MASTERARBEIT

EINSATZ VON IOT-GERÄTEN IN UNTERNEHMEN

Identifikation und Beherrschbarkeit von entstehenden Risiken

ausgeführt am

Studiengang

Informationstechnologien und Wirtschaftsinformatik

Von: Philipp Rammer

Personenkennzeichen: 1710320022

Graz, am 12. Juli 2019 .....

Unterschrift

EHRENWÖRTLICHE ERKLÄRUNG

Ich erkläre ehrenwörtlich, dass ich die vorliegende Arbeit selbstständig und ohne fremde Hilfe verfasst, andere als die angegebenen Quellen nicht benützt und die benutzten Quellen wörtlich zitiert sowie inhaltlich entnommene Stellen als solche kenntlich gemacht habe.

.....

Unterschrift

DANKSAGUNG

Ich bedanke mich besonders bei meinen Freunden und Mitbewohnern Martina und Moe, die es in den letzten Wochen und Monaten nicht ganz leicht mit einem nachtaktiven, mürrischen Studenten hatten.

Für die Unterstützung während dieser Nachtschichten gilt ein weiterer Dank den Getränken MAKAvA und Club-Mate. Ohne diese Unterstützung wäre es wesentlich schwieriger gewesen.

Ein Dank gilt auch meinem Masterarbeitsbetreuer Christian Schmid für seine Geduld, Flexibilität und besonders den Vorschlag des Themas, aus welchem durch die intensive Beschäftigung damit auf jeden Fall ein persönlicher Erkenntnisgewinn hervorgeht: So schnell kommt mir kein IoT-Gerät in die Wohnung.

Aus Sicherheitsgründen.

KURZFASSUNG

Thema der vorliegenden Masterarbeit ist die Betrachtung von Aspekten der Informationssicherheit beim Einsatz von Geräten aus dem Kontext des Internet of Things (IoT) in Unternehmensnetzwerken. Medienberichte und Analysen der letzten Jahre deuten auf frappierende Sicherheitslücken in IoT-Geräten und damit einer, durch die unabhängig davon zunehmende Bedrohungslage im Internet verschärften, Gefährdung der Sicherheit hin. Eine Frage, die sich dabei stellt, ist, ob vorhandene Sicherheitskonzepte für den Einsatz von IoT-Geräten ausreichend sind. Um dies zu beantworten war es notwendig, eine für die Arbeit gültige Definition des sehr abstrakten Begriffs "IoT" zu entwickeln und mögliche Anwendungsbereiche in Unternehmensnetzwerken aufzuzeigen. Darauf folgt eine Beschreibung der grundlegenden Aspekte der Informationssicherheit (Vertraulichkeit, Integrität und Verfügbarkeit) und eine Analyse von Bedrohungen und Angriffen auf Netzwerke. Ausgehend von diesen Erkenntnissen wurde ein Sicherheitskonzept zusammengestellt, welches heute übliche Maßnahmen zur Sicherstellung der Informationssicherheit in Unternehmensnetzwerken beinhaltet. Um ein Konzept unter Berücksichtigung des Einsatzes von IoT-Geräten entwickeln und mit derzeitigen Maßnahmen zu vergleichen, wurden IoT-spezifische Rahmenbedingungen und Angriffe beschrieben. Dabei zeigen sich vor allem Einschränkungen hinsichtlich technischer Ressourcen, Anforderungen an die Skalierbarkeit von Lösungen sowie eigene Angriffsszenarien. Unter Zuhilfenahme von Standards zur Sicherstellung von Informationssicherheit wurde davon ausgehend ein Katalog von erkannten IoT-bezogenen Risiken zusammengestellt. Darauf basiert das vorgeschlagene, verbesserte Modell, welches organisatorische, applikationsbezogene und technische Maßnahmen zur Behandlung dieser Risiken beinhaltet. Dabei zeigt sich, dass nur Teile davon überhaupt durch Weiterentwicklung bestehender Sicherheitsmaßnahmen realisiert werden können, einige Ansätze jedoch neuartig sind und eine Veränderung der Sicherheitsarchitektur in einem Unternehmen notwendig wird. In der Praxis werden dabei insbesondere Mechanismen zur Authentifizierung, Autorisierung und der Sicherstellung des Datenschutzes zur Herausforderung, da dazu derzeit keine universell realisierbaren Konzepte vorliegen. Entsprechend dieser Erkenntnisse ist davon auszugehen, dass heute übliche Maßnahmen zur Sicherstellung der Informationssicherheit nicht ausreichend für einen IoT-Anwendungsfall sind.

ABSTRACT

Recent and current media coverage as well as studies describe an alarming picture of the state of security in the Internet of Things (IoT). Prevalent vulnerabilities result in a comprehensive threat landscape, affecting information security in many aspects. This thesis aims to determine whether existing security models can cover security risks arising with the use of IoT devices in an enterprise network or new controls are necessary. As IoT is a very abstract term, exploring and defining an idea of this concept is the first step, followed by the identification and specification of the objectives of information security, which are confidentiality, integrity and availability. Attackers are permanently targeting computer networks, so enterprises need to implement suitable measures to protect data and information. A recapitulation of these procedures show that they consist of organizational, application specific and technical elements. Analyzing frame conditions of IoT devices infer, that new weak points and limitations must be considered when targeting IoT security. The application of a risk management process in this context, based on standards and best-practice approaches, reveals new IoT specific risks that need to be treated. The subsequent design of an adapted security model, consisting of controls in the identified scopes of application, shows that some of the existing measures can be extended to the use of IoT. But some issues cannot be covered, so that new approaches need to be applied. The discovered, insufficiently treated key fields are authorization, authentication and data privacy.

INHALTSVERZEICHNIS

1 EINLEITUNG

The S in IoT stands for security.
- Tim Kadlec (@tkadlec)

Liest man dieses Zitat, kommt man möglicherweise kurz ins Grübeln. Ist es im Internet der Dinge (*Internet of Things*, IoT), einem der großen Hype-IT-Themengebiete der letzten Jahre, denn tatsächlich so schlecht um die Sicherheit bestellt? Eine kurze Recherche zu diesem Thema in den Medien liefert jedenfalls kein beruhigendes Bild:

- Datenlecks durch intelligente Glühbirnen (Loeb, 2018).
- Warum Glühlampen das nächste Ziel von Hackern werden (Markoff, 2016).
- Wie Drohnen genutzt werden können, das eigene Heim zu hacken (Thompson, 2015).
- Wie eine Drohne einen Raum voller Glühbirnen von außen hackt (Ricker, 2016).
- Sollte man Angst vor dem eigenen Kühlschrank haben? 70% der populärsten IoT-Geräte sind nicht sicher (Matthews R. , 2017).
- Der intelligente Kühlschrank kann einen töten – die dunkle Seite des IoT (Bhartiya, 2017).
- Ein virtueller Toaster zeigt, wie schnell Dinge gehackt werden können (Limer, 2016).
- IoT-Botnet legt das halbe Internet an der US-Ost- und Westküste lahm (The Hacker News, 2016), (Turton, 2016), (DynDNS, 2016).
- Ganz Liberia durch IoT-Botnetz offline genommen (Matthews L. , 2016).

Gewiss sind diese Artikel schon zwei bis drei Jahre alt. Welche skurrilen Stilblüten die Sicherheitslage im IoT aber in der Zwischenzeit bereits treibt, zeigt sich beispielsweise daran, dass es sich wohlgesinnte Hacker mittlerweile zur Aufgabe gemacht haben, verwundbare IoT-Geräte derart zu infizieren, dass andere Schadsoftware sie nicht mehr übernehmen kann (Coache & Salihoglu, 2018). Auf der anderen Seite schafft es offenbar ein 14jähriger Teenager trotzdem, aus Spaß binnen Stunden tausende IoT-Geräte im Internet lahmzulegen (Petereit & von Westernhagen, 2019). Somit kann nicht davon ausgegangen werden, dass sich die Sicherheitslage in der Zwischenzeit merklich verbessert hat.

Es sei vorweggenommen: Diesem dystopischen und verstörenden Bild kann im Verlauf der vorliegenden Arbeit wenig Positives entgegengesetzt werden. Informationssicherheit ist in vielen Ausprägungen eines der größten Problemfelder des IoT. Warum der Umgang mit Sicherheit in der Informationstechnologie generell schwierig scheint, wird in Bartsch & Frey (2018) folgendermaßen analysiert:

„[...] ob wir als Gesellschaft zu dumm sind für adäquate IT-Sicherheit, die wie Umweltschutz eine nachhaltige Planung und eine Regulierung mit Fingerspitzengefühl benötigt. Dabei arbeiten wir verschiedene Themen heraus, die dazu führen, dass die IT-Sicherheit immer komplexer wird und als vielköpfige, monsterähnliche Hydra wahrgenommen wird, der nach dem Abschlagen eines Kopfes sofort mehrere nachwachsen."
Zur Lage der IT-Sicherheit (Bartsch & Frey, 2018)

Dass die Sicherheit im Bereich der Informationstechnologie, trotz dieser Komplexität und dem offensichtlich mangelhaften Umgang damit, ausgesprochen relevant ist, zeigt die aktuelle Qualität und Quantität von Angriffen auf Systeme. Übliche Ziele dabei sind finanzieller, ökonomischer oder politischer Natur und die Methoden reichen von Spionage bis hin zu Sabotage. Dabei ist eine zunehmende Professionalisierung der Angriffe zu beobachten (Bartsch & Frey, 2018). Welche Dimensionen dies erreicht hat, lässt eine kürzliche veröffentlichte Zahl der Deutschen Telekom nur erahnen. Dort registriert man bis zu 46 Millionen Angriffe – pro Tag. Umso wichtiger scheint es, Unternehmensinfrastruktur bestmöglich zu schützen, denn es entsteht allein in Deutschland der Wirtschaft durch Angriffe auf die Informationssicherheit jährlich ein geschätzter Schaden von 55 Milliarden Euro, wobei im Jahr 2018 70% aller Unternehmen nachweislich von Angriffen betroffen waren (Braun, 2019). Sicherheit ist also ein für Unternehmen relevantes Thema – und ein Teilbereich davon ist die Betrachtung der Sicherheit beim Einsatz von IoT-Geräten.

Bei der Betrachtung des IoT stellt es allgemein ein Problem dar, dass, trotz vieler Versuche und aktiver Forschung in diesem Themenfeld, nicht ganz klar ist, was dieser Begriff „IoT" eigentlich konkret umschreibt und welche sozialen, technischen und wirtschaftlichen Implikationen er hat (Atzori, Iera, & Morabito, 2010). Trotzdem oder gerade deswegen soll im Rahmen dieser Arbeit versucht werden, ein wenig Klarheit über Bedeutung und Anwendungsbereiche zu schaffen.

Wie in der Folge noch dargelegt wird, ist der Einzug von IoT in Unternehmensnetzwerke keine optionale Vorgehensweise. IoT ist Realität, und es stellt sich damit eigentlich nur die Frage, ob ein Unternehmen hinsichtlich der Informationssicherheit dafür gerüstet ist oder nicht. Konkret ist die Frage offen, ob vorhandene Sicherheitsmaßnahmen im Rahmen der Netzwerksicherheit ausreichend sind, um mit durch den Einsatz von IoT-Geräten und -Anwendungen gegebenenfalls auftretenden, identifizierten neuen Risiken umzugehen oder ob neue Ansätze benötigt werden. Zur Beantwortung wird ein Ansatz in starker Anlehnung an die *Soft Systems Theory* (siehe Abbildung 1) gewählt. Das heißt, es werden aus der Problemstellung in der realen Welt wesentliche Anforderungen abstrahiert und eine allgemeine Analyse und Modellierung einer verbesserten Situation durchgeführt, um daraus allenfalls notwendige Maßnahmen zur Verbesserung des Istzustands abzuleiten. Die initiale Problemsituation, Sicherheitsaspekte des IoT, wurde bereits umschrieben und wird in der weiteren Folge auf die Betrachtung von Informationssicherheitsrisiken beim Einsatz von IoT-Geräten in Unternehmensnetzwerkwerken eingeschränkt.

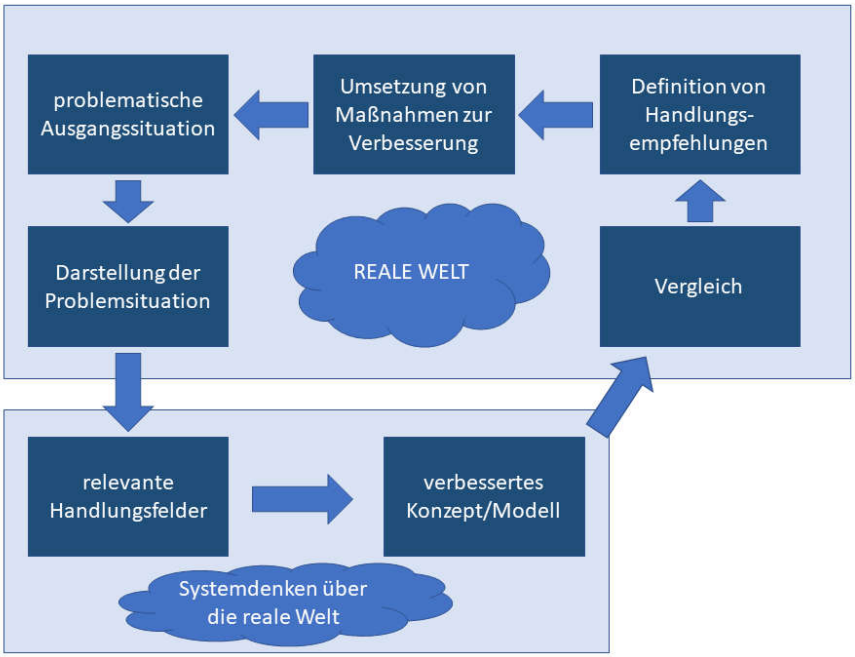

Abbildung 1: Soft Systems Theory als methodischer Leitfaden, nach (Kuhn, 2011)

Um ein besseres Verständnis für die Eigenschaften von IoT und der Problemsituation zu erhalten, werden zuerst einige Begriffsdefinitionen vorgenommen. Der erste Schwerpunkt liegt hierbei auf einer Exploration des Begriffes IoT, um eine Vorstellung von diesem sehr abstrakten Themenfeld zu bekommen. Dazu werden verschiedene Definitionen dieses Begriffs zusammengetragen und gegenübergestellt. Ebenso werden oftmals verwendete Synonyme und Homonyme betrachtet und eine IoT-Architektur sowie Anwendungsbereiche, Einsatzszenarien und einige Beispiele für aktuelle IoT-Geräte aufgezeigt. Ein weiterer Schwerpunkt liegt auf der Bestimmung des Begriffs Informationssicherheit. Dabei werden eine Abgrenzung zum Datenschutz und weiteren, in diesem Umfeld vorkommenden Begriffen vorgenommen sowie die Ziele der Informationssicherheit definiert. In der Folge wird ein Auszug aktueller, in diesem Bereich vorhandener Standards und Vorgehensmodelle beschrieben, auf welche später zurückgegriffen wird.

Um überhaupt Aussagen über die Effektivität vorhandener Sicherheitskonzepte machen zu können und diese mit konzeptionellen Vorschlägen zu vergleichen, wird in Kapitel 3 eine Beschreibung vorhandener Sicherheitsmaßnahmen für Unternehmensnetze durchgeführt. Neben einer Definition des Begriffs Netzwerksicherheit wird auch dargelegt, welche Angriffe überhaupt und durch wen auf Netzwerke ausgeführt werden können und wo die Ursachen für Schwachstellen in diesem Kontext liegen. Danach folgt eine Aufstellung üblicher Sicherheitsmaßnahmen für Unternehmensnetzwerke.

Nun muss identifiziert werden, wo mögliche Handlungsfelder für Verbesserungen liegen. Dabei ergibt sich das Problem, dass im IoT-Umfeld in vielen Bereichen sehr spezielle Rahmenbedingungen gegeben sind, welche die Erstellung eines Modells einschränken. Um entsprechend sinnvolle Ansatzpunkte für Verbesserungen zu finden, werden diese Rahmenbedingungen in Kapitel 4 geschildert. Auch wird dargelegt, welchen speziellen Angriffen IoT-Geräte und -Anwendungen ausgesetzt sind, um entsprechende Maßnahmen ableiten zu können.

Relevante Verbesserungen können nur dann vorgeschlagen werden, wenn bekannt ist, wo gegebenenfalls Schwachstellen in bestehenden Konzepten vorliegen. Um dies zu bestimmen, wird ein risikobasierter Ansatz verwendet. Dieses Vorgehen und eine Analyse von beim Einsatz von IoT entstehenden neuen Risiken werden in Kapitel 5 erläutert bzw. durchgeführt. Diese Analyse basiert auf anerkannten Rahmenwerken der Informationssicherheit im Unternehmensumfeld und auch, da viele Aspekte des IoT sich darin wiederspiegeln, auf Handlungsempfehlungen für die produzierende Industrie.

Auf Basis dieser vorliegenden Informationen wird in der Folge in Kapitel 6 versucht, ein verbessertes Konzept zur Behandlung von Informationssicherheit zu erstellen. Dieses folgt vom Aufbau grundlegend der Struktur des zuvor geschilderten vorhandenen Sicherheitskonzepts.

Um mögliche Diskrepanzen zu erkennen und damit die zuvor erwähnte Frage zu beantworten, werden ein Vergleich dieser Modelle durchgeführt und ggf. notwendige Handlungsfelder identifiziert und Handlungsempfehlungen abgegeben. Aus diesen Erkenntnissen wird abschließend eine Checkliste zusammengestellt, die diese Handlungsfelder übersichtlich zusammenfasst und eine konzeptionelle Anleitung zur Erreichung eines hohen bzw. des geplanten Informationssicherheitsschutzniveaus für den Einsatz von IoT-Geräten in Unternehmensnetzwerken sein soll. Der letzte Schritt des Modells, die Umsetzung, muss dann in einem konkreten Anwendungsfall erfolgen. Diese Arbeit soll neben Handlungsempfehlungen und der Checkliste als Ergebnis auch einen Weg aufzeigen, Risiken im IoT-Kontext systematisch zu erkennen und zu behandeln.

Im IoT-Umfeld stellen sich natürlich nicht nur Fragen zur Sicherheit, es gibt allgemein eine große Bandbreite von technischen Herausforderungen wie die Entwicklung und Nutzung von zu den Anforderungen passenden Protokollen, der Entwicklung von Plattformen und Software oder der Senkung des Energieverbrauchs für autonome Geräte. Ausdrücklich nicht Ziel dieser Arbeit ist die Betrachtung dieser Aspekte oder von Security-Konzepten für IoT-(Software-)Architekturen an sich, wenngleich dies aktuelle und vieldiskutierte Themenfelder sind. In einem Unternehmen bzw. Unternehmensnetzwerk kann davon ausgegangen werden, dass viele der möglicherweise eingesetzten Geräte und Anwendungen fertig zugekauft werden, so wie dies auch im BYOD- und Industriebereich erfolgt. Damit ist eine Beeinflussung von Informationssicherheitsaspekten der Geräte z.B. in der Entwicklungsphase an sich oft nicht möglich, dennoch müssen oder sollen diese aber in ein Unternehmensnetzwerk in möglichst sicherer Art und Weise integriert werden. Der Schwerpunkt dieser Arbeit liegt nicht auf der Betrachtung von Produktionsnetzen und den darin eingesetzten Maschinen und Geräten, sondern auf der allgemeinen Untersuchung von Einsatzszenarien von IoT in einem Unternehmensnetzwerk (dies schließt diesen Aspekt indirekt mit ein).

2 BEGRIFFSBESTIMMUNGEN

Nachfolgende Abschnitte behandeln für diese Arbeit wesentliche Grundbegriffe. Zum ersten wird der Begriff des Unternehmensnetzwerks, welches den Betrachtungskontext darstellt, definiert. Nachfolgend wird eine Bestimmung des Begriffes IoT vorgenommen, da dies, wie sich auch in den angeführten Definitionen zeigt, ein sehr uneinheitlich verwendeter Terminus ist, welcher ein unklar abgegrenztes Gemenge an Betrachtungswinkeln umfasst. Zuletzt wird eine Erläuterung der Grundkonzepte von Informationssicherheit sowie in diesem Bereich relevanter Normen und Richtlinien durchgeführt.

2.1 Unternehmensnetzwerk

Als Kontext für die Betrachtung wurde in dieser Arbeit der abstrakte Begriff des Unternehmensnetzwerks gewählt. Es ist somit eine kurze inhaltliche Abgrenzung dieses Begriffs notwendig.

2.1.1 Aufgabe und Definition

Computernetzwerke sind verteilte Systeme, in welchen Computer und andere Geräte aus der Informations- und Kommunikationstechnologie (IKT) lose zusammengekoppelt werden. Solche angeschlossenen Geräte können über dieses Kommunikationsnetzwerk unter Einhaltung vorgegebener Protokolle miteinander kommunizieren. Die Kopplung erfolgt durch aktive Netzwerkelemente, welche je nach Aufgabe verschiedene Bezeichnungen erhalten, z.B. Switch oder Router (Kizza, 2015).

Als Unternehmensnetzwerk ist nun grundsätzlich jenes Netzwerk zu sehen, das den notwendigen IKT-Unterbau für das Handeln eines Unternehmens bereitstellt (Boger, 2014). Begriffsdefinitionen lassen sich aus verschiedenen Blickwinkeln finden. So findet sich in den *Requests for Comments* (RFCs), welche in vielen Bereichen der Internet-Technologie de-facto-Standards darstellen, eine allgemeine technische und vor allem klare organisatorische Abgrenzung für den Begriff Unternehmensnetzwerk:

> *[…] A network that has multiple internal links, one or more router connections to one or more Providers, and is actively managed by a network operations entity.*
> *(RFC 4057, 2005)*

2.1.2 Bestandteile

Eine geografische Abgrenzung für die Bestandteile eines Netzwerks findet sich bei Tanenbaum und Wetherall (2012): Wird ein lokales Netz (*Local Area Network*, LAN) in einer Firma eingesetzt, nennt man es Unternehmensnetzwerk. Für Oppenheimer (2011) scheint diese Definition etwas zu kurz gegriffen. Sie definiert ein Enterprise-Netzwerk als Komposition aus mehreren möglichen Bestandteilen in Anlehnung an die Schichten des *Open Systems Interconnection* (OSI)-Modells:

- Segment (einzelnes Netzwerk, abgegrenzt durch einen Switch oder Router)
- LAN (Verbund von Segmenten)
- WAN (*Wide Area Network*: geographisch verstreute Netzwerke, verbunden über Weitverkehrsstrecken)
- Wireless Network (WLAN oder WWAN, Funkverbindungen im Nah- oder Fernbereich)

Es ist anzumerken, dass solche Netze nicht nur von Firmen (bzw. Unternehmen im engeren betriebswirtschaftlichen Sinn) betrieben werden, sondern auch von Behörden, Universitäten sowie anderen Institutionen (Bin Ali, Hossain, & Parvez, 2015). Nicht enthalten in dieser Beschreibung sind weitere Komponenten (z.B. Computer, Drucker, …), welche in Netzwerken naturgemäß vorhanden sind – das Netzwerk an sich erfüllt keinen unternehmerischen Selbstzweck[1] (siehe auch Abschnitt 3.1).

Das in Unternehmensnetzwerken durch das Internet üblich gewordene Kommunikationsmuster ist das Client-Server-Prinzip. Dabei stößt der Client eine Anfrage am Server an, welche dieser mit den entsprechenden Daten oder Aktionen beantwortet. Dabei greifen üblicherweise viele Clients auf einen Server zu, es findet jedoch keine direkte Kommunikation zwischen Clients statt (Oluwatosin, 2014).

2.2 Internet of Things (IoT)

Da der Begriff IoT nur im zeitlichen Kontext seiner Evolution verstanden werden kann, wird die Entstehung und Entwicklung betrachtet, bevor ein Überblick über aktuelle (normative) Definitionen des Begriffs gegeben wird. Es erfolgt eine Gegenüberstellung der Definitionen, um die Kernbereiche herauszuarbeiten und darzulegen. Im Anschluss erfolgt eine Abgrenzung zu anderen in diesem Kontext oft verwendeten Begriffen. Danach werden Anwendungsfälle dieser Technologie skizziert, um auch seine wirtschaftliche Relevanz aufzuzeigen. Am Ende des Kapitels werden zur besseren Anschaulichkeit dieses abstrakten Themas konkrete Beispiele von IoT-Geräten und -Technologien angeführt.

2.2.1 Entwicklung und Wahrnehmung des IoT

Der Begriff IoT an sich ist für IKT-Verhältnisse keineswegs neu. Die erste Verwendung wird Kevin Ashton zugeschrieben. Er hat ihn 1999 in einer Präsentation über Supply Chain Management verwendet, in welcher er den Aspekt bzw. Begriff der „Dinge“ als integralen Bestandteil der Interaktionen und des Lebens in der physischen Welt als überarbeitungswürdig einstuft. Eine Neubewertung sei auf Grund der technischen Entwicklungen im Bereich Computing, dem Internet und der Datengenerierungsrate von intelligenten Geräten (*smart devices*) notwendig (Buyya &

[1] Dies gilt selbst für Netzwerkserviceprovider, da auch in diesen Unternehmensnetzen weitere Bestandteile als nur Netzwerkkomponenten vorhanden sind.

Dastjerdi, 2016). Etwa zeitgleich war der Trend jedoch auch von anderen erkannt worden. So veröffentlichte Neil Gershenfield eine Publikation, in welcher er Ähnliches vorhersagte: „[…] as things start to use the Net so that people don't need to". Parallel dazu forschte man bei Xerox in Kalifornien an der sog. „dritten Ära" des *modern computing*, in welcher ein Konzept des *ubiquitous computing* (in etwa: allgegenwärtiges Rechnen) skizziert wurde (Hassan, Khan, & Madani, 2017). Damit zeigt sich, dass dieses Thema von mehreren Seiten als großer Trend erkannt wurde.

Ashtons Aussagen sind im Kontext der damals verfügbaren Technologie zu betrachten: Der Stand der Technik der zunehmenden Vernetzung von Objekten um die Jahrtausendwende bestand vor allem aus *Radio Frequency Identification*(RFID)-Chips und Barcodes, welche vornehmlich im Logistikbereich vor allem zur Markierung und Nachverfolgung von Gütern verwendet wurden. Ermöglicht wurde das durch zunehmend kleinere Sensoren und stark erhöhte Rechenleistung (Bassi, et al., 2013). Es ist davon auszugehen, dass die Einführung des Terms IoT 1999 eigentlich zur Bekanntmachung und damit in der Folge Förderung und Weiterentwicklung dieser Technologien gedacht war (Lueth, 2014). RFID war dann auch lange Zeit allgemein die dominante Technologie hinter Entwicklungen im IoT-Bereich, bis drahtlose Sensornetzwerke (*wireless sensor networks*, WSN) und Bluetooth für eine Adaption dieses Konzepts im technologischen Mainstream sorgten (Buyya & Dastjerdi, 2016).

Im Logistikbereich haben sich Technologien wie RFID durch unternehmerische Vorteile etwa im Supply Chain Management etabliert, wenngleich diese Lösungen ohne Interoperabilität und Interkonnektivität untereinander eingesetzt wurden. Sie stellten und stellen damit eher geschlossene Systeme dar, welche nicht auf andere Bereiche übertragbar waren bzw. sind. Solche Anwendung können als *Intranet of Things* bezeichnet werden, welchen – wenngleich in kleinen Bereichen durchaus erfolgreich – im Allgemeinen keine Nachhaltigkeit bzw. Langlebigkeit vorausgesagt wird (Bassi, et al., 2013).

Zehn Jahre nach der ersten Verwendung, als der Begriff doch allmählich größere Aufmerksamkeit erlangte (Lueth, 2014), konkretisierte Ashton in einem Interview den Ursprungsgedanken sowie die zu diesem Zeitpunkt bereits stattgefundene technische Entwicklung. Im letzten Jahrtausend seien Computer nur Gehirne ohne Sinne gewesen und verarbeiteten nur die Informationen, die ihnen bereitgestellt wurden. Es gebe aber wesentlich mehr Information auf der Welt als jemand über ein Keyboard oder einen Barcode in ein System einfließen lassen könne. Im 21. Jahrhundert, getrieben eben durch IoT, können Systeme nun selbst Informationen „wahrnehmen". Als Beispiel führt er die zivile Nutzung des Satellitennavigationssystems GPS bzw. die damit verbundene Möglichkeit eines Gerätes an, die eigene Position selbstständig zu erfassen und zu verarbeiten. Seit der behördlichen Freigabe habe sich diese Technologie so in der breiten Verwendung z.B. in Mobiltelefonen zur Navigation verankert, dass es schwierig sei, sich eine Welt ohne diese Technologie vorzustellen (Gabbai, 2015).

Im Jahr 2013 bestand Ashton dann bereits auf die Feststellung, das IoT sei kein Zukunftsthema mehr, sondern bereits gegenwärtige Realität. Das Marktforschungsinstitut Gartner deklarierte im selben Jahr dieses Thema als einen der Top-Ten strategischen Technologietrends mit einem vom Netzwerkausrüster Cisco geschätzten Marktvolumen von 14 Billionen US-Dollar bis 2020. Nicht nur Technologiekonzerne oder andere Unternehmen mit technischem Fokus, sondern auch

Medienkonzerne wie die britische BBC kündigten Forschungs- und Entwicklungsaktivitäten sowie Produkte und andere Tätigkeiten in diesem Umfeld an. Man sah sich an der Schwelle eines entstehenden „mega-markets“ mit starkem Einfluss auf Sektoren wie Gebäudeautomatisierung, Energieerzeugung und -Verteilung, Logistik, die Automobilbranche und natürlich Telekommunikations- und Informationstechnologie. Die vollumfänglichen Konsequenzen aus der Vernetzung all dieser „smart objects“ mit dem Internet konnte man noch nicht einschätzen (Bassi, et al., 2013).

Bereits damals wurde aber auch festgestellt, dass man das IoT als solches nicht explizit wahrnehmen werden wird. Wahrgenommen werde nur die zunehmende Vernetzung von Objekten. Das Internet der Dinge ist damit eine Kombination aus technologischen und menschlichen Faktoren, welche in einer Ausweitung der Verbindung von Allem, was in der (näheren) Umgebung passiert, mündet. Die zwei dominanten Charakteristika dabei sind:

- Die Verbindung zum Internet ist zunehmend allgegenwärtig (*ubiquitiuos*).
- Alles, auch banale/alltägliche Dinge, ist miteinander verbunden (Bassi, et al., 2013).

Aktuelle Schätzungen gehen davon aus, dass bis 2020 bis zu 30 Milliarden „Dinge“ an das Internet angeschlossen sind. Im Kontrast dazu: 1999, bei der ersten Erwähnung des IoT, waren es 2 Millionen (Hassan, Khan, & Madani, 2017). Mit diesen Zahlen wird deutlich, welch immenses Wachstum in diesem Segment in den letzten 20 Jahren passiert ist und welche gewaltigen Ausmaße die Vernetzung in den kommenden Jahren annehmen wird.

2.2.2 Normative Definitionen

Es gibt für den Begriff IoT keine allgemein gültige bzw. verbindliche Definition, gleichwohl gab es mehrfache Anläufe von unterschiedlichen Institutionen zur Erstellung einer ebensolchen. Alleine in den letzten Jahren gab es zahlreiche neue oder abgewandelte Definitionen (Voas, 2016) Trotz einer fehlenden universell akzeptierten Definition, erscheint es dennoch wichtig, diese Versuche zu unternehmen und zumindest ein gemeinsames Grundverständnis der Begriffe zu erreichen. Ansonsten kommt es (weiterhin) zur Entwicklung von Insellösungen, was einem Grundgedanken des IoT, nämlich Interoperabilität, diametral entgegenwirkt (IEC, 2016).

Einer der ältesten von einer öffentlichen Organisation aus dem Bereich Telekommunikation veröffentlichten Definitionsversuche ist in einer Publikation der International Telecommunication Union (ITU) aus dem Jahr 2005 enthalten, in welcher das IoT – etwas abstrakt - wie folgt beschrieben wird:

> *“ […] communications will be extended to things, from everyday household objects to sensors […]. Everything from tyres to toothbrushes will fall within communications range, heralding the dawn of a new era, one in which today’s internet (of data and people) gives way to tomorrow’s Internet of Things […]. The creation of the Internet of Things will entail the connection of everyday objects and devices to all kinds of networks, e.g. company intranets, peer-to-peer networks and even the global internet. For this reason, its development is of great significance to the telecommunication industry. It will challenge existing structures within established companies, and form the*

basis for entirely new opportunities and business models."
IoT-Definition der ITU aus 2005 (ITU, 2005)

Auffallend ist dabei, dass in dieser Beschreibung noch davon ausgegangen wird, dass die Verbindung der Dinge mit dem (globalen) Internet noch nicht im Fokus steht, sondern es durchaus z.B. Unternehmensnetzwerke sein können – auf welche diese Technologie massive Auswirkungen haben werde. Einige Jahre später (2012) definiert die ITU-T, einer der normativen Sektoren der ITU, in der Empfehlung[2] Y.2060 den Begriff bereits etwas kürzer wie folgt:

"A global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies."
IoT-Definition aus der ITU-T Empfehlung ITU-T Y.2060 (ITU-T, 2012)

Folgende Erkenntnisse können aus dem Vergleich dieser zwei Begriffsbestimmungen abgeleitet werden: Zum ersten wird 2012 nur noch von einer globalen Vernetzung gesprochen, etwaige lokale Begrenzungen oder Anwendungsbeispiele sind in der neueren Definition nicht mehr enthalten. Wesentlich erscheint zudem, dass die Definition der *Dinge* explizit um virtuelle Dinge erweitert wird. Damit sind beliebige Objekte der Informationswelt (im Gegensatz zu physischen Objekten wie Alltagsgegenständen, Robotern und anderen Gütern) gemeint, welche als solche identifiziert und in ein Kommunikationsnetzwerk integriert werden können. Beide Begriffsbeschreibungen gehen davon aus, dass IoT ein wesentlicher Faktor für neue Geschäftsmodelle (2005) bzw. „Ermöglicher" erweiterter Dienstleistungen (2012) und somit ein wesentlicher wirtschaftlicher Treiber – nicht mehr nur für den Telekommunikationssektor – ist.

Ein Gedanke, der bereits in der Publikation 2005 enthalten war, wird auch in der Empfehlung von 2012 wiedergegeben: Das IoT führe eine „Dritte Dimension" in die Telekommunikationswelt ein. War bisher durch IKT eine jederzeitige und ortsunabhängige Verbindung möglich, sei nun zusätzlich auch eine Verbindung zwischen allen Dingen möglich. Dies schließt für die ITU interessanterweise auch menschliche Interaktionen mit ein (Human-to-Human-Interaction, H2H), genauso wie ein neues Kommunikationsmuster: Thing-to-Thing (T2T). Eine grafische Darstellung dieser Idee findet sich in Abbildung 2.

[2] Wenngleich die ITU dies als „Empfehlung" bezeichnet, haben diese eigentlich den Anspruch eines internationalen technischen Standards. Als solche werden sie von der ITU in den allgemeinen Erläuterungen auch mehrfach bezeichnet (ITU-T, 2007).

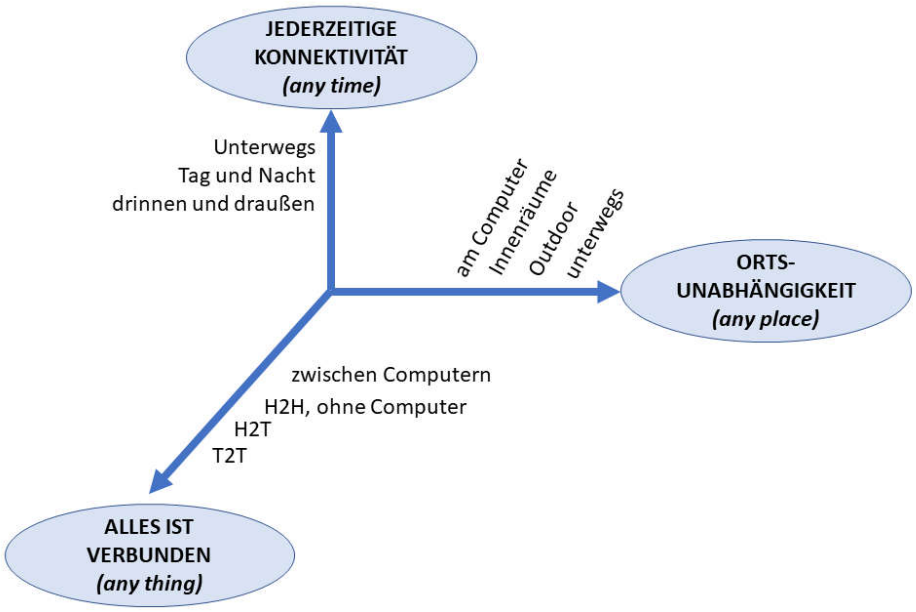

Abbildung 2: Einführung einer dritten Dimension im Umfeld der Telekommunikation, nach (ITU, 2005)

Im Standard *ISO/IEC 20924: Internet of things (IoT)-Vocabulary* der Standardisierungsgremiums ISO (International Organization for Standardization) und der Normungsorganisation IEC (International Electrotechnical Commission) findet sich folgende Definition für IoT:

> *"Internet of Things (IoT): infrastructure of interconnected entities, people, systems and information resources together with services which processes and reacts to information from the physical world and virtual world. "*
>
> *IoT-Definition aus ISO/IEC 20924: IoT – Vocabulary (ISO/IEC, 2018)*

Ebenso wie in der ITU-Definition wird hier IoT als Infrastruktur für vernetzte Objekte gesehen. Objekte können hier ebenso virtuelle (Informationsressourcen) wie physische Objekte sein, wobei Personen als Interaktionspartner in der ISO/IEC explizit genannt werden. Der Aspekt der Services wird in letzterer auf Services (im Gegensatz zu *fortgeschrittenen*) reduziert[3] und ein wesentlicher Aspekt von IoT findet sich in dieser Definition: Reaktion (in Form einer Aktion) als Ergebnis der Verarbeitung von Informationen.

Abschließend sei hier noch eine Definition erwähnt, welche vom IERC (*European Research Cluster on Internet of Things*) veröffentlicht wurde. Ziel dieses Clusters ist die Zusammenbringung von EU-finanzierten Forschungsprojekten zur Entwicklung einer gemeinsamen (europäischen) Vision der IoT-Technologie und Förderung sowie Koordination der damit verbundenen Herausforderungen in der Forschung.

> *[…] "A dynamic global network infrastructure with self-configuring capabilities based on standard and interoperable communication protocols where physical and virtual*

[3] In einem Entwurf zum Standard war an dieser Stelle noch *intelligent services* zu lesen (ISO/IEC, 2016), interessanterweise wurde dieser zusätzliche, den Begriff eigentlich erweiternde Aspekt in der finalen Definition entfernt.

“things” have identities, physical attributes, and virtual personalities and use intelligent interfaces, and are seamlessly integrated into the information network."

IoT-Definition der IERC (IERC, 2014)

Wie in den anderen Definitionen sind auch hier wieder der Aspekt der Infrastruktur sowie auch die Loslösung der Definition von rein physischen Dingen zu finden. Der Aspekt der Services fehlt hier, stattdessen wird der Begriff einer *intelligenten Schnittstelle* eingeführt. Offensichtlich wird hier in kleinteiligeren Strukturen gedacht, so dass nicht nur ein gesamtes Service, sondern bereits eine einzelne Schnittstelle erweiterte Informationsverarbeitung betreiben soll.

Zusammenfassend lässt sich sagen, dass diese Definitionen im Kerngedanken der gleichen Idee einer Infrastruktur zum Zusammenschluss von physischen und virtuellen Dingen zum Informationsaustausch und -Verarbeitung folgen. Es mögen grundsätzliche Ähnlichkeiten der Definitionen auch nicht überraschen, da die IERC beispielsweise aktiv in der ITU-T mitarbeitet und auch an deren IoT-Definition beteiligt war. Somit bleibt etwas unklar, warum dennoch eine eigene Definition durch die IERC und damit – neben vielen anderen – eine weitere notwendig war.

Allen genannten Definitionen gemein ist, dass keine konkreten Technologien für die Vernetzung angegeben werden. Von der ITU-T wurden jedoch Bereiche für eine Verbreitung von IoT identifiziert, in denen weitere technische Entwicklungen notwendig sind und welche zu leistbaren Preisen bereitgestellt werden müssen. Es betrifft dies unter anderem folgende Themenfelder:

- Konnektivität (allgegenwärtiger/ubiquitärer Zugang zu Breitbandanbindung wie 3G/4G-Netzen)
- Identifizierung von Objekten (einfache und unauffällige Identifikationssysteme wie RFID)
- Echtzeitinformationen, z.B. von Sensoren
- Smart Devices (Intelligenz ist in Geräten eingebettet)
- Verkleinerung, z.B. Nanotechnologie (Jamoussi, 2010)

Es wird aus den genannten Definitionen auch wieder ersichtlich, dass das IoT kein konkretes Produkt oder ein „Ding“ an sich ist, sein kann oder wird, sondern vielmehr einen Sammel- bzw. Überbegriff für Konzepte, Technologien und (Kommunikations-)Charakteristika darstellt. Folgende Kerncharakteristika lassen sich festhalten, weil sie sich in den genannten Definitionen in der einen oder anderen Art wiederfinden:

- Konnektivität/Vernetzung
- Dinge (Sensoren, Aktoren, Geräte) und „Ding-bezogene“ Services
- Daten/Informationen
- Kommunikation (Datenflüsse)
- Intelligenz („smarte“ Geräte, Data Analytics)
- Aktionen als Ergebnis (Entscheidungen, Automatisierung)
- Heterogenität und Ökosystem (globale Community, Partnerschaften)

- Enorme Skalierung (größere Anzahl an Geräten und Menge an Informationen als im derzeitigen Internet)

(i-SCOOP, 2016); (Vermesan & Friess, 2014)

Es ist anzumerken, dass der Begriff „Internet“ sich in der Verwendung im Zusammenhang mit IoT wohl implizit auf seine ursprüngliche Definition bezieht: die Zusammenschaltung von hochentwickelten (globalen) Computernetzen, im Englischen als *Interconnected Networks* (kurz: Internet) bezeichnet. Die IoT-Definitionen selbst beziehen sich dabei wie erwähnt weder auf eine konkrete Technologie oder spezifische Protokolle (bzw. werden diese in der Begriffsdefinition nicht angeführt), wenngleich z.B. die ITU in ihrer Definition des *Internet* schon implizit die Verwendung des Internet Protocol (IP) definiert. Diese Festlegung auf ein spezifisches Protokoll scheint jedoch etwas zu eng gefasst. Konnektivität und Vernetzung können im IoT-Bereich auch ohne die Verwendung von IP erfolgen, das zeigt insbesondere die Verwendung moderner Drahtlostechnologien in Sensornetzen (siehe auch Abschnit 4.1).

2.2.3 Praktische Definition

Wohl weil die im vorigen Abschnitt angeführten Definitionen eine gewisse allgemeine Gültigkeit beanspruchen, sind sie sehr abstrakt gehalten und schwer konkret in einer Umsetzung vorstellbar. Nachfolgend sollen daher noch einige Definitionen diskutiert werden, welche praktisch orientiert und leichter verständlich den Gedanken von IoT darlegen.

> *“The Internet of Things (IoT) paradigm promises to make “things” including consumer electronic devices or home appliances such as medical devices, fridge, cameras, and sensors part of the Internet environment. This paradigm opens the doors to new […] interactions among things and humans and enables the realization of smart cities, infrastructures, and services […].“*
>
> *IoT-Definition, aus (Buyya & Dastjerdi, 2016)*

Interessant an diesem Zugang ist die Fokussierung auf den Consumer-Bereich und die Anführung von konkreten Beispielen von Geräten. Es wird erwartet, dass diese mit dem Internet verbunden werden und dadurch die Realisierung konkreter IoT-Anwendungen ermöglicht wird.

> *“We define the Internet of Things as a network of connected devices with*
> *1) unique identifiers in the form of an IP address which*
> *2) have embedded technologies or are equiped with technologies*
> *that enable them to sense, gather data and communicate about the environment in which they reside[…]. The potential […] resides in the ways the IoT is used to […] automate, digitize, digitalize, optimize and […] transform processes, business models and even industries.“*
>
> *IoT-Definition, aus (i-SCOOP, 2016)*

Auch diese Definition stellt explizit auf IP als Protokoll für das Internet der Dinge ab, was, wie erwähnt, eine wohl etwas zu enge Definition ist. Der Mehrwert wird hier erst in der Zusammenschaltung der Dinge zur Nutzung des IoT zur Neugestaltung von Prozessen und Ermöglichung neuer Geschäftsmodelle gesehen.

> *"The basic idea of this concept is the pervasive presence around us of a variety of Things or objects – such as […] sensors, actuators, mobile phones, etc. – which, through unique addressing schemes, are able to interact with each other and cooperate with their neighbors to reach common goals."*
> *IoT-Definition, aus (Atzori, Iera, & Morabito, 2010)*

Diese Definition bringt den Aspekt der „gemeinsamen Zielerreichung" als Aufgabe von IoT-Geräten ein. Dieser sehr abstrakte Begriff zeigt auf, was das Internet der Dinge durch Kooperation der Geräte leisten soll.

Neben diesen Definitionen gab es in den letzten Jahren noch dutzende weitere Versuche einer Definition, aus welchen man auch einen gewissen Trend ableiten kann. Waren es im ersten Jahrzehnt dieses Jahrhunderts noch Themen wie Vernetzung und Interaktion zwischen den Dingen, die die Begriffsbestimmung dominierten, finden sich insbesondere in den neueren normativen Definitionen – der technischen Weiterentwicklung geschuldet – wesentliche Erweiterungen des Konzepts (z.B. IoT als Infrastruktur, Einbindung virtueller Ressourcen als Dinge). Die normativen Beschreibungen sind etwas weiter bzw. allgemeiner gefasst und beschreiben weniger konkrete Anwendungsfälle, sondern eine Idee, die als IoT-Paradigma bezeichnet werden kann. Als gute Zusammenfassung der Idee kann entsprechend die Definition gemäß ISO/IEC 20924 herangezogen werden, da sie alle wesentlichen Aspekte beinhaltet und in knappen Worten eine Charakterisierung von IoT liefert. Die praktischen Definitionen können dabei unterstützen, sich eine etwas konkretere Vorstellung von IoT zu machen.

2.2.4 Abwandlungen, Erweiterungen und Abgrenzung des Begriffes

Neben dem Begriff IoT selbst werden in der Behandlung dieses Themengebietes immer wieder Begriffe unscharf als Homo- oder Synonyme verwendet, welche zumeist aber einen Unter- oder Überbegriff von IoT darstellen. In diesem Abschnitt wird daher für die vorliegende Arbeit eine Abgrenzung dieser Begriffe vorgenommen.

