit, wobei sich die Person von Experten beraten lassen sollte (zum Beispiel von Kammern und Fachverbänden, IT-Experten). Die benannte Person sollte auch überlegen, welche Sicherheitsvorkehrungen notwendig sind (Sicherheitskonzept) und Ansprechpartner für Experten sein, die die IT-Sicherheitsüberlegungen umsetzen. Schließlich sollte diese Person auch darauf achten, dass die IT-Sicherheitsmaßnahmen dokumentiert sowie kontrolliert und ständig verbessert werden.
- Sensibilisierung und Schulung der Anwender/innen für den korrekten Umgang mit vernetzten Daten, zum Beispiel durch den Datensicherheitsbeauftragten, aber auch durch externe Experten, wie Hersteller, Handwerksorganisationen. Oftmals besteht wenig Bewusstsein für Risiken beim Umgang mit Daten, besonders für Datensicherheitsrisiken bei ortsflexibler Arbeit. Dabei ist nicht das spezifische IT-Detailwissen zentral, sondern das grundlegende Vermögen, die genutzten Geräte „richtig“ einzusetzen. Grundsätzlich ist die Nutzung privater Geräte im Arbeitskontext („Bring your own Device“) nicht zu empfehlen. Ist die Nutzung nicht zu vermeiden, sind Führungskräfte und Beschäftigte in Bezug auf den sicheren Umgang mit Daten anzuweisen, zu unterweisen und für potenzielle Risiken zu sensibilisieren.
- Verbindliche Festlegung von Regeln für die Nutzung von smarten Anwendungen wie Cloud-Dienste, Messenger wie zum Beispiel WhatsApp besonders für Smartphones mit betrieblichen und privaten Daten. Dazu gehört auch die Schaffung klarer Regelungen für den Umgang mit betriebsübergreifenden Daten, wenn mehrere Partner miteinander kooperieren und Daten austauschen. › *Siehe Umsetzungshilfen 2.1.5 Beschaffung digitaler Produkte; 2.5.3 Plattformökonomie.*
- Bei Zulieferketten und mehreren Partnern reicht der Schutz des eigenen Unternehmens nicht aus. Auch die Partner müssen in Sicherheitsmaßnahmen und Richtlinien eingebunden werden. Es sollte beispielsweise mit Herstellern, Kunden, Lieferanten, Crowdworkern verbindlich und schriftlich vereinbart werden, wie mit den Daten umgegangen wird und welche Basisanforderungen an eine sichere und vertrauensvolle Kooperation gestellt werden. Hier kann zum Beispiel definiert werden, dass Daten aus Aufträgen oder Prozessen innerhalb des Netzwerkes sicher und ohne Zugriffe durch Unbefugte zwischen den beteiligten Unternehmen ausgetauscht werden können oder dass für den Aufbau und die Nutzung von Wertschöpfungsnetzwerken zuerst die Datenströme eindeutigen und sicheren Identitäten, zum Beispiel über IP-Adressen, zugeordnet werden.
- Die Maßnahmen zur Datensicherheit smarter Arbeitsmittel hängen oft von den Vorgaben des Herstellers ab, die dem Betrieb nicht immer bekannt sind. Diese sollten beim Hersteller oder Anbieter angefordert werden. › *Siehe Umsetzungshilfe 1.1.5 Kriterien zur Erklärbarkeit der 4.0-Technologien.*
- Verpflichtung für Beschaffer und Führungskräfte, bei der Anschaffung und beim Einsatz von intelligenter Software (inkl. KI) Kriterien der Datensicherheit zu berücksichtigen. › *Siehe Umsetzungshilfe 2.1.5 Beschaffung digitaler Produkte.*
- Einrichten eines Erkennungssystems für Angriffe (Unternehmen verschweigen oft Sicherheitspannen, um einen Imageschaden zu vermeiden). Den Führungskräften und Beschäftigten zu verstehen geben, dass Verstöße gegen vereinbarte Vorgehensweisen und Pannen sofort gemeldet werden müssen.

