PLATTFORM INDUSTRIE 4.0

ERGEBNISPAPIER

Technischer Überblick: Sichere unternehmensübergreifende Kommunikation

Impressum

Herausgeber
Bundesministerium für Wirtschaft
und Energie (BMWi)
Öffentlichkeitsarbeit
11019 Berlin
www.bmwi.de

Redaktionelle Verantwortung
Plattform Industrie 4.0
Bertolt-Brecht-Platz 3
10117 Berlin

Gestaltung und Produktion
PRpetuum GmbH, München

Stand
April 2016

Druck
Spreedruck Berlin GmbH

Bildnachweis
MaximP – Shutterstock (Titel); BillionPhotos.com – Fotolia (S. 6, S. 8); GKSD – Fotolia (S. 11); sdecoret – Fotolia (S.17); Artur Marciniec – Fotolia (S. 20); Syda Productions – Fotolia (S. 21)

Das Bundesministerium für Wirtschaft und Energie ist mit dem audit berufundfamilie® für seine familienfreundliche Personalpolitik ausgezeichnet worden. Das Zertifikat wird von der berufundfamilie gGmbH, einer Initiative der Gemeinnützigen Hertie-Stiftung, verliehen.

Diese und weitere Broschüren erhalten Sie bei:
Bundesministerium für Wirtschaft und Energie
Referat Öffentlichkeitsarbeit
E-Mail: publikationen@bundesregierung.de
www.bmwi.de

Zentraler Bestellservice:
Telefon: 030 182722721
Bestellfax: 030 18102722721

Inhalt

1. Einleitung

Ziel des Papiers ist es, eine gemeinsame Position hinsichtlich der Security-Herausforderungen, grundsätzlichen Anforderungen und Ansätze für eine sichere Kommunikation in Industrie 4.0-Umgebungen zu formulieren, die speziell die Bedarfe unternehmensübergreifender Wertschöpfungsnetzwerke berücksichtigt.

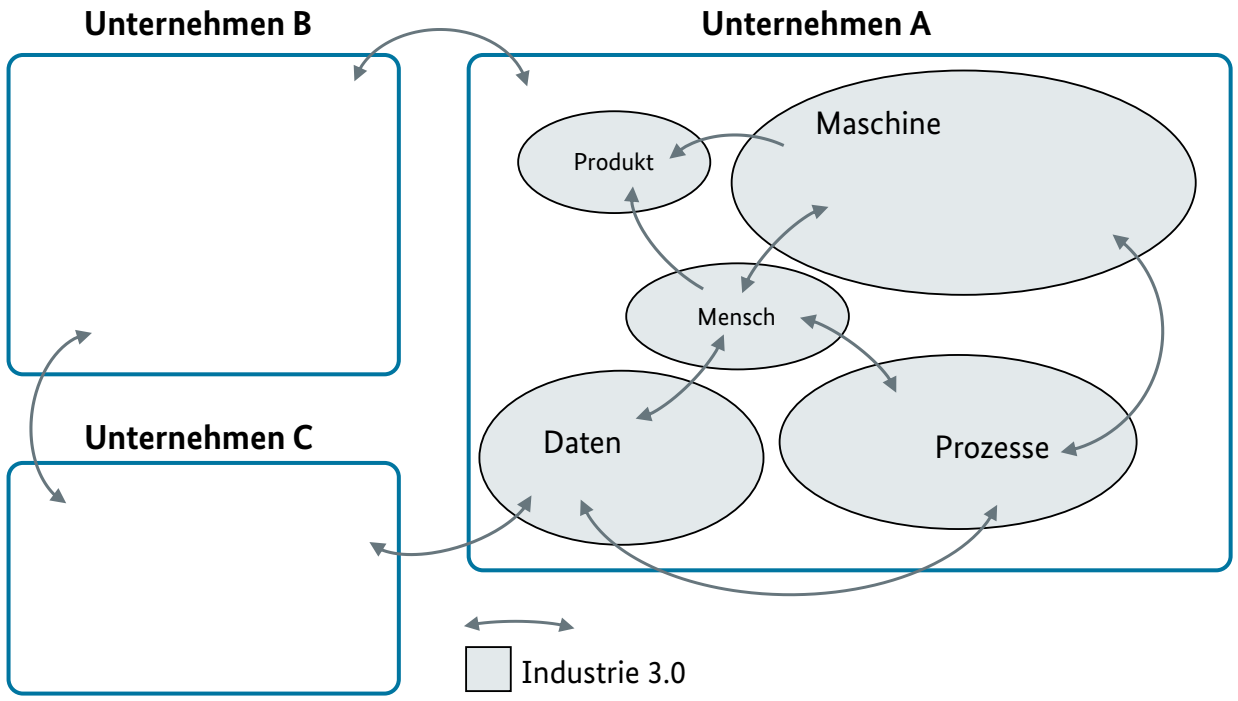
Die Inhalte werden bewusst auf einer generischen Ebene skizziert, um eine gute Übertragbarkeit sicherzustellen. Denn jede detaillierte Security-Betrachtung muss eine Einzelfallbetrachtung sein, um die ausschlaggebenden Rahmenbedingungen zu berücksichtigen. Entsprechend wird von einer konkreten Projekt- oder Implementierungsbeschreibung abgesehen.

Das Dokument richtet sich an Entscheider und Anwender im Industrie 4.0-Kontext, für die grundlegend die zu beachtenden Rahmenbedingungen, Leitprinzipien und gewonnenen Erkenntnisse zu Security exemplarisch dargestellt werden.

1.1 Realität bei Industrie 3.0

Viele Teilaspekte von Industrie 4.0 sind heute schon Stand der Technik oder werden sich als Weiterentwicklung aktueller Technologien erweisen. Unter dem Begriff Industrial Ethernet sind in weiten Teilen der Automatisierung bereits heute proprietäre Bus-Systeme durch Ethernet und Internet Protocol ersetzt. Eine automatisierte Kommunikation zwischen Unternehmen findet zumeist an wenigen Schnittstellen statt: So hat sich zwar die Kommunikation bis in die Automatisierungsebene, beispielsweise für Fernwartung, teilweise etabliert, wird allerdings in vielen anderen Bereichen unter anderem wegen Sicherheitsbedenken abgelehnt. Kommunikationsbeziehungen ohne Vertrauen in den Kommunikationspartner erschließen daher nur einen Teil des technisch möglichen Potentials, siehe Abbildung 1.

Abbildung 1: Kommunikations- und Vertrauensbeziehungen bei Industrie 3.0



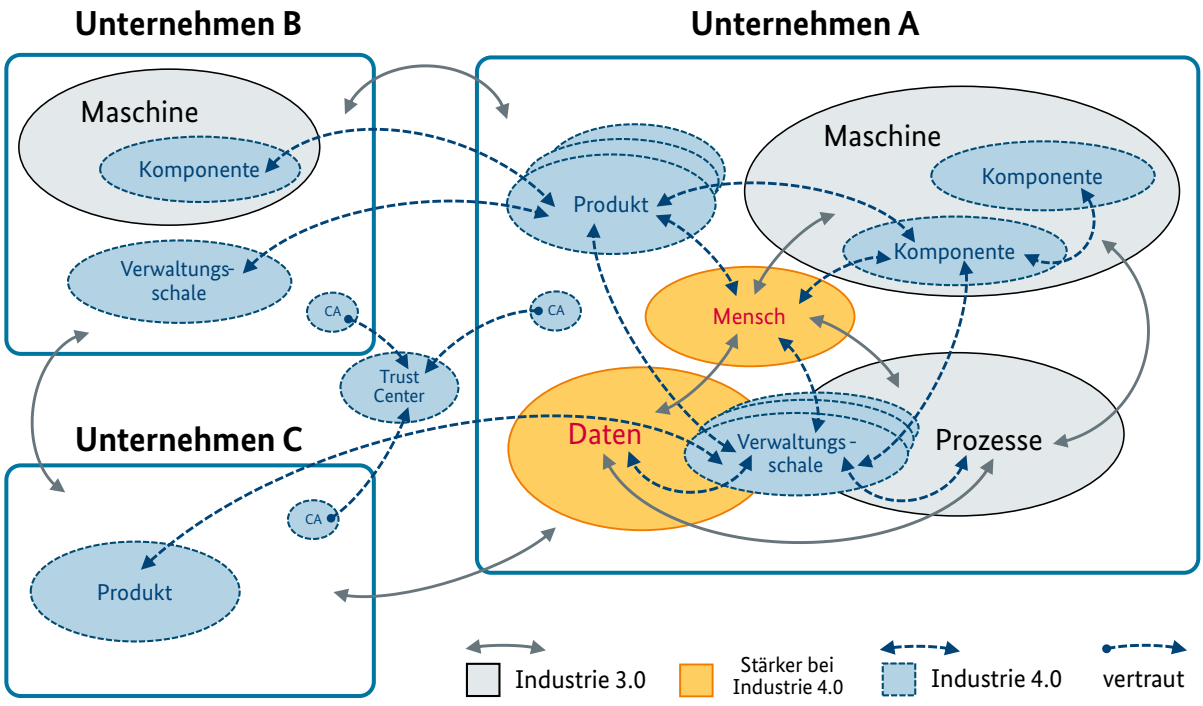
Quelle: Plattform Industrie 4.0

1.2 Was ist neu bei Industrie 4.0?

Um Industrie 4.0 umzusetzen, werden agile Kommunikationsbeziehungen auch über Unternehmensgrenzen hinweg benötigt. Für die auftragsgesteuerte Produktion in Losgröße 1 stehen notwendige Informationen nicht mehr lange im Voraus in zentralen Systemen zur Verfügung, sondern werden dezentral „Just-in-Time“ geliefert. Die Teilnahme an Marktplatzkonzepten und dynamischen Wertschöpfungsnetzwerken setzt die jederzeitige Bereitschaft zur elektronischen Interaktion voraus. Hierdurch ergeben sich zusätzliche Anforderungen an die Sicherheit von Kommunikationsbeziehungen bei Vertraulichkeit, Integrität und Verfügbarkeit.

Für den erfolgreichen Austausch von Information muss das Vertrauen in die Sicherheit der Kommunikationsbeziehung ebenso gegeben sein wie das Vertrauen in die weitere sichere Verarbeitung der Information beim Kommunikationspartner. Neben technischen Aspekten setzt dies eine belast- und bewertbare operative Verankerung von Security bei den beteiligten Partnern voraus – etwa durch ein Information Security Management System ISMS, siehe (1).