2.2.4.1 M2M

Wenn Kommunikation nur zwischen Maschinen erfolgt, wird dies als Machine-to-Machine(M2M)-Kommunikation bezeichnet. Solche Systeme und Kommunikationsmuster sind integraler Bestandteil des IoT. Das Konzept von M2M-Kommunikation ist nicht auf einen spezifischen Industriezweig oder Anwendungsfall limitiert, da es die gesamte Bandbreite an möglichen Formen an automatischer oder semiautomatischer Gerätekommunikation beinhaltet. Heutzutage bereits ver-

breitete und als solche bezeichnete M2M-Systeme sind beispielsweise Point-of-Sale (POS, semiautomatisch) und Fahrzeuglokalisierungs- und Verfolgungstechnologien (automated vehicle location services/AVL, vollautomatisch) im Logistikbereich.

Eine wesentliche Charakteristik heutiger M2M-Systeme ist die Unidirektionalität des Datenflusses. So sind beispielsweise POS-Systeme an ein Zentralsystem angeschlossen und können im Allgemeinen keine eingehenden Anfragen verarbeiten. AVL-Systeme senden überhaupt nur Daten an ein zentrales System wo sie verarbeitet werden und bieten keine Möglichkeit für einen Informationsrückkanal (Macaulay, 2017). Dem gegenüberzustellen sind aber die erwähnten Definitionen von IoT, welche wesentlich mehr beinhalten – insbesondere eine Bidirektionalität der Kommunikation, der gegenseitige Informationsaustausch sowie das Auslösen von Aktionen.

2.2.4.2 IoE

Das *Internet of Everything* (IoE) ist ein vom Netzwerkausrüster Cisco seit ca. 2013 getriebener Begriff, der zuweilen anzutreffen ist und im Wesentlichen eine konzeptionelle Erweiterung des Begriffes IoT um Prozesse und in manchen Anwendungen auch Orte (im räumlichen Sinn, engl. *places*) ist (Lopez Research, 2013). Es soll die intelligente End-zu-End-Kommunikation zwischen Personen, Prozessen Daten (insb. Big Data) und Dingen den eigentlichen Mehrwert des IoE darstellen (Saleh, Ammi, & Szoniecky, 2018). Bei diesem Begriff gibt es allerdings starke Unterschiede in der tatsächlichen Verwendung. So wird er teilweise synonym zu IoT bzw. nur als sozusagen mengenmäßige Erweiterung (hohe Geräteanzahl – „alles ist verbunden“) des IoT (Jara, Ladid, & Skarmeta, 2013) oder aber als tatsächliche inhaltliche Erweiterung (Prozesse als zusätzlicher expliziter Bestandteil) gesehen (Miraz, Maaruf, Excell, & Picking, 2018). Ob diese Unterscheidung tatsächlich eine echte inhaltliche Frage ist, scheint ungeklärt (Karl, 2018). Die zuvor diskutierten normativen IoT-Begriffe lassen allerdings so viel Spielraum, dass dieser eigene Begriff in der Zwischenzeit eigentlich überflüssig erscheint. Er findet in den betrachteten Unterlagen der Standardisierungsorganisationen auch keine Verwendung.

2.2.4.3 IIoT

Der Begriff Industrial IoT (IIoT), manchmal auch als *Industrial Internet* bezeichnet, bezieht sich auf eine spezielle Form von IoT-Anwendungen in High-Tech-Unternehmen, im speziellen in hoch technologisierten Produktionsunternehmen. Da Maschinen manche Aufgaben wie Datenerfassung und Kommunikation akkurater (i.S.v. exakter, genauer) als Menschen durchführen können, hat sich die Verwendung in diesen Bereichen beschleunigt. Wesentliche Bestandteile von IIoT sind daher M2M-Kommunikation, Big Data-Analyse und Machine Learning-Techniken. Das führt zum Einsatz von IIoT-Technologien zur Früherkennung von Problemen, effizienterer Planung von Supply Chains, Durchführung von Qualitätskontrollen oder der Reduktion des Energieverbrauchs (Buyya & Dastjerdi, 2016). Die Verbindung von Industriemaschinen und -Geräten war eine der ersten konkreten Anwendungen für IoT-Technologien. Aus dieser frühen, praktischen Anwendung hat sich eigentlich erst der heute wesentlich weiter gefasste IoT-Begriff hin zur Vernetzung

beliebiger alltäglichen Objekten entwickelt (Lopez Research, 2013), wie er z.B. in den (normativen) Definitionen zu finden ist.

In diesem Kontext sei auch der Begriff Industrie 4.0 erwähnt, welcher (stark getrieben von der deutschen Regierung) eine weite Verbreitung erfahren hat, jedoch an sich sehr limitiert in seiner allgemeinen Aussagekraft ist, da er sich nur auf die herstellende Industrie bezieht. Vom Begriff des (I)IoT unterscheidet er sich in seinem Umfang vor allem dadurch wesentlich, dass er weiter gefasst ist und auch tatsächliche Änderungen der physischen Welt wie beispielsweise 3D-Druck und Augmented Reality-Anwendungen umfasst („*beyond connectivity*“) und als Konzept für eine nächste industrielle Revolution gedacht ist (Lueth, 2014).

2.2.4.4 IoMT

Technische Fortschritte haben auch zur Anwendung moderner Technologien im Gesundheitswesen geführt. Beispiele für Applikationen in diesem Bereich sind z.B. durch IoT unterstützte elektronische Patientenakten, was Vorteile in der Kommunikation zwischen Ärzten bzw. Ärztinnen und Patienten bzw. Patientinnen bringen soll. Für diesen Anwendungsfall hat sich der Begriff des *Internet of Medical Things* (IoMT) als anwendungsbereichsbezogene Subkategorie des IoT gebildet (Wieler, 2017).

2.2.4.5 Grafische Zusammenfassung

Die Darstellung des Zusammenhangs in Abbildung 3 enthält den Begriff des IoE noch explizit als erweiterten IoT-Begriff. Diese Unterscheidung verdeutlicht den historischen Werdegang dieser Begriffe, in der Zwischenzeit können jedoch die oberen beiden Bereiche gemeinhin als IoT bezeichnet werden. Es wird deutlich, dass M2M nur einen Teil der Aspekte hinsichtlich des Fokus abdeckt. Das bedeutet, dass M2M nicht die ganze Breite an konzeptioneller Änderung mit sich bringt, wie die anderen Technologien. Die anderen Konzepte haben bereits wesentlich mehr Auswirkung auf die physische Welt, zum Teil durch explizite Platzierung von neuen Dingen. Die geografische Ausbreitung zeigt auch, dass IIoT aller Erwartung nach in einem geografisch oder logisch begrenztem Bereich, wie etwa einem Unternehmensnetzwerk, anzufinden sein wird, während das IoT durchaus globale Ansprüche hat.

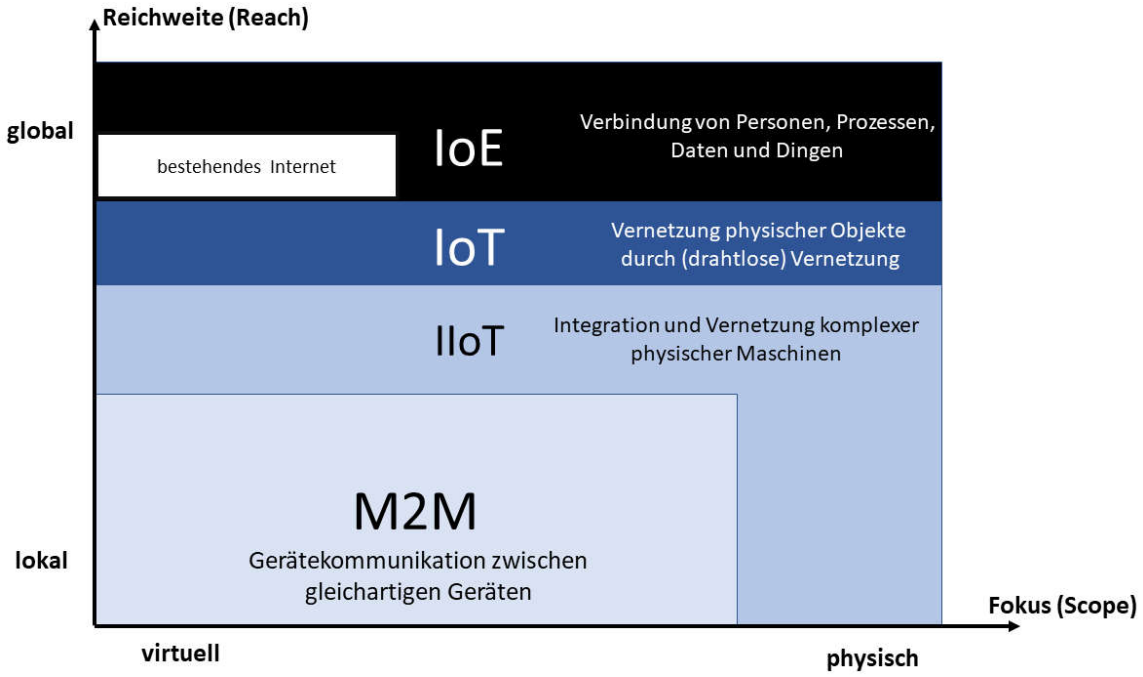

Abbildung 3: Grafische Darstellung des Zusammenhangs von Begriffen aus dem IoT-Umfeld nach (Lueth, 2014)

2.3 IoT-Architektur

Eine typische IoT-Architektur kann in drei Domänen bzw. Schichten unterteilt werden: Sensor- oder Perzeptionsschicht, Netzwerkschicht und Applikationsschicht. Dieser Zusammenhang ist in Abbildung 4 dargestellt. Die Sensorschicht spielt in diesem Zusammenhang eine große Rolle. Sie besteht aus den „intelligenten“ Dingen, welche in ihren Domänen miteinander kommunizieren und/oder Daten erheben. Sollte ein Übergang zu einer anderen Kommunikationstechnologie oder einem anderen Kommunikationsprotokoll notwendig sein, ist der Einsatz von Gateways möglich bzw. notwendig (siehe auch Abschnitt 6.2.3). Dabei kann auf dieser Ebene auch eine Vorverarbeitung von Informationen erfolgen. Die größten Herausforderungen auf dieser Ebene stellen niedriger Energieverbrauch und Kosten sowie möglichst leichtgewichtige Protokolle dar.

Die Netzwerkschicht baut auf vorhandener oder aufkommender Kommunikationsinfrastruktur, wie Mobilfunktechnologien oder dem Internet, auf. Das Ziel ist die Übermittlung der Daten aus der Perzeptionsschicht an entfernte Destinationen, im konkreten Fall die IoT-Anwendungen.

Auf der Anwendungsschicht erfolgt der Hauptteil der Datenverarbeitung sowie die eigentliche Bereitstellung der IoT-Anwendung als Service. Auf dieser Schicht werden den Nutzern und Nutzerinnen die entsprechenden Applikationen bereitgestellt (Chen, Jia, & Li, 2011).

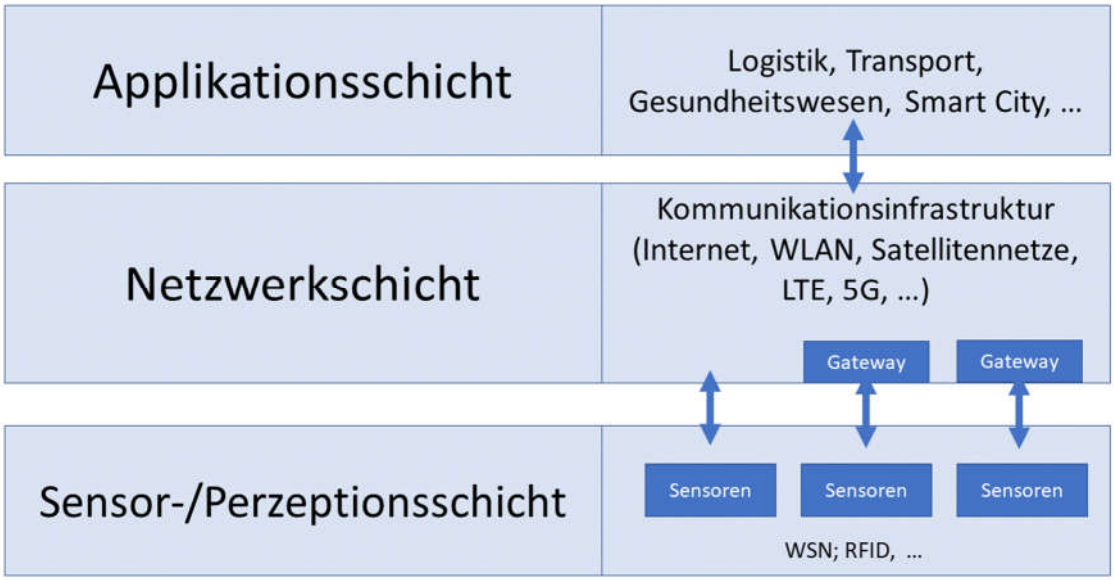

Abbildung 4: Dreischichtige IoT-Architektur, nach (Chen, Jia, & Li, 2011) und (Zhu, Wang, Chen, Liu, & Qiny, 2010)

Dieses Modell soll zur einfachen Veranschaulichung der gängigen IoT-Architektur dienen. Es existieren auch wesentlich komplexere und umfangreichere Architekturmodelle wie das *IoT Architectural Reference Model* (IoT-ARM), welches durch das von der Europäischen Kommission getriebene *IoT-Architecture Project* (IoT-A) erstellt wurde (Bassi, et al., 2013).

2.4 Beispiele für IoT-Anwendungsbereiche und Geräte

Grundsätzlich lassen sich im IoT-Umfeld zwei Differenzierungen hinsichtlich der Anwendungsbereiche feststellen. Zum einen erfolgt eine allgemeine Darstellung hinsichtlich der Bereiche, dem einzelnen Anwendungsfälle zuzuordnen sind. Auf der anderen Seite wird zwischen einer Anwendung im Unternehmensumfeld und dem Verbraucherumfeld unterschieden. Nachfolgend werden dafür jeweils Beispiele aufgeführt und erläutert. Zudem werden in diesem Abschnitt aktuelle IoT-Geräte aus verschiedenen Bereichen angeführt, um eine konkretere Vorstellung der Anwendbarkeit zu bekommen.

2.4.1 Anwendungsbereiche

Nach Anwendungsbereichen lässt sich nachfolgende Unterscheidung durchführen. Dabei handelt es sich jedoch nicht um eine erschöpfende Aufzählung, sondern nur um Beispiele. Es lassen sich vermutlich in jedem denkbaren – auch zukünftigen – Bereich Anwendungsgebiete für IoT-Technologien finden.

- **Logistik, Transport und Handel**

Moderne Autos, Busse und Züge, aber auch Straßen und Schienenstrecken werden zunehmend mit einer größeren Anzahl an Sensoren und Aktuatoren versehen. Die auf diesen Strecken transportierten Güter können mit RFID-Tags ausgestattet werden. Das ermöglicht eine Vielzahl von IoT-Anwendungen, welche beispielsweise Aufgaben in der Verkehrssteuerung, Nachverfolgung

von Gütern, Überwachung von Lebensmitteltransporten etc. übernehmen können oder Unterstützung bei der Wegfindung z.B. im Tourismusbereich bieten können (Atzori, Iera, & Morabito, 2010).

- **Gesundheitswesen**

Im Bereich Gesundheitswesen bietet Io(M)T diverse Anwendungsbereiche. So können gesicherte Patientenidentifizierung zur Vermeidung von Fehlbehandlungen, Datenerfassung und -Übermittlung zur Minimierung von Schreibarbeit und Beschleunigung von Prozessen oder das automatische Erfassen des Gesundheitszustands durch Sensoren mögliche Anwendungsbereiche sein (Atzori, Iera, & Morabito, 2010)

- **Smart Environment / Smart City**

In den Bereich der „intelligenten" Umgebung fallen Anwendungen im Büro-, Heim-, Industriebereich (Fabriken) wie auch im öffentlichen Raum. Konzepte zur Erhöhung des Komforts in Innenräumen wie intelligente Heizung/Kühlung, Anpassung der Beleuchtung, Alarmanlagen oder das automatische An- und Abschalten elektronischer Geräte zur Senkung des Stromverbrauchs fallen in diesen Anwendungsbereich und werden oftmals auch als Gebäudeautomatisierung bezeichnet. Im Industriebereich kann eine Erhöhung des Automatisierungsgrades zur Steigerung der Produktivität beitragen (Atzori, Iera, & Morabito, 2010).

Ausgedehnt auf den öffentlichen Raum gibt es im Zusammenhang mit IoT beispielsweise die Vision einer intelligenten Stadt (Smart City).

- **Smart Grid**

Einer der am häufigsten genannten Anwendungsbereiche für IoT ist das intelligente Stromnetz (Smart Grid). In einem solchen Stromnetz wird das Verhalten der am Netz angeschlossenen Nutzer und Nutzerinnen erfasst und darauf entsprechend reagiert, so dass eine nachhaltige, wirtschaftliche und sichergestellte Energieversorgung erfolgt (Jamoussi, 2010).

- **persönliche/soziale Anwendungsbereiche**

In diesem Bereich fallen beispielsweise Anwendungen, die es Menschen ermöglichen, soziale Interaktionen bzw. Beziehungen herzustellen oder zu vertiefen. So ist eine Verzahnung mit Sozialen Medien oder die Auswertung persönlicher Aktivitäten (privat wie beruflich) auf Basis der durch IoT erfassten Daten denkbar. Sind viele unserer Geräte vernetzt bzw. lokalisierbar, ist auch das leichtere Wiederfinden von verlorenen, verlegten oder gestohlenen Gegenständen möglich. (Atzori, Iera, & Morabito, 2010).

2.4.2 Unterscheidung Consumer IoT vs. Enterprise IoT

Consumer IoT ist jener Anwendungsbereich von IoT, über den am meisten (z.B. in Medien) gesprochen wird und welcher allgemein am weitesten bekannt ist. In diesen Anwendungsbereich fallen z.B. Wearables, Smartphones, Smart TV-Geräte, Hausüberwachung/-automatisierung etc. (i-SCOOP, 2016). Der Anteil dieser Geräte an allen IoT-Geräten wird Prognosen zur Folge 2020 bei 63% liegen (Petrov, 2019).

Spricht man im Gegensatz dazu über den IoT-Einsatz in Unternehmen, gibt es dazu zwei gefährliche Trugschlüsse: Erstens: CIoT ist nicht das Gegenstück zu IIoT, bzw. IIoT nicht IoT in Unternehmen. IIoT ist selbst nur einer von vielen denkbaren Anwendungsfällen im IoT-Bereich. Zum zweiten werden sehr wohl auch CIoT-Geräte in Unternehmen eingesetzt – man nehme nur Smartphones oder SmartTV-Geräte, welche sich sicherlich in einem Großteil der Unternehmensnetzwerke heute schon wiederfinden lassen (Gold, 2018). Daraus erwächst eine nicht irrelevante Problematik, denn diese Geräte sind insbesondere hinsichtlich ihrer Sicherheitseigenschaften nicht immer für einen Einsatz in Unternehmen geeignet.

2.4.3 Beispiele für IoT-Geräte

Zur besseren Veranschaulichung des sehr abstrakten Konstrukts „IoT“ seien nachfolgend einige Beispiele für am Markt befindliche IoT-Geräte und -Technologien angeführt. Vieles davon ist CIoT zuzuordnen, soll aber eine Idee davon liefern, welche verschiedenen Arten von Geräten im IoT-Kontext behandelt werden müssen.

- **Sprachsteuerung** (Bsp.: *Google Home Voice Controller*, *Amazon Echo*)**:** Geräte, die in ein (Heim-)Netzwerk integriert werden können und dabei durch Sprachsteuerung verschiedene andere Geräte steuern oder Aktionen ausführen können. Möglichkeiten dabei sind das Abspielen von digitalen Medien (Musik, Videos), Steuerung von Fernsehern, Beleuchtung, anderen IoT-Geräten oder das Abrufen von Informationen aus dem Internet (Software Testing Help, 2019).
- **Geräte aus dem Bereich Smart Home** (Bsp.: *Amazon Dash Button*, *August Doorbell Cam* und *Smart Lock*, *Belkin WeMo Smart Light Switch*, *Footbot Air Quaility Monitor*, *Nest Learning Themostate Easy Temperature Control, GreenIQ Controller, Keen Home Smart Vent, Philips Hue, Samsung Family Hub Fridge, Panasonic Autocare, Bosch Home-Connect-Waschmaschinen*). Dabei handelt es sich um IoT-Geräte, die den Alltag durch Vernetzung vereinfachen sollen und dabei z.B. herkömmliche Geräte wie Thermostate, Glühbirnen, Lichtschalter oder Türsprechanlagen ersetzen oder den Alltag durch Vereinfachung von Bestellvorgängen, das Messen der Luftqualität, Steuerung der Gartenbewässerung oder Lüftungssteuerung in Wohnräumen verbessern sollen (Software Testing Help, 2019), (Postscapes, 2019), (Nahius, 2016). Auch werden Haushaltsgeräte wie Kühlschränke und Waschmaschinen zu IoT-Geräten weiterentwickelt (Samsung, 2019), (Otter, 2019).
- **Wearables** (*ProGlove Smart Glove*, *Medtronic GUARDIAN*, div. Smartwatches und Fitnesstracker). Als Wearables werden IoT-Geräte bezeichnet, die am Körper getragen werden. Beispiele hierfür sind Smartwaches (Uhren) und Fitnesstracker, Geräte zur Überwachung medizinischer Parameter wie Blutzucker oder Handschuhe mit integriertem Scanner und haptischem Feedback (snyxius, 2016), (Maddox, 2016), (Nahius, 2016).
- **Intelligentes Baumaterial (Bsp.: *Nanite* von oceanit)**. Durch Sensoren, welche in verschiedene Baumaterialen eingebettet werden, ist eine jederzeitige Erfassung von mecha-

nischen, akustischen oder magnetischen Umgebungswerten möglich. Dies kann beispielsweise in Straßen zur Erfassung von Verkehrsdaten oder des Zustands einer Straße dienen (oceanit, kein Datum).

Werden IoT-Applikationen selbst entwickelt, bieten sich dafür kostengünstige Einplatinencomputer als möglich Plattform an. Diese zumeist im unteren zweistelligen Preissegment angesiedelten Geräte ermöglichen die Erstellung von eigenen IoT-Applikationen. Beispiele für solche Plattformen sind *Arduino, BeagleBone, Dragino, Espruino, Hummingboard, Intel Galileo* oder *Raspberry*. Je nach Ausstattung (und entsprechendem Preis) handelt es sich dabei um unterschiedliche Computerarchitekturen, die verschiedene Betriebssysteme und Schnittstellen unterstützen bzw. anbieten (Postscapes, 2019).

Anhand dieser Beispiele wird deutlich, wie breit gefächert die Palette an IoT-Geräten ist. In Unternehmen werden sicherlich einige dieser Geräte eingesetzt, aber auch noch viele andere aus anderen Anwendungsgebieten.

2.4.4 Relevanz von IoT

Das Marktforschungsinstitut Gartner sieht IoT als Hype-Technologie, welche den Status der Produktivität im Sinne einer weiten Verbreitung und Massenmarkttauglichkeit erst in 5-10 Jahren erreichen wird. 2018 wird IoT noch in dem Status gesehen, dass es auf Grund von Erfolgsgeschichten hohe öffentliche Aufmerksamkeit erfährt, aber noch nicht von allen Unternehmen adaptiert wurde. Erste Aspekte von IoT erfahren bereits ein leichtes Abflauen des Hypes, da Implementierungen aus unternehmerischer Sicht bereits fehlgeschlagen sind (Panetta, 2016).

Es besteht aber kein Zweifel daran, dass IoT als Ganzes eine weiterhin zunehmende Verbreitung erfahren wird. Das macht sich vor allem an den Zahlen und Prognosen bemerkbar, welche die Entwicklung der Anzahl an IoT-Geräten sowie das Marktvolumen prognostizieren. So sollen die globalen Ausgaben im Zusammenhang mit IoT-Technologien 2022 1,2 Billionen US-Dollar erreichen (Columbus, 2018), bis 2025 sollen 64 Milliarden IoT-Geräte an das Internet angeschlossen sein. Derzeit werden laut einer Statistik 127 neue IoT-Geräte pro Sekunde(!) in Betrieb genommen (Petrov, 2019). Zwar schwanken Zahlen und Prognosen zu diesem Thema durchaus erheblich, an keiner der Zahlen kommt aber ein Zweifel an der künftigen Marktrelevanz von IoT auf. Die Relevanz für Unternehmen kann auch aus Umfragen von Markforschungsinstituten abgeleitet werden. So gaben 2017 bei einer Umfrage von PwC 73% der befragten Unternehmen an, bereits aktiv in IoT-Projekte zu investieren (pwc, 2017). Dabei wird IoT mehrheitlich als essentieller Bestandteil der digitalen Transformation identifiziert (Hill, 2018).

IoT wird auch als wesentliche Technologie zur Steigerung des Kundennutzens in Unternehmen gesehen. Das kann für ein Unternehmen durch den Einsatz in verschiedenen eigenen Bereichen erfolgen, aber auch durch die Entwicklung entsprechender IoT-Produkte für den Markt. Beispiele hierfür sind Produkte aus dem Smart-Home-Umfeld, vernetzte/intelligente Produkte oder eine Verbesserung des Einkaufserlebnisses im Handel (Lee & Lee, 2015). Dabei ist interessant, dass der Anteil an Services und Software an den erwarteten Erlösen durch Firmen wesentlich höher ist als durch Entwicklung und Verkauf von IoT-Geräten (Hardware) selbst (Rayes & Salam, 2017).

2.4.5 Einsatzszenarien von IoT in Unternehmen

Nachfolgend sollen Beispiele genannt werden, wie IoT als Technologie in Unternehmen bereits eingesetzt wird und dort Vorteile durch die Vernetzung von Dingen realisiert werden. Viele der in Abschnitt 2.4.1 diskutierten Anwendungsbereiche haben gemein, dass sie aufzeigen, was mittels IoT realisierbar wäre – konkrete Beispiele für (realisierte) IoT-Szenarien sind allerdings wesentlich schwieriger zu finden. Ein solches Beispiel ist der Aufbau eines IoT-Sensornetzwerks für Kohleminen in China. Basierend auf einem Ringnetzwerk und dem Einsatz von Feldbusprotokollen werden in den Minenschächten Sensoren und andere Kontrollsysteme eingesetzt, welche verschiedenste Echtzeitdaten, wie die Position von Arbeitern und das Austreten von gefährlichen Gasen, liefern. Auf Basis dieser Daten kann die Arbeitssicherheit in einer Mine durch die auf den Datenauswertungen basierenden Entscheidungen wesentlich erhöht werden (Chen, Xu, Lui, Hu, & Wang, 2014).

Obwohl es sich nicht direkt um ein Unternehmen handelt[4], kann die Stadt Santander (Spanien) als Beispiel für eine IoT-Integration im Rahmen einer Smart-City-Lösung herangezogen werden. Dabei wurden etwa 10.000 Geräte, wie Sensoren, Kameras, Aktuatoren und RFID-Tags, in der Stadt verteilt und gemäß dem IoT-Paradigma vernetzt. Daten wie Temperatur, Luftdruck, Geräuschpegel und CO_2-Konzentration werden erfasst und den Bürgern zur Verfügung gestellt. Konkrete Projekte wurden dabei auf Basis dieser Daten bereits umgesetzt. Dazu zählen etwa eine Steuerung der Bewässerung öffentlicher Parks, ein Parkleitsystem, Verkehrsüberwachung, eine mobile Erfassung der Luftqualität und Augmented Reality-Anwendungen für Touristen (Medina, Pérez, & Trujillo, 2017).

Diese Beispiele zeigen, dass es sich bei IoT nicht nur um abstrakte Projekte und Ideen, sondern eine bereits im Alltag angekommene Technologie mit viel Potenzial handelt.

2.5 Informationssicherheit

In einem Unternehmen wird IT heutzutage als überlebenswichtiger *Enabler* der Unternehmensaufgaben gesehen. Der anhaltende und starke Trend zur Digitalisierung bewirkt, dass wirtschaftliche Prozesse in Unternehmen zunehmend digital stattfinden. Gleichzeitig sind damit aber auch viele für das Unternehmen negative Auswirkungen verbunden, wenn der Aspekt der Informationssicherheit unzureichend betrachtet wird und es zu Schadensszenarien kommt. Diese Schäden können konkreter materieller (z.B. Produktivitätsverlust, Umsatzverlust) oder immaterieller Art (z.B. Imageverlust, rechtliche Konsequenzen) sein. Ein Problem dabei ist, dass kurz- oder langfristige Auswirkungen fehlender Informationssicherheit nicht sofort ersichtlich sind und die Komplexität dieses Themas, welche durch das Zusammenspiel vieler Systeme entsteht, wenig transparent ist (Gadatsch & Mangiapane, 2017).

[4] gemäß Abschnitt 2.1 kann ein städtisches IKT-Netzwerk aber durchaus in die Kategorie der Unternehmensnetzwerke eingereiht werden

Dieser Abschnitt beleuchtet zum besseren Begriffsverständnis die Zieldimensionen und Grundbegriffe und geht dabei insbesondere auf die Unterscheidung der Begriffe Informationssicherheit und Datenschutz ein. Weiters werden typische Arten von Angriffen sowie übliche Konzepte zur Abwehr beleuchtet. Zudem wird ein Überblick über Standards und Normen in diesem Bereich gegeben, welche eine systematische Betrachtung von Informationssicherheit ermöglichen sollen.

Es ist wichtig zu erwähnen, dass es keine absolute Sicherheit geben kann – weder in der Natur, noch in der Technik. Es handelt sich dabei lediglich um eine Sachlage, die, in diesem Fall für ein Unternehmen, nach gewissen Kriterien betrachtet akzeptabel ist (DIN 31000, 2017).

2.5.1 Unterschiede zwischen Informationssicherheit und Datenschutz

Im Kontext der Informationssicherheit werden weitere Begriffe oftmals verwendet, die jedoch in ihrer Bedeutung unterschieden bzw. voneinander abgegrenzt werden müssen.

2.5.1.1 Informationssicherheit

Als Informationssicherheit wird allgemein definiert, dass sowohl Informationen als auch die zugehörigen Daten, Systeme und Prozeduren zu schützen sind, welche Informationen für das Unternehmen enthalten, liefern, verarbeiten oder speichern (Königs, 2013).

2.5.1.2 Datenschutz

Der Datenschutz bezieht sich auf die Verarbeitung personenbezogener Daten, welche als besonders schützenswert erachtet werden und deswegen besonderen Rahmenbedingungen unterliegen.

Der Datenschutz manifestiert sich in einer gesetzlichen Anforderung an ein Unternehmen und erhält dadurch eine immer höhere Wichtigkeit hinsichtlich Compliance. Eine große Herausforderung ist dabei die große Anzahl an Beteiligten in den Dienstleistungsketten heutiger Informationsverarbeitung. Beispiele dafür sind die zunehmende Nutzung von sozialen Netzwerken, Cloud-Computing oder die mittlerweile verbreitete Nutzung mobiler Geräte und ihrer Möglichkeiten im Bereich Ton-, Bild- und Videoaufzeichnungen (Königs, 2013).

Im englischsprachigen Raum werden hierfür zwei Begriffe verwendet: *Privacy* (etwa „Schutz der Privatsphäre“) und *Data Protection*.

2.5.1.3 Gegenüberstellung der Begriffe

Der Begriff der Informationssicherheit gemäß obiger Definition ist weiter gefasst als der oftmals verwendete Begriff IT-Sicherheit (*IT-Security*). Beispielsweise trägt die Verfügbarkeit von IT-Systemen auch zur Verfügbarkeit von Informationen bei, da damit die angeforderten Informationen dem Benutzer bzw. der Benutzerin zur vorgesehenen Zeit zur Verfügung stehen. Informationssi-

cherheit bezieht sich aber nicht nur auf die technische (IT-)Infrastruktur, sondern auch auf Informationen in nichttechnologischer Form, etwa auf Papier. Dieser Zusammenhang ist in Abbildung 5 grafisch dargestellt. In der weiteren Arbeit wird primär auf Informationssicherheit im digitalen Kontext Bezug genommen, wenngleich für die erfolgreiche Sicherstellung von Informationssicherheit in einem Unternehmen auch die Betrachtung analoger oder abstrakter Assets notwendig ist. Das gilt insbesondere, da sich z.B. durch prozessuale Schwächen Risiken für die digitale Informationssicherheit ergeben können (siehe auch Kapitel 5).

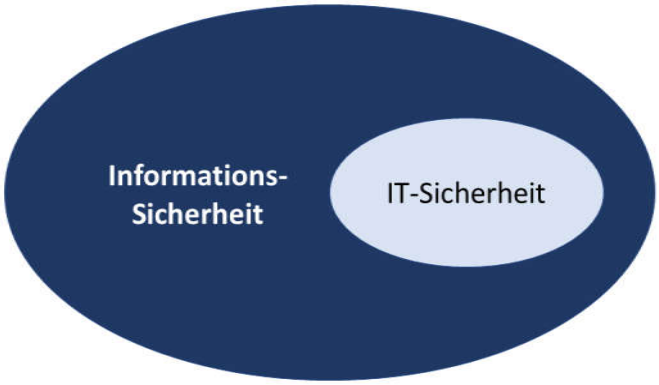

Abbildung 5: Kontextueller Zusammenhang zwischen IT- und Informationssicherheit, nach (Königs, IT-Risikomanagement mit System. 4. Auflage, 2013)

Der Datenschutz kann ebenso im Rahmen der Informationssicherheit betrachtet werden, da es sich letztendlich um Daten handelt. Zwar unterliegt der Datenschutz speziellen Bedingungen, es liegt aber auf Grund der thematischen Ähnlichkeit nahe, diese Themen gemeinsam zu betrachten (Schonschek, 2018). Dabei gibt es natürlich Aspekte, die ausschließlich auf eines der beiden Felder zutreffen, doch es liegt auch eine Schnittmenge vor (siehe Abbildung 6).

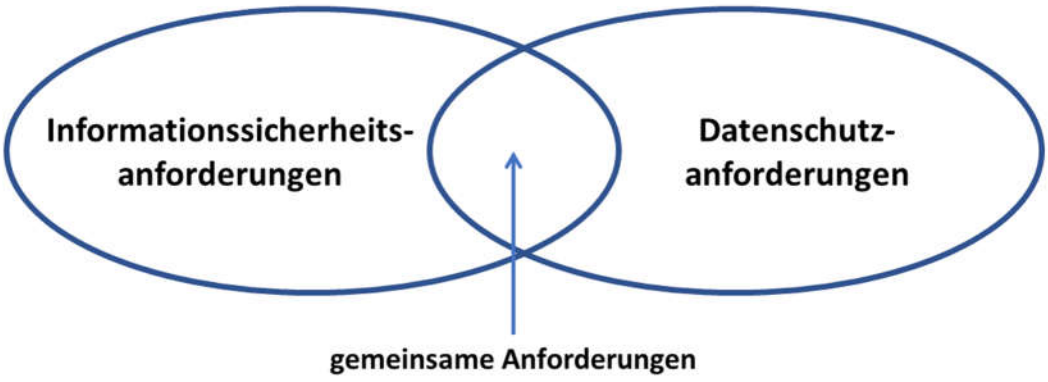

Abbildung 6: Zusammenhang zwischen Informationssicherheit und Datenschutz nach NIST SP800-53 (NIST, 2013)

Ein weiterer Begriff, der in diesem Kontext immer wieder auftaucht, ist der Begriff Cybersecurity. Gemäß einer Definition von Gartner aus 2013 umfasst dieser Begriff als Überbegriff der Informationssicherheit zusätzlich den Aspekt der „offensiven“ Sicherheit (siehe Abbildung 7), d.h. auch Angriffe. Da dies in den meisten Teilen der Welt strafbar sein dürfte, ist dieser Begriff wohl nicht auf Unternehmen, sondern nur auf staatliche Stellen anwendbar (Rout, 2015).

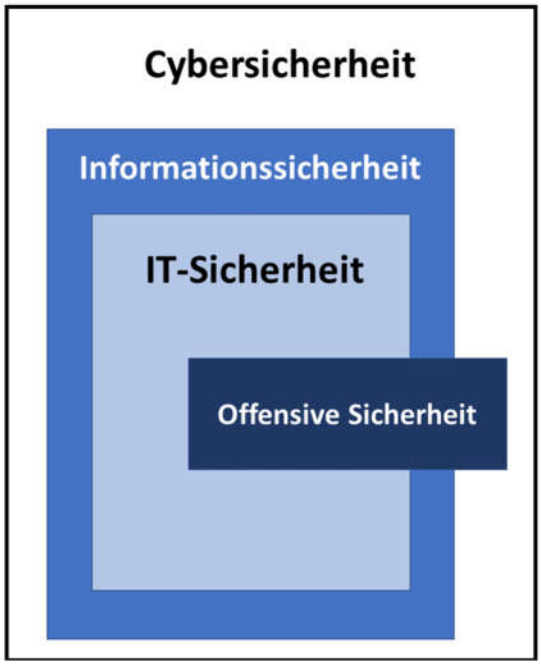

Abbildung 7: Zusammenhang zwischen Informationssicherheit und Cybersecurity, nach (Rout, 2015)

Eine andere Definition von Cybersicherheit ist die Anwendung der Prinzipien der Informationssicherheit auf große Netzwerke, so wie beispielsweise dem Internet (Bartsch & Frey, 2018). Da in der Folge die Eingrenzung der Domäne auf ein Unternehmensnetzwerk erfolgt, wird der Begriff Informationssicherheit beibehalten.

Ein weiterer Problemfall bei der Begriffsdefinition ist der Umstand, dass die beiden englischen Begriffe *Safety* und *Security* im Deutschen mit Sicherheit übersetzt werden. Es besteht jedoch in der Tat ein Bedeutungsunterschied. Mit *Safety* wird im Allgemeinen eine Unfallvermeidung bzw. der Schutz von Menschen und Umwelt vor physischem Schaden bezeichnet, mit *Security* die Informationssicherheit (Geiger, 2018). Allgemein ausgedrückt: *Safety* bezeichnet die Unfähigkeit eines Systems, die Umwelt unerwünscht zu beeinflussen, während *Security* die Unfähigkeit der Umwelt bezeichnet, ein System unerwünscht zu beeinflussen (Line, Rostad, Nordland, & Tondel, 2006).

Diese Begriffsunterscheidungen und die Definition der Informationssicherheit als allgemeiner Überbegriff im Sinne der *Security* werden im weiteren Verlauf der Arbeit beibehalten.

2.5.2 Ziele von Informationssicherheit

Um Gefahren im Kontext von Informationssicherheit anschaulich darzustellen und ein Modell bilden zu können, werden sogenannte „Schutzobjekte“ (engl. *Assets*) gebildet. Der englische Begriff verdeutlich besser, dass es um Werte eines Unternehmens geht, die es zu schützen und zu erhalten gilt. Diese Werte können entweder materiell (z.B. Hardware) oder immateriell (z.B. Daten, Informationen, Image) sein. Informationen sind durch ihre enorm wichtige Rolle für die heutige Gesellschaft und damit auch die darin agierenden Unternehmen eine (über-)lebenswichtige Ressource geworden. Eine endlose Anzahl von abstrakten Informationen und die für die Verarbeitung

notwendigen Grundlagen wie Computer, Netzwerke und Energieversorgung stellen das reibungslose Funktionieren von Prozessen in der technisierten Gesellschaft sicher. Beispielhaft erwähnt seien hier Finanz- und Zahlungsinformationen für den bargeldlosen Zahlungsverkehr, Konstruktionspläne für Häuser, Maschinen oder Geräte (Königs, 2013).

„Information" ist in diesem Zusammenhang nicht Synonym zum Begriff „Daten" zu verwenden. Im Kontext der IT ist der Begriff Information weiter gefasst und umfasst neben den computerlesbar vorhandenen Daten auch weitere Attribute oder Metainformationen welche ihnen zugeordnet werden können, so dass sie damit einen *Kontext* haben (Gadatsch & Mangiapane, 2017). Dieser Bedeutungskontext und der Umstand, dass diese so vorliegenden Daten als Entscheidungsgrundlage für das betriebswirtschaftliche Handeln dienen, definiert in diesem Umfeld den Begriff der Information (North, Brandner, & Steininger, 2016).

Bei diesen wichtigen Objekten aus der Kategorie „Information" gibt es drei primäre Schutzziele:

- Vertraulichkeit
- Integrität
- Verfügbarkeit (Königs, 2013).

Vertraulichkeit ist dann gegeben, wenn eine Information niemals gegenüber einem unberechtigten Individuum oder Prozess zugänglich gemacht oder offengelegt wird. **Integrität** bezeichnet den Zustand eines Werts, wenn Richtigkeit und Vollständigkeit gewähreistet sind. **Verfügbarkeit** ist gegeben, wenn einer berechtigten Entität (Individuum, Prozess) Zutritt, Zugang oder Zugriff gewährt wird, wenn diese es verlangt. Im Zusammenhang bedeutet dies, dass die Vertraulichkeit die Verfügbarkeit einschränkt (Klipper, 2011). Als Subaspekt der Verfügbarkeit kann der Begriff der **Datenexistenz** eingeführt werden. Der Verlust gespeicherter Daten schränkt implizit die Verfügbarkeit ein (Gadatsch & Mangiapane, 2017).

In weiterer Folge gibt es auch noch das Schutzziel „Non-Repudiation" (deutsch in etwa „Nicht-Abstreitbarkeit", **Verbindlichkeit**), welches zwei Sichten beinhaltet (sichergestelltes Senden/Empfangen). Für Königs (2013) zählt es nicht zu den primären Schutzzielen, da es erst durch eine Prozedur der Beweisführung zustande kommt und keine immanente Eigenschaft ist.

Informationssicherheit muss sich durch die Digitalisierung von Prozessen und unternehmerischen Vorgängen auch mit weiteren Aspekten zur Sicherstellung von Leistungsfähigkeit, Qualität und Vertrauenswürdigkeit von IT-Prozessen beschäftigen. Die schutzwürdigen Systemziele in diesem Kontext können wie folgt zusammengefasst werden:

- Effektivität
- Effizienz
- Zuverlässigkeit
- Compliance

Effektivität bedeutet in diesem Zusammenhang, dass für Geschäftsprozesse notwendige und relevante Informationen zeitgerecht, aktuell und fehlerfrei in verwendbarer Form geliefert werden.

Die Bereitstellung soll dabei mit einer optimalen Verwendung von Ressourcen erfolgen (**Effizienz**). Die **Zuverlässigkeit** bezieht sich hier auf die Eignung der bereitgestellten Informationen zur Steuerung von Unternehmensentscheidungen durch das Management und zur korrekten, gesetzestreuen Berichterstattung. Dieses Ziel ist nicht mit der zuvor erwähnten Verfügbarkeit zu verwechseln. Als **Compliance** wird die Einhaltung von rechtlichen und vertraglichen, internen und externen Erfordernissen und Vorgaben bei der Ausführung der Geschäfts- und IT-Prozesse verstanden (Königs, 2013).

2.5.3 Organisatorische Behandlung von Informationssicherheit

Sicherheit ist kein erreichbarer Zustand, der durch einmaliges Agieren erreicht werden kann, sondern eine permanente Aufgabe. Idealerweise wird Sicherheit als formeller Management-Prozess aufgesetzt, wodurch sich die Permanenz dieses Themas gut darstellen lässt. Die Aufgaben dieser Prozesse sind ein akzeptables Sicherheitsniveau zu konzipieren, zu erreichen und danach auch aufrechtzuerhalten. Dazu kommt die Forderung nach notwendigen Anpassungen, wenn sich Anforderungen ändern, und ein allgemeines Bestreben nach Weiterentwicklung und Verbesserung. Deswegen sind eine klare Aufgabenbeschreibung und Definition personeller Verantwortlichkeiten für das Management der Informationssicherheit notwendig. Eine anerkannte Praxis dabei ist es, die Wahrnehmung dieser Managementaufgaben direkt der Leitung des Unternehmens zu unterstellen, zumindest jedoch einen direkten Berichtsweg zur Leitungsebene sicherzustellen. Es spielt dabei keine unmittelbare Rolle, ob diese Aufgabe von einer einzelnen Person (z.B. einem IT-Sicherheitsbeauftragten) oder durch eine Gruppe wahrgenommen wird (Kersten & Klett, 2015). Die Ziele der Durchführung dieser Aufgaben orientieren sich an der Ausrichtung der Unternehmensstrategie und schaffen Mehrwerte durch Investitionen in die Informationssicherheit, welche die strategischen Ziele des Unternehmens unterstützen. Das erwähnte *akzeptable Sicherheitsniveau* ist dabei jenes, welches die Informationssicherheitsrisiken so weit reduziert, dass die Auswirkungen für das Unternehmen tragbar oder akzeptabel sind. Als Überbegriff für all diese Aufgaben kann der Begriff der (Corporate) *Security Governance* verwendet werden (Gerbino, 2017).

Um einen strukturierten Informationssicherheitsmanagementprozess zu ermöglichen, gibt es mittlerweile durch jahrzehntelange Erfahrung praktisch erprobte Vorgehensmodelle für das Informationssicherheitsmanagement, deren Anwendung als nutzbringend angesehen werden kann (Kersten & Klett, 2015). Verbreitete Beispiele dafür werden in Abschnitt 2.5.5 behandelt.

Eine der wesentlichen Aufgaben dieses Prozesses ist es, in Abstimmung mit der Unternehmensleitung eine IT-Sicherheitsrichtlinie (IT Security Policy) zu erarbeiten und diese durch die Leitung in Kraft setzen zu lassen. Diese Richtlinie sollte folgende Punkte bzw. Aufgaben behandeln:

- Ableitung eines Sicherheitskonzeptes[5] aus der Richtlinie
- Prüfung der Einhaltung des Sicherheitskonzeptes

[5] Ein solches Konzept enthält u.a. die individuell betrachteten und bewerteten Informationssicherheitsrisiken, Gegenmaßnahmen und deren Wirksamkeit sowie eine Darstellung des verbliebenen Restrisikos. Siehe dazu auch Abschnitt 5.1

- Behandlung von Sicherheitsvorfällen
- Regelmäßige Wartung der enthaltenen Dokumentationsvorschriften, Prozesse und Maßnahmen
- Planung und Umsetzung von Sensibilisierung, Schulung und Training der Mitarbeiter und Mitarbeiterinnen

Bei Großkonzernen kann es notwendig sein, diese Richtlinie hierarchisch in mehrere Teilbereiche aufzuspalten, einzelne Bestandteile der Richtlinie sind zudem nur in größeren Unternehmen notwendig bzw. in kleineren Unternehmen entsprechend angepasst durchzuführen (Kersten & Klett, 2015).

Um diese Themen systematisch zu behandeln und auch die Einhaltung des geplanten Sicherheitsniveaus sicherzustellen, kann ein Informationssicherheitsmanagementsystem (ISMS) eingeführt werden. Im Rahmen des ISMS werden geeignete Prozesse, Verantwortlichkeiten, Verfahren, Ressourcen und Hilfsmittel sowie eine entsprechende Aufbauorganisation festgelegt und (nachweisbar) umgesetzt. Das erfordert eine ganzheitliche und praxiserprobte Methodik, damit dies unter Berücksichtigung interner und externer (z.B. gesetzlicher) Vorgaben erfolgen kann. In verschiedenen Standards und Best Practices wie der Normenreihe ISO/IEC 27000 oder dem IT-Grundschutzkatalog des BSI (siehe Abschnitt 2.5.5) finden sich, in unterschiedlicher Ausprägung, Konkretisierung und Qualität, verschiedene Teilbereiche und Kernelemente eines ISMS (Müller, 2018).