Beispiele für technische Maßnahmen

- Der Geltungsbereich sollte eingegrenzt werden: Welche smarten Geräte müssen hinsichtlich des Umgangs mit Daten überprüft werden?[23]
- Auswahl passender Kontrollmechanismen beim Umgang mit Daten (zum Beispiel Zutrittskontrolle, Zugangskontrolle – Datenzugriff erfolgt nur von berechtigten Personen, Zugriff durch Dritte auf die Daten der Beschäftigten ist reguliert).
- Die Daten, die durch smarte Geräte erzeugt und verwendet werden, sollten vor technischen Defekten geschützt sein (zum Beispiel Systemfehler oder Stromausfall). In Notsituationen muss intelligente Software (inkl. KI) autonom, das heißt ohne menschliche Unterstützung, in einen „sicheren Zustand“ gelangen können.
- Verwaltung der Benutzerkonten und Berechtigungen bei der Nutzung smar-

[22] Betreiber Kritischer Infrastrukturen, Betreiber öffentlicher Telekommunikationsnetze oder öffentlich zugänglicher Telekommunikationsdienste müssen einen Sicherheitsbeauftragten zur Datensicherheit benennen und ein Sicherheitskonzept erstellen.
[23] Alberts & Schildt 2018, S. 15

ter Arbeitsmittel auch über die Grenzen des eigenen Betriebes hinweg.
- Sicherstellung des Schutzes der Kommunikation zwischen vernetzten Systemen und der in diesen von vernetzten Geräten produzierten Daten, zum Beispiel durch „End-to-End-Verschlüsselung“ oder starke Authentifizierung.
- Regelmäßige Aktualisierung der intelligenten Software (inkl. KI), um jeweils aktuelle Schutzmaßnahmen gegenüber Schadsoftware zu nutzen. Dies sowie aktuelle Betriebssysteme und Sicherheitsupdates können beim Hersteller eingefordert werden.[24]
- Regelmäßige Analyse der Ist-Situation und bei Bedarf Umsetzung von Anpassungen und Verbesserungen. So kann erkannt werden, an welchen Stellen das Unternehmen Sicherheitsmaßnahmen ergreifen sollte, um diese Gefahren abzuwehren. Der Betrieb sorgt so für kontinuierliche Eigenkontrolle und Optimierung (ISO 27001).

Für die Datensicherheit bei der Nutzung eines Cloud-Dienstes sind darüber hinaus weitere Maßnahmen relevant. › *Siehe Umsetzungshilfe 2.5.1 Anforderungen an eine Cloud.*

[24] BMWi 2016

Quellen und weitere Informationsmöglichkeiten:

Alberts, K., & Schildt, H. (2018). Einstieg leicht gemacht. Basis-Absicherung nach IT-Grundschutz. In BSI (Hrsg.), *Mit Sicherheit* (S. 14–15). https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Magazin/BSI-Magazin_2018_01.pdf?__blob=publicationFile&v=8. Zugegriffen: 25.08.2018.

BMWi – Bundesministerium für Wirtschaft und Energie (2016). *IT-Security in der Industrie 4.0. Erste Schritte zu einer sicheren Produktion*. https://www.plattform-i40.de/I40/Redaktion/DE/Downloads/Publikation/wegweiser-it-security.pdf?__blob=publicationFile&v=16. Zugegriffen: 25.08.2018.

BSI – Bundesamt für Sicherheit in der Informationstechnik (2018). *Glossar der Cyber-Sicherheit*. https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/Empfehlungen/cyberglossar/cyberglossar_node.html. Zugegriffen: 30.11.2018.

