2.2.3 Risikobetrachtung und IT-Sicherheit

Stichwörter: Risiken, vorausschauende Planung, kontinuierliche Verbesserung

› Warum ist das Thema wichtig?

Durch die Nutzung von 4.0-Technologien[1] und intelligenter Software[2] mit ihren Modellen der künstlichen Intelligenz (KI) gewinnen die Informationstechnologie und das Thema Risikobetrachtung der IT-Sicherheit im Unternehmen an Bedeutung. IT-Sicherheitsmaßnahmen zu diesen cyber-physischen Systemen (CPS)[3] sind nicht zwangsläufig mit hohen Investitionen in Sicherheitstechnik und der Beschäftigung von hoch qualifiziertem Personal verknüpft. Auch kleine und mittlere Unternehmen können mit leicht umsetzbaren Maßnahmen eine IT-Sicherheit im Unternehmen mittels einer Risikobetrachtung der 4.0-Technologien und der intelligenten Software (inkl. KI) realisieren.

In dieser Umsetzungshilfe werden die IT-Sicherheit sowie ihre Risiken betrachtet. Die allgemeinen Risiken (Chancen und Gefahren) der 4.0-Technologie und der intelligenten Software (inkl. KI) für den Betrieb sind Thema der Umsetzungshilfe 2.2.1 „Risikobetrachtung von 4.0-Prozessen". In der Umsetzungshilfe 2.2.2 „Gefährdungsbeurteilung 4.0" werden die Risiken der 4.0-Technologie und der intelligenten Software (inkl. KI) für das sichere und gesundheitsgerechte Arbeiten thematisiert.

› Worum geht es bei dem Thema?

Begriffe: IT und IT-Sicherheit

Informationssicherheit hat den Schutz von Informationen als Ziel. Dabei können Informationen sowohl auf Papier, in Technik und auch in der Software gespeichert und verarbeitet werden. Bei der Informationssicherheit geht es um den Schutz der Informationen, die erfasst, gespeichert und erarbeitet werden (siehe auch IT-Sicherheit). Der Begriff Informationssicherheit ist weitergehend als IT-Sicherheit.[4]

Informationstechnik (IT) umfasst alle technischen Mittel, die der Verarbeitung oder Übertragung von Informationen dienen (wie 4.0-Technologien, intelligente Software inkl. KI). Zur Verarbeitung von Informationen gehören Erhebung, Erfassung, Nutzung, Speicherung, Übermittlung, programmgesteuerte Verarbeitung, interne Darstellung und die Ausgabe von Informationen.[5]

IT-Sicherheit bezeichnet einen Zustand, in dem die Risiken für die Informationssicherheit, die beim Einsatz von Informationstechnik aufgrund von Bedrohungen und Schwachstellen vorhanden sind, durch angemessene Maßnahmen auf ein tragbares Maß reduziert sind. IT-Sicherheit ist also der Zustand, in dem Vertraulichkeit, Integrität und Verfügbarkeit von Informationen und Informationstechnik durch angemessene Maßnahmen geschützt sind.[6]

Neue Qualität der Informationssicherheit in 4.0-Prozessen

In dem Maße, wie die 4.0-Technologien und die intelligente Software (inkl. KI) sich in der Arbeitswelt etablieren, wächst die Bedeutung der Informationssicherheit auch für kleine und mittlere Unternehmen. Dies geschieht vor allem durch diese Entwicklungen:

- Der Einsatz von 4.0-Technologien und intelligenter Software (inkl. KI) kann die Informationssicherheit für einen Betrieb zunehmend beeinträchtigen, da die Menge der Daten (Big Data) und die Orte sowie die Art der Verarbeitung (Clouds, KI) nicht auf die Rechner im Betrieb beschränkt bleiben: Wenn Unternehmen intelligente Software (inkl. KI) nutzen, werden zum Beispiel Informationen und Daten digital gespeichert, elektronisch verarbeitet und im Rahmen von 4.0-Prozessen[7] und der Vernetzung smarter Arbeitsmittel in lokalen, globalen, privaten oder öffentlichen Netzen übermittelt und dort mit anderen Systemen vernetzt. Diese Daten und Informationen verlassen somit in der Regel die Grenzen des Betriebes.
- Mit der Nutzung von mehr und mehr smarten Anwendungen sowie mit dem

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] 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.

[2] 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.

[3] 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 Software 4.0 auf Grundlage von Modellen der künstlichen Intelligenz. Genutzt werden dazu unter anderem auch Sensoren/Aktoren, Verwaltungsschalen, Plattformen/Clouds.

[4] nach BSI 2013

[5] nach BSI 2013

[6] nach BSI 2013

[7] Unter 4.0-Prozessen werden hier alle Arbeitsprozesse verstanden, in denen cyber-physische Systeme (CPS) oder andere autonome technische Systeme (wie Plattformen, Messenger-Programme) beteiligt sind. 4.0-Prozesse sind in den Arbeitsprozessen bisher selten vollständig, aber in Ansätzen in allen Betrieben umgesetzt.

