ECONSTOR
Make Your Publications Visible.

A Service of
ZBW
Leibniz-Informationszentrum Wirtschaft
Leibniz Information Centre for Economics

Bretschneider, Wolfgang; Rieckmann, Johannes; Stuchtey, Tim; Szanto, Alexander

Research Report

Cybersicherheit als Katalysator für Innovation und Wachstum

Studien zum deutschen Innovationssystem, No. 11-2020

Provided in Cooperation with:
Expertenkommission Forschung und Innovation (EFI)

Suggested Citation: Bretschneider, Wolfgang; Rieckmann, Johannes; Stuchtey, Tim; Szanto, Alexander (2020) : Cybersicherheit als Katalysator für Innovation und Wachstum, Studien zum deutschen Innovationssystem, No. 11-2020, Expertenkommission Forschung und Innovation (EFI), Berlin

This Version is available at:
https://hdl.handle.net/10419/222526

Standard-Nutzungsbedingungen:

Die Dokumente auf EconStor dürfen zu eigenen wissenschaftlichen Zwecken und zum Privatgebrauch gespeichert und kopiert werden.

Sie dürfen die Dokumente nicht für öffentliche oder kommerzielle Zwecke vervielfältigen, öffentlich ausstellen, öffentlich zugänglich machen, vertreiben oder anderweitig nutzen.

Sofern die Verfasser die Dokumente unter Open-Content-Lizenzen (insbesondere CC-Lizenzen) zur Verfügung gestellt haben sollten, gelten abweichend von diesen Nutzungsbedingungen die in der dort genannten Lizenz gewährten Nutzungsrechte.

Terms of use:

Documents in EconStor may be saved and copied for your personal and scholarly purposes.

You are not to copy documents for public or commercial purposes, to exhibit the documents publicly, to make them publicly available on the internet, or to distribute or otherwise use the documents in public.

If the documents have been made available under an Open Content Licence (especially Creative Commons Licences), you may exercise further usage rights as specified in the indicated licence.

WWW.ECONSTOR.EU

Mitglied der Leibniz-Gemeinschaft

BIGS
BRANDENBURGISCHES INSTITUT
für GESELLSCHAFT und SICHERHEIT

Cybersicherheit als Katalysator für Innovation und Wachstum

Wolfgang Bretschneider, Johannes Rieckmann, Tim Stuchtey, Alexander Szanto

Weitere Mitwirkung:

Luise Bendfeldt (Humankapital), Josef Lenglachner (Institutionen, Marktversagen), Anna Peters (Experten-interviews) sowie Friederich Boeker, Caroline von der Heyden, Trystan Stahl

---

Studien zum deutschen Innovationssystem Nr. 11-2020

Brandenburgisches Institut für Gesellschaft und Sicherheit

Februar 2020

Diese Studie wurde im Auftrag der Expertenkommission Forschung und Innovation (EFI) erstellt. Die Ergebnisse und Interpretationen liegen in der alleinigen Verantwortung der durchführenden Institute. Die EFI hat auf die Abfassung des Berichts keinen Einfluss genommen.

Studien zum deutschen Innovationssystem

Nr. 11-2020

ISSN 1613-4338

Herausgeber:

Expertenkommission Forschung und Innovation (EFI)

Geschäftsstelle:
c/o Stifterverband für die Deutsche Wissenschaft
Pariser Platz 6
10117 Berlin

Alle Rechte, insbesondere das Recht der Vervielfältigung und Verbreitung sowie die Übersetzung, vorbehalten. Kein Teil des Werkes darf in irgendeiner Form (durch Fotokopie, Mikrofilm oder ein anderes Verfahren) ohne schriftliche Genehmigung der EFI oder der Institute reproduziert oder unter Verwendung elektronischer Systeme gespeichert, verarbeitet, vervielfältigt oder verbreitet werden.

Kontakt und weitere Informationen:

Brandenburgisches Institut für Gesellschaft und Sicherheit gGmbH
Geschäftsführender Direktor: Dr. Tim H. Stuchtey

Dianastraße 46
14482 Potsdam

Telefon: +49-331-704406-0
Telefax: +49-331-704406-19

E-Mail: direktor@bigs-potsdam.org
www.bigs-potsdam.org

Danksagung

Bei der Erstellung dieser Studie bekamen wir die Unterstützung zahlreicher, hier anonym bleibender Experten aus Unternehmen, Verbänden, staatlichen Einrichtungen und der Wissenschaft. Ganz besonders danke ich Christian Köhler für seine Unterstützung, insbesondere für den Zugang zu diesen Experten. Außerdem bedanke ich mich bei den Teilnehmern des PizzaSeminars vom 20.08.2019, mit denen wir die ersten Analysen und Handlungsempfehlungen diskutiert haben. Ihnen allen gilt unser Dank, dass sie meiner Devise gefolgt sind:

Wissen ist das einzige Gut, das durch Teilung mehr wird.

Für den Verlauf der Analyse waren die Diskussionen mit den Mitgliedern sowie den Mitarbeiterinnen und Mitarbeitern der Expertenkommission Forschung und Innovation (EFI) von großem Nutzen. Auch ihnen gilt mein Dank für Ihr Vertrauen und die Argumente, die sie uns mit auf den Weg gegeben haben. Mein ganz besonderer Dank gilt dabei Dr. Jano Costard für viele Anregungen und die konstruktive Begleitung dieser Studie.

Für die dennoch verbliebenen Fehler in dieser Studie tragen alleine die Autoren die Verantwortung.

Inhaltsverzeichnis

Abkürzungsverzeichnis iv

Abbildungsverzeichnis vii

Tabellenverzeichnis ix

0 Kurzfassung/Executive Summary 1

1 Einleitung 4

2 Grundlagen zur Cybersicherheit 5

2.1 Was ist Cybersicherheit? 8

2.2 Cybersicherheit als Funktion von Bedrohung und Schutz 9

2.3 Bedrohungsakteure 16

2.4 Fallstudien 22

2.5 Cyberangriffe – Trends der Gegenwart und Zukunft 27

2.6 Schutz und optimales Sicherheitsniveau 31

2.7 Mehrstufigkeit des Schutzes 41

2.7.1 Rolle des Staates 44

2.7.2 Märkte für Cybersicherheit 46

2.7.3 Institutionen der Cybersicherheit in Deutschland 50

2.8 Risikomanagement und Cyberversicherung 58

3 Allokatives Marktversagen auf privaten Märkten für IT-SP/PSK 62

3.1 Informationsdefizite 62

3.1.1 Zur Entscheidungssituation über Cybersicherheits-Investition von Schutzguteigentümern 63

3.1.2 Zur Bedrohungsinformation 67

3.1.3 Zur Qualitätsinformation 73

3.1.4 Vorläufige Schlussfolgerungen und Handlungsempfehlungen 79

3.2 Externe Effekte 81

4 *Enabler*- und *Driver*-Analyse im Lichte von Innovation und Wachstum 89

4.1 *Enabler*-Analyse im Lichte von Innovation und Wachstum 89

4.1.1 Beratungsangebote 96

4.1.2 Standardisierung 97

4.2 *Driver*-Analyse im Lichte von Innovation und Wachstum 101

5 Humankapital: Mangel an IT-Fachkräften als Wachstumshemmnis 119

5.1 Zum Status quo 120

5.2 Studiengänge in IT-Sicherheit 123

5.3 Handlungsempfehlungen 131

6. Zusammenfassung & Handlungsempfehlungen 133

Anhang 141

Literaturverzeichnis 145

Abkürzungsverzeichnis

ACS	Allianz für Cybersicherheit
AfA	Absetzung für Abnutzung
APT	Advanced Persistent Threat
BaFin	Bundesanstalt für Finanzdienstleistungsaufsicht
BAMAD	Bundesamt für den Militärischen Abschirmdienst
BBK	Bundesamt für Bevölkerungsschutz und Katastrophenhilfe
BDI	Bundesverband der Deutschen Industrie e. V.
BfV	Bundesamt für Verfassungsschutz
BIGS	Brandenburgisches Institut für Gesellschaft und Sicherheit, Potsdam
Bitkom	Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V.
BKA	Bundeskriminalamt
BMI	Bundesministerium des Innern, für Bau und Heimat
BMVg	Bundesministerium der Verteidigung
BMWi	Bundesministerium der Wirtschaft
BND	Bundesnachrichtendienst
BPol	Bundespolizei
BSI	Bundesamt für Sicherheit in der Informationstechnik
BSIG	Gesetz über das Bundesamt für Sicherheit in der Informationstechnik
BW	Bundeswehr
CaaS	*Cybercrime-as-a-service*
CEN	Comité Européen de Normalisation
CERT-Bund	Computer Emergency Response Team des Bundes
DARPA	Defense Advanced Research Projects Agency
DCSO	Deutsche Cyber-Sicherheitsorganisation

DESTATIS	Statistisches Bundesamt
DDoS	*Distributed-Denial-of-Service*
DHS	The United States Department of Homeland Security
DIN	Deutsches Institut für Normung e. V.
EE	Externe Effekte
EGC	European Governmental CERTs Group
ENISA	The European Union Agency for Cybersecurity
FuE	Forschung und Entwicklung
GDV	Gesamtverband der Deutschen Versicherungswirtschaft
GK	Grenzkosten
GN	Grenznutzen
IEC	International Electrotechnical Commission
IKT	Informations- und Kommunikationstechnik
IoT	*Internet of Things* (Internet der Dinge)
IP	*Intellectual Property* (geistiges Eigentum)
ISMS	Informationssicherheitsmanagement
ISO	International Organization for Standardization
IT	Informationstechnologie, informationstechnologisch
ITSiBe	IT-Sicherheitsbeauftragter (Ausbildung, Bitkom Akademie)
IT-SP/PSK	IT-Sicherheitsprodukte bzw. IT-Produkte mit Sicherheitskomponente
IT-TK	Informationstechnologie und Telekommunikation
ITU	International Telecommunication Union
IU	Innovative Unternehmen
KdoCIR	Kommando Cyber- und Informationsraum der Bundeswehr
KfW	Kreditanstalt für Wiederaufbau
KI	Künstliche Intelligenz

KITS	Koordinierungsstelle IT-Sicherheit bei DIN
KMU	Kleine und Mittelständische Unternehmen
KRITIS	Kritische Infrastruktur
LSI	Landesamt für Sicherheit in der Informationstechnik
ML	Maschinelles Lernen
PCP	Pre-Commercial Procurement
P SD2	Payment Services Directive2
PSK	Produkte mit Sicherheitskomponente
ROSI	Return on Security Investment
SP	Sicherheitsprodukte
UniBw	Universität der Bundeswehr München
WID	Warn- und Informationsdienst
WifOR	Wirtschaftsforschungsinstitut
WSC	World Standards Cooperation
WTO	World Trade Organization
ZKA	Zollkriminalamt

Abbildungsverzeichnis

Abbildung 1 Cybersicherheit als Funktion aus Bedrohung und Schutz 9
Abbildung 2 Angriff und Schutz (einstufig) 10
Abbildung 3 Bedrohung und Schutz 32
Abbildung 4 Optimaler Einsatz von Schutzleistungen 34
Abbildung 5 Cyberschäden der Industrie pro Jahr 37
Abbildung 6 Schäden durch Cybercrime gem. Bundeslagebild des BKA 38
Abbildung 7 Ausgaben für IT-Sicherheit in Deutschland (in Mrd. EUR) 39
Abbildung 8 Gesamtausgaben für Cybersecurity in den USA von 2010 bis 2018 (in Mrd. USD) .. 40
Abbildung 9 Angriff und Schutz auf Stufen unterschiedlicher Präventivität 42
Abbildung 10 Akteure auf den Märkten um den Markt für IT-SP/PSK 47
Abbildung 11 Schutzguteigentümer zwischen Cyberproblemen und Anbietern von Sicherheitsmaßnahmen / Versicherungen 64
Abbildung 12 Optimale Informiertheit bzw. Unwissenheit als Funktion aus GK und GN der Informationsbeschaffung 66
Abbildung 13 Wunsch nach einem genaueren periodischen Lagebild 69
Abbildung 14 Transfer der Bedrohungsinformation über zwei Stufen 70
Abbildung 15 Nachfrageverhalten ohne asymmetrische Informationsverteilung 74
Abbildung 16 Nachfrageverhalten mit asymmetrischer Informationsverteilung 74
Abbildung 17 Ergebnisse der Cybersicherheits-Umfrage 77
Abbildung 18 Direkter Vergleich der Antworten 78
Abbildung 19 Umfang/Qualität der Sicherheitsmaßnahmen und externer Nutzen 82
Abbildung 20 Umfang der Digitalisierung und externe Kosten 83
Abbildung 21 Digitalisierungsumfang und Sicherheitsmaßnahmen als Determinanten für Externalitäten 84
Abbildung 22 Positive und negative externe Effekte zwischen Digitalisierungs- und Sicherheitswachstum 85
Abbildung 23 Innovationsintensität nach Branche 90
Abbildung 24 Betroffene Unternehmen nach Branchen 90
Abbildung 25 Meldeaufkommen von KRITIS-Betreibern 91
Abbildung 26 Betroffene Unternehmen nach Betriebsgrößenklassen 92

Abbildung 27 Grad der Digitalisierung – gesamt und nach Betriebsgrößenklasse 92
Abbildung 28 Kuznets-Kurve beim Zusammenhang von Digitalisierungsgrad und Betroffenheit von Cyberangriffen 93
Abbildung 29 Nationale und europäische Sicherheitsforschung im Vergleich 105
Abbildung 30 Angaben zu Wachstumsentwicklung und -erwartung bis 2019, nach Angebotsportfolio, im Vergleich zur Gesamtwirtschaft 112
Abbildung 31 KMU/Großunternehmen und Hochschulforschung/Forschungsinstitute in der IKT im Vergleich 116
Abbildung 32 Anzahl der beschäftigten IT-Fachleute in Deutschland 120
Abbildung 33 Abschlüsse der beschäftigten IT-Fachleute 121
Abbildung 34 Anzahl der Informatikstudierenden an deutschen Hochschulen zwischen 2010 und 2018 125
Abbildung 35 Sicherheitsnachhaltiger und nicht-sicherheitsnachhaltiger Wachstumspfad 134

Tabellenverzeichnis

Tabelle 1 Zielstellungstyp und Spezifitätsgrad von Angriffen 11

Tabelle 2 Übersicht der Arten von Cyberangriffen 21

Tabelle 3 Relevante Behörden und Institute der Cybersicherheitsarchitektur 58

Tabelle 4 Bedrohungsinformationen als privates und als öffentliches Gut 68

Tabelle 5 Technologiereifegrad 106

Tabelle 6 Anzahl der Informatikstudierenden an deutschen Hochschulen 2010 bis 2018 124

Tabelle 7 Studiengänge im Bereich IT-/Cybersicherheit an Universitäten und Fachhochschulen in Deutschland 129

0 Kurzfassung/Executive Summary

Die Sicherheit eines Landes gilt als einer der wichtigsten Standortfaktoren, die über Wirtschaftswachstum und letztlich den Wohlstand einer Gesellschaft entscheiden. Mangelt es an Sicherheit, dann werden langlaufende Investitionen möglicherweise unrentabel und unterlassen. Produktivitätssteigerung unterbleibt und Wachstumspotential wird nicht ausgeschöpft.