BSI – Bundesamt für Sicherheit in der Informationstechnik (Hrsg.). (2016a). *Cyber-Sicherheit als Wettbewerbsvorteil in der Digitalisierung*. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Cyber-Sicherheit_als_Wettbewerbsvorteil.pdf?__blob=publicationFile&v=3. Zugegriffen: 25.08.2018.

BSI – Bundesamt für Sicherheit in der Informationstechnik (Hrsg.). (2016b). *Das IT-Sicherheitsgesetz. Kritische Infrastrukturen schützen*. Bonn: BSI.

BSI – Bundesamt für Sicherheit in der Informationstechnik (Hrsg.). (2016c). *Sichere Nutzung von Cloud-Diensten. Schritt für Schritt von der Strategie bis zum Vertragsende*. Bonn: BSI. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Sichere_Nutzung_Cloud_Dienste.pdf?__blob=publicationFile&v=8. Zugegriffen: 25.08.2018.

BSI – Bundesamt für Sicherheit in der Informationstechnik (Hrsg.). (2011). *Studie zur IT-Sicherheit in kleinen und mittleren Unternehmen*. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/KMU/Studie_IT-Sicherheit_KMU.pdf;jsessionid=1E49D3CE44F1A3FC61DC30334B5750DE.2_cid360?__blob=publicationFile&v=3. Zugegriffen: 25.08.2018.

datenschutz nord GmbH (2016). *Zertifizierte Informationssicherheit. ISO 27001 und andere Normen*. Bremen: datenschutz nord GmbH.

DSGVO – *Datenschutz-Grundverordnung*, 04.05.2016.

EuroCloud Deutschland – eco e. V. (2010). Leitfaden *Cloud Computing. Recht, Datenschutz & Compliance*. http://www.eurocloud.de/wp-content/blogs.dir/5/files/eurocloud-leitfaden_rdc.pdf. Zugegriffen: 25.08.2018.

Fallenbeck, N., & Eckert, C. (2015). IT-Sicherheit und Cloud Computing. In T. Bauernhansl, M. ten Hompel, & B. Vogel-Heuser, (Hrsg.), *Industrie 4.0 in Produktion, Automatisierung und Logistik* (S. 397–431). Wiesbaden: Springer Vieweg.

IT-Sicherheitsgesetz, 24.07.2015.

Röcher, D.-J. (2013). *Eine vernetzte Industrie ist anfälliger für Angriffe*. ComputerWoche 22.08.2013 https://www.computerwoche.de/a/eine-vernetzte-industrie-ist-anfaelliger-fuer-angriffe,2544607. Zugegriffen: 25.08.2018.

Schröter, W. (2015). *Fragen der IT-Sicherheit in der „Arbeitswelt 4.0“* E_05. Entscheidungshilfen Arbeit 4.0 der Offensive Mittelstand. https://www.offensive-mittelstand.de/fileadmin/user_upload/pdf/mittelstand_40/Entscheidungshilfe_05_0604.pdf. Zugegriffen: 25.08.2018.

Zu diesem Thema könnten Sie auch folgende weitere Umsetzungshilfen interessieren:

- 2.1.2 Integration von intelligenter Software (inkl. KI) in die Organisation
- 2.1.5 Beschaffung digitaler Produkte
- 2.1.8 Digital-Berater („Kümmerer“)
- 2.2.1 Risikobetrachtung von 4.0-Prozessen
- 2.3.2 Datenschutz in 4.0-Prozessen
- 2.3.3 Datenqualität in 4.0-Prozessen
- 2.3.5 Umgang mit Messengern und sozialen Medien
- 2.5.1 Anforderungen an eine Cloud
- 2.5.2 Cloud-Modelle der Bereitstellung und Dienstleistungen

Herausgeber: „Offensive Mittelstand – Gut für Deutschland“ – Stiftung „Mittelstand – Gesellschaft – Verantwortung“ Kurfürsten-Anlage 62, 69115 Heidelberg, E-Mail: info@offensive-mittelstand.de; Heidelberg 2019