Safety und Security bei Mittelstand-Digital: Sicherheit in kleinen und mittleren Unternehmen

Die zunehmende Digitalisierung und Vernetzung von Maschinen, Unternehmensprozessen und Unternehmen erfordert ein immer größeres Maß an Sicherheit. Denn IT-Systeme müssen stets verfügbar und die Vertraulichkeit und Integrität der übertragenen Daten und Informationen gewährleistet sein. Im Rahmen der Initiative „Mittelstand-Digital“ des Bundesministeriums für Wirtschaft und Energie wurden daher Mittelstand 4.0-Kompetenzzentren geschaffen. Diese sensibilisieren und informieren kleine und mittlere Unternehmen zu den Herausforderungen und Fragen der Sicherheit im Unternehmen in Zeiten der Industrie 4.0. Auch die Plattform Industrie 4.0 bietet zahlreiche Handlungsempfehlungen und Leitfäden.

Herausforderungen der künftigen Netzwerkökonomie

Mit der schrittweisen Verwirklichung von Industrie 4.0-Anwendungen verändern sich grundlegend die Anforderungen an den sicheren Ablauf von Prozessen in der Produktion und im Dienstleistungssektor. Verlässlichkeit und jederzeitige Verfügbarkeit werden zum essenziellen Strukturmerkmal der kommenden Netzwerkökonomie. Die Vision der digitalen Transformation basiert darauf, dass bislang meist noch isoliert ablaufende Prozesse der Wertschöpfung, einschließlich aller vor- und nachgelagerten Servicetätigkeiten in den Unternehmen, sich künftig in ein Ensemble flexibler Wertschöpfungsnetzwerke verwandeln werden.

So ist beispielsweise denkbar, dass Unternehmen mit Unterauslastung ihre freien Fertigungskapazitäten im Rahmen einer auftragsgesteuerten Produktion sporadisch oder dauerhaft über eine Internetplattform anbieten, um so ihre Produktivität und ihren Umsatz zu erhöhen. Je mehr Betriebe sich an einer derartigen Form kooperativer Wertschöpfung beteiligen, umso mehr entstehen Produktionsverbünde, die unterschiedlichste Produkte und Dienstleistungen in nahezu beliebiger Menge und mit hoher Qualität zeitnah erzeugen und „on demand“ zuliefern können.

Produktionsnetzwerke ermöglichen aber nicht nur neue Formen einer bisher nicht gekannten Tiefe der Arbeitsteilung, sondern sie schaffen durch die umfassende horizontale und vertikale Vernetzung ihrer Abläufe auch ganz neue Abhängigkeiten und Risiken. Die Partner eines Netzwerks müssen sich jederzeit darauf verlassen können, dass die zugesagten oder eingekauften Leistungen genau so erbracht werden, wie sie in Bezug auf Form, Qualität und Zeit vereinbart wurden, und dass diese Prozesse störungsfrei ablaufen. Eine Voraussetzung hierfür ist die Sicherheit von Prozessen, wobei Sicherheit in der Industrie eine andere Bedeutung hat als in der IT-Wirtschaft. Sicherheit hat zwei Dimensionen. Die erste Dimension der Sicherheit wird mit dem Fachterminus Safety bezeichnet. Darunter wird die Sicherung eines Bedieners, eines Herstellungsprozesses oder der Produktionsumgebung verstanden. Eine Produktionsanlage gilt dann als sicher im Sinne von „Safety“, wenn für die Mitarbeiter eines Betriebes Risiken für Leib und Leben nach bestehenden Sicherheitsstandards als ausgeschlossen gelten können. Die zweite Dimension der Sicherheit nennt sich Security. Sie bezeichnet die Sicherheit von Produktionsanlagen und der dazugehörigen Infrastruktur. Sie beinhaltet unter anderem, dass Daten, die für die Herstellung eines Produktes benötigt werden, nicht von unbefugten Dritten eingesehen, entwendet oder verändert werden können. Daher brauchen diese Daten eine Verschlüsselung und einen geschützten Zugang.