Rückgriff auf immer mehr externe Daten können neue Gefahren entstehen wie Geräteausfall, die Fehlsteuerung von Arbeitsmitteln oder Datenverlust. Beispielsweise kann auch eine Sicherheitslücke auf einer Systemkomponente, wie einem Tablet, in einer stark vernetzten Infrastruktur erhebliche Auswirkungen auf die Sicherheit des Gesamtsystems haben. Bei der Nutzung smarter Arbeitsmittel, wie Maschinen oder autonom fahrende Fahrzeuge, kann sich diese beeinträchtigte Informationssicherheit auch auf die Sicherheit der Nutzer auswirken. Nur wenn die verwendeten Technologien, Daten und Softwareprogramme sicher und die Informationen, die verarbeitet werden, verlässlich sind, können die Potenziale der 4.0-Technologien und der intelligenten Software (inkl. KI) genutzt werden.

- Die 4.0-Technologien und intelligente Software (inkl. KI) entwickeln sich aufgrund von Updates und selbstlernenden Systemen kontinuierlich weiter. Daher verändert sich der Stand der Informationssicherheit auch kontinuierlich.

Wie soll nun ein kleiner und mittlerer Betrieb mit dieser Problematik umgehen? Informationssicherheit ist eine Aufgabe der Führung. Die Führungskräfte sollten bei Planungen zur Integration der 4.0-Technologien und der intelligenten Software (inkl. KI) immer auch die Frage der Informationssicherheit mitdenken und die damit verbundenen Risiken (Chancen und Gefahren) identifizieren und bewerten.

Fragen der Informationssicherheit sind für Führungskräfte häufig keine originäre Aufgabe. Zielführend ist es daher, schon bei den ersten Überlegungen zu den 4.0-Technologien und der intelligenten Software (inkl. KI) fachliche Expertise zur Informationssicherheit hinzuziehen. Dies kann der eigene Digital-Mentor sein › *siehe Umsetzungshilfe 2.1.8 Digital-Mentor („Kümmerer“)*, der Datenschutzbeauftragte oder ein unabhängiger externer IT-Experte (zum Beispiel ein IT-Berater einer Kammer oder eines Verbandes).[8]

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat für fast alle IT-Sicherheitsprobleme Grundsätze und Standards entwickelt, die Experten und IT-Beratern helfen, IT-Sicherheit herzustellen und die Risiken der Informationssicherheit zu erkennen.[9] Diese Informationen sind meist sehr umfangreich, bieten aber grundsätzlich eine Orientierung mit konkreten Inhalten. Auf deren Grundlage sollten IT-Experten den Betrieb beraten.

Risikobetrachtung der IT-Sicherheit

Grundlegende Mängel der IT-Sicherheit bestehen in folgenden Aspekten:[10]

- *Verlust der Verfügbarkeit*: Wenn grundlegende Informationen eingeschränkt zur Verfügung stehen oder ganz fehlen, werden die betrieblichen Prozesse gestört oder können gar nicht stattfinden.
- *Verlust der Vertraulichkeit von Informationen*: Mit personenbezogenen Daten muss vertraulich umgegangen werden. Das heißt, dass diese Daten im Rahmen der gesetzlichen Regelungen geschützt werden müssen. Die ungewollte Offenlegung von Informationen kann in vielen Bereichen schwere Schäden nach sich ziehen.
- *Verlust der Integrität (Korrektheit von Informationen)*: Gefälschte oder verfälschte Daten oder Daten in nicht ausreichender Qualität › *siehe Umsetzungshilfe 2.3.3 Datenqualität in 4.0-Prozessen* können beispielsweise zu Störungen in Prozessen, Fehlbuchungen, falschen Lieferungen oder fehlerhaften Produkten führen. Auch können personenbezogene Daten verwechselt oder falsch zugeordnet werden (Verlust der Authentizität) oder beispielsweise Zahlungsanweisungen oder Bestellungen zu Lasten einer dritten Person verarbeitet werden.