Abbildung 2: Kommunikations- und Vertrauensbeziehungen bei Industrie 4.0



Quelle: Plattform Industrie 4.0

2. Kommunikation

Kommunikation *(lat. communicatio, ‚Mitteilung') ist der Austausch oder die Übertragung von Informationen (Quelle: Wikipedia).*

Es gibt keine einheitliche Definition von Kommunikation. Die Kommunikationswissenschaft ist eine Disziplin der Sozial- und Geisteswissenschaften, die sich mit menschlichen Kommunikationsvorgängen befasst. Im Kontext dieses Dokuments wird Kommunikation als technischer Prozess betrachtet.

2.1 Sichere Kommunikation als Kernthema

2.1.1 Kommunikation wird wichtiger

Industrie 4.0 beschreibt die Möglichkeiten, die durch die Weiterentwicklung von Hard- und Software entstehen. Eine wesentliche Voraussetzung ist, dass Daten und Informationen zur Verfügung gestellt werden, um sie zu verarbeiten. In Industrie 3.0 geschieht das zumeist auf lokaler Ebene, etwa Kommunikationsbeziehungen zu Sensoren und Aktoren, also aktive Elemente wie Motoren, innerhalb einer Anlage. Auf Unternehmensebene wird mit Manufacturing-Execution-Systemen (MES) oder darüberliegenden Enterprise-Resource-Planning-Systemen (ERP) kommuniziert. Betriebs- und Qualitätsdaten werden in entsprechenden Systemen erfasst.

In zukünftigen Szenarien eröffnet der direkte Austausch von Daten und Informationen über Unternehmensgrenzen hinweg neue Möglichkeiten. Als Kommunikationspartner sind dabei sowohl Menschen als auch Maschinen zu betrachten. Zudem wird nicht mehr nur über die Management-Ebene (MES/ERP) über Unternehmensgrenzen hinweg kommuniziert, sondern auch auf darunterliegenden Ebenen, zum Beispiel von einer Maschine oder einer Komponente direkt zu ihrem Lieferanten. Hierbei sind auch Ende-zu-Ende-Verbindungen zu berücksichtigen, die durch den Wechsel auf IPv6 skalierbar möglich werden.

2.1.2 Kommunikation muss sicher sein

Aus Sicht der Security sind Anforderungen aus vielen Bereichen wie Schutz von Know-how, Daten und Geschäftsgeheimnissen zu berücksichtigen, die immer durch die klassischen Schutzziele

- Vertraulichkeit
- Integrität und
- Verfügbarkeit

abgebildet werden, siehe Abschnitt 4.1. Mit einer unternehmensübergreifenden Kommunikation, die über organisato-

rische Grenzen wie auch über WAN-Verbindungen (Wide Area Network) stattfinden wird, steigen die Anforderungen an die Vertraulichkeit der Kommunikation. Im Kontext des Industrie 4.0-Geschäftsprozesses wird es zudem immer wichtiger, die Verfügbarkeit der Daten und der Kommunikationsverbindungen sicherzustellen.

Industrie 4.0 sieht auch vor, rechtlich relevante Kommunikation abzubilden, zum Beispiel im Rahmen von Bestell- und Logistikprozessen. Daher sind bei der Betrachtung weitere nachgeordnete Schutzziele wie

- Authentizität
- Nichtabstreitbarkeit
- Verbindlichkeit und
- Zurechenbarkeit

zu berücksichtigen (siehe Abschnitt 4.1).

2.2 Betrachtungsebene und Abgrenzungen

Sichere Kommunikationsbeziehungen lassen sich mit vielen verschiedenen technischen Mitteln erreichen. Ziel des Papiers ist es, Anforderungen und Konzepte für die Umsetzung zu formulieren, die unabhängig von Technologien, die sich weiterentwickeln, gültig bleiben. Entsprechend wird auf einer höheren Betrachtungsebene vorgegangen, der Darstellungsschicht (Schicht 6) und der Anwendungsschicht (Schicht 7) im OSI-7-Schichtenmodell (siehe Abschnitt 11.1).

2.2.1 Kommunikation auf der Darstellungsschicht und darüber

Ein Beispiel für eine vertrauliche Kommunikation ist der sichere Dateitransfer. Eine Datei kann direkt für einen bestimmten Empfänger verschlüsselt und ohne weitere Maßnahmen übertragen werden. Sie kann aber auch, selbst unverschlüsselt, über eine verschlüsselte Verbindung zwischen zwei Rechnern übertragen werden. Weiterhin ist eine unverschlüsselte Übertragung zwischen zwei Rechnern denkbar, wenn die Fernverbindung zwischen zwei Standorten als Virtual Private Network (VPN) verschlüsselt ist, was wiederum durch firmeneigene VPN-Gateways oder als Leistung eines Telekommunikationsunternehmens realisiert werden kann. Jede dieser Möglichkeiten hat Vorzüge und Nachteile hinsichtlich Archivierbarkeit, Kontrollmöglichkeiten, Skalierbarkeit und anderen Eigenschaften, die betrachtet werden müssen.

2.2.2 Zusammenhang zu unteren Schichten im Kommunikationsmodell

Die genaue technische Umsetzung, etwa mit welchen Algorithmen gearbeitet werden soll, welche Schlüssellängen Verwendung finden müssen, mit welcher Technik (drahtlos, drahtgebunden) übertragen werden soll, ist nicht Bestandteil der Betrachtungen. Diese Themen werden in anderen Gremien bearbeitet, die durch die Spezialisierung und fortlaufende Pflege für eine Weiterentwicklung der benötigten Basistechnologien sorgen. Ein Beispiel hierfür sind die Technischen Richtlinien des Bundesamts für Sicherheit in der Informationstechnik (BSI). Auf europäischer Ebene ist etwa die Europäische Agentur für Netz- und Informationssicherheit (ENISA) zu nennen. Das amerikanische National Institute for Standards and Technology (NIST) prägt viele international verwendete Technologien im Bereich der Kryptographie. Die Internet Engineering Task Force (IETF) formuliert Protokollstandards im Internet und das Europäische Institut für Telekommunikationsnormen (ETSI) und die Internationale Fernmeldeunion (ITU) sind im Bereich Standardisierung in der Telekommunikation tätig.

Voraussichtlich entstehen für Industrie 4.0-Anwendungen Anforderungen an diese Basistechnologien, etwa im Bereich der Dienstgüte. Dabei orientieren sich die Diskussionen am Referenzarchitekturmodell für Industrie 4.0, siehe (2).

2.3 Auswirkungen auf Organisationen

Unternehmen, die sich an den unternehmensübergreifenden Wertschöpfungsnetzwerken beteiligen wollen, werden sich entsprechend dem Geschäftsmodell organisatorisch weiterentwickeln müssen. Technische Lösungen im Bereich IT-Security alleine sind nicht ausreichend, wenn diese nicht durch entsprechende organisatorische Maßnahmen unterstützt werden. Die für den Vertrauensaufbau notwendige Bewertung der Security-Standards muss entsprechend dem Reifegrad bezüglich IT-Security etwa entsprechend dem Capability Maturity Model Integration (CMMI) erfolgen.

Damit kleine und mittelständische Unternehmen dies leisten können, müssen sie durch geeignete Standards unterstützt werden. Auch größere Unternehmen werden ihre Information Security Management Systeme (ISMS) entsprechend weiterentwickeln müssen.

3. Nutzen und Ziele sicherer Kommunikation

Im Industrie 4.0-Umfeld ermöglichen vielfältige Wertschöpfungsnetzwerke von Unternehmen neue Geschäftsfelder und Produktionsprozesse. Der Datenaustausch zwischen verschiedenen Unternehmen erfolgt mehrheitlich über die Kommunikationsinfrastruktur des Internets, wodurch sich generell die Angriffsfläche auf Industrie 4.0-Abläufe erhöht. Daher gilt ein spezielles Augenmerk der sicheren Kommunikation über Unternehmensgrenzen hinweg. Das Ziel sicherer Kommunikation ist es, ein hohes Vertrauen in die Sicherheit von neuartigen Industrie 4.0-Prozessen zu schaffen, so dass bezüglich dieses Aspektes des Informationsaustausches keine Vorbehalte und Hindernisse für deren Etablierung existieren. Das herauszustellende Hauptziel ist dabei der Schutz wichtiger Unternehmenswerte.

Der Nutzen sicherer Kommunikation besteht darin, den sicheren Betrieb von Industrie 4.0-Szenarien grundsätzlich zu ermöglichen. Sichere Kommunikation kann in Deutschland und Europa die Akzeptanz für diese Szenarien erhöhen und einen Industrie 4.0-Schub erzeugen oder beibehalten, das heißt, den damit verbundenen Innovationen ein nachhaltiges Gelingen ermöglichen. Da Kommunikationssicherheit zukünftig sofort in den Szenarien miteingebaut ist, wird es für produzierende Unternehmen einfacher, an den neuen Produktionsprozessen teilzunehmen und auch diese mitzugestalten, da die Kommunikationsteilnehmer (zum Beispiel Maschinen) Sicherheitsmindeststandards bereits erfüllen. Des Weiteren ist für Maschinen-Hersteller eine eingebaute Industrie 4.0-Kommunikationssicherheit ein Verkaufsargument – zunächst als ein wichtiges Merkmal der Zukunftsfähigkeit der Maschinen, später als generelle, essenzielle Eigenschaft aller produzierenden Maschinen, ohne die sie nur noch schwer oder nicht mehr verkäuflich sein werden.

3.1 Schutz wichtiger Unternehmenswerte

Industrie 4.0 erzeugt zusätzlichen elektronischen Kommunikationsbedarf, der über die bisherigen Unternehmensgrenzen hinweggeht. Um zielgerichtet in Sicherheit zu investieren, sind zunächst Unternehmenswerte mit Schutzbedarf zu identifizieren (zum Beispiel Rezepte, verfahrenstechnologische Parameter, prozesstechnische Qualitätssicherungsmethoden). Alle schützenswerten Informationen besitzen einen sogenannten Schutzbedarf, den jeweils geeignete Maßnahmen sicherstellen sollten. Dieser ist – je nach geplanter Aufgabenteilung – im Gesamtprozess der Industrie 4.0 sicher aufrechtzuerhalten, um insbesondere den Schutz der eigenen Unternehmenswerte im Kommunikationsprozess mit anderen Unternehmen durch vertrauliche Behandlung sicherzustellen. Je besser die Risiken für die eigenen Unternehmenswerte erkannt werden, desto effizienter können Schutzziele geplant und umgesetzt werden. Bereits bei der Investitionsplanung lassen sich aus diesen Zielen Mindestanforderungen für unternehmensinterne und unternehmensübergreifende Sicherungsmaßnahmen ableiten.