Die Digitalisierung von Wirtschaftsprozessen führt dazu, dass Unternehmen immer mehr Schnittstellen mit dem Cyberraum haben und die Wertschöpfung in diesen verlegt wird. Damit setzen sich Unternehmen neuen Risiken aus, die sie im Rahmen ihres Risikomanagements bewerten und mit denen sie umgehen müssen. Grundsätzlich stehen zum Schutz vor Cyberrisiken zahlreiche technische, organisatorische und personelle Optionen zur Verfügung, die entweder durch das Unternehmen selbst umgesetzt oder von darauf spezialisierten Dritten eingekauft werden können. In jedem Fall entstehen dem zu schützenden Unternehmen, wie in der Kohlenstoffwelt, beim Schutz vor Bedrohungen in der digitalen Welt Kosten.

In dieser Studie wird untersucht, ob mangelnde Cybersicherheit in Deutschland dazu führt, dass hier ansässige Unternehmen mögliche Produktivitäts- und Wachstumspotentiale nicht ausschöpfen, die durch eine Digitalisierung der Wertschöpfungskette möglich wären. Zudem wird analysiert, ob IT-Sicherheitsunternehmen in Deutschland, also jene Unternehmen, die Schutzleistungen vor Cyberbedrohungen anbieten, noch stärker wachsen könnten und damit selbst einen größeren Anteil zu Innovation und Wachstum in Deutschland beitragen können.

Es besteht der begründete Anspruch von Haushalten und Unternehmen, dass der Staat sein Gewaltmonopol auch im Cyberraum durchsetzt und für die Durchsetzung des Rechts auch in diesem Bereich Sorge trägt. Diesem Anspruch wird der Staat noch ungenügend gerecht; und von daher kann man hier von einem Staatsversagen sprechen, das es mit Hilfe der Sicherheitspolitik zu heilen gilt. Eine Analyse von Angebot und Nachfrage von Cyberschutzleistungen zeigt aber auch, dass hier ebenfalls Tatbestände von Marktversagen vorliegen und wirtschaftspolitische Eingriffe notwendig sind. Asymmetrische Informationsverteilung und erhebliche Informationsdefizite über das Ausmaß der Bedrohung eines Unternehmens im Cyberraum machen es unmöglich, den optimalen Umfang und die Art des Schutzes im Rahmen des Risikomanagements festzulegen. Zum Teil erhebliche positive externe Effekte von Schutzmaßnahmen führen zu einem unterkritischen Umfang von Cyberschutzmaßnahmen. Bei alledem ist die Messbarkeit von Cybersicherheit ein grundsätzliches (auch methodisches) betriebs- und volkswirtschaftliches Problem.

Mit zunehmender Digitalisierung muss auch der Aufwand für und Umfang der Schutzleistungen parallel steigen, damit die Cybersicherheit nicht abnimmt. Damit die konkreten Maßnahmen und der Umfang des Schutzes bestimmt werden können, müssen verlässliche Informationen über Art und Umfang von Bedrohungen im Cyberraum bereitgestellt werden. Der BSI-Lagebericht ist diesbezüglich weiterzuentwickeln. Auch über die Effektivität einzelner Schutzmaßnahmen herrscht Unsicherheit, die z.B. mit Hilfe von Zertifikaten oder Standards gemildert werden kann. Gleiches gilt letztlich auch für herkömmliche IoT-Produkte, deren Schutzniveau und das Wissen darüber durch solche Maßnahmen, aber auch durch klare Haftungsregelungen, verbessert werden können.

Die zum Teil erheblichen positiven externen Effekte von Schutzleistungen, die Haushalte und Unternehmen vornehmen, sollten durch entsprechende Förderprogramme bis hin zur freien Zurverfügungstellung basaler Schutzleistungen kompensiert werden. Auch eine Verkürzung der Abschreibungsdauer von IT-Sicherheitsprodukten kann Unternehmen deren Anschaffung erleichtern und eine schnellere Modernisierung fördern. Ein weiterer Ausbau der Forschungsförderung zum Thema IT-Sicherheit stößt wegen des ungenügenden Angebots einschlägiger Wissenschaftler am Arbeitsmarkt an Grenzen. Bei Forschungs- und Entwicklungsprogrammen sind aber neben der Spitzenforschung auch solche Projekte zu fördern, die dem einfachen Nutzer digitaler Produkte und Dienstleistungen einen sicheren Umgang ermöglichen.

Der Nachfrageüberhang auf dem Arbeitsmarkt für IT-Fachkräfte ist ein bekanntes Problem, welches das Ausschöpfen von Innovationspotentialen behindert und eine erhebliche Wachstumsbremse darstellt. Dem Mangel an qualifiziertem Personal lässt sich u.a. durch eine Senkung der Eintrittshürden bei Studien- und Ausbildungsgängen mildern, vor allem wenn es um Abschlüsse von ausländischen Bewerbern geht. Ebenso können mit Hilfe einer fokussierten Studienförderung junge Leute in den Bereich der Cybersicherheit gezogen werden. Auch der nichtakademische Aus- und Weiterbildungsbereich muss besser adressiert werden. Schon heute ist ein C*rowding-Out*-Effekt durch die stark gestiegene staatliche und private Nachfrage nach IT-Fachpersonal erkennbar.

Neben technischen Lösungen und besser ausgebildeten Personal ist ein effizienter Risikotransfer bzw. eine adäquate Risikominderung in Form von Versicherungslösungen ein weiter wichtiger Baustein des Risikomanagements. Erst wenn die finanziellen Folgen eines möglichen Cyberangriffs für ein Unternehmen beherrschbar und nicht mehr existenzbedrohend sind, werden

Digitalisierungsprojekte umgesetzt. Die Versicherungsbedingungen und deren Weiterentwicklung auf Grundlage der Daten aus Schadensfällen machen Versicherungen zu einem wichtigen Quasi-Regulierer.

Der hohe Anteil kleiner Unternehmen in der deutschen IT-Sicherheitswirtschaft führt dazu, dass Skaleneffekte und Verbundvorteile nicht hinreichend ausgenutzt werden. Die mit der Unternehmensgröße einhergehende geringe Kapital- und Personalkraft führt zudem dazu, dass deutsche Anbieter bei langlaufenden Ausschreibungen für große Beschaffungs- und Betreiberprojekte (z.B. von Behörden oder Bundeswehr) oftmals nicht mitbieten können. Ein Systemintegrator könnte diesen Mangel heilen, doch fehlt ein solcher bislang in Deutschland. Der Staat kann diesem systemischen Problem durch kleinere Losgrößen bei Ausschreibungen für IT-Sicherheitsdienstleistungen begegnen. Gilt es aber, innovativen Produkten oder Lösungen aus Deutschland zum Marktdurchbruch zu verhelfen, dann trifft das Gegenteil zu. Großvolumige Ausschreibungen helfen, Skaleneffekte überhaupt erst auszunutzen. Hierfür sollte auch mehr Gebrauch von innovativen Beschaffungsverfahren von Seiten staatlicher Institutionen gemacht werden. In diesem Zusammenhang wäre es sowohl aus sicherheitspolitscher Perspektive als auch für die internationale Wettbewerbsfähigkeit Deutschlands ratsam, bestehende IT-Cluster zu stärken, um die *Spillover*-Effekte der persönlichen Beziehungen und schnellen Interaktionen von Experten in der interdisziplinären Zusammenarbeit auszunutzen.

Damit das volle Potential der Digitalisierung ausgeschöpft werden kann, sind Sicherheitsaspekte sowohl in betriebswirtschaftliche als auch in politische Entscheidungen zu integrieren. Sollen deutsche IT-Sicherheitsunternehmen einen stärkeren Wachstumsbeitrag liefern, müssen sie international wettbewerbsfähig sein und sich dem Wettbewerb stellen können und dürfen. Das setzt Unternehmens- wie auch Marktgröße voraus. Die Diskussion über staatliche Hintertüren in deutschen Softwareprodukten oder besonders restriktive Exportkontrollen sind hier kontraproduktiv. Insofern gilt es, die richtige Balance zwischen sicherheits- und wirtschaftspolitischen Bedürfnissen zu finden.

1 Einleitung

Cybersicherheit hat in den letzten Jahren auf der sicherheitspolitischen, aber auch der wirtschaftspolitischen Agenda zunehmend an Bedeutung gewonnen. Spektakuläre Angriffe wie durch den legendären Stuxnet-Virus oder der Blackout in der Ukraine im Jahr 2015 haben die Politik bewegt, Sicherheitsbehörden und Bundeswehr bei ihren Cyberfähigkeiten zu ertüchtigen. Datendiebstahl und die Veröffentlichung sensibler Daten haben dazu geführt, dass sich Unternehmen verstärkt damit beschäftigen, wie Sie ihre Unternehmensgeheimnisse und Produktionsanlagen vor Diebstahl, Missbrauch und Sabotage schützen können. Nicht zuletzt die stark wachsende Branche der IT-Sicherheitsunternehmen und deren Beitrag zum volkswirtschaftlichen Wohlstand haben die Aufmerksamkeit von Wirtschafts- und Sicherheitspolitik erregt.

Welchen Einfluss hat (fehlende) Cybersicherheit auf die Innovationsfähigkeit und das Wirtschaftswachstum der Bundesrepublik Deutschland? Welchen Beitrag hierzu leistet die nationale IT-Sicherheitswirtschaft? Und was legitimiert einen staatlichen Eingriff in den Markt für Cybersicherheitsprodukte und -dienstleistungen? Diesen Fragen gehen wir in der vorliegenden Studie nach. Dabei wird nicht der Anspruch auf eine abschließende Antwort erhoben. Vielmehr soll ein hilfreicher Beitrag aus der wirtschaftswissenschaftlichen Perspektive zu dieser Debatte geleistet werden. Hierzu wird zunächst der Begriff Cybersicherheit operationalisiert und anschließend die Bedrohung und der mögliche Schutz im Cyberraum analysiert. In Kapitel 3 werden die Gründe für ein mögliches Marktversagen aufgezeigt, aus denen sich überhaupt eine Legitimität staatlicher Eingriffe in den IT-Sicherheitsmarkt ableiten lässt. Kapitel 4 widmen wir uns zunächst der Bedeutung der Cybersichersicherheit im Kontext der Digitalisierung der Wirtschaft, um anschließend auf das Wachstum und die Hemmnisse der IT-Sicherheitswirtschaft einzugehen. Kapitel 5 widmet sich dem besonders bedeutsamen Problem der Humankapitalknappheit auf dem Arbeitsmarkt im Bereich Cybersicherheit. Im Fazit zeigen wir mögliche Handlungsempfehlungen auf, welche die die Diskussion bereichern können.

2 Grundlagen zur Cybersicherheit

In der Debatte um Cybersicherheit in der Wirtschaft standen in den vergangenen Jahren besonders die Sektoren der sog. Kritischen Infrastruktur (KRITIS), im Mittelpunkt. Mit dem ersten IT-Sicherheitsgesetz wurde 2015 eine rechtliche Grundlage geschaffen, mit deren Hilfe der Schutz vor Cyberangriffen sowie Meldepflichten rechtlich geregelt wurden. Die aktuelle Debatte und die Vorlage eines sog. „IT-Sicherheitsgesetzes 2.0“ indizieren, dass für die Regulierung der KRITIS ein *dynamisches* Regelwerk vorgesehen ist, mithin eine Weiterentwicklung der rechtlichen Normierung im Zeitablauf. Trotz möglicher Ausweitungen des Anwendungsbereiches dürfte und sollte der Begriff der KRITIS gem. § 2 Abs. 10 des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik (BSIG) sich auf „Einrichtungen, Anlagen oder Teile davon, die […] von hoher Bedeutung für das Funktionieren des Gemeinwesens sind, weil durch ihren Ausfall oder ihre Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit eintreten würden.“[1] beziehen (und beschränken). Die Zielstellung richtet sich somit vor allem auf Cyberbedrohungen, die eine *erhebliche Auswirkung auf das gesellschaftliche Leben und die Volkswirtschaft haben.* Es werden also wirtschaftliche Unternehmen in den Blick genommen, deren Ausfall kurzfristig zu negativen gesellschaftlichen Folgen führen kann.