Wie bereits in Abschnitt 2.5.1 dargelegt wurde, sind Informationssicherheit und Datenschutz nicht deckungsgleich. Eine entsprechende Erweiterung des ISMS um datenschutzrechtliche Aspekte empfiehlt sich daher, falls kein eigenes Datenschutzmanagementsystem eingesetzt wird (Schonschek, 2018).

2.5.4 Begriffsunterscheidungen im Zusammenhang mit Informationssicherheit

In den folgenden Teilen der Arbeit werden immer wieder Begriffe verwendet, die im Themenbereich der Informationssicherheit oftmals falsch oder zumindest unscharf verwendet werden. Daher soll an dieser Stelle eine für diese Arbeit gültige Definition dieser Begriffe erfolgen.

Eine **Schwachstelle** (engl. *vulnerability*) ist ein (sicherheitsrelevanter) Fehler in einem IT-System oder einer Organisation. Ursachen können in der Konzeption, den verwendeten Algorithmen, der Implementation, der Konfiguration, dem Betrieb oder der Organisation selbst liegen (BSI, 2019).

Eine **Bedrohung** ist ein Umstand oder Ereignis, der oder das die Verfügbarkeit, Integrität oder Vertraulichkeit von Informationen beeinträchtigen, wodurch dem Besitzer oder der Besitzerin bzw. dem Benutzer oder der Benutzerin der Informationen ein Schaden entstehen kann. Beispiele dafür sind höhere Gewalt, technisches oder menschliches Versagen und vorsätzliche Handlungen (BSI, 2019).

Eine **Gefährdung** ist eine Bedrohung, die konkret über eine Schwachstelle auf ein Schutzobjekt einwirkt. Eine Bedrohung wird erst durch eine vorhandene Schwachstelle (insbesondere techni-

sche oder organisatorische Mängel) zur Gefährdung. Zur Veranschaulichung sei ein Computervirus genannt: Ein Anwender ist dadurch erst gefährdet, wenn sein Computer anfällig für den konkreten Virentyp ist (BSI, 2019).

Etwas problematisch ist in diesem Fall der Umstand, dass der in der englischen Literatur oft verwendete Begriff *threat* sich sowohl mit Bedrohung als auch Gefährdung übersetzen lässt, wodurch eine gewisse Bedeutungsunschärfe entsteht.

Ein **Angriff** ist eine unerwünschte oder unberechtigte Handlung mit dem Ziel, sich Vorteile zu verschaffen und/oder einen Dritten zu schädigen. Er stellt damit eine vorsätzliche Form der Gefährdung dar (BSI, 2019).

Als **Schaden** kann in diesem Kontext grundsätzlich jedes Ergebnis bezeichnet werden, das eines der drei wesentlichen Schutzziele der Informationssicherheit verletzt, also Vertraulichkeit, Integrität oder Verfügbarkeit von Informationen bzw. Daten. Ob und welche anderen konkreten (z.B. wirtschaftliche, persönliche bzw. materielle/immaterielle) Schäden dadurch entstehen, ist vom Einzelfall abhängig.

Als **Maßnahmen** (eng. *controls*) werden sämtliche Vorkehrungen bezeichnet, die ein Asset schützen können. In diesem Kontext kann eine Schwachstelle auch als Stelle mit ungenügenden oder fehlenden Maßnahmen gesehen werden.

Eine vereinfachte Formulierung des wesentlichen Zusammenhangs lautet: Bedrohungen verursachen über Schwachstellen an Assets (Schutzobjekten) Schäden (Königs, 2013), welche durch entsprechende Schutzmaßnahmen abgewehrt werden können.

2.5.5 Vorgehensmodelle, Normen und Standards

Methodische Vorgehensweisen zur Sicherstellung von Informationssicherheit sind sinnvoll, um nicht Gefahr zu laufen, Aspekte zu übersehen und damit Bereiche ohne entsprechende Maßnahmen Bedrohungen auszusetzen. Nachfolgend werden einige allgemeine und branchenspezifische Normen bzw. Best-Practice-Sammlungen dargestellt. Neben diesen gibt es auch noch zwei Sonderfälle, nämlich gesetzliche Vorgaben zu den Themen Datenschutz und Informationssicherheit, welche ebenso kurz erläutert werden.

Diese Modelle können, wie in Abschnitt 5.3 dann auch gezeigt, einerseits dazu dienen, relevante Handlungsfelder der Informationssicherheit zu identifizieren und zu behandeln. Auf der anderen Seite sind bei gewissen Standards Zertifizierungen möglich, so dass ein Unternehmen nach außen hin nachweisen kann, dass ein hoher Standard an Informationssicherheit erreicht wurde. Dies kann bei der Einhaltung von vertraglichen Bedingungen hilfreich sein, da dies mittlerweile durchaus von Kunden oder Lieferanten gefordert wird (Schuster, 2019).

2.5.5.1 ISO27000-Reihe

Die Normenreihe ISO/IEC 27000:2013 mit dem Titel „Informationstechnik – Sicherheitsverfahren – Informationssicherheitsmanagementsysteme“ beschreibt einen Standard für ISMS. In der ISO/IEC 27000 selbst erfolgt die Definition wesentlicher Begriffe. So ist ein **Kontrollelement** dabei eine Maßnahme, die ein **Risiko** (Auswirkung von Unsicherheit auf Ziele) verändert (siehe auch Abschnitt 5.1). Die weiteren Standards werden in drei Kategorien unterteilt. Die erste Gruppe (27001, 27006) legt Anforderungen fest, während die zweite Gruppe (u.a. 27002, 27003, 27004, 27005, 27013, 27014) allgemeine Richtlinien enthält. Die dritte Gruppe enthält sektorspezifische Anforderungen (z.B. 27011 für Telekommunikationsunternehmen, 27018 zum Schutz personenbezogener Daten, 27019 für Energieversorger). Nachfolgend werden einige Standards näher beschrieben:

- **ISO/IEC 27001:2013**: Innerhalb dieser Norm werden u.a. die Themen Organisation, Führung, Planung, Betrieb und Verbesserung behandelt. Sie folgt dabei einem PDCA-Zyklus (Plan/Do/Check/Act). Es werden in diesem Kapitel der Geltungsbereich des ISMS, die Darlegung der Führungsrolle, Festlegung von Prozessen, Ressourcen- und Kompetenzplanung, Betriebsprozesse und Risikobewertungen, Leistungsbewertungskriterien der Umgang mit Nicht-Konformität behandelt. Ein Anhang führt Kontrollziele und Kontrollen zu verschiedenen Themenfeldern an.
- **ISO/IEC 27002:2013**: Unter dem Titel „Leitfaden für Informationssicherheitsmaßnahmen“ verbirgt sich einer der wesentlichen Teile dieser Norm. Sie behandelt insgesamt vierzehn Themenfelder, wobei je Thema ein Ziel definiert, Kontrollelemente und – als wesentlicher Teil – Implementierungsanleitungen gegeben werden. Die behandelten Themen umfassen unter anderem die Informationssicherheitspolitik und -Richtlinien, die Organisation der Informationssicherheit, Ziele für die Zugangs- und Zugriffskontrolle, Betriebs- und Kommunikationssicherheit, Beschaffung, Entwicklung und Wartung sowie das Management sicherheitsrelevanter Ereignisse.
- **ISO/IEC 27004:2013**: Dieser Standard enthält Richtlinien zur Bewertung der Leistungsfähigkeit des Informationssicherheitsmanagements, also wie diese im Rahmen von Prozessen gemessen und evaluiert werden kann.
- **ISO/IEC 27005:2013**: Im Rahmen dieser Norm wird ein Risikomanagementprozess definiert. Sie enthält die Festlegung des Geltungsbereichs, eine definierte Vorgehensweise und die Kriterien bei der Risikobewertung sowie die Risikobehandlung.
- **ISO/IEC 27014:2013**: Im Rahmen dieses Standards wird die Governance der Informationssicherheit behandelt, d.h. ein System, mit dem sich die Aktivitäten zur Informationssicherheit steuern und überwachen lassen.
- **ISO/IEC 27017:2013**: Innerhalb dieser Richtlinie werden Rahmenbedingungen für Informationssicherheit bei Bereitstellung und Nutzung von Cloud-Services behandelt. Es wird insbesondere definiert, welche Teile der ISO/IEC 27002 in diesem Fall unverändert anwendbar sind oder ob zusätzliche Implementierungshinweise zu beachten sind.

Interessant im IoT-Kontext sind für Unternehmen sicherlich auch noch die Normen 27033 (Netzwerksicherheit) und 27034 (Applikationsmanagement) (Müller, 2018).

Die ISO 27001 spielt auch im Zusammenhang mit der DSGVO (siehe Abschnitt 2.5.5.5) eine relevante Rolle, da eine Einhaltung bzw. Zertifizierung als Garantie gemäß den Artikeln 28 und 32 DSGVO (Auftragsverarbeitung bzw. Datensicherheitsmaßnahmen) gelten kann (Schuster, 2019).

2.5.5.2 BSI Grundschutz

Das deutsche Bundesamt für Informationssicherheit hat unter der Bezeichnung IT-Grundschutz eine Reihe von Empfehlungen veröffentlicht, welche sich mit verschiedenen Aspekten der Informationssicherheit und dem Informationssicherheitsmanagement befassen. Die grundlegende Veröffentlichung ist das sog. IT-Grundschutz-Kompendium. Die Bausteine dieses Kompendiums sind in zehn Schichten aufgebaut und befassen sich mit unterschiedlichsten Themen der Informationssicherheit, von Anwendungen über industrielle Sicherheit bis hin zum Themengebiet ISMS. Das Kompendium unterscheidet dabei zwischen Prozess- und Systembausteinen und schlägt dabei eine spezifische Umsetzungsreihenfolge der Bausteine vor, da sie teilweise aufeinander aufbauen. Zu den Bausteinen gibt es auch entsprechende Umsetzungshinweise (BSI, 2019b), (BSI, 2019c).

Zusätzlich gibt es im Rahmen der sog. 200er-Reihe einige Standards, welche sich auf die Themen ISMS (200-1), die Methodik des Grundschutzes (200-2) sowie die Risikoanalyse auf der Basis des IT-Grundschutzes (200-3) beziehen. Im Bezug auf das Notfallmanagement gibt es noch den Standard 100-4 aus 2008 (Müller, 2018).

2.5.5.3 NIST Cybersecurity Framework

Das Cybersecurity Framework des US-amerikanischen *National Institute of Standards and Technology* (NIST) ist eine auf einer Verfügung des US-Präsidenten (Executive Order, kurz EO Nr. 13636) basierende Sammlung an nicht verbindlichen Ratschlägen innerhalb eines organisatorischen Rahmenwerks (Framework). Dieses soll gemäß der Verfügung unter anderem eine priorisierte, flexible, wiederholbare und kosteneffektive Liste an Ansätzen für Maßnahmen zur Erkennung und Behandlung von Risiken im Umfeld der Cybersecurity liefern.

Dass hier explizit auf Cybersecurity abgestellt wird, ist mit obiger Definition dieses Begriffes nur bedingt vereinbar, da hier im Wesentlichen auf Betreiber kritischer Infrastruktur abgestellt wird, diese aber nicht zwingend öffentlich sind und damit auch kein Mandat zu „aktiven“ Aktivitäten besitzen. Es wird daher davon ausgegangen, dass die diesem Framework zugrundeliegende Definition von Cybersecurity den hier definierten Begriff der Informationssicherheit inkl. IT-Security meint. Das zeigt sich an den darin befindlichen Handlungsempfehlungen.

Im Rahmen des Frameworks wird eine risikobasierte Vorgangsweise zur Behandlung von Informationssicherheit als grundlegend notwendig erachtet, wobei es als flexibel genug dafür angesehen wird, verschiedene ggf. bereits im Unternehmen implementierte Risikomanagementprozesse zu unterstützen.

Obwohl dieses Framework für einen speziellen Sektor und auf gesetzliche Anweisung hin von einer öffentlichen, amerikanischen Organisation erstellt wurde, ergibt sich durch die Struktur und den intensiven Verweis auf allgemeine Standards insbesondere im *Framework Core* doch eine allgemeine Anwendbarkeit für eine Vielzahl von Organisationen und Branchen.

2.5.5.4 NIST Special Publication 800-53 (Revision 5)

War dieser von der NIST herausgegebene Standard für Informationssicherheit und Datenschutz bis Revision 4 explizit für US-amerikanische Bundesbehörden geschrieben („*Security and Privacy Controls for Federal Information Systems and Organizations*"), so wurde mit Revision 5 zumindest im vorliegenden Entwurf ein wesentlich breiterer Ansatz gewählt. Der Titel lautet nun *Security and Privacy Controls for Information Systems and Organizations*, womit dieser eine wesentlich breitere Anwendbarkeit suggeriert. In der Tat handelt es sich um eine umfangreiche, beinahe 500 Seiten umfassende Sammlung an Maßnahmen zur Sicherstellung von Informationssicherheit. Da diese nicht nur von gesetzlichen Anforderungen oder Verfügungen abgeleitet wird, sondern auch allgemeine Bedrohungen wie feindliche Angriffe, Naturkatastrophen, strukturelle und menschliche Fehler sowie Aspekte der Privatsphäre/Datenschutz beinhaltet, kann diese sehr aktuelle Publikation als universell anwendbar eingestuft werden.

Da dieser Maßnahmenkatalog ebenso von der NIST erstellt wird, ist eine tiefe Integration mit dem zuvor vorgestellten NIST Security Framework erkennbar und gemäß den Autoren auch durchaus gewollt – wenngleich darin festgehalten wird, dass dies keine Voraussetzung darstellt, sondern dieser Maßnahmenkatalog auch explizit in anderen Risikomanagementansätzen eingesetzt werden kann.

Das erste inhaltliche Kapitel (*Chapter Two*) befasst sich umfassend mit fundamentalen Zusammenhängen zwischen Anforderungen und Maßnahmen sowie der Struktur des Maßnahmenkatalogs. Das umfangreichste Kapitel (*Chapter Three*) ist dann der eigentliche Katalog, in welchem die Maßnahmen ausführlich dargestellt und auch begründet werden. Dabei werden Aspekte der Informationssicherheit und des Datenschutzes gemeinsam behandelt. Inwieweit insbesondere die Aspekte des Datenschutzes dem geltenden europäischen Recht entsprechen (siehe insb. 2.5.5.5), ist für ein Unternehmen jeweils individuell zu betrachten.

Des Weiteren finden sich zahlreiche Anhänge wie Glossare, Zusammenfassungen und Zusammenhänge mit anderen internationalen Standards in der Publikation.

2.5.5.5 Sonderfall Datenschutzgrundverordnung (DSGVO)

Die seit 25.5.2018 in Kraft befindliche **DSGVO** ist kein optional anwendbarer Standard, sondern eine in allen EU-Mitgliedsländern gültige gesetzliche Vorgabe der Europäischen Union und damit

ein wesentlicher Aspekt der (IT-) Compliance eines Unternehmens. Das Ziel der DSGVO ist (so im Titel der Verordnung ersichtlich) der „Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten“ (EU, 2016). Explizit wird hier auf personenbezogene Daten abgestellt, was eine Untermenge der üblicherweise durch ein Unternehmen verarbeiteten Daten darstellt. Damit ist der Datenschutz eine Teilmenge der Informationssicherheit, welcher aber besonderen (gesetzlichen) Bedingungen unterliegt.

Genauso wie für die Informationssicherheit gelten die Grundsätze der Vertraulichkeit, Integrität und Verfügbarkeit[6] dieser Daten. Es sind bei der Verarbeitung geeignete technische und organisatorische Maßnahmen zu treffen, um ein angemessenes Schutzniveau zu erreichen[7], zum Beispiel Pseudonymisierung und Verschlüsselung von Daten und andere Maßnahmen zur Vermeidung von Sicherheitsverletzungen. Zu diesen Anforderungen gibt es noch eine Reihe von Grundsätzen zur Verarbeitung (Zweckbindung, Datenminimierung, Richtigkeit, ...) sowie generelle Einschränkungen (notwendige Einwilligung der betroffenen Person). Zudem haben die betroffenen Personen gewisse Rechte gegenüber dem Verarbeiter, so zum Beispiel ein Auskunfts- und Widerspruchsrecht. Bei einer Verletzung des Schutzes personenbezogener Daten muss binnen 72 Stunden eine Meldung bei der zuständigen Aufsichtsbehörde erfolgen, unter gewissen Bedingungen müssen auch die betroffenen Personen informiert werden (Burgstaller, 2016). Die hier erwähnten Punkte stellen nur einen Auszug aus den umfangreichen Vorgaben der DSGVO dar, eine genaue Betrachtung dieser Verordnung ist für jedes Unternehmen alleine auf Grund des hohen möglichen Strafmaßes von bis zu 20 Millionen € oder 4% des weltweiten Jahresumsatzes (Voigt & Bussche, 2018) ratsam.

Die DSGVO selbst nennt keine konkreten technischen oder organisatorischen Maßnahmen, sondern schreibt einen im Einzelfall zu bestimmenden Umsetzungsgrad des „Stands der Technik“ vor – allerdings mit wenig Anhaltspunkten dazu. Da jedoch eben Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit explizit genannt werden (Bartels & Backer, 2018), kann eine entsprechende Betrachtung bzw. Umsetzung der in den zuvor genannten Standards und Publikationen diskutierten Maßnahmen wohl einen guten Anhaltspunkt darstellen (siehe auch Kapitel 3).

2.5.5.6 Sonderfall NIS-Richtlinie

Eine weitere Sonderstellung nimmt die EU-Richtlinie 2016/1148 ein, welche die erste EU-weite Regelung zum Thema Informationssicherheit darstellt. Sie trägt den Titel *Richtlinie über Maßnahmen zur Gewährleistung eines hohen Sicherheitsniveaus von Netz- und Informationssystemen in der Union*, ist aber unter dem Kurztitel NIS-Richtlinie (NIS-RL) geläufig. Sie bildet einen Rechtsrahmen für den EU-weiten Aufbau von Kapazitäten für die Cybersicherheit (sic!), einer stärkeren

[6] Zu diesen drei Zielen kommt in der DSGVO auch „Belastbarkeit“ der Systeme hinzu, als die Fähigkeit, trotz Störungen wieder in einen stabilen Ausgangszustand zurückzukehren (Kamp, 2018).

[7] Es zeigt sich aus der Verwendung von Begriffen wie „geeignet“ und „angemessen“, dass die DSGVO keine konkreten Vorgaben macht, sondern diese immer auf den Einzelfall bezogen interpretiert und angewendet werden müssen.

Zusammenarbeit der Nationalstaaten, sowie Mindestanforderungen und Meldepflichten für kritische Infrastrukturen sowie bestimmter Anbieter digitaler Dienstleistungen (z.B. Cloud-Services und Online-Marktplätzen). Diese Richtlinie musste bis Mai 2018 in nationalem Recht umgesetzt werden (BSI, 2019b), in Österreich ist dies im Rahmen des Netz- und Informationssystemsicherheitsgesetzes (NISG) mit 29.12.2018 erfolgt (RIS, 2019).

Im Fokus der NIS-RL stehen sog. Betreiber wesentlicher Dienste (BwD), welche öffentliche oder private Einrichtungen in verschiedenen Bereichen wie Energie, Verkehr, Gesundheitswesen, Bankwesen oder Trinkwasserversorgung sind. Die wesentlichen daraus erwachsenden Pflichten sind geeignete und verhältnismäßige technische und organisatorische Sicherheitsvorkehrungen sowie z.B. die unverzügliche Meldung von Sicherheitsvorfällen (Becker, 2018). Das Gesetz sieht dabei für betroffene BwD eine Verpflichtung zur Übermittlung einer Aufstellung der vorhandenen Sicherheitsvorkehrungen sowie eines Zertifizierungsnachweises durch qualifizierte Stellen vor. Aus dem Gesetzestext selbst geht keine expliziter Standard hervor, nachdem dies zu erfolgen hat (RIS, 2019), jedoch lassen verschiedene Quellen darauf schließen, dass dies im Regelfall über eine Zertifizierung nach ISO 27001 (s.o.) mit zusätzlichen Anforderungen (z.B. ISO 27019 für Leitsysteme, ISO 22301 für Business Continuity) erfolgen kann (CIS, 2018), (Tretzmüller, 2018), (IT Governance Europe, 2016).

2.5.5.7 Normen aus dem Produktionsumfeld

Die beschriebenen und auch weithin etablierten Normen und Ansätze zur Sicherstellung von Informationssicherheit beziehen sich allerdings in weiten Teilen auf „Office IT“ und sind nicht ohne weiteres auf das Produktionsumfeld übertragbar[8]. Daher gab und gibt es national wie international Bestrebungen, Normen und Empfehlungen auch für die IT-Sicherheit in der Anlagen-IT und dem Produktionsumfeld zu entwickeln. Da ein großer Anwendungsbereich von IoT (insb. IIoT) auf diesen Bereich entfällt, soll auch ein kurzer Blick auf diese Standards geworfen werden.

IEC 62443

Diese von der IEC 2008 veröffentlichte technische Spezifikation behandelt das Themengebiet der IT-Sicherheit für industrielle Leitsysteme. Sie empfiehlt ein ganzheitlich betrachtetes IT-Sicherheitsmanagement und beinhaltet konkrete technische (z.B. Zugriffskontrollen, Verschlüsselung, Anwendungssicherheit) und auch organisatorische (z.B. Bedrohungsanalyse, Risikobewertung) Sicherheitsmaßnahmen (Sowa, 2017).

VDI/VDE Richtlinie 2182

In dieser Richtlinie zur IT-Sicherheit in der industriellen Automatisierung ist ein Vorgehensmodell zu Bewertung von IT-Risiken enthalten. Dieses generische Modell beginnt bei der Identifikation von Assets und Bedrohungen und beinhaltet in der Folge Vorgaben zur Bewertung von Risiken

[8] Der BSI-Grundschutz wurde aus diesem Grund mittlerweile um einige Aspekte (Bausteine) hinsichtlich der IT-Sicherheit industrieller Steuerungen erweitert. Daneben existiert für dieses Anwendungsfeld das *ICS* (Industrial Control System) *Kompendium* des BSI (Sowa, 2017).

und Schutzzielen sowie der Auswahl geeigneter Schutzmaßnahmen. Auch Audits sind hier explizit vorgesehen. In weiteren Teilen der Richtlinie sind Umsetzungshinweise für Hersteller und Integratoren zu konkreten Einsatzszenarien wie *Speicherprogrammierbaren Steuerungen* (SPS) und anderen Anlagen beschrieben (Sowa, 2017).

ISO/IEC TR 27019

Die seit dem Jahr 2013 verfügbar ISO/IEC-Spezifikation widmet sich branchenbezogen dem Management der Informationssicherheit für Prozessleitsysteme und Automatisierungstechnik in der Energieversorgung. Sie passt die Anforderungen aus der ISO:27002-Norm an diesen in seinen Gegebenheiten sehr spezifischen Bereich an und hält sich dabei an die Gliederung ebendieser. Die hier enthaltenen Erläuterungen und Maßnahmenempfehlungen beschränken sich auf diejenigen Sachverhalte, zu denen es in diesem Sektor Besonderheiten gibt, da er der sogenannten kritischen Infrastruktur einer Gesellschaft zugeordnet wird. Besonderes Augenmerk liegt daher auf Verfügbarkeit und Integrität der Systeme. Die enge Anlehnung an die ISO-Normen der 27000er-Reihe ermöglichen es den betroffenen Unternehmen, ein einheitliches IT-Sicherheitsmanagement für alle Unternehmensbereiche aufzubauen (Sowa, 2017).

NIST ICS Security Guide

Der *Guide to Industrial Control Systems* (ICS) Security ist weniger als Norm, denn als Sammlung von Best Practices zu verstehen (Stöwer & Kraft, 2017) und widmet sich sehr ausführlich konkreten industriellen Leitsystemen wie z.B. SCADA oder DCS und den dort möglichen Schwachstellen und Bedrohungen. Es wird sehr ausführlich beschrieben, wie solche Systeme sicher miteinander verbunden werden können und liefert dazu auch konkrete Handlungsvorschläge. Darin enthalten sind z.B. Designvorschläge für Netzkopplungen, Grundkonzepte für Firewall-Policies und Hinweise zum Umgang mit einzelnen Protokollen. Auf organisatorischer Seite findet sich neben einem Grundgerüst für einen Sicherheitsmanagementprozess eine Vielzahl an Verweisen zu in diesen Bereichen weiterführenden anderen NIST-Empfehlungen (NIST, 2011).

2.6 Zusammenfassung

Unternehmensnetzwerke lassen sich anhand weniger Parameter allgemein definieren und haben eine klare Aufgabe. Die verwendete Definition ist bewusst sehr allgemein gehalten, da die eingesetzten Technologien und Strukturen je nach Bedarf sehr unterschiedlich ausfallen können.

Das IoT ist eine umfassende Materie, die nicht ganz klar abgegrenzt werden kann. Wichtig ist festzuhalten, dass Dinge nicht nur im physischen Sinn gemeint sind. Es wurden die grundlegenden Eigenschaften umfassend beschrieben und Beispiele für Anwendungsbereiche aufgezeigt. Diese Anwendungsbereiche sind wohl für viele Unternehmen mögliche Tätigkeitsfelder, so dass das IoT in einem großen Teil aller Unternehmen in der einen oder anderen Form Anwendung finden wird.

Informationssicherheit und Datenschutz sind zwei grundlegende Themen, mit denen sich ein Unternehmen im Rahmen von entsprechenden Managementprozessen und auch im laufenden Be-

trieb auseinandersetzen muss. Die Ziele dabei sind klar und einfach zu beschreiben (primär Vertraulichkeit, Integrität und Verfügbarkeit). Um diese entsprechend systematisch zu erreichen, gibt es eine ganze Reihe von Hilfestellungen in Form von Standards oder umfangreichen Empfehlungen. Einige davon wurden in den vorherigen Abschnitten genannt, je nach Branche und Unternehmensart können aber auch andere, an dieser Stelle ggf. nicht behandelte Quellen herangezogen werden. Die Verwendung einer solche Publikation empfiehlt sich in jedem Fall, da ein unsystematischer Zugang zu dieser Thematik auf keinen Fall dazu führen wird, dass eine umfassende Informationssicherheit im Unternehmen erreicht wird. Dafür erscheint diese Materie erheblich zu komplex.

3 AUFBAU BESTEHENDER SICHERHEITSKONZEPTE FÜR UNTERNEHMENSNETZWERKE

Der Betrachtungsbereich für Informationssicherheit in dieser Arbeit sind Unternehmensnetzwerke. Um einen Vergleich mit einem Sicherheitsmodell im IoT-Kontext zu ermöglichen, muss definiert werden, was Netzwerksicherheit eigentlich bedeutet, welche Bedrohungen und Angriffsmöglichkeiten es auf solche Netzwerke gibt und wo die Ursachen von Schwachstellen liegen. In der Folge wird ein Netzwerksicherheitskonzept beschrieben, das übliche Maßnahmen zur Sicherstellung der Informationssicherheit in Unternehmensnetzwerken beinhaltet.

3.1 Netzwerksicherheit

Eine enge Definition von Netzwerksicherheit beschreibt diesen Begriff als Bereitstellung eines „sicheren Netzwerks“ für die geschützte Übertragung von Daten und eng verwoben mit dem *Physical Layer*, also der untersten Schicht des ISO/OSI-Netzwerkreferenzmodells (Daya, 2008).

Die zunehmende und komplexer werdende Vernetzung und Integration von Geräten, Produkten wie Software und ganzen IT-Services zur Bereitstellung von Netzwerkdiensten führt aber zu einer immer schwierigeren Umsetzung von Sicherheit. Letztendlich ist nicht nur die Sicherheit der Datenübertragung als solche, sondern auch die Sicherheit der End-User-Daten (für welche das System eigentlich gebaut wurde) relevant. In einem Netzwerk muss daher sowohl die Sicherheit der Komponenten oder Services als auch die Art und Weise der Vernetzung und Integration gesamtheitlich nach Sicherheitsaspekten betrachtet werden (McGee, et al., 2004).

Netzwerksicherheit wird dabei von manchen Autoren als wichtigster Bestandteil der Informationssicherheit erachtet, da sie schlussendlich verantwortlich für die Sicherheit aller Informationen ist, welche zwischen vernetzten Geräten ausgetauscht werden (Alabady, 2009). Das schließt die Sicherheit der am Datenaustausch beteiligten Endgeräte (Daya, 2008), allgemeiner gesprochen aber die gesamte Hardware, Software, betriebliche Prozesse, Verantwortlichkeiten und Zugangsbeschränkungen ein (Alabady, 2009).

Diese etwas weiter gefasste Definition von Netzwerksicherheit erscheint plausibler, da sie die Komplexität des Netzwerkbegriffs in modernen Unternehmensnetzwerken besser erfasst und wird entsprechend für die weitere Arbeit beibehalten. Eingebettet in den Kontext der Informationssicherheit kann die Netzwerksicherheit als Teilaspekt ebendieser betrachtet werden. Sicherheit in einem Netzwerk kann dann als gegeben bezeichnet werden, wenn alle darin enthaltenen Schutzobjekte vor unbefugtem Zugriff geschützt sind (Kizza, 2015).

3.2 Angriffsvektoren auf Computernetzwerke

Nach Art und Weise kann zwischen zwei groben Kategorien von Bedrohungen unterschieden werden, die durch einen Angreifer bzw. eine Angreiferin in Form von Angriffen umgesetzt werden

können. Passive Attacken zielen auf die Beobachtung bzw. Überwachung des Informationsaustausches (Datenverkehr) ab, dabei werden keine Systemressourcen aktiv in Anspruch genommen. Mögliche Ausprägungen sind das reine Beobachten des Datenverkehrs sowie das Auslesen der Inhalte, welche vom Sender zum Empfänger gesendet werden. Aktive Angriffe hingegen zielen auf die Modifikation des Datenverkehrs, die Erstellung eines gefälschten neuen Datenverkehrs, die Veränderung von Systemen oder die Beeinflussung des ordnungsgemäßen Betriebs ab (Kumar, 2015).

Angriffe auf einzelne Bestandteile eines Netzwerks (Router, Firewalls, Server, Clients, ...) haben unterschiedliche Absichten und Ziele. Dabei geht es aber immer um einen Aspekt der Informationssicherheit, also Vertraulichkeit, Integrität, Verfügbarkeit oder Verbindlichkeit (siehe 2.5.2). Angriffe können damit wie folgt eingeteilt und benannt werden:

- Ein Angriff auf die **Vertraulichkeit** wird ***Interception*** (Abhören, Abfangen) genannt. Hierbei erhält eine unbefugte bzw. außenstehende Partei Zugriff auf ein Schutzobjekt (*Asset*). Diese Partei kann dabei eine Person, ein Programm oder Computersystem sein.
- Wird ein bestehendes Asset durch eine unbefugte Partei verfälscht oder verändert, spricht man von ***Modification*** (Änderung, Modifikation). Dies ist ein Angriff auf die **Integrität**.
- Ein Angriff auf die **Verfügbarkeit** wird als ***Interruption*** (Unterbrechung, Störung) bezeichnet. Dabei geht ein Schutzobjekt verloren, wird unbrauchbar oder unverfügbar.
- Angriffe auf die **Verbindlichkeit** werden als ***Fabrication*** (Fälschung) bezeichnet. Dabei hat eine unbefugte Partei soweit Zugriff auf ein Netzwerk oder System, dass gefälschte Objekte erstellt werden können, wobei dies unbemerkt und unerkannt erfolgt (McGee, et al., 2004).

3.2.1 Potenzielle Angreifer und Angreiferinnen und deren Interessen

Obschon eine große Anzahl and Sicherheitsbedrohungen einzig durch Naturkatastrophen und unbeabsichtigte menschliche Fehlhandlungen besteht, entspringt ein Großteil dennoch beabsichtigten, menschlichen Handlungen mit illegalen oder kriminellen Absichten. Das können dabei unternehmensinterne wie -externe Personen, Hacker bzw. Hackerinnen und andere Interessensgruppen sein. Beispiele für Angriffsmotive sind

- **Cyberterrorismus**: Verbreitung von Angst, Beeinflussung von Politik
- **Militärische Spionage**: ausgeführt von staatlichen Stellen, Ziel ist Informationsgewinnung zur Erlangung militärischer oder finanzieller Vorteile
- **Industriespionage**: Erlangung von Firmengeheimnissen und geistigem Eigentum aller Art durch Mitbewerber bzw. Mitbewerberinnen oder andere Interessensgruppen
- **Rache** für von Angreifern bzw. Angreiferinnen als ungerecht empfundenen Handlungen
- **Hassmotive** aufgrund von Staatsangehörigkeit, Geschlecht, …
- **Publicity**: Erlangung von Bekanntheitsgrad durch erfolgreiches Eindringen in Systeme

- **Unwissenheit**: unbeabsichtigte Angriffe durch mangelndes Wissen/Verständnis (Kizza, 2015)
- **Finanzielle Interessen**: Betrug, Erpressung, Konto- und Kreditkartendatenmissbrauch (Pfeiffer & Kafka, 2011)

Daraus zeigt sich, dass potentiell jedes Netzwerk aus verschiedensten Gründen Ziel eines Angriffs werden kann. Ein schlichtes Abtun der eigenen Schutzobjekte als „uninteressant“ für Außenstehende kann somit kein valides Argument für die Vernachlässigung von Informationssicherheit sein.

3.2.2 Ursachen von Schwachstellen von Informationssystemen

Im Zusammenhang mit Informationssystemen gibt es eine ganze Reihe von möglichen Schwachstellen. Diese können zum einen durch organisatorische, wie auch technologische Mängel und Fehler entstehen. Auf organisatorischer Seite des Unternehmens finden sich beispielsweise folgende Ursachen für Schwachstellen:

- **Fehlende/unklare Sicherheitsanforderungen**: Ein unzureichend ausgeprägtes und kommuniziertes Sicherheitsbewusstsein in einem Unternehmen führt zu individuellen Lösungen mit unterschiedlichen Sicherheitsniveaus. Die Vernetzung solcher Systeme hat jedoch häufig die Absenkung auf das niedrigste Niveau zur Folge.
- **Unvollständiges Vorgehensmodell**. Durch unzureichende Einführung eines durchgängigen Vorgehensmodells im Sicherheitsmanagement kommt es oft zu reaktivem und symptomorientiertem Verhalten, d.h. Probleme (die durch Schwachstellen entstanden sind) werden erst nach Auftreten einer Sicherheitsverletzung behoben.
- **Mangelnde Lebenszyklusorientierung**. Die Beschäftigung mit Sicherheit erfolgt oftmals erst bei der Inbetriebnahme von Systemen, da die Fokussierung auf dem Betrieb liegt. Der Grundstein für Sicherheit, d.h. die Abwesenheit von Schwachstellen in einem System, wird jedoch schon wesentlich früher in Entwicklungs- und Testphasen gelegt.
- **Unzureichende Notfall- und Katastrophenvorsorge**. Die Zuständigkeit für Notfall- und Katastrophenvorsorgeplanung liegt oft in der für IT-Services zuständigen Abteilung, wobei das Ziel dieser Maßnahmen eigentlich die Aufrechterhaltung des Geschäftsbetriebs (Business Continuity) darstellt. Der Grad an Vorsorge für Notfälle und Katastrophen, welche oftmals die Nichtverfügbarkeit der Informationssysteme zur Folge haben, muss gesamtheitlich mit der Bedeutung für die Geschäftsprozesse betrachtet werden (Müller, 2018).

Auf der technischen Seite gibt es ebenso keine vollständige Liste von möglichen Schwachstellen in Netzwerken und Computersystemen, und eine zu starke Technikfokussierung allein ist auch nicht empfehlenswert. Dennoch kann aus den von großen Organisationen wie verschiedenen Computer Emergency Response Teams (CERTs) und anderen, welche sich mit Zwischenfällen in der Informationssicherheit beschäftigen, herausgegebenen Informationen eine Sammlung an gehäuft auftretenden, typischen Ursachen für Schwachstellen zusammengestellt werden.

- **Designfehler**: Die Hauptkomponenten von Systemen, also Hardware und Software, haben oftmals Designfehler. Wenngleich Hardwaredesignfehler seltener auftreten, sind sie dennoch nicht vernachlässigbar. Insbesondere muss jedoch verschiedenen möglichen Softwarefehlern begegnet werden. Diese haben wiederum verschiedene häufige Ursachen:
    - Menschliche Fehler (durch Programmierfehler, Zeitdruck, Verwendung eigener ungetesteter Algorithmen auf Grund von Selbstüberschätzung, Böswilligkeit, Nachlässigkeit)
    - Softwarekomplexität (schwieriges Testen, mangelnde Ausbildung, Missverständnis der Spezifikationen)
    - Mangel an zuverlässiger Software durch niedrige Qualität am Markt angebotener Produkte
    - Weiterverwendung oder Reengineering existierender Software trotz vorhandener Designschwächen
- **Fehlerhafte Implementierung**: Beispiele dafür sind inkompatible Interfaces, welche zu Sicherheitsproblemen führen können. Dies betrifft sowohl Hardware als auch Software.
- **Schwachstellen in gängigen Internettechnologien**, welche nicht selbst entwickelt wurden aber auf Grund von betrieblichen Notwendigkeiten eingesetzt werden. Die rasante Entwicklung dieser Technologien führte in der letzten Zeit zu einer besorgniserregenden Zunahme an Schwachstellen.
- **Probleme beim Patchen von verwundbaren Systemen**. Die schiere Anzahl an Geräten in einem Netzwerk und die zunehmende Anzahl an Patches und Bugfixes für von Schwachstellen betroffenen Geräten führt zu einem sehr großen administrativen Aufwand. Die zuständigen Personen kämpfen mit Ressourcenmangel, fehlendem Verständnis für Wartungsarbeiten und sich stetig erhöhender Komplexität der Sicherheitssysteme. Das führt zu einer niedrigen Priorität bei der Behebung von Schwachstellen, was teilweise auch auf mangelndem Wissen über Sicherheitsrisiken beruht.
- **Mangelnde Effektivität reaktiven Verhaltens**. Die gleichzeitige Zunahme von Schwachstellen in Systemen und der Anzahl der Angriffe führt zur Annahme eines stetig steigenden Sicherheitsproblems, dem mit reaktiven Methoden kaum mehr beizukommen ist.
- **Social Engineering**. Externe Angreifer und Angreiferinnen nutzen hierbei psychologische Tricks gegenüber legitimen Usern oder Userinnen eines Systems, um an Informationen (Benutzernamen, Passwörter) zu kommen, die für einen Zugriff benötigt werden (Kizza, 2015).
- **Unzureichende Standardisierung**.

Es herrscht durchaus die Einschätzung vor, dass in heutigen Systemen vor allem durch mangelnde Softwarequalität zu viele Fehler eingebaut sind, was unumgänglich zu Schwachstellen

führt (Pohlmann, 2015). Besonders besorgniserregend scheint die stetige Zunahme an Schwachstellen in Standard-IT-Produkten wie Web-Browsern und darin enthaltenen Plugins (BSI, 2015).

3.2.3 Ausprägungen von Schwachstellen

In der Netzwerksicherheit wird im Allgemeinen von drei Ausprägungen von Schwachstellen gesprochen, welche wie im letzten Abschnitt gezeigt eine Vielzahl verschiedener Ursachen haben können:

- **Technologische Schwachstellen**. Computer und Netzwerktechnologien haben inhärente Sicherheitsschwachstellen, dazu zählen z.B. Schwachstellen in den verwendeten Kommunikationsprotokollen oder Betriebssystemen.
- **Konfigurationsschwachstellen**. Dazu zählen alle Schwachstellen, die durch manuelle (durch z.B. Administratoren und Administratorinnen) vorgenommene Einstellungen bedingt sind. Das sind beispielsweise ungesicherte Benutzerzugänge, fälschlicherweise aktivierte Netzwerkdienste, unsichere und belassene Standardeinstellungen oder schlichtweg falsch konfigurierte Komponenten.
- **Schwachstellen bedingt durch die Sicherheitspolitik.** Dazu zählen Schwachstellen, die durch unzureichende Vorgaben oder mangelhafte Sicherheitsprozesse bedingt sind (Alabady, 2009).

3.2.4 Bedrohungen und Angriffe

Im Zusammenhang mit der Sicherheit von Informationssystemen und Netzwerksicherheit besteht konstant eine ganze Reihe von Bedrohungen. Diese sind unterschiedlichster Art. Eine Gruppe von Bedrohungen, welche insbesondere das Schutzziel der Verfügbarkeit gefährden, erwächst aus der Umwelt in der Form höherer Gewalt. Dazu zählen beispielsweise Erdbeben, Wassereinbruch oder Brand. Auch kriminelle Bedrohungen sind allgegenwärtig, das können Einbruch, Diebstahl oder auch unwahrscheinlich anmutende Vorfälle wie Geiselnahmen und Spionage sein. Ein weiterer Umweltaspekt ist technisches Versagen, was sich in der Form einer Unterbrechung der Strom-, Gas- oder Wasserversorgung und dem darauffolgenden Ausfall von IT-Systemen manifestieren kann. Gibt es in diesen Bereichen Mängel in der Vorbereitung (also Schwachstellen), kann dies zu einer akuten Gefährdung des gesamten Geschäftsbetriebs werden (Müller, 2018).

Dass auch im Zusammenhang mit den erwähnten technischen Aspekten eine permanente Bedrohung existiert, sollte durch die Aufzählung von potentiellen Angreifern oder Angreiferinnen in Abschnitt 3.2.1 deutlich geworden sein. Ein allgemeiner Bedrohungskatalog lässt sich damit insgesamt wie folgt zusammenstellen:

- Höhere Gewalt
- Organisatorische Mängel
- Menschliche Fehlhandlungen

- Technisches Versagen
- Vorsätzliche Handlungen (Klipper, 2011)

Da Schwachstellen in Informationssystemen letztendlich unvermeidlich sind, erwachsen daraus fortwährende Gefährdungen, welche durch Angreifer oder Angreiferinnen beispielsweise durch folgende Angriffsformen ausgenutzt werden können:

- **Abhören (Eavesdropping), Abfangen und Beeinflussen des Datenverkehrs**: Passives oder aktives Abhören von Netzwerkkommunikation zum Zweck des Datendiebstahls; Erstellen einer künstlichen Informationssenke; Manipulation übertragener Daten.
- **Man-in-the-Middle, Spoofing/Masquerarding:** Mechanismen um zuvor erwähnte Angriffe durchzuführen. Ein Angreifer oder eine Angreiferin schaltet sich als angeblich legitimer Knoten in die Kommunikation zweier Endgeräte ein oder gibt sich als ein solcher Knoten aus (Chen, et al., 2018).
- **Denial of Service (DoS)**: Klassischer Angriff auf die Verfügbarkeit. Darunter versteht man die Flutung eines Angriffsziels mit Anfragen mit hoher Netzwerkbandbreite bis zur Erschöpfung der vorhandenen Ressourcen. Dadurch ist das Ziel für legitime Nutzer und Nutzerinnen auch nicht mehr verfügbar (Chen, et al., 2018).
- **Distributed DoS (DDos)**: Variante von DoS, bei der eine Vielzahl von Angreifern oder Angreiferinnen, beispielsweise ein Botnetz, das Ziel angreifen (Wendzel, 2018).
- **Malware** (Viren, Würmer, Trojaner und *Remote Control*-Tools): Bösartige Software (*malicious software,* kurz Malware) stellt im Internet ein zunehmendes Problem dar. Viren attackieren dabei vorhandene Programme und Dateien, während das primäre Ziel von Würmern die Ausbreitung im Netzwerk zur Verteilung von Schadcode auf andere Geräte ist. Trojaner geben nach außen hin vor, nützliche Software zu sein, während im Hintergrund schadhafte Aktivitäten ausgeführt werden. Programme, die die Fernsteuerung von Geräten durch Angreifer oder Angreiferinnen ermöglichen, nisten sich in unbemerkt in einem System ein. Das Gerät wird dabei zu einem sogenannten Bot, der durch einen Angreifer bzw. Angreiferin kontrolliert wird und für (schadhafte) Aktivitäten aller Art genutzt werden kann (Chen & Walsh, 2014).

Im Kontext des *Social Engineering* seien folgende aktuelle Angriffsformen erwähnt:

- ***Phishing, Spear Phishing* und *Dynamite Phishing***: Bei diesen Verfahren wird versucht, jemandem einen Link für eine gefälschte Webseite unterzujubeln und den Benutzer bzw. die Benutzerin dazu zu bringen, sensible Daten herauszugeben. Dies erfolgt zumeist mit Massenemails. Handelt es sich jedoch um einen gezielten Angriff auf eine Person, spricht man von *Spear Phishing* (Wendzel, 2018). Als *Dynamite Phishing* wird ein aktueller, sehr gefährlicher Angriff im Rahmen der versuchten Verbreitung des Emotet-Schädlings bezeichnet, welcher bestehende Kommunikationsbeziehungen analysiert und daraus Anreden, Mailinhalte und persönliche Signaturen extrahiert und für gezielte Angriffe missbraucht (Harnisch, 2019).

- **CEO Fraud, Fake President:** Dabei geben sich Angreifer oder Angreiferin als Geschäftsführer bzw. Geschäftsführerin einer Firma aus und veranlassen einen Mitarbeiter oder eine Mitarbeiterin zur Überweisung eines größeren Geldbetrages ins Ausland (BKA, 2017).

Andere Angriffsformen sind passiv und warten beispielsweise den Besuch einer Webseite ab, wobei durch Lücken in Webbrowsern und Betriebssystemen der Download einer Schadsoftware initiiert wird (sog. Drive-By-Download). Dabei werden oftmals vielbesuchte Webseiten kompromittiert und entsprechender Schadcode eingefügt (Chen & Walsh, 2014).

Es gibt noch viele weitere Angriffsmöglichkeiten auf unterschiedlichen Ebenen eines Netzwerkes (z.B. auf spezifische Protokolle) bzw. genutzten Applikationen. Dabei sei unter anderem auf Chen und Walsh (2014), Bishop (2005), Wendzel (2018), Kappes (2013) oder, speziell in Bezug auf Drahtlosnetzwerke verschiedenster Art, auf Chen et al. (2013) verwiesen.

3.2.5 Moderne Entwicklungen

Zusätzlich ergeben sich durch die Mobilität der User bzw. Userinnen und die zunehmende Verwendung von mobilen Geräten (Laptops, Smartphones) neue Angriffsvektoren. Bring Your Own Device (BYOD) ist ein Schlagwort, das ab 2009 Einzug in Unternehmen gehalten hat. Dabei wird es Mitarbeitern und Mitarbeiterinnen ermöglicht, auf den eigenen Geräten sowohl private als auch dienstliche Aufgaben zu erledigen. Dabei ist die Mobilität dieser Geräte eines der größten Probleme, da sie leicht verloren gehen oder gestohlen werden können, was einen Verlust der Vertraulichkeit von Unternehmensdaten bedeuten kann. Zudem können Applikationen auf den Geräten potenziell die Integrität der Geräte und damit der darauf befindlichen Daten beeinflussen. Die Herausforderung dabei ist, eine Balance zwischen strikten Sicherheitsvorgaben seitens des Unternehmens und den persönlichen Daten auf dem Gerät andererseits zu finden, vor allem da das Gerät nicht im Eigentum des Unternehmens steht (Gajar, Ghosh, & Rai, 2013).