Ursachen für diese Mängel der Informationssicherheit sind technisch, organisatorisch und/oder in Personen begründet. Die entsprechenden Rahmenbedingungen sollten bei der Risikobetrachtung einbezogen werden. Im Folgenden werden für diese Rahmenbedingungen einige Beispiel aufgeführt:

Technische Rahmenbedingungen, zum Beispiel:

- Funktion der Sicherheitseinrichtungen
- Prozesse und Formen der Löschung von Daten
- Art der Internetverbindung
- Art der Verbindung zu anderen Netzen
- Ausfall oder Störung von Kommunikationsnetzen
- Art und Form der Back-ups
- Kompatibilität der unterschiedlichen Systeme, Programme und Komponenten
- Art des Zugriffs auf die Datenbestände und Art der Identifizierung der Benutzer
- Zugriff auf sensible betriebsinterne Daten
- Möglichkeiten der Ausbreitung von Schadsoftware
- Technische Datensicherung beim Cloud-Dienstleister und anderen verbundenen Netzwerken
- Art der Installation und Funktionen von Sicherheitsgateway (Firewall)
- Fehlfunktion von Arbeitsmitteln, Geräten oder Systemen
- Sensorik und Funktion von Arbeitsmitteln

Organisatorische Rahmenbedingungen, zum Beispiel:[11]

- Organisation und Art der Wartung der Soft- und Hardware
- Abstimmung und Planung mit IT-Experten
- Festlegung der Verantwortlichkeiten
- Regelungen zum Umgang mit der 4.0-Technologie und der intelligenten Software (inkl. KI)
- Nutzer-Anweisungen zum Umgang mit eventuell auftretender Schadsoftware
- Zutrittsregelungen in schutzbedürftige Räume
- Weitergabe von Passwörtern oder Zugangscodes, zum Beispiel für Daten auf einer Cloud
- Überprüfung der Abhängigkeit von Anwendungen, zum Beispiel Datenformat, technischer Support
- Gefährdungsbeurteilung der gesundheitlichen Belastungen und Gefährdungen bei der Nutzung von 4.0-Technologie und der intelligenten Software (inkl. KI)
- Verstöße gegen Gesetze, Vorschriften oder Verträge, wie zum Beispiel Beeinträchtigung des informationellen Selbstbestimmungsrechts und der Beeinträchtigung der persönlichen Unversehrtheit

[8] siehe u. a.: BSI-Standard 100-1; BSI-Standard 100-2; BSI-Standard 100-3; BSI 2016a; DIN EN ISO/IEC 27000:2017-10; DIN EN ISO/IEC 27001:2017-06 und andere Normen aus der 27000-Reihe

[9] siehe: www.bsi.bund.de/DE/Themen/ITGrundschutz/itgrundschutz_node.html

[10] Die Gefährdungskataloge des BSI bilden ein wichtiges Fundament für die Anwendung der IT-Grundschutz-Vorgehensweise (BSI-Standard 100-2) und der Risikoanalyse auf der Basis von IT-Grundschutz (BSI-Standard 100-3). BSI 2016a, S. 69f.

[11] BSI 2016a

- Notfallmanagement für den Ausfall des Systems und die Nichtverfügbarkeit von Anwendungen

Personelle Rahmenbedingungen, zum Beispiel:

- Kompetenzen der Führungskräfte und Beschäftigten im Umgang mit 4.0-Technologie und der intelligenten Software (inkl. KI)
- Kenntnis über Kriterien zur Einschätzung der Vor- und Nachteile der 4.0-Technologie und der intelligenten Software (inkl. KI)
- Kenntnis über Regelungen im Betrieb zum Umgang mit 4.0-Technologie und der intelligenten Software (inkl. KI)
- Bewusstsein zum Umgang mit Risiken der 4.0-Technologie und der intelligenten Software (inkl. KI)
- Sensibilisierung zu möglichen Mängeln und deren Auswirkungen auf den Betrieb
- Sensibilisierung und Information Dritter (andere Gewerke, Kunden) beim Umgang mit der 4.0-Technologie und der intelligenten Software (inkl. KI)

Durch diese Rahmenbedingungen können Mängel und Sicherheitslücken verursacht werden. Daher sind Maßnahmen im Rahmen der Risikobetrachtung nach folgenden Schritten[12] zu ermitteln und umzusetzen: › *Siehe Umsetzungshilfe 2.2.1 Risikobetrachtung von 4.0-Prozessen*

1. Identifizieren des Zustands der IT-Sicherheit
2. Analyse der erkannten Mängel und Sicherheitslücken
3. Beurteilung und Bewertung der erkannten Risiken
4. Festlegen und Umsetzen von Maßnahmen sowie
5. Wirksamkeitskontrolle

› Welche Chancen und Gefahren gibt es?

Eine vorausschauende und systematische Risikobetrachtung der Informationssicherheit von 4.0-Technologien und intelligenter Software (inkl. KI) bringt zahlreiche **Chancen**. Diese können unter anderem sein:[13]

- Der Schutz vor unerwünschten Effekten wie Verlust von Daten, Sabotage oder falschen Funktionsweisen der 4.0-Technologie.
- Die benötigten Daten sind immer verfügbar und es kommt nicht zu Datenausfällen und Störungen.
- Die Datenqualität ist gegeben. Die Führungskräfte und die Beschäftigten können den Informationen vertrauen und die Informationen sind korrekt.
- Führungskräfte und Beschäftigte können sicher sein, dass mit ihren personenbezogenen Daten vertraulich umgegangen wird.
- Nachgewiesene Informationssicherheit schafft Vertrauen bei Kunden und anderen Geschäftspartnern und wird zunehmend von diesen auch eingefordert.
- Die Wartungsarbeiten an IT-Systemen erfordern deutlich weniger Zeit.
- IT-Verantwortliche/Administratoren arbeiten effektiver.
- Die Akzeptanz und die Expertise von Führungskräften und Beschäftigten steigen, weil sie die Sicherheitssysteme kennen (Transparenz) und adäquat auf den Ernstfall vorbereitet sind.