4. Sichere Kommunikationswege

4.1 Einleitung

Die im Industrie 4.0-Umfeld üblichen Kommunikationswege sind bezüglich der Kommunikationspartner unterscheidbar. Bei einer **Mensch-zu-Mensch-Kommunikation** findet neben dem Transport von Nachrichten (zum Beispiel telefonisch oder per E-Mail) keine weitere elektronische Datenverarbeitung statt.

Bei der **Mensch-zu-Maschine-Kommunikation** regelt ein Mensch die Funktionsweise einer Maschine. Hierbei findet eine elektronische Datenverarbeitung an der Schnittstelle Mensch zu Maschine statt. Bei der **Maschine-zu-Maschine-Kommunikation** beeinflusst eine Maschine die Funktionsweise anderer Maschinen, um zum Beispiel eine Maschinenübergreifende Automatisierung zu implementieren. Dabei findet auf beiden Seiten eine elektronische Datenverarbeitung statt. Eine menschliche Einflussnahme findet nicht oder maximal überwachend statt, die Maschinen kommunizieren autonom miteinander.

Bei der im Industrie 4.0-Kontext intensiv eingesetzten Maschine-zu-Maschine-Kommunikation ist sicherzustellen, dass die Kommunikationspartner vertrauenswürdig sind (siehe Abbildung 2: Kommunikations- und Vertrauensbeziehungen bei Industrie 4.0). Die Identität der Kommunikationspartner muss ebenso sichergestellt sein, wie die Unverfälschbarkeit der ausgetauschten Daten auf dem Kommunikationsweg. Beide Aspekte sind durch Cyber-Attacken einem Risiko ausgesetzt. Abhängig von den Kommunikationslokationen und -partnern ist die Herstellung der Vertrauenswürdigkeit zwischen verschiedenen beteiligten Partnern auszuhandeln.

Bei einer **Lokalen Kommunikation** werden Daten innerhalb eines Standortes eines Unternehmens ausgetauscht. Die Kommunikations-Infrastruktur wird in der Regel von einer IT-Organisation gemanagt. Diese kann mit den lokalen Kommunikationsteilnehmern technisch das Vertrauen aushandeln und sicherstellen. Bei einer **Lokationsübergreifenden Kommunikation** findet ein Datenaustausch zwischen verschiedenen Standorten eines Unternehmens statt. Die Kommunikations-Infrastruktur wird gegebenenfalls von verschiedenen IT-Organisationen innerhalb des Unternehmens gemanagt. Der Informationsaustausch zwischen den Lokationen erfolgt über WAN-Verbindungen (Wide Area Network) von Telekommunikationsprovidern. Dabei verlassen die Daten zwischenzeitlich den Einflussbereich des Unternehmens. Die Aushandlung und Sicherstellung der Vertrauenswürdigkeit wird hierbei durch die verschiedenen beteiligten Partner erschwert, da sich nicht alle erforderlichen Kommunikationskomponenten im Einflussbereich des Unternehmens befinden (zum Beispiel DNS-Server). Bei einer **Unternehmensübergreifenden Kommunikation** werden Daten zwischen verschiedenen Unternehmen ausgetauscht. Hier gelten die gleichen Rahmenbedingungen wie bei der Lokationsübergreifenden Kommunikation. Zusätzlich ist zu berücksichtigen, dass der Kommunikationspartner technisch und organisatorisch außerhalb des Einflussbereichs des Unternehmens liegt. Die Aushandlung und Sicherstellung der Vertrauenswürdigkeit wird zusätzlich erschwert, wenn die Zahl der beteiligten Partner ansteigt.

Bei der Einführung sicherer Kommunikationswege sind generell folgende Sicherheitsaspekte zu berücksichtigen:

1. **Verfügbarkeit:** Die Infrastruktur ist vor einem Ausfall zu schützen. So könnte zum Beispiel ein Angreifer versuchen, die Steuerung einer Chemieanlage durch Sabotage der Kommunikationsinfrastruktur zu stören, so dass erheblicher Schaden für Produkte und Anlagen entstehen kann.

2. **Integrität:** Die Daten sind vor unberechtigter Veränderung zu schützen. Ein potentieller Angreifer könnte beispielsweise versuchen, die Steuerbefehle für eine Maschine abzufangen, durch andere zu ersetzen und damit kritische Fehlfunktionen auszulösen. So beschädigten Hacker laut BSI-Sicherheitsbericht 2014 einen Hochofen in einem deutschen Stahlwerk (3).

3. **Vertraulichkeit:** Die Daten sind vor unberechtigtem Zugriff zu schützen. Eine Kernherausforderung ist die Authentifizierung der Kommunikationspartner. Wie erkennt die Maschine, dass es sich um eine bestimmte andere Maschine handelt und kein Angreifer die Identität dieser anderen Maschine vortäuscht, um zum Beispiel sensitive Daten von dort abzuholen? Als kritische Angriffe werden sogenannte Man-In-The-Middle-Szenarien gesehen, bei denen ein Angreifer den Datenstrom über eine Zwischenstation umleitet, diesen abhören oder sogar manipulieren kann (betrifft auch Integritätsaspekte). Eng verbunden mit der Authentifizierung ist die Autorisierung. Ihre Aufgabe besteht darin, dem Kommunikationspartner Zugriff auf bestimmte Funktionen zu gewähren. Fortgeschrittene Angriffstechniken bestehen darin, einen bestehenden Zugang illegal um Berechtigungen für kritische Funktionen zu erweitern.

Mit Hilfe von Authentifizierungsmechanismen wird die Authentizität, also die Echtheit des Kommunikationspartners beziehungsweise die Originalität einer Datenquelle,

sichergestellt. Sie spielt eine entscheidende Rolle bei der Sicherstellung der Vertraulichkeit und Integrität.

Um im Fehler- oder Angriffsfall den Vorgang nachvollziehen zu können, ist es essentiell, dass zwischen Kommunikationspartnern ausgetauschte Nachrichten nicht abgestritten werden können (Nichtabstreitbarkeit). Hierzu dienen häufig Protokoll-Funktionen, die den Datenverkehr zusätzlich aufzeichnen und im Bedarfsfall auswertbar machen. Im Kontext rechtlicher Betrachtungen ist Nichtabstreitbarkeit ebenfalls ein relevantes Schutzziel.

Die Sicherheitsziele Authentizität und Nichtabstreitbarkeit definieren zusammen den Begriff Verbindlichkeit. Eine Maschine stellt gegenüber einer anderen ihre Authentizität durch Authentifizierungsmechanismen sicher und der Nachrichtenverkehr zwischen den beiden Maschinen wird zum Beispiel auswertbar aufgezeichnet.

Um im Fehler- oder Angriffsfall den Gesamtvorgang nachträglich betrachten zu können, ist zusätzlich der Nachweis der Zurechenbarkeit sicherzustellen. Wenn etwa eine Maschine fehlerhafte Materialien produziert, muss es möglich sein, die Grundursachen für die Fehlfunktion zuzuordnen, also zuzurechnen (zum Beispiel Verwendung falscher Parameter, kommend aus einer bestimmten Quelle, gesendet zu einem bestimmten Zeitpunkt vom authentifizierten Kommunikationspartner).

Die klassischen proaktiven Security-Maßnahmen zur Sicherstellung von Vertraulichkeit und Integrität sind typischerweise:

- Benutzer- und Identitätsmanagement (Authentifizierung, Autorisierung). Hier sei für weitere Details auf den Technischen Überblick Sichere Identitäten (4) zu verweisen.
- Datenverschlüsselung und Signatur

Beide Maßnahmen dienen zur Sicherstellung der Authentizität.

Die Verfügbarkeit stellt ein zentrales Sicherheitselement für IT-unterstützte Prozesse dar. Im industriellen Umfeld wird die Verfügbarkeit von Systemen, Komponenten, Netzwerkverbindungen und Daten sehr hoch bewertet. Klassische proaktive Security-Maßnahmen zur Sicherstellung der Verfügbarkeit erfordern zusätzliche Infrastrukturkomponenten (zum Beispiel spezielle Hard- und Software-Lösungen sowie Mehrfachauslegung des Kommunikationssystems).

Die klassischen reaktiven Security-Maßnahmen bestehen typischerweise aus Security-Monitoren/-Detektoren, gegebenenfalls unterstützt durch automatische Reaktionsmethoden, die zum Beispiel einen verdächtigen Kommunikationspartner automatisch blockieren. Die von ihnen aufgezeichneten Ereignisse gestatten die nachträgliche Untersuchung von sicherheitsrelevanten Vorfällen und geben so wertvolle Hinweise auf zusätzlich zu ergreifende Sicherheitsmaßnahmen.

Die Sicherheitsmechanismen Verbindlichkeit und Nichtabstreitbarkeit sind wichtige Voraussetzungen für die reaktiven Maßnahmen.

4.2 Kommunikationsdesign

Um in der vernetzten Welt der Industrie 4.0 Menschen und Maschinen unternehmensübergreifend miteinander zu verbinden und stets die Prinzipien der Vertraulichkeit, Integrität und Verfügbarkeit zu wahren, ist eine ganzheitliche Betrachtung in Form eines Kommunikationsdesigns erforderlich.

Das Kommunikationsdesign hilft dabei, die verschiedenen Verbindungen zum Informationsaustausch zu identifizieren, dokumentieren und der Kritikalität für den Geschäftsprozess durch Schutzmaßnahmen gerecht zu werden. Hierbei kann die Unterscheidung verschiedener Netzwerkzustände wie Regelbetrieb, Notbetrieb, Wartungsbetrieb oder Analysebetrieb hilfreich sein. Übergeordnetes Ziel ist dabei die Aufrechterhaltung der Kommunikationsfähigkeit. Denn auf diese wirken besondere Bedrohungen – insbesondere bei dynamischer, unternehmensübergreifender Vernetzung. Die Unterscheidung verschiedener Netzwerkzustände – wie Wartung und Notbetrieb – ist sinnvoll, weil damit auffälliges, ungewöhnliches Kommunikationsverhalten bereits frühzeitig proaktiv erkannt werden kann. Jedoch auch bei der nachträglichen Reaktion auf Sicherheitsvorfälle ergeben sich Vorteile, da die gezielte Analyse eines Sicherheitsvorfalls bei vorliegendem Kommunikationsdesign erheblich vereinfacht werden kann. Insbesondere bei fortschrittlichen und gezielten Angriffen hat dies eine Beschleunigung des Response-Verfahrens zur Folge. Darüber hinaus kann es im Rahmen der Reaktion auf ungezielte Angriffe sinnvoll sein, das Kommunikationsverhalten kurzzeitig auf ein erforderliches Minimum zu reduzieren, um die Angriffsfläche zu reduzieren.