Safety

Für den Bereich der Safety gibt es zahlreiche IEC-Normen und ISO-Standards. Er wird mit dem zunehmenden Einsatz von Robotern, Mensch-Maschine-Schnittstellen oder Sensoren kontinuierlich weiterentwickelt und umfasst auch die Risikobewertung, wie zum Beispiel Häufigkeit, Dauer oder Wahrscheinlichkeit einer Risikoexposition[1]. Die Weiterentwicklung von Safety-Kriterien und deren Anwendung ist ein wichtiges Handlungsfeld aller 4.0-Aktivitäten. Mitarbeiter müssen gefahrlos in der Umgebung von Robotern oder autonomen Transportsystemen arbeiten können.

Das Ziel des Safety-Engineering besteht darin, Maschinen, Komponenten, Produktionsumgebungen und Prozesse sicher zu gestalten, die Gestaltung ausführlich zu dokumentieren und darauf aufbauend Risiken zu bewerten. Das Design eines Systems wird solange angepasst, bis vorhandene Restrisiken (z. B. Lärm- oder Staubemissionen) nach festgelegten Standards als tolerierbar eingestuft werden können.[2]

Nach Einschätzung der mit Standardisierungsprozessen befassten Normierungsgremien sind die Herausforderungen bei Safety durch Industrie 4.0 gewaltig. Sie werden jedoch durch die betroffenen Akteure seit längerem schon klar adressiert. Unterstützung erhalten diese durch die Mittelstand 4.0-Kompetenzzentren zum Beispiel in Dortmund, in Chemnitz oder in Augsburg. Diese haben es sich zur Aufgabe gemacht, praxisgerechte Safety-Lösungen für den Mittelstand etwa im Bereich der Logistik oder des Robotereinsatzes zu entwickeln und zu transferieren.