Folgende **Gefahren** können bei einer nicht systematischen oder versäumten Risikobetrachtung der Informationssicherheit von 4.0-Technologien und intelligenter Software (inkl. KI) unter anderem auftreten:[14]

- Zugriff von außen auf sensible Daten – Verlust von Daten, Sabotage oder falsche Funktionsweisen der 4.0-Technologie.
- Verlust der Verfügbarkeit von Daten und Informationen und dadurch Störung oder Stilllegung von Arbeits- und Produktionsprozessen.
- Verlust von Betriebssicherheit zum Beispiel durch Geräteausfall, die Verbreitung von Schäden auf sämtlichen Arbeitsmitteln.
- In vernetzten Infrastrukturen kann die Sicherheitspanne einer Komponente grundlegende Auswirkungen auf die Sicherheit des Gesamtsystems haben.
- Die Störung der Systemsicherheit smarter Arbeitsmittel wie Maschinen oder autonom fahrender Fahrzeuge kann die Sicherheit der Nutzer beeinträchtigen.
- Missbrauch personenbezogener Daten von Beschäftigten, Führungskräften, Kunden oder Lieferanten kann zu einem Vertrauensverlust führen.
- Verlust der Integrität (Korrektheit von Informationen) – Nutzung gefälschter oder verfälschter Daten kann zu Gefahren im Arbeitsprozess, zu falschen Lieferungen oder fehlerhaften Produkten führen.

› Welche Maßnahmen sind zu empfehlen?

Allgemeine Maßnahmen zur IT-Informationssicherheit

Um die Risiken für die Informationssicherheit von 4.0-Technologien und von intelligenter Software (inkl. KI) zuverlässig einzuschätzen und zu bewerten, sollten in kleinen und mittleren Betrieben zunächst unter anderem folgende Maßnahmen festgelegt werden:[15]

- Die Führungskräfte sollten definieren, welche Anforderungen sie an die IT-Sicherheit der geplanten 4.0-Technologien und der intelligenten Software (inkl. KI) stellen. Aufbauend darauf sollten die Führungskräfte ein Sicherheitskonzept für die Informationssicherheit von 4.0-Technologien und der intelligenten Software (inkl. KI) im Betrieb erstellen. Hierbei sollten die Führungskräfte die allgemeinen Anforderungen an die Datensicherheit zugrunde legen. › *Siehe Umsetzungshilfe 2.3.1 Datensicherheit in 4.0-Prozessen*. Zusätzlich sollten sie auf die Grundsätze und Standards des Bundesamtes für Sicherheit in der Informationstechnik (BSI) sowie auf die entsprechenden DIN-Normen verweisen.[16] Im Sicherheitskonzept sollten zum Beispiel die folgenden grundlegenden Aspekte beschrieben werden:

[12] BSI-Standard 100-1, S. 28f.
[13] vgl. u. a. BSI 2012; Tauss 2017
[14] BSI 2018a
[15] KAS-44 2017
[16] vgl. u. a. BSI-Standard 100-1; BSI-Standard 100-2; BSI-Standard 100-3; BSI 2016a; DIN EN ISO/IEC 27000:2017-10; DIN EN ISO/IEC 27001:2017-06 und andere Normen aus der 27000-Reihe