Darüber hinaus aber gilt es, gerade auch jenseits (sicherheits-)„kritischer“ Unternehmen die wirtschaftlichen, mittel- und langfristigen Zielstellungen Wachstum und Innovation unter den neuen und dynamischen Bedingungen in den Blick zu nehmen. Schließlich kann das volkswirtschaftliche Wachstumspotenzial der Digitalisierung erst dann voll ausgeschöpft werden, wenn den damit einhergehenden Bedrohungen im Cyberraum angemessen begegnet wird. Mit anderen Worten führt eine hinreichende Cybersicherheit dazu, dass sich die Innovationskraft entfalten kann und auf dieser Grundlage zusätzliches Wachstum entsteht. Damit einher gehen weitere ökonomische Ziele, wie eine hohe Beschäftigung, Wohlstand und die Erzielung von Standortvorteilen der Bundesrepublik im internationalen Wettbewerb. Im Gegensatz zum KRITIS-Ansatz geht es hier somit um volkswirtschaftlich mittel- und langfristige, mithin „indirekte“, aber nichtsdestotrotz gesellschaftlich äußerst relevante Effekte.[2]

[1] Im Gesetz werden zunächst die einzelnen Sektoren aufgelistet. Dies sind „die Sektoren Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung sowie Finanz- und Versicherungswesen“.

[2] Es ist zu erwarten, dass eine angemessene Regulierung der KRITIS ebenfalls zu diesen mittel- und langfristigen Effekten beiträgt. Hier aber sollen gerade auch alle anderen wirtschaftlichen Sektoren betrachtet werden, deren

Vor diesem Hintergrund geht die vorliegende Studie den Fragen nach,

- wie Cybersicherheit als Katalysator für Innovation und Wachstum wirken kann,
- welche Herausforderungen dabei für Wirtschaftssubjekte und Volkswirtschaft bestehen und
- wie die Politik Einfluss nehmen kann, um diesen Herausforderungen wirksam zu begegnen.

Dabei wird eine doppelte Perspektive eingenommen.

(i) Mit einer *Enabler*-Perspektive wird der Blick auf Unternehmen aller Sektoren außer der IT-Sicherheitswirtschaft gerichtet, die sich einer Cyberbedrohung ausgesetzt sehen und damit umzugehen haben. Dabei werden besonders Bedingungen und Bedrohungen *innovativer* Unternehmen betrachtet; d.h.

a. Unternehmen, für die geistiges Eigentum (*intellectual property*, IP) als Kapital im Mittelpunkt des Geschäftserfolgs steht, bzw. die selbst Forschung und Entwicklung (FuE) betreiben, und
b. Unternehmen, deren Kerngeschäft auf einer innovativen Idee beruht, die nicht notwendigerweise so eng technisch gefasst ist wie unter a.

(ii) Mit der *Driver*-Perspektive wird dagegen das Branchenwachstum der Anbieter von IT-Sicherheitsdienstleistungen, IT-Sicherheitsprodukten (IT-SP) bzw. IT-Produkten mit Sicherheitskomponenten (PSK) in den Blick genommen.[3] Für sie ergeben sich offenkundig Wachstumschancen aufgrund der Nachfrage von der *Enabler*-Seite. Dabei ist zu berücksichtigen, dass (auch) diese Unternehmen im internationalen Wettbewerb stehen.

Der Umgang sowohl für Wirtschaftssubjekte wie für die Politik mit neuen und derart dynamischen Herausforderungen wie der Cybersicherheit ist grundsätzlich durch eine gewisse zeitliche Verzögerung charakterisiert. Angesichts der Wucht der Herausforderungen sind in den letzten

---

Umgang mit Cybersicherheit eben auch einen Einfluss auf diese Zielstellung haben. – Für das einzelne Nicht-KRITIS-Unternehmen können die Cyberbedrohung im Übrigen sehr wohl gravierende *kurzfristige* Konsequenzen haben, insbesondere auch den Konkurs. Der Unterschied zu einem KRITIS-Unternehmen besteht darin, dass das herkömmliche Unternehmen nach Einschätzung des Regulierers *nicht* „von hoher Bedeutung für das Funktionieren des Gemeinwesens“ ist und der Ausfall entsprechend *nicht* zu „Gefährdungen für die öffentliche Sicherheit“ führt (§ 2 Abs. 10 Nr. 2 BSIG).

[3] Im weiteren Verlauf der Studie wird aufgrund dieser Abkürzungen in weiten Teilen von einem „Markt für IT-SP/PSK“ die Rede sein. Da IT-Sicherheitsdienstleistungen heute oft im Rahmen von Systemlösungen gemeinsam mit IT-SP/PSK angeboten werden, werden diese im Folgenden nicht weiter von letzteren unterschieden, sondern sind – so nicht explizit separat angesprochen – als integraler Bestandteil des Angebotsspektrums zu verstehen.

Jahren vielfach „Weckrufe“ an unternehmerische Entscheidungsträger gerichtet worden.[4] Im Mittelpunkt zahlreicher Kampagnen zur Erhöhung der Cybersicherheit stand und steht regelmäßig die Bewusstseinsschaffung gerade in der obersten Managementebene für die Notwendigkeit eines hinreichenden Schutzes vor Cyberbedrohungen. Während in der Vergangenheit unisono das Bewusstsein als unzureichend beschrieben wurde, scheint es hier jedoch mittlerweile zu einer Verbesserung gekommen zu sein. Diesen Schluss kann man zumindest ziehen, wenn man die kürzlich erschienenen deutlich positiveren Einschätzungen mit in Betracht zieht.[5] Grundsätzlich scheint es in jedem Fall plausibel zu sein, das „Bewusstsein für die Bedeutung der IT-Sicherheit weiter [zu, Erg. d. Verf.] schärfen“.[6] Dies gilt nicht zuletzt, weil es bislang nur wenigen Unternehmen gelungen ist, ihren erhöhten Schutzaufwand und das damit einhergehende höhere Sicherheitsniveau ihrer Produkte und Dienstleistungen den Kunden als echten Mehrwert zu verkaufen, für den letztere auch eine höhere Zahlungsbereitschaft zeigen.[7]

Ein der Problemlage angemessenes Bewusstsein bei den Akteuren ist sicher eine notwendige Voraussetzung des produktiven Umgangs mit den durch Cyberbedrohungen entstehenden Herausforderungen. Das Bewusstsein allein ist aber bei Weitem nicht hinreichend, wenn auf den Märkten für IT-SP/PSK strukturelle Defizite bestehen, darunter insbesondere auch solche im Zusammenhang mit Marktversagen. Denn dies sind Hemmnisse, die sich mit bloßen Appellen an die Akteure nicht beheben lassen.[8] Hier ist eine genauere (Marktversagens-) Analyse notwendig, um zu eruieren, inwieweit eine Ergänzung privaten Handelns durch staatliche Aktivitäten angezeigt ist. Diese Perspektive soll im weiteren Verlauf der vorliegenden Studie verfolgt werden.

---

[4] Dies geschah etwa mit Sätzen wie: „Es ist Zeit aufzuwachen.“ Hillebrand et al. 2017, S. 3.

[5] Das Bundesamt für Sicherheit in der Informationstechnik (BSI) kommt in seinem Lagebericht 2018 aufgrund von Umfragen zu dem Schluss: „Das Bewusstsein für die Gefahren, die den Unternehmen aus dem Cyberraum drohen, ist hoch.“ BSI 2018, S. 15. Das Autorenteam Wrede et al. (2018) hingegen kommt nach Experteninterviews mit Vertretern der Versicherungs- und Beratungsbranche sowie Interessenverbänden zu dem Ergebnis, „dass in der Unternehmenspraxis ein mangelndes Risikobewusstsein für Cyberbedrohungen einen bedeutenden Einflussfaktor für die IT-Sicherheit darstellt und Cyberrisiken im Risikomanagement häufig unzureichend berücksichtigt werden.“ Ebd., S. 405.

[6] BSI 2018, S. 4.

[7] So ist etwa davon die Rede, dass sich die Bedrohungslage „massiv zugespitzt“ habe (Bartsch/Frey 2017, S. 12). Andernorts ist etwa von einer „hochdynamischen, extrem wandlungsfähigen Risikolandschaft“ (Wrede et al., S. 405) die Rede.

[8] Eine ähnliche Debattenstruktur ist aus der Umweltpolitik bekannt. Auch dort wird von ökonomischer Seite mit Recht darauf hingewiesen, dass mehr Umweltbewusstsein bei den Wirtschaftssubjekten (allein) bei Weitem keinen dem (Umwelt-) Problem angemessenen Effekt erzielt. Bloße Appelle laufen grundsätzlich leer (vgl. statt vieler Fritsch 2018, S. 105 f.).

2.1 Was ist Cybersicherheit?

Während im nächsten Abschnitt mit konzeptionellen auch begriffliche Grundlagen erarbeitet werden, soll bereits an dieser Stelle der grundlegende Begriff der Cybersicherheit konkretisiert werden. In weiten Teilen der Literatur hat sich die Konvention durchgesetzt, dass unter dem Begriff der – früher als Problem und Begriff dominanten – IT-Sicherheit lediglich *technische* Risiken und Sicherheitsaspekte verstanden werden. Demgegenüber beinhaltet alles, was nun unter dem Präfix „Cyber-“ diskutiert wird, integrativ auch die vielfältigen nicht-technische Aspekte, die im Umfeld der neuen technischen Möglichkeiten liegen.[9] Somit sind alle Probleme und Fragen der IT-Sicherheit ein Teil (eine Teilmenge) der Fragen um die Cybersicherheit: „IT-Sicherheit ist Teil der Cybersicherheit, aber Cybersicherheit ist viel komplexer und schließt neben den technischen auch nicht-technische Aspekte wie organisatorische, physische und personelle Aspekte ein.“[10]

Eine in diesem Sinne integrative Perspektive wird auch eingenommen, wenn im Folgenden Cybersicherheit als Funktion aus Bedrohung und Schutz verstanden wird.[11] Auf der einen Seite (links in der Abbildung) ist zu berücksichtigen, dass Bedrohungen, durch die sich das Cybersicherheitsproblem manifestiert, von unterschiedlichen Akteuren ausgehen können. Auf der anderen Seite können die Bedrohungen mit unterschiedlichen Schutzmaßnahmen der Wirtschaftssubjekte zumindest teilweise kompensiert werden (rechts in der Abbildung). Dazu gehören neben technologischen Lösungen (Hard- und Software) auch Lösungen des Risikotransfers für potenzielle Schäden (Cyberversicherungen) sowie Investitionen in Humankapital (*Awareness*, (Fort-)Bildung, Übungen auf *Cyberranges* etc.).

[9] Vgl. etwa Bartsch und Frey 2017, S. vii.

[10] Bartsch und Frey 2017, S. 8.

[11] Vgl. Abbildung 1.

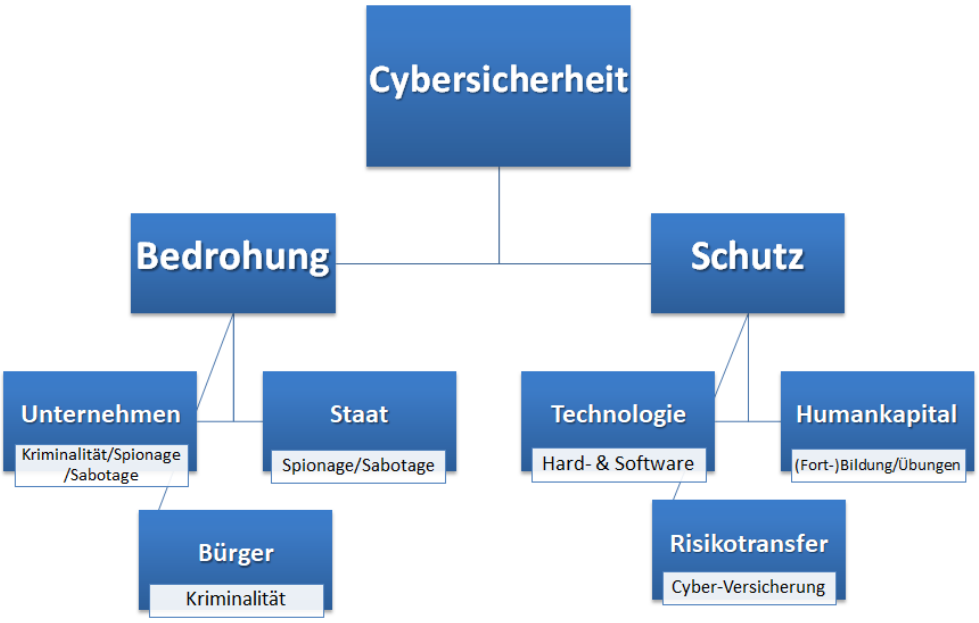


Abbildung 1 Cybersicherheit als Funktion aus Bedrohung und Schutz
Quelle: Schematisches Konzept des Brandenburgischen Instituts für Gesellschaft und Sicherheit, BIGS.

Da es noch keine konsolidierte Begrifflichkeit zu einem, insbesondere ökonomisch geprägten, Verständnis von Cybersicherheit gibt, sollen in diesem Abschnitt entsprechende Grundlagen bereitgestellt werden. Dabei schließen die Überlegungen an das Grundkonzept des Brandenburgischen Instituts für Gesellschaft und Sicherheit (BIGS) von Sicherheit als Funktion aus Bedrohung und Schutz an, wie in Abschnitt 1 oben vorgestellt.