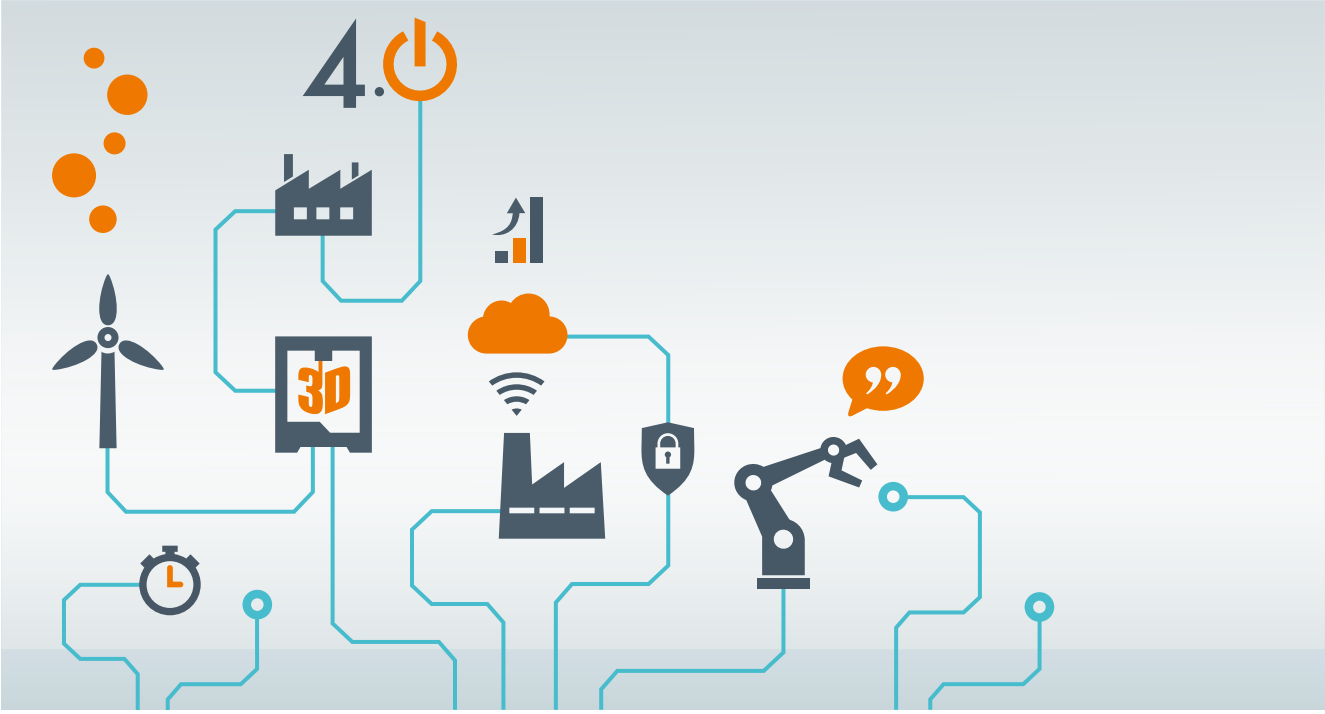
Security

Die andere Dimension der Sicherheit ergibt sich aus dem nahezu flächendeckenden Einsatz von IT-Komponenten und Infrastrukturen. Wertschöpfungsnetzwerke können erst durch die innerbetriebliche und unternehmensübergreifende IT-Vernetzung der beteiligten Unternehmen entstehen. Je mehr der Vernetzungsgrad der Einzelunternehmen und in der Gesamtwirtschaft über das Internet voranschreitet, umso wichtiger werden die Verfügbarkeit der IT-Systeme sowie die Vertraulichkeit und die Integrität der übertragenen Daten und Informationen: Die IT-Sicherheit von Produktionsanlagen und der dazugehörigen Infrastruktur müssen deshalb vor Angriffen geschützt werden. Diese Dimension der Sicherheit von IT- oder so genannten Cyber-Physischen-Systemen wird mit dem Fachterminus der IT-Security beschrieben. Werden zum Beispiel Produktinformationen oder Steuersignale bei der Übertragung manipuliert oder ausgespäht, so können die Schäden für die betroffenen Unternehmen beträchtlich sein.

Obwohl der firmenübergreifende Austausch von Daten sich noch in den Anfängen befindet, haben schon heute die durch unzureichende IT-Sicherheitsmaßnahmen verursachten Schäden volkswirtschaftlich relevante Größenordnungen. Nach einer Erhebung des Branchenverbandes BITKOM betrugen die durch IT-Sicherheitsvorkommnisse verursachten Kosten für die deutsche Wirtschaft zuletzt fast 51 Milliarden Euro pro Jahr.[3] Rund 61 Prozent der Vorfälle, also der größte Teil, entfiel auf kleine und mittlere Unternehmen. Auch wenn die durchschnittliche Schadenssumme weniger als 10.000 Euro betrug, musste immerhin jeder dritte Betrieb Schäden von bis zu 100.000 Euro verkraften und geriet dadurch nicht selten in eine existenzbedrohende Schieflage.[4]

Vor diesem Hintergrund gewinnen die mit der voranschreitenden Digitalisierung und Vernetzung der IT-Systeme verbundenen Sicherheitsanforderungen weiter an Bedeutung.

1 Vgl. z. B. die DIN EN ISO 12100:2010, die Maschinenrichtlinie 2006/42/EG oder die CE-Norm.
2 Vgl. Schneider, U. (2015): Industrie 4.0 und die Sicherheit. Ist der Zug bereits abgefahren?
3 Vgl. DsiN: 51 Milliarden Euro Schaden durch digitale Angriffe auf Unternehmen. www.sicher-im-netz.de/print/1049. Zugriff am 6. Juli 2017.
4 Vgl. www.pwc.de/de/pressemitteilungen/2014/mittelstand-unterschaetzt-cyber-risiken.html. Zugriff am 6. Juli 2017.



Als Haupttreiber der Veränderung von Security nennen laut einer Untersuchung des eco – Verband der Internetwirtschaft e.V. mehr als 50 Prozent der befragten Unternehmen im Jahr 2016 das „Internet of Things“ (IoT).[5] Die digitale Transformation bringt nach übereinstimmender Meinung der Fachleute völlig neue Bedrohungsszenarien mit sich und macht damit fortgeschrittene IT-Security-Maßnahmen erforderlich.[6] Diese sind durchaus gleichzustellen mit den Schutzanforderungen kritischer Infrastrukturen, also etwa von Kernkraftanlagen oder der Wasserversorgung.

Digitalisierung und Sicherheitsrisiken sind für Unternehmen eng miteinander verbunden. Mehr als 70 Prozent der Unternehmen geben an, dass die Digitalisierung in ihrem Unternehmen zu erhöhten Sicherheitsrisiken geführt hat.[7] Für viele verzögert sich durch IT-Sicherheitsaspekte die Einführung digitaler Technologien. Sicherheitsbedenken werden immer wieder als eines der meistgenannten Hemmnisse auf dem Weg der Unternehmensdigitalisierung genannt.[8]

Ähnlich wie im Bereich Safety wurde in den vergangenen Jahren auch im Bereich IT-Security eine ganze Reihe von Klassifikations-, Normungs- und Standardisierungsschritten entwickelt, etwa für den Fall, dass Information Security Management Systeme (ISMS) in Betrieben eingerichtet werden. Zu nennen ist hier vor allem die ISO 27xxx-Normenfamilie, die auf den Aufbau beziehungsweise den Betrieb von IT-Schutzmechanismen in Unternehmen zielt.