  - Grundwerte der Informationssicherheit (Vertraulichkeit, Integrität, Verfügbarkeit)
  - Sicherheitsziele, eine angemessene Sicherheitsstrategie und Erfolgsfaktoren (wie Verlässlichkeit des Handelns, Sicherung der materiellen Werte, Schutz von betrieblichem Wissen, Sicherung der Qualität der Informationen, Sicherstellung der Arbeitsabläufe, Sicherheit, Gesundheit und Umweltschutz bei der Arbeit, Rechtskonformität, Schadensvermeidung und Schadensverhütung)
  - Steuerung des Sicherheitsprozesses durch die verantwortliche Führungskraft
  - Grundlegende Sicherheitsmaßnahmen, Maßnahmen zur Pflege und zum Verbesserungsprozess[17]
- Eine Führungskraft sollte als Verantwortlicher für die IT-Sicherheit benannt werden. Diese Führungskraft sollte sich vom internen Digital-Mentor *› siehe Umsetzungshilfe 2.1.8 Digital-Mentor („Kümmerer")*, dem Administrator, dem Datenschutzbeauftragten oder einem unabhängigen IT-Experten (zum Beispiel IT-Berater der Kammer oder eines Verbandes) unterstützen lassen.
- Die Führungskräfte sollten darauf achten, dass die Informationssicherheit der 4.0-Technologien und der intelligenten Software (inkl. KI) durch Maßnahmen auf folgenden Ebenen ermöglicht wird:[18]
  - Sicherheit der Infrastruktur (wie zum Beispiel Schutz der Gebäude, Räume, Serverräume vor Angriffen und natürlichen Gefahren – wie Feuer, Wasser, ungünstigen klimatischen Bedingungen, Naturkatastrophen)
  - Sicherheit der IT-Systeme (wie zum Beispiel Server, Clients, Netzkomponenten)
  - Sicherheit im Netz (wie zum Beispiel sichere Verbindungen und Übergänge zu anderen Netzen, Plattformen und Systemen)
  - Sicherheit in Anwendungen (wie zum Beispiel Umgang mit intelligenter Software (inkl. KI), Arten der Intervention, Angaben von Handlungsträgerschaft, Sicherung des E-Mail-Verkehrs)
- Alle Beschäftigten und Führungskräfte sollten über die Maßnahmen zur Informationssicherheit informiert und gegebenenfalls qualifiziert werden. Jeder Einzelne kann durch verantwortungs- und qualitätsbewusstes Handeln helfen, Schäden zu vermeiden, und zum Erfolg beitragen.[19]
- Die Führungskräfte sollten ein Arbeitsklima mit gemeinsamen Wertvorstellungen fördern, in dem sich das Risikobewusstsein zur Informationssicherheit möglichst selbstverständlich im Alltagshandeln entwickeln kann[20] (zum Beispiel dadurch, dass Informationssicherheit zum regelmäßigen Thema in Teambesprechungen wird, dass Verbesserungsvorschläge der Beschäftigten zur IT-Sicherheit aktiv eingefordert werden oder durch Förderung einer aktivierenden Fehlerkultur).

Maßnahmen zur Risikobetrachtung der IT-Informationssicherheit

Bei der **Risikoidentifikation und -analyse** der Informationssicherheit der geplanten 4.0-Technologien und der intelligenten Software (inkl. KI) sollten unter anderem folgende Fragen untersucht werden:

Technische Rahmenbedingungen – Beispiele:

- Wie sicher sind die eingesetzte 4.0-Technologie und die intelligente Software (inkl. KI)? (zum Beispiel Schutz bei Ausfall oder Störung von Versorgungsnetzen, vor unbefugtem Eindringen in IT-Systeme, gegen Schadsoftware, bei Integritätsverlust schützenswerter Informationen, bei Fehlfunktion von Geräten oder Systemen)
- Ist eine Anbindung der geplanten 4.0-Technologien und der intelligenten Software (inkl. KI) an bestehende Datensicherheitssysteme möglich? (zum Beispiel durch die eingesetzten Protokolle und Schnittstellen)
- Mit welchen weiteren technischen Netzwerken sind die geplanten 4.0-Technologien und die intelligente Software (inkl. KI) verbunden beziehungsweise welche Akteure/Programme greifen dort auf Daten zurück? Wie sind diese Netzwerke technisch gesichert?
- Erfolgen die Software-Updates so, dass die bestehenden Anwendungen (wie Programme, Technologien, smarte Arbeitsmittel) weiter funktionieren und die vorhandenen Daten nicht unbemerkt verändert werden?
- Sind bestimmte Geräte, Anlagen und Netze mit ähnlichem Schutzbedarf zu trennen (segmentieren), um Angriffe zu erschweren? Kann in diesen Fällen die Kommunikation zwischen den Zonen trotz Trennung stattfinden, weil die Übergänge klar definiert und entsprechend abgesichert sind?[21]
- Ist sichergestellt, dass die verwendete 4.0-Technologie und die intelligente Software (inkl. KI) nicht von sich aus ungeplant eine Verbindung nach außen (in das Internet) herstellen?[22]
- Wie sicher sind die Netzverbindungen zwischen den beteiligten Netzwerken und Systemen (wie zum Beispiel WLANs, Backbone-Techniken) und wie sicher sind die Verbindungen des betrachteten Bereichs nach außen (wie Einwahl-Zugänge, Internet-Anbindungen, Plattformen)?
- Sind Eingriffe und Manipulation durch Cyberkriminelle verhindert, die eine mittelbare oder unmittelbare Auswirkung auf die funktionale Sicherheit von Anlagen und autonomen technischen Systemen haben? (zum Beispiel auf sicherheitsrelevante Komponenten, Bauteile, Software; alle Netzwerk-Ein- und Ausgangspunkte zu anderen Netzwerken; alle IT-Systeme außerhalb des Produktionsbereiches, von denen eine Kommunikationsbeziehung in den Betrieb aufgebaut werden kann; alle sicherheitsrelevante Dokumentationen)