2.2 Cybersicherheit als Funktion von Bedrohung und Schutz

Wenn man Fragen der „Cybersicherheit“ betrachtet, ist es hilfreich, zunächst von dem *Problem* auszugehen, dem sich Individuen (insbes. auch Unternehmen) und die Gesellschaft als Ganzes gegenübersehen. Dieses Problem ist, vereinfacht gesagt, ein möglicher Angriff bzw. eine Attacke auf ein Schutzgut.[12] [13]

[12] Eine solche Problembeschreibung ist eine basale ökonomische Beschreibung des Sicherheitsproblems im Allgemeinen, in einer Tradition, die auf John Locke zurückgeht, vgl. *John Locke*: Two Treatises of Government, hrsg. von *Peter Laslett*, Cambridge: Cambridge University Press 1988 [1689], S. 330-349. Dabei steht der Schutz von Eigentum, in einem breiten Sinne, im Zentrum des Sicherheitsbegriffs, vgl. ebd. Rn. 120, S. 348. Es gibt andere, beispielsweise soziologische, Ansätze, die anders und bspw. unmittelbar an der Wahrnehmung ansetzen.

[13] Vgl. Abbildung 2.

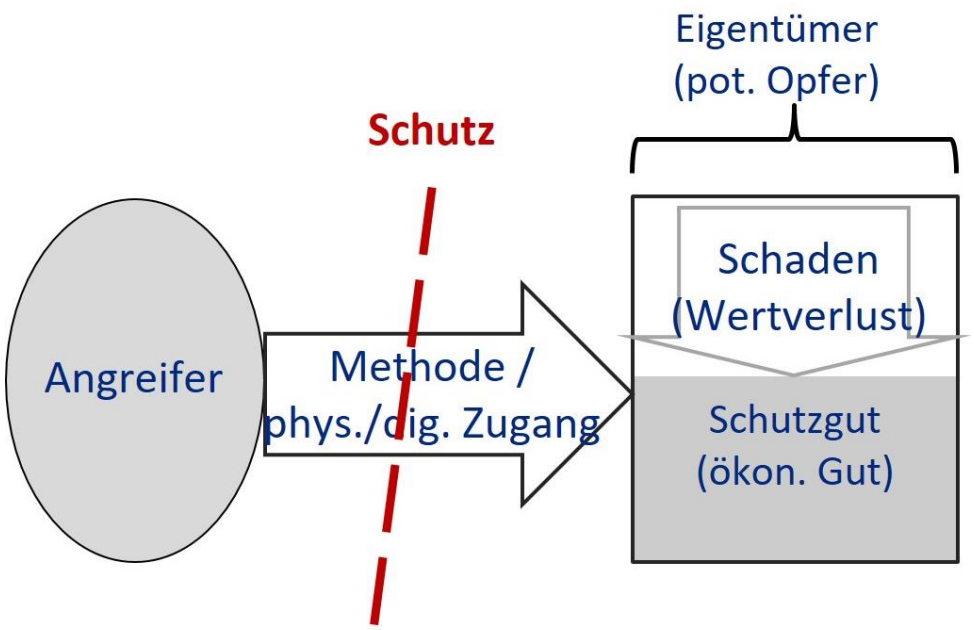


Abbildung 2 Angriff und Schutz (einstufig)
Quelle: Eigene Darstellung.

Abbildung 2 stellt von Menschen absichtlich herbeigeführte Sicherheitsprobleme als eine Trias dar,[14] bestehend aus:[15]

(1) dem **Angreifer** (Täter),[16] mit bestimmten Zielen und Möglichkeiten (ökonomisch: Intentionen und Restriktionen), sowie

(2) bestimmten, sich ständig wandelnder, zumeist technischer **Methoden**, die ihm einen Zugang verschaffen; und zwar zum sog.

[14] Dies ist eine Problembeschreibung, die für alle derartige Sicherheitsprobleme gilt, die mit Angriffen / Attacken verbunden sind, also auch bei *offline*-Sicherheitsproblemen (vgl. Bretschneider et al. 2018, S. 8 ff.). Abzugrenzen ist dieses Feld von bedrohungsbedingter Beeinträchtigung der Sicherheit (Bedrohungssicherheit, im Englischen *security*) von unabsichtlich versachten Beeinträchtigungen der Sicherheit (Störfallsicherheit, *safety*), die aus systeminternen Bedrohungen erwachsen. Beispiele wären Brände, Arbeitsunfälle und Ähnliches.

[15] Alle im Folgenden betrachteten Cybersecurity-Probleme sind solche, "*that have their origin in human intentions and actions*" (Johnston und Shearing 2013, S. 9). Künftig wird diese Unterscheidung freilich durch mögliche KI-Angriffe herausgefordert werden.

[16] In der juristischen Literatur auch regelmäßig „Störer" genannt (vgl. etwa Isensee 1983, S. 38; Burgi 2007, S. 655).

(3) **Schutzgut**; ein ökonomisches Gut, welches einem anderen, nämlich dem (rechtmäßigen) Eigentümer gehört, der im Lichte eines derartigen Angriffs zum Opfer wird. Als Schutzguteigentümer werden im Rahmen dieser Studie *Unternehmen* betrachtet.[17]

(1) *Angreifer*: Um das Feld der Angreifer im Cyberbereich abzustecken, ist es sinnvoll, einerseits relevante *Zielstellungen* und andererseits die zu erwartenden *Möglichkeiten* der Angreifer für einen Cyberangriff abzustecken.[18] Mit Blick auf die Zielstellungen kann es den Angreifern um grundsätzlich um Sabotage oder um Inbesitznahme eines Schutzgutes gehen. Ferner können Angreifer ganz bestimmte, oder aber beliebige Unternehmen angreifen. Dazwischen mag es als Angriffsziel noch Unternehmen mit bestimmten Eigenschaften geben. Hier richten sich die Angriffe gegen bestimmte Kategorien von Unternehmen, bspw. solcher einer vom Angreifer gewählten Unternehmens(mindest)größe, wenn es etwa um den Diebstahl von Geld geht. Diese beiden Dimensionen sind in Tabelle 1 dargestellt.

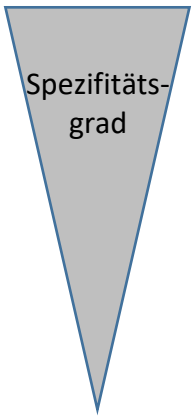
		Typ der Zielstellung	
Spezifitätsgrad des Angreifer-Interesses mit Blick auf das anzugreifende Unternehmen		*Sabotage* des Schutzgutes	*Inbesitznahme* des Schutzgutes
	*unternehmens*-spezifisch	konkurrenz-spezifische Sabotage	IP-Diebstahl (Cyberspionage), Diebstahl von Kunden-, Personal-, Rechnungsdaten
	eigenschafts-spezifisch	z.B. KRITIS-Sabotage	cyber-gestützter Diebstahl von; Diebstahl von Kunden-, Personal-, Rechnungsdaten
	un-spezifisch	Generelle Sabotage	cyber-gestützter Diebstahl von Geld

Tabelle 1 Zielstellungstyp und Spezifitätsgrad von Angriffen
Quelle: Eigene Darstellung.

[17] Angesichts der Ausrichtung der Studie werden private Personen bzw. private Haushalte in den Hintergrund gerückt. Das spiegelt sich auch an den im Folgenden verwendeten Begriffspaaren Präferenzen und Restriktionen sowie Wollen und Können wider, die sich auf Unternehmen und staatliche Organisationen beziehen.

[18] Dies entspricht der doppelten Determinierung von Entscheidungen der neoklassischen Mikroökonomik.

Ist das Ziel die Sabotage bzw. Zerstörung des Schutzgutes (Sabotage, linke Spalte der Tabelle 1), dann kann man – mit absteigendem Spezifitätsgrad – unterscheiden wie folgt: Unternehmensspezifisch kann die (Zer-)Störung von konkurrierenden Unternehmen vorgenommen werden, zwecks Schwächung des Wettbewerbers. Eigenschaftsspezifisch können das Ziel etwa Unternehmen der KRITIS oder andere größere Unternehmen sein, wenn es Angreifern darum geht, möglichst viel Schaden anzurichten und ggf. Aufmerksamkeit zu generieren. Unspezifisch schließlich sind Ansätze des generellen Vandalismus, wie etwa eine völlig unspezifische Verbreitung von Viren o.ä.

Auf der Seite der Zielstellung „Inbesitznahme" (rechte Spalte der Tabelle 1) kann ebenfalls anhand eines abnehmenden Spezifitätsgrads unterschieden werden. Unternehmensspezifisch ist insbesondere das Ziel der Inbesitznahme von geistigem Eigentum (*intellectual property*, IP). Hier geht es um Cyberspionage (als Teil der Wirtschafts- oder Industriespionage), an der grundsätzlich auf dem Markt konkurrierende Unternehmen sowie ggf. Staaten ein Interesse haben. Unterhalb dieses höchsten Spezifitätsgrades mag es Angreifern insbesondere um cyber-gestützten Gelddiebstahl, aber etwa auch um den Diebstahl von Kundendaten gehen. Dabei werden – mit mittlerem Spezifitätsgrad – Unternehmen adressiert, von denen besonders nennenswerte oder besonders einfach zu erbeutende Geldsummen zu erwarten sind (eigenschaftsspezifisch). Grundsätzlich kann aber jedes beliebige Unternehmen (unspezifisch) Adressat eines derart motivierten Angriffs sein.

Vor dem Hintergrund der Trennung von Destruktion und Sabotage einerseits und Inbesitznahme andererseits stellen erpresserische *Distributed-Denial-of-Service*- (DDoS) bzw. *Botnet*-Angriffe oder die erpresserische „Geiselnahme" von Daten (mittels sog. *Ransomware*) eine gewisse Besonderheit dar. Das eigentliche Ziel ist die Geldbeute; zahlt der erpresste Schutzguteigentümern nicht, führt dies (zwecks Glaubwürdigkeit der Drohung bei künftigen Erpressungen) in der Regel zu einer Zerstörung bzw. dauerhaften Kryptierung von Daten.

Einen Sonderfall stellen Sabotage und (Wirtschafts-)Spionage in staatlichem Auftrag dar. Hier steht in der Regel nicht eine unmittelbare Gewinnerzielungsabsicht dahinter, sondern vielmehr der Versuch, (wirtschafts- und industrie-) politische Ziele durch Zerstörung oder die verdeckte Beschaffung von Wissen zu fördern. Staatlich betriebene Spionage und Sabotage spielen im weiteren Verlauf der Studie nur eine nachgeordnete Rolle in der Analyse, ohne dabei die Relevanz zu negieren.

Mit Blick auf die ***Möglichkeiten*** der Angreifer gilt, dass sie für die Durchführung ihrer Angriffe auf methodische Kompetenzen angewiesen sind. In irgendeiner Weise muss also jeder Angreifer, der mit einer der o.g. Zielstellungen den Cyberraum nutzen will, im Vorfeld entsprechende (IT-) Kompetenzen erwerben. Hierbei gibt es zwei Möglichkeiten. Entweder erwirbt der Angreifer selbst solch eine Kompetenz, oder aber er kauft sich diese Kompetenz ein.[19] Bei letzterer Variant handelt es sich um ein Phänomen in einem global stark wachsenden Markt, dem des *cybercrime-as-a-service* (CaaS).[20] Die zunehmende Professionalisierung und Arbeitsteilung krimineller Strukturen im Cyberraum hat zu einer florierenden illegalen Dienstleistungsgesellschaft insbesondere im Dark Web geführt. Hier entsteht mit CaaS analog zum Rauschgifthandel eine Kommerzialisierung krimineller Online-Aktivitäten. Bedrohungsakteure können sich auf Marktplätzen im Dark Web mit Angriffs-Werkzeugen ausrüsten und ohne fortgeschrittene technische Fähigkeiten Cyberangriffe durchführen. Damit sind auch weniger kompetenten Individuen mit einer Angriffs-Zielstellung weitreichende Möglichkeiten gegeben. Nötig ist lediglich eine hinreichende Zahlungsbereitschaft und -Fähigkeit – und die Inkaufnahme aller Folgen. Dabei gibt es gerade bei spezifischem Interesse regelmäßig und zunehmend eine wirkliche Produktionsfunktion, also eine auf Effektivität und Effizienz ausgerichtete, oftmals in der Produktion komplexe unternehmerische Aktivität.

(2) *Methoden / Zugang*: Die wachsenden Herausforderungen der Cybersicherheit sind im Kern der zunehmenden Digitalisierung[21] geschuldet, die neue Ansatzpunkte für kriminelles Handeln schafft. Dabei bietet theoretisch jede neue Verknüpfung eine neue Verwundbarkeit. Weitere Ursache der besonderen Dynamik der Bedrohung – und ein wichtiger Unterschied zu Problemen der herkömmlichen Sicherheit – ist ferner, dass im Cyberraum geographische Lage grundsätzlich (nahezu)[22] überhaupt keine Rolle spielt.

Darin liegt eine der entscheidenden Herausforderungen im Umgang mit diesem Phänomen. Ferner ist in den letzten Jahren eine zunehmende technische Reife der Angriffe zu beobachten, da Bedrohungsakteure und Gruppierungen ihre Instrumente und Taktiken, basierend auf den

---

[19] In der ökonomischen Debatte wird diese grundsätzliche Fragestellung unter dem Schlagwort *make or buy* behandelt (vgl. Coase 1937, Hirshleifer 1980).

[20] Vgl. Mirian et al. 2019; BKA 2018, S. 24; Manky 2013; sowie Sood und Enbody 2013.

[21] Diese Zunahme schlägt sich beispielsweise auch in der ZEW ICT Survey nieder: "*Modern Information and Communication Technologies (ICT) have been proliferating through the entire business sector over recent decades. This increasing digitalization is having a substantial impact on economic activity and is continuously changing the nature of production processes* (…)" (Bertschek, Ohnemus und Viete 2018, S.87).