Ein Kommunikationsdesign identifiziert die schützenswerten Komponenten (etwa Asset-Identifizierung) und Kom-

munikationswege, beinhaltet eine Risiko-Bewertung, klassifiziert die Komponenten sowie die ausgetauschten Daten, und definiert geeignete Maßnahmen der Ausfallsicherheit (etwa redundante Auslegungen).

4.3 Verfügbarkeit/Zuverlässigkeit

Im Kontext der Industrie 4.0 werden Funktionen und Möglichkeiten des Internets auf reale Objekte erweitert. Diese werden untereinander vernetzt und können so miteinander kommunizieren (Maschine-zu-Maschine-Kommunikation). Im Industrie 4.0-Anwendungsszenario „Auftragsgesteuerte Produktion", siehe Abschnitt 11.2, wird eine flexible Fertigungskonfiguration dargestellt, die sich durch eine werks- und unternehmensübergreifende Vernetzung von Produktionsfähigkeiten und Kapazitäten schnell an sich ändernde Markt- und Auftragsbedingungen anpasst. Die Fähigkeiten und Kapazitäten der bestehenden Produktionsmittel optimal auszunutzen, setzt allerdings eine gesicherte Kommunikation voraus.

Ein Schlüsselfaktor für gesicherte Kommunikation ist die Sicherstellung der dazu benötigten **Kommunikations-Verfügbarkeit**. Um die beispielhafte Zielsetzung des Anwendungsszenarios, „eigene" Fertigungsfähigkeiten und Kapazitäten ad hoc entsprechend der Auftragslage weitgehend automatisiert zu erweitern, einzuhalten, müssen alle beteiligten technischen Systeme im passenden Zeitverhalten, innerhalb des vereinbarten Zeitraums operativ agieren und zur Verfügung stehen („Just-in-Time", „Just-in-Sequence"). Dieses Zeitverhalten wird im industriellen Kontext oft als Echtzeit bezeichnet. In der Folge wird der Begriff „anwendungs- und prozessgerechtes Zeitverhalten" als erklärendes Synonym für Echtzeit verwendet, um den Bezug und die Abhängigkeiten des Zeitverhaltens zu verdeutlichen. Anwendungs- und prozessgerechtes Zeitverhalten in Kommunikationsprozessen definiert die vorgegebene Zeitspanne, in der Informationen zur Verfügung stehen beziehungsweise transportiert werden müssen. Dies kann sowohl synchron als auch asynchron und somit „on Demand" erfolgen. Eine durchgehende Zeitsynchronisierung aller am Prozess beteiligten technischen Systeme ist dazu allerdings zwingend zu gewährleisten. Somit ist es unumgänglich, wichtige Design-Faktoren für die Verfügbarkeit und Zuverlässigkeit einer Kommunikation von Beginn an, sprich bereits im Designprozess, festzulegen und kontinuierlich auf Wirksamkeit zu überprüfen. Je nach Kritikalität und Prozessketten-Abhängigkeit der Teilnehmer im Kommunikationsprozess müssen sowohl technische als auch organisatorische Aspekte zur Verfügbarkeit und **Robustheit** der Kommunikationsinfrastruktur betrachtet werden. Zu berücksichtigende technische Aspekte sind u. a. Dienstgüte (Quality of Service), Bandbreite der genutzten Kommunikationsinfrastruktur und anforderungsrelevante kommunikative Eigenschaften der teilnehmenden Systeme,

sowie die Sicherstellung einer Zeitsynchronisierung. Aus Sicht von organisatorischen Design-Aspekten zu Verfügbarkeit und Zuverlässigkeit von sicherer Kommunikation müssen Bewertungen und Maßnahmenplanungen für mögliche Stör-, Manipulations- und Ausfallszenarien in Kommunikationsprozessen vorgenommen werden. Daraus resultierende mögliche Maßnahmen, wie Redundanz- und Resilienz-Konzepte, sowie sich gegebenenfalls selbst wieder funktional reparierende Wiederherstellungsprozesse sind ebenfalls in Abhängigkeit der Bewertung von Kritikalität von betroffenen Prozessketten umzusetzen.

4.4 Absicherungsmaßnahmen

Ab wann eine unternehmensübergreifende Kommunikation als sicher gilt, hängt stark von den Schutzanforderungen und den auszutauschenden Informationen ab.

4.4.1 Klassifizierung als ständiger Prozess

Die Regeln zur späteren Verwendung von Informationen, also die Klassifizierung im Allgemeinen, entstammen üblicherweise direkt unternehmensinternen Katalogen oder auch indirekt bereits bestehenden Verträgen. Sie werden durch externe Regelwerke, wie zum Beispiel nationale gesetzliche Grundlagen oder internationale Standards und Abkommen, definiert. Die Klassifizierung stellt auch eine **regelmäßige** Aufgabe dar – auf Grundlage individueller Einschätzungen von Informationserstellern selbst, um etwa den IP-Schutz zu gewährleisten (patentrechtliche, wettbewerbsrechtliche Auswirkungen). Die korrekte Anwendung einheitlicher Klassifizierungs-Metriken innerhalb der Unternehmen führt letztlich zu einer konsistenten unternehmens**internen** Dokumentenlage. Dieser Vorgang ist folglich auch bei automatisierten Prozessen vorzusehen (Produktionsdaten, Rezepturen).

4.4.2 Feststellung des Schutzbedarfs

Eine grundlegende Maßnahme ist es, die Schutzwürdigkeit durch eine Risikobewertung zu bestimmen. Es ist die Frage zu beantworten, wie groß der entstandene Schaden innerhalb eines Unternehmens wäre, wenn im Falle eines Sicherheitsvorfalles zum Beispiel bestimmte Typen von Daten gestohlen, manipuliert oder Produktionsprozesse verändert würden.

Für die Risikoabwägung ist eine Klassifizierung der kritischen Unternehmenswerte (Systeme, Datenblätter, Pläne, Rezepte, Marketinginformationen) sinnvoll beziehungsweise erforderlich. Diese soll Auskunft darüber geben, inwiefern diese mit anderen (zum Beispiel Partnerunternehmen) austauschbar sind oder nur intern zur Verfügung stehen dürfen.

Um unternehmensübergreifend bezüglich der Klassifizierung interoperabel zu sein und Missverständnissen vorzubeugen, ist eine unternehmensübergreifende, einheitliche Klassifikation zu fordern. Ein Vorschlag für ein einheitliches und einfaches Klassifikationsschema ist:

- Keine Schutzmaßnahmen: **Öffentlich**
- Mittlere Schutzwürdigkeit:
  Vertraulich Geschäftspartner
  (neuartig bei Industrie 4.0-Szenarien)
- Hohe Schutzwürdigkeit:
  Vertraulich intern

Eine detailliertere Betrachtung von Schutzbedarfen und Klassifikationen befindet sich in Abschnitt 4.5.

4.4.3 Tragweite von Schutzmaßnahmen

Sind im klassischen IT-Bereich Standards (ISO 2700x, BSI-Grundschutz) etabliert, so gelten diese für die Produktionsinfrastrukturen nur eingeschränkt (vergleiche hierzu ISO 27002 mit 27019). Folgende Übersicht dient einem ersten Überblick der bei Industrie 4.0 zu erwartenden Schutzbereiche.

Sicherheitseigenschaften beteiligter Komponenten und Netzwerk-Entitäten: Dies setzt zunächst das Vorhandensein dokumentierter Sicherheitseigenschaften voraus. Primär ist das die Aufgabe des Herstellers. Diese Eigenschaften müssen nun maschinen- und gegebenenfalls unternehmensübergreifend sicher ausgetauscht und gegenseitig konsolidiert werden. Hierbei sollte jedes Unternehmen seine Mindestanforderungen für den Informationsaustausch definieren können. Auf dieser Mindestbasis erfolgt dann eine Einigung auf das akzeptierte Sicherheitsniveau. Der Austausch und – sofern automatisiert – die Aushandlung müssen dabei nachweisbar und jederzeit auf Plausibilität prüfbar bleiben.

Informationen zum einerseits gewünschten, andererseits unterstützten Sicherheitsniveau zwischen der Angebots- und Nachfrageseite müssen gegebenenfalls vertraulich ausgehandelt werden. Das betrifft horizontal/vertikal verbundene Unternehmen wie etwa Maschinen-Lieferant, Kunden, Zulieferer, Betreiber. Hierbei sollte berücksichtigt werden, dass bei automatisierter Aushandlung auch die vertrauliche Behandlung zu Dokumentationszwecken nachweisbar und nachvollziehbar bleiben muss (siehe Abschnitt 4.4.4).

Ein wichtiger Aspekt von Industrie 4.0 ist die Resilienz. Die beteiligten Komponenten sollten robust gegenüber (ungezielten) menschlichen Fehlern und (gezielter) Sabotage sein. So sollte etwa die falsche Parametrisierung einer Maschine nicht möglich sein. Vor der Verarbeitung von kritischen Steuerbefehlen, wie zum Beispiel dem aktiven Setzen eines Geschwindigkeitsparameters für eine Motorsteuerung, könnte eine Plausibilitätsprüfung seitens der Komponente vorgenommen werden. Die Herausforderung hierbei ist, den Raum plausibler Parameter zu erkennen. Die Robustheit von Netzwerkkomponenten wird klassischerweise durch redundante Netzwerktechnik erreicht, bei der eine Umschaltung erfolgt, wenn eine Route ausfällt. Ob und in welcher Ausprägung eine redundante Auslegung wirtschaftlich sinnvoll ist, muss von der Risikobewertung abhängig gemacht werden.

Akzeptiert man den Umstand, dass unbekannte, fortschrittliche und häufig gezielte Angriffe erst erkannt werden, wenn sie erfolgreich waren (siehe Trojaner Stuxnet oder BlackEnergy oder die IT-Angriffe auf die ukrainische Stromversorgung), sollten Unternehmen die kontinuierliche Überwachung (Monitoring) in Betracht ziehen. Bei höherem Sicherheitsreifegrad kann dies um automatisierte Korrelationen von Sicherheitsmeldungen über System- und Unternehmensgrenzen hinweg erweitert werden. Der Markt für Expertensysteme zur Angriffserkennung ist im industriellen Umfeld derzeit noch auf wenige Unternehmen beschränkt. Ein weiterer Sicherheitsaspekt moderner Netzwerküberwachungs- und Alarmierungssysteme (SIEM) liegt darin, dass sie auch nachträglich forensische Analysen über etwa fehlerhafte Steuerbefehle durchführen können. Somit kann vermieden werden, dass ein Sicherheitsbruch zwar erkannt, jedoch der Vorgang der Unterwanderung der Systeme nicht nachvollzogen werden kann. Sollte die Nachvollziehbarkeit nicht möglich sein und dadurch die Schwachstellen und der Angriffspfad, über die ein Angriff erfolgte, nicht gefunden werden, kann nicht davon ausgegangen werden, dass der Angreifer erfolgreich entfernt wurde. In diesem Fall kann es zu einem notwendigen Austausch aller Komponenten kommen, was insbesondere in Maschinennetzwerken zu massiven Kosten führen kann, die weit über die heute bekannten Fälle SONY-PSN und Bundestags-Hack hinausgehen.