Das Bundesamt für Sicherheit in der Informationstechnologie (BSI) hat mit dem IT-Grundschutz einen entsprechenden Rahmen von Maßnahmen abgesteckt, der als Anleitung und Handbuch für die Unternehmens-IT gelten kann.[9] Die Grundschutzkataloge stellen ein Vorgehensmodell zur Verfügung, das Unternehmen befähigt, das eigene Risikoniveau zu bestimmen, das entsprechende Schutzprofil zu definieren und darauf basierend adäquate Schutzmaßnahmen zu ergreifen. Sie beinhalten aber auch eine Sammlung von Best-Practice-Beispielen, um Unternehmen anzuleiten, konkrete Maßnahmen auf betrieblicher Ebene umzusetzen.

5 eco – Verband der Internetwirtschaft (2016): eco Umfrage IT-Sicherheit 2016.
6 Vgl. BMWi (Hg.) (2016): IT-Security in der Industrie 4.0. – Handlungsfelder für Betreiber. Berlin.
7 Vgl. DIHK (Hg.) (2016): Wirtschaft digital: Perspektiven erkannt, erste Schritte getan. Berlin.
8 Vgl. zum Beispiel Ernst & Young (2016): Industrie 4.0: Status quo und Perspektiven in Deutschland.
9 Vgl. BSI (Hg.) (2013): Grundschutzkataloge. Diese wurden seither kontinuierlich aktualisiert.

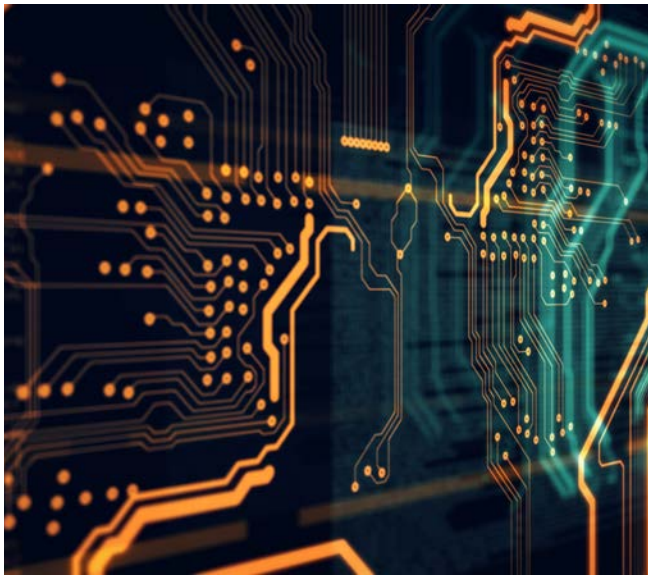
Auch die Plattform Industrie 4.0 hat einen Leitfaden IT-Sicherheit entwickelt, der kleinen und mittleren Unternehmen Handlungsempfehlungen speziell für die Informationssicherheit in der Produktion gibt.[10] Neben rein technischen Schutzmaßnahmen werden insbesondere die notwendigen organisatorischen Rahmenbedingungen beschrieben. Beispielsweise wird empfohlen, Security by Design einzuführen, das heißt, den Aspekt der Security von vornherein bei neuen Produkten oder der Einführung neuer Produktionsprozesse mitzudenken. Ferner wird angeraten, einen so genannten C(I)SO, einen Chief (Information) Security Officer, zu benennen – ähnlich dem bereits in vielen IT-Bereichen bekannten CIO, dem Chief Information Officer. Es geht dabei nicht nur darum, die IT-Security im Betrieb sicherzustellen. Es geht auch darum, die Grundlagen dafür zu schaffen, in Wertschöpfungsnetzwerken mitwirken zu können.

Das Thema der Standardisierung von Security-Anforderungen wird im internationalen Kontext eine immer größere Bedeutung einnehmen. So waren sich anlässlich der im März in Berlin im Rahmen der deutschen G20-Präsidentschaft abgehaltenen „Digitising Manufacturing Conference“ Vertreter aus den USA, Frankreich, Japan und Deutschland einig, dass die Standardisierung zu IT-Security international vorangetrieben werden muss.

Anders als bei einer Safety-Risikoanalyse, bei der ein Evaluierungsprozess beendet ist, sobald ein Risiko als ausreichend eingegrenzt und minimiert gilt, stellen die Risikobewertung und Verminderung bei IT-Security-Maßnahmen einen kontinuierlichen Prozess dar, der immer wieder an den Anforderungen einer sich stetig verändernden Bedrohungslage ausgerichtet werden muss.

Safety und Security: neue Herausforderungen durch Industrie 4.0

Safety- und Security-Anforderungen überlappen sich im praktischen Alltag der Unternehmen häufig. Gleichzeitig können sie bei der Risikobewertung im konkreten Anwendungsfall weit auseinanderfallen, wenn etwa im Bereich der Fernwartung ein System durch technische Vorkehrungen gegen einen Ausfall geschützt, gleichzeitig aber der



Zugang über die elektronische Schnittstelle zum System (Gateway) durch ein schwaches Passwort gefährdet wird. Es existiert demnach eine Lücke zwischen zwei Wahrnehmungs- und Bewertungsperspektiven, die in einer 4.0-Welt geschlossen werden muss. Beide Seiten müssen die Sprache sowie die Denk- und Vorgehensweise der jeweils anderen Seite verstehen lernen.

1. Wissensebene: Safety und Security müssen zusammen betrachtet und zu einer neuen 4.0-Sicherheitsphilosophie verschmolzen werden. Dies beinhaltet sowohl eine einheitliche Dokumentation bei der Risikobewertung als auch eine integrierte Vermittlung in den Lehr- und Lernstoffen der Ausbildungssysteme. Nur durch eine sinnvolle Verbindung beider Welten können neue Tools und Dokumentationen geschaffen werden, die eine adäquate Risikobewertung für ein Gesamtsystem und eine integrierte Vorgehensweise in einem Betrieb ermöglichen.[11]

2. Hardware-/Softwareebene: Vielen Bedienern und Experten fiele eine integrierte Risikobewertung deutlich leichter, würden die verwendeten Hard- und Softwarekomponenten beide Blickrichtungen (Safety und Security by Design) unterstützen. Auch hier gilt es in den nächsten Jahren, entsprechende Lösungen neu zu konzeptionieren und insbesondere unternehmensweit zu implementieren.[12]

10 Vgl. Plattform Industrie 4.0 (2016), IT-Security in der Industrie 4.0 – Handlungsfelder für Betreiber, Berlin.

11 Vgl. Schneider, U. (2015), a.a.O., S. 9ff.

12 Man denke hier z. B. an nutzerfreundliche Authentifizierungssysteme für kooperierende Netzwerkpartner, die es durch automatisierte Integritätsprüfungen erlauben, Bestellungen, Stornierungen, Reklamationen etc. unzweideutig und ohne großen Aufwand einem Unternehmen zuordnen zu können.

3. Infrastrukturebene: Die große Vielzahl der beteiligten Akteure, Maschinen und Werkzeuge macht es erforderlich, Plattformen zu organisieren, mit deren Hilfe Benutzerkonten erstellt, Berechtigungen verwaltet und der Austausch zwischen allen Beteiligten durch einfache, standardisierte und insbesondere sichere Verfahren mit vertretbarem ökonomischen und administrativen Aufwand abgebildet werden können.

Der Mittelstand und die Implementierung von Security 4.0

In einer künftigen Netzwerkökonomie werden kleine und mittlere Unternehmen aller Voraussicht nach ungleich höheren IT-Sicherheitsrisiken ausgesetzt sein als bisher. Es muss daher gelingen, die Betriebe hinreichend zu sensibilisieren und sie bei der Implementierung adäquater Sicherheitsmaßnahmen zu unterstützen. Doch erst auf Basis einer angemessenen Bedrohungs- und Risikoanalyse können adäquate Schutzmaßnahmen definiert und umgesetzt werden. Wichtige Fragen und Maßnahmen für jede Geschäftsführung sollten sein:[13]

- Erstellung eines Plans bezüglich der IoT-Charakteristiken des Unternehmens: Welche Strukturen, Maschinen und Fertigungskomponenten sollen eingebunden werden, damit sie Teil eines Kooperationsnetzwerks werden können?
- Identifizierung und Bewertung der Risiken mit Blick auf kritische Systeme, Anlagen und Werte: Wie können mittelständische Unternehmen in die Lage versetzt werden, mit vertretbarem Aufwand ein eigenes Risikoprofil zu erstellen?
- Angemessener Schutz der Security/Safety-relevanten Anlagen und Daten: Welche Schutzmaßnahmen müssen für eine gesicherte Kommunikation nach außen, etwa gegen Fehlsteuerung oder Manipulation, ergriffen werden?
- Sensibler Umgang mit Daten: Welche Daten muss ein Betrieb wann, wem, in welcher Form bereitstellen und wer darf über ein entsprechendes Rollenmanagement darauf zugreifen?

13 Vgl. z. B. BMWi (Hg.) (2016), ebenda; vgl. auch Plattform Industrie 4.0 und Robot Revolution Initiative (2017): Facilitating International Cooperation for Secure Industrial Internet of Things/Industrie 4.0, Berlin und Tokio.

- Erreichung der Schutzziele: Wie können im Prozess mit Kooperationspartnern die Vertraulichkeit der Daten von Kunden gesichert und deren Integrität geschützt werden? Bei wem liegt die Verwaltungshoheit für die Daten?

- Rechtliche Aspekte im Umgang mit Risiken: Welche Verträge sind mit Kooperationspartnern in Bezug auf die Zurechnung von Eigentums- oder Haftungsfragen z. B. im Falle von Qualitätsmängeln oder Leistungsausfällen zu schließen und wie kann dies zu geringen Transaktionskosten verwirklicht werden?

- Fortbildung auch im Bereich IT-Security: Wie müssen Belegschaften auf die neuen Anforderungen etwa durch neue Berufsbilder („Prozessmanager“) oder durch Schulungen vorbereitet werden und in welcher Weise müssen die bestehenden Curricula weiterentwickelt werden?[14]

- Ergreifen von Gegenmaßnahmen bei Angriffen: Welche Prozesse technischer Art oder im Netzwerk können für Gegenmaßnahmen genutzt werden?

- Sicherstellen der Produktion bei Angriffen: Wie kann ein sicherer Betrieb und Informationsfluss gewährleistet werden?

Security als ein Schwerpunkt der Mittelstand 4.0-Kompetenzzentren

Zu den wichtigen Aufgaben der Mittelstand 4.0-Kompetenzzentren gehört, nicht nur Safety-Lösungen zu entwickeln (siehe oben), sondern im Rahmen ihrer Lernfabriken auch Best-Practice-Beispiele für Security zu entwickeln und an die Unternehmen ihrer Region zu vermitteln. Das Zentrum in Darmstadt zum Beispiel arbeitet an Lösungen, die automatisierte Produktion und ihre Vernetzung nach außen möglichst sicher zu machen. Das Zentrum Hannover wiederum verfolgt im Rahmen der Lernfabrik „IT-Security“ die Integration vielfältiger Sicherheitsaspekte in die bestehenden Curricula von Hochschulen und die Ausbildungslehrgänge.

Insgesamt wird es in der Netzwerkökonomie darum gehen, auf der Basis dieser Arbeiten kleine und mittlere Betriebe zu einer validen Einschätzung zu befähigen. Unternehmen sollen individuell erkennen und bewerten können, welche Maßnahmen ergriffen werden müssen, um den Schutz für das eigene Unternehmen fortlaufend auf einem angemessenen Niveau zu halten. Nur so wird sich in den Betrieben das notwendige Vertrauen in ihre integrierten Safety- und Security-Prozesse entwickeln, so dass sie ohne Befürchtungen an Wertschöpfungsnetzwerken teilnehmen können.

Kontakt: Ralf Franke
Referat: Mittelstand-Digital
und Dr. Franz Büllingen
Leiter Begleitforschung Mittelstand-Digital
(WIK GmbH)

14 Vgl. auch Plattform Industrie 4.0 (2016), Industrie 4.0-Security in der Aus- und Weiterbildung: Neue Aspekte für Unternehmensorganisation und Kompetenzen, Berlin.