[22] Wir ignorieren der Einfachheit halber an dieser Stelle Unterschiede in Fragen der Konnektivität und Netzabdeckung ebenso wie regionale technische Einschränkungen durch Staaten, wie etwa in China.

jeweiligen Erfahrungen sowie Erfolgen oder Misserfolgen, weiter verfeinern.[23] Dabei wurden in den letzten Jahren neben technischen auch nicht-technische Methoden zwecks Erreichung des Angriffsziels eingesetzt. Schließlich zählen zu den betrachteten Angriffen insbesondere auch solche, bei denen technische mit nicht-technischen Methoden kombiniert werden.[24]

Einschlägig und zentral ist dabei das sog. *social engineering*: „Bei Cyberangriffen durch Social Engineering versuchen Kriminelle, ihre Opfer dazu zu verleiten, eigenständig Daten preiszugeben, Schutzmaßnahmen zu umgehen oder selbstständig Schadprogramme auf ihren Systemen zu installieren."[25] Die Angriffsmuster des *social engineering* konzentrieren sich auf die Manipulation von Menschen mit dem Ziel, zum Zweck der Informationsbeschaffung, des Betrugs oder des Zugriffs auf das IT-System das Vertrauen der Zielpersonen zu gewinnen.[26]

(3) *Schutzgut*: Schutzgüter sind diejenigen (ökonomischen) Güter, auf die sich die Angriffe richten und welche bedingt dadurch einen Wertverlust (Schaden) erleiden. Dadurch entstehen dem Schutzguteigentümer (Unternehmer) Kosten und der Volkswirtschaft entsprechend relative Wachstumsdefizite.

Es ist nicht trivial, das Schutzgut im Cyberkontext zu spezifizieren. Klar ist, dass *Daten* als Schutzgüter eine zentrale Rolle spielen. Teils sind sie bereits das „finale" Gut, teils sind sie aber ihrerseits für Angreifer ein Mittel bzw. Instrument, um andere Schutzgüter zu attackieren. Ersteres ist bei der durch Angreifer angestrebten Inbesitznahme von geistigem Eigentum (IP) oder anderer Daten (etwa Kunden-, Personal-, Rechnungsdaten) der Fall. Geht es den Angreifern dagegen um Inbesitznahme von Geld, dann sind die Daten selbst ein Instrument – und das Geld ist das finale Schutzgut. Bei Angriffen, die auf Destruktion angelegt sind, sind Daten grundsätzlich lediglich ein Instrument. Hierbei stehen Prozessdaten im Mittelpunkt, mit dem Angreifer den Betrieb, also physische oder informationsbezogene Prozesse, beeinträchtigen oder unterbrechen können. Allerdings: Insoweit Daten der geeignetste bzw. einzige Zugang zu einem „dahinterliegenden" Schutzgut sind, können und sollten sie selbst als Schutzgut betrachtet werden.

[23] Vgl. CaaS; Symantec Threat Report 2019, S. 17 ff.

[24] In diesem Sinne siehe auch die Abgrenzung zwischen dem technischen und somit enger gefassten Begriff der „IT-Sicherheit" und dem weiter gefassten, integrativen Begriff der Cybersicherheit in Abschnitt 2.1.

[25] BSI 2018, S. 98.

[26] Vgl. CAPEC (Common Attack Pattern Enumeration and Classification) List – 403: Social Engineering (Version 3.1) https://capec.mitre.org/data/definitions/403.html.

Gerade bei Angriffen auf Prozesse sind neben Eigenschäden auch Fremdschäden zu berücksichtigen, auf welche Angreifer mehr oder weniger abzielen. Dabei können die Fremdschäden gerade auch Kunden des Unternehmens betreffen. Darauf zielen sowohl vielfach Angriffe auf KRITIS ab, aber etwa auch Angriffe auf KMU, die einerseits in komplexe Wertschöpfungs- und Lieferketten eingebettet sind und andererseits eine vergleichsweise hohe Cybervulnerabilität aufweisen.[27] [28] Die zunehmende Anzahl an digitalen Schnittstellen und der informationstechnologischen Vernetzung entlang der Wertschöpfungskette zwischen Zulieferern, Produzenten, (Logistik-)Dienstleistern, dem Handel und den Konsumenten, schaffen viele neue Einfallstore für potentielle Bedrohungsakteure die es zu berücksichtigen und zu schließen gilt. Tendenziell sind größerer Unternehmen besser geschützt, da eher Ressourcen und eine gewisse Sensibilität für das Thema IT- und Cybersicherheit vorhanden sind.[29]

Bei gezielten Cyberangriffen suchen die Täter zunächst nach Schwachstellen in einem System. Von daher ist es nicht ungewöhnlich, dass die schwächsten Glieder einer Wertschöpfungs- und Lieferkette angegriffen werden, um letztlich das ursprüngliche Ziel zu infiltrieren. Sie dienen somit lediglich als Einfallstor. Fremdschäden können zudem auf das betrachtete Unternehmen zurückfallen, bspw. in Form von Vertragsstrafen, Bußgeldern sowie Reputationskosten.[30] Die Komplexität der Schädigungen, mit Eigen- wie Fremdschäden, führt schließlich dazu, dass die empirisch-quantitative Erfassung bzw. Messung von Schäden durch Cyberangriffe eine besondere Herausforderung ist.[31] Wichtig ist, dass für eine unternehmerische wie auch volkswirtschaftliche Bewertung der Probleme eine Perspektive auf den ökonomischen Schadenswert nötig ist; und eine rein technische Perspektive darauf nicht ausreichend ist.

Für den einzelnen Schutzguteigentümer (hier insbesondere das einzelne Unternehmen) wie auch für die gesamte Gesellschaft lautet die zentrale These der bisherigen Ausführungen dieses Abschnitts: **Ein „erfolgreicher“ Angriff führt zu einer Wertminderung des Schutzgutes.**

[27] Mit Blick auf die Einleitung lassen sich hier noch einmal zwei „gesellschaftliche Schutzgüter“ unterscheiden. Bei KRITIS geht es um das „Schutzgut öffentliche Sicherheit“, bei anderen Unternehmen – etwa im Rahmen derartiger Wertschöpfungsketten – geht es um das „Schutzgut Wachstum“. Vgl. zur Cybervulnerabilität von KMU auch Abschnitt 3.1. Fremdschäden können aber auch gegenüber Nicht-Geschäftspartnern ausgelöst werden, etwa indem externe Effekte provoziert werden. Im Rahmen von KRITIS zielt ein Angriff bspw. auf ein Kernkraftwerk wohl letztlich nicht allein auf den bezweckten Stromausfall.

[28] Vgl. etwa Bartsch und Frey 2017, S. 33.

[29] Vgl. Bitkom 2018a, S.14.

[30] Vgl. Bartsch und Frey 2017, S. 31.

[31] Vgl. Ebd.

Vor diesem Hintergrund kann man eine Bedrohung definitorisch als eine bestimmte Wahrscheinlichkeit eines schadensinduzierenden Angriffs fassen. In diesem Zusammenhang ist häufig auch von „Risiko“ die Rede, welches hier synonym zur Bedrohung verwendet wird.[32]

Stochastisch betrachtet geht es in vereinfachter Form um den Erwartungswert eines Schadens (Umfang des Schadens, multipliziert mit der Eintrittswahrscheinlichkeit des Angriffs):[33]

$$b = P \cdot l \qquad (2\text{-}1)$$

Und dies ist, als Bedrohungsinformation[34], die Größe, die für Schutzguteigentümer bzw. Staat, Gesellschaft und Unternehmen unter Sicherheitsgesichtspunkten – bzw., bzgl. Ressourceneinsatz für Schutzzwecke – relevant ist.

2.3 Bedrohungsakteure

Komplementär zur Differenzierung nach Angreifer – Methode/Zugang – Schutzgut ist es hilfreich, die unterschiedlichen Arten von Cyberangriffen über alle drei Aspekte zu betrachten. Dies wird in der wissenschaftlichen wie praxisbezogenen Literatur vielfach vorgenommen.[35] Eine Übersicht bietet etwa die folgende Tabelle 2.[36]

Darüber hinaus sind potentielle Angreifer näher zu differenzieren und zu definieren, um eine genauere Vorstellung zu Motiven, dem Reifegrad der Angreifer und der Eintrittswahrscheinlichkeit (z.B. *targeted attack* vs. *collateral damage*) zu bekommen und darauf basierend entsprechend Maßnahmen treffen zu können.[37]

Der Begriff *Threat Agent* (Bedrohungsakteur) wird verwendet, um eine Person oder Gruppe zu bezeichnen, die eine Bedrohung für den einzelnen Bürger, Unternehmen oder den Staat darstellen. Im Folgenden werden die gängigsten Bedrohungsakteure aufgelistet:

[32] So spricht etwa auch Bundesinnenminister Seehofer während der Vorstellung des BSI-Lageberichts in der Bundespresskonferenz am 17.10.2019 von Risiken: „Wenn wir die Chancen der Digitalisierung voll ausschöpfen wollen, müssen wir die mit ihr verbundenen Risiken beherrschbar machen.“ (Seehofer 2019).

[33] Legende: b - Bedrohung; P – Wahrscheinlichkeit; l (*loss*) – Schaden/Verlust.

[34] Eine der großen Herausforderungen im Bereich der Cybersicherheit besteht darin, dass Schutzguteigentümer über diese (Bedrohungs-)Information nicht hinreichend verfügen, vgl. weiter unten, Abschnitt 3.1.2.

[35] Vgl. nur Bendovschi 2015; Kim et al. 2011; KPMG 2017; Jouini et al. 2014; KPN et al. 2018, S. 5.

[36] Vgl. Bartsch und Frey 2015, S. 20.

[37] Vgl. dazu auch Abschnitt 2.5.

1. *Nation State Actor/Government Hacker*

Hacker, die für Staaten/Regierungen arbeiten, arbeiten gewissermaßen mit Lizenz bzw. als Söldner. In den letzten Jahren haben immer mehr Nationen Fertigkeiten im Cyberraum aufgebaut und weiterentwickelt. Sowohl finanzielle Investitionen in die Infrastruktur als auch in das Humankapital wurden weiter erhöht. Vor diesem Hintergrund haben sich viele nationalstaatliche Akteure, sowie von Regierungen „geduldete“ und ggf. unterstützte Gruppierungen fortgeschrittene Fähigkeiten angeeignet und sie weiterentwickelt, die ihnen im Cyberraum einen Vorteil verschaffen. In diesem Zusammenhang hat sich für solche Gruppierungen der Begriff *Advanced Persistent Threats* (APT) etabliert.

APTs gewinnen auch deshalb an Bedeutung, da staatlich gesteuerte offensive Operationen gegenüber defensivem Cyberschutz zunehmen.[38] So wird behauptet,[39] dass in bestimmten autoritär regierten Staaten wie beispielsweise Nordkorea ausgebildete Hacker beauftragt werden, Devisen im Cyberraum zu erbeuten. Sie eröffnen damit eine Einnahmequelle für den Staatshaushalt, der durch digitale Beutezüge aufgebessert wird. Darüber hinaus verfolgen die Hacker im Staatsauftrag auch politische und strategische Ziele und versuchen, ökonomische und militärische Defizite des Staates mit aggressiven asymmetrischen Kampagnen zu kompensieren.[40] Des Weiteren, werden in Ländern wie China und Russland derartig viele IT-Fachkräfte ausgebildet, dass die Nachfrage in den staatlichen Behörden und im Militär sowie in der nationalen IT-Industrie das Angebot an qualifizierten Arbeitskräften nicht abdeckt.[41] In der Folge und aufgrund mangelnder beruflicher Alternativen kann der nicht in der legalen Wirtschaft eingesetzte „Angebotsüberschuss”, sein Einkommen als krimineller sog. *Black Hat Hacker* bestreiten.

Spektakuläre Cybervorfälle wie der in 2010 entdeckte, äußerst komplexe Computer-Wurm ***Stuxnet***[42], der bis dahin unbekannte *Zero-Day*-Schwachstellen ausnutzen konnte, um mit dem Ziel einer physischen Wirkung (Überlastung von Zentrifugen die zur Anreicherung von Uran verwendet wurden) Computer zu infizieren, haben gezeigt, was einige Staaten bereits damals für Fähigkeiten hatten.[43] Die Tatsache, dass Staaten ihre Cyberfähigkeiten zunehmend vorantreiben und weit oben auf ihrer Prioritäten-Agenda setzen, trägt zu einer höheren Aktivität und

[38] Vgl. Arts 2018.
[39] Interview 4, staatliche Stelle.
[40] Vgl. Rosenbach und Wagner 2018.
[41] Interview 4, staatliche Stelle.
[42] Vgl. Zetter 2015.
[43] Vgl. Fruhlinger 2017.

Bedrohungsentwicklung dieser *Threat-Agent*-Gruppe bei. Angesichts der fortgeschrittenen Fähigkeiten sind Cyberangriffe, die von diesen Akteuren ausgehen, oft besonders schwer zu identifizieren und abzuwehren. Dabei sind die bekannten Vorfälle vermutlich nur die Spitze des Eisbergs; die nicht in Statistiken ausgewiesene Dunkelziffer dürfte erheblich sein.

Die zunehmende staatliche Fokussierung auf offensive Cyberoperationen, sei es zur offensiven Verteidigung, der Abschreckung potenzieller Angreifer dienenden Aufbau von Fähigkeiten, zur Gewinnung von nachrichtendienstlicher Informationen, oder um seinen Spielraum im Krisenfall zu erweitern, tragen zu einer erhöhten Aktivität dieser Akteure im Cyberraum bei.[44] Dabei werden oftmals neue und innovative Ansätze genutzt, um sich (bzw. zur Daten-Exfiltration) Zugang zu Systemen zu verschaffen.