Im Allgemeinen ist zu empfehlen, sich kontinuierlich über aktuelle Schwachstellen und Angriffsverfahren zu informieren. Dies setzt das Vorhandensein eines Registers eingesetzter Komponenten, einer Asset-Datenbank, voraus.

4.4.4 Nachvollziehbarkeit/Überprüfbarkeit

Die Fähigkeit eines Unternehmens, angemessene Sicherheitsmaßnahmen zu etablieren, ist ein Aspekt. Diese auch nachweisbar zu halten, ist eine weitere Herausforderung. Es gilt: Etablierte Sicherheitsmaßnahmen sollten dem Risiko angemessen sein und dem allgemein üblichen Umfang entsprechen (siehe zum Beispiel IT-Sicherheitskatalog (5), IT-Sicherheitsgesetz (6)). Deren Durchführung sollte dokumentiert sein. Dies stellt Unternehmen vor Herausforderungen, da der angemessene und übliche Umfang von verschiedenen Faktoren abhängt: der Branche, in dem sich das Unternehmen bewegt, von eventuell vorhandenen regulatorischen Anforderungen und nicht zuletzt vom organisatorischen Reifegrad (das heißt den zur Verfügung stehenden Möglichkeiten) des Unternehmens/der Partnerunternehmen. Um auf aktuelle Bedrohungslagen reagieren zu können, ist zudem die Kenntnis aktueller, öffentlich zugänglicher und ausreichend dokumentierter Sicherheitsbrüche erforderlich.

Bei zunehmender unternehmensübergreifender Wertschöpfung dürfte die Notwendigkeit der Nachweisbarkeit etwa im Rahmen von Audits zunehmen. Es handelt sich hierbei primär um eine sinnvolle Vorsorgemaßnahme: Mittels regelmäßiger Dokumentation ist eine Ableitung der organisatorischen Fähigkeiten möglich. Doch auch nach einem Sicherheitsbruch kann diese Dokumentation hilfreich sein. So kann mit ihrer Hilfe nachgewiesen werden, dass alle erforderlichen Gefahren angemessen berücksichtigt wurden und die entsprechenden Prozesse auch eingehalten werden. Daneben sind solche Nachweispflichten (je nach Reifegrad) auch intern – etwa für die Revision – von Bedeutung: Sie machen eine Überprüfung möglich, ob Sicherheitsmaßnahmen eingehalten wurden.

Die Dokumentation besteht aus zwei Bereichen: Zum einen führt sie Maßnahmen auf, die Nachweise zu einer aktuellen Richtlinie/Handlungsanweisung beschreiben. Zum anderen weist sie nach, dass die darin enthaltenen Schritte auch

regelmäßig erfolgen. Dabei kann es sich sowohl um organisatorische wie auch technische Maßnahmen handeln.

Eine besondere Herausforderung besteht hier im Zielkonflikt zwischen der Nachweisbarkeit sowie Analysefähigkeit auf der einen sowie der etwaigen Verschlüsselung auf der anderen Seite. Der Bedarf, vertrauliche Kommunikation zu verschlüsseln, kann dazu führen, dass die Analysefähigkeit beeinträchtigt wird. Denn verschlüsselte Daten lassen sich in der Regel nicht auswerten. Unternehmen sind daher vor dem Einsatz von Verschlüsselungstechniken gut beraten, die Konsequenzen daraus, speziell eine unter Umständen eingeschränkte, nachträgliche Sicherheitsanalyse, zu berücksichtigen. Auch hier gilt: Die Entscheidung „Verschlüsselung versus Nachvollziehbarkeit“ sollte im Rahmen einer Risikobetrachtung erfolgen.

4.5 Schutzbedarf und Klassifizierung kritischer Unternehmenswerte

4.5.1 Bestimmung der Schutzwürdigkeit

Eine grundlegende Maßnahme ist die Bestimmung der Schutzwürdigkeit. Dies kann in Form einer Risikobewertung erfolgen. Hierbei steht die Frage im Vordergrund, welche Sicherheitsvorfälle möglich und wahrscheinlich sind und ob – und wenn ja, welche – Sicherheitsanforderungen definiert und zu erfüllen sind. Bei der Bewertung des Schutzumfangs sollten sowohl die Fachabteilung wie auch der Daten- und Diensteigentümer hinzugezogen werden. Die Klassifizierung von Daten und Diensten sollte dabei einen Einfluss auf die Art und den Umfang der Schutzmaßnahmen haben.

4.5.2 Klassifizierung der kritischen Unternehmenswerte

Die Klassifizierung von Dokumenten und Produktionsdaten folgt der Überlegung, welcher konkrete Schutzbedarf sich für einzelne Informationen aufgrund der vorgenannten Regelwerke (siehe Abschnitt 4.4.2) ergibt. Die Mindesteinteilung sollte grundsätzlich in die Klassen „Vertraulich“ und „Öffentlich“ möglich sein. Öffentlich bedeutet in diesem Sinne uneingeschränkter öffentlicher Zugriff (zum Beispiel Produktdatenblatt, Handbuch, Marketinginformationen). Diese Informationen können und sollten per Definition jedem zugänglich gemacht werden können (Open-Data). Die Klasse „Vertraulich“ sollte in jedem Fall weiter unterteilt werden (zum Beispiel „normal“, „hoch“, „sehr hoch“ gemäß BSI Grundschutz) und weiter baumartig in **Schutzbedarfsklassen** unterteilbar sein (etwa rollenbasierte Zugriffsrechte für Entwicklungsabteilungen, Fertigung A, B, C, Leitungsebene).

Diese Art der Klassifizierung verfolgt vornehmlich das Ziel, eine prüfbare und konsistente Umsetzung des Schutzbedarfsniveaus innerhalb eines Unternehmens zu erreichen, um als Grundlage für den nächsten Schritt, der schutzbedarfskonformen unternehmens**übergreifenden** Kommunikation, zu dienen.

4.5.3 Unternehmensübergreifende einheitliche Einstufungen

Aus den genannten Klassifizierungsanforderungen an unternehmens**interne** Informationen wird schnell deutlich, dass auf der Basis einer sicher identifizierten, unternehmens**übergreifenden** Kommunikation die Kataloge zur Klassifizierung allen Teilnehmern innerhalb des Kommunikationsverbunds bekannt sein müssen. Diese Kataloge sind daher vorher zwischen den Beteiligten auszuhandeln. Die konsequente Einhaltung der Einstufung lässt prinzipiell inhaltlich keinen Interpretationsspielraum zu. Sie soll also semantisch eindeutig sein. Die festgelegten Übernahmeverbote zwischen unterschiedlichen Klassifizierungen, die zuvor entsprechend eingestuft wurden, sind unbedingt einzuhalten, um keinen unbeabsichtigten oder subversiv motivierten Wechsel der Informationen in eine andere Schutzbedarfsklasse zu ermöglichen. Eine verbreitete Maßnahme zur Einhaltung dieser Art von Schutzzielen basiert auf dem Einsatz von „Digital-Rights-Management-Technologien“ (DRM). Speicherungsverbote außerhalb betreffender Geschäftsprozesse sind strikt einzuhalten. Entsprechend einheitliche Einstufungen und Einhaltung der Vorgaben innerhalb der Prozesse stellen eine regelmäßige Aufgabe dar.

4.5.4 Neue Chancen durch Koexistenz der Schutzbedarfsklassen „Öffentlich“ und „Vertraulich“

Informationen, die zum Beispiel von Common Creative-Lizenzen bereits „Öffentlich“ klassifiziert und öffentlich verfügbar sind, haben ihre Wirkungen im Markt bereits entfaltet und sind zunehmend bedeutsam. Sie haben ihren festen Platz **neben** den als „Vertraulich“ klassifizierten Informationen eingenommen und können in gemeinsamen Produktionsprozessen vorkommen. In diesem Sinne stellt die Umsetzung einer **universellen** Strategie der Informationsklassifizierung eine gute Basis der künftigen automatisierten Produktion dar.

4.5.5 Schutzbedarf am Beispiel der Punkt-zu-Punkt-Verbindung zwischen zwei Maschinen

Das Ziel „der autonomen und automatisierten Vernetzung von Produktionsfähigkeiten über die eigenen Fabrikgrenzen hinaus zur Optimierung des Portfolios im Hinblick auf Kunden- und Marktanforderungen“ erfordert besonderes Augenmerk auf erweiterte Kommunikationsformen, um geschäftssichere Prozesse zu sichern und das geistige Eigentum bei der Informationsklassifizierung (IP) zu schützen. Zukünftig ist etwa die Punkt-zu-Punkt-Verbindung der autonomen Maschine-zu-Maschine-Kommunikation mit neuartigem Schutzbedarf zu berücksichtigen.

In Abhängigkeit von der bereits verfügbaren „I4.0-Automationstiefe“ und „I4.0-Readyness“, die der Absicherung einer Punkt-zu-Punkt-Verbindung dient, entsteht der Bedarf nach tragfähigen pragmatischen Geschäftsprozessen, die auch in einer einfachen Variante bereits als „On-Demand-Produktionen“ ohne besonderen Schutzbedarf möglich sind. Dies muss möglich sein, ohne von Beginn an den gesamten komplexen Lösungsansatz beherrschen zu müssen. Die Verhaltensweisen am Markt basieren auf erweiterten Trust-Modellen, die auch einen erweiterten Schutzbedarf berücksichtigen. Es bieten sich zum Beispiel Methoden zur Kommunikation von öffentlich erkennbaren Rankings an, basierend auf den Erfahrungen mit den betreffenden Herstellern.

4.5.6 Erweiterte Kommunikationsformen

Da prinzipiell keine Begrenzungen der Kommunikation innerhalb der Industrie 4.0 existieren, können sich aus den heutigen Unternehmen neue Unternehmensformen mit neuartigen Kommunikationsformen entwickeln. Autonome Maschine-zu-Maschine-Kommunikation ist nicht zwangsläufig auf die autonome Punkt-zu-Punkt-Verbindung zwischen zwei Maschinen in unterschiedlichen Unternehmen reduziert. Diese Kommunikation kann beliebiger Bestandteil künftiger Wallet-Lösungen werden, die nach dem Prinzip bestehender Lösungen aus dem Finanzmarkt vollständig autonom nach Aufträgen suchen, diese verhandeln, abschließen und ausführen. Hiermit wird eine weitere Zielsetzung von Industrie 4.0 möglich: die automatisierte Auslastungssteuerung für individualisierte Standardprodukte.