Eine weitere moderne Entwicklung stellt der sogenannte *Advanced Persistant Threat* (APT) dar. Diese ausgesprochen zielgerichteten Angriffe haben vielfach die Absicht, unbemerkt in IT-Systeme des Angriffsopfers einzudringen und dort einen spezifischen Schaden anzurichten. Dies kann sich in Form von (unbemerktem) Diebstahl sensitiver Informationen oder dem Lahmlegen von Systemen äußern. Das Angriffsschema hierbei ist immer mehrstufig: Nach einer Recherche in öffentlichen Quellen erlangt der Angreifer bzw. die Angreiferin nutzbare Informationen (E-Mailadressen, IP-Adressen, Zugangsdaten, …). Mit diesen Informationen erfolgt eine Infiltration interner Kommunikationsnetze und die Anwendung von Methoden wie Social Engineering. Danach erfolgt eine laterale Ausbreitung im unternehmensinternen Kommunikationsnetz zur Erlangung der gewünschten Informationen – ist dieses Ziel erreicht, werden die entsprechenden Systeme gekapert oder übernommen. Danach erfolgt in der Regel eine Exfiltration der Informationen, welche unbemerkt stattfindet (Bartsch & Frey, 2018). Somit stellt diese Angriffsform eine komplexe Kombination zuvor erwähnter Angriffsvektoren statt und erlangt zunehmende Popularität. Die Abwehr solcher Angriffe erfordert in der Regel ebenso eine Verknüpfung aus modernen Abwehrmechanismen (siehe z.B. Abschnitt 3.3.3.6).

3.3 Bestandteile eines Sicherheitskonzepts

Ein modernes Sicherheitskonzept für Netzwerke zum Schutz vor den in den vorigen Abschnitten erwähnten Angriffen besteht aus vier Mechanismen, welche gleichzeitig implementiert sein müssen:

- **Abschreckung**: Die üblicherweise erste Verteidigungslinie, welche auf der Generierung einer für Angreifer und Angreiferinnen abschreckenden Atmosphäre beruht. Beispiele dafür sind Warnungen vor ernsten Konsequenzen beim Versuch oder erfolgter Verletzung der Sicherheit.
- **Vermeidung**: Hierbei handelt es sich um den Prozess der Vermeidung eines Eindringens in ein Netzwerk durch verschiedenste Sicherheitsmechanismen.
- **Erkennung**: Hat ein Eindringling den Zugriff auf das Netzwerk oder System erlangt, so muss dies erkannt und entsprechend alarmiert werden. Das kann in Echtzeit oder durch regelmäßige weiterführende Analyse dieser Alarme durch das für Sicherheit zuständige Personal erfolgen.
- **Reaktion**: Es muss nach der Erkennung eines (erfolgreichen) Angriffs, also wenn alle drei vorigen Mechanismen versagt haben, eine nachgelagerte Aktion geben, welche darauf reagiert und eine Weiterführung des Angriffs bzw. zukünftige Angriffe und Schäden vermeidet.

Keinesfalls Bestandteil eines Sicherheitskonzepts sollte *Security Through Obscurity* (STO) sein. Dabei wird davon ausgegangen, dass ein Schutzobjekt so lange sicher ist, solange kein Außenstehender Kenntnis von seiner Existenz hat. Dies erweist sich jedoch als – leider noch sehr verbreiteter – gefährlicher Trugschluss und führte bereits in mehreren Bereichen zu massiven Sicherheitsproblemen (Kizza, 2015).

Maßnahmen zur Daten- und Informationssicherheit umfassen eine Vielzahl von Schritten, welche dafür sorgen, dass die Schutzziele erreicht werden können. Grundlegende Anleitungen zum Schutz gehen bereits in die Frühzeiten der digitalen Informationsverarbeitung zurück. So lassen sich bereits zahlreiche Grundsätze moderner Sicherheitsarchitekturen bis in die 60er und 70er Jahre zurückverfolgen, siehe z.B. Saltzer & Schroeder (1975).

Gesamtheitliche Informationssicherheit kann durch die Behandlung verschiedener Themenbereiche erreicht werden, welche nachfolgend auf organisatorische, applikationsbezogene und technische Aspekte aufgeteilt werden.

3.3.1 Organisatorische Aspekte

Nachfolgend werden organisatorische Maßnahmen zur Sicherstellung der Informationssicherheit in einem Unternehmensnetzwerk angeführt.

3.3.1.1 Informationssicherheitsmanagement

Die Einführung eines ISMS (siehe Abschnitt 2.5.3) dient dazu, die Einhaltung des Sicherheitsniveaus durch entsprechende Prozesse, Verantwortlichkeiten, Verfahren und Ressourcen sicherzustellen und aufrechtzuerhalten. Dazu ist es notwendig, dass das Unternehmen (konkret die Geschäftsführung) festlegt, welche Bedeutung und Ausprägung das Thema Informationssicherheit (und Datenschutz) im Unternehmen haben soll. Dies wird als Sicherheitspolitik bezeichnet, bezieht sich nicht ausschließlich – aber auch – auf die Informationssicherheit und leitet sich von der Unternehmenspolitik ab. Das Management verpflichtet sich zur Übernahme seiner Verantwortung für die Sicherheit, damit geht auch die Verantwortung für die Umsetzung der selbst auferlegten Regeln einher. Somit müssen entsprechende Mittel und Ressourcen für die Umsetzung zur Verfügung gestellt werden.

Ausgehend von dieser Politik werden die Sicherheitsziele festgelegt und eine angepasste Sicherheitsarchitektur entwickelt. Darin enthalten sind alle Sicherheitsanforderungen, aber auch die möglichen Bedrohungen. Damit ist das gewünschte Sicherheitsniveau definiert, welches durch die Einhaltung formulierter Sicherheitsrichtlinien erreicht werden soll. In diesen Sicherheitsrichtlinien werden (noch relativ generisch) allgemeingültige Regelungen, Vorgaben, Standards und Checklisten formuliert. Auf dieser Basis werden konkrete Sicherheitskonzepte für system-, plattform- oder organisationsspezifische Elemente definiert. Im letzten Schritt werden diese als reale Sicherheitsmaßnahmen durchgeführt und dokumentiert (Müller, 2018).

Damit schließt sich gewissermaßen ein Kreis, denn an dieser Stelle wird die Einführung bzw. Verwendung eines strukturierten Informationssicherheitsmanagements selbst als Maßnahme zur Erhöhung der Netzwerksicherheit angeführt. Die Netzwerksicherheit ist aber natürlich nur ein Teil des gesamten Informationssicherheitsmanagements, da dieses in der Regel auch noch weitere Aspekte der Informationssicherheit berücksichtigt.

3.3.1.2 Schutzbedarf und Datenklassifizierung

Damit ein Unternehmen Leistungen erbringen kann, sind Prozesse, insbesondere Kerngeschäftsprozesse erforderlich. Diese wiederum nutzen andere Ressourcen, unter anderem auch Daten und Informationen. Ein Unternehmen hat gewisse Anforderungen hinsichtlich der Sicherheit dieser Daten, da von diesen die Leistungsfähigkeit des Unternehmens abhängt. Diese Anforderungen müssen im Rahmen der Geschäftsflussanalyse (Business Impact Analysis) definiert werden. Aus diesen spezifischen Anforderungen lässt sich der Schutzbedarf für Daten und Informationen ableiten. Um festzulegen, wie hoch der individuelle Schutzbedarf ist, empfiehlt es sich, diese zu klassifizieren, da ansonsten für jedes einzelne System unterschiedliche Schutzbedarfe entstehen können und dafür individuelle Lösungen notwendig wären – was die Komplexität enorm erhöht (Müller, 2018). Bei diesen Klassen können beispielsweise Kategorien wie niedrig, normal, hoch und sehr hoch eingeführt werden. Für diese werden wiederum entsprechende Informationssicherheitsmaßnahmen festgelegt.

Wenn keine Klassifizierung notwendig erscheint, ist es fraglich, ob Daten dann überhaupt eine unternehmerische Relevanz haben. Denn wenn eine Veränderung oder ein Verlust für ein Unternehmen ohne Konsequenzen ist, können diese eigentlich nicht vernünftig für betriebsinterne Prozesse genutzt werden. Insofern liegt der Umkehrschluss nahe, dass alle verarbeiteten Daten bzw. Informationen eine gewisse Schutzwürdigkeit aufweisen.

Zu beachten ist, dass beim Datenschutz auf Grund der Verarbeitung personenbezogener Daten und dem damit bereits erfolgten Eingriff in die Grundrechte einer Person niemals ein niedrigerer Schutzbedarf als „normal“ festgelegt werden darf. Ein hoher oder sehr hoher Schutzbedarf kommt bei verschiedenen, für die betroffene Person möglicherweise schwerwiegenden Folgen des Verlusts der Vertraulichkeit zum Tragen. Beispiele dafür sind Fälle, in denen die Gefahr von Diskriminierung, finanziellem Schaden, Reputationsschaden oder Profilbildung besteht oder wenn ein Eingriff in einen besonders schützenswerten persönlichen Lebensbereich erfolgt (Rost, 2017).

3.3.1.3 Beschaffungsprozess

Neu zu beschaffende und in einem Unternehmensnetzwerk einzusetzende IKT-Komponenten sollen gewisse Sicherheitsanforderungen erfüllen. Deswegen ist beim Kauf nicht nur auf entsprechende, geforderte Funktionalität, sondern auch auf die sichere Integrierbarkeit in das Netzwerk zu achten. Diese müssen im Einklang der Security Policy stehen und deswegen, je nach Art und Klassifizierung der darauf künftig verarbeiteten Daten, gewisse Standards einhalten. Dies ist vor dem Kauf auch zu testen und verifizieren. Dazu empfiehlt es sich, gewisse Zertifizierungsprozesse vorzusehen und entsprechend zu durchlaufen (Kizza, 2015). Ein konsequenter Ausschluss von Produkten, die diesen Richtlinien nicht entsprechen, ist dabei notwendig (Gies & Steil, 2018).

3.3.1.4 Personal

Mitarbeiter und Mitarbeiterinnen, insbesondere wenn ihre Tätigkeit in (informations-)sicherheitsrelevanten Bereichen erfolgt, sollten bereits beim Einstellungsprozess nach gewissen Kriterien ausgewählt werden. Dazu können das Vorlegen eines Strafregisterauszugs oder eine sicherheitspolizeiliche Überprüfung herangezogen werden. Auf jeden Fall sollten durch Bewerber und Bewerberinnen in den entsprechenden IT-Bereichen Kenntnisse im Bereich Informationssicherheit nachgewiesen werden können und in der Folge (für das gesamte Personal) regelmäßig Security-Awareness-Trainings durchgeführt werden (Bartsch & Frey, 2018). Sollte bei Fachpersonal entsprechende Kenntnisse nicht vorliegen, sind Schulungen durchzuführen.

3.3.1.5 Datensicherung, Configuration- und Change-Management

Ein weiterer Aspekt zur Sicherstellung des Schutzziels der Verfügbarkeit ist die Verwendung von Datensicherungen (Backups). Bei dieser präventiven Maßnahme werden Daten in regelmäßigen Abständen so gespeichert, dass sie bei Auftreten eines Fehlers oder Angriffs in einer festgelegten

Wiederherstellzeit restauriert werden können. Dazu gibt es unterschiedlichste Methoden, Zeitpunkte, Anforderungen an den Aufbewahrungsort des Backups sowie die Varianten des Transports an den gewählten Ort (Müller, 2018).

Alle Computersysteme benötigen Konfiguration. Werden in einem Unternehmensnetzwerk mehrere hundert bis tausend Geräte eingesetzt, ergibt sich die große Herausforderung, alle Konfigurationen vorzuhalten, um im Fehler- oder Angriffsfall einen betriebsbereiten Zustand möglichst schnell wiederherstellen zu können. Dies ist in manchen Fällen nicht mit den gleichen Mechanismen wie die normale Datensicherung abbildbar und benötigt zudem Metainformationen, daher gibt es für diesen Fall eine eigene *Configuration Management DataBase* (CMDB). In dieser werden die relevanten (und aktuellen) Konfigurationen abgelegt (Müller, 2018). Dabei ist zu beachten, dass jenes System, das für die Verwaltung der Konfigurationen zuständig ist, natürlich selbst besonders hohen Schutzbedarf hat.

Unter Change Management versteht man einen methodischen Prozess, Änderungen an Konfigurationen im Unternehmensnetzwerk geplant und nur nach erfolgter Abstimmung und Genehmigung durchzuführen. Fehlerhafte Änderungen haben durch Ausfälle Auswirkungen auf das Schutzziel der Verfügbarkeit (Mansoor, 2014).

3.3.1.6 Schwachstellen- und Patchmanagement

Ein wesentlicher Bereich zur Sicherstellung von Netzwerksicherheit ist die Anforderung, Sicherheitspatches, welche Schwachstellen in Softwareprodukten beseitigen, zeitnah und verlässlich in die betroffenen Systeme einzuspielen. Konsequenterweise muss hier aber eigentlich Schwachstellenmanagement betrieben werden, da die Schwachstelle zumeist bekannt ist, bevor ein Patch dafür überhaupt existiert. Um diesen Erfordernissen nachzukommen, sind mehrere Schritte nötig.

Zum einen sollte dieses Vorgehen im Rahmen des ISMS behandelt werden, da dafür (Personal-)Ressourcen und Verantwortlichkeiten zu klären sind. Zudem muss ein aktuelles Inventar aller Schutzobjekte vorliegen, in welchem die aktuellen Softwarestände gespeichert sind. In der Folge ist es wichtig zu wissen, welche Schutzbedürftigkeit ein System besitzt, um über weitere Vorgangsweisen entscheiden zu können. Eine Maßnahme, die nun gesetzt werden kann, ist die regelmäßige und koordinierte Prüfung verfügbarer Informationsquellen auf neue Schwachstellen. Werden solche gemeldet, ist zu prüfen, ob die eigenen Systeme davon betroffen sind, ggf. der Patch zu testen (um Seiteneffekte zu vermeiden) und zeitnah einzuspielen (Brykczynski & Small, 2003).

3.3.1.7 Mobile Device Management

Um im Zusammenhang mit BYOD entstehenden Schwachstellen zu begegnen, bietet sich in einem Unternehmen der Einsatz eines *Mobile Device Management*(MDM)-Systems an. Dieses kann durch Zugriff auf standardisierte Geräteschnittstellen die Ausrollung von Richtlinien, Datenverschlüsselung, Löschung oder Sperrung von mobilen Geräten veranlassen. Auf Geräten aktivierte Richtlinien betreffen etwa die Gewährleistung der Aktivierung von Sicherheitseinstellungen

(Passwort/PIN-Code), die Installation für das Unternehmensnetzwerk notwendiger Zertifikate oder Sicherstellung der Authentifizierung des Geräts im Netzwerk. Zusätzlich können Applikationen installiert, deinstalliert, aktualisiert oder die nutzerseitige Installation verhindert werden. Mit Hilfe dieses Systems kann auch Konfigurationsmanagement sowie Inventarisierung dieser Geräte sichergestellt werden (siehe auch Abschnitt 3.3.1.5). Ein MDM-System ist somit ein wichtiges Werkzeug zur Sicherstellung der Informationssicherheit bei BYOD-Geräten (Gajar, Ghosh, & Rai, 2013). Zusätzlich sollten im Unternehmen organisatorische Richtlinien zum Umgang mit Diebstahl oder Verlust von Geräten eingeführt werden (Mansoor, 2014).

3.3.1.8 Audits, Vulnerability und Pen-Testing

Sicherheitsaudits dienen dazu, die gesetzten Maßnahmen zur Sicherstellung der Informationssicherheit in den Anwendungsbereichen auf ihre Effektivität und Effizienz hin zu überprüfen und mögliche noch existierende Schwachstellen zu identifizieren. Sie sind ein bewährtes Instrument für eine nachhaltige und kontinuierliche Verbesserung im Rahmen der unternehmerischen Steuerung der Informationssicherheit. Sie müssen regelmäßig durchgeführt werden, da sich die Geschäftsprozesse und damit einhergehend die informationstechnischen Ressourcen sowie unabhängig davon die allgemeine Bedrohungslage laufend verändern. Normenwerke und Standards wie die ISO 27001 und der BSI Grundschutz können dabei als bewährte Rahmenwerke für die Festlegung der Relevanzkriterien einzelner Prüfgegenstände dienen, also festlegen, was mit welcher Intensivität geprüft werden soll (Stöwer & Kraft, 2017).

Das aktive Scannen eines Unternehmensnetzwerks und dessen Komponenten nach Schwachstellen und darauf aufbauenden Verwundbarkeiten wird als *Vulnerability Testing* bezeichnet. Es zeigt sich in der Regel, dass viele der im Rahmen dieser Maßnahme gefundenen Schwachstellen durch Patches behoben werden könnten (siehe 3.3.1.6). Ein Penetrationstest (*Penetration Testing*) geht noch einen Schritt weiter und simuliert aktive hypothetische Angriffe, welche zur Kompromittierung eines Hosts eingesetzt werden könnten. Dies erfolgt wieder mit dem Ziel, darauf entsprechend durch Maßnahmen reagieren zu können (Chen & Walsh, 2014). Die im Zusammenhang mit den Audits genannten Sicherheitsstandards sehen solche Maßnahmen teilweise im Rahmen der Audits sogar vor (Stöwer & Kraft, 2017).

3.3.2 Applikationsbezogene Aspekte

Die applikationsbezogene Ebene des Sicherheitskonzepts bezieht sich auf die sichere Identifikation von Benutzern und Benutzerinnen sowie weiteren Zugriffskontrollmechanismen auf Applikationsebene zur Sicherstellung der Einhaltung der Schutzziele. Nachfolgend werden dafür in Netzwerk übliche Sicherheitsmaßnahmen angeführt und erläutert.

3.3.2.1 Authentifizierung und Autorisierung

Als Authentifizierung wird der Vorgang der Identifizierung eines Users oder einer Userin eines Systems bezeichnet. Dabei muss sichergestellt werden, dass sich eine Person (z.B. ein Angreifer

oder eine Angreiferin) nicht als legitimer Nutzer oder Nutzerin des Systems ausgeben kann. Verfahren zur Sicherstellung beruhen dabei auf etwas, was die tatsächliche Person weiß (Username, Passwort), ist (Fingerabdruck, Retina) oder hat, wie einen Ausweis oder ein Token (Kizza, 2015). Die Kombination mehrerer Merkmale ist sinnvoll und wird als Multifaktorauthentifizierung bezeichnet. Ein populäres Beispiel ist die Verwendung zweier Merkmale im Rahmen einer Zweifaktorauthentifizierung, der sog. *Two Factor Authentication* (Chen & Walsh, 2014), kurz 2FA. Die physische Lokalität oder ähnliche Eigenschaften wie Netzwerkadressen sollten dabei maximal eine unterstützende Rolle spielen, können aber die anderen Verfahren nicht sinnvoll ersetzen. Ein zentraler Access Control Server (ACS) kann Benutzer über verschiedene Protokolle und Verfahren authentifizieren, Beispiele hierfür sind Kerberos, RADIUS oder auch Public-Key-Verfahren (s.u.) (Kizza, 2015).

Ein weiterer wichtiger Bestandteil eines Sicherheitskonzepts ist die Autorisierung. Darunter versteht man den Prozess, zu eruieren, was ein authentifizierter User bzw. eine authentifizierte Userin in einem System tun kann (Schutz des Zugriffs auf Ressourcen). Viele Systeme unterscheiden hierbei beispielsweise die Berechtigungen für lesenden und schreibenden Zugriff. Ein häufig dafür verwendeter Ansatz ist die sog. *Discretionary Access Control* (DAC). Dabei werden Berechtigungen in Matrixform abgebildet und ausgewertet. Werden Zugriffsrechte für mehrere Benutzer und Benutzerinnen oder Gruppen realisiert, spricht man von sogenannten *Access Control Lists* (ACLs). Eine Erweiterung dieses Prinzips ist die *Role Based Access Control* (RBAC). Dabei wird nicht mehr auf Grund der Identität entschieden, sondern auf Grund der Zugehörigkeit einer Person zu einer oder mehreren Gruppen (Wendzel, 2018).

Für die effektive Verwaltung solcher Zugriffbeschränkungen gibt es zentrale und dezentrale Ansätze. In vielen Fällen ist ein zentrales Modell zu empfehlen, bei dem (gesteuert durch die Geschäftsführung) die entsprechenden Zugriffsrechte für die im Unternehmen vorhandenen Rollen zentral definiert und auf die entsprechenden Systeme ausgerollt werden. Diese Herangehensweise ermöglicht einen hohen Grad an Sicherheit. Um die zentrale Verwaltung trotz der Verwendung unterschiedlicher dezentraler Systeme mit verschiedenen Anforderungen zu ermöglichen, bietet sich der Einsatz eines *Meta-Directories* (etwa: Verzeichnis der Verzeichnisse) an. Dabei handelt es sich um ein führendes System, welches andere Verzeichnisse über Konnektoren mit aufbereiteten Daten (also Identitäten, Rollen, …) versorgt (Tsolkas & Schmidt, 2017).

3.3.2.2 Verschlüsselung

Um das Schutzziel der **Vertraulichkeit**, also den Schutz vor unbefugter Offenlegung, bei Speicherung und insbesondere Übertragung von Daten und Informationen sicherzustellen, wird Verschlüsselung eingesetzt. Die dabei eingesetzten Mechanismen benutzen Verschlüsselungsalgorithmen, um den Klartext an der Quelle in chiffrierten Text umzuwandeln. Der Empfänger kann durch Anwendung des Algorithmus in umgekehrter Form daraus den Klartext wiederherstellen. Abhängig vom eingesetzten Verfahren werden dazu entweder gemeinsam der gleiche Schlüssel (symmetrische Kryptographie) oder je Seite zwei verschiedene Schlüssel verwendet, ein öffentlicher und ein privater (asymmetrische Kryptographie). Bei letzterem Verfahren verwendet der Sender den öffentlichen Schlüssel des Empfängers, um eine Nachricht zu verschlüsseln. Der

Empfänger kann mit seinem privaten Schlüssel die Entschlüsselung vornehmen und vice versa (Kizza, 2015).

Um ein für eine möglichst große Nutzerbasis ein anwendbares Konzept von asymmetrischer Kryptographie herzustellen, wurden dazu Standards geschaffen. Einer der wichtigsten Vertreter ist der Public-Key Cryptography Standard (PKCS). Dieser dient als Basis für weitere tatsächliche und de-facto-Standards wie beispielsweise der zur Sicherung von Datenübertragungen eingesetzten Transport Layer Security, kurz TLS[9] (Kizza, 2015).

Im Bereich gängiger drahtloser Verbindungen in einem Unternehmen (*Wireless LAN*, WLAN) kommt in der Regel das Protokoll WPA2 zum Einsatz, welches – neben einer Sicherstellung der Authentifizierung über verschiedene Mechanismen – die Datenübertragung mittels eines symmetrischen Verfahrens verschlüsselt (Wendzel, 2018).

3.3.2.3 Hashfunktionen

Um das Schutzziel der **Integrität**, also den Schutz vor unbefugter bzw. unbemerkter Veränderung, bei der Übertragung von Daten und Informationen sicherzustellen, werden sogenannte Hashfunktionen eingesetzt. Eine Hashfunktion übernimmt eine Nachricht als Eingangswert und berechnet daraus einen (i.d.R. kürzeren) Ausgangswert. Dabei werden mathematische Einweg- oder Falltürfunktionen verwendet, bei denen vom Ausgangswert nicht auf den Eingangswert rückgeschlossen werden kann, bei gleichem Eingangswert jedoch immer dasselbe Ergebnis herauskommt. Das Ergebnis der Hashfunktion wird, zusammen mit der Nachricht, verschlüsselt und an den Empfänger übertragen. Dieser entschlüsselt die Nachricht und verifiziert den übermittelten Hashwert. Durch die Kombination dieser beiden Verfahren wird sichergestellt, dass die Inhalte bei der Übertragung nicht abgeändert wurden (Kizza, 2015).

3.3.2.4 Digitale Signaturen

Um das erweiterte Schutzziel der **Nicht-Abstreitbarkeit** zu erreichen, werden digitale Signaturen in Kombination mit verschlüsselter Übertragung eingesetzt. Bei diesem Verfahren unterzeichnet der Absender die Nachricht eindeutig (z.B. durch Verwendung asymmetrischer kryptographischer Verfahren), so dass er zu einem späteren Zeitpunkt die Urheberschaft der Nachricht nicht abstreiten kann (Kizza, 2015).

3.3.2.5 Public Key Infrastructure

Um nun zwischen verschiedenen Nutzern oder Systemen ein Vertrauensverhältnis herzustellen, zum Beispiel bei der Einleitung eines asymmetrischen Verschlüsselungsvorgangs bzw. der Herstellung einer verschlüsselten Verbindung über TLS, sollte die Identität des Gegenübers einwand-

[9] bzw. dessen Vorgänger SSL (Secure Sockets Layer)

frei sichergestellt werden (Authentifizierung). Dabei können Verfahren asymmetrischer Verschlüsselung eingesetzt werden. Dafür muss zuvor ein Schlüsselpaar aus privatem und öffentlichem Schlüssel erzeugt werden. Eine für beide Kommunikationspartner vertrauenswürdige dritte Partei, die sog. Certificate Authority (CA), signiert nach geeignetem Nachweis der Identität den öffentlichen Schlüssel einmalig (Ausstellung eines digitalen Zertifikats). Dadurch kann ein Kommunikationsteilnehmer seinem Kommunikationspartner seine Identität nachweisen, wenn beide Parteien der übergeordneten CA vertrauen. Eine solche Infrastruktur aus vertrauenswürdiger CA und davon abgeleiteten Identitätsnachweisen über signierte Zertifikate wird als Public Key Infrastructure (PKI) bezeichnet (Kizza, 2015).

Grundsätzlich spielt es bei diesem Verfahren keine Rolle, ob es sich um eine öffentliche, d.h. allgemein verwendbare CA, oder eine unternehmensinterne CA handelt. Einzige Voraussetzung ist, dass beide Kommunikationspartner diesem sog. Trust Anchor (etwa: Vertrauensanker) vertrauen.

3.3.3 Technische Aspekte

Auf technischer Ebene gibt es verschiedenste Maßnahmen, die auf die Vermeidung eines Eindringens in das Netzwerk abzielen oder die Schutzziele der Informationssicherheit auf dieser Ebene sicherstellen sollen.

3.3.3.1 Absicherung von Geräten

Für übliche Betriebssysteme existieren zahlreiche Best-Practice-Anleitungen zur sicheren Konfiguration eines Systems, so beispielsweise für Unix-/Linux (Beuchelt, 2009) oder Windows (Rackspace Support, 2016). Dies gilt für Clientsysteme, Serversysteme und Infrastrukturkomponenten (wie Netzwerkgeräte) gleichermaßen. Die Einhaltung solcher Konfigurationsempfehlungen wird für alle Komponenten empfohlen.

3.3.3.2 Netzwerksegmentierung

Nach dem alten römischen Prinzip *divide et impera* (teile und herrsche) sollte auch in einem Unternehmensnetzwerk vorgegangen werden. Dabei werden verschiedene Sicherheitsdomänen gebildet und der Übergang zwischen ihnen strikt kontrolliert bzw. eingeschränkt. In einem Netzwerk erfolgt das durch die Aufteilung in verschiedene Netzbereiche und die Absicherung des Überganges durch ein Sicherheitsgateway (z.B. eine Firewall, siehe Abschnitt 3.3.3.4). Dadurch entstehen mehrere Vorteile. Eine Störung oder Angriff kann sich dadurch nicht in andere Sicherheitsdomänen ausbreiten. Dies hilft z.B. bei APT-Angriffen gegen laterale Fortbewegung oder schlicht zur Verhinderung der Ausbreitung von Störungen. Auch können so vertrauenswürdige und weniger vertrauenswürdige Teilnehmer im selben Netzwerk betrieben werden. Ein weiterer Vorteil ist die Minimierung der Angriffsfläche durch Konzentration auf klare Schnittstellen. Eine solche Segmentierung wird von vielen Informationssicherheitsstandards wie beispielsweise dem

IT-Grundschutz explizit gefordert. Möglichkeiten der Umsetzung bestehen durch physische, logische, zeitliche oder kryptographische Separation der Domänen (Bartsch & Frey, 2018).

3.3.3.3 Netzwerkzugangsschutz

Ein Verfahren zur Erhöhung der Netzwerksicherheit stellt der Schutz vor dem Anschluss von unbekannten und/oder möglicherweise bereits kompromittierten Geräten an das Netzwerk dar. Solche Verfahren werden unter dem Begriff *Network Access Control* (NAC) zusammengefasst. Dabei erlangt ein Gerät erst Zugriff auf das Netzwerk, wenn ein gewisser Beweis für eine Vertrauensstellung erbracht wird. Die Beweisführung kann sehr umfangreich ausfallen, so gibt es Ansätze, bei denen Betriebssystem, Patchlevel oder das Vorhandensein aktueller Antivirensoftware überprüft wird, bevor Zugang zum Netzwerk erlaubt wird. In diesem Bereich existieren wenig standardisierte Lösungen. Zumeist läuft auf dem Gerät eine eigene Software, die diese Rahmenbedingungen überprüft und bei Verlangen des Zugriffs mit einem zentralen Policy-Server kommuniziert. Dieser bestimmt dann, ob und in welcher Form Zugang erlaubt wird (Chen & Walsh, 2014).

Ein verbreiteter Standard für die Authentifizierung eines Gerätes im Netzwerk ist IEEE 802.1X. Die Nutzung des Netzwerks ist dabei nur nach einer erfolgten Authentifizierung über einen zentralen *Authentication Service* möglich. Dieses Protokoll kann sowohl im drahtlosen als auch im kabelgebundenen Bereich eingesetzt werden. Typischerweise wird dieses Protokoll von professionellem Netzwerkequipment, wie es in Unternehmen zumeist vorhanden ist, unterstützt. Moderne Betriebssysteme verfügen über 802.1X-fähige Netzwerkstacks (Wendzel, 2018).

Für mobile bzw. BYOD-Geräte kann ein Netzwerkzugangsschutz mittels eines MDM-Systems realisiert werden. Durch ein Zusammenspiel der Systeme kann sichergestellt werden, dass sich nur BYOD-Geräte mit dem Unternehmensnetzwerk verbinden dürfen, die durch das MDM-System verwaltet werden.

3.3.3.4 Einsatz von Firewalls

Die wohl bekannteste Form eines Vermeidungsmechanismus zum Schutz vor dem Eindringen in ein Netzwerk ist der Einsatz von Firewalls. Dabei handelt es sich um Geräte, die verschiedene Netzwerksegmente miteinander verbinden und dabei ein Regelwerk anwenden, welches Verbindungen (und damit Datenaustausch) entweder zulässt oder blockiert. Blockieren bedeutet dabei, dass die Firewall den entsprechenden Datenverkehr verwirft. Firewalls sind als äußerst bewährtes Mittel in praktisch allen Netzwerken im Einsatz, oftmals auch auf den angeschlossenen Endgeräten. Der größte Nachteil von Firewalls besteht darin, dass sie nicht immer mit getunneltem Datenverkehr umgehen können. Dabei handelt es sich um Datenverkehr, der aus verschiedenen Gründen in einem anderen Datenverkehr eingebettet wurde (Wendzel, 2018).

Es kommen in einem Unternehmensnetzwerk durchaus mehrstufige Firewall-Konzepte zum Einsatz. Dabei werden die Netze in unterschiedliche Stufen der Vertrauenswürdigkeit getrennt und

ein direkter Zugriff aus nicht vertrauenswürdigen Netzbereichen auf kritische, speziell geschützte Netzbereiche unterbunden (Gies & Steil, 2018).

3.3.3.5 Virtual Private Networks

Durch den Einsatz von Firewalls werden oftmals unternehmensinterne Ressourcen vor dem Zugriff aus dem Internet geschützt. Das wirft dann Probleme auf, wenn legitime Nutzer und Nutzerinnen (wie beispielsweise Außendienstmitarbeiter und Außendienstmitarbeiterinnen) aus verschiedenen Gründen dennoch Zugriff aus dem Internet benötigen. Hierfür werden sogenannte *Virtual Private Network*(VPN)-Lösungen eingesetzt, um einen Fernzugriff zu ermöglichen. Dabei kommen Mechanismen wie Verschlüsselung zur Wahrung der Vertraulichkeit und ausgereifte Authentifizierungsmechanismen zum Einsatz (Kappes, 2013), bei hohen Sicherheitsanforderungen kann auch eine Multifaktorauthentifizierung eingesetzt werden (siehe Abschnitt 3.3.2.1).

Ein weiterer Anwendungsfall für VPNs ist die Herstellung einer virtuellen, scheinbar direkten Punkt-zu-Punkt-Verbindung zwischen zwei Unternehmensnetzen oder dislozierten Standorten desselben Unternehmensnetzes, beispielsweise über das Internet. Dabei kommen entsprechend wieder Technologien zur Verschlüsselung des Datenverkehrs zum Einsatz. Ein Beispiel dafür ist das Protokoll IPSec (Kappes, 2013).

3.3.3.6 Einsatz von *Intrusion Detection* / *Intrusion Prevention*

Sogenannte *Intrusion Detection Systems* (IDS) sind Programme, die passiv arbeiten (d.h. nicht in den Datenverkehr eingreifen) und Angriffe erkennen können. Ein erkannter Angriff wird dabei protokolliert und gemeldet. Ein *Intrusion Prevention System* (IPS) handelt aktiv und ist dazu in der Lage, nach einem detektierten Angriff Firewall-Regeln so zu verändern, dass Angreifer bzw. Angreiferinnen blockiert oder bestimmte Dienste komplett deaktiviert werden. Ein IPS muss dabei die Angriffserkennung nicht zwangsweise selbst durchführen, in der Praxis kommen aber oftmals Geräte zum Einsatz, welche beide Technologien kombinieren (Wendzel, 2018) und durch ihr Verhalten (z.B. Änderung von Firewall-Regeln) die Funktionalität bestehender Firewalls ergänzen.

Die Erkennung von Angriffen durch diese Systeme beruht dabei auf verschiedenen technischen Ansätzen. Dazu zählen:

- **Anomalieerkennung** auf Basis statistischer Modelle und maschinellen Lernverfahren
- **signaturbasierte Erkennung** auf Basis fester Regeln, welche einen Angriff explizit beschreiben und in einer internen Signaturdatenbank abgelegt sind
- **spezifikationsbasierte Erkennung**, welche auf formale Eigenschaften von Netzwerkprotokollen abzielt, Abweichungen erkennt und Bewertungen durchführt (Wendzel, 2018)

3.3.3.7 Endpoint Security

Die zunehmende Verbreitung von Schadsoftware (Malware) erfordert Maßnahmen auf den im Netzwerk angeschlossenen Geräten. Ein klassischer Ansatz dazu ist die Verwendung einer Antivirensoftware auf Computern. Diese dient dazu, Viren und andere Schadsoftware zu erkennen, zu entfernen und das Gerät vor weiteren Infektionen zu schützen. Dazu werden beispielsweise vorhandene Dateien mittels signaturbasierter Verfahren überprüft oder auch das Verhalten von aktiven Programmen mittels verhaltensbasierter Erkennungsverfahren überwacht und ggf. eingeschritten. Eine weitere Möglichkeit stellt eine isolierte emulierte Ausführung von Code in einer geschützten Umgebung dar, um schadhaftes Verhalten zu erkennen und die Ausführung auf dem echten System zu unterbinden (Chen & Walsh, 2014).

Wenn eine solche Software nicht nur signaturbasierte Verfahren sondern auch moderne Ansätze zur Erkennung von Bedrohungen einsetzt, also Verfahren, die beispielsweise auch in IDS/IPS-Systemen zum Einsatz kommen, wird als Bezeichnung oftmals der Begriff einer *Endpoint Security*-Lösung verwendet (Canner, 2018).

3.3.3.8 Redundanz

Zur Sicherstellung der Verfügbarkeit in Unternehmensnetzen kommen verschiedene Redundanzmechanismen zum Einsatz. Dabei werden üblicherweise Verbindungen, Komponenten oder Services doppelt oder mehrfach ausgelegt und parallel betrieben, so dass im Fehlerfall kein Komplettausfall bzw. eine Störung der Leistungsbereitschaft eintritt (Dooley, 2017).

3.3.3.9 Logging und SIEM

Ein *Security Incident and Event Monitoring*-System, kurz SIEM, dient dazu, die von Geräten im Netzwerk (das können sowohl Computer als auch Infrastrukturkomponenten sein) generierten Protokolldateien, auch Logdaten genannt, zu sammeln und auszuwerten. Dabei korreliert das SIEM-System diese Daten und untersucht sie nach möglichen Hinweisen auf Probleme. Bei Erkennung eines sicherheitsrelevanten Vorfalls wird ein Alarm ausgelöst. Es ist einiges an Sachkenntnis und Aufwand erforderlich, um ein solches System so zu konfigurieren, dass falsche Alarme unterdrückt und wichtige Alarme entsprechend hervorgehoben werden (Bartsch & Frey, 2018).

3.4 Zusammenfassung

Netzwerksicherheit ist ein umfangreiches Themengebiet, das auf Grund der Vielzahl an Bedrohungen in der Regel sehr ausgedehnt zu behandeln ist. Das skizzierte Sicherheitskonzept stellt dabei eine Sammlung verschiedener Maßnahmen dar, mit denen auf die durch Angreifer oder Angreiferinnen entstehenden Gefährdungen auf Grund der mit hoher Wahrscheinlichkeit auftretenden Schwachstellen reagiert werden kann. Ursachen für diese Schwachstellen wurden ebenso identifiziert wie Beispiele für praktische Angriffe.

4 INFORMATIONSSICHERHEIT IM IOT-KONTEXT

Das IoT stellt einige besondere Anforderungen an die Informationssicherheit, welche sich insbesondere aus den Limitierungen der eingesetzten Geräte oder grundsätzlichen Aspekten des IoT-Paradigmas ergeben. Diese werden im ersten Abschnitt dieses Kapitels behandelt. In der Folge werden IoT-spezifische Quellen von Unsicherheit untersucht und Bedrohungen und Angriffsvektoren auf IoT-Geräte dargestellt. Am Ende des Kapitels wird auf die Besonderheiten hinsichtlich des Datenschutzes im IoT eingegangen, da es hier tatsächlich einige wichtige, zu beachtende Aspekte gibt.

4.1 Rahmenbedingungen und Anforderungen an Sicherheit

Im Kontext von IoT ergeben sich einzigartige Herausforderungen und Rahmenbedingungen. Wesentliche Aspekte können dabei wie folgt zusammengefasst werden:

- **Heterogenität / multiple Technologien**. Beim Einsatz von IoT werden unterschiedlichste Technologien kombiniert. Das umfasst beispielsweise RFID, drahtlose Sensornetzwerke, Cloud Computing und (Funktions-)Virtualisierung. Jede dieser Technologien besitzt eigene, inhärente Schwachstellen. Für den sicheren Einsatz von IoT muss die gesamte Kette dieser Technologien abgesichert werden, da das schwächste Glied die Sicherheit der IoT-Applikation bestimmt (Rayes & Salam, 2017). Dazu kommt, dass im Regelfall Produkte und Protokolle unterschiedlichster Hersteller im Einsatz sind, welche aber in einem gemeinsamen Kommunikationsnetzwerk beheimatet sind und miteinander (direkt oder indirekt) kommunizieren müssen (Georgakopoulos & Zhang, 2018).
- **Skalierbarkeit**. Die schiere Anzahl an Geräten im Milliardenbereich stellt eine große Herausforderung für die Entwicklung von Abwehrmaßnahmen gegen Angriffe dar. Zentrale Sicherheitskonzepte, wie derzeit in Netzwerken üblich (siehe Kapitel 3), können hier nicht mehr zur Anwendung kommen. Zur Erreichung von Sicherheit muss ein Wechsel auf dezentrale Mechanismen erfolgen, da ansonsten eine Skalierung auf Tausende bis Millionen von Geräten in einem Unternehmensnetzwerk nicht sinnvoll – auch im Hinblick auf Kosten – erfolgen kann.
- **Big Data**. Da mit IoT die Anzahl an Geräten stark zunimmt, wachsen dabei auch die entstehenden und zu verarbeitenden Datenmengen. Dies geschieht, da davon auszugehen ist, dass ein „smartes“ Objekt (Thing) mehrere Sensoren besitzt, welche über die Zeit große Datenströme erzeugen. Daher werden auch Mechanismen benötigt, die diese entsprechend schützen können (Rayes & Salam, 2017).
- **Cloud Computing**. Ein Aspekt von IoT ist das intelligente Verarbeiten der Unmengen von erfassten Daten. Dazu eignen sich Cloud Computing-Infrastrukturen hinsichtlich verfügbarer Rechenleistung und Speicherplatz (Xiaohui, 2013). Auf der anderen Seite benutzen viele Geräte aus dem CIoT-Bereich Cloud-Dienste.

- **Verfügbarkeit**. In klassischen Netzwerken wird oftmals zugunsten der Verfügbarkeit auf gewisse Sicherheitsaspekte verzichtet. So wird beispielsweise auf Abschaltungsautomatismen bei der Anwendung von IPS- oder IDS-Systemen verzichtet. Die Argumentation dahinter ist, dass kritische Systeme bei einer falsch positiven Erkennung einer Bedrohung oder eines Angriffs vom Netz getrennt werden und damit die Verfügbarkeit des Systems reduziert wird. Damit wird jedoch die Sichtbarkeit von Bedrohungen massiv reduziert.
- **Limitierte Ressourcen**. Eines der wesentlichen Problemfelder im IoT-Umfeld stellt die nur limitierte Verfügbarkeit von Ressourcen wie CPU-Rechenleistung, (Arbeits-)Speicher, Akkuleistung oder Sendereichweite dar (Rayes & Salam, 2017).
- **M2M-Kommunikation.** Diese Kommunikationsform ist ein wesentlicher Bestandteil des IoT, wobei sie dort eher als T2T-Kommunikation bezeichnet wird. Dass aber Dinge miteinander sprechen, setzt einen verfügbaren Kommunikationskanal voraus, d.h. der Zugriff auf diese Geräte in einem Unternehmensnetzwerk, auch aus dem Internet, kann bzw. darf in diesen Fällen nicht vollständig unterbunden werden.
- **Dezentrale bzw. entfernte Standorte**. In gewissen Anwendungsbereichen von IoT (z.B. Smart Grid, Eisenbahn- oder Straßenverkehrswesen) werden IoT-Geräte wie Sensoren in schwer erreichbaren und unbemannten Standorten eingesetzt. Dazu kommen extreme Umweltbedingungen und Platzbeschränkungen (Rayes & Salam, 2017).
- **Mobilität**. Es ist in vielen Anwendungsbereichen von IoT davon auszugehen, dass Dinge oftmals ihre Lokation verändern (Rayes & Salam, 2017).
- **Drahtlose Netzwerke.** Eine wesentliche Eigenschaft von IoT ist die umfangreiche Nutzung verschiedenster Drahtlostechnologien (Atzori, Iera, & Morabito, 2010), welche zum Teil besondere Erfordernisse hinsichtlich niedrigen Energieverbrauchs erfüllen. Beispiele hierfür sind NFC, 802.11ah, LoRaWAN[10], ZigBee, Bluetooth LowEnergy (BLE) oder 6LoWPAN[11] oder NBIoT[12]

Gerade die letzten drei Punkte führen zu einem relevanten Aspekt beim Einsatz von IoT in Unternehmen: die IoT-Geräte werden – je nach Anwendung – möglicherweise nicht im klassischen unternehmenseigenen Netzwerk (z.B. LAN, WLAN) betrieben. Aktuelle Entwicklungen wie der 5G-Mobilfunkstandard werden erwartungsgemäß zu einer rasanten Verbreitung und Anwendung von IoT in fremden Netzwerken (z.B. des Mobilfunkbetreibers) führen.

Eine weitere Problematik ergibt sich – trotz zahlreicher Bemühungen in dieser Richtung – aus der fehlenden Standardisierung. Diese ergibt sich zum einen aus den schnellen Innovationszyklen, auf der anderen Seite sind insbesondere strenge Regulierungen im Bereich der Funkfrequenzen ein Hindernis dafür (Buyya & Dastjerdi, 2016).

[10] LoRa steht in diesem Fall für *Long Range* (Ram, 2018)

[11] Viele der Technologien zielen auf die Schaffung von Weitverkehrsinfrastruktur (WANs) bei möglichst niedrigem Energieverbrauch ab, daher spielen viele dieser Begriffe mit dem dafür eingeführten Begriff Low-Power-WAN (LPWAN) (Ram, 2018)

[12] Schmalband-Funktechnologie für IoT (*NarrowBand IoT*) (Ram, 2018)

Innerhalb dieser Rahmenbedingungen müssen gewisse Sicherheitsanforderungen erfüllt werden. Diese spiegeln naturgemäß die in Abschnitt 2.5.2 skizzierten allgemeinen Anforderungen an Informationssicherheit wider. Um einige konkrete Aspekte erweitert seien sie hier wie folgt zusammengefasst:

- **Vertraulichkeit**. Ausgetauschte Nachrichten und deren Inhalte dürfen nur von den vorgesehenen Entitäten (Dingen, Applikationen, …) nachvollzogen werden können.
- **Integrität**. Es muss sichergestellt sein, dass ausgetauschte Nachrichten nicht von Dritten geändert oder verfälscht werden können.
- **Authentifizierung**. Es muss sichergestellt sein, dass an einer beliebigen Operation beteiligte Entitäten auch jene sind, die sie vorgeben zu sein.
- **Autorisierung**. Es muss sichergestellt sein, dass eine Entität dazu berechtigt ist, die angeforderte Operation durchführen zu können.
- **Verfügbarkeit**. Services müssen störungsfrei zur Verfügung stehen.
- **Aktualität**. Ausgetauschte Daten müssen aktuell sein.
- **Nicht-Abstreitbarkeit**. Eine Entität kann keine Operation abstreiten, welche sie durchgeführt hat.
- **Forward Secrecy**. Wenn eine Entität das Kommunikationsnetzwerk verlässt, darf es die darin in der Folge stattfindende Kommunikation nicht mehr verstehen.
- **Backward Secrecy**. Eine neue Entität im Netzwerk darf die zuvor darin stattgefundene Kommunikation nicht verstehen (Rayes & Salam, 2017).

Es ist naheliegend, dass viele der in Kapitel 3 beschriebenen Sicherheitsmechanismen wie z.B. Verschlüsselung zur allgemeinen Sicherstellung dieser Anforderungen grundsätzlich anwendbar sind – allerdings ergeben sich durch die genannten Rahmenbedingungen spezielle Herausforderungen, denen bei der weiteren Betrachtung von Risiken im IoT-Kontext Rechnung getragen werden muss.

4.2 IoT-spezifische Quellen von Unsicherheit

Neben den vorangehend beschriebenen Quellen von Unsicherheiten in Informationssystemen gibt es noch einige Aspekte der Informationssicherheit, die im Themengebiet IoT zwar nicht neuartig sind, aber durch die Eigenschaften von IoT eine stärkere Relevanz erhalten.