2. Hacktivist

Hacktivismus hat sich ab der Mitte der 90er Jahre als Ausdruck etabliert und wird häufig mit dem Hacker-Kollektiv *Cult of the Dead Cow* in Verbindung gebracht.[45] Der Begriff ist eine Kombination aus *Hacking* und Aktivismus. Damit wird die Verwendung von Informations- und Kommunikationsmitteln zur Verdeutlichung und Durchsetzung einer politischen oder sozialen Botschaft bezeichnet.[46] Akteure, die dieser Gruppe zuzuordnen sind, handeln aus ideologischen Beweggründen. Sie wollen ihren Protest gegen politische, gesellschaftliche oder unternehmerische Maßnahmen und Handlungen zum Ausdruck bringen oder verfolgen Propagandazwecke. Sie sind dabei jedoch typischerweise nicht profitgetrieben. Das Spektrum der Fähigkeiten der Einzelpersonen und Gruppen reicht über die verschiedensten Leistungsstufen.[47] Sie haben ein ausreichendes Verständnis der Architektur der Netzwerke, verfügen z.T. über umfangreiche Programmierkenntnisse und können damit Angriffe gut vorbereiten, wobei sie politische Botschaften in zeitnaher Abfolge zu den Aufmerksamkeit erzielenden Taten transportieren möchten.

3. Insider

Die Gefahr eines Angriffs auf eine Institution durch einen Insider ist kein unbekanntes Phänomen, birgt für hochvernetzte Umgebungen die Informationen in Echtzeit verarbeiten jedoch besonders große Gefahren. Dies ist vor allem dann der Fall, wenn Systeme nicht voneinander

[44] Vgl. World Economic Forum 2012.
[45] Vgl. Jordan and Taylor 2004.
[46] Vgl. BKA 2015.
[47] Vgl. Radware 2017.

getrennt sind (Netzwerksegmentierung) bzw. über keine adäquaten Sicherheitssysteme verfügen. Beim *Insider* kann es sich sowohl um einen verärgerten ehemaligen oder aktuellen Mitarbeiter mit der Absicht, dem Unternehmen Schaden zuzufügen, handeln, als auch um einen Zulieferer oder Berater, der Zugriff auf Teile oder (auch unwissentlich) die Gesamtheit des IT-Systems hat und entweder Daten abschöpfen, Malware einschleusen oder Informationen über die Infrastruktur sammeln will.

Insider fallen immer wieder auch als Bedrohungsakteure auf, die unabsichtlich – aus Unwissenheit, Unachtsamkeit oder fahrlässigem Verhalten – Cyberkriminellen als Einfallstor dienen. Der Verzicht auf bewährte Passwort-Verfahren, unsachgemäße Systemeinstellungen und fahrlässige Konfigurationen von Servern, Cloud Umgebungen etc., sowie unachtsames Verhalten bei *Phishing* und *Social Engineering* Angriffen zählen zu den häufigsten Ursachen für unbeabsichtigte Bedrohungen durch Insider.[48]

4. Cyberkriminelle

Erpressungs-Trojaner, oben erwähnte *Ransomware*, werden im großen Stil von Cyberkriminellen eingesetzt, da sie sich ein hohes Monetarisierungspotenzial erhoffen. Sie zählen derzeit zu den aktivsten Bedrohungs-Akteuren im Cyberraum und sind mit Abstand für die meisten Cyberangriffe, gleichzeitig mit den höchsten Kosten (sowohl direkte Kosten als auch Folgekosten), verantwortlich.[49] Bei Cyberkriminalitätsdelikten geht es den Akteuren in erster Linie um den (persönlichen) Profit, jenseits von ideologischen Motiven. Diese Delikte können von Einzelpersonen oder auch von Gruppierungen verübt werden. Darüber hinaus können Cyberkriminelle auch im staatlichen Auftrag mit dem Ziel handeln, Einkommen für den Staatshaushalt zu beschaffen.[50] Die Qualität der Angriffe dieser Akteure ist oft besonders hoch, und reicht über die gesamte Bandbreite der technischen, organisatorischen und strategischen Fähigkeiten.

Verbunden mit der zunehmenden Professionalisierung der *Dark Web Economy*, die leicht zu erwerbende und zu nutzende *Malware* für jedermann anbietet, hat Cyberkriminalität zu hohen volkswirtschaftlichen Schäden geführt. Die Opferzahlen steigen jährlich.[51] Die Vorgehensweise der Angreifer ist sehr dynamisch und passt sich neuen Schutzmaßnahmen schnell an. Die

[48] Vgl. IBM 2019.
[49] Vgl. McAfee 2018.
[50] S.o. zusätzlich Peteranderl 2019.
[51] Vgl. Kapitel 2.4.

Auswahl und Ausspähung bestimmter Objekte zwecks zielgerichteter Angriffe (*targeted attack*) scheint zuzunehmen, während breit gestreute Angriffe auf breite Benutzersegmente (l*ow hanging fruit*) weiterhin ein probates Mittel sind.[52] Ein weiterer Trend ist die Monetarisierung von unrechtmäßig (durch Datenschutzverletzungen oder dezidierten Datendiebstahl) erworbenen Informationen, da die Taten für Cyberkriminelle nach wie vor lukrativ und in großem Stil skalierbar sind.[53]

Die hier vorgenommene begriffliche Abgrenzung berücksichtigt weder Cyberterrorismus noch Cyberkriegsführung oder sog. *Skript Kiddies*, da sie für die vorliegende Betrachtung weniger relevant sind.

[52] Vgl. Symantec Threat Report 2019.
[53] Vgl. Verizon 2019.

Bedrohungsarten	*Cybercrime*, Hacktivismus, Cyberspionage, Cybersabotage			
Methode	***Hacking***: Überwindung von technischen Hürden, um Zugriff auf Computersysteme und Netzwerke zu erlangen	***Malware***: Schadsoftware zur Automatisierung von Hacking	**DDoS**: Ein verteilter und überlastender Angriff auf Computersysteme, damit diese nicht mehr ordnungsgemäß funktionieren	***Social Engeneering***: Informationsbeschaffung durch zwischenmenschliche Beziehungen in sozialen Netzwerken
Täter	Einzelpersonen, Gruppen oder Staaten	Einzelpersonen, Gruppen oder Staaten	Gruppen	Einzelpersonen
Angriffsziele	Unternehmen und Staaten	Alle Nutzer von Computersystemen	Betreiber von Internetservern und öffentlich zugängliche Infrastrukturen von Behörden und Unternehmen	Alle Nutzer von Computersystemen
Fallbeispiele[54]	NSA, Sony Hack, Saudi Aramco	Online Banking, iranisches Atomprogramm (Stuxnet), Datenverschlüsselung (U-Cash-Trojaner, Locky and Cryptomlocker	Anonymous Bayer (Operation Greenrights), Cyberangriff auf Estland	Kevon Mitnick, WikiLeaks

Tabelle 2 Übersicht der Arten von Cyberangriffen
Quelle: Bartsch und Frey 2017, S. 20.

[54] Vgl. Bartsch und Frey 2017, S. 20.

2.4 Fallstudien

Ob Mittelständler oder Großkonzern, die durch Cyberangriffe verursachten geschäftsschädigenden Folgen sind längst keine Ausnahmefälle mehr, sondern ein Massenphänomen in der deutschen Wirtschaft. Gemäß einer repräsentativen Studie des Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (Bitkom) von September 2018, sind nach Aussage der 503 befragten Geschäftsführer und Sicherheitsverantwortlichen von Industrieunternehmen aus verschiedenen Branchen, fast 70 Prozent der Unternehmen in den letzten beiden Jahren Opfer von Sabotage, Datendiebstahl oder Spionage geworden.[55] Dabei entstand der deutschen Industrie innerhalb von zwei Jahren ein Gesamtschaden von knapp 43 Milliarden Euro. Das Dunkelfeld dürfte den tatsächlichen Betrag noch deutlich erhöhen.

Oft werden Vorfälle der Öffentlichkeit und den mit der Thematik befassten Behörden gar nicht erst bekannt, da zum einen viele Unternehmen nicht wissen, dass sie überhaupt von einem „Cybervorfall“ betroffen sind, und zum anderen, da sich in Führungsetagen immer noch hartnäckig die Meinung hält, Reden sei Silber, Schweigen jedoch Gold. Zum anderen scheuen sich Unternehmensleitungen einen Vorfall publik zu machen, da sie einen Reputationsverlust und damit einhergehend, einen Nachfragerückgang fürchten.

Die Angst vor öffentlicher Brandmarkung scheint immer noch über die ersichtlichen Synergiegewinne durch Kooperation und das Teilen von Erkenntnissen einzelner Cybervorfälle zu überwiegen.

Beim Eindringen in Netzwerke spielt der Faktor Mensch stets eine bedeutende Rolle. Mithilfe von *social engineering* versuchen die Eindringlinge, sich das Vertrauen der Zielpersonen zu erschleichen, um entweder an wichtige Informationen zu gelangen oder die Personen dazu zu verleiten, infizierte Dateien zu öffnen oder auf manipulierte Links zu klicken. Der Täterkreis stammt oft aus dem unmittelbaren Umfeld des Unternehmens. Laut Bitkom stammen 63 Prozent der Täter aus den eigenen Reihen.[56]

Vernetzung führt zu mehr Angriffsflächen, aber auch zu neuen Geschäftsmodellen; und hat enormes Einsparpotenzial durch Synergieeffekte. Sie ist gewissermaßen Fluch und Segen zugleich. Die derzeit (noch) gute konjunkturelle Lage in Deutschland zieht Cyberkriminelle an, vor allem, da es ihnen durch z.T. ungenügende oder nicht vorhandene einfachste IT-Sicherheitsmaßnahmen von kleinen und mittelständischen Unternehmen, oft zu einfach gemacht wird.

[55] Vgl. Bitkom 2018a, S. 24 f.
[56] Ebd.

Laut einer repräsentativen Forsa-Befragung im Auftrag des Gesamtverband der Deutschen Versicherungswirtschaft (GDV) erfüllen nur 16 Prozent der deutschen Mittelständler zehn der einfachsten Schutzmaßnahmen.[57] Dazu gehören personalisierte Passwörter für Mitarbeiter, der Einsatz von Virenscannern, das automatische und zeitnahe Einspielen von Sicherheitsaktualisierungen der Software; und auch die regelmäßige Anfertigung von Sicherungskopien sowie der regelmäßige Test, ob Sicherungskopien auch alle relevanten Daten enthalten und wiederhergestellt werden können.

Während der volkswirtschaftliche Schaden schwer zu bemessen und in Umfang und Wirkung nur schwer zu greifen ist, können Fallstudien den Effekt auf einzelne Unternehmen verdeutlichen. Im Folgenden sollen daher einige Beispiele von erfolgreichen Cyberangriffen dargestellt werden:

[57] Vgl. GDV 2019a, S. 18.

Box I: Lukaskrankenhaus Neuss

Das Lukaskrankenhaus in Neuss ist ein akademisches Lehrkrankenhaus der Heinrich-Heine-Universität Düsseldorf. Es verfügt über ca. 540 Krankenhausbetten, rund 1.400 Mitarbeiter, darunter 200 Ärzte, 900 Pflegekräfte und 300 Beschäftigte in der Administration; und erwirtschaftete als eine GmbH einen Umsatz von 131 Millionen Euro in 2015.[58] In dem Jahr wurden 28.600 Patienten stationär und 80.700 ambulant behandelt. Das Krankenhaus verfügte in 2016 über etwa 800 Desktop-Rechner und 500 Drucker, die von in etwa 800 IT-Nutzern verwendet wurden.[59]

Am 10. Februar 2016, gegen 9 Uhr morgens, stellten einige Mitarbeiter der zentralen Ambulanz des Krankenhauses und einige Radiologen fest, dass die IT-Systeme ungewöhnlich langsam arbeiteten.[60] In der Folge tauchten immer wieder Fehlermeldungen sowie ein in englischer Sprache formulierter Hinweis über den Hintergrund der IT-Probleme an einigen der Rechner auf. Daraufhin war schnell klar, dass es sich um einen Verschlüsselungstrojaner handelte, der fast alle Daten und Rechner im Krankenhaus mit dem einzigen Zweck befallen hatte, Lösegeld in einer Kryptowährung zu erpressen.

Der Trojaner fand vermutlich den Weg ins Netz über einen unachtsamen Mitarbeiter, der einen infizierten E-Mail-Anhang mit dem Betreff „Rechnung“ geöffnet hatte. Das geforderte Lösegeld wurde an die Erpresser nie gezahlt. Das Krankenhaus musste alle Systeme herunterfahren und wie vor 15 Jahren mit Klemmbrett, Stift und Papier arbeiten. Laborbefunde wurden zwischen den Abteilungen wieder hin- und hergetragen, Rezepte per Boten verschickt und Untersuchungsergebnisse an die einzelnen Abteilungen per handgeschriebenen Zettel verteilt.

Das komplette IT-System musste heruntergefahren werden, konnte jedoch aus dem vor dem Angriff erstellten *backup* wieder eingespielt werden.[61] Dennoch wurde das System nicht einfach wiederhergestellt, sondern komplett neu aufgesetzt, mit erweiterten und neuen Sicherheitsmaßnahmen.

[58] Vgl. Stadt Neuss 2015.
[59] Vgl. Krämer und Dahmen 2017.
[60] Vgl. Barczok 2017.
[61] Ebd.