Viele Effekte aus vollkommen autonomen algorithmischen Businessprozessen sind aus entsprechenden Handelsplätzen der Finanzmärkte bekannt. Künftige erweiterte Kommunikationsformen der Industrie 4.0 erfordern daher entsprechende Sicherungsmaßnahmen, die alle Ebenen der neuen Kommunikation betreffen und sichere Ausführungen insbesondere auf den Ebenen Technik, Business und Recht zulassen. Um auch **sicherheitstechnischen** Anforderungen gegen Angriffe gerecht zu werden, ist die schrittweise Einführung von Industrie 4.0 unter Berücksichtigung entsprechender Sicherheitsvorgaben sinnvoll.

4.5.7 Neuartiger Schutzbedarf

Der effiziente Einsatz von Sicherheitsmaßnahmen erfordert eine risikobasierte Behandlung von Informationen. Der Umfang von Schutzmaßnahmen sollte sich daher daran orientieren, ob eine Information oder ein Dienst schützenswert ist oder nicht. Von pauschalen „Alles ist schützenswert“-Ansätzen ist abzuraten, da diese bedingt durch die damit verbundenen Kosten dazu tendieren, die Wettbewerbsfähigkeit zu senken. Insbesondere bei der Einführung sollten nicht zu viele Klassen definiert werden, um die Maßnahmen handhabbar zu halten. Der Zugriff sollte immer dem „Need-to-Know“-Prinzip unterliegen: Für die Freigabe auf Daten und Dienste ist immer ein Grund erforderlich, der im geschäftlichen Kontext plausibel und nachvollziehbar ist. Im Folgenden werden drei Klassen beschrieben, die in einer ersten Untersuchung innerhalb der Organisation ausreichen könnten: zwei der Klasse „Vertraulich“ und die „Öffentlich“-Klasse:

4.5.7.1 Vertraulich Intern

Höchste Schutzklasse: Daten oder Dienste dürfen nur im eigenen Unternehmen geteilt werden und die Unternehmensgrenzen nicht überschreiten. Hierzu gehören in der Regel vertrauliche Rezepturen oder noch nicht veröffentlichte Patente.

4.5.7.2 Vertraulich Geschäftspartner

Mittlere Schutzklasse: Im Industrie 4.0-Kontext ist der unternehmensübergreifende Austausch von Informationen zwingend erforderlich. Hierbei ist der sachgemäße Umgang – wie auch die Dokumentation der korrekten Behandlung – mit Geschäftsinformationen grundlegend. Dies gilt etwa für den automatischen Austausch von Produktionsinformationen und Legierungen.

Daneben ist es im Maschinenbau durchaus üblich, das Risiko eines Datenverlusts sensibler Produktionsdaten durch Aufteilung über verschiedene Dienstleister zu reduzieren.

Für das Anwendungsszenario relevante Daten dieser Klasse umfassen etwa vertrauliche Fertigungsschritte, -kapazitäten und insbesondere Sicherheitseigenschaften beteiligter Komponenten und Entitäten (also etwa die Fabrik, in der die Komponenten physisch stehen).

4.5.7.3 Öffentlich

Hier ist keine Geheimhaltung erforderlich. Die Informationen und Dienste sind entweder insgesamt nicht schützenswert beziehungsweise gewollt öffentlich verfügbar. Dazu gehören zum Beispiel Maschinen-Bewegungsdaten oder Sensordaten, wenn diese unkritisch bei einer Veröffentlichung sind.

5. Kommunikationspartner

5.1 Agile Kommunikation zwischen Sicherheitsdomänen

Agile Kommunikation bedeutet, dass die Sicherheitsspezifikationen vor dem Kommunikationsaufbau klar sind und von den Kommunikationspartnern akzeptiert und verstanden werden. Erst dann ist ein unbürokratischer und flexibler Austausch von Steuerungs- und Anlagendaten möglich. Insofern bedeutet agile Kommunikation nicht, ohne Verbindungssicherheit zu kommunizieren. Solch ein Vorgehen währt in keinem Netzwerk lange, denn es lädt förmlich zum Missbrauch von sensiblen Steuerungs- und Anlagendaten ein.

Grundlegende Anforderung von Sicherheitsdomänen ist daher die Identifikation und die Authentifizierung von Kommunikationspartnern (Produktionsanlagen). Das Ziel ist es, nur mit identifizierten Nutzern/Anlagen/Komponenten eine Kommunikation aufzubauen, um Vertrauen für den Austausch von Steuerungs- und Anlagendaten zu schaffen. Für die Kommunikation kommen logische Gruppierungen von Kommunikationskanälen (Conduits) zum Einsatz, die zwei oder mehr Zonen beziehungsweise Domains mit gemeinsamen IT-Sicherheitsanforderungen miteinander verbinden.

5.2 Identifikation

Zu Beginn eines Kommunikationsvorgangs müssen sich die beteiligten Parteien identifizieren. In bestehenden Systemen der Industrie 3.0 findet diese Identifikation häufig nur über Adressinformationen statt, zum Beispiel über die IP-Adresse einer Komponente. Benutzer werden teils gar nicht identifiziert, da keine Zugriffskontrolle implementiert wurde oder Zugangsdaten öffentlich zugänglich sind.

Für Industrie 4.0 ist eine sichere Identifikation der beteiligten Parteien essentiell, die entsprechend der Security-Anforderungen konzipiert sein muss, siehe Abschnitt 3.1. Weitergehende Ausführungen zu sicheren Identitäten finden sich im entsprechenden Technischen Überblick (4).

5.2.1 Adressierbarkeit des Kommunikationspartners

Eine der größten Herausforderungen bei der Identifikation des Kommunikationspartners ist die Adressierung. Jede Entität kann mehrere Identitäten haben, die im Laufe des Lebenszyklus hinzukommen oder sich verändern. Bei der Adressierung ist es in einer unternehmensübergreifenden Kommunikation häufig relevant, welche Rolle von einer Entität gerade eingenommen wird. Für die Adressierung muss daher die Abbildung der gerade relevanten Identität unterstützt werden.

Beispiel: Bei der Adressierung einer Maschine durch den Maschinenbauer ist für diesen wahrscheinlich die Identität aus Herstellersicht, zum Beispiel die Seriennummer, wichtig, während für den Betreiber der aktuelle Aufstellungsort oder der Einsatzzweck die Maschine identifiziert.

Eine entsprechende Adressierung könnte im Industrie 4.0-Kontext durch die Verwaltungsschalen (1) geschehen, die diese Informationen in den verschiedenen Lebenszyklen beinhalten können. Neben der reinen Verwaltung der Informationen ist jedoch auch die sichere Integration der Identitätsprüfung in der Verbindungsaushandlung vorzusehen. Dabei könnten verschiedene Wege beschritten werden:

- Die Adressierung erfolgt über die Verwaltungsschale, wobei die gewünschte Identität auf die sichere Identität abgebildet wird, die auf der Entität hinterlegt ist. Wich-

tig ist, dass dann die Abbildungsfunktion durch die Verwaltungsschale mindestens genauso gut gesichert sein muss wie die Identität auf der Entität.

- Die Adressierung erfolgt über die Verwaltungsschale, wobei die gewünschte Identität auch sicher auf der Entität hinterlegt ist. Beim Aushandeln der Verbindung prüfen dann die Kommunikationspartner „Ende-zu-Ende" gegenseitig, ob die Kommunikationspartner die gegenseitigen Anforderungen hinsichtlich Identität und Schutzprofil erfüllen (siehe Abschnitt 5.2.3).

Diese Anforderungen sind im Sinne des Security-by-Design schon bei der Gestaltung der Kommunikationsmechanismen zu berücksichtigen, da eine Nachrüstung kaum möglich ist, wie es im Anhang 11.3 am Beispiel der E-Mail-Kommunikation kurz dargestellt wird.

Es ist daher notwendig, im Protokoll zur Aushandlung der Kommunikationsbeziehung der beteiligten Parteien vorzusehen, dass die Information, welche Identität adressiert werden soll, sicher mit übertragen wird. Im heute gängigen Transportation Layer Security-Konzept (TLS) ist dies bis zu einem bestimmten Punkt durch die „Server Name Indication"-Erweiterung vorgesehen. Für komplexere Identitätsanforderungen ist die Einbindung in die Semantik beim Aushandeln von Kommunikationsbeziehungen vorzusehen (siehe Abschnitt 5.2.3). Alle entsprechenden Eigenschaften und notwendigen Daten, etwa ein digitales Zertifikat zur Bestätigung der Identität, sind Merkmale einer Industrie 4.0-Komponente und somit in der Verwaltungsschale abgebildet.

5.2.2 Rechte und Rollen

Die Erwartungen an die Identität des Kommunikationspartners spiegeln sich entsprechend im Rechte- und Rollenmodell. Auch wenn technische Verbindungen zwischen einzelnen Menschen beziehungsweise Maschinen aufgebaut werden, sind im Wesentlichen die Rollen und die damit verbundenen Rechte von Bedeutung.

Im Fall der Zugriffskontrolle ist hier Role Based Access Control (RBAC) hervorzuheben. Ein Benutzer weist sich hier mit seinen Zugangsdaten aus, zumeist Benutzername und Passwort, und wird entsprechend authentifiziert. Die Autorisierung zu weitergehenden Handlungen erhält der Benutzer dann entsprechend seiner Rolle über eine Rechteverwaltung. Im Fall eines unternehmensübergreifenden Zugriffs entsteht nun die neue Herausforderung, dass sowohl die eben benannte Authentifikation als auch die Rechteverwaltung zwischen den Unternehmen abgestimmt und nach notwendigen Sicherheitsmaßstäben umgesetzt sein muss.

In den unternehmensübergreifenden, dynamischen Wertschöpfungsnetzwerken von Industrie 4.0 wird eine Erweiterung des Rechte- und Rollenverständnisses notwendig. Wenn Industrie 4.0-Komponenten autonom geschäftliche Handlungen über Unternehmensgrenzen hinweg ausführen, müssen auch für diese Komponenten entsprechende standardisierte Festlegungen getroffen werden. Innerhalb von Unternehmen ist dies zumeist durch eine Wertgrenzenrichtlinie geregelt, die einzelne Handlungsspielräume definiert. Im unternehmensübergreifenden Kontext wird die Frage zu klären sein, wie Rechtsverbindlichkeit, die für Personen etwa durch Prokura realisiert werden kann, auf Maschinen abzubilden ist.