Ein wesentlicher Sicherheitsfaktor, der sich auch schon in normalen Netzwerken ergibt, ist die zunehmende Vernetzung von Geräten. Abgesehen von den Computernetzwerken nimmt diese Vernetzung auch im Fertigungsbereich immer stärker zu und diese werden mittlerweile oft mit den Computernetzwerken verbunden, ohne dabei ein volles Verständnis für die genauen Kommunikationsabläufe zu haben. Dadurch werden die Schwachstellen solcher Geräte einer wesentlich größeren Zahl an potenziellen Angreifern und Angreiferinnen zugänglich gemacht (NIST SP 800-82, 2011). Der Einsatz von IoT und die damit einhergehende wesentlich höhere Anzahl an

untereinander vernetzten Geräten (Aspekt der Skalierung) vergrößert die dadurch entstehende Gefährdung erheblich.

Weitere Ursachen für Unsicherheit ergeben sich durch die Time-To-Market im IoT-Umfeld (Buchs, 2017). Unter diesem Begriff versteht man den Zeitraum zwischen der Entstehung einer Produktidee bis zum Erreichen der Marktreife bzw. der Platzierung des Produktes oder der Dienstleistung am Markt (Kreutzer, 2018). Informationssicherheit wird bei Produkteinführungen im IoT-Markt auf Grund des hohen Zeitdrucks zur Markteinführung und der damit niedrigen Time-To-Market sowie aufgrund eines Kostendrucks oftmals vernachlässigt. Hersteller verschieben unter Umständen die Implementierung von Sicherheitsmechanismen auf einen Zeitpunkt nach der Markteinführung – damit bleiben die Geräte, wie auch viele der in der Einleitung erwähnten Beispiele zeigen, einfach dauerhaft verwundbar im Internet (Wurm, Hoang, Arias, Sadeghi, & Jin, 2016). Es scheint leider weiterhin so, als hätten viele Hersteller wenig aus den zahlreichen Vorfällen und daraus abgeleiteten Empfehlungen für sichere IoT-Geräte gelernt und bringen weiterhin verwundbare Geräte auf den Markt (Naste, 2018).

Ein weiteres Problemfeld stellen oftmals die Hersteller von IoT-Geräten selbst dar, denn sie haben zwar viel Erfahrung beim Bau von Waschmaschinen oder Staubsaugern, aber keine Erfahrung im Bereich der Entwicklung sicherer Software. Um also „sichere“ IoT-Lösungen zu entwickeln, müssten Experten im Bereich Informationssicherheit einstellt oder die eigenen Mitarbeiter und Mitarbeiterinnen diesbezüglich kostenintensiv geschult werden. Es scheint auf Grund der Trivialität der oft vorgefundenen Schwachstellen in Produkten so gut wie sicher, dass viele Hersteller diesen Weg nicht beschritten haben. Zudem sind die Voraussetzungen für normalen und dauerhaft physisch sicheren Betrieb dieser Geräte zwar bedacht worden, kaum ein Hersteller sorgt sich aber in der Folge um jahrelange sicherheitskritische Softwareupdates der Produkte (Kleinhans, 2017). Zudem sind diese Informationen oftmals nicht transparent, so dass gar nicht bekannt ist, ob ein IoT-Gerät überhaupt noch irgendwelche Updates erhalten wird (Bhartiya, 2017).

4.3 Bedrohungen und Angriffsvektoren

Im IoT-Kontext gibt es einige spezifische Bedrohungen. Diese treten zwar auch in normalen Unternehmensnetzwerken auf, es zeigt sich jedoch aus den geschilderten Rahmenbedingungen und der Erfahrung, dass IoT-Geräte dafür besonders anfällig sind.

- **DoS-Attacken**. Durch die limitierten technischen Ressourcen sind IoT-Geräte besonders anfällig für DoS-Attacken. Gegen IoT-Infrastrukturen können nicht nur klassische DoS-Angriffe auf z.B. die geringe verfügbare Netzwerkbandbreite, sondern Angriffe auf die häufig verwendeten Drahtlosinfrastrukturen gefahren werden.
- **(Physische) Zerstörung**. Vor allem bei fehlenden technischen Kenntnissen, um mittels ausgefeilter Angriffe Zugriff auf ein System zu bekommen und eine IoT-Anwendung zu (zer-)stören, kommt es bei IoT durchaus dazu, dass die Dinge schlichtweg physisch zerstört werden. Das ist eine latente Gefahr, da sich viele Geräte in einem schlecht geschützten (öffentlichen) Raum befinden.

- **Übernahme von IoT-Geräten (Kontrolle)**. Anstatt es zu zerstören, kann ein Angreifer oder eine Angreiferin auch die vollständige Kontrolle über ein Gerät übernehmen und diese unbemerkt behalten (Roman, 2013). Dabei werden verschiedene Ziele verfolgt. Neben kontinuierlicher Datenextraktion oder der Nutzung für laterale Ausbreitung bei einem APT-Angriff kann auch das infiltrierte Gerät als sog. Bot in einem Botnetz (BSI, 2018) durch einen Angreifer bzw. eine Angreiferin dazu verwendet werden, größere Angriffe gegen andere Infrastrukturen zu unterstützen.

Im IoT können Angriffe auf Unterschiedlichen Ebenen der IoT-Architektur (siehe Abschnitt 2.3) erfolgen. Die Angriffsvektoren sind dabei keine technisch Neuen, lassen sich den Ebenen aber beispielsweise wie folgt zuordnen:

- **Perzeptionsschicht**: Unbefugter physischer Zugang, Abhören von Kommunikation (Eavesdropping), Störung von Funksignalen (Jamming), Spoofing-Angriffe, Vampirangriffe[13]
- **Netzwerkschicht:** DoS-Angriffe, Verkehrsdatenanalyse, Man-in-the-Middle-Angriffe
- **Applikationsschicht:** Code Injection, Buffer Overflows, Phishing-Angriffe, Angriffe auf Authentifizierung und Autorisierung, Datenmanipulation

Um einen Eindruck des derzeitigen Stands der Sicherheit von IoT-Devices im Internet zu bekommen, seien Zahlen einer Untersuchung aus 2014 genannt: zum damaligen Zeitpunkt waren von knapp über 35.000 untersuchten Geräten aus dem IoT- bzw. ICS-Umfeld je nach Anwendungsbereich 0,5 bis 3,5% verwundbar. Wenn diese Zahlen einigermaßen repräsentativ sind, ließe das auf mehrere tausend verwundbare Geräte pro Million IoT-Devices schließen (Patton, et al., 2014). Betrachtet man die in der Einleitung erwähnten Medienberichte, scheint dieser Schluss nicht einmal abwegig zu sein. Eine Studie aus 2014 geht sogar davon aus, dass damals bis zu 70% der populärsten IoT-Produkte mit im Durchschnitt 25 Schwachstellen ausgeliefert wurden (Lee & Lee, 2015). Weitere Publikationen zeigen ein ähnliches Bild, so bestätigt eine Untersuchung von Wurm et al. (2016), dass sowohl ausgewählte CIoT- als auch IIoT-Geräte im Hinblick auf Security ausgesprochen schlecht designt sind. Auch Olawumi et al. (2014) und Dhanjani (2016) zeigen, dass viele Protokolle und Implementierungen von Sicherheit (auch in kritischen Bereichen wie Türschlössern) sehr einfach auszuhebeln sind.

4.4 Besonderheiten beim Datenschutz

Dieser Bereich kann als einer der sensibelsten Bereiche im IoT-Kontext gesehen werden. Für manche Autoren gilt der Datenschutz, insbesondere was die Zustimmung etc. zur Verarbeitung von personenbezogenen Daten betrifft, im IoT-Kontext als grundsätzlich hochproblematisch bis

[13] bewusste Erhöhung des Energieverbrauchs und damit Reduktion der Lebenszeit bei batteriebetriebenen Geräten, auch als *Sleep Deprivation Attack* bezeichnet

unlösbar. Personen können beispielsweise in Bereichen, in denen IoT-Sensornetzwerke aufgebaut sind, überhaupt nicht steuern, welche Informationen über sie gesammelt werden. Als Beispiel sei ein Bereich genannt, in welchem Sensoren Personenbewegungen erfassen: die einzige Möglichkeit, eine Datenverarbeitung grundsätzlich zu verhindern, ist, den Bereich überhaupt nicht zu betreten (Atzori, Iera, & Morabito, 2010). Weitere Gefahren ergeben sich in diesem Kontext durch die massiven Fortschritte im Bereich der Sprach-, Gesichts- und Bewegungserkennung, da dadurch wesentlich mehr, auch sensible, Informationen vorliegen (Rayes & Salam, 2017), welche zudem theoretisch aggregiert und zur Erstellung von umfangreichen Profilen missbraucht werden können (Kozlov, Veijalainen, & Ali, 2012).

Kritisch zu sehen ist, dass in der Diskussion des Themas Datenschutz sehr oft dieselben Konzepte angewendet werden wie bei der Auseinandersetzung mit dem „normalen“ Internet. Ein wesentlicher Unterschied, der berücksichtigt werden muss, ist jedoch, dass die IoT-Kommunikation ohne Einwilligung oder expliziter Zustimmung eines Users bzw. einer Userin mit möglicherweise unerwarteten bzw. unerwünschten Ergebnissen stattfinden kann (automatische M2M-Kommunikation mit Informationsaustausch). Es muss daher für IoT-Anwendungen bei Bedarf geklärt werden, wie diese Zustimmung rechtssicher erfolgen kann. Derzeit dafür eingesetzte Mechanismen, wie sie beispielsweise bei Webseiten verwendet werden, sind nicht anwendbar (Perera, Ranjan, Wang, Khan, & Zomaya, 2015). Zudem gibt es die Anforderung, Daten unter bestimmten Umständen löschen zu müssen (Anfrage, entfall der Begründung der Verarbeitung, …). Da an der Verarbeitung dieser Informationen bei IoT-Anwendungen möglicherweise tausende Geräte beteiligt sind, stellt dies eine durchaus große Herausforderung dar.

5 IDENTIFIKATION ENTSTEHENDER SICHERHEITSRISIKEN

Um Risiken, die im IoT-Kontext entstehen können, zu identifizieren, muss zuallererst eine Definition des Begriffs Risiko erfolgen. Dabei wird auch dargelegt, warum ein risikobasierter Ansatz sinnvoll scheint, um mit dem Thema Informationssicherheit umzugehen. Den Hauptteil dieses Kapitels bildet die Erarbeitung und Zusammenstellung von Risiken für die Informationssicherheit in einem Unternehmen, welche sich aus IoT-spezifischen Schwachstellen ergeben.

5.1 Der risikobasierte Ansatz als Ausgangsbasis

Fehlende Informationssicherheit kann auf ein Unternehmen massive kurz- und langfristige Auswirkungen haben (siehe Tabelle 1). Es ist jedoch für das Management oftmals schwer zu bewerten, wie es um die Informationssicherheit bestellt ist und welche Auswirkungen sich dadurch ergeben können. Dies beruht auf verschiedenen Faktoren wie beispielsweise der Komplexität der eingesetzten Systeme und dem unbekannten Umfang oder der Wahrscheinlichkeit eines Sicherheitsvorfalls (Gadatsch & Mangiapane, 2017).

Kurzfristige Auswirkung	*Langfristige Auswirkung*
Produktivitätsverlust	**Imageverlust**
+ Kosten der Wiederherstellung	+ Negative Medienpublikationen
+ Eingeschränkte Produktivität	+ Verlust von Kunden nach Datendiebstahl
Direkte Kosten	**Rechtliche Konsequenzen**
+ Kosten für Externe Experten	+ Ansprüche gegenüber Dritten
+ Training und Ausbildung	+ Strafen
Umsatzverlust	**Verlust von Innovationen**
+ Ausfall von betriebsnotwendigen Systeme	+ Gebundene IT-Ressourcen
+ Website nicht verfügbar	+ Reaktivität statt Innovation

Tabelle 1: Kurz- und langfristige Auswirkungen unzureichender Informationssicherheit, nach (Gadatsch & Mangiapane, 2017)

Es ist offensichtlich, dass viele dieser Auswirkungen den Geschäftszielen, also wirtschaftlichen Interessen der Stakeholder (Gillenkirch, 2018), diametral gegenüberstehen. Es ergeben sich latente Bedrohungen für die Existenz, Handlungsfähigkeit und das Image eines Unternehmens (Müller, 2018). Das Problem dabei: Sicherheit ist kein absoluter, erreichbarer Zustand, sondern ein fortwährend andauernder Prozess (Schanze, 2015).

Um also unter Berücksichtigung der vorhandenen Bedingungen den in Zukunft möglichen (vor allem negativen) Entwicklungen wie Sicherheitsvorfällen begegnen zu können, ist die systematische Beschäftigung mit Risiken ein zentraler Aspekt. Ein Risiko kann dabei wie folgt definiert werden:

„Risiko ist die Auswirkung von Ungewissheit auf Ziele."

Definition eines Risikos aus dem ISO/IEC Guide 73:2009 (ISO/IEC, 2009)

Gemäß dieser Definition sind jedoch auch positive Auswirkungen miterfasst. Für die vorliegende Fragestellung im Kontext der Informationssicherheit ist es jedoch üblich, nur negative Folgen von Zielabweichungen zu betrachten. Dieses wird auch als „Downside-Risiko“ bezeichnet. Den folgenden Betrachtungen, insbesondere in Abschnitt 5.3, liegt damit eine engere Definition des Risikos zu Grunde:

> *„Risiko ist eine nach Wahrscheinlichkeit […] und Konsequenz bewertete Bedrohung hinsichtlich der Abweichungen von erwarteten System-Zielen. Das […] Risiko betrachtet dabei stets die unerwünschten Abweichungen von den System-Zielen und deren Folgen.“*
>
> *Risikodefinition (Königs, 2017)*

Als Systemziele werden in dieser Arbeit die elementaren Ziele der Informationssicherheit gemäß 2.5.2 betrachtet. Damit lassen sich folgende Zielabweichungen festlegen, welche durch Bedrohungen entstehen und durch ein Risiko beschrieben werden können:

- Verlust von Vertraulichkeit
- Verlust von Integrität
- Verlust von Verfügbarkeit

Bedrohungen wirken sich umso häufiger und stärker aus, als Schwachstellen vorhanden sind und geeignete Maßnahmen fehlen, da (Eintritts-)Wahrscheinlichkeit oder Konsequenz eines Schadensfalles höher sind. Besteht hingegen keine Möglichkeit von Zielabweichungen mehr, kann definitionsgemäß kein Schaden entstehen – dieser Zielzustand wird als „sicher“ bezeichnet (Königs, 2017). Zur Sicherstellung von Informationssicherheit ist es also das Ziel, Schwachstellen zu identifizieren, daraus entstehende Risiken zu bewerten, geeignete[14] Maßnahmen abzuleiten und zu implementieren.

Dabei ist es durchaus möglich, dass ein gewisses Restrisiko (Risiko nach der Behandlung mit Maßnahmen) bestehen bleibt. Ob ein Restrisiko akzeptiert werden kann oder eine weitere Behandlung durch Maßnahmen erfordert, ist z.B. im Rahmen von Akzeptanzvorgaben durch die Geschäftsleitung eines Unternehmens festzulegen, da die Risiko-Toleranz von der Art des Geschäfts(-zweiges) abhängt und im Verhältnis zu verfügbaren Ressourcen definiert werden muss (Königs, 2017).

5.2 Risikomanagementprozess

Es erscheint durch die geschilderten Aspekte notwendig und sinnvoll, Informationssicherheit mit Hilfe eines risikobasierten Ansatzes in Angriff zu nehmen. Der Fallstrick dabei ist, wenn die Betrachtung der Risiken nur einmalig erfolgt und damit veränderten Sicherheits-, Technologie- oder Umweltsituationen und dem Umstand, dass Sicherheit selbst wie beschrieben ein Prozess ist,

[14] „geeignet“ bedeutet in diesem Zusammenhang: an die unternehmerischen Ziele, Vorgaben und Rahmenbedingungen angepasst

nicht Rechnung getragen wird. Deswegen ist es erforderlich, auch das Informationssicherheitsrisikomanagement als Prozess zu betrachten.

Ein solcher Risikomanagementprozess (RMP) in inhärent rekursiv, das heißt mit bedarfsbezogenen Rückkopplungen der Komplexität und vor allem der Dynamik heutiger Risikosituationen im Informationssicherheitskontext angepasst und keine strikte einmalige Abfolge von einzelnen Aktivitäten. Die Grundstruktur des nachfolgend erläuterten Prozesses orientiert sich an den Standards ISO:31000 und ISO/IEC:27005 (Königs, 2013).

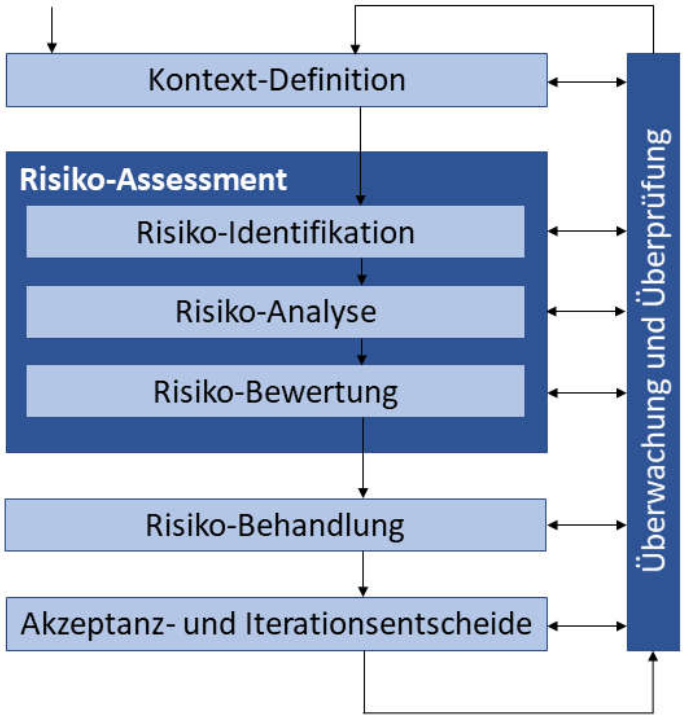

Abbildung 8: grafische Darstellung des Risikomanagementprozesses, nach (Königs, 2013)

5.3 Zusammenstellung von Risiken im IoT-Kontext

Die zuvor erfolgte Definition eines Risikos umfasst die Bewertung einer Wahrscheinlichkeit oder Häufigkeit. Da der folgenden Analyse kein konkreter IoT-Anwendungsfall in einem Unternehmen zu Grunde liegt, aus dessen Kontext sich eine Wahrscheinlichkeit oder ein quantifiziertes Schadensausmaß ableiten ließe, wird auf eine (abstrakte) Festlegung verzichtet. Das heißt, die laut RMP geforderte Risikoanalyse- und Bewertung finden an dieser Stelle nicht in dem Ausmaß statt, wie es im Unternehmen im Anwendungsfall notwendig sein wird. Für alle angeführten Schwachstellen wird jedoch die Bedrohung mit einer Wahrscheinlichkeit und Konsequenz (im Sinne eines Schadens) größer null erwartet, was zu einem Risiko führt. Betrachtet wird zudem, auf welche Schutzziele sich ein Risiko auswirken kann.

Als Ausgangsbasis, für die gemäß dem RMP geforderte Identifikation der Risiken, werden Schwachstellen im Kontext der Informationssicherheit betrachtet, die im Rahmen des Einsatzes von IoT zu speziellen, neuartigen Schwachstellen führen (RMP: Kontext-Definition). In diesen

Fällen entsteht oftmals ein neuartiges Risiko der Verletzung der definierten Schutzziele, was eine Risikobehandlung notwendig macht (wobei Akzeptanz gemäß Definition eine mögliche Form der Behandlung darstellt).

Ziel der nachfolgenden Auflistung der Risiken ist es, ein möglichst umfassendes, durch strukturierte Erhebung zusammengestelltes Kompendium zur Hand zu haben, auf Basis dessen die individuelle Bewertung innerhalb eines (IoT-)Anwendungsfalles erfolgen kann. Im Kontext des Risikomanagementprozesses muss jedoch immer darauf geachtet werden, dieses Kompendium entsprechend technologischen, organisatorischen oder gesellschaftlichen Entwicklungen zu erweitern bzw. anzupassen (RMP: Überwachung und Überprüfung).

Konzeptionelle Hinweise für eine Schwachstellenanalyse für sichere IoT-Integration können aus mehreren Bereichen gewonnen werden: BYOD-Securitykonzepte (auf Grund einiger Ähnlichkeiten zu IoT), Empfehlungen für OT-Netze (Produktions-/Infrastrukturnetze) wie NIST ICS oder aus generischen Informationssicherheits-Frameworks wie BSI Grundschutz oder der ISO 27000. Alle der genannten Richtlinien zielen jedoch nicht explizit auf IoT ab, weswegen in der Folge eine eigenständige Ableitung von IoT-spezifischen Schwachstellen und daraus resultierenden Risiken erfolgt. Es wird dabei auch individuell betrachtet, auf welche Schutzziele sich diese auswirken.

Für die nachfolgende Analyse wurden zwei Rahmenwerke exemplarisch herangezogen. Zum einen die ISO/IEC 27000 (konkret 27002) und die NIST-ICS-Guideline. Erstere auf Grund ihrer großen lokalen Relevanz (insb. auf Grund der DSGVO) und ihrer umfassenden Betrachtung organisatorischer Aspekte. Die NIST ICS wurde gewählt, da IoT und ICS gewisse Ähnlichkeiten, vor allem hinsichtlich der Einschränkungen und Rahmenbedingungen der Geräte selbst (z.B. begrenzte Ressourcen), aufweisen. Für eine Durchführung eines solchen Schritts in einem konkreten Anwendungsfall kann aber jedes zur Verfügung stehende Rahmenwerk herangezogen werden, wenn es besser zu den unternehmerischen Anforderungen passt.

5.3.1 Organisatorische Risiken

Nachfolgende abgeleitete Risiken werden dem Bereich der organisatorischen Risiken zugeordnet.

Nummer	**O1**	Auswirkung auf:	Alle Schutzziele	Referenz:	ISO27002: 5.1, 6.1
Schwachstelle		fehlende Vorgaben und Unterstützung der Informationssicherheit seitens der Unternehmensleitung (Informationssicherheitspolitik); fehlende Verantwortlichkeiten			
Schwachstelle(n) im IoT-Kontext		keine Vorgaben und Unterstützung der Informationssicherheit im IoT-Bereich durch die Unternehmensleitung mangels Wissens über den Einsatz von IoT oder Unkenntnis der Geschäftsrelevanz			
Risiko		**fehlende Ressourcen für die Sicherstellung von Informationssicherheit beim Einsatz von IoT; dadurch potenziell höhere Wahrscheinlichkeit der Verletzung der Informationssicherheit**			

Nummer	**O2**	Auswirkung auf:	Alle Schutzziele	Referenz:	ISO27002: 6.1.2
Schwachstelle		keine Trennung von in Konflikt stehenden Aufgaben und Verantwortlichkeitsbereichen			
Schwachstelle(n) im IoT-Kontext		durch kurze Time-to-Market und Lifecycles entsteht bei Entscheidern ein Konflikt zwischen ausgereifter Implementierung von Sicherheit und schneller Marktreife bzw. schnellem Einsatz, was bei gleicher Zuständigkeit zu Vernachlässigung von Sicherheit führen kann			
Risiko		**niedriges Sicherheitslevel von IoT-Implementierungen; dadurch potenziell höhere Wahrscheinlichkeit der Verletzung der Informationssicherheit**			

Nummer	**O3**	Auswirkung auf:	Alle Schutzziele	Referenz:	NIST ICS 3.3.1
Schwachstelle		unzulängliche Security-Policy			
Schwachstelle(n) im IoT-Kontext		kein Vorliegen einer überhaupt an generelle IoT-Bedürfnisse angepassten Security-Policy			
Risiko		**uneinheitliches Sicherheitslevel von IoT-Implementierungen; dadurch potenziell höhere Wahrscheinlichkeit der Verletzung der Informationssicherheit**			

Nummer	**O4**	Auswirkung auf:	Alle Schutzziele	Referenz:	ISO27002: 7.1 NIST ICS 3.3.1
Schwachstelle		Beschäftigte und Auftragnehmer bzw. Auftragnehmerinnen verfügen nicht über die notwendige Kompetenz im Bereich Informationssicherheit; fehlende Verantwortlichkeiten für Informationssicherheit			
Schwachstelle(n) im IoT-Kontext		Beschäftigte und Auftragnehmer bzw. Auftragnehmerinnen verfügen nicht über die notwendige Kompetenz hinsichtlich der speziellen Aspekte der IoT-Sicherheit; keine organisatorische Klärung der Verantwortlichkeit für Informationssicherheit bei IoT-Applikationen			
Risiko		**niedriges Sicherheitslevel von IoT-Implementierungen; dadurch potenziell höhere Wahrscheinlichkeit der Verletzung der Informationssicherheit**			

Nummer	**O5**	Auswirkung auf:	Alle Schutzziele	Referenz:	ISO27002: 8.1 NIST ICS 3.5
Schwachstelle		fehlende oder unzureichende Identifizierung der Werte der Organisation			
Schwachstelle(n) im IoT-Kontext		IoT-Geräte/Applikationen werden nicht oder nicht ausreichend als eigenständige, schützenswerte Unternehmenswerte erkannt			
Risiko		**vorhandene Informationssicherheitsprozesse werden nicht angewandt, da IoT-Geräte/Applikationen nicht als Assets gesehen werden; daraus resultieren ein niedrigeres Sicherheitsniveau und potenziell höhere Wahrscheinlichkeit der Verletzung der Informationssicherheit**			

Nummer	**O6**	Auswirkung auf:	Alle Schutzziele	Referenz:	NIST ICS 3.3.1 ISO27002: 7.2
Schwachstelle		kein formelles Informationssicherheits- oder Sensibilisierungs-Training, fehlende Qualifikationsmaßnahmen des Personals, fehlendes Bewusstsein für Verantwortlichkeiten			
Schwachstelle(n) im IoT-Kontext		getroffene Maßnahmen im Unternehmen zielen nur auf klassische Informationssicherheit ab, IoT-Aspekte werden nicht berücksichtigt			
Risiko		**niedriges Sicherheitslevel von IoT-Implementierungen; dadurch potenziell höhere Wahrscheinlichkeit der Verletzung der Informationssicherheit**			

Nummer	**O7**	Auswirkung auf:	Alle Schutzziele	Referenz:	NIST ICS 3.3.1 ISO27002: 12.7
Schwachstelle		fehlende, unzureichende oder unangemessene Security-Audits			
Schwachstelle(n) im IoT-Kontext		IoT-Applikationen werden nicht oder mit unpassenden Mitteln bei Security-Audits berücksichtigt; Einschränkung der Systemverfügbarkeit bei IoT-Applikationen durch zu intensive Auditvorgänge; fehlende Protokollierung			
Risiko		**Security-Audits sind unvollständig und tragen damit nicht zu einer umfassenden Sicherstellung des Schutzniveaus bei (damit verfehlen sie ihren Zweck)**			

Nummer	**O8**	Auswirkung auf:	Alle Schutzziele	Referenz:	NIST ICS 3.3.1
Schwachstelle		unangemessene Sicherheitsarchitektur und -Design und fehlende Sicherheitsmechanismen durch ungeschultes Personal und Einsatz von Komponenten, die keine Sicherheitseigenschaften aufweisen			
Schwachstelle(n) im IoT-Kontext		Einbettung neuartiger Komponenten in vorhandene Netzwerke ohne Abänderung oder Anpassung der Sicherheitsarchitektur, Verwendung von (Consumer-)IoT-Geräten und Applikationen mit mangelhaften Sicherheitseigenschaften			
Risiko		**Aufweichung des Sicherheitsstandards durch Erhöhung der Anzahl an Schwachstellen (Senkung des Schutzniveaus); dadurch potenziell höhere Wahrscheinlichkeit der Verletzung der Informationssicherheit**			

Nummer	**O9**	Auswirkung auf:	Alle Schutzziele	Referenz:	ISO27002: 8.2
Schwachstelle		das Schutzniveau von Informationen ist nicht ihrer Bedeutung für das Unternehmen angemessen			
Schwachstelle(n) im IoT-Kontext		die starke Zunahme des Datenaufkommens in IoT-Umgebungen führt dazu, dass darin enthaltene relevante Informationen nicht als solche oder überhaupt nicht klassifiziert werden			
Risiko		**fehlen angemessener Schutzmaßnahmen für wichtige Informationen; dadurch potenziell höhere Wahrscheinlichkeit der Verletzung der Informationssicherheit**			

Nummer	**O10**	Auswirkung auf:	Alle Schutzziele	Referenz:	ISO27002: 8.1
Schwachstelle		mangelhafte Verwaltung der Werte (Life Cycle Management)			
Schwachstelle(n) im IoT-Kontext		IoT-Geräte werden nicht in einem passenden Life Cycle Management erfasst; unvollständiges Inventar (auf Grund hoher Anzahl an verschiedenartigen Geräten) und fehlende Verantwortlichkeiten sorgen insbesondere am Ende des Lebenszyklus für eine nicht ordnungsgemäße Deprovisionierung und Entfernung von Geräten aus dem Netzwerk			
Risiko		**IoT-Geräte bleiben unerkannt als Zombie-Geräte im eigenen Netz, erhalten keine Sicherheitspatches mehr und führen zu immer mehr angreifbaren Schwachstellen**			

Nummer	**O11**	Auswirkung auf:	Alle Schutzziele	Referenz:	NIST ICS 3.3.1 ISO27002: 8.2, 12.1
Schwachstelle		fehlendes Configuration Change Management			
Schwachstelle(n) im IoT-Kontext		durch neuartige Geräte, heterogene Produktlandschaften und potenziell große Anzahl an Devices gibt es keine oder nur mangelhafte Integration in ggf. bestehende Configuration Change Management-Prozesse und -Systeme			
Risiko		**die Integrität der Systemkonfigurationen ist nicht sichergestellt, was eine Erhöhung der Anzahl an unentdeckten bzw. unbekannten Schwachstellen zur Folge haben kann**			

Nummer	**O12**	Auswirkung auf:	Vertraulichkeit	Referenz:	ISO27002: 6.1.2
Schwachstelle		fehlende Richtlinie und Sicherheitsmaßnahmen bei der Nutzung von Mobilgeräten			
Schwachstelle(n) im IoT-Kontext		fehlende Richtlinie und Sicherheitsmaßnahmen bei der Nutzung von (mobilen) IoT-Geräten (insb. schwerwiegend, da es sehr viele mobile IoT-Geräte geben kann); klassische Maßnahmen wie sie aus dem BYOD-Bereich bekannt sind, können durch Systemlimitierungen nicht angewendet werden			
Risiko		**Diebstahl, Verlust und unkontrollierter Zugang stellen bei mobilen Geräten ein zusätzliches Risiko dar; ein Datenverlust ist leichter möglich**			

Nummer	**O13**	Auswirkung auf:	Vertraulichkeit, Verfügbarkeit	Referenz:	ISO27002: 8.3 NIST ICS 3.4
Schwachstelle		Verlust von Vertraulichkeit, Integrität oder Verfügbarkeit von Informationen auf Wechseldatenträgern durch fehlende Maßnahmen entsprechend der Informationsklassifizierung			
Schwachstelle(n) im IoT-Kontext		IoT-Geräte sind klein, ggf. mobil oder zumindest leicht beweglich, darauf gespeicherte Informationen können somit ebenfalls leicht abhandenkommen, wenn keine besonderen Maßnahmen getroffen werden; auch bei Außerbetriebnahme/Entsorgung			
Risiko		**Verlust von Informationen (Bruch der Vertraulichkeit) oder abhandenkommen von Informationen (Verletzung der Verfügbarkeit) durch Diebstahl, Verlust oder unsachgemäße Entsorgung von IoT-Geräten**			

Nummer	**O14**	Auswirkung auf:	Vertraulichkeit, Integrität	Referenz:	ISO27002: 9.1
Schwachstelle		der Zugang zu Informationen ist nicht eingeschränkt (fehlende Zugangssteuerungsrichtlinie, mangelhafte Benutzerzugangsverwaltung, fehlerhafte Zuteilung von Rechten)			
Schwachstelle(n) im IoT-Kontext		im Unternehmen eingesetzte, bewährte Zugangs- und Zugriffssteuerungsmechanismen sind auf Grund technischer Limitierungen nicht möglich; Erteilung und Entziehung von Zugriffsrechten für IoT-Applikationen und -Geräte folgen nicht den normalen Verfahren; neuartige Situation des Zugriffs von IoT-Geräten auf andere Geräte ohne Benutzerinteraktion und fehlende Zugangssteuerung auf Gerätebasis; limitierte Möglichkeiten granularer Zugriffssteuerung (Rollenmodelle); keine Anbindung an unternehmenseigene Verzeichnisdienste möglich			
Risiko		**Beeinträchtigung der Vertraulichkeit und des „Need-to-Know"-Prinzips; Daten- und Informationsverlust durch unbefugte Weitergabe; ggf. (datenschutz)rechtliche Konsequenzen**			

Nummer	**O15**	Auswirkung auf:	Alle Schutzziele	Referenz:	ISO27002: 11.1, 11.2 NIST ICS 3.5
Schwachstelle		mangelnder physischer Zugangsschutz (Schutz vor unbefugtem Zutritt, Beschädigung oder Beeinträchtigung von Informationen)			
Schwachstelle(n) im IoT-Kontext		viele Einsatzgebiete von IoT sind gerade darauf ausgelegt, dass IoT-Geräte in der Alltagsumgebung vorhanden sind (Smart Home, Sensoren, …) und daher nicht wie klassische Informationssysteme z.B. in einem Serverraum physisch leicht abgeschottet bzw. zugriffsgeschützt betrieben werden können; IoT-Geräte sind Umweltbedingungen ausgeliefert; auf physische Schnittstellen der Geräte kann einfach zugegriffen werden; Drahtlosübertragungen von Informationen in ungeschützten Bereichen			
Risiko		**Beeinträchtigung der Verfügbarkeit (Diebstahl, Verlust, Vandalismus), Gefahr des Verlustes sensibler Daten insb. auf Grund von elektromagnetischer Abstrahlung; Erlangung des Zugriffs auf Geräte durch physischen Zugriff**			

Nummer	**O16**	Auswirkung auf:	Alle Schutzziele	Referenz:	ISO27002: 12.1 NIST ICS 3.3.2
Schwachstelle		fehlende Dokumentation von Betriebsabläufen (Installation, Konfiguration, Verarbeitungsarten, Backup, Wiederherstellung, …)			
Schwachstelle(n) im IoT-Kontext		durch große Anzahl und heterogene Landschaften wird eine entsprechende Dokumentation nicht durchgeführt; zentrale Verwaltung durch (Standard-)Werkzeuge deswegen ebenso nicht möglich			
Risiko		**Senkung des Sicherheitsniveaus, insb. hinsichtlich Verfügbarkeit, durch mangel- oder fehlerhafte Dokumentation, fehlende Standardabläufe (Backup, Wiederherstellung) und mangelhafte Kapazitätsplanung**			

Nummer	**O17**	Auswirkung auf:	Vertraulichkeit,	Referenz:	ISO27002: 14.1
Schwachstelle		Informationssicherheit ist kein organisationsweit geplanter fester Bestandteil des gesamten Lebenszyklus von Informationssystemen			
Schwachstelle(n) im IoT-Kontext		durch schnelle Lebenszyklen und kurze Time-to-Market im IoT-Umfeld wird der Aspekt der Informationssicherheit besonders vernachlässigt			
Risiko		**bei Beschaffung, Konfiguration, Integration und Bereitstellung von IoT-Applikationen wird nur ein niedrigeres Schutzniveau erreicht als bei normalen Informationssystemen**			

Nummer	**O18**	Auswirkung auf:	Alle Schutzziele	Referenz:	ISO27002: 14.2
Schwachstelle		der Aspekt der Informationssicherheit ist nicht im (Software-) Entwicklungszyklus von Informationssystemen geplant und umgesetzt.			
Schwachstelle(n) im IoT-Kontext		durch schnelle Lebenszyklen und kurze Time-to-Market im IoT-Umfeld wird der Aspekt der Informationssicherheit bei der Softwareentwicklung vernachlässigt			
Risiko		**entwickelte IoT-Applikationen entsprechen nicht dem für andere Anwendungen geplanten und umgesetzten Sicherheitsniveau und sind damit verwundbarer (mehr Schwachstellen) gegenüber Bedrohungen**			

Nummer	**O19**	Auswirkung auf:	Vertraulichkeit	Referenz:	ISO27002: 15.2
Schwachstelle		die Informationssicherheit ist bei Dienstleistungserbringern und Lieferanten nicht gewährleistet			
Schwachstelle(n) im IoT-Kontext		vermehrter Einsatz von Applikationen und Plattformen von Drittanbietern (z.B. Cloud-Plattformen) ohne entsprechende Verträge und Sicherstellung eines geforderten Mindeststandards bezüglich der Informationssicherheit beim Dienstleister			
Risiko		**Verlust von Informationen (Bruch der Vertraulichkeit) oder abhandenkommen von Informationen durch Diebstahl oder Weitergabe (Verletzung der Verfügbarkeit) durch Angriffe auf Cloud-Provider; Verletzung rechtlicher Pflichten (z.B. DSGVO) des Unternehmens**			

Nummer	**O20**	Auswirkung auf:	Alle Schutzziele	Referenz:	ISO27002: 16.1
Schwachstelle		fehlende Regelung im Umgang mit Informationssicherheitsvorfällen (Meldung, Beurteilung, Reaktionen, Erkenntnisse)			
Schwachstelle(n) im IoT-Kontext		potenziell hohe Anzahl an Sicherheitsvorfällen durch hohe Anzahl an Geräten und Applikationen, durch unangepasste Prozesse findet kein, langsamer oder ungeeigneter Umgang damit statt			
Risiko		**durch Fehlen eines wirksamen organisatorischen Umgangs mit Sicherheitsvorfällen können keine angemessenen Gegenmaßnahmen eingeleitet werden, das Informationssicherheitsniveau sinkt kontinuierlich**			

Nummer	**O21**	Auswirkung auf:	Verfügbarkeit, Vertraulichkeit	Referenz:	ISO27002: 17.1 NIST ICS 3.3.2
Schwachstelle		die Aufrechterhaltung der Informationssicherheit ist nicht in das Business Continuity Management / Disaster Recovery Management eingebettet			
Schwachstelle(n) im IoT-Kontext		IoT-Anwendungen sind nicht in das Business Continuity Management / Disaster Recovery Management eingebettet, da diese z.B. nicht als geschäftskritisch erkannt werden			
Risiko		**im Krisen- oder Katastrophenfall ist die Informationssicherheit nicht mehr sichergestellt (das Schutzniveau kann nicht aufrechterhalten werden), es kommt zu einer Beeinträchtigung der Verfügbarkeit (bis hin zum Produktionsausfall) oder einem Verlust der Vertraulichkeit**			

Nummer	**O22**	Auswirkung auf:	Verfügbarkeit	Referenz:	ISO27002: 17.2 NIST ICS 3-5
Schwachstelle		wichtige informationsverarbeitende Einheiten sind nicht redundant ausgelegt			
Schwachstelle(n) im IoT-Kontext		durch technische Limitierungen nur geringe Möglichkeiten Redundanzen bei IoT-Geräten sicherzustellen, wie sie bei normalen Informationsverarbeitungssystemen möglich sind.			
Risiko		**im Fehler- oder Ausfallfall ist die Verfügbarkeit von Informationen beeinträchtigt.**			

Nummer	**O23**	Auswirkung auf:	Vertraulichkeit	Referenz:	ISO27002: 18.1.4
Schwachstelle		fehlende Datenrichtlinie zum Umgang mit personenbezogenen Daten entsprechend gesetzlicher Vorschriften			
Schwachstelle(n) im IoT-Kontext		fehlende Datenrichtlinie zum Umgang mit personenbezogenen Daten in IoT-Applikationen			
Risiko		**unangemessenes Schutzniveau oder unerlaubte Verarbeitung von Daten; entsprechend eine Nichteinhaltung gesetzlicher Vorschriften (z.B. DSGVO), Strafzahlungen oder andere Sanktionen, Imageschaden**			

5.3.2 Technische Risiken

Die ISO 27002 fordert in Abschnitt 12.6 eine Verhinderung der Ausnutzung technischer Schwachstellen. Dies ist allerdings ein sehr umfangreiches Unterfangen, da solche Schwachstellen an den unterschiedlichsten Stellen und durch verschiedenste Gründe auftreten können. Nachfolgend werden daher übliche technische Schwachstellen aufgezählt, welche im IoT-Umfeld zu relevanten Risiken führen. „Technisch“ bedeutet in diesem Kontext, dass sich eine Schwachstelle direkt auf die IoT-Geräte, Applikationen, Vernetzung oder im Zusammenhang damit eingesetzte Technologien bezieht. Auf eine abschnittsweise Unterteilung wird auf Grund vieler thematischer Überlappungen verzichtet.

Nummer	**T1a**	Auswirkung auf:	Alle Schutzziele	Referenz:	ISO27002: 13.2 NIST ICS 3-6
Schwachstelle		die Sicherheit der Information bei Informationsübertragungsvorgängen (intern wie extern) ist nicht sichergestellt			
Schwachstelle(n) im IoT-Kontext		Einsatz unangemessener Technologien, wie es z.B. bei der Verwendung von Consumer-Geräten mit unzureichenden Sicherheitsmechanismen der Fall sein kann; die unternehmensüblichen Standards können durch Limitierungen bei IoT-Geräten nicht eingehalten werden; Übertragung auf nicht üblichen Kanälen (Funk-/Mesh-Netze, …) oder durch Geräte direkt im Internet außerhalb des Unternehmensnetzwerks, welche nicht mit den unternehmensüblichen Mechanismen abgesichert werden bzw. werden können			
Risiko		**Informationen können abgefangen, kopiert, verändert oder gelöscht werden; Offenlegung vertraulicher Informationen; Nachweisprobleme bei Nachverfolgbarkeit und Nicht-Abstreitbarkeit**			

Nummer	**T1b**	Auswirkung auf:	Alle Schutzziele	Referenz:	NIST ICS 3-6
Schwachstelle		Verwendung von Kommunikationsprotokollen ohne eingebaute Sicherheitsmechanismen			
Schwachstelle(n) im IoT-Kontext		neuartige Kommunikationsprotokolle bei IoT wurden oftmals nicht auf Sicherheitseigenschaften ausgerichtet oder implementieren nur schwache Schutzmechanismen, dadurch sehr oft Einsatz von Technologien, gegen welche einfache Angriffe möglich sind			
Risiko		**verschiedene (einfache) Angriffe gegen IoT-Geräte oder -Applikationen möglich, welche eines der Schutzziele verletzen**			

Anm.: Die Risiken 1a und 1b ähneln sich sehr stark, jedoch zielt 1a auf die generell fehlende Sicherstellung der Sicherheit bei einer Informationsübertragung ab, während 1b schwache Protokolle und Implementierungen referenziert.