Die hinzugezogenen IT-Experten vom LKA, dem Bundesamt für Sicherheit in der Informationstechnik (BSI) und externen Berater waren sich bei ihrer Analyse einig – das Lukaskrankenhaus sei sehr transparent mit dem Vorfall vorgegangen. Es handele sich zudem nicht um einen gezielten Angriff, sondern um einen, der möglichst viele Opfer treffen sollte. Das dahinterstehende Kalkül sei gewesen, dass ausreichend viele Betroffene aus Angst vor dem Verlust der Daten schon zahlen würden.[62] In den ersten Monaten des Jahres 2016 waren allein in NRW mehr als zwei Dutzend Krankenhäusern von ähnlichen Cybervorfällen betroffen.[63]

Dabei spielen den Cyberkriminellen zwei Aspekte in die Karten: Zum einen sind die IT- und Cybersicherheitskenntnisse der meisten Angestellten – sowohl der Ärzte als auch des Pflegepersonals und der Verwaltung – zumeist begrenzt, und beschränken sich auf das für den Alltag Nötigste. Dies ist auch nicht weiter verwunderlich, da Telemedizin und andere Bereiche der Digitalisierung in Krankenhäuser bisher nur aus der Kosten- und Versorgungseffizienz betrachtet, und Gefahren der Vernetzung oftmals übersehen werden. Zudem haben Mediziner und Pflegepersonal wenig Zeit, sich mit der digitalen Sicherheit vertraut zu machen. Zumindest aber wird der Mehraufwand als störend und bis vor kurzem nicht als relevant empfunden. Zum anderen werden in medizinischen Einrichtungen Soft- und Hardware-Komponenten verwendet, die anderswo längst ausgemustert worden wären. Diese Systeme sind häufig für die medizinische Versorgung völlig ausreichend, jedoch aus der Perspektive der IT-Sicherheit überholt. Diese Systeme waren nie für eine Vernetzung ausgelegt, und sind höchst verwundbar, da sie über keine eigenen Sicherheitssysteme verfügen.[64]

Besonders in Regionen mit einer dünnen medizinischen Versorgung können Einschränkungen im täglichen Betrieb, zu ernsthaften Konsequenzen führen. Im Falle des eigentlich hochdigitalisierten Lukaskrankenhauses konnten einige Patienten für einige Wochen nicht entsprechend operiert bzw. stationär aufgenommen werden. Das Krankenhaus beteuert jedoch, dass es trotz der Einschränkungen keine Beeinträchtigung der Patientengrundversorgung gab. Der Schaden belief sich auf in etwa eine Million Euro, wobei der größte Teil auf Honorarzahlungen an externe IT-Dienstleister im Zuge der Abwehr des Cyberangriffs und der Neukonzipierung der IT-Sicherheitsstruktur zurückzuführen ist.[65]

[62] Vgl. Krämer und Dahmen 2017.
[63] Vgl. Ludwig 2016.
[64] Vgl. Krämer und Dahmen 2017.
[65] Vgl. Ebd.

Dieses einschneidende Ereignis wurde vom Krankenhaus als Anlass genommen, um seine Vorreiterrolle im Bereich der Digitalisierung auch auf den Bereich der IT- und Cybersicherheit auszuweiten. Dazu gehörten auf technischer Seite die Segmentierung einzelner vorher vernetzter Systeme, die Einführung des *sandbox*-Verfahrens[66] zur Überprüfung und Isolierung verdächtiger E-Mail-Anhänge, und auf administrativer Seite die Schulung von Mitarbeitern und die Einführung eines adäquaten Passwortmanagementsystems.[67]

Box II: Angriff auf die Deutsche Telekom

Der Staat Liberia, die Deutsche Telekom, DSL-Router, sowie ein britischer Staatsangehöriger, welcher finanzielle Mittel für seine Hochzeit suchte: Was klingt wie die Aneinanderreihung von wild zusammengewürfelten Begriffen, führte Ende 2016 zu einem der bis dahin umfangreichsten Cyberangriffe auf DSL-Router weltweit. U.a. waren etwa 1,2 Millionen Router eines deutschen Telekommunikationsanbieters betroffen. Der Angreifer hatte die Absicht, mittels eines *botnets* – bestehend aus u.a. gekaperten Routern der Deutschen Telekom – ein liberianisches Telekommunikationsunternehmen lahmzulegen.[68] Ein nationaler Konkurrent hatte einen britischen Hacker mit diesem Auftrag betraut, und ihm für die erfolgreiche Ausführung 10.000 US Dollar zugesagt.

Eine zuvor entdeckte Sicherheitslücke wurde mittels eines fertigen *exploits* ausgenutzt, verfehlte jedoch den eigentlichen Zweck, die Kontrolle über Hundertausende/Millionen von Geräten zu gewinnen und sie zu einem *botnet*, mittels eines Quell-Codes des sogenannten *Mirai* Botnet, zusammenzufassen. Der Täter der sich selbst *„Spiderman“* nannte, wollte diese gekaperten Geräte dazu nutzen, einen DDoS-Angriff auf das betroffene Unternehmen zu starten, um das System mittels einer großen Anzahl von Anfragen zum Erliegen zu bringen. Die zugrundeliegende Sicherheitslücke befand sich im Port 7547, ein Teil des Fernwartungsprotokolls TR-069, die es ermöglichte, auf andere, eigentlich nicht aus dem öffentlichen Netz erreichbare Bereiche zuzugreifen.[69] Darüber hinaus hatten die in Deutschland und anderen

[66] Die Sandbox ist ein von der Systemumgebung isolierter Bereich in dem z.B. Software oder Dateien auf eine Funktionsweise mit schädlichen Auswirkungen getestet werden können. Siehe dazu auch https://www.security-insider.de/was-ist-eine-sandbox-a-740133/.

[67] Vgl. Liedtke 2017.

[68] Vgl. Nagel 2017.

[69] Vgl. Scherschel 2016.

Ländern betriebenen Router eine weitere Sicherheitslücke, die es erlaubte, Schadcode über eine Schnittstelle einzuschleusen. Dennoch gelang es dem Angreifer nicht, die Kontrolle über die deutschen Router zu erlangen. Anstatt sich mit dem Netz zu verbinden, fielen die Router immer wieder aus. Der Schadcode wurde im Arbeitsspeicher abgelegt und durch den Neustart wieder gelöscht. Somit entwickelte sich ein immer wiederkehrender Ablauf, der zum Ausfall der ca. 1,2 Millionen Routern führte.

Der Täter konnte wenig später durch die Datenanalyse des BSI in Zusammenarbeit mit der Deutschen Telekom ausfindig gemacht werden; und wurde mit Haftbefehl, koordiniert durch die Zentrale- und Ansprechstelle Cybercrime (ZAC) bei der Staatsanwaltschaft Köln, gesucht. Drei Monate später wurde er von der britischen *National Crime Agency* an einem Londoner Flughafen gefasst. Er wurde zunächst nach Deutschland ausgeliefert, wo ihm in Köln der Prozess gemacht wurde. Der Hacker wurde zu einem Jahr und acht Monaten Haftstrafe auf Bewährung verurteilt, bevor er im Anschluss zurück nach Großbritannien ausgeliefert wurde, wo er wegen anderer Online-Vergehen ebenfalls angeklagt war.[70] Es entstand ein Schaden in Höhe von ca. zwei Millionen Euro.

2.5 Cyberangriffe – Trends der Gegenwart und Zukunft

Wirksame Schutzmaßnahmen benötigen eine verlässliche Informationspolitik, die Schadensfälle analysiert, kategorisiert und darauf basierend Bedrohungsszenarien identifiziert; und geeignete Gegenmaßnahmen initiiert. Die politische, wissenschaftliche und auch wirtschaftliche Debatte der vergangenen Jahre war häufig getrieben von Reaktionen auf Vorfälle und neuen Phänomenen. Dabei zeichnete sich ab, dass die tatsächliche Bedrohungslage nur sehr unzureichend erfasst und verstanden wird;[71] und es sich um eine äußerst diffuse Gemengelage an unterschiedlichen Akteuren, Intentionen und Einschätzungen handelt.[72] Der Mangel an validen

[70] Vgl. Böhm 2017.

[71] Für die frühe Erkennung und schnelle Reaktion auf neue Bedrohungslagen ist ein umfassendes und zeitnahes Lagebild erforderlich, das gefährdete Akteure informiert und Handlungsempfehlungen ausspricht. Der jährlich veröffentlichte BSI-Lagebericht bspw. liefert Informationen zur Bedrohung im Cyberraum und zu möglichen Schutzmaßnahmen. Zwar besteht z.T. im Rahmen des IT-Sicherheitsgesetzes (KRITIS-Verordnung) bspw. eine vertrauliche Kommunikation zwischen BSI und Betreiber Kritischer Infrastrukturen, allerdings ist dies nur punktuell der Fall. Die sich dynamisch entwickelnde Bedrohungslandschaft bedarf eines umfassenden und leistungsfähigen Lagebildes, dass Informationen zusammenführt, zeitnah verarbeitet und an die entsprechenden Stellen weiterleitet. Vgl. dazu auch Abschnitt 6.

[72] Vgl. https://www.bmi.bund.de/DE/themen/sicherheit/spionageabwehr-wirtschafts-und-geheimschutz/cyberspionage/cyberspionage-artikel.html und Bitkom 2018a, S. 5.

Informationen, die nach wissenschaftlichen Kriterien bewertet werden können, erschwert die Implementierung von wirksamen Schutzmaßnahmen.[73] Die Bewertungs- und Beurteilungsgrundlage ist fragmentiert, diffus und lückenhaft. Darüber hinaus sind detaillierte Informationen zu Schadensvorfällen und spezifischen Angriffsmechanismen z.T. nicht öffentlich zugänglich. Zwar werden gezielt Informationen zu aktuellen Bedrohungsquellen an einzelne entsprechende Adressaten verteilt, jedoch führt diese Praxis dazu, dass wichtige Erkenntnisse der Öffentlichkeit und auch der Wissenschaft vorenthalten werden.

Vor diesem Hintergrund basiert die folgende Analyse auf Berichten von privaten Cybersicherheitsunternehmen wie Symantec, Cisco, Avast und FireEye, von Beratungsunternehmen wie Deloitte, sowie von Behörden wie dem BSI. Die systematische, kategorisierte und homogene Akkumulation von Daten zu digitalen Bedrohungslagen in Form einer Datenbank, analog bspw. der Datenbanken des Statistischen Bundesamtes, ist eine der grundlegenden Maßnahmen zur Verringerung der Informationsasymmetrie.[74]

Die Gefährdungslage im Bereich der Kritischen Infrastrukturen ist laut BSI weiterhin auf einem hohen Niveau, auch wenn sich Bedrohungen nicht ausschließlich und exklusiv gegen KRITIS Betreiber richten.[75] Den Meldungszahlen (im Berichtszeitraum 1. Juni 2018 bis 31. Mai 2019) zufolge waren vor allem die KRITIS-Bereiche mit dem Fokus auf Informations- und Telekommunikationstechnologien, im speziellen des Gesundheits- und Finanzwesens, betroffen.[76] Insgesamt verfolgt die Mehrzahl der Cyberangriffe aktuell im Bereich der Cyberkriminalität vor allem monetäre Interessen.[77] Eine signifikante Zunahme von *Ransomware*-Kampagnen mit dem Ziel, unmittelbar Daten zu verschlüsseln und dadurch mittelbar Geld bei den betroffenen Unternehmen zu erpressen, war branchenübergreifend zu verzeichnen. Zudem haben Cyberangriffe wie ExPetr/NotPetya und WannaCry gezeigt, dass viele Unternehmen über unzureichende *backup*-Strategien verfügen, keine ausreichend kleinteilige Segmentierung ihrer Netzwerke haben und häufig auch ein adäquates Passwortmanagement fehlt.[78] Im Bereich KRITIS wird jedoch positiv festgestellt, dass die Nachweispflicht zur Umsetzung des IT-Sicher-

[73] Vgl. Moore 2010a.
[74] Vgl. Kapitel 3.
[75] Vgl. BSI-Lagebericht 2019, S. 46.
[76] Ebd.
[77] Ebd. S. 7.
[78] Ebd. S. 49 ff.

heitsgesetzes und die damit verbundene Implementierung des Informationssicherheitsmanagementsystems (ISMS), mit den dazugehörigen Prozessen und Verantwortlichkeiten, zu einer Verbesserung der IT-Sicherheit geführt hat.[79]

Grundsätzlich sind zu den Cyberrisiken auf der technischen und organisatorischen Ebene auch Risiken auf der politischen und gesellschaftlichen Ebene durch Fake News, Social Bots und Desinformationskampagnen hinzugekommen, wie der Deloitte Cyber Security Report 2019[80] vermerkt. Cyberattacken können politische Krisen auslösen oder verstärken, wenn z.B. Wahlvorgänge manipuliert werden oder der Verdacht besteht, diese seien manipuliert worden. Staatlich finanzierte Hacker sind in der Lage, geopolitische Krisen zu verstärken und verdeckt Einfluss zu nehmen. Zwar ist die Wirkungen und Auswirkungen dieser Kampagnen kaum mit quantitativen Methoden erforscht und es gibt Studien, die die quantitative Relevanz in Zweifel ziehen, aber allein die Verunsicherung in Zeiten einer ehedem stattfindenden gesellschaftliche Polarisierung, zeigt die Relevanz dieser Methoden.[81]

Neben neuen Risiken, die durch den stark zunehmenden und weitflächigen Einsatz von schwachstellenbehafteten IoT-Geräten (*Internet of Things*, Internet der Dinge) sowie von Kryptowährungen[82] entstehen, tragen vor allem lang etablierte Technologien und Protokolle des Cyberraums wie bspw. die E-Mail dazu bei, dass sich Angriffe verbreiten; und der Bedrohungsgrad weiterhin hoch bleibt.[83] Beachtlich ist dabei, dass der Cyberraum mehr und mehr einem alternativen digitalen Wirtschaftsraum gleicht. Ein ökonomisches Monitoring wird immer dringender, um beispielsweise zyklisch wiederkehrende Muster frühzeitig zu erkennen und ein effektives Risikomanagement zu gewährleisten.

So hat die Volatilität des Bitcoin Kurses auch Einfluss auf die Anzahl bestimmter Cyberattacken. *Cryptojacking* und *Ransomware*-Attacken profitieren von einem hohen Bitcoin-Kurs;

[79] Ebd. S. 46.

[80] Vgl. Deloitte Cyber Security Report 2019.