5.2.3 Sicherheitsprofil

Zu den Eigenschaften einer Entität gehört beim Aushandeln der Kommunikationsbeziehung nicht nur die relevante Identität, sondern auch das Security-Profil des Partners. Dieses Security-Profil, das jede Industrie 4.0-Komponente aufweisen muss, beschreibt die gegebenenfalls zertifizierten Security-Merkmale und umfasst Eigenschaften wie den eigenen Schutzbedarf, etwa im Fall einer Information, oder die verfügbaren Schutzmechanismen und Bewertung dieser Mechanismen. Im Rahmen der Aushandlung der Industrie 4.0-Kommunikation werden das entsprechende Anforderungsprofil und die verfügbaren Security-Eigenschaften abgeglichen und der Informationsaustausch wird entsprechend des erreichten Security-Niveaus abgebrochen oder auf reduziertem bis vollem Niveau fortgeführt. Hierbei sind nicht nur die einzelnen Industrie 4.0-Komponenten zu betrachten, sondern auch die Betriebsumgebung.

Die folgenden Beispiele sollen dieses Konzept illustrieren:

- In einer noch lieferantengebundenen Variante der auftragsgesteuerten Produktion sollen Daten nur an eine Maschine übertragen werden, wenn diese vom Maschinenbauer X geliefert wurde und vom Betreiber Y betrieben wird.

- In einer flexibleren Variante der auftragsgesteuerten Produktion sollen Daten nur an eine Maschine übertragen werden, die die Vertraulichkeit der Information nach Schutzlevel Z entsprechend einer Baumusterprüfung nach Standard ABCDE gewährleistet und bei einem Betreiber mit hohem Reifegrad installiert ist.

Die technische Umsetzung ist hierbei durchaus herausfordernd. Die Integrität des Kommunikationspartners ist entsprechend den Security-Richtlinien und der Einstufung sicherzustellen. Es reicht zum Beispiel nicht, nur das Sicherheitsprofil zu evaluieren. Durch Implementierung ist sicherzustellen, dass das Sicherheitsprofil auch dem realen Systemzustand entspricht, ein Gerät also nicht kompromittiert ist. Dies könnte auf physischen Schutz des Geräts hinauslaufen, der entweder durch Installation in einer vertrauenswürdigen Umgebung (Organisation), regelmäßige Kontrollen der Unversehrtheit (Prozess) oder technische Maßnahmen (etwa automatisches Löschen beim Öffnen des Geräts) umgesetzt werden muss.

Die Security-Merkmale von Industrie 4.0-Komponenten werden zurzeit ausgearbeitet, stehen zum Zeitpunkt der Veröffentlichung dieses Dokuments aber noch nicht nur Verfügung.

5.2.4 Sicherheitsdomänen

Eine Sicherheitsdomäne beschreibt einen Bereich, in dem einheitliche Sicherheitsrichtlinien gelten beziehungsweise unter einheitlicher Sicherheitsverwaltung stehen. Im Kontext der unternehmensübergreifenden Kommunikation findet der Informationsaustausch zwischen verschiedenen Sicherheitsdomänen statt, so dass die Adressierung und Rechteverwaltung über Sicherheitsprofile erfolgen muss, die zwischen den Kommunikationspartnern abgestimmt sind (siehe Abschnitte 5.2.2 und 5.2.3). Im Kontext agil ausgehandelter Geschäftsbeziehungen wird dies ohne Standardisierung nicht möglich sein, auch wenn die Vertragsfreiheit im Einzelfall natürlich besondere Möglichkeiten eröffnet.

5.2.5 Lebenszyklus

Die Industrie 4.0-Komponenten verändern im Laufe ihres Lebenszyklus ihre Merkmale, was sich unter anderem in sich ändernden Identitäten oder Sicherheitsprofilen ausdrückt. Neben der Inbetriebnahme mit der initialen Konfiguration und Parametrierung ist der normale Betrieb ebenso zu unterstützen wie der Austausch und die Außerbetriebnahme.

In den agilen Produktionsstätten der Industrie 4.0 können sich die Aufgaben einer Industrie 4.0-Komponente schnell verändern. Eine wesentliche Rolle hierbei spielt die Adressierung, siehe Abschnitt 5.2.1. Der Lebenszyklus der Identitäten ist im Technischen Überblick Sichere Identitäten (4) im Bereich Identity Management beschrieben.

5.2.6 Semantische Entitäten

Produktive Industrie 4.0-Szenarien sind ständigen Änderungen unterworfen. Zum Beispel können neue Produktionsschritte mit Hilfe weiterer Maschinen eingeführt werden, Produktionsmaschinen müssen ausgetauscht oder kurzfristig temporär ersetzt werden, weil sie defekt oder abgeschrieben sind. Eine Herausforderung für den Prozess besteht hierbei in der Robustheit des Produktionsprozesses, das heißt, er muss trotz beziehungsweise inklusive der notwendigen Sicherheitsbetrachtungen jederzeit weiterlaufen oder nur kurzen Unterbrechungen unterworfen sein. Ein fliegender Austausch von Produktionsmaschinen ist daher mit einer vollautomatisierten Einrichtung der Sicherheitsattribute und deren Einbindung in das jeweilige Szenario verbunden.

Um das Lifecycle-Management des Produktionsprozesses zu vereinfachen, ist die Einführung semantischer Entitäten sinnvoll. Die semantische Entität besteht im Wesentlichen aus einem semantisch interpretierbaren Namen für die Maschine oder den Produktionsschritt (zum Beispiel Schuhsohlenverklebungseinheit) sowie deren zugeordneten technischen Parameter (zum Beispiel IP-Adresse, MAC-Adresse, Maschinen-Nummer, Werk, Platz, Reihe etc.). Über den semantisch interpretierbaren Namen erfolgt die vollständige Adressierung der Maschine, sowohl zum Einrichtungszeitpunkt als auch während des Produktionsprozesses. Ein Austausch der Maschine und die Einbindung einer Ersatzmaschine würden dadurch erfolgen, indem der vorhandene semantische Namen übernommen und neue aktuell aktive technische Parameter zugeordnet werden. Dadurch blieben der Produktionsprozess und die zugehörigen semantischen Entitäten auch bei größeren Umbauten stabil, leicht zu verwalten und hochflexibel.

6. Ausgewählte rechtliche Aspekte

An dieser Stelle sollen wenige ausgewählte allgemeine Hinweise die Sensibilisierung verstärken, dass bisher bekannte rechtliche Anforderungen auch weiterhin künftig zu bedenken sind. Nähere Überlegungen und auch Diskussionen zur Haftung oder Rechtsverbindlichkeit (siehe Abschnitt 5.2.2) bei Maschine-zu-Maschine-Kommunikation erfolgen in der Arbeitsgruppe „Recht“ der Plattform Industrie 4.0.

- **Datenschutz**
  Im Bereich Industrie 4.0 kann das bis 2018 weiterhin geltende deutsche Datenschutzrecht zur Anwendung kommen, auch dann, wenn „lediglich“ Maschine-zu-Maschine-Kommunikation ausgeführt wird. Der entsprechende Schutzbedarf, wie zum Beispiel Vertraulichkeit, ist beim autonomen Austausch personenbezogener Daten zwischen Maschinen weiter zu berücksichtigen. Ab 2018 setzt die Europäische Datenschutzgrundverordnung zusammen mit nationalen Ergänzungen die neuen Vorgaben – immer in Verbindung mit dem dann jeweils geltenden nationalen Recht der Mitgliedsstaaten. Im Wesentlichen soll dieses Konstrukt jedoch heutiges Recht weitgehend widerspiegeln. Im Falle von Industrie 4.0-Produktionen über Ländergrenzen hinweg gelten künftig neben der Europäischen Datenschutzgrundverordnung die jeweiligen nationalen Ergänzungen.

- **Wettbewerbsrecht**
  Im Zusammenhang mit Implementierungen von Sicherheitstechnologie für sichere Kommunikation und sichere Identitäten für Industrie 4.0 bestehen weitreichende Möglichkeiten von wettbewerbsrechtlichen Einschränkungen durch die Anwendung von Technik und Organisation.
  Beispielhaft sei erwähnt, dass **branchenspezifische Vertrauensdienste**, die bestimmten Herstellern oder Zulieferern die erforderlichen „Unbedenklichkeitsbestätigungen“ in Form von elektronischen Zertifikaten für die vertrauensvolle Kommunikation erteilen, unmittelbar in den Markt eingreifen können – durch Entzug oder Nichterteilung von Zertifikaten. Heutige, branchenspezifische Best-Practice-Lösungen setzen auf gewachsene Vertrauensmodelle, die in künftige Industrie 4.0-Vertrauensmodelle diskriminierungsfrei umzusetzen sind.

- **Sabotageschutz**
  Für bewusste Wettbewerbseinschränkungen kommen üblicherweise subversive Techniken zum Einsatz, die es zu erkennen und zu verhindern gilt. Aus diesem Grund kommen gewöhnlich – aus ökonomischer Sicht minimalinvasive – technische Verfahren zum Einsatz, um die Kommunikation zu schützen. Diese Gefahren bedürfen aber auch der rechtlichen Betrachtung. Es muss daher fallspezifisch entschieden werden, inwieweit Sicherheitsbehörden über die einzusetzenden Technologien und Kommunikationslösungen einzubinden sind. Der Bereich Industrie 4.0 kann auch aus nationaler Sicht sicherheitsrelevant sein und betrifft in jedem Fall Anbieter kritischer Infrastrukturen, die in Industrie 4.0-Prozesse eingebunden sind.

7. Handlungsempfehlungen

Aus den vorangegangenen Darstellungen ergeben sich Empfehlungen für die Einbettung sicherer Kommunikation in die Einführung von Industrie 4.0.

7.1 Verlässliche Kommunikationswege

Wesentliche Elemente von Industrie 4.0 sind die agile Bildung von Wertschöpfungsnetzwerken und die Realisierung von Diensten unter Verwendung privater und öffentlicher Cloud-Infrastrukturen. Um teilnehmen zu können, müssen Unternehmen Zugriff auf verlässliche Internetanbindungen haben. Dabei ist die notwendige Bandbreite nicht nur auf dem Papier bereitzustellen, sondern auch zu garantieren. Verfügbarkeitszusagen müssen möglich sein, siehe Abschnitt 4.3.

7.2 Sichere Identitäten

Basis für alle sicheren Kommunikationsprozesse sind die sichere Identifikation des Kommunikationspartners und die sichere Aushandlung der Security-Profile, siehe Abschnitt 5.2. Im technischen Überblick Sichere Identitäten (4) werden Anforderungen und technische Konzepte diskutiert.