Organisatorische Rahmenbedingungen – Beispiele:

- Sind die Informationen über die geplanten 4.0-Technologien und die intelligente Software (inkl. KI) ausreichend, um Aussagen über mögliche Risiken zu liefern (sonst werden Risiken nicht oder zu spät erkannt oder es werden Risiken vermutet, wo gar keine bestehen)? Hier kann es sinnvoll sein,

[17] BSI-Standard 100-1, S. 27ff.; BSI-Standard 100-2, S. 18ff.
[18] BSI-Standard 100-1, S. 37. Zu diesen Themen gibt es in den BSI-Grundsätzen umfassende Gestaltungshinweise – siehe BSI 2016a.
[19] BSI-Standard 100-1, S. 23
[20] BSI-Standard 100-1, S. 23
[21] BMWi 2016c, S. 20ff.
[22] BMWi 2016c, S. 37

weitere Informationen vom Hersteller/Anbieter einzufordern.
- Entstehen durch die geplanten 4.0-Technologien und die intelligente Software (inkl. KI) Abhängigkeiten von Anwendungen der Anbieter? (wie zum Beispiel Lizenzen, Updates, Softwarestandards)
- Sind vertrauliche Dokumente oder Dateien als „vertraulich" gekennzeichnet, sodass diese Informationen nicht versehentlich an Unbefugte weitergegeben werden?
- Wie kann sichergestellt werden, dass die Identität der Benutzer eindeutig definiert ist, und wie wird verhindert, dass ein Angreifer die Identität annehmen kann?[23] (Berechtigungsmanagement)
- Wie wird verhindert, dass unberechtigte Personen Veränderungen an autonomen technischen Systemen und Steuerungskomponenten vornehmen können? (zum Beispiel durch abschließbare Bedienungspanel, durch physische Separation von Bediener- und Administrator-Funktionen oder durch Funktionsfreischaltung unter der Verwendung von Funk-Chips [RFID])[24]
- Ist die Dokumentation der Datenflüsse und der Abläufe sowie der Handlungsträgerschaft der intelligenten Software (inkl. KI) sichergestellt?[25]
- Ist eine Gefährdungsbeurteilung zu gesundheitlichen Belastungen und Gefährdungen bei Sicherstellung der Informationssicherheit von 4.0-Technologie und der intelligenten Software (inkl. KI) erforderlich? (wenn ja, diese in der Phase der Risikoidentifizierung durchführen und entsprechende Maßnahmen festlegen und umsetzen)
- Welche Notfallvorkehrungen sind zu treffen, um im Gefährdungsfall schnell reagieren zu können?

Personelle Rahmenbedingungen – Beispiele
- Wie können die Führungskräfte und die Beschäftigten für die Wahrnehmung möglicher Risiken sensibilisiert werden?
- Welche Kompetenzen benötigen die Führungskräfte und die Beschäftigten für die Umsetzung der Informationssicherheit der 4.0-Technologie und der intelligenten Software (inkl. KI)?
- Wie kann allen Personen bekannt werden, welche Risiken bei der geplanten 4.0-Technologie und der intelligenten Software (inkl. KI) auftreten können (wie beim versehentlichen Löschen von Daten in der Cloud) und welche Verhaltensweisen getroffen werden müssen?

Bei der **Risikobewertung** der Informationssicherheit durch 4.0-Technologien und intelligente Software (inkl. KI) sollten folgende Kriterien berücksichtigt werden:[26]
- Beeinträchtigung der verlässlichen Information und Kommunikation (auch zwischen den beteiligten Netzen, Plattformen und Systemen)
- Beeinträchtigung der Aufgabenerfüllung
- Beeinträchtigung des informationellen Selbstbestimmungsrechts (Datenschutz)
- Beeinträchtigung der Sicherheit und Gesundheit bei der Arbeit und des Umweltschutzes
- Negative Innen- oder Außenwirkungen
- Verstoß gegen Gesetze/Vorschriften/Verträge
- Finanzielle Auswirkungen