[81] Vgl. Reuter 2019.

[82] Die steigende Beliebtheit von Kryptowährung ruft auch Cyberkriminille auf den Plan. Sie versuchen mit Fake-Webseiten, -Apps und betrügerischen E-Mails an das Geld ihrer Opfer zu gelangen. Vgl. https://www.kaspersky.de/resource-center/definitions/cryptocurrency-scams. Darüber hinaus führen steigende Werte dazu, dass Kryptowährungen zunehmend geschürft und dazu u.a. gekaperte Rechner eingesetzt werden. Vgl. https://www.e-commerce-magazin.de/die-neuen-goldgraeber-heimliches-schuerfen-von-kryptowaehrungen-nimmt-zu/ & https://www.watchguard.com/de/wgrd-about/press-releases/hacker-lieben-kryptowaehrungen.

[83] Vgl. Cisco 2019.

und nehmen mit Kursgewinnen an Häufigkeit zu.[84] Zudem ist zu beobachten, dass ein Kursrückgang bei Kryptowährungen dazu führt, dass das sog. Schürfen – die energie- und zeitaufwändige Generierung neuer Einheiten von Kryptowährungen – für Marktteilnehmer an Attraktivität verliert.

Weitere zu beobachtende Trends sind die Kommerzialisierung und Professionalisierung der Cyberkriminalität. Dieser hat sich unter dem bereits angeführten Begriff *Cybercrime as a Service* (CaaS) etabliert und wird durch Arbeitsteilung, Internationalisierung und der Entwicklung eines Schattenmarktes für kriminelle Dienstleistungen und Produkte charakterisiert.[85] Selbst Laien ist es im Dark Web mittlerweile möglich, sich Dienstleistungen in Form von verschiedensten Cyberangriffen einzukaufen oder sich zumindest das technologische Werkzeug hierfür zu beschaffen.

Gewinnorientierte, kriminelle Strukturen folgen grundsätzlich denselben Marktmechanismen und Wirtschaftsprinzipien, wie die legale Wirtschaft. Technische Entwicklung, Spezialisierung und Arbeitsteilung haben zu Effizienzvorteilen auch im illegalen Bereich der Wirtschaft geführt. Diese Entwicklung wird auch durch die Zunahme von *targeted attacks* deutlich, die sich durch technische Komplexität, mittel- bis langfristig ausgelegte Zielsetzungen und strategische Ausrichtung auszeichnen.[86] Die Angriffe sind geplant und nutzen neben den technischen Schachstellen auch den Faktor Mensch mithilfe von *social engineering* aus. An dieser Stelle müsste ein stärkeres *Dark Web Market Monitoring* für Analysten der Strafverfolgungsbehörden, aber auch der Wissenschaft, ansetzen.

Zu den positiven Entwicklungen der Gefahrenabwehr zählten die jüngsten weltweiten Erfolge in der Strafverfolgung. Diese sind auf eine zunehmende Kooperation zwischen staatlichen Stellen, aber auch auf verbesserte technisch-forensische Methoden der Attribution sowie auf verbesserte Expertise (Humankapital) in den Strafverfolgungsbehörden zurückzuführen. Auch die Zeitspanne vom ersten Verdachtsmoment bis zur Aufdeckung des Angriffs (sogenannte *dwell time*), ist im Median über die letzten Jahre deutlich kürzer geworden. Mit anderen Worten: Die Fähigkeiten und Prozesse der Cyberabwehrsysteme werden auch besser bzw. schneller.[87]

[84] Vgl. Symantec Threat Report 2019, S. 15 ff.
[85] Vgl. Ablon und Libicki 2015.
[86] Vgl. Symantec Threat Report 2019, S. 16 ff.
[87] Vgl. FireEye M-Trends 2019, S. 5 ff.

Ein Zukunftstrend, der sich bereits jetzt abzeichnet, ist das Katz-und-Maus-Spiel der Angreifer und Verteidiger unter Hinzuziehung sog. künstlicher Intelligenz (KI, oder auch *artificial intelligence*, AI). Wo Firewalls und Antiviren-Programme noch statisch verteidigen, sollen die Cyberabwehrsysteme der neuen Generation, die mit automatisierten Algorithmen arbeiten, in der Lage sein, sich dynamisch neuen Angriffsarten anzupassen und so noch besser auf Bedrohungen reagieren können.[88] Insbesondere die Fähigkeit, Netzwerk-Anomalien erkennen zu können, gilt als Meilenstein zur Verbesserung des Risikomanagements.[89] Dennoch ist die Technologie noch nicht ausgereift und insbesondere die hohe Rate an falsch-positiven Meldungen stellt noch ein Hindernis für den Marktdurchbruch dieser Innovation dar.

Auf der anderen Seite erweitern *Machine Learning* (ML) und KI-basierte Technologien auch die Möglichkeiten der Cyberangreifer: Manipulation von (Künstlicher Intelligenz) KI oder Angriffe mittels KI werden neue Herausforderungen für den digitalen Raum schaffen.[90] Letztendlich wird Technologie allein die Cyberbedrohungen unserer Zeit nicht verhindern können. Intelligente Regulierung und Monitoring sind notwendige Bedingungen, um Resilienzen proportional zum Risiko aufzubauen.

2.6 Schutz und optimales Sicherheitsniveau

Die individuelle wie auch gesellschaftliche Antwort (*response*) auf eine bestimmte Bedrohung besteht darin, Schutzmaßnahmen unterschiedlicher Art zu ergreifen (rote Markierung in Abbildung 2, weiter oben).[91] Deren Ziel ist es, das Bedrohungsniveau, mithin den Erwartungswert von Schäden, für Individuen zu senken. Abbildung 3 verdeutlicht diesen Zusammenhang mit einer einfachen Darstellung.

[88] Vgl. Kubovič 2019.

[89] Vgl. CyberPedia.

[90] Vgl. Avast 2019.

[91] Das Verständnis von Schutzmaßnahmen bzw. Sicherheitspolitik als Antwort bzw. *response* wird wiederkehrend in der Literatur verwendet, so etwa bei Ehrlich (1996, S. 4), bereits mit Rückgriff auf Jeremy Bentham, oder bei Gill (2017, S. 982).

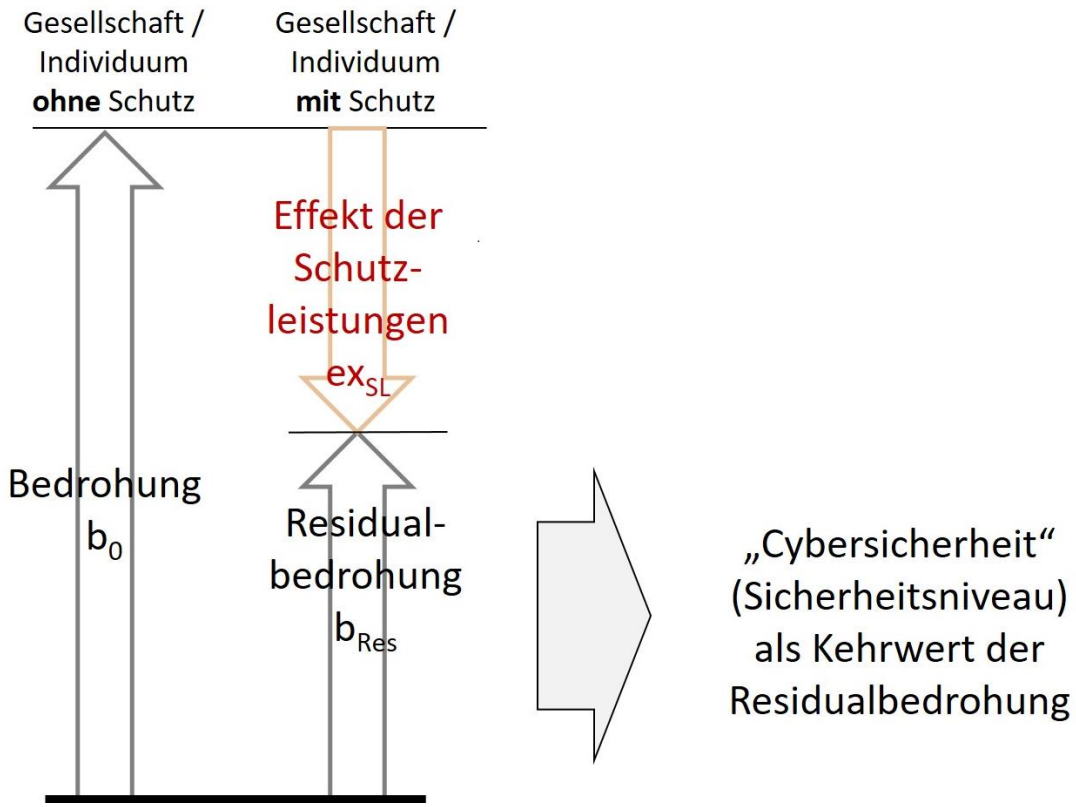


Abbildung 3 Bedrohung und Schutz
Quelle: Eigene Darstellung.

Der linke Pfeil der Abbildung stelle den Umfang der (Ausgangs-)Bedrohung b_0 dar, wie sie in Formel 2-1 wiedergegeben ist. Dieses Maß an Bedrohung besteht also, wenn Schutzguteigentümer möglichen Angriffen „schutzlos“ ausgeliefert sind. Auf der rechten Seite der Abbildung ist dargestellt, wie das Bedrohungsniveau sinkt, wenn Schutzleistungen bzw. Schutzmaßnahmen wirksam und effektiv werden. Somit ergibt sich die Residualbedrohung als Differenz:[92]

$$b_{Res} = b_0 - e \cdot x_{SL} \quad (2\text{-}2)$$

$$b_{Res} = P \cdot l - e \cdot x_{SL} \quad (2\text{-}3)$$

Mit $SN = \frac{1}{b_{Res}}$ (Sicherheitsniveau als Kehrwert der Residualbedrohung) ergibt sich für das Sicherheitsniveau (die Cybersicherheit):[93]

$$SN = \frac{1}{P \cdot l - x_{SL} \cdot \mathrm{e}} \qquad (2\text{-}4)$$

Fasst man das Sicherheitsniveau (Cybersicherheit) derart, dann

[92] Legende (Forts.): b_{Res} – Residualbedrohung; x_{SL} – Umfang der Schutzleistungen; e – Effektivität.
[93] Legende (Forts.): SN – Sicherheitsniveau.

- steigt (sinkt) es, wenn die Ausgangsbedrohung sinkt (steigt);
- steigt (sinkt) es, wenn der Schutzleistungsumfang (x_{SL}) steigt (sinkt);
- steigt (steigt) es, wenn die Effektivität der Schutzleistung (e) steigt.

Für einen Schutzguteigentümer bzw. Staat und Gesellschaft stellt sich nun normativ eine zentrale Frage: In welchem Umfang sollen denn, angesichts einer gegebenen Bedrohung, Schutzmaßnahmen ergriffen werden?[94] Mit anderen Worten: Welche Residualbedrohung ist gesellschaftlich optimal bzw. wünschenswert? Der Hintergrund dieser Frage ist, dass nicht nur die Bedrohung zu Kosten (in Form eines Schadens oder Verlusts) führt, sondern dass auch Schutzmaßnahmen kostenträchtig sind. Schutzmaßnahmen sind also ökonomische, d.h. knappe und ressourcenzehrende Güter, deren Einsatz (ökonomisch: Nachfrage) am Umfang der, ebenfalls kostentreibenden, Bedrohung gemessen werden muss. Zudem sind die Opportunitätskosten zu beachten. Schließlich führen mehr Ausgaben für Schutzleistungen dazu, dass die Mittel nicht für alternative Verwendungen (z.B. Bildung oder Gesundheit) zur Verfügung stehen. Damit ist zugleich die Vermutung verbunden, dass ein „absoluter", „vollständiger" Schutz – ein Schutz mit einer Residualbedrohung „gleich null" – gesellschaftlich gerade *nicht* optimal ist. Die „richtige" Balance[95] zwischen einem Einsatz von Schutzmaßnahmen einerseits und einer bestimmten Residualbedrohung „größer Null" andererseits, ist durch zwei (Kosten-)Größen bestimmt:

- Die Kosten $K_{P \cdot l}$, die sich als Verlust aus dem Schaden durch einen Angriff ergeben.
- Die Kosten $K_{x_{SL}}$, die sich durch den Einsatz von Sicherheitsmaßnahmen ergeben.

Der optimale Umfang an Sicherheitsmaßnahmen ergibt sich nun dort, wo die *Summe* dieser beiden Arten von Kosten am geringsten, also ein Minimum erreicht ist. Die Funktion der Gesamtkosten laute also:

$$K_{ges} = K_{P \cdot l} + K_{x_{SL}} \quad (2\text{-}5)$$

Deren Minimum ergibt sich, wenn gilt (*first order condition*):

$$\frac{dK_{ges}}{dx_{SL}} = 0 \qquad (2\text{-}6)$$

[94] Natürlich stellt sich in der Praxis gerade auch die Frage, *welche* (Art von) Sicherheitsmaßnahmen ergriffen werden sollen. Es geht gewissermaßen nicht nur um Quantität, sondern auch um Qualität. Auf dieser abstrakten Ebene sei davon zunächst abstrahiert. Es wird an dieser Stelle zunächst – ganz neoklassisch – von einer bestimmten „homogenen" Sicherheitsmaßnahme ausgegangen.

[95] Zur ökonomischen Perspektive im Bereich der Sicherheitspolitik vgl. etwa Bretschneider et al. 2018.

mit (*second order condition*)

$$\frac{d^2 K_{ges}}{dx_{SL}^2} > 0 \qquad (2\text{-}7).$$

Mit Hilfe von Abbildung 4 lässt sich dies auch grafisch nachvollziehen.