Nummer	**T2**	Auswirkung auf:	Alle Schutzziele	Referenz:	n/a
Schwachstelle		schlecht programmierte oder unsichere Kommunikationsschnittstellen			
Schwachstelle(n) im IoT-Kontext		schlechte bzw. unsichere Implementierung von Kommunikationsschnittstellen (Interfaces), welche zum Datenaustausch zwischen IoT-Geräten verwendet werden			
Risiko		**Senkung des zuvor gegebenen Schutzniveaus im Netzwerk; Angriffe auf IoT-Geräte und Applikationen durch zusätzliche Schwachstellen leichter möglich**			

Nummer	**T3**	Auswirkung auf:	Alle Schutzziele	Referenz:	ISO27002: 13.1
Schwachstelle		keine Trennung in separate Netzwerkdomänen in größeren Netzwerken und fehlende Regelung der Übergänge zwischen den Domänen			
Schwachstelle(n) im IoT-Kontext		Vermischung der Domänen des normalen Unternehmensnetzwerks mit IoT-Netzwerken; durch per Definition intensiven Datenaustausch zwischen IoT-Geräten ungenügende Absicherung der Übergangspunkte			
Risiko		**Senkung des zuvor gegebenen Schutzniveaus im Netzwerk; Ausbreitung von Schadsoftware und anderen Gefährdungen im Netzwerk dadurch leichter möglich**			

Nummer	**T4**	Auswirkung auf:	Alle Schutzziele	Referenz:	ISO27002: 13.1 NIST ICS 3-13
Schwachstelle		unzureichende Absicherung von Drahtlosnetzwerken			
Schwachstelle(n) im IoT-Kontext		intensive Verwendung drahtloser Technologien im IoT-Bereich; die dabei eingesetzten Protokolle und Technologien weichen ggf. vom Unternehmensstandard ab			
Risiko		**Informationen können abgefangen, kopiert, verändert oder gelöscht werden; Offenlegung vertraulicher Informationen; Nachweisprobleme bei Nachverfolgbarkeit und Nichtabstreitbarkeit**			

Nummer	**T5**	Auswirkung auf:	Alle Schutzziele	Referenz:	NIST ICS 3.3.2
Schwachstelle		Betriebssystempatches werden nicht zeitgerecht nach Bekanntwerden einer Schwachstelle bereitgestellt			
Schwachstelle(n) im IoT-Kontext		durch Consumerization und kurze Life Cycles kann es auch auftreten, dass überhaupt keine Patches (betreffend Betriebssystem und/oder Applikation) mehr bereitgestellt werden			
Risiko		**potenziell große Anzahl an verwundbaren Geräten im Netzwerk sowie verwundbare Applikationen, bei denen Schwachstellen öffentlich bekannt und sie damit frei angreifbar sind.**			

Nummer	**T6**	Auswirkung auf:	Alle Schutzziele	Referenz:	NIST ICS 3.3.2
Schwachstelle		Betriebssystem- und Applikationspatches werden ohne ausreichende (Sicherheits-)Tests eingespielt			
Schwachstelle(n) im IoT-Kontext		durch die Vielzahl an Geräten und Applikationen stehen nicht ausreichend (Personal-)Ressourcen für umfangreiches Testen aller Patches zur Verfügung			
Risiko		**potenziell große Anzahl an verwundbaren Geräten im Netzwerk, welche frei angreifbar sind.**			

Nummer	**T7**	Auswirkung auf:	Alle Schutzziele	Referenz:	NIST ICS 3.3.2
Schwachstelle		Nutzung der Standardkonfiguration eines Devices, wodurch nicht benötigte Ports und Services aktiviert bleiben			
Schwachstelle(n) im IoT-Kontext		die letzten großen Attacken auf IoT-Devices im Internet haben genau auf solche Konfigurationen abgezielt, da diese oft mangelhaft sind und von Usern bzw. Userinnen nicht angepasst werden. Geräte können dadurch kompromittiert oder übernommen werden			
Risiko		**Verlust der Kontrolle über IoT-Devices oder Teilnahme der Geräte an Botnetzen, Nutzung der Devices für DoS-Attacken, Datenverlust, Datenmanipulation, Nutzung der Geräte als Einstiegspunkt in das Unternehmensnetz (APT)**			

Nummer	**T8**	Auswirkung auf:	Alle Schutzziele	Referenz:	NIST ICS 3.3.2, 3.4 ISO27002: 9.2, 9.4
Schwachstelle		keine Nutzung von Passwörtern, Nutzung von Standardpasswörtern oder zu schwachen/erratbaren Passwörtern, Speicherung von Passwörtern an ungeeigneten Stellen im Klartext; ungeeignete Algorithmen zur Passwortverarbeitung			
Schwachstelle(n) im IoT-Kontext		Änderung von Passwörtern auf Geräten nicht möglich; unternehmensseitige Passwort-Vorgaben können auf Grund von technischen Limitierungen nicht eingehalten werden; Nachlässigkeit bei der Einrichtung/Konfiguration der Geräte (keine Änderung von Standardpasswörtern); schlechte/schwache eigene oder bei gekauften Geräten eingesetzte Algorithmen			
Risiko		**Verlust der Kontrolle über IoT-Devices oder Teilnahme der Geräte an Botnetzen, Nutzung der Devices für DoS-Attacken, Datenverlust, Datenmanipulation, Nutzung der Geräte als Einstiegspunkt in das Unternehmensnetz (APT)**			

Nummer	**T9**	Auswirkung auf:	Vertraulichkeit, Integrität	Referenz:	ISO27002: 10
Schwachstelle		angemessener und wirksamer Gebrauch von Kryptographie zum Schutz der Vertraulichkeit, Authentizität und Integrität von Information ist nicht sichergestellt			
Schwachstelle(n) im IoT-Kontext		durch technische Limitierungen von IoT-Geräten hinsichtlich Rechenleistung oder unterstützter Protokolle kann unter umständen der Stand der Technik oder der sonst übliche hohe Kryptographiestandard im Unternehmen nicht eingehalten werden.			
Risiko		**Verlust von Vertraulichkeit, Authentizität oder Integrität bei der Informationsübertragung**			

Nummer	**T10**	Auswirkung auf:	Alle Schutzziele	Referenz:	ISO27002: 12.2
Schwachstelle		Informationen und Informationsverarbeitungssysteme sind nicht ausreichend vor Schadsoftware geschützt			
Schwachstelle(n) im IoT-Kontext		durch den Einsatz verschiedenartigster IoT-Plattformen und -Geräten können unternehmensübliche Ansätze zum Schutz vor Schadsoftware ggf. nicht eingesetzt werden (z.B. Schadsoftwareerkennungssoftware); bei proprietären Systemen ist eine individuelle Anpassung der laufenden Software z.B. durch manuelle Einschränkungen nicht möglich			
Risiko		**Infektion mit und Ausbreitung von Schadsoftware und dadurch Verlust von Vertraulichkeit, Integrität oder Verfügbarkeit (z.B. Weitergabe/Offenlegung, Datenmanipulation, Datenverlust durch Löschung)**			

Nummer	**T11**	Auswirkung auf:	Alle Schutzziele	Referenz:	ISO27002: 9.1
Schwachstelle		der Zugang zum Netzwerk und Netzwerkdiensten ist nicht angemessen eingeschränkt.			
Schwachstelle(n) im IoT-Kontext		die Einbringung neuer IoT-Geräte in Netzwerke ist nicht ausreichend eingeschränkt, Geräte können unerkannt im Unternehmensnetzwerk betrieben werden; normale Verfahren zur Netzwerkzugangskontrolle können auf Grund technischer Limitierungen nicht verwendet werden; IoT-Geräte müssen ggf. aus dem Internet erreichbar sein			
Risiko		**ohne Zugangssteuerungsmechanismen sind Geräte im Netzwerk, die nicht den Sicherheitsstandards des Unternehmens entsprechen; durch den Einsatz ungeeigneter Geräte mit fehlender Funktionalität müssen Ausnahmen von den allgemeinen Zugangsmechanismen gemacht werden; in allen Fällen wird das allgemeine Schutzniveau gesenkt**			

Nummer	**T12**	Auswirkung auf:	Vertraulichkeit, Integrität	Referenz:	ISO27002: 12.4 NIST ICS 3-6
Schwachstelle		Ereignisse (Benutzeraktivitäten, Ausnahmen, Störungen und Informationssicherheitsvorfälle) werden nicht in Ereignisprotokollen aufbewahrt und regelmäßig überprüft			
Schwachstelle(n) im IoT-Kontext		durch technische Limitierungen von IoT-Geräten hinsichtlich Rechenleistung oder Speicherplatz, unpassende und/oder nicht veränderbare Logging-Einstellungen, Nichtverfügbarkeit von Logdaten auf IoT-Geräten, heterogene Umgebungen mit verschiedenartigen Logformaten, zu große Datenmengen etc. werden Eregnisprotokolle nicht (zentral) aufbewahrt und analysiert.			
Risiko		**unerkannte Informationssicherheitsvorfälle, fehlende Nachvollziehbarkeit von Aktivitäten, Verletzung von Aufbewahrungspflichten für Audits, mangelnder Datenschutz bei Aufbewahrung personenbezogener Logdaten**			

Nummer	**T13**	Auswirkung auf:	Verfügbarkeit	Referenz:	NIST ICS 3-6
Schwachstelle		Anfälligkeit für DoS-Attacken			
Schwachstelle(n) im IoT-Kontext		durch technische Limitierungen von IoT-Geräten z.B. hinsichtlich Rechenleistung schwierige Absicherung gegen DoS-Attacken; Erreichbarkeit aus öffentlichen Netzen/Internet von IoT-Geräten bietet wesentlich größere Bedrohungslandschaft; durch Einsatz von Funktechnologien Möglichkeiten zur Betriebsstörung (Jamming, …)			
Risiko		**Einschränkung der Betriebsfähigkeit von Komponenten und Applikationen; Ausfall von Applikationen bis hin zu Einschränkung der Produktivität des Unternehmens**			

5.4 Zusammenfassung

Die zuvor aufgezeigten Risiken lassen sich nach einigen Grundaspekten zusammenfassen. Organisatorische Risiken können, bedingt zumeist durch mangelhafte betriebsinterne Prozesse, zu einer Senkung des allgemeinen Informationssicherheitsniveaus (hinsichtlich meistens aller Schutzziele) führen. Mangelhaft bedeutet in diesem Fall, dass kein Bewusstsein für eine Notwendigkeit der Anpassung beim Einsatz von IoT-Applikationen und/oder -Geräten entwickelt wurde, jedoch eine IoT-spezifische Ausprägung der Schwachstelle existiert. Im Informationssicherheitsmanagement des Unternehmens kommen diese Aspekte dann nicht vor, den geschilderten Risiken wird in der Folge nicht mit entsprechenden Maßnahmen entgegengewirkt. Rückblickend auf Abschnitt 3.2.3 handelt es sich also mehrheitlich um durch mangelhafte Sicherheitspolitik des Unternehmens bedingte Schwachstellen.

Technische Risiken ergeben sich oftmals aus den inhärenten Eigenschaften und Limitierungen von IoT-Geräten, welche in Abschnitt 4.1 bzw. 4.2 erläutert wurden. Weitere Ursachen sind konkrete, praktische Resultate organisatorischer Schwächen. Die verletzten Schutzziele betreffen entweder Vertraulichkeit/Integrität oder die Verfügbarkeit, in manchen Fällen allerdings ebenso alle. Entsprechend der Kategorisierung in Abschnitt 3.2.3 handelt es sich dabei um technologische oder konfigurationsbedingte Schwachstellen.

Die vorhergehende Analyse erhebt keinen Anspruch auf Vollständigkeit, je nach unternehmerischem Anwendungsfall können hier durchaus weitere Risiken entstehen, welche im Einzelfall zu ergänzen sind. Um einigermaßen sicherzustellen, dass mit der gewählten Methodik in dieser Aufstellung auf jeden Fall keine wesentlichen derzeit aktuellen IoT-relevanten Schwachstellen übersehen wurden, erfolgt ein kurzer Abgleich mit der aktuellen Top10-Liste von IoT-Schwachstellen des *OWASP IoT-Projects* (OWASP, 2018). Das Ergebnis dieses Abgleichs ist in Tabelle 2 zu sehen.

OWASPTop 10 2018 Nr.:	Beschreibung	erfasst in:
1	schwache, erratbare oder fest voreingestellte Passwörter	T8
2	unsichere Netzwerkdienste	T1b, T3, T11
3	unsichere Interfaces	T2
4	Fehlen eines sicheren Updatemechanismus	-
5	Nutzung alter oder unsicherer Geräte	T5, T6
6	mangelhafter Datenschutz	O5, O9, O14
7	unsichere Speicherung oder Übertragung von Daten/Informationen	T1a/b, T4, T9
8	fehlendes Gerätemanagement	T5, T7, O10, O16
9	unsichere Voreinstellungen	T7
10	unzureichende physische Absicherung	O15

Tabelle 2: Gegenüberstellung erkannter Risiken und OWASP-Top10 2018

Aus der Tabelle ist ersichtlich, dass fast jedem Punkt der OWASP IoT-Top10 zumindest ein erkanntes Risiko zugeordnet werden kann. Damit zeigt sich, dass die Analyse grundsätzlich zielführend ist. Festzustellen ist aber, dass Punkt 4 nicht behandelt wird. Da sich daraus ein reales Risiko ergeben kann (sonst wäre diese Schwachstelle nicht in den OWASP Top10 gelandet), wird dieser Punkt im nächsten Kapitel explizit behandelt (Abschnitt 6.3.2). Dieser Aspekt könnte alternativ auch als Erweiterung der IoT-Schwachstelle in T10 definiert werden (Schutz vor schadhaften Softwareupdates). Dieses Beispiel zeigt, dass es hilfreich ist, möglichst mehrere und in ihrer Art und Weise verschiedene Quellen zur Identifikation entstehender Sicherheitsrisiken zu verwenden.

Gewiss stellt auch dieser Abgleich nicht endgültig sicher, dass alle möglichen Schwachstellen und Risiken erkannt wurden. Es kann aber als guter Indikator dafür dienen, ob aktuelle (und damit auch häufig für Angriffe genutzte) Schwachstellen abgedeckt sind und daraus ein relevantes Risiko abgeleitet wurde. Die Zusammenstellung in Abschnitt 5.3 liefert also einen guten Ausgangspunkt für die weiteren Überlegungen.

6 KONZEPTION EINES VERBESSERTEN MODELLS

In diesem Kapitel wird ein Sicherheitskonzept erstellt, welches ein hohes Maß an Sicherheit beim Einsatz von IoT im Unternehmensnetzwerk sicherstellen soll. Dazu werden die zuvor identifizierten Risiken herangezogen. Auf Grundlage dieser Erkenntnisse wird (basierend auf entsprechender Literatur und Publikationen) versucht, Maßnahmen zu definieren, welche bei Umsetzung einen verbesserten Zustand darstellen. „Verbessert“ bedeutet in diesem Fall, dass alle Maßnahmen auf IoT-spezifische, erkannte Schwachstellen abgestimmt sind und ein möglichst breites Spektrum an Risiken, insbesondere aber jene im vorigen Kapitel identifizierten, abdecken.

Die Struktur des Modells orientiert sich dabei an Kapitel 3. Wie dort schon erkennbar war, besteht ein Sicherheitskonzept aus vielen einzelnen Bausteinen (Maßnahmen), welche im Zusammenspiel ineinandergreifen und ein gewisses Sicherheitsniveau herstellen sollen. In diesem Kapitel wird nicht näher auf eine (wirtschaftliche oder praktische) Realisierbarkeit der Konzepte eingegangen, sondern aufgezeigt, welche Aspekte zur Erreichung von IoT-Sicherheit betrachtet werden müssen, um diese nachfolgend mit den Maßnahmen vorhandener Netzwerksicherheitskonzepte zu vergleichen.

Gemäß dem eingangs skizzierten Vorgehensmodell werden Themengebiete dieser Maßnahmen als relevante Handlungsfelder definiert, weil, wie im vorhergehenden Kapitel nachgewiesen, Risiken existieren, welche die Informationssicherheit negativ beeinflussen können. Entsprechend werden zu jeder Maßnahme auch die jeweiligen Risiken aus Abschnitt 5.3 genannt, welche sie behandeln können.

6.1 Organisatorische Aspekte

In diesem ersten Abschnitt werden organisatorische Maßnahmen behandelt, welche eine Verbesserung der Informationssicherheit zur Folge haben sollen.

6.1.1 Informationssicherheitsmanagement

Aus den in Abschnitt 5.3.1 aufgezeigte Risiken ergibt sich, dass eine organisatorische Behandlung der Informationssicherheit beim Einsatz von IoT-Geräten unumgänglich ist, da ansonsten durch viele verschiedene Faktoren eine Senkung des Schutzniveaus droht.

Beim (geplanten) Einsatz von IoT-Anwendungen müssen daher das gesamte Informationssicherheitsmanagement in allen Punkten von Beginn an um die Betrachtung der IoT-Aspekte erweitert und die daraus erwachsenden Konsequenzen verstanden werden. Dies beginnt bei einer Bewusstseinsschaffung im letztendlich für Informationssicherheit verantwortlichen Management des Unternehmens für die durch IoT-Einsatz erhöhte Gefährdungslage. Ausgehend von der Informationssicherheitspolitik des Unternehmens müssen für IoT entsprechende Sicherheitsziele definiert werden. Dabei ist es auch entscheidend, die Schutzwürdigkeit der verarbeiteten Daten zu

ermitteln und festzulegen. Die durch die speziellen Rahmenbedingungen auftretenden Bedrohungen sind in der Sicherheitsarchitektur zu berücksichtigen. Daraus abgeleitete Richtlinien enthalten dann klare Vorgaben, auf Basis derer die Sicherheitskonzepte für IoT-Geräte und -Anwendungen entwickelt werden können. Nur im Rahmen eines solchen durchgängigen Prozesses wird es möglich sein, den durchaus entstehenden Mehraufwand und/oder notwendige organisatorische Änderungen für eine sichere Implementierung zu rechtfertigen und entsprechende Mittel und Ressourcen zur Verfügung gestellt zu bekommen.

Das Themengebiet Business Continuity/Disaster Recovery sollte für IoT-Anwendungen ebenso im Rahmen der organisatorischen Informationssicherheit behandelt werden. Dabei muss sichergestellt sein, dass IoT-Anwendungen, insbesondere wenn sie geschäftskritisch sind oder sensible Informationen verarbeiten, im Rahmen der Planung mitbetrachtet und die Aufrechterhaltung der Informationssicherheit in widrigen Situationen auch für die IoT-Anwendungen und -Geräte sichergestellt ist.

Diese Maßnahmen sind geeignet, die identifizierten Risiken O1, O2, O3, O5, O8, O9, O12, O13, O17, O19, O20, O21 und O22 zu behandeln.

6.1.2 Beschaffungsprozess und Life Cycle

Es gilt, vorhandene strenge Maßstäbe hinsichtlich der Sicherheitsaspekte von zu beschaffenden Komponenten, welche für normale IKT-Infrastruktur gelten, auch an IoT-Geräte anzulegen. Dabei sind einige Herausforderungen erkennbar. Zum einen müssen die Beschaffungsprozesse hinsichtlich ihrer Anforderungen auf IoT-spezifische Rahmenbedingungen und Merkmale sowie das im Rahmen der Sicherheitspolitik definierte Schutzniveau angepasst werden. Vorhandene Leistungskataloge etc. werden nicht unmittelbar auf IoT-Geräte angewendet werden können. Es gilt auch zu beachten, dass IoT-Geräte aller Erwartung nach wesentlich einen kürzere Life Cycle haben und manche Hersteller sehr intransparent mit den Informationen zur Softwarewartung von IoT-Geräten umgehen. Dementsprechend ist genau zu prüfen, ob zeitliche Anforderungen hinsichtlich der Bereitstellung von sicherheitskritischen Patches überhaupt erfüllt werden können. Dabei gilt derselbe Grundsatz wie für normale Beschaffungsvorgänge: Ausnahmen sollten tunlichst vermieden werden.

Diese Maßnahmen sind geeignet, die identifizierten Risiken O8, O10, O17 und T5 zu behandeln.

6.1.3 Personal

Da im IoT-Umfeld zahlreiche neue Technologien zum Einsatz kommen können (was wiederum zu Schwachstellen führen kann), gibt es im Wesentlichen zwei Handlungsoptionen. Auf der einen Seite sollte, insbesondere wenn im Rahmen von IoT-Projekten ohnehin Personal eingestellt wird, darauf geachtet werden, dass auch und vor allem Personen mit umfassenden Sicherheitskenntnissen in den betroffenen Bereichen (Technologien, Applikationen, Protokolle, …) ausgewählt werden. Werden IoT-Projekte durch bestehende Mitarbeiter und Mitarbeiterinnen umgesetzt, so sind entsprechende Schulungen durchzuführen. Alle Mitarbeiter und Mitarbeiterinnen sollen im

Rahmen von Awareness-Schulungen darüber informiert werden, wie die Unternehmensprozesse im Umgang mit Sicherheitsvorfällen gestaltet sind, damit diese auch eingehalten werden (können).

Diese Maßnahmen sind geeignet, die identifizierten Risiken O4, O6, O8, O20 und T2 zu behandeln.

6.1.4 IoT Device Management/Data Management Systeme

Die Betrachtung von IoT weist gewisse Ähnlichkeiten zur Problematik im Zusammenhang mit BYOD auf. Viele, insbesondere CIoT-Geräte, werden von Usern und Userinnen oder auch Administratoren und Administratorinnen in das Unternehmensnetzwerk eingebracht und stellen damit ein Sicherheitsrisiko dar (Cybersecurity Matters, 2015). Eine fehlende oder unangemessen strenge Sicherheitspolicy im Unternehmen kann – analog zu BYOD – die Entstehung einer „Schatten-IT“ bzw. in diesem Fall eines „Schatten-IoT“ zur Folge haben. Dabei werden an der Policy vorbei mehr oder weniger heimlich trotzdem IoT-Geräte genutzt, was massive Sicherheitslücken zur Folge haben kann (Gold, 2018). Ein frappantes Beispiel dafür, was in so einem Fall passieren kann, lieferte wohl unfreiwilliger Weise die NASA im April 2018[15]. Ein einziger Einplatinencomputer, der vorbei an den Policies im Netz angeschlossen wurde, ermöglichte einen APT-Angriff und führte zu einem Datenverlust von 500MByte aus hochsensiblen Bereichen der Marsmissionen (Cimpanu, 2019).

Zudem stellen „vergessene Devices“ ein Problem dar, also Geräte, bei denen man sich nicht mehr bewusst ist, dass sie noch im Unternehmensnetzwerk sind. Das stellt eine besondere Gefahr da, weil diese damit auch nicht dem üblichen Patch-Managementprozess unterliegen und möglicherweise über die Zeit vermehrt Schwachstellen bekanntwerden, welche für Angriffe ausgenutzt werden können.

Es liegt also der Gedanke nahe, ein System analog zu MDM einzuführen, um die Geräte bzw. das IoT-Inventar aktiv zu verwalten. Dafür können spezielle IoT *Device Management*-Plattformen (IoT-DMP) eingesetzt werden. Diese übernehmen Aufgaben im Bereich automatischer Geräteerkennung, Patchmanagement, Over-the-Air-Provisioning von Updates (siehe auch Abschnitt 6.3.2) sowie der Verwaltung des IoT-Inventars. Dabei ist es unwesentlich, ob dies im Rahmen einer eigenen Plattform oder einer Erweiterung bestehender MDM- oder Netzwerkmanagementsysteme erfolgt.

Ein wesentlicher Vorteil bei spezialisierten Plattformen ergibt sich dabei aus weiteren Fähigkeiten. Diese können beispielsweise auch das Konfigurations- und Datenmanagement übernehmen. Letzteres wird als IoT *Data Management* bezeichnet und beinhaltet weitere Aspekte wie die Normalisierung, Speicherung, Verarbeitung und Analyse entstehender Daten. Es ist somit die gesamte organisatorische Abbildung des Life Cycles von IoT-Geräten, von der Erstinbetriebnahme (Onboarding) im Netzwerk bis hin zur De-Provisionierung möglich. Zudem können Richtlinien für

[15] Intensives Medienecho gab es dazu im Juni 2019 auf Grund der Veröffentlichung eines Prüfberichts.

die Geräte analog zu BYOD definiert und die Einhaltung sichergestellt werden. Entsprechende spezialisierte Softwareprodukte sind bereits am Markt erhältlich (i-SCOOP, 2018).

Diese Maßnahmen sind geeignet, die identifizierten Risiken O10, O11, O12, O13, O14, O16, T5, T6 und T7 zu behandeln.

6.1.5 Schwachstellenmanagement

Da sich gerade im IoT-Bereich in sehr kurzen Abständen viele neue Schwachstellen auftun können, empfiehlt es sich, einschlägige Informationsquellen (z.B. Webseiten oder darauf spezialisierte Dienstleister) in Anspruch zu nehmen (Russel & Van Duren, 2018). Dadurch werden Veränderungen in der Bedrohungslage erkannt und es kann in dem Fall, dass eigene Geräte betroffen sind, möglicherweise noch vor einem Angriff darauf reagiert werden. Voraussetzung für eine sinnvollen Abgleich der bereitgestellten Daten mit der eigenen Infrastruktur ist ein vorhandenes und gepflegtes Inventar der IoT-Geräte und -Applikationen, welches zum Beispiel durch eine IoT-DMP bereitgestellt werden kann. Auf Grund der hohen möglichen Anzahl an Geräten empfiehlt sich eine Automatisierung dieser Abgleiche und die Einführung entsprechender Reaktionsprozesse bei erkannten Übereinstimmungen zwischen neuen Schwachstellen und im Unternehmensnetzwerk befindlichen, verwundbaren Geräten.

Diese Maßnahmen sind geeignet, das identifizierte Risiko O7 zu behandeln.

6.1.6 Umgang mit Datenschutz

Auf Seite des Betreibers einer IoT-Applikation ergeben sich, um Datenschutzprobleme wie in Abschnitt 4.4 geschildert zu vermeiden, beispielsweise folgende Handlungsoptionen:

- Sensoren übermitteln nur anonymisierte/pseudonymisierte Daten
- Aggregation von Daten, so dass keine Rückschlüsse auf einzelne Personen möglich sind

Beides steht aber möglicherweise im Gegensatz zur eigentlichen Intention der IoT-Anwendung, welche für ihre ordnungsgemäße Funktion detailliertere Daten benötigt (Atzori, Iera, & Morabito, 2010). Es muss aber sichergestellt werden, dass die eigenen Applikationen diese Daten weder erheben noch austauschen, sofern keine Einwilligung besteht. Für das Problem der zuvor einzuholenden Einwilligung zur Verarbeitung personenbezogener Daten gibt es derzeit wohl keine alternative oder „bessere“ Lösung als diese tatsächlich nach den normalen Verfahren im Unternehmen einzuholen.

In der Zukunft könnte es in diesem Bereich interessante Entwicklungen geben, die aus dem Bereich der Automobilindustrie bzw. vernetzten Autos stammen und die dabei entstehenden datenschutzrechtlichen Anforderungen durch den Einsatz von speziellen PKIs zu lösen versuchen (Russel & Van Duren, 2018). Damit können evtl. datenschutzrechtliche Probleme bei der Erfassung oder dem Austausch von Daten eliminiert werden, ohne dass sie dazu anonymisiert oder aggregiert werden müssen (nicht ohne Einwilligung rückverfolgbarer Personenbezug).

Für die Sicherstellung der rechtskonformen Löschung von Daten, sofern diese – da sie rechtmäßig verarbeitet werden – vorliegen, kann dies als Aufgabe der Middleware (siehe 6.2.3) implementiert werden. Ansonsten scheint eine dezentrale Löschung von Daten nur schwer realisierbar, da dazu möglicherweise tausende Geräte entsprechend auf das Vorliegen etwaiger Daten überprüft werden müssen.

Als beste mögliche Maßnahme zur Lösung der Datenschutzproblematik erscheint damit zusammengefasst eher „Privacy by Design“ zu sein, also eine von vornherein auf Datenschutz und Datensparsamkeit ausgelegte Implementierung einer IoT-Applikation (Buyya & Dastjerdi, 2016). Weitere Möglichkeiten können sich durch den Einsatz von *Privacy Enhancing Technologies* (PET) ergeben (Traunmüller, 2003). Die Anwendung dieser Technologien im IoT-Umfeld scheint allerdings noch nicht wirklich fortgeschritten und konnte auch nicht weiter in aktuellen Publikationen nachvollzogen werden.

Diese Maßnahmen sind bei entsprechender Umsetzung geeignet, das identifizierte Risiko O23 zu behandeln.

6.1.7 Audits, Pen-Testing

Werden im Unternehmen regelmäßig Audits oder Penetration Tests von IKT-Systemen durchgeführt, so ist eine Ausweitung auf die IoT-Landschaft notwendig. Sollten solche Verfahren nicht etabliert sein, empfiehlt sich zumindest ein regelmäßiges Pen-Testing der eingesetzten IoT-Geräte zur Auffindung von bekannten Schwachstellen, von denen es erwartungsgemäß zahlreiche gibt.

Diese Maßnahmen sind geeignet, das identifizierte Risiko O7 zu behandeln.

6.2 Applikationsbezogene Aspekte

Diffizil gestaltet sich bei IoT die Modellierung applikationsbezogener Aspekte, da hier einige Eigenschaften des IoT voll zum Tragen kommen.

6.2.1 Authentifizierung und Autorisierung

Eines der Hauptprobleme stellt die Bereitstellung von Authentifizierungs- und Autorisierungsmechanismen im IoT-Umfeld dar. Dies tritt insbesondere in jenen Fällen auf, wo (viele) IoT-Geräte direkt untereinander kommunizieren. Dabei muss sichergestellt sein, dass die Geräte auch nachweisen können, dass sie sind, wer sie vorgeben zu sein – eine Herausforderung, wenn IoT-Netze sich regelmäßig und dynamisch in Art und Anzahl der an der Kommunikation beteiligten Geräte ändern.

Ein möglicher Ansatz zur Authentifizierung wäre, bereits eingesetzte Technologien zur (gegenseitigen) Authentifizierung von Geräten im Netzwerk, wie sie in Abschnitt 3.3.3.3 diskutiert wurden, auch für diesen Anwendungsfall einzusetzen.

Gerade beim Einsatz passiver Technologien wie RFID können aber diese üblichen Sicherheitsmechanismen, beispielsweise vom Unternehmen eingesetzte Authentifizierungsinfrastrukturen (Server, Verzeichnisdienste, …) nicht genutzt werden, da eine dafür notwendige Datenübertragung technisch nicht oder nur sehr eingeschränkt möglich ist. Zudem ist es eine Eigenschaft von IoT, dass möglicherweise auch unternehmensfremde IoT-Geräte mit den eigenen Geräten kommunizieren dürfen. Dabei stellt sich die Frage, wie in diesem Fall eine Authentifizierung bzw. Autorisierung möglich sein kann (Atzori, Iera, & Morabito, 2010), da die eigene Vertrauensdomäne verlassen wird – was insbesondere bei Verwendung unternehmensinterner Mechanismen wie einer eigenen PKI problematisch ist.

Die Nutzung von vorhandenen, rechenintensiven Technologien wie asymmetrischen kryptographischen Verfahren, z.B. im Rahmen einer PKI zur Geräteauthentifizierung, ist aber ohnehin auf Grund technischer Limitierungen, insbesondere hinsichtlich des benötigten Rechenaufwands, als mindestens unpraktisch bis unmöglich einzustufen (Eschenauer & Gligor, 2002). Obschon die in diesem Paper durchgeführte Analyse einige Jahre her ist, wird davon ausgegangen, dass sich die grundsätzliche Situation nicht wesentlich geändert hat, da die eingesetzten Verfahren immer noch auf den selben Prinzipien beruhen und mittlerweile durch Weiterentwicklungen noch wesentlich ressourcenintensiver geworden sind (Ali, 2015).

Durch den IoT-Aspekt der Skalierbarkeit und eine gegebenenfalls zu Beginn unklare Topologie des Endausbaus oder den andersartigen Kommunikationsmustern einer IoT-Anwendung (z.B. Mesh-Kommunikation in einem Sensornetzwerk) ergeben sich weitere Probleme. Es wäre ein Vorab-Ausrollen aller entsprechenden Zertifikate notwendig, zudem besitzen diese üblicherweise ein Ablaufdatum, was eine regelmäßige Erneuerung ebendieser auf entfernten Geräten notwendig machen würde. Es ist auch davon auszugehen, dass insbesondere viele IoT-Geräte aus dem Consumer-Bereich sollte Technologien überhaupt nicht oder nur sehr rudimentär unterstützen, da diese oftmals nur um Unternehmensumfeld anzutreffen sind.

Es gibt verschiedene Ansätze, mit diesen Problemen umzugehen:

Eine Möglichkeit ist die Einführung eines eigenen dezentralen Mechanismus zur Verteilung von applikationsspezifischen Vertrauensschlüsseln innerhalb eines IoT-Netzes, wie beispielsweise Eschenauer und Gligor (2002) es skizzieren. Innerhalb dieser Vertrauensdomäne werden Themen wie das dynamische Hinzufügen oder Entfernen von Knoten und die regelmäßige Erneuerung der Vertrauensstellung durch kryptografisch explizit schlank gehaltene Verfahren behandelt. Zudem sind Mechanismen vorgesehen, Knoten bei einer Übernahme oder Manipulation durch einen Angreifer oder eine Angreiferin die Vertrauensstellung zu entziehen, ohne dass das restliche Netzwerk dadurch im gegenseitigen Vertrauen beeinträchtigt wird.

Ein weiterer Ansatz ist der Einsatz von Middleware-Systemen oder IoT-Gateways, welche den Aspekt des Vertrauens zwischen den Geräten durch Bereitstellung einer Vertrauensinfrastruktur (siehe dazu auch 6.2.3) herstellen können. Dabei übernimmt diese Komponente für den entsprechenden Zuständigkeitsbereich die Verwaltung und Verteilung entsprechender Schlüssel. Diese Vorgehensweise ist nicht ganz ohne Nachteile, z.B. hinsichtlich Redundanz oder der Anwendbarkeit auf ad-hoc Netzwerke (Heer, et al., 2011), stellt aber generell eine valide Lösung des Problems dar. Ein solcher Ansatz, basierend auf dem Einsatz für IoT angepasster kryptographischer

Mechanismen, findet sich auch bei Mahalle et al. (2013). Dieser stellt die Basis für die Vertrauensstellung innerhalb einer IoT-Domäne über einen für den jeweiligen Bereich zentralen Schlüsselserver her, wobei auf dieser Basis durch die Geräte weitere Schlüssel für die Authentifizierung der Geräte untereinander abgeleitet werden können.

Eine Zusammenfassung über mögliche Authentifizierungsoptionen bei der Verwendung gängiger IoT-Technologien findet sich bei Chaudhuri (2015). Dabei zeigt sich, dass viele vorhandene Protokolle nur sehr rudimentäre Verfahren wie Username/Passwort, Pre-Shared-Keys oder ressourcenintensive Verfahren wie PKIs unterstützen. Damit dürften sich viele der vorhandenen Protokolle nicht sonderlich für (sichere) Implementierungen eigenen, die tatsächlich dem IoT-Paradigma entsprechen.

Durch Authentifizierungsverfahren kann sichergestellt werden, dass nur authentifizierte Geräte miteinander kommunizieren können. Es bleibt jedoch das Problem der Autorisierung: wie kann, insbesondere dezentral, sichergestellt werden, dass der Zugriff auf bestimmte Daten oder Operationen auch zulässig ist? Hier ist ebenso absehbar, dass in Unternehmen übliche Verfahren wie RBAC nur sehr schwer auf das IoT-Umfeld umlegbar sind. Ursachen dafür sind die enorme Skalierung von IoT mit möglicherweise hunderten oder tausenden verschiedenen Rollen und die erwartete Nicht-Integrierbarkeit von (C)IoT-Geräten in diese Infrastrukturen mangels entsprechender Protokollunterstützung oder Ressourcen. Auch für dieses Problem lassen sich am ehesten Lösungsansätze durch die Implementierung eines Middleware-Systems finden, welches auch die Aufgabe der Prüfung und Autorisierung von Anfragen übernimmt. Dazu muss es entsprechende Informationen (ggf. dezentral) vorhalten.

Ein Ansatz, der dabei implementiert werden kann, ist die Verwendung einer sogenannten *Attribute-Based Access Control* (ABAC). Dabei verlässt man sich bei der Gewährung von Rechten auf gewisse Attribute, welche ein anfragendes Gerät mitbringen muss. Attribute können dabei der Gerätename, Lokation, Hersteller oder auch – zur Absicherung – Passwörter oder auch digitale Zertifikate in der einen oder anderen Form sein. Basierend auf diesen Eigenschaften von Geräten können Zugriffe gewährt oder verweigert werden (Russel & Van Duren, 2018). Ein weiterer Ansatz ist die Verwendung von Capability Based Access Control (CBAC), wie beispielsweise von Mahalle et al. (2013) oder Gusmerolia et al. (2013) vorgeschlagen.

Viele praktische Anwendungsbeispiele und damit einhergehende Problemstellungen lassen sich im RFC7744 finden, welches sich mit Autorisierung in Umgebungen mit beschränkten Ressourcen beschäftigt (wozu IoT-Geräte eindeutig zu zählen sind) und liefert dabei Lösungsansätze, welche jedoch technisch nicht näher beschrieben werden.

Diese Maßnahmen sind geeignet, die identifizierten Risiken O14 und (eingeschränkt) T11 zu behandeln.

6.2.2 Sicherstellung der Vertraulichkeit und Integrität

Um Vertraulichkeit sicherstellen zu können, sind bei IoT-Geräten zwei Aspekte zur berücksichtigen. Zum einen muss bei entsprechend klassifizierten (z.B. personenbezogenen) Daten, die auf einem Gerät gespeichert sind, gewährleistet werden, dass diese z.B. bei Abhandenkommen des

Geräts nicht von unbefugten ausgelesen werden können. Zum anderen muss sichergestellt sein, dass diese bei der Übertragung nicht abgehört werden können.

Verschlüsselung ist und bleibt auch bei IoT-Geräten auf technischer Ebene ein wesentlicher Faktor zur Sicherstellung der Vertraulichkeit. Im Gegensatz zu den Ressourcenproblemen beim Einsatz asymmetrischer Verfahren können jedoch symmetrische Verfahren durchaus eingesetzt werden, da diese wesentlich weniger Rechenleistung benötigen (Eschenauer & Gligor, 2002). Damit kann beiden Problemfeldern mit dem Einsatz symmetrischer Verschlüsselung begegnet werden. Wird der Speicher eines IoT-Geräts verschlüsselt, kann ein Angreifer bzw. eine Angreiferin bei physischem Zugriff darauf keine Daten auslesen. Dafür können spezielle Speicherbereiche auf Geräten eingeführt bzw. genutzt werden (Atzori, Iera, & Morabito, 2010). Wird die Übertragung verschlüsselt, ist auch ein abhören der Kommunikation nicht zielführend, da nicht auf die Inhalte der Kommunikation rückgeschlossen werden kann.

Vorhandene Mechanismen zur Herstellung eines symmetrisch verschlüsselten Kanals bedienen sich jedoch im Regelfall wieder asymmetrischer Verschlüsselung, welche bereits im Vorgehenden Abschnitt als prinzipiell unpassend für IoT-Anwendungen identifiziert wurden. Insbesondere Verfahren wie TLS oder IKEv2/IPSec haben einen sehr hohen Protokolloverhead bei der Herstellung eines sicheren Übertragungskanals, was insbesondere in Mesh-Netzwerken auf Grund notwendiger T2T-Kommunikation zu sehr viel Rechenaufwand führen kann – also in einem Umfeld, wo Rechenleistung extrem begrenzt ist. Ein weiterer, im selben Sinne limitierender Faktor ist die verfügbare Energie. Gerade bei batterie- oder akkubetriebenen IoT-Geräten erscheint es wenig sinnvoll, viel Leistung in den Einsatz ungeeigneter Protokolle zu investieren und damit das Energiebudget zu belasten (Heer, et al., 2011).

Ein für IoT passenderer moderner Ansatz ist die Verwendung einer sog. objektbasierten Sicherheit, welche nur die relevanten Applikationsdaten anstatt des gesamten Übertragungskanals sichert. Dabei verschlüsselt der Sender nur die entsprechenden Applikationsdaten und übermittelt diese dem Empfänger, welcher in der Lage ist, diese zu entschlüsseln und zu verwenden. Ein Nebenaspekt bei Verwendung objektbasierter Sicherheit ist, dass es für das empfangende Gerät keine Rolle spielt, über welchen Kanal bzw. letzten Kommunikationspartner die Information erhalten wurde, was insbesondere in Mesh-Netzwerken vorteilhaft ist. Integrität und Authentizität der Information beruhen eben nicht mehr auf dem zuvor aufgebauten, gesicherten Kanal, sondern dem Objekt selbst (Shang, Yu, Droms, & Zhang, 2016).

Dieser Ansatz lässt sich zudem auch dazu einsetzen, die Integrität der übertragenen Daten durch Verwendung entsprechender vorhandener Mechanismen (z.B. Hash-Funktionen) sicherzustellen. Bekannte oder u.U. optimierte Hash-Funktionen sind auf Grund ihrer überschaubaren Anforderungen an die Rechenleistung als Mittel der Wahl für die Sicherstellung der Integrität im IoT-Umfeld zu sehen (Eschenauer & Gligor, 2002).

Da sich bei all diesem Themen wieder das Problem einer Verteilung der notwendigen Schlüssel stellt, wäre es wohl sinnvoll, auf ein entsprechend passendes, an IoT-Bedürfnisse angepasstes Verfahren zur Schlüsselverteilung, wie in Abschnitt 6.2.1 erwähnt, zu setzen. Dieses muss auch Aspekte hinsichtlich Forward- und Backward-Secrecy (siehe Abschnitt 4.1) berücksichtigen.

Diese Maßnahmen sind geeignet, die identifizierten Risiken O15, T1a, T1b, T4 und T9 zu behandeln.

6.2.3 Einsatz von Middleware

Ein Vorschlag für ein Modell zur Erhöhung der Sicherheit in IoT-Netzen ist die Einführung einer Zwischenschicht in die IoT-Architektur (siehe 2.3). Diese wird in der Folge als IoT Serviceplattform bzw. Middleware bezeichnet und liegt zwischen Netzwerk- und Applikationsschicht.

Die Notwendigkeit einer solchen Erweiterung der Architektur ergibt sich aus verschiedenen Anforderungen. Die Heterogenität der eingesetzten IoT-Geräte ist groß, daher ist es schwierig, gemeinsame Kommunikationsstandards wie Drahtlostechnologien, Netzwerkprotokolle oder Programmschnittstellen sicherzustellen. Zudem erfordern verschiedene IoT-Anwendungen zur Kommunikation untereinander möglicherweise eine Abstraktion bzw. Übersetzung der ausgetauschten Information. Diese Aufgaben sowie insbesondere Aspekte der Sicherheit (insb. Authentifizierung und Autorisierung, s.o.) können durch eine Middleware übernommen werden (Bandyopadhyay, Sengupta, Maiti, & Dutta, 2011). Auch das Anonymisieren oder Löschen von personenbezogenen Daten kann an dieser Stelle erfolgen, wenn die Ressourcen oder technischen Möglichkeiten dazu in einem IoT-Gerät selbst nicht gegeben sind.

IoT-Gateways können als solches Middleware-Element eingesetzt werden. Netzwerkknoten wie Sensoren verbinden sich über diese mit dem Internet, damit fungieren sie genau als Middleware. Das kann technologisch sogar notwendig sein, wenn die Sensoren selbst keine Internetverbindung besitzen. Auf der anderen Seite können allerdings auch Verarbeitungstätigkeiten von den Sensoren an die Gateways ausgelagert werden, wenn diese selbst keine Ressourcen dafür haben (Buyya & Dastjerdi, 2016).

Solche IoT-Gateways können auch implizit nur für dedizierte Sicherheitsaufgaben eingesetzt werden (*IoT Security Gateways).* Diese werden aus Sicherheitsgründen in den Informationsweg eingehängt und vorverarbeiten alle Anfragen, die an einzelne IoT-Geräte gesendet werden. Dabei können Sicherheitsüberprüfungen der übermittelten Befehle und Informationen durchgeführt werden. Moderne Entwicklungen wie Containertechnologien erlauben eine hochskalierbare Bereitstellung vieler solcher Gateways mit wenig Ressourcenverbrauch auch in kleineren Umgebungen (Yu, Sekary, Seshany, Agarwaly, & Xu, 2015). Eine solche Architektur ermöglicht auch die Absicherung von Programmschnittstellen.

Diese Maßnahmen sind geeignet, die identifizierten Risiken O8, O14, T1a, T2 und T3 zu behandeln.

6.2.4 Cloud-Computing

Der Einsatz von IoT führt aus verschiedenen Gründen oftmals zur Nutzung von *Cloud Services*. Dabei überlässt ein Unternehmen einem fremden Anbieter die erhobenen Daten, welcher sie verarbeitet. Es sollte in diesem Zusammenhang sichergestellt sein, dass es sich dabei um einen verlässlichen Provider handelt, der die überlassenen Informationen entsprechend schützt

(Stergiou, Psannis, Kim, & Gupta, 2018) und verfügbar hält. Einer solchen Verarbeitung sollte jedenfalls eine intensive unternehmensseitige Beschäftigung mit Cloud-spezifischen Sicherheitsproblemen vorausgehen. Maßnahmen können entsprechende vertragliche Zusicherung von definierten Verfügbarkeiten mit entsprechenden Pönalen und der Nachweis eines etablierten Informationssicherheitsmanagements sein, z.B. eine Zertifizierung nach ISO 27001 oder BSI Grundschutz (Gies & Steil, 2018).

Wenn Cloud-Computing für die Verarbeitung von Daten unternehmensinterner IoT-Geräte genutzt wird, bieten einige Cloud-Anbieter die Möglichkeit der Nutzung eines Gateways an. Dieses befindet sich im Unternehmensnetz und ist der einzige nach außen hin sichtbare Kommunikationspartner für den Datenaustausch. Damit müssen die einzelnen IoT-Geräte nicht mehr direkt aus dem Internet erreichbar sein und die Prüfung und Steuerung der Kommunikation erfolgt über dieses Gateway (Gies & Steil, 2018). Dies ähnelt einer Architektur, wie sie in Abschnitt 6.2.3 beschrieben wird.

Da es zahlreiche spezifische mögliche Angriffe auf Cloud-Infrastrukturen gibt, siehe beispielsweise Gurkok (2014) oder Rayes und Salam (2017), empfiehlt sich hier – neben der intensiven Beschäftigung mit diesem Thema – die Ausarbeitung spezieller Richtlinien.

Diese Maßnahmen sind geeignet, die identifizierten Risiken O4, O19 und T11 zu behandeln.

6.2.5 Entwicklung von IoT-Applikationen

In vielen Fällen wird es notwendig sein, eine eigene IoT-Anwendung zu erstellen, wenn beispielsweise vorhandene Applikationen, Produkte oder Frameworks gestellte Anforderungen nicht erfüllen.

Im Entwicklungsprozess von IoT-Applikationen muss dann dafür gesorgt werden, dass mögliche Angriffsflächen verhindert werden. Die Auswahl einer passenden Architektur und geeignete sicherheitsbezogene Entwurfsentscheidungen sind frühzeitig im Entwicklungsprozess durchzuführen. Es ist weiters dafür zu sorgen, dass nur solche hard- und softwareseitigen Funktionen entwickelt und eingesetzt werden, die für den Betrieb des Geräts oder der Applikation auch tatsächlich notwendig sind. Diese müssen hinsichtlich der Sicherheit Priorität genießen. Der Grundsatz hierbei: Was nicht existiert, kann auch nicht angegriffen werden (und somit auch nicht als Ziel für DoS-Attacken genutzt werden). Ebenso muss auf die sichere Implementierung von Schnittstellen geachtet werden, da nicht davon ausgegangen werden kann, dass keine Angriffe in Form manipulierter Anfragen ausgeführt werden (Erlijn & Schreiber, 2017).

Als Knackpunkte bei der Umsetzung dieser Vorschläge können sich IoT-spezifische Rahmenbedingungen erweisen. So sind etwa Ressourcenlimitierungen auf den IoT-Plattformen oder die Anforderungen hinsichtlich der Time-to-Market sicherlich Hindernisse für eine sichere Softwareentwicklung.

Diese Maßnahmen sind geeignet, die identifizierten Risiken O8, O18, T2 und (eingeschränkt) T13 zu behandeln.

6.3 Technische Aspekte

Auf technischer Seite lassen sich die nachfolgenden Sicherheitsmaßnahmen für das Modell identifizieren.

6.3.1 Absicherung der Geräte

Ein großes Sicherheitsrisiko im IoT-Umfeld stellt der Umstand dar, dass IoT-Geräte die meiste Zeit unbeaufsichtigt (teilweise im öffentlichen oder frei zugänglichen Raum) sind. Damit ist es einfach, sie physisch unter Kontrolle zu bringen (Atzori, Iera, & Morabito, 2010).

Die Zunehmende Komplexität von IoT-Geräten macht die Absicherung der Geräte selbst aufwändiger. In vielen Fällen kommt in den Geräten eine Reihe von verschiedenen v.a. Softwareprodukten zum Einsatz, dazu zählen Betriebssystem, Laufzeitumgebungen, Drittanbietersoftware oder eigenentwickelte Programme. Zuallererst sollte die Bedienungsanleitung des Herstellers konsultiert werden, welche Anweisungen zur sicheren Konfiguration geben kann. Sollte eine solche nicht vorhanden sein, empfiehlt sich eine Recherche zu Best Practices zur Konfiguration ähnlicher Geräte. Auf jeden Fall sollten Softwarekomponenten und Benutzerzugänge deaktiviert werden, welche nicht benötigt werden. Für verwendete IoT-Protokolle sollte ebenso eine Recherche zur sicheren Konfiguration erfolgen, da die Standardeinstellungen unter Umständen (wie bei ZigBee) fatal unsicher sind (Russel & Van Duren, 2018). Das erscheint insbesondere relevant, da es sich um Protokolle handeln wird, die im normalen Unternehmensnetzwerk nicht eingesetzt werden und daher keine Erfahrung damit vorhanden sein wird. Anleitung dazu findet man beispielsweise in einschlägigen Dokumenten der NIST.

Ein weiterer wichtiger Punkt sind Passwörter, welche oftmals zumindest für den administrativen Zugang benötigt werden[16]. Am wichtigsten ist es, Standardpasswörter sofort zu ändern. Idealerweise verwendet man pro Gerät ein eigenes Passwort – das erfordert allerdings in Anbetracht der möglicherweise hohen Anzahl an Geräten eine eigene Softwarelösung zur automatisierten Passwortverwaltung. Ist eine solche im Einsatz, kann auch eine regelmäßige Änderung dieser Passwörter wesentlich leichter erfolgen. Dies sollte im Einklang mit den Vorgaben für Passwörter gemäß der Informationssicherheitsrichtlinie erfolgen (Russel & Van Duren, 2018).

Weitere Angriffspunkte können aktivierte (physische) Interfaces sein, welche üblicherweise nur für Tests und Fehlersuche vorgesehen sind, diese sollten im Produktivbetrieb deaktiviert werden. Möglicherweise sehen die Geräte auch Mechanismen vor, welche aktiv Manipulationsversuche an Hard- oder Software erkennen können und darauf beispielsweise durch das Löschen sensibler Daten reagieren. Die Nutzung solcher Mechanismen wird empfohlen (Russel & Van Duren, 2018).