Maßnahmen aus der Risikobewertung

Technische Rahmenbedingungen – Beispiele:[27]
- Sicherstellung der Kompatibilität der intelligenten Software (inkl. KI) zu den bestehenden Systemen
- Anbindung der geplanten 4.0-Technologien und intelligenten Software (inkl. KI) an bestehende Datensicherheitssysteme
- Einrichten von Zugangsbeschränkungen
- Sichere Identifizierung der Benutzer und Zugriffsschutz entsprechend den Zugriffsberechtigungen
- Verschlüsselung von sensiblen Daten
- Schutz bei Ausfall oder Störung von Versorgungsnetzen
- Trennung von Netzwerken mit lebenserhaltenden Funktionen von anderen IT-Komponenten zur Minimierung des Ausfallrisikos bei Störung eines anderen Subsystems
- Sichtbarmachung der Handlungsträgerschaft der intelligenten Software (inkl. KI) und Festlegen von Interventionsmöglichkeiten
- Verhinderung, dass die intelligente Software (inkl. KI) von sich aus ungeplant eine Verbindung nach außen (in das Internet) herstellen kann
- Technische Datensicherung in verbundenen Netzwerken, Systemen und Plattformen,[28] Schutz vor (auch unbeabsichtigter) Datenlöschung auch von mobilen Geräten oder in Clouds
- Schutz personenbezogener Daten
- Sicherheitsgateway (Firewall) – Schutz des vertrauenswürdigen (internen) Netzes gegen unbefugten Zugriff und Schadsoftware
- Sicherstellung der Aktualisierungen von Daten ohne Datenverluste, Störungen und neue Zugriffsmöglichkeiten

Organisatorische Rahmenbedingungen – Beispiele:
- Überprüfen, ob die festgelegten Maßnahmen zueinander passen und sich nicht konterkarieren.
- Schutz der Daten vor Datenverlust oder Missbrauch anhand von vertraglichen Vereinbarungen mit dem Hersteller/Anbieter von Cloud-Diensten oder IT-Dienstleistern sicherstellen.
- Eine Arbeitsanweisung erstellen, wie mit der geplanten 4.0-Technologie und der intelligenten Software (inkl. KI) informationssicher umzugehen ist (hier unter anderem Zutrittsregelungen, Vergabe von Zutrittsberechtigungen, Zugangscodes, Passwortgebrauch, Umgang mit Schadsoftware, Verhalten im Notfall). Die Arbeitsanweisung im Betrieb zur Verfügung stellen. Dabei auch sicherstellen, dass die Benutzer die festgelegten Maßnahmen nicht umgehen können.
- Rechtzeitige Beteiligung der Beschäftigten, um deren Erfahrungen berücksichtigen zu können (falls vorhanden auch den Betriebsrat einbinden).[29]
- Wartung der Soft- und Hardware organisieren.

[23] BMWi 2016c, S. 25ff.
[24] BMWi 2016c, S. 35
[25] BMWi 2016c, S. 38
[26] BSI-Standard200-2, S. 50ff.
[27] BSI 2016b
[28] Bei diesem Schritt kann zum Beispiel über die Einführung eines Informationssicherheitsmanagementsystems (wie ISO 27001 oder BSI IT-Grundschutz) reflektiert werden.
[29] Bei allen Maßnahmen, die prinzipiell die Verhaltens- oder Leistungsüberwachung von Beschäftigten ermöglichen, zum Beispiel Protokollierung, bedarf es der Mitbestimmung der Personalvertretung. Grundlage dessen sind in Deutschland die Betriebsverfassungs- und Personalvertretungsgesetze von Bund und Ländern. BSI 2014.

- Liste der vernetzten und nicht vernetzten IT-Systeme erstellen beziehungsweise aktualisieren und vervollständigen.
- Grafische Darstellung des Netzes und seiner Verbindungen erstellen (Netzpläne).
- Notfallmanagement für den Ausfall des Systems und der Nichtverfügbarkeit von Anwendungen festlegen. Dabei auch einfache, konkrete Handlungsanweisungen und Maßnahmenpläne für den Schadensfall erstellen.[30]
- Sicherstellen, dass mögliche Bedienungs- und Betriebsfehler die festgelegten Maßnahmen nicht aushebeln können.

Personelle Rahmenbedingungen – Beispiele:

- Sicherstellen, dass die Führungskräfte und die Beschäftigten die erforderlichen Kompetenzen im Umgang mit den Maßnahmen zur Informationssicherheit der 4.0-Technologien und der intelligenten Software (inkl. KI) besitzen – gegebenenfalls qualifizieren.
- Führungskräften und Beschäftigten die Anweisungen im sicheren und gesundheitsgerechten Anwenden der Maßnahmen zur Informationssicherheit der 4.0-Technologien und der intelligenten Software (inkl. KI) übergeben und diese erklären. Dabei auch die Handlungsanweisungen und Maßnahmenpläne für den Schadensfall aushändigen und erklären.[31] Führungskräfte und Beschäftigte entsprechend einweisen und unterweisen. Hierbei auch das Sicherheitskonzept generell vorstellen und erklären.
- Neuen Beschäftigten die Arbeitsanweisungen zur IT-Informationssicherheit vorstellen und sie befähigen, die Anweisungen umzusetzen.[32]

Die hier dargestellten Hinweise und Maßnahmen zur Informationssicherheit von 4.0-Technologien und intelligenter Software (inkl. KI) sind Beispiele, die Führungskräften in kleinen und mittleren Unternehmen den Rahmen der Maßnahmen bei der Risikobetrachtung verdeutlichen und eine ganz grundlegende Orientierung bieten sollen. Sie ersetzen keine systematische, auf den konkreten Betrieb zugeschnittene Risikobetrachtung, bei der IT-Experten, Administratoren oder IT-Berater der Kammern und Verbände hinzugezogen werden sollten.