7.3 Aushandlung von Sicherheitsprofilen

Ein wesentlicher Aspekt beim Informationsaustausch ist die Gewährleistung der Informationssicherheit. Hierzu müssen die Kommunikationspartner ihre Sicherheitsprofile beim Aushandeln der Kommunikationsbeziehung austauschen können. Dies muss in den Kommunikationsprotokollen berücksichtigt werden, siehe Abschnitt 5.2.3. Das Sicherheitsprofil wird zu einem wesentlichen Merkmal einer Industrie 4.0-Komponente.

7.4 Technische Unterstützung der Informationsklassifizierung

Informationen, die zwischen Kommunikationspartnern ausgetauscht werden, benötigen eine Einstufung entsprechend einer Informationsklassifizierung, siehe Abschnitt 4.5. Für den automatisierten Informationsaustausch in der Industrie 4.0 muss die Einstufung technisch unterstützt werden, indem sie in der Information (etwa einem Dokument), sicher aber in der dazugehörigen Verwaltungsschale abgebildet wird. Zur technischen Umsetzung des Schutzes wird digitales Rechtemanagement (DRM) relevant, siehe Abschnitt 4.5.3.

8. Zusammenfassung und Ausblick

Der Inhalt dieses Dokuments spiegelt den Arbeitsstand der Arbeitsgruppe „Sicherheit vernetzter Systeme“ der Plattform Industrie 4.0 zur Hannover Messe 2016 als Zwischenergebnis wider. Ausgehend von den zu schützenden Unternehmenswerten werden sichere unternehmensübergreifende Kommunikationsbeziehungen dargestellt und erste Handlungsempfehlungen abgeleitet.

Die Arbeiten werden fortgeführt. Hierbei werden die vorliegenden Erkenntnisse ausgebaut und vertieft. Weitere Themen wie die Überwachung des Informationsflusses und daraus abgeleitete Reaktionsmaßnahmen auf Sicherheitsvorfälle werden zusätzlich ausgearbeitet.

9. Abbildungsverzeichnis

10. Literaturverzeichnis

1. *Umsetzungsstrategie Industrie 4.0.* Berlin/Frankfurt: Plattform Industrie 4.0, 2015.

2. *Referenzarchitekturmodell Industrie 4.0* (RAMI4.0). DIN SPEC 91345.

3. *Die Lage der IT-Sicherheit in Deutschland 2014*. Bonn: BSI, 2014.

4. *Technischer Überblick „Sichere Identitäten“.* Berlin: Plattform Industrie 4.0, 2016.

5. *IT-Sicherheitskatalog gemäß §11 Absatz 1a Energiewirtschaftsgesetz*. Bonn: Bundesnetzagentur, 2015.

6. *Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme.* IT-Sicherheitsgesetz, 2015.

7. *VERORDNUNG (EU) Nr. 910/2014 DES EUROPÄISCHEN PARLAMENTS UND DES RATES* vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG. eIDAS-Verordnung.

11. Anhang

11.1 OSI 7-Schichtenmodell

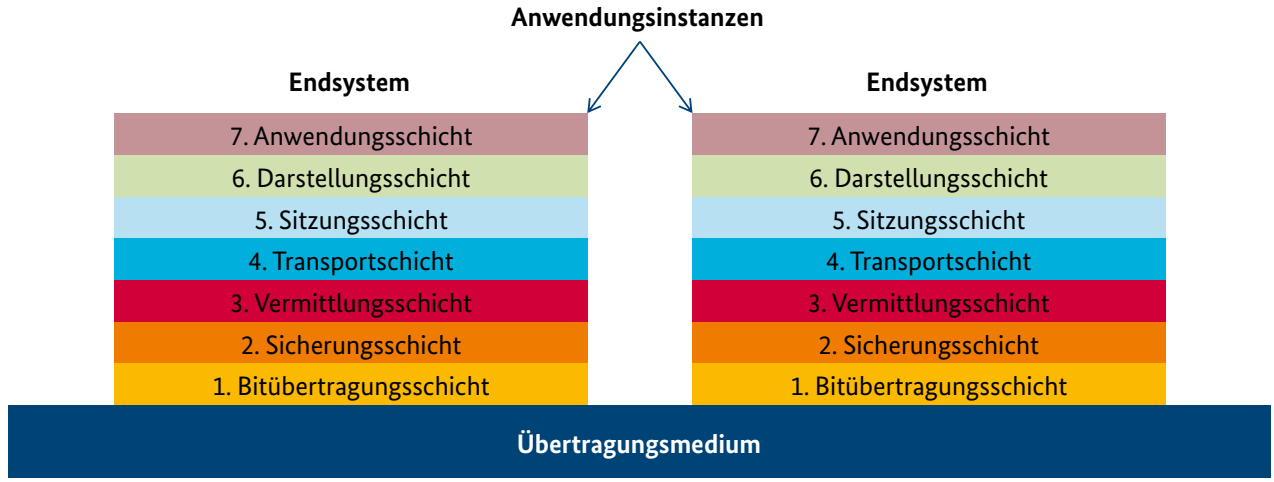
Das OSI 7-Schichtenmodell beschreibt Ebenen, die für einen erfolgreichen Kommunikationsvorgang zwischen Applikationen durchlaufen werden. Für jede Schicht stehen unterschiedliche technische Implementierungen zur Verfügung, die auf den jeweils anderen Schichten nicht relevant sind. So kann eine Applikation über kurze oder lange Strecken, drahtgebunden oder drahtlos kommunizieren, ohne die technischen Details berücksichtigen zu müssen.

11.2 Anwendungsszenario S1 der Plattform Industrie 4.0: Auftragsgesteuerte Produktion

Um die Anforderungen und Lösungen für Industrie 4.0 bewerten zu können, wurden von der Arbeitsgruppe „Forschung“ der Plattform Industrie 4.0 mehrere Anwendungsszenarien ausgearbeitet. Im Rahmen der Arbeiten zum Thema „Sichere unternehmensübergreifende Kommunikation“ wurde auf das Anwendungsszenario „Auftragsgesteuerte Produktion“ zurückgegriffen.

Die auftragsgesteuerte Produktion basiert im Wesentlichen auf standardisierten Prozessschritten und der Fähigkeit der Selbstbeschreibung von Fähigkeiten der Produktionsmittel. Das kann beispielsweise bedeuten, dass eine Bohrmaschine weitergeben kann, in welchem Material welche Größe von Bohrungen mit ihr möglich sind. Durch die Standardisierung ist es möglich, die digitale Produktentwicklung mit der automatisierten Auftragsplanung, -vergabe und -steuerung zur Einbindung aller benötigten Fertigungsschritte und Produktionsmittel zu verbinden. Durch diese Art der vernetzten Steuerung können interne Prozessmodule wesentlich flexibler kombiniert werden. Ferner lassen sich über sichere (vertrauenswürdige) Schnittstellen, entsprechend den Anforderungen an Zeit und Qualität, (Partner-) Dienstleistungen in die Produktion einbinden. Sollte die Produktion in Engpässe laufen, kann auf freie Fertigungskapazitäten von weiteren Unternehmen zurückgegriffen werden, um so die Auslastung kurzfristig zu erhöhen. Die Zulieferer werden durch neue Transportintelligenz (direkte Steuerungsinformation aus der Produktion und Wetterdiensten) in die Lage versetzt, zu bestimmen, welche Art der Logistik (Schiene, Straße oder Luft zum Beispiel über Drohnen) nötig ist, um Liefertermine zu halten.

Abbildung 3: OSI 7-Schichtenmodell



Im Kontext dieses Dokuments sind nur die obersten Schichten relevant.

Quelle: Plattform Industrie 4.0

Ziel ist es, die Einbindung von externen Produktionsstätten und Partnern in den Produktionsablauf zielgerichtet, effektiver und selbstständig ablaufen zu lassen. Die notwendige Auftragsvergabe kann über standardisierte Schnittstellen und Vertrauensstellungen weitgehend automatisiert durchgeführt werden. Produzierende Unternehmen fokussieren sich somit nur noch auf die Wertschöpfungsschritte, mit denen sie sich am Markt deutlich von den Wettbewerbern abgrenzen.

11.3 Sichere Kommunikation zwischen Mailservern

Als Beispiel für schlecht konzipierte agile Kommunikation wird der Austausch von E-Mails zwischen Mailservern erläutert. Als der Austausch von E-Mails über das Internet in den 1980er Jahren konzipiert wurde, war sichere Kommunikation noch nicht relevant.

Soll eine E-Mail von einer Domäne zu einer anderen Domäne verschickt werden, wird über den Domain Name Service (DNS) der zuständige Mailserver (Mail Exchange MX) ermittelt und die E-Mail an den benannten Mailserver zugestellt, der die E-Mail dann direkt ausliefert oder weitervermittelt.

Um diesen Prozess sicher zu gestalten, kann der Transfer zwischen den Mailservern verschlüsselt erfolgen, wie in RFC2487 beschrieben, der die Verwendung von Transportation Layer Security (TLS) für das Simple Mail Transfer Protocol (SMTP) beschreibt. Dieses Konzept konnte sich in der Praxis nie durchsetzen, da im Protokoll keine Methode vorgesehen war, anhand welchen Merkmals beim Verbindungsaufbau geprüft werden soll, ob der empfangende Mailserver zum Empfang der E-Mail berechtigt ist. Auch ist die Unterstützung multipler Identitäten im TLS-Protokoll nicht optimal. Die STARTTLS-Erweiterung wurde daher in der Praxis lediglich für sicheren Zugang vom Client zum eindeutig konfigurierten Mailserver verwendet. Zur Lösung dieses Problems wurde über 15 Jahre später DNS-Based Authentication of Named Entities (DANE) für SMTP mit RFC7672 veröffentlicht, welches zusätzlich Secure DNS (DNSSEC) benötigt.

AUTOREN DER AG SICHERHEIT VERNETZTER SYSTEME:

Ulf Feger, HUAWEI TECHNOLOGIES Deutschland GmbH | Dr. Lutz Jänicke (Leitung), PHOENIX CONTACT Cyber Security AG | Michael Jochem, Bosch Rexroth AG | Marcel Kisch, IBM Deutschland GmbH | Michael Krammel, Koramis GmbH | Jens Mehrfeld, Bundesamt für Sicherheit in der Informationstechnik | Torsten Nitschke, PHOENIX CONTACT Software GmbH | Michael Sandner, Volkswagen AG | Dr. Michael Schmitt, SAP SE | Andreas Teuscher, SICK AG | Thomas Walloschke, Fujitsu Technology Solutions GmbH

Diese Publikation ist ein Ergebnis der AG Sicherheit vernetzter Systeme (Plattform Industrie 4.0).

www.plattform-i40.de