[16] Bei Fehlen alternativer Authentifizierungs- und Autorisierungsmechanismen kommen für die genutzten Dienste ebenso Passwörter vor, diese sind gleich zu behandeln.

Eine große Herausforderung bei tausenden von Geräten stellt überhaupt die Erkennung eines erfolgreichen Angriffs dar, wenn zum Beispiel ein Gerät von einem Angreifer oder einer Angreiferin bisher unbemerkt übernommen wurde. Dabei können moderne Analytics-Ansätze, wie in Abschnitt 6.3.8 diskutiert, angewendet werden.

Diese Maßnahmen sind geeignet, die identifizierten Risiken O12, O13, O14, T7, T8 und T10 zu behandeln.

6.3.2 Sicheres Einspielen von Updates

Es wurde bereits festgestellt, dass es zwingend notwendig ist, IoT-Geräte regelmäßig im Rahmen des Life Cycle Managements mit Updates der darauf laufenden Software zu versorgen. Dabei stellen sich jedoch auf technischer Ebene einige Herausforderungen.

Um Updates überhaupt einspielen zu können, müssen Geräte entsprechende Schnittstellen zur Einbringung und Aktivierung von aktualisierter Software oder Firmware, d.h. hardwarenaher Software, bereitstellen. Bei bestehenden IKT-Systemen erfordert dies oftmals einen physischen Zugang zum Gerät – dies erscheint aber bei IoT auf Grund der großen Anzahl und der physischen Verteilung als eher unpraktischer Ansatz. Mittels Over-the-Air(OTA)-Provisionierung über entsprechende Schnittstellen sind Aktualisierungen aus der Ferne über die bei IoT per Definition vorhandene Netzwerkanbindung möglich. Diese Verteilung kann bzw. sollte dabei automatisiert und im Rahmen eines definierten Prozesses erfolgen, der sowohl Funktionstests vor der Ausrollung als auch Mechanismen zur Fehlerbehandlung (Wiederherstellung eines funktionalen Betriebszustands bei fehlgeschlagenen Updates) einschließt. Ein großes Problem dabei ist, dass viele Geräte Integrität und Authentizität einzuspielender Updates nur mangelhaft oder gar nicht überprüfen. Das bedeutet, dass es für einen Angreifer oder eine Angreiferin möglich ist, den Update-Prozess selbst anzugreifen, manipulierte Updates einzuspielen und damit z.B. Kontrolle über Geräte zu erlangen oder diese zu zerstören. Gerade die Ressourcenlimitierungen von IoT-Geräten hinsichtlich Rechenleistung und Speicherplatz stellen hier ein Problem dar, weil übliche Mechanismen wieder auf rechenintensive kryptographische Verfahren und gesicherte Transportwege zurückgreifen. Das heißt, der Download- und Verifikationsprozess von Firmwareupdates muss an diese Erfordernisse speziell angepasst werden. Ein Beispiel für ein Software-Framework, im Rahmen dessen ein solcher sicherer Prozess abgebildet werden kann, ist das ESPer-Projekt. Dieses zeigt am Beispiel des in IoT-Geräten populären ESP8266-Mikroprozessors auf, wie ein solcher Updateprozess gestaltet werden kann (Frisch, Reißmann, Pape, & Rieger, 2018).

Diese Maßnahmen ist geeignet, die durch die Analyse der OWASP Top10 entdeckte Schwachstelle „Fehlen eines sicheren Updatemechanismus“ und das daraus entstehende Risiko (siehe Abschnitt 5.4) zu behandeln.

6.3.3 Absicherung des Netzwerks

802.1X-basierte Mechanismen zur Beschränkung des Zugangs zu Netzwerken sind auch für IoT-Geräte anwendbar, sofern diese allerdings das Protokoll unterstützen (Russel & Van Duren, 2018). Davon ist insbesondere im CIoT-Bereich nicht unbedingt auszugehen.

Moderne Netzwerkkonzepte (siehe auch Abschnitt 6.3.7) sollen durch den Einsatz von Virtualisierungstechnologien die Erkennung von neu angeschlossenen Geräten und die entsprechende Kategorisierung und Einordnung in eine entsprechende Umgebung vollautomatisch vornehmen. Damit ist sichergestellt, dass einerseits unautorisierten Geräten der Zugang zum Netzwerk verwehrt wird bzw. diese nur eingeschränkte Konnektivität haben. Andererseits sollen legitime Geräte automatisch mit den entsprechenden Zugriffsrechten versehen werden, damit diese Zugang zu den zugehörigen anderen (IoT-)Geräten in der selben virtuellen Umgebung besitzen. Dies entspricht einem vollautomatischen sog. *Onboarding*-Prozess (ALE International, 2018).

Diese Maßnahmen sind geeignet, das identifizierte Risiko T11 zu behandeln.

6.3.4 Absicherung von Drahtlostechnologien

Eine immanente Eigenschaft von IoT ist die Nutzung von drahtloser Übertragung. Damit sind Datenübertragungen einfach abzuhören. Zudem können in drahtlosen Umgebungen durch Angreifer bzw. Angreiferinnen sehr leicht Attacken auf die Verfügbarkeit durch Jamming oder Vampirangriffe erfolgen.

Gegen das Mitlauschen durch einen Angreifer oder eine Angreiferin bieten sich zwei Maßnahmen an. Alle drahtlosen Sendeanlagen sollten mit der minimal benötigten Sendeleistung betrieben werden, um die Reichweite der Funksignale zu minimieren und so eine physische Barriere aufzubauen. Zudem empfiehlt sich der Einsatz von Drahtlostechnologien, welche von Haus aus verschlüsselte Übertragung unterstützen. Ansonsten muss die übertragene Information anderweitig geschützt werden (siehe Abschnitt 6.2.2).

Gegenüber der aktiven Störung von drahtlosen Verbindungen gibt es einige Verfahren, die einen solchen Angriff erschweren. Dazu zählen beispielsweise, um Jamming zu verhindern, das laufende Wechseln der genutzten Funkfrequenz, Spektrumsspreizung, gerichtete Antennen und geeignete Erkennungsmechanismen. Um *Vampire Attacks* und somit einem DoS entgegenzuwirken, können Mechanismen wie die Beschränkung der Anzahl an erlaubten Anfragen, Sequenznummern und verschlüsselte Kontrollpakete zum Einsatz kommen (Rayes & Salam, 2017). Letztendlich eingesetzte Protokolle sollten entsprechende Mechanismen beinhalten.

Im drahtlosen Bereich gibt es Produkte, welche einen großen Frequenzbereich überwachen und bei erkannten Anomalien (wie beispielsweise neu eingebrachte, unbekannte Geräte) alarmieren können. Solche Szenarien werden von normalen Monitoring-Tools nicht abgedeckt und können sowohl die Verbindungsqualität erhöhen als auch die Erkennung von Angriffen ermöglichen.

Diese Maßnahmen sind geeignet, die identifizierten Risiken O8, T1b, T4, T9 und T13 zu behandeln.

6.3.5 Herstellung von Redundanzen

Zur Vermeidung von Ausfällen, also einer Verletzung der Verfügbarkeit einer IoT-Anwendung, können auch im IoT-Bereich Redundanzen eingesetzt werden. Dabei ist es unwesentlich, ob ein Ausfall durch einen Angriff oder beispielsweise einen Hardwaredefekt verursacht wurde. Von letzterem ist bei der Verwendung von Tausenden oder Millionen von Geräten durchaus regelmäßig auszugehen.

Es zeigt sich dabei, dass zentral (z.B. durch Middleware) gesteuerte IoT-Anwendungen besser auf Ausfälle reagieren können, da die Middleware über viele Informationen betreffend den Aufbau und Verteilung der IoT-Geräte verfügt (Roman, Zhou, & Lopez, 2013). So kann eine Middleware beispielsweise einen Datenverlust durch einen ausgefallenen Sensor durch Daten eines anderen für diesen als Ersatz vorgesehenen, in der Nähe befindlichen Sensor kompensieren, dessen Existenz und Lokation die Middleware kennt.

Diese Maßnahme ist geeignet, das identifizierte Risiko O22 zu behandeln.

6.3.6 Segmentierung und Kommunikationseinschränkung

Ein Ansatz, der bei der Implementierung von IoT-Anwendungen im Unternehmensnetzwerk eingesetzt werden kann, ist die Einführung einer sogenannten Zero-Trust-Policy (ZTP). Das entspricht dem Gegenteil von herkömmlichen Herangehensweisen im Unternehmen, bei denen oftmals den im Netzwerk befindlichen Geräten vertraut wird, bis etwas Gegenteiliges festgestellt wird. Im Fall einer ZTP wird grundsätzlich kein Vertrauen vorgeschossen, sondern von Beginn an ein strenges Regelwerk hinsichtlich der Kommunikationsmöglichkeiten an ein Gerät angelegt. Ein Ansatz dabei ist eine rigorose Segmentierung des Netzwerkes durch verschiedene Mechanismen wie virtuelle Netzwerke (Valerio, 2018), jedenfalls aber eine Trennung der IoT-Geräte von der traditionellen IT-Infrastruktur wie Clients oder Servern.

Ein weiterer Schwerpunkt liegt auf einer sichergestellten Identifizierung der Geräte durch zumeist mehrere Verfahren. Der Vorteil einer ZTP ist, dass es bei der konsequenten Implementierung dieser Maßnahme keine Rolle mehr spielt, ob sich ein Gerät innerhalb oder außerhalb des Unternehmensnetzwerks (z.B. im Internet) befindet, da die Vertrauensstellung in beiden Fällen erst hergestellt werden muss. Das scheint ein brauchbarer Ansatz für echte IoT-Anwendungen zu sein, bei denen genau solche Szenarien berücksichtigt werden müssen. Die Einführung einer solchen Policy kann sich sehr mühsam gestalten, doch haben Erfahrungswerte gezeigt, dass Unternehmen danach wesentlich schneller auf Angriffe und Unregelmäßigkeiten reagieren können als mittels traditioneller Architekturen (Di Salvo, 2018).

Eine ZTP kann dabei, das sei angemerkt, nicht nur im IoT-Kontext eingesetzt werden, sondern stellt möglicherweise einen grundlegend besseren Ansatz zur Erhöhung von Netzwerksicherheit dar (Pratt, 2018).

Diese Maßnahmen sind geeignet, die identifizierten Risiken O8, T3 und T11 zu behandeln.

6.3.7 Software Defined Networks

Traditionelle Netzwerkarchitekturen, wie sie heute in Unternehmen üblich sind, unterliegen einigen Beschränkungen. Üblicherweise werden geschlossene (proprietäre) Plattformen für die Bereitstellung der essentiellen Transport- und Sicherheitsmechanismen eingesetzt (Switches, Router, Firewalls, IPS…). Diese werden individuell administriert und liefern einzeln keinen Überblick über die gesamte Struktur oder den detaillierten Datenverkehr in einem Netzwerk. Software Defined Networks (SDN), ein Ansatz, der seit etwa 2007 diskutiert wird, bricht mit einigen dieser Grundlagen. Ziel ist es, ein über Schnittstellen programmierbares Netzwerk zu errichten, in welchem der Datenverkehrsfluss sowie die Bereitstellung von Ressourcen individuell und aktiv an jeder Stelle im Netzwerk durch einen entsprechenden zentralen Controller beeinflusst werden kann (Caraguay, Peral, López, & Villalba, 2014). Damit ist in diesem Kontext die Realisierung einer Mikrosegmentierung, d.h. die aktive Reglementierung jedes Datenverkehrsflusses zwischen jedem einzelnen IoT-Gerät möglich.

In IoT-Umgebungen ergeben sich mittels dieser Technologie interessante weitere Anwendungsbereiche wie (optimierte) Wegefindung und Protokollübersetzung (Jararweh, et al., 2015), aber auch hinsichtlich der Sicherheit. So kann der Datenfluss von IoT-Geräten dezentral im Netzwerk überwacht und beeinflusst werden. Basierend auf entsprechend konfigurierten Sicherheitsparametern im Controller kann jede Verbindung eines IoT-Geräts überprüft und zugelassen oder verweigert, Anomalien erkannt und auf diese reagiert werden (Caraguay, Peral, López, & Villalba, 2014).

Eine Erweiterung für Anwendungen auch außerhalb des Unternehmensnetzes ist die Ausrollung von SDN-Mechanismen in dezentrale Bereiche durch Bildung von SDN-Domänen. Zwar könne n IoT-Geräte auf Grund ihrer begrenzten Ressourcen nicht selbst Teil des SDN werden, doch gibt es im Regelfall einen Nachbarknoten oder Middleware-Knoten, z.B. ein IoT-Gateway, das dazu in der Lage ist. So können SDN-Controller im Unternehmensnetz auch die Analyse und Steuerung dezentralen IoT-Datenverkehrs übernehmen (Flauzac, Gonzalez, & Nolot, 2015). Dies ist im Idealfall auch in drahtlosen Umgebungen möglich. Daneben ermöglicht es dieser Ansatz, durch intelligentes Routen von Datenverkehr auch die Verfügbarkeit von IoT-Anwendungen zu erhöhen (Sood, Yu, & Xiang, 2016).

Diese Maßnahmen sind geeignet, die identifizierten Risiken O8, T3 und T11 zu behandeln.

6.3.8 Fortgeschrittene Analytics-Ansätze

Maschinelles Lernen und moderne Analytics-Ansätze, angewandt auf vorliegende Log- und Verkehrsdaten (letztere beispielsweise aus dem SDN generiert), bieten im IoT-Umfeld die Möglichkeit, mit der stetig zunehmenden Diversität an Geräten und damit einhergehenden unterschiedlichen Angriffsszenarien umzugehen. Zudem werden durch die T2T-Kommunikation neue Kommunikationsmuster geschaffen, in welchen Anomalien auf andere Art und Weise auftreten können (Yu, Sekary, Seshany, Agarwaly, & Xu, 2015).

Als Weiterentwicklung von klassischen SIEM-Systemen ist in diesem Bereich die sogenannte „kognitive Sicherheit“ zu sehen, die seit etwa 2016 ein vieldiskutiertes Thema ist. Dabei werden zur Erkennung von informationssicherheitsrelevanten Vorfällen Ansätze von Big Data und maschinellem Lernen angewandt. Das bedeutet, dass Häufungen und Muster in vorliegenden Datenansammlungen (wie z.B. Logdaten) erkannt, diverse weitere Materialien wie Forschungsarbeiten und Blogbeiträge in den Datenbestand aufgenommen und durch moderne Verfahren die durch Menschen erstellten Sicherheitsvorkehrungen dynamisch erweitert werden können. Dies ist ein notwendiger Ansatz, da durch Informationssicherheitspersonal die schiere Menge an verfügbaren aktuellen sicherheitsrelevanten Informationen schlichtweg nicht mehr bearbeitet werden kann. Dass ein solches System keine fiktive Zukunftsmusik ist, zeigt beispielsweise IBM mit der Weiterentwicklung seines KI-Programms Watson hin zu einem „*Watson for Cybersecurity*“, welches die Zahl der Informationen, die für Entscheidungen im Bereich der aktiven Bedrohungsabwehr verwendet werden können, signifikant erhöht (Andrecht, et al., 2017). Dabei kann auch automatisiert auf erkannte Sicherheitsvorfälle reagiert und der entsprechende Unternehmensprozess zumindest angestoßen werden.

Zu beachten ist in diesem Zusammenhang allerdings, dass eine überbordende Sammlung und Auswertung von IoT-Daten datenschutzrechtlich bedenklich werden kann, da es die Privatsphäre von Nutzern (insbesondere durch mögliches Profiling) verletzen kann (Hossain, Fotouhi, & Hasan, 2015). Es muss eine ausgewogene Balance zwischen für die Sicherheit relevanten Informationen und möglicherweise unnötigen Informationen gefunden werden. Ein eingesetztes System sollte jedenfalls die Möglichkeit bieten, bei Bedarf personenbezogene Daten entweder direkt bei der Erfassung/Speicherung oder zumindest nach Ablauf von Fristen zu anonymisieren oder zu löschen.

Diese Maßnahmen sind geeignet, die identifizierten Risiken O20 und T12 zu behandeln. Allerdings stehen sie möglicherweise in Konflikt mit O23.

6.4 Zusammenfassung

Es zeigt sich beim Versuch der Erstellung dieses Modells, dass es für viele relevante Bereiche der IoT-Sicherheit keine eindeutigen Antworten auf Sicherheitsrisiken in Form von konkreten Maßnahmen gibt. In der Literatur und insbesondere in Forschungspublikationen der letzten fünf bis zehn Jahre finden sich zwar viele – teilweise sehr abstrakte – Ansätze, doch kaum Industriestandards oder Beispiele für erfolgreiche Implementierungen solcher Vorschläge in Unternehmensnetzwerken. Vieles, insbesondere auf Applikationsebene, scheint auch nur realisierbar, wenn man als Unternehmen eine IoT-Lösung selbst entwickelt und dabei diese Vorschläge aufgreift und, wo möglich unter Zuhilfenahme existierender Plattformen, implementiert. Gerade in CIoT-Produkten dürften kaum manche dieser teils ausgefeilten und komplexen Maßnahmen implementiert sein. Die Anreize dazu dürften mangels Interoperabilität auf Grund fehlender Standards nicht unbedingt groß sein.

Dennoch sollte das Ziel sein, die identifizierten Themenfelder bei einer IoT-Anwendung zu beachten und alle möglichen Maßnahmen vorzusehen, um einem Idealzustand (d.h. Beachtung der

erwähnten Punkte) so nahe wie möglich zu kommen. Dieses Modell ist jedoch keinesfalls als in allen Anwendungsbereichen vollständig zu betrachten. Das breite Anwendungsgebiet von IoT macht es in jedem Fall notwendig, dieses Konzept um weitere spezifische Aspekte zu erweitern.

Weitere zu behandelnde Felder auf den unterschiedlichen Ebenen der IoT-Architektur finden sich beispielsweise bei Jing et al. (2014), wobei dort ausschließliche technische und applikationsbezogene, aber keine organisatorischen Schwachstellen und Risiken behandelt werden. Diese decken dafür verschiedene technische IoT-Themengebiete (RFID, WSN, ad-hoc-Netze, …) ab.

Was sich aus der Zusammenstellung der durch die jeweiligen Maßnahmen behandelten Risiken erschließen lässt, ist die zuvor erwähnte Verzahnung. So können organisatorische Maßnahmen durchaus positiven Einfluss auf technische Risiken haben und umgekehrt. Damit zeigt sich, dass aus dem Zusammenspiel verschiedenster Maßnahmen ein wirksames Sicherheitskonzept aufgebaut werden kann.

7 VERGLEICH UND HANDLUNGSEMPFEHLUNGEN

In diesem Kapitel erfolgt ein Vergleich zwischen den in Kapitel 3 beschriebenen Sicherheitsmaßnahmen in Unternehmensnetzwerken und den im vorhergehenden Kapitel zusammengetragenen Maßnahmen für ein verbessertes Konzept. Dabei wird betrachtet, welche Aspekte durch Anwendung und Weiterentwicklung bestehender Konzepte abgedeckt werden können und welche Bereiche neuartige Herangehensweisen erfordern, da in bisherigen Sicherheitskonzepten keine ähnlichen Maßnahmen vorhanden bzw. entsprechend adaptierbar sind. Dabei werden auch entsprechende Handlungsempfehlungen abgegeben, welche auf der umfangreichen Betrachtung der Materie in den vorigen Kapiteln sowie der dazu durchgeführten Literaturrecherche beruhen.

Eine bisherige Erkenntnis ist, dass viele Maßnahmen der bestehenden Sicherheitskonzepte auf zentralen, steuernden Komponenten in der Infrastruktur fußen. Solche Ansätze können theoretisch auch in die IoT-Welt übertragen werden und führen dort zur relativ einfachen Lösung von Problemstellungen, doch widerspricht das zu einem gewissen Grad dem IoT-Gedanken an sich: Dinge sollen auch ad-hoc untereinander Informationen zur Erreichung eines gemeinsamen Ziels austauschen können. Probleme kommen dabei insbesondere in den Bereichen Authentifizierung, Autorisierung und Datenschutz zum Tragen.

Ein anderer großer Unterschied manifestiert sich in vielen der zuvor aufgezeigten Maßnahmen: die limitierten Ressourcen und andere Rahmenbedingungen von IoT verhindern den Einsatz bekannter und verbreiteter Technologien in vielen Fällen. Notwendig sind spezielle, „leichtgewichtige“ Ansätze, die den technischen Möglichkeiten der Geräte angepasst sind (Jing, Vasilakos, Wan, Lu, & Q, 2014). Dadurch sind Abweichungen von in Unternehmen eingesetzten Standards möglich bzw. nötig – die Hauptgefahr dabei ist, den Aspekt der Sicherheit mangels Integrationsfähigkeit in die bestehende Infrastruktur zu vernachlässigen und damit eine Lösung zu implementieren, die nicht dem im Unternehmen angestrebten Informationssicherheitsschutzniveau entspricht.

7.1 Anwendung und Weiterentwicklung bestehender Konzepte

Einige der vorgeschlagenen Maßnahmen lassen sich durch die Weiterentwicklung bestehender Sicherheitsmaßnahmen beschreiben und werden nachfolgend diskutiert.

7.1.1 Organisatorische Aspekte

Ein im Unternehmen eingeführtes Informationssicherheitsmanagement kann als solide Ausgangsbasis für den Einsatz von IoT gesehen werden. Jedoch muss eine Anpassung an den geplanten Einsatz von IoT-Technologien auf mehreren Ebenen erfolgen. Die dabei erforderlichen Schritte wurden bereits in Abschnitt 6.1.1 skizziert. Wird in einem Unternehmen kein solches Management betrieben, sollte spätestens beim Einsatz von IoT eine zumindest teilweise Einführung überlegt werden, da sich durch neue und teilweise unbekannte Technologien neben der Unzahl

an damit möglichen Schwachstellen auch die Komplexität des Unternehmensnetzwerkes erhöht. Ein systematischer Zugang zur Informationssicherheit spielt dann eine noch größere Rolle. Gängige ISMS-Standards wie die ISO 27000-Reihe oder der BSI Grundschutz stellen dafür eine auch auf IoT-Anwendungen ausweitbare, empfehlenswerte Grundlage dar. Die durchgeführte Schwachstellen- und Risikoanalyse konnte stark davon profitieren, dass insbesondere viele organisatorische Aspekte identifiziert und entsprechende Maßnahmen vorgeschlagen werden konnten.

Die bei IoT-Geräten erwarteten kürzeren Life Cycles der Geräte spielen im Beschaffungsprozess eine wesentliche Rolle. Dabei stellen sich einige Herausforderungen, welche aber durch die konsequente Weiterführung und Erweiterung bestehender Beschaffungsprozesse hinsichtlich der Sicherheitsanforderungen handhabbar erscheinen. Demnach müssen die Beschaffungskriterien nur entsprechend der vorgegebenen IoT-Sicherheitskonzepte und der Besonderheiten in diesem Bereich angepasst werden.

Auch bei der Auswahl und Weiterbildung von Personal kommen im Prinzip bei beiden Modellen die gleichen Maßnahmen zur Anwendung. Hier muss als Erweiterung ein Fokus auf Informationssicherheitsaspekte des IoT bereits im Auswahlprozess sowie bei Fortbildungsmaßnahmen gelegt werden. Eine große Herausforderung stellt dabei die Vielzahl vorhandener, unterschiedlicher IoT-Technologien dar, welche nicht alle durch Wissen der eigenen Mitarbeiter und Mitarbeiterinnen abgedeckt werden können – daher sollten etwaige Maßnahmen gezielt auf jene Technologien abgestellt werden, die auch tatsächlich im Einsatz oder dafür vorgesehen sind.

Eine größere Veränderung stellt der Einsatz von IoT-DM-Plattformen dar. In Grundzügen kann dies zwar als Fortführung des MDM-Gedankens gesehen werden, durch die potenziell wesentlich größere Anzahl an IoT-Geräten in inhomogenen Landschaften werden sich im Betrieb einige Rahmenbedingungen ändern. Trotzdem sind solche IOT-DMP nicht als neuartige Technologien zu sehen, sondern eher als fortgeschrittene Evolution des MDM. Wird ein solches noch nicht eingesetzt, lohnt eventuell ein Blick auf Systeme, die beide Welten (BYOD und IoT) zusammen verwalten können. In ein solches System kann im IoT-Bereich auch das notwendige Configuration Management sowie Maßnahmen des Patchmanagements inkludiert werden. Ob im Unternehmen bestehende Change-Management-Prozesse einer IoT-Skalierung auf zehntausende IoT-Geräte mit oftmaligen Änderungen standhalten, scheint zumindest zweifelhaft. Insofern ist hier eine Adaption aller Erwartung nach notwendig.

Aktives Schwachstellenmanagement sollte im IoT-Bereich nach Möglichkeit automatisiert erfolgen, folgt aber ansonsten dem gleichen Prinzip wie in normalen Netzwerken. Idealerweise kann dafür ebenfalls eine Integration in die IoT-DMP erfolgen.

Audits und Pen-Testing sind etablierte Maßnahmen und werden in beiden Modellen vorgeschlagen. Wie Stöwer und Kraft (2017) bemerken, liegt der Fokus üblicher Audits aber oftmals auf der Office-IT. Deswegen sind sicherlich bei der Ausweitung auf die IoT-Landschaft die speziellen Rahmenbedingungen zu berücksichtigen und Audits und Pen-Testing entsprechend anzupassen.

7.1.2 Applikationsbezogene Aspekte

Auf dieser Ebene lassen sich nur in wenigen Anwendungsfällen bestehende Konzepte weiterverwenden. Insbesondere im Umfeld von Authentifizierung und Autorisierung können diese nur eingesetzt werden, wenn eine zentralistische IoT-Architektur geplant ist und die eingesetzten IoT-Geräte so leistungsstark sind (z.B. gut ausgestattete Einplatinenrechner), dass die Verwendung etablierter Infrastrukturen wie zentraler Authentifizierungsserver, PKIs und/oder VPNs möglich ist. In allen anderen Fällen sind neuartige Konzepte notwendig.

Middleware-Konzepte sind grundsätzlich in Unternehmen verbreitet, verfolgen aber in der Regel nicht oder nicht hauptsächlich dezentrale Sicherheitsziele. Daher wird diese Maßnahme als neuartig eingestuft und ebendort behandelt.

Der Einsatz von Cloud-Computing gehört in vielen Unternehmen schon zum Alltag[17]. Insofern können bestehende Sicherheitsmaßnahmen, die sich oftmals in Richtlinien zur Verwendung, Vertragsgestaltung oder der intensiven Beschäftigung mit Informationssicherheit bei Cloud-Services manifestieren, ebenso für IoT-Anwendungen eingesetzt werden. Für jene Unternehmen, die solche Dienste noch nicht nutzen, bringt ggf. der Einsatz von IoT den ersten Schritt in die Cloud mit sich. In diesem Fall muss sich ein Unternehmen entsprechend damit beschäftigen (z.B. durch Studie der ISO/IEC 27017), Cloud-Services fallen aber heutzutage keinesfalls mehr in die Kategorie neuartiger Konzepte.

Sollen beim Einsatz von IoT Eigenentwicklungen von Software stattfinden, so muss man sich dabei auf die speziellen IoT-Rahmenbedingungen einstellen. Wird ohnehin Software in einem Unternehmen entwickelt, sollte Sicherheit dabei bereits eine große Rolle spielen, die in Abschnitt 6.2.5 genannten Maßnahmen können dabei ergänzend eingesetzt werden. Von Entwicklungstätigkeiten, insbesondere im IoT-Umfeld, sollte dann ganz abgesehen werden, wenn keine umfassende Erfahrung mit (sicherer) Softwareentwicklung vorliegt. Dies führt schon bei genug etablierten, fachfremden Herstellern von IoT-Geräten und -Anwendungen zu massiven Sicherheitslücken (siehe Abschnitt 4.2), so dass man sich als Unternehmen nicht auch noch in diese unrühmliche Liste einreihen sollte. Hier empfiehlt sich die Auftragsvergabe an erfahrene Dritte.

7.1.3 Technische Aspekte

Bei im Unternehmen bereits eingesetzten Geräten wie Client-PCs und Servern erfolgt in der Regel eine Sicherheitskonfiguration nach Best-Practice-Anweisungen. Dieses Konzept ist auf IoT-Geräte ebenso anzuwenden. Das Problem dabei ist, dass dies durch die mögliche Inhomogenität und Vielzahl an Geräten einen erhöhten Aufwand darstellt und für die spezifischen Produkte möglicherweise passende Anleitungen fehlen. Dennoch muss eine Absicherung erfolgen, da ansons-

[17] wenngleich der Prozentsatz der Nutzung in Österreich mit nicht einmal 25% der Unternehmen auch im EU-Vergleich (noch) relativ niedrig ist (eurostat, 2019)

ten gravierende Verwundbarkeiten vorhanden sind. Die in 6.3.1 geschilderten Maßnahmen sollten auf jeden Fall umgesetzt werden, dabei kann eine IoT-DMP beispielsweise zur Verwaltung individueller Passwörter eingesetzt werden.

Ein Netzwerkzugangsschutz ist dringend anzuraten, ob vorhandene Technologien wie 802.1X dabei eingesetzt werden können, hängt jedoch stark von den eingesetzten Geräten ab. Bei Implementierungen von WSNs oder mit anderen stark ressourcenlimitierten IoT-Geräten ist davon auszugehen, dass neuartige Konzepte angewendet werden müssen.

Eine Segmentierung des Netzes, wie sie in vielen Unternehmensnetzwerken üblich ist (Trennung Clients/Server, …), ist im IoT-Kontext als absolute sicherheitstechnische Untergrenze zu sehen. Bestehen im Unternehmensnetzwerk keine granularen Möglichkeiten, sollte also zumindest eine Trennung des IoT-Netzes vom restlichen Netz mit definierten Regeln am Übergangspunkt (z.B. Firewall) erfolgen. Von einer direkten Integration von IoT-Geräten in die Office-IT ist jedenfalls abzuraten.

7.2 Neuartige Konzepte

Traditionelle Sicherheitsmechanismen stellen stark auf die Kommunikation zwischen Menschen und Maschinen ab, d.h. durch Benutzer getriggerten Informationsaustausch. Hingegen ist die IoT-Kommunikation gerätezentriert, was sich beispielsweise in der geschilderten Problematik der Authentifizierung und Autorisierung wiederspiegelt. Ein IoT-Gerät ist schwierig einer Person und deren Rollen und Rechten zuzuordnen – dieses Schema stellt allerdings den Kernpunkt vieler vorhandener Maßnahmen in Unternehmen dar. Damit stellt dieses Themengebiet die größte Herausforderung beim Einsatz von IoT dar. Im Folgenden werden einzelne vorgeschlagene Maßnahmen diskutiert, welche nur durch neuartige Sicherheitskonzepte und -Maßnahmen in Unternehmen realisierbar sind.

7.2.1 Organisatorische Aspekte

Während viele organisatorischen Aspekte durch Weiterentwicklung bestehender Konzepte behandelt werden können, bleibt der Umgang mit dem Datenschutz im IoT-Umfeld als (mit bestehenden bzw. mangels brauchbarer neuartiger Konzepte) derzeit schwer lösbare Aufgabe übrig – es sei denn, man verzichtet auf die Verarbeitung personenbezogener Daten, benutzt Anonymisierung oder Aggregation. Es bleibt abzuwarten, ob es in den nächsten Jahren in diesem Bereich vielversprechende Weiterentwicklungen gibt oder es jedem Unternehmen weiterhin überlassen werden muss, die datenschutzrechtlichen Aspekte pro IoT-Anwendungsfall zu klären und anschließend individuell zu implementieren.

7.2.2 Applikationsbezogene Aspekte

In diesem Kontext stellen vor allem die Authentifizierung und Autorisierung große Herausforderungen dar, da die dafür skizzierten neuartigen Lösungsansätze (z.B. ABAC) möglicherweise

nicht zu den bestehenden Sicherheitskonzepten des Unternehmensnetzwerks passen und deswegen ein Neudenken von Maßnahmen erfordern. Die größte Aufgabe dürfte dabei in der Entwicklung oder Einführung entsprechender, an die Sicherheitsbedürfnisse angepasster dezentraler Infrastruktur, Anwendungen oder Protokolle bestehen. Diese müssen zusätzlich zu den vorhandenen Verzeichnisdiensten, RBAC-Modellen etc. eingeführt und gewartet werden. Dies erfordert – neben einem einmalig aufwändigen, individuellen Design – personelle und finanzielle Ressourcen, auch im Betrieb.

Vorhandene Mechanismen und Protokolle für Vertraulichkeit und Integrität sind in echten IoT-Anwendungsfällen durch Ressourcenlimitierungen ebenso schlecht einsetzbar. Es gibt einige Lösungsansätze für neue oder adaptierte leichtgewichtige Algorithmen, die aber so bisher nicht in vorhandenen Unternehmensnetzwerken eingesetzt werden dürften und damit als neuartig einzustufen sind.

Sollten sich vorhandene Sicherheitsmechanismen in den genannten Bereichen aus individuellen Gründen für eine IoT-Anwendung dennoch eignen, stellt wiederum die Skalierbarkeit bei IoT eine Herausforderung dar. Es ist zu hinterfragen, ob die erwartete Vielzahl an Geräten bestehende Infrastruktur nicht vor zu große Aufgaben hinsichtlich der Leistungsfähigkeit stellt.

Der Einsatz von (Security-)IoT-Gateways/Middleware stellt einen brauchbaren Lösungsansatz für viele der geschilderten Probleme dar. Da solche Technologien aber ohne IoT noch nicht im Einsatz sein dürften, wird dieser Ansatz als neuartig klassifiziert. Zudem brechen sie teilweise das IoT-Paradigma auf, da in diesen Fällen keine echte T2T-Kommunikation mehr stattfindet.

7.2.3 Technische Aspekte

Für die Absicherung des Zugangs zu einem Netzwerk bieten sich diverse Lösungsvorschläge an, die eine Veränderung bzw. grundlegende Modernisierung bestehender Netzwerke bedeuten. Sowohl der Einsatz von Virtualisierungstechnologien und vollautomatischer zentraler Steuerung eines Netzwerks (siehe auch SDN weiter unten) sind noch keine weit verbreiteten Konzepte. Die Implementierung einer Zero-Trust-Policy ist ein vielversprechender Ansatz, mündet jedoch ebenso in einer massiven Änderung der gesamten Netzwerksicherheitsarchitektur und ist damit als neuartig anzusehen.

Drahtlostechnologien und ihre Absicherung stellen eine besondere Herausforderung dar, da die eingesetzten Technologien oftmals selbst neuartig sind und wenig mit den weitverbreiteten WLAN-Technologien gemein haben. Für Unternehmensnetzwerke bedeutet dies, dass neue Konzepte für die Absicherung notwendig sind. Bei der Auswahl von IoT-Geräten sollte daher genau auf die Möglichkeiten der eingesetzten Technologien geachtet werden, mit Störungen oder Angriffen umzugehen.

Die Herstellung von Redundanzen im IoT-Umfeld ist nicht mit bestehenden Redundanzszenarien zu vergleichen, da sie schlichtweg in dieser Form nicht realisierbar sind. So kann beispielsweise ein IoT-Türschloss nicht einfach doppelt ausgelegt werden, da dies im Fehlerfall bei einer Tür nicht zu einem gewünschten Zustand (z.B. offene Tür) führen kann. Hier muss individuell festgelegt werden, welche Konsequenzen eine Störung hat und wie die Verfügbarkeit maximiert werden

kann (z.B. durch Auswahl der Geräte nach Verfügbarkeitsaspekten). Im Fall von Sensornetzwerken können hier wie zuvor beschrieben bestimmte Maßnahmen ergriffen werden, um Ausfälle zu kompensieren, diese bedürfen jedoch ebenfalls einer vorhergehenden Planung und entsprechender Implementierung in Applikation oder Middleware.

Der vorgeschlagene Einsatz von SDN zur Segmentierung bietet zahlreiche Vorteile im Kontext von IoT. Eine solch granulare Sichtbar- und Steuerbarkeit von (auch IoT-)Datenverkehr ist in traditionellen Unternehmensnetzwerken nicht möglich, da sich die Beeinflussung des Datenverkehrs zumeist nur an logischen Netzknotenpunkten wie Firewalls steuern lässt. Durch SDN ist die Schaffung einer feingranularen Segmentierung möglich. Damit lässt sich in der Folge auch eine Zero-Trust-Policy technisch realisieren.

Diese Technologie, wenngleich schon durchaus marktreif, muss aber als neuartiges Konzept gesehen werden, da die Adaptionsrate in vorhandenen Netzwerken noch sehr gering ist. Eine Umfrage unter IT-Führungskräften aus 2018 zeigt, dass nur knapp ein Zehntel aller befragten Unternehmen davon ausgehen, eine SDN-Architektur in drei bis fünf Jahren unternehmensweit implementiert bzw. ausgerollt zu haben. Zwar werden die Vorteile, insbesondere auch im Bereich Sicherheit erkannt (Vizard, 2018), die Einführung von SDN stellt allerdings eine komplette Neugestaltung der Netzwerkstruktur durch Einführung neuer Konzepte und Komponenten dar.

Die zentrale Erfassung von Logdaten auch im IoT-Umfeld ist kein neuer Ansatz und an und für sich ein geforderter Minimalstandard zur Erreichung bzw. Erhaltung der Informationssicherheit. Doch um mit den durch die hohe Anzahl an Geräten zu erwartenden schieren Mengen an Daten sinnvoll umzugehen, werden moderne Ansätze wie Big Data, Machine Learning und KIs benötigt. Diese Technologien dürften aber noch keineswegs in (vor allem kleinere) Unternehmensnetzwerke Einzug gehalten haben, zudem ist für die sinnvolle Integration sicherlich einiges an Spezialwissen notwendig. Der Ansatz an sich ist vielversprechend, insbesondere wenn er auch für intelligentes Schwachstellenmanagement genutzt werden kann, muss aber eindeutig als neuartig kategorisiert werden.

7.3 Zusammenfassung

Es zeigt sich, dass vor allem viele der organisatorischen Maßnahmen durch Weiterentwicklung bestehender Elemente aus dem in Kapitel 3 skizzierten Sicherheitskonzept abgeleitet werden können. Das ermöglicht es, auf relativ einfachem Wege, die geforderte Informationssicherheit auch in IoT-Umgebungen in diesen Bereichen sicherzustellen.

Hingegen lassen sich viele der in 6.2 bzw. 6.3 beschriebenen applikationsbezogenen und technischen Maßnahmen nicht ohne gravierende Änderungen der Sicherheitsarchitektur implementieren. Zudem fehlen in einigen Bereichen vorhandene Standardlösungen, so dass eine individuelle Entwicklung von Lösungen in diesen Bereichen notwendig sein kann. Es steht daher zu befürchten, dass, wenn eine IoT-Anwendung im Unternehmen nicht mit der vorhandenen Infrastruktur realisierbar ist, auf gewisse Aspekte der Sicherheit verzichtet werden wird. Das könnte auf Grund mangelndem entsprechenden Know-Hows oder finanziellem bzw. zeitlichem Druck (Stich-

wort Time-to-Market) passieren. Dadurch bleiben aber möglicherweise Risiken für die Informationssicherheit unbehandelt, was zu einem niedrigen Sicherheitsniveau der IoT-Anwendung führen kann bzw. wird.

Ein Blick in Best Practices im Bereich IoT-Sicherheit zeigt oftmals IoT-Implementierungen als relativ leicht „sicher“ in ein Unternehmensnetzwerk zu integrierende (Insel-)Lösungen[18], welche auf wenigen Seiten beschrieben werden können. Demgegenüber wirken die hier in den letzten Kapiteln diskutierten Maßnahmen möglicherweise schwergewichtig, aufwändig und kompliziert. Eine solche Best-Practice-Herangehensweise kann für ein Unternehmensnetzwerk natürlich sinnvoll sein, wenn man nur einzelne IoT-Geräte in das Netzwerk integrieren möchte oder ein lokales *Intranet of Things* als Ziel anstrebt. Es sei aber klargestellt, dass die in dieser Arbeit diskutierten Sicherheitskonzepte jedoch auf eine dem IoT-Paradigma entsprechende, hochskalierende und heterogene Integration von IoT in ein Netzwerk abzielen, welche wesentlich komplexere Anforderungen an die Informationssicherheit stellt.

[18] so z.B. die Hub-Architektur der „IoT Security Foundation“ (IoT Security Foundation, 2018)

8 CHECKLISTE FÜR DEN EINSATZ VON IOT

Die nachfolgende Checkliste in Tabelle 3 stellt eine Zusammenfassung aus Handlungsfeldern und Maßnahmen bzw. Handlungsempfehlungen der vorhergehenden beiden Kapitel dar. Sie kann dazu dienen, bei einer IoT-Implementierung in einem Unternehmensnetzwerk die verschiedenen Teilbereiche systematisch zu betrachten und einen individuellen, an den Schutzbedarfen und Rahmenbedingungen der der IoT-Anwendung orientierten Realisierungsgrad der einzelnen Maßnahmen abzuleiten. Diese Liste soll dazu dienen, IoT-Geräte in Unternehmensnetzwerken sicher einzusetzen. Die Umsetzung zumindest einer Maßnahme aus jedem Handlungsfeld wird dabei empfohlen, da diese Handlungsfelder direkt aus der Risikoanalyse abgeleitet wurden und deswegen jeweils ein konkretes Risiko für die Verletzung der Schutzziele der Informationssicherheit besteht.

	Handlungsfeld	**Maßnahmen**
ORGANISATORISCHE HANDLUNGSFELDER	Informationssicherheitsmanagement	Anpassung des Informationssicherheitsmanagements an IoT-spezifische Rahmenbedingungen und Definition des Schutzniveaus (Sicherheitspolitik, Sicherheitsziele, Sicherheitsanforderungen/Schutzwürdigkeit, Sicherheitsarchitektur, Sicherheitskonzepte); Einsatz von Standards und Best Practices
	Datenklassifizierung	Identifikation und Klassifikation der in IoT-Anwendungen verarbeiteten Daten; Business Impact Analysis
	Beschaffungsprozess und Life Cycle Management	Anpassung des IKT-Beschaffungsprozesses auf IoT-spezifische Rahmenbedingungen; Einführung einer IoT-DMP
	Personal	Sicherstellung von im Unternehmen benötigten IoT-spezifischen Sicherheitskenntnissen; Awareness-Schulungen; Schulung im Umgang mit Sicherheitsvorfällen
	Configuration und Change Management	Nutzung einer IoT-DMP als CMDB und Datenmanagementplattform; Anpassung der Change Management-Prozesse an IoT-Rahmenbedingungen
	Schwachstellen- und Patchmanagement	Nutzung einer IoT-DMP für das Patchmanagement; Nutzung einschlägiger Informationsdienste;
	Audits und Pen-Testing	Erweiterung von Audits auf IoT-Umgebung; Erweiterung oder Einfürhung von Pen-Testing für IoT-Umgebung
	Datenschutz	Verzicht auf personenbezogene Daten; Anonymisierung oder Aggregierung; Privacy by Design; Einsatz von Middleware zur Sicherstellung der Einhaltung von Datenschutzprozessen; Nutzung von Privacy Enhancement Technologies

APPLIKATIONSBEZOGENE HANDLUNGSFLEDER	Authentifizierung und Autorisierung	Zentraler ACS; PKI; RBAC; ABAC; CBAC; Nutzung von Middleware; eigenentwickeltes Key Management; Schlüsselserver
	Verschlüsselung	TLS; IPSec; symmetrische leichtgewichtige Protokolle; objektbasierte Sicherheit (optional Key Management)
	Integrität	Hashverfahren; Digitale Signaturen
	Cloud Computing	Beschäftigung mit Cloud Security; Forderung von ISMS-Zertifizierung; Cloud Gateways; vertragliche Absicherungen
	Entwicklung von IoT-Applikationen	Sicherheitsbezogener Entwurf; Beschränkung der Funktionalität; Beschäftigung mit IoT-Ressourcenlimitierungen; Verfahren sicherer Softwareentwicklung; Auslagerung an Dritte
TECHNISCHE HANDLUNGSFELDER	Absicherung von Geräten	Konfiguration nach Best Practices oder Bedienungsanleitung; Anpassung von Standardeinstellungen; Deaktivierung nicht benötigter Komponenten, Dienste und Benutzerzugänge; Abschaltung physischer Interfaces; Löschmechanismen; Nutzung verschlüsselter Speicherbereiche
	Sicherer Updateprozess	Nutzung von abgesicherten OTA-Mechanismen; Nutzung entsprechender Softwareframeworks bei Eigenentwicklungen; Fehlerbehandlung
	Netzwerkzugangsschutz	NAC (z.B. 802.1X); Policy Server und Beweisführung (Posturing); IoT-DMP; Netzwerkvirtualisierung und Geräteerkennung/Onboarding; SDN
	Segmentierung	Schaffung von IoT-Netzsegmenten; Einsatz von Firewalls; Abschottung der IoT-Umgebung; Middleware/IoT-Gateways; Zero Trust Policy; SDN
	Absicherung von Drahtlostechnologien	Funkfrequenzwechsel; Spektrumsspreizung; gerichtete Antennen; Beschränkung von Requests; Sequenznummern; verschlüsselte Kontrollpakete; Frequenzbereichsüberwachung
	Schutz vor Schadsoftware	IPS; Endpoint Security; kognitive Sicherheit/KI; SDN
	Logging	Zentrale Logserver; SIEM; SDN; kongitive Sicherheit/KI

Tabelle 3: Checkliste. Zusammenstellung von Handlungsfeldern und Maßnahmen zur Sicherstellung von Informationssicherheit beim Einsatz von IoT-Geräten in einem Unternehmensnetzwerk

9 CONCLUSIO

Wird das Thema Sicherheit bei IoT nicht zunehmend ernster genommen, wird es weiterhin fatale und medienwirksame Sicherheitsvorfälle in diesem Kontext geben. Der vorliegende Blick auf die Sicherheitsaspekte von IoT zeigt, dass die Ursachen dafür verbreitet und mannigfaltig sind, da es sehr viele unterschiedliche Bereiche gibt, in denen Schwachstellen auftreten können. Dieser Umstand, gepaart mit einer verheerenden Bedrohungslage im Internet, mangelhaftem Sicherheitsbewusstsein und fehlenden „einfachen“ Konzepten für IoT-Sicherheit macht dies zu einem Thema, welches in der IKT-Welt noch für einiges Kopfzerbrechen sorgen wird. Das Beispiel des Datenverlusts bei der NASA in Abschnitt 6.1.4 zeigt eindrücklich, dass bereits ein einziges IoT-Gerät ausreichen kann, um die Informationssicherheit eines Unternehmens in Stücke zu reißen.