Quellen und weitere Informationsmöglichkeiten:

BMWi (Hrsg.), (2016a). *„Technischer Überblick: Sichere unternehmensübergreifende Kommunikation“*, Ergebnispapier der Plattform Industrie 4.0. https://www.plattform-i40.de/I40/Redaktion/DE/Downloads/Publikation/sichere-unternehmensuebergreifende-kommunikation.pdf?__blob=publicationFile&v=8. Zugegriffen: 10.10.2018.

BMWi (2016b). *IT-Sicherheit für die Industrie 4.0*, Abschlussbericht. Berlin: Bundesministerium für Wirtschaft und Energie (BMWi).

BMWi (2016c). *IT-Security in der Industrie 4.0 – Handlungsfelder für Betreiber*. Berlin: Bundesministerium für Wirtschaft und Energie (BMWi).

BSI (2012). *Leitfaden Informationssicherheit – IT-Grundschutz kompakt*. Bonn: Bundesamt für Sicherheit in der Informationstechnik (BSI).

BSI (2013). *IT-Grundschutz Glossar*. https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/Glossar/glossar_node.html. Zugegriffen: 26.10.2018.

BSI (2016a). *IT-Grundschutz-Kataloge:* 15. EL Stand 2016, Bonn: Bundesamt für Sicherheit in der Informationstechnik (BSI), https://download.gsb.bund.de/BSI/ITGSK/IT-Grundschutz-Kataloge_2016_EL15_DE.pdf. Zugegriffen: 26.10.2018.

BSI (2018). *Checklisten zum IT-Grundschutz-Kompendium*, Bonn: Bundesamt für Sicherheit in der Informationstechnik (BSI). https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/checklisten.html. Zugegriffen: 26.10.2018.

BSI-Standard 100-1: *Managementsysteme für Informationssicherheit (ISMS)*, Bonn: Bundesamt für Sicherheit in der Informationstechnik (BSI). https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzStandards/ITGrundschutzStandards100/Standard01/ITGStandard01_node.html. Zugegriffen: 10.10.2018.

BSI-Standard 100-2: *IT-Grundschutz-Vorgehensweise*, Bonn: Bundesamt für Sicherheit in der Informationstechnik (BSI). https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzStandards/Standard202/ITGStandard202_node.html. Zugegriffen: 26.10.2018.

BSI-Standard 100-3: *Risikoanalyse auf der Basis von IT-Grundschutz*, Bonn: Bundesamt für Sicherheit in der Informationstechnik (BSI). https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzStandards/ITGrundschutzStandards100/Standard03/ITGStandard03_node.html. Zugegriffen: 10.10.2018.

DIN EN ISO/IEC 27000:2017-10. *Informationstechnik – Sicherheitsverfahren – Informationssicherheits-Managementsysteme – Überblick und Terminologie*. Berlin: Beuth Verlag.

DIN EN ISO/IEC 27001:2017-06. *Informationstechnik – Sicherheitsverfahren – Informationssicherheitsmanagementsysteme – Anforderungen*. Berlin: Beuth Verlag.

KAS-44 (2017). *Leitsätze der Kommission für Anlagensicherheit zum Schutz vor cyberphysischen Angriffen*. Bonn: GFI Umwelt – Gesellschaft für Infrastruktur und Umwelt mbH.

Strametz, R. (2018). *Digitalisierung und Risikomanagement – APS-Handlungsempfehlung für Behandler – APS-Jahrestagung 2018 – Digitalisierung und Patientensicherheit*. http://www.aps-ev.de/wp-content/uploads/2018/05/KP-02_Strametz.pdf. Zugegriffen: 04.02.2018.

Tauss, C. (2017). *Digitalisierung braucht Risikomanagement*. https://www.pm-blog.eu/themen/prozesse/digitalisierung-braucht-risikomanagement.html. Zugegriffen: 04.02.2018.

[30] Strametz 2018
[31] Strametz 2018
[32] Strametz 2018

Zu diesem Thema könnten Sie auch folgende weitere Umsetzungshilfen interessieren:

- 1.3.3 Handlungsträgerschaft im Verhältnis Mensch und intelligente Software (inkl. KI)
- 2.1.8 Digital-Mentor („Kümmerer“)
- 2.3.1 Datensicherheit in 4.0-Prozessen
- 2.3.2 Datenschutz in 4.0-Prozessen
- 2.3.3 Datenqualität in 4.0-Prozessen
- 3.2.1 Technische Assistenzsysteme – allgemein
- 3.2.2 Smartphone, -watch, -glasses
- 3.2.6 Augmented Reality – Virtual Reality (künstliche Welten)

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