Auch wenn viele der eingangs erwähnten, medial publizierten Vorfälle CIoT-Anwendungen betreffen, müssen Unternehmen dennoch einen genauen Blick auf ihre Netzwerksicherheitskonzepte legen – nicht zuletzt, da CIoT-Geräte auch in Unternehmensnetzen vorhanden sein werden. Zudem hat M2M-Kommunikation, insbesondere im Umfeld von IIoT, schon Einzug in viele Unternehmensnetze gehalten. Ob und welche anderen IoT-Anwendungen eingesetzt werden (die Bandbreite an Möglichkeiten ist immens), hängt vom Unternehmensumfeld, Innovationsfreudigkeit und erkannten wirtschaftlichen oder markt-/kundenorientierten Vorteilen ab. Wichtig ist dabei, die verarbeiteten Informationen zu erheben und entsprechend ihrer Wichtigkeit für das Unternehmen zu klassifizieren, damit klar ist, welche Schutzbedürftigkeit gegeben ist. Dies ist insbesondere auch aus datenschutzrechtlichen Gründen anzuraten.

Die durchlaufene, auf spezielle IoT-Rahmenbedingungen ausgelegte Risikoanalyse hat IoT-spezifische Schwachstellen aufgezeigt. Daraus wurde ein Risikokatalog abgeleitet, welcher in die Zusammenstellung eines Katalogs von Maßnahmen zur Behandlung der Risiken eingeflossen ist. Damit handelt es sich dabei um einen Ansatz, der als Ergänzung in das Informationssicherheitsmanagement bzw. den Informationssicherheitsrisikomanagementprozess des Unternehmens integriert werden kann, um mögliche Lücken oder blinde Flecke zu eliminieren und eine Risikobehandlung anzustoßen. Wie sich dabei gezeigt hat, ist es ungemein sinnvoll, mehrere möglichst unterschiedliche Quellen zur Identifizierung von Schwachstellen heranzuziehen. Ansonsten besteht die Gefahr, Risiken durch eine zu einseitige Betrachtung zu übersehen.

Die im Rahmen dieser Arbeit identifizierten, üblicherweise in Unternehmensnetzwerken eingesetzten Sicherheitsmaßnahmen erscheinen in beinahe allen Fällen als nicht ausreichend für eine sichere IoT-Integration gemäß dem IoT-Paradigma, wenn sie nicht zumindest entsprechend IoT-spezifischen Risiken angepasst werden. Viele der erkannten Risiken können durch die Weiterentwicklung bzw. konsequente Anwendung bestehender Konzepte im Hinblick auf IoT-Schwachstellen weitgehend abgemildert werden, so dass in diesen Bereichen ein für das Unternehmen akzeptables Sicherheitsniveau (im Hinblick auf verbleibende Restrisiken) erreicht werden kann.

Es bleiben aber etliche Aspekte offen, welche auch durch die Erweiterung bestehender Konzepte nicht abgedeckt werden können und daher gänzlich neue Sicherheitsmaßnahmen bis hin zur Änderung von großen Teilen der Netzwerksicherheitsarchitektur erfordern. Dazu zählen unter

anderem die Themengebiete Authentifizierung, Autorisierung und Datenschutz. Es konnten dafür allerdings keine allgemeinen oder generischen Lösungsansätze identifiziert werden, die bereits erfolgreich in die Praxis umgesetzt wurden, so dass diese Themen anwendungsspezifisch im Einzelfall betrachtet und entsprechend dem angestrebten Sicherheitsniveau gelöst werden müssen. Den darunter besonders heiklen Punkt stellt der Datenschutz dar, da dieser auf Grund gesetzlicher Vorgaben speziell geregelt ist und Verstöße erhebliche rechtliche und finanzielle Konsequenzen nach sich ziehen. Im europäischen Umfeld kommen hier insbesondere die Anforderungen der DSGVO und, falls das Unternehmen betroffen ist, die NIS-RL zum Tragen.

Den Abschluss der Arbeit bildet eine Checkliste, welche die identifizierten Handlungsfelder und die dargestellten möglichen Maßnahmen zur Behandlung in diesen Bereichen entstehender Risiken zusammengefasst darstellt. Es zeigt sich dabei, dass in vielen Bereichen mehrere verschiedene Maßnahmen zur Beherrschung von Risiken bestehen, aus denen je nach Unternehmensanforderungen und technischen Möglichkeiten der IoT-Geräte für den Anwendungsfall geeignete Vorgehensweisen ausgewählt werden können. Maßnahmen sollten jedoch aus jedem Handlungsfeld umgesetzt werden, um eine möglichst umfassende Sicherheit herzustellen. Diese Checkliste sollte laufend an technische Entwicklungen und die aktuelle Bedrohungslage angepasst werden.

Eine Frage, die sich nach der Betrachtung der IoT-Sicherheitslage im Rahmen dieser Arbeit stellt, ist ob ein Unternehmen überhaupt eine für alle Internetteilnehmer zugängliche IoT-Anwendung im Internet betreiben muss, denn damit setzt sich ein Unternehmen gewaltigen Bedrohungen der Informationssicherheit aus. Es hängt natürlich vom Anwendungsfall ab – ist eine Abschottung allerdings möglich, verletzt dies zwar einen der Grundgedanken von IoT (es handelt sich dann strenggenommen um keine „echte“ IoT-Anwendung mehr), die Bedrohungslage wird aber massiv entschärft. Deswegen sollte ein solcher Schritt – wenn möglich – auf jeden Fall unternommen werden.

Eine weitere Erkenntnis ist, dass die Vielfalt an möglichen Risiken wohl durch die in vielen Bereichen fehlende oder stark zersplitterte Standardisierung vergrößert wurde und wird. Dieser Umstand führt zu einer zu großen Anzahl an (proprietären) Technologien und unausgereiften bzw. unsicheren Geräten und Applikationen; entwickelt oftmals von Herstellern ohne tiefgehendes Wissen im Bereich Informationssicherheit. Das wiederum führt in der Praxis zu eklatanten und zahlreichen Schwachstellen in den Produkten. Es bleibt nur zu hoffen, dass sich der Markt in diesen Bereichen in den kommenden Jahren entsprechend weiterentwickelt, so dass es in Zukunft einfacher wird, eine sichere IoT-Integration in ein Unternehmensnetzwerk vorzunehmen.

Kritisch ist festzuhalten, dass sich ein großer Teil der untersuchten Forschungspublikationen zum Thema IoT-Sicherheit intensiv mit technischen oder applikationsbezogenen Informationssicherheitsrisiken von IoT beschäftigt und teilweise Lösungswege aufzeigt, organisatorische Aspekte aber unbehandelt bleiben. Es scheint jedoch wichtig, sich in weiteren Arbeiten insbesondere vertieft mit diesem Themengebiet auseinanderzusetzen, da die durchgeführte Risikoanalyse aufgezeigt hat, dass eine Nichtbehandlung zu Schwachstellen und damit einem sinkenden Schutzniveau führen kann.

Fortgesetzte Forschung sollte auch und vor allem im Bereich der Analyse bestehender bzw. daraus abgeleiteter Mechanismen zur Authentifizierung und Autorisierung im Umfeld von IoT unternommen werden. Dabei muss ein wesentlicher Fokus sein, für Unternehmen auch praktisch anwendbare Modelle zu identifizieren bzw. die Umsetzbarkeit zu demonstrieren. Durchaus komplex und nicht final beantwortet scheint auch die Lage beim Thema Datenschutz und IoT zu sein. Wie in Zukunft datenschutzrechtlich konforme IoT-Applikationen in der Praxis aussehen können, bedarf weiterer Untersuchungen und ebenso der Entwicklung praktikabler, das heißt auch für Unternehmen wirtschaftlich realisierbarer, Ansätze.

ABKÜRZUNGSVERZEICHNIS

2FA	Two-Factor Authentication
5G	Fifth Generation (Mobilfunkstandard)
ABAC	Atrribute Based Access Control
ACS	Access Control Server
APT	Advanced Persistent Threat
BLE	Bluetooth Low Energy
BSI	Bundesamt für Sicherheit in der Informationstechnologie
BwD	Betreiber wesentlicher Dienste
BYOD	Bring Your Own Device
CA	Certificate Authority
CBAC	Capability Based Access Control
CERT	Computer Emergency Response Team
CIoT	Consumer IoT
DAC	Discretionary Access Control
CMDB	Configuration Management Database
DDoS	Distributed DoS
DoS	Denial of Service
DSGVO	Datenschutzgrundverordnung
EO	Executive Order
GPS	Global Positioning System
H2H	Human-to-Human
ICS	Industrial Control Systems
IDS	Intrusion Detection System
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IERC	European Research Cluster on Internet of Things
IIoT	Industrial IoT
IKEv2	Internet Key Exchange, Version 2
IKT	Informations- und Kommunikationstechnologie
IoE	Internet of Everything
IoMT	Internet of Medical Things
IoT	Internet of Things
IoT-A	IoT Architecture Project
IoT-ARM	IoT Architecture Reference Model
IoT-DM	IoT Device Management
IoT-DMP	IoT Device Management Platform
IP	Internet Protocol
IPS	Intrusion Prevention System
IPSec	Internet Protocol Security
ISO	International Organization for Standardization

ISMS	Informationssicherheitsmanagementsystem
ITU	International Telecommunication Union
IT	Informationstechnologie
KI	Künstliche Intelligenz
LAN	Local Area Network
LoRaWAN	Long Range WAN
LPWAN	Low Power WAN
M2M	Machine-to-Machine
MDM	Mobile Device Management
NAC	Network Access Control
NBIoT	NarrowBand IoT
NFC	Nearfield Communication
NIS-RL	NIS-Richtlinie[19]
NIST	National Institute of Standards and Technology
OSI	Open Systems Interconnection
OT	Operational Technology
OTA	Over-the-Air(-Provisioning)
OWASP	Open Web Application Security Project
PET	Privacy Enhancing Technologies
PKCS	Public-Key Cryptography Standard
PKI	Public Key Infrastructure
RBAC	Role Based Access Control
RFC	Request for Comment
RFID	Radio Frequency Identification
RMP	Risikomanagementprozess
SDN	Software Defined Network
SIEM	Security Incident and Event Management
SSL	Secure Sockets Layer
T2T	Thing-to-Thing
TLS	Transport Layer Security
VDE	Verband der Elektrotechnik Elektronik Informationstechnik e. V.
VDI	Verein Deutscher Ingenieure
VPN	Virtual Private Network
WAN	Wide Area Network
WLAN	Wireless LAN
WPA2	Wi-Fi Protected Access 2
WSN	Wireless Sensor Network
WWAN	Wireless Wide Area Network
ZTP	Zero Trust Policy

[19] Voller Titel: Richtlinie über Maßnahmen zur Gewährleistung eines hohen Sicherheitsniveaus von **Netz- und Informationssystemen** in der Union

ABBILDUNGSVERZEICHNIS

TABELLENVERZEICHNIS

LITERATURVERZEICHNIS

Alabady, S. (Juni 2009). Design and Implementation of a Network Security Model for Cooperative Network. *International Arab Journal of e-Technology*(Vol. 1, No. 2).

ALE International. (2018). *The Internet of Things in the Enterprise.* Alcatel Lucent Enterprise.

Ali, A. I. (2015). *Comparison and Evaluation of Digital Signature Algorithms Schemes Employed in NDN Network.* doi:10.5121/ijesa.2015.5202

Andrecht, T., Kres, A., Machado, J., Mayr, R., Murhammer, M. W., Schmengler, A., . . . Wieprecht, H. (2017). Cognitive Security. In A. Sowa (Hrsg.), *IT-Prüfung, Sicherheitsaudit und Datenschutzmodell* (S. 145-169). Wiesbaden: Springer Verlag.

Atzori, L., Iera, A., & Morabito, G. (31. Mai 2010). Internet of Things: A survey. (E. /. Direct, Hrsg.) *Computer Networks COMPNW 4247*.

Bandyopadhyay, S., Sengupta, M., Maiti, S., & Dutta, S. (2011). ROLE OF MIDDLEWARE FOR INTERNET OF THINGS: A STUDY. *International Journal of Computer Science & Engineering Survey (IJCSES) Vol.2 No.3*, (S. 94-). doi:10.5121/ijcses.2011.2307

Bartels, K. U., & Backer, M. (2018). Die Berücksichtigung des Stands der Technik in der DSGVO. *DuD - Datenschutz und Datensicherheit*(04), S. 214-215.

Bartsch, M., & Frey, S. (Hrsg.). (2018). *Cybersecurity Best Practices.* Springer Vieweg.

Bassi, A., Bauer, M., Fiedler, M., Kramp, T., Kranenburg, R. v., Lange, S., & Meissner, S. (2013). *Enabling Things to Talk. Designing IoT solutions with the IoT Architectural Reference Model.* Springer Open.

Becker, V. (2018). NIS-RL und die Umsetzung im NISG. *Präsentation*. Wirtschaftskammer Österreich. Von http://wko.at/ic/NIS_RLuNISG.pdf abgerufen

Beuchelt, G. (2009). Unix and Linux Security. In *Network and System Security* (S. 127-154). elsevier. doi:http://dx.doi.org/10.1016/B978-0-12-416689-9.00005-8

Bhartiya, S. (2017). *Your smart fridge may kill you: The dark side of IoT*. Abgerufen am 08. Juli 2019 von InfoWorld: https://www.infoworld.com/article/3176673/your-smart-fridge-may-kill-you-the-dark-side-of-iot.html

Bin Ali, M., Hossain, M., & Parvez, M. (07 2015). Design and Implementation of a Secure Campus Network. *International Journal of Emerging Technology and Advanced Engineering*, S. 370-374.

Bishop, M. (2005). *Introduction to Computer Security.* Boston: Pearson Education.

BKA. (2017). 11 Opfer sind genug - das Bundeskriminalamt informiert über den CEO-Betrug. *Informationsblatt CEO Betrug*.

Boger, P. (Hrsg.). (2014). *Scaling Networks.* Indianapolis: Cisco Press.

Braun, T. (2019). *Bis zu 46 Millionen Cyber-Attacken pro Tag auf Unternehmen*. Abgerufen am 02. Juli 2019 von ZDnet: https://www.zdnet.de/88363957/bis-zu-46-millionen-cyber-attacken-pro-tag-auf-unternehmen/

Brykczynski, B., & Small, R. A. (2003). Reducing Internet-Based Intrusion: Effective Security Patch Management. *IEEE Software*, S. 50-57.

BSI. (2015). *Die Lage der IT-Sicherheit in Deutschland 2015.* Bundesamt für Sicherheit in der Informationstechnik.

BSI. (2018). *Die Lage der IT-Sicherheit in Deutschland 2018.* Bonn: Bundesamt für Sicherheit in der Informationstechnik.

BSI. (2019). IT-Grundschutz. *Glossar und Begriffsdefinitionen*. Bundesamt für Sicherheit in der Informationstechnologie. Abgerufen am 07. Juli 2019 von https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/Glossar/glossar_node.html

BSI. (2019b). *Bundesamt für Sicherheit in der Informationstechnologie*. Abgerufen am 18. Juni 2019 von Gesetz zur Umsetzung der NIS-Richtlinie: https://www.bsi.bund.de/DE/DasBSI/NIS-Richtlinie/NIS_Richtlinie_node.html

BSI. (2019b). *IT-Grundschutz-Kompendium - Edition 2019*. Abgerufen am 07. Juli 2019 von Bundesamt für Sicherheit in der Informationstechnologie: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/itgrundschutzKompendium_node.html

BSI. (2019c). *Mindmap zum IT-Grundschutz-Kompendium 2019.* Von Bundesamt für Sicherheit in der Informationstechnologie: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-Grundschutz-Modernisierung/Struktur_2019.pdf?__blob=publicationFile&v=11 abgerufen

Buchs, M. (2017). *Bedrohung durch IoT: Unsicherheiten in den Griff bekommen*. Abgerufen am 07. Juli 2019 von ipt: https://ipt.ch/bedrohung-durch-iot-unsicherheiten-in-den-griff-bekommen/

Burgstaller, P. (2016). *DATENSCHUTZ & NETZ-UND INFORMATIONSSICHERHEIT in der EU.* Von Präsentation: https://www.wko.at/service/ooe/innovation-technologie-digitalisierung/WS4_Digitales_Datensicherheitsrecht_Burgstaller_freigegeben.pdf abgerufen

Buyya, R., & Dastjerdi, A. V. (2016). *Internet of Things: Principles and Paradigms.* Elsevier.

Canner, B. (2018). *Endpoint Security vs Legacy Antivirus: What's the Difference?* Abgerufen am 07. Juli 2019 von Solutions Review: https://solutionsreview.com/endpoint-security/endpoint-security-vs-legacy-antivirus-whats-difference/

Caraguay, Á. L., Peral, A. B., López, L. I., & Villalba, L. J. (2014). SDN: Evolution and Opportunities in the Development IoT Applications. *International Journal of Distributed Sensor Networks.* doi:10.1155/2014/735142

Chaudhuri, A. (2015). Identity and Access Management for the Internet of Things. In p. b. IoT Working Group (Hrsg.).

Chen, H., Jia, X., & Li, H. (2011). A Brief Introduction to IoT Gateway. *Proceedings of ICCTA 2011*.

Chen, K., Zhang, S., Li, Z., Zhang, Y., Deng, Q., Ray, S., & Jin, Y. (2018). Internet-of-Things Security and Vulnerabilities: Taxonomy, Challenges, and Practice. *Journal of Hardware and Systems Security*(2), S. 97-110. doi:https://doi.org/10.1007/s41635-017-0029-7

Chen, L., Ji, J., & Zhang, Z. (2013). *Wireless Network Security.* Peking/Berlin/Heidelberg: Higher Education Press/Springer Verlag.

Chen, S., Xu, H., Lui, D., Hu, B., & Wang, H. (August 2014). A Vision of IoT: Applications, Challenges, and Opportunities With China Perspective. *IEEE INTERNET OF THINGS JOURNAL*(Vol 1, No 4).

Chen, T. M., & Walsh, P. J. (2014). Guarding Against Network Intrusions. In *Network And System Security* (Second Edition Ausg., S. 57-82). Elsevier Inc.

Cimpanu, C. (2019). *NASA hacked because of unauthorized Raspberry Pi connected to its network*. Abgerufen am 08. Juli 2019 von https://www.zdnet.com/article/nasa-hacked-because-of-unauthorized-raspberry-pi-connected-to-its-network/

CIS. (Juni 2018). *NIS-Gesetz: Verbund AG und Tochtergesellschaften zertifiziert nach ISO 27001 und 27019*. Abgerufen am 07. Juli 2019 von CIS - Certification & Information Security Services GmbH: https://at.cis-cert.com/News-Presse/Newsletter/NL-Juni-2018/Verbund-Zertifizierung-ISO-27001-und-ISO-27019-NIS-Gesetz.aspx

Coache, S., & Salihoglu, M. (2018). *The Internet of (Insecure) Things: How an IoT Toaster Can Burn You*. Abgerufen am 7. Juli 2019 von Crowe Cybersecurity Watch blog: https://www.crowe.com/cybersecurity-watch/internet-of-insecure-things?utm_source=forbes

Columbus, L. (2018). *2018 Roundup Of Internet Of Things Forecasts And Market Estimates*. Abgerufen am 04. Juli 2019 von Forbes.com: https://www.forbes.com/sites/louiscolumbus/2018/12/13/2018-roundup-of-internet-of-things-forecasts-and-market-estimates/#3befa89a7d83

Cybersecurity Matters. (2015). *The IoT is a lot like BYOD*. Abgerufen am 23. Januar 2019 von DXC.technology: https://blogs.dxc.technology/2015/03/08/the-iot-is-a-lot-like-byod/

Daya, B. (2008). *Network Security: History, Importance, and Future.* University of Florida Department of Electrical and Computer Engineering.

Dhanjani, N. (2016). *IoT-Hacking.* Heidelberg: dpunkt.verlag.

Di Salvo, C. (2018). *How Blockchain Will Change Cybersecurity Practices.* (M. Bartsch, & S. Frey, Hrsg.) Wiesbaden: Springer Vieweg.

DIN 31000. (2017). Allgemeine Leitsätze für das sicherheitsgerechte Gestalten von Produkten. DIN.

Dooley, K. (2017). *Simple Network Redundancy: Creating Maximum Availability With Minimum Complexity*. Abgerufen am 08. Juli 2019 von auvik: https://www.auvik.com/franklymsp/blog/simple-network-redundancy/

DynDNS. (2016). *Dyn Status Updates. DDoS Attack Against Dyn Managed DNS*. Abgerufen am 08. Juli 2019 von dynstatus: https://www.dynstatus.com/incidents/nlr4yrr162t8

Erlijn, v. G., & Schreiber, S. (2017). Der IoT-Penetrationstest. In A. Sowa (Hrsg.), *IT-Prüfung, Sicherheitsaudit und Datenschutzmodell* (S. 93-105). Wiesbaden: Springer Verlag.

Eschenauer, L., & Gligor, V. D. (2002). *A Key-Management Scheme for Distributed Sensor Networks.*

EU. (27. April 2016). VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES. *zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung)*.

eurostat. (2019). *Nutzung von Cloud Computing Diensten [isoc_cicce_use]*. Abgerufen am 08. Juli 2019 von eurostat: http://appsso.eurostat.ec.europa.eu/nui/show.do?dataset=isoc_cicce_use&lang=de

Flauzac, O., Gonzalez, C., & Nolot, F. (2015). New Security Architecture for IoT Network. *Procedia Computer Science 52*, (S. 1028-1033). doi:10.1016/j.procs.2015.05.099

Frisch, D., Reißmann, S., Pape, C., & Rieger, S. (Dezember 2018). Internet of Things: Sicherheit kein Ding der Unmöglichkeit. *DFN Mitteilungen, Ausgabe 94*.

Gabbai, A. (Januar 2015). Interview. *Kevin Ashton Describes "the Internet of Things"*. Von https://www.smithsonianmag.com/innovation/kevin-ashton-describes-the-internet-of-things-180953749/ abgerufen

Gadatsch, A., & Mangiapane, M. (2017). *IT-Sicherheit. Digitalisierung der Geschäftsprozesse und Informationssicherheit.* Wiesbaden: Springer Vieweg.

Gajar, P. K., Ghosh, A., & Rai, S. (April 2013). BRING YOUR OWN DEVICE (BYOD): SECURITY RISKS AND MITIGATING STRATEGIES. *Journal of Global Research in Computer Science*(Volume 4, No. 4).

Geiger, M. (2018). *sichere industrie*. Abgerufen am 18. Juni 2019 von Safety vs. Security: Der Unterschied einfach erklärt (Und wie Sie beide Ziele kombinieren können): https://www.sichere-industrie.de/safety-security-unterschied-erklaert-kombination-ziele-industrial-security/

Georgakopoulos, D., & Zhang, L.-J. (Hrsg.). (2018). Internet of Things – ICIOT 2018. *Third International Conference Held as Part of the Services Conference Federation, SCF 2018.* Seattle.

Gerbino, F. (6. April 2017). *Corporate-, IT- und Security Governance*. Von scip AG: https://www.scip.ch/?labs.20170406 abgerufen

Gies, D., & Steil, T. (2018). *Sicherheitsanforderungen an Netzarchitektur und Netzdesign eines Gebäudes der Zukunft.* ComConsult Research, Jürgen Suppan.

Gillenkirch, R. (2018). *Zielsystem der Unternehmung*. Abgerufen am 17. Juni 2019 von Gabler Wirtschaftslexikon: https://wirtschaftslexikon.gabler.de/definition/zielsystem-der-unternehmung-53968

Gold, J. (2018). *Q&A: Jeff Wilbur of the Online Trust Alliance on why enterprise IoT security is a lot like BYOD*. Abgerufen am 23. Januar 2019 von NetworkWorld: https://www.networkworld.com/article/3292223/qanda-jeff-wilbur-of-the-online-trust-alliance-on-why-enterprise-iot-security-is-a-lot-like-byod.html

Gurkok, C. (2014). Securing Cloud Computing Systems. In *Network and System Security* (S. 83-126). elsevier. doi:http://dx.doi.org/10.1016/B978-0-12-416689-9.00004-6

Gusmerolia, S., Piccionea, S., & Rotondib, D. (2013). A capability-based security approach to manage access control in the Internet of Things. *Mathematical and Computer Modelling 58*, (S. 1189–1205).

Harnisch, H. (2019). Zur Sicherheitslage. Leibnitz Universität Hannover.

Hassan, Q. F., Khan, A. u., & Madani, S. A. (2017). *Internet of Things: Challenges, Advances, and Applications.* CRC Press.

Heer, T., Garcia-Morchon, O., Hummen, R., Keoh, S. L., Kumar, S. S., & Wehrle, K. (2011). Security Challenges in the IP-based Internet of Things. *Wireless Pers Commun.* doi:10.1007/s11277-011-0385-5

Hill, K. (2018). *IoT Devices for the Enterprise: The Key Roles of Design, Testing and Security.* RCRWireless.

Hossain, M., Fotouhi, M., & Hasan, R. (2015). Towards an Analysis of Security Issues, Challenges, and Open Problems in the Internet of Things. *2015 IEEE World Congress on Services.* doi: 10.1109/SERVICES.2015.12

IEC. (2016). *IEC role in the IoT.* (International Electrotechnical Commission). Von https://www.iec.ch/about/brochures/pdf/technology/iec_role_IoT.pdf abgerufen

IERC. (2014). *IERC - European Research Cluster on the Internet of Things*. Von Internet of Things: http://www.internet-of-things-research.eu/about_iot.htm abgerufen

IoT Security Foundation. (2018). *IoT Security Architecture and Policy for the Enterprise - a Hub Based Approach.* Abgerufen am 07. Juli 2019 von https://www.iotsecurityfoundation.org/wp-content/uploads/2018/11/IoT-Security-Architecture-and-Policy-for-the-Enterprise-a-Hub-Based-Approach.pdf

i-SCOOP. (2016). *Internet of Things definitions. What is the Internet of Things?* (i-SCOOP, Herausgeber) Abgerufen am 19. 01 2018 von i-scoop: https://www.i-scoop.eu/internet-of-things/

i-SCOOP. (2018). *IoT device management: challenges, solutions, platforms, choices, market and future*. Abgerufen am 18. Juni 2019 von i-SCOOP: https://www.i-scoop.eu/internet-of-things-guide/iot-device-management/

ISO/IEC. (2009). Risk Management - Vocabulary. *ISO/IEC Guide 73:2009*. International Organization for Standardisation.

ISO/IEC. (23. August 2016). CD 20924. *Text of CD 20924, Information technology - Internet of Things - Definition and Vocabulary*.

ISO/IEC. (Dezember 2018). International Standard. *ISO/IEC 20924 1.0: Internet of Things (IoT) Vocabulary*.

IT Governance Europe. (2016). *Die Richtlinie zur Gewährleistung einer hohen Netzwerk- und Informationssicherheit (NIS-Richtlinie)*. Abgerufen am 18. Juni 2019 von itgovernance.eu: https://www.itgovernance.eu/de-de/nis-directive-de

ITU. (2005). The Internet of Things. *ITU Internet Reports*.

ITU-T. (2007). *ITU-T Standardization: Helping the world communicate.* Von https://www.itu.int/dms_pub/itu-t/opb/gen/T-GEN-OVW-2007-E09-PDF-E.pdf abgerufen

ITU-T. (06 2012). Recommendation Y.2060. Overview of the Internet of things. *SERIES Y: Global Information Infrastructure, Internet Protocol Aspects and Next-Generation Networks*.

Jamoussi, B. (2010). *IoT Prospects of Worldwide Development and Current Global Circumstances.* Wuxi.

Jara, A. J., Ladid, L., & Skarmeta, A. (2013). The Internet of Everything through IPv6: an analysis of challenges, solutions and opportunities. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications.*(4), S. 97-118.

Jararweh, Y., Al-Ayyoub, M., Darabseh, A., Benkhelifa, E., Vouk, M., & Rindos, A. (2015). SDIoT: a software defined based internet of things framework. *J Ambient Intell Human Comput.* doi: 10.1007/s12652-015-0290-y

Jing, Q., Vasilakos, A. V., Wan, J., Lu, J., & Q, D. (2014). Security of the Internet of Things: perspectives and challenges. *Wireless Netw.* doi: 10.1007/s11276-014-0761-7

Kamp, T. (9. Januar 2018). *datenschutz notizen*. Von Was ist Belastbarkeit im Sinne von Art. 32 DSGVO?: https://www.datenschutz-notizen.de/was-ist-belastbarkeit-im-sinne-von-art-32-dsgvo-3319778/ abgerufen

Kappes, M. (2013). *Netzwerk- und Datensicherheit, 2. Auflage.* Wiesbaden: Springer.

Karl, A. (27. Februar 2018). *Internet of Everything vs. Internet of Things*. Von http://techgenix.com/internet-of-everything/ abgerufen

Kersten, H., & Klett, G. (2015). *Der IT Security Manager. Aktuelles Praxiswissen für IT Security Manager und IT-Sicherheitsbeauftragte in Unternehmen und Behörden. 4. Auflage.* Wiesbaden: Springer Vieweg.

Kizza, J. M. (2015). *Guide to Computer Network Security.* London: Springer Verlag.

Kleinhans, J.-P. (2017). *Internet of Insecure Things.* Berlin: Stiftung Neue Verantwortung.

Klipper, S. (2011). *Information Security Risk Management.* Wiesbaden: Vieweg+Teubner.

Königs, H.-P. (2013). *IT-Risikomanagement mit System. 4. Auflage.* Wiesbaden: Springer Vieweg.

Königs, H.-P. (2017). *IT-Risikomanagement mit System, 5. Auflage.* Wiesbaden: Springer Verlag.

Kozlov, D., Veijalainen, J., & Ali, Y. (2012). *Security and Privacy Threats in IoT Architectures.* SeTTiT. doi:10.4108/icst.bodynets.2012.250550

Kreutzer, R. (2018). *Time-to-Market. Ausführliche Definition*. Abgerufen am 18. Juni 2019 von Gabler Wirtschaftslexikun: https://wirtschaftslexikon.gabler.de/definition/time-market-54271

Kuhn, J. R. (2011). *Soft systems theory*. Abgerufen am 23. Januar 2019 von is.theorizeit.org: https://is.theorizeit.org/wiki/Soft_systems_theory

Kumar, S. N. (2015). Review on Network Security and Cryptography. *International Transaction of Electrical and Computer Engineers System*, S. 1-11. doi:10.12691/iteces-3-1-1

Lee, I., & Lee, K. (2015). The Internet of Things (IoT): Applications, investments, and challenges for enterprises. *Business Horizons vol 58*, S. 431-440.

Limer, E. (2016). *A Virtual Toaster Shows How Quickly Smart Appliances Can Get Hacked*. Abgerufen am 08. Juli 2019 von Popular Mechanics: https://www.popularmechanics.com/technology/security/a23602/virtual-toaster-hacked-immediately/

Line, M. B., Rostad, L., Nordland, O., & Tondel, I. A. (2006). Safety vs. Security? *Proceedings of the 8th International Conference on Probabilistic Safety Assessment and Management.* New Orelans.

Loeb, L. (2018). *https://www.securitynow.com/author.asp?section_id=649&doc_id=745701*. Abgerufen am 08. Juli 2019 von SecurityNow: https://www.securitynow.com/author.asp?section_id=649&doc_id=745701

Lopez Research. (2013). *An Introduction to the Internet of Things (IoT).* Bericht. Part 1. of "The IoT Series", San Francisco.

Lueth, K. L. (19. Dezember 2014). *Why the Internet of Things is called Internet of Things: Definition, history, disambiguation*. (IOT Analytics) Abgerufen am 14. Januar 2018 von https://iot-analytics.com/internet-of-things-definition/

Macaulay, T. (2017). *RIoT Control. Understanding and Managing Risks and the Internet of Things.* Cambridge: Morgan Kaufmann.

Maddox, T. (2016). *Top IoT and wearable tech trends for 2016: Smartwatches in transition as smartglasses rule*. Abgerufen am 18. Juni 2019 von Techrepublic.com: https://www.techrepublic.com/article/top-iot-and-wearable-tech-trends-for-2016-smartwatches-in-transition-as-smartglasses-rule/

Mahalle, P. N., Anggorojati, B., Prasad, N. R., & Prasad, R. (2013). Identity Authentication and Capability Based Access Control (IACAC) for the Internet of Things. *Journal of Cyber Security and Mobility 1(4)*, (S. 309-348).

Mansoor, B. (2014). Intranet Security. In *Network and System Security* (Second Edition Ausg.). Elsevier Inc. doi:http://dx.doi.org/10.1016/B978-0-12-416689-9.00008-3

Markoff, J. (2016). *Why Light Bulbs May Be the Next Hacker Target*. Abgerufen am 08. Juli 2019 von The New York Times: https://www.nytimes.com/2016/11/03/technology/why-light-bulbs-may-be-the-next-hacker-target.html

Matthews, L. (2016). *Someone Just Used The Mirai Botnet To Knock An Entire Country Offline*. Abgerufen am 08. Juli 2019 von Forbes: https://www.forbes.com/sites/leemathews/2016/11/03/someone-just-used-the-mirai-botnet-to-knock-an-entire-country-offline/#106ac3516c4f

Matthews, R. (2017). *Should I be afraid of my fridge? Threats of….* Abgerufen am 08. Juli 2019 von WardSolutions: https://www.ward.ie/threats-of-the-iot/

McGee, A. R., Vasireddy, S. R., Xie, C., Picklesimer, D. D., Chandrashekhar, U., & Richman, S. H. (2004). A Framework for Ensuring Network Security. *Bell Labs Technical Journal*(8(4)), S. 7-27. doi:10.1002/bltj.10083

Medina, C. A., Pérez, M. R., & Trujillo, L. C. (2017). IoT Paradigm into the Smart City Vision: A Survey. *2017 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, (S. 695-704). doi:DOI 10.1109/iThings-GreenCom-CPSCom-SmartData.2017.109

Miraz, M. H., Maaruf, A., Excell, P. S., & Picking, R. (28. Juli 2018). A Review on Internet ofThings (loT), Inte et of Everything (IoE) and Inte et ofNano Things (IoNT). *MDPI Journal: future internet*(doi:10.3390/fi10080068).

Müller, K.-R. (2018). *IT-Sicherheit mit System* (6. Auflage Ausg.). Wiesbaden: Springer.

Nahius, I. (2016). *5 promising examples of IoT and wearable devices that enable people with disabilities*. Abgerufen am 18. Juni 2019 von medium.com: https://medium.com/@imn/5-promising-examples-of-iot-and-wearable-devices-that-enable-people-with-disabilities-f50df601e046

Naste, S.-D. (2018). Your toaster as a threat to critical infrastructure: A multidisciplinary study on DDoS attacks in the EU IoT ecosystem. Tilburg University.

NIST. (Juni 2011). Guide to Industrial Control Systems (ICS) Security. Special Publication 800-82. *Recommendations of the National Institute of Standards and Technology*.

NIST. (2013). Security and Privacy Controls for Federal Information Systems and Organizations: Special Publication 800-53. Recommendations of the National Institute of Standards and Technology. Abgerufen am 08. Juli 2019 von https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

North, K., Brandner, A., & Steininger, T. (2016). *Wissensmanagement für Qualitätsmanager. Erfüllung der Anforderungen nach ISO 9001:2015.* Wiesbaden: Springer Gabler.

oceanit. (kein Datum). *Nanite*. Abgerufen am 18. 06 2019 von https://www.oceanit.com/products/nanite

Olawumi, O., Haataja, K., Asikainen, M., Vidgren, N., & Toivanen, P. (2014). Three Practical Attacks Against ZigBee Security: Attack Scenario Definitions, Practical Experiments, Countermeasures, and Lessons Learned. *International Conference on Hybrid Intelligent Systems (HIS)* (S. 199-206). IEEE.

Oluwatosin, H. S. (Februar 2014). Client-Server Model. *Haroon Shakirat Oluwatosin, Volume 16, Issue 1, Ver. IX* , S. 67-71.

Oppenheimer, P. (2011). *Top-Down Network Design.* Indianapolis: Cisco Press.

Otter, R. (2019). *Vernetzte Waschmaschinen im Vergleich*. Abgerufen am 07. Juli 2019 von https://www.smart-wohnen.de/haus-garten/artikel/vernetzte-waschmaschinen-im-vergleich/

OWASP. (2018). *OWASP 2018 IoT Top10 Final.* Abgerufen am 03. Juli 2018 von OWASP.org: https://www.owasp.org/images/7/79/OWASP_2018_IoT_Top10_Final.jpg

Panetta, K. (2016). *The challenges of creating, implementing and preparing for the IoT.* Abgerufen am 04. Juli 2019 von Gartner: https://www.gartner.com/smarterwithgartner/7-technologies-underpin-the-hype-cycle-for-the-internet-of-things-2016/

Patton, M., Gross, E., Chinn, R., Forbis, S., Walker, L., & Chen, H. (2014). Uninvited Connections. A Study of Vulnerable Devices on the Internet of Things (IoT). *IEEE Joint Intelligence and Security Informatics Conference*, (S. 232-235). doi:10.1109/JISIC.2014.43

Perera, C., Ranjan, R., Wang, L., Khan, S. U., & Zomaya, A. Y. (May/June 2015). Big Data Privacy int the Internet of Things Era. *IT Pro*, S. 32-39.

Petereit, D., & von Westernhagen, O. (26. Juni 2019). Silex: Neue Malware legt schlecht gesicherte Geräte im Internet of Things still. *heise.de*. Abgerufen am 08. Juli 2019 von https://www.heise.de/security/meldung/Silex-Neue-Malware-legt-schlecht-gesicherte-Geraete-im-Internet-of-Things-still-4455677.html

Petrov, C. (2019). *Internet of Things Statistics 2019 [The Rise Of IoT]*. Abgerufen am 05. Juli 2019 von TechJury: https://techjury.net/stats-about/internet-of-things-statistics/

Pfeiffer, R., & Kafka, M. (Juni. 2019 2011). Ausgewählte Angriffsvektoren. 18: DeepSec InDepth Security Conference. Von https://deepsec.net/docs/Talks/Angriffsvektoren_AAk.pdf abgerufen

Pohlmann, N. (2015). *Lagebild zur Bedrohung der IT-Sicherheit.* Abgerufen am 17. Juni 2018 von Präsentation.: https://norbert-pohlmann.com/app/uploads/2015/08/263-Lagebild-zur-Bedrohung-der-IT-Sicherheit-durch-Smartphones-und-Co-Prof-Norbert-Pohlmann.pdf

Postscapes. (2019). *IoT Hardware Guide*. Abgerufen am 07. Juli 2019 von https://www.postscapes.com/internet-of-things-hardware/#iot-board-comparison/

Postscapes. (2019). *IoT-Devices & Products*. Abgerufen am 18. Juni 2019 von https://www.postscapes.com/internet-of-things-award/winners/

Pratt, M. K. (16. Januar 2018). *What is Zero Trust? A model for more effective security*. Von Tutorial: https://www.csoonline.com/article/3247848/network-security/what-is-zero-trust-a-model-for-more-effective-security.html abgerufen

pwc. (2017). *2017 Global Digital IQ Survey: 10th anniversary edition.* Abgerufen am 04. Juli 2019 von https://www.pwc.com/sk/en/publikacie/assets/2017/pwc-digital-iq-report.pdf

Rackspace Support. (2016). *rackspace Support Network. Windows Server security best practices*. Abgerufen am 07. 07 2019 von https://support.rackspace.com/how-to/windows-server-security-best-practices/

Ram, P. (2018). *LPWAN, LoRa, LoRaWAN and the Internet of Things*. Abgerufen am 18. Juni 2019 von Coinmonks: https://medium.com/coinmonks/lpwan-lora-lorawan-and-the-internet-of-things-aed7d5975d5d

Rayes, A., & Salam, S. (2017). *Internet of Things - From Hype to Reality.* Cham: Springer.

RFC 4057. (2005). *IPv6 Enterprise Network Scenarios.* (IETF, Hrsg.) Von https://www.ietf.org/rfc/rfc4057.txt abgerufen

Ricker, T. (2016). *Watch a drone hack a room full of smart lightbulbs from outside the window*. Abgerufen am 08. Juli 2019 von The Verge: https://www.theverge.com/2016/11/3/13507126/iot-drone-hack

RIS. (2019). *Rechtsinformationssystem des Bundes.* Abgerufen am 18. Juni 2019 von Netz- und Informationssicherheitsgesetz: https://www.ris.bka.gv.at/Dokumente/Bundesnormen/NOR40210949/NOR40210949.html

Roman, R., Zhou, J., & Lopez, J. (2013). On the features and challenges of security and privac. *Computer Networks 57*, (S. 2266–2279). doi:10.1016/j.comnet.2012.12.018

Rost, M. (2017). Organisationen grundrechtskonform mit dem Standard-Datenschutzmodell gestalten. In A. Sowa (Hrsg.), *IT-Prüfung, Sicherheitsaudit und Datenschutzmodell* (S. 23-56). Wiesbaden: Springer Verlag.

Rout, D. (2015). Developing a Common Understanding of Cybersecurity. *ISACA Journal*(Volume 6, 2015). Abgerufen am 07. Juli 2019 von https://www.isaca.org/Journal/archives/2015/volume-6/Pages/developing-a-common-understanding-of-cybersecurity.aspx?utm_referrer=

Russel, B., & Van Duren, D. (2018). *Practical Internet of Things Security.* Birmingham: Packt Publishing.

Saleh, I., Ammi, M., & Szoniecky, S. (2018). *Challenges of the Internet of Things. Volume 7: Technology, Use, Ethics.* Wiley.

Saltzer, J. H., & Schroeder, M. D. (1975). *The Protection of Information in Computer Systems.*

Samsung. (2019). *Rethink the refridgerator*. Abgerufen am 07. Juli 2019 von https://www.samsung.com/us/explore/family-hub-refrigerator/overview/

Schanze, R. (2015). *IT-Sicherheit ist ein Prozess, kein Zustand*. Abgerufen am 06. Juli 2019 von com!professional: https://www.com-magazin.de/news/sicherheit/it-sicherheit-prozess-zustand-880292.html

Schonschek, O. (16. Dezember 2018). Was bringt ein Informations-Sicherheits-Management-System für den Datenschutz? *Datenschutz Praxis. ISMS und Datenschutz*.

Schuster, A. (2019). *Sec4You. Advanced IT-Audit Services*. Abgerufen am 07. Juli 2019 von Soll ich mein Unternehmen nach ISO 27001 zertifizieren?: https://www.sec4you.com/warum-unternehmen-27001-zertifizieren/

Shang, W., Yu, Y., Droms, R., & Zhang, L. (2016). Challenges in IoT Networking via TCP/IP Architecture. *NDN Technical Report NDN-0038, 2016.*

snyxius. (2016). *7 Internet of Things Examples That Show the Power of IoT*. Abgerufen am 18. Juni 2019 von https://www.snyxius.com/7-internet-of-things-examples-show-power-iot/

Software Testing Help. (2019). *18 Most Popular IoT Devices in 2019 (Only Noteworthy IoT Products)*. Abgerufen am 18. Juni 2019 von https://www.softwaretestinghelp.com/iot-devices/

Sood, K., Yu, S., & Xiang, Y. (2016). Software-Defined Wireless Networking Opportunities and Challenges for Internet-of-Things: A Review. *IEEE INTERNET OF THINGS JOURNAL, VOL. 3, NO. 4.* doi:10.1109/JIOT.2015.2480421

Sowa, A. (2017). *IT-Prüfung, Sicherheitsaudit und Datenschutzmodell. Neue Ansätze für die IT-Revision.* Wiesbaden: Springer Vieweg.

Stergiou, C., Psannis, K. E., Kim, B.-G., & Gupta, B. (2018). Secure integration of IoT and Cloud Computing. *Future Generation Computer Systems 78*, (S. 964–975).

Stöwer, M., & Kraft, R. (2017). IT-Sicherheitsaudits im Bereich der industriellen Produktion. In A. Sowa (Hrsg.), *IT-Prüfung, Sicherheitsaudit und Datenschutzmodell* (S. 107-125). Wiesbaden: Springer Verlag.

Tanenbaum, A. S., & Wetherall, D. J. (2012). *Computernetzwerke.* Hallbergmoos: Pearson Deutschland.

The Hacker News. (2016). *An Army of Million Hacked IoT Devices Almost Broke the Internet Today*. Abgerufen am 08. Juli 2019 von The Hacker News: https://thehackernews.com/2016/10/iot-dyn-ddos-attack.html

Thompson, C. (2015). *How drones can be used to hack your home*. Abgerufen am 08. Juli 2019 von Business Insider: https://www.businessinsider.com/how-drones-can-hack-your-home-2015-8?IR=T

Traunmüller, R. (2003). Electronic Government. *Second International Conference, EGOV 2003.* Prag.

Tretzmüller, T. (2018). *Die Auswirkungen der NIS-Richtlinie für Unternehmer.* Abgerufen am 18. Juni 2019 von Knyrim.Trieb Rechtsanwälte: https://www.kt.at/wp-content/uploads/2018/10/NIS-RL_TT_20181017_Newsletter.pdf

Tsolkas, A., & Schmidt, K. (2017). *Rollen und Berechtigungskonzepte.* Wiesbaden: Springer Vieweg.

Turton, W. (2016). *This Is Why Half the Internet Shut Down Today*. Abgerufen am 08. Juli 2019 von Gizmodo: https://gizmodo.com/this-is-probably-why-half-the-internet-shut-down-today-1788062835

Valerio, P. (2018). *Zero Trust & Network Segmentation: Keys to Securing IoT*. Abgerufen am 18. Juni 2019 von securitynow: https://www.securitynow.com/author.asp?section_id=613&doc_id=746264

Vermesan, O., & Friess, P. (2014). Internet of Things – From Research and Innovation to Market Deployment. River Publishers.

Vizard, M. (2018). *Rate of SDN adoption is slow but steady*. Abgerufen am 08. Juli 2019 von smartermsp: https://smartermsp.com/rate-sdn-adoption-slow-steady/

Voas, J. (Juni 2016). Demystifying the Internet of Things. *Computer, Vol 49, Issue 6*(10.1109/MC.2016.162), S. 80-83.

Voigt, P., & Bussche, A. v. (8. Februar 2018). Rechtsdurchsetzung und Sanktionennach der DSGVO. *EU-Datenschutz-Grundverordnung (DSGVO)*.

Wendzel, S. (2018). *IT-Sicherheit für TCP/IP und IoT-Netzwerke.* Wiesbaden: Springer Verlag.

Wieler, H. (30. Dezember 2017). *Medizinische IoT-Geräte durch interne Segmentierungs-Firewalls absichern*. Von Infopoint Security: https://www.infopoint-security.de/medizinische-iot-geraete-durch-interne-segmentierungs-firewalls-absichern/a13861/ abgerufen

Wurm, J., Hoang, K., Arias, O., Sadeghi, A.-R., & Jin, Y. (2016). *Security Analysis on Consumer and Industrial IoT Device.* IEEE.

Xiaohui, X. (2013). Study on Security Problems and Key Technologies of The Internet of Things. *International Conference on Computational and Information Sciences*, (S. 407-410). doi:10.1109/ICCIS.2013.114

Yu, T., Sekary, V., Seshany, S., Agarwaly, Y., & Xu, C. (2015). Handling a trillion (unfixable) flaws on a billion devices: Rethinking network security for the Internet-of-Things. *HotNets '15 November.* doi: http://dx.doi.org/10.1145/2834050.2834095

Zhu, Q., Wang, R., Chen, Q., Liu, Y., & Qiny, W. (2010). IOT Gateway: Bridging Wireless Sensor Networks into Internet of Things. *2010 IEEE/IFIP International Conference on Embedded and Ubiquitous Computing.* doi:DOI 10.1109/EUC.2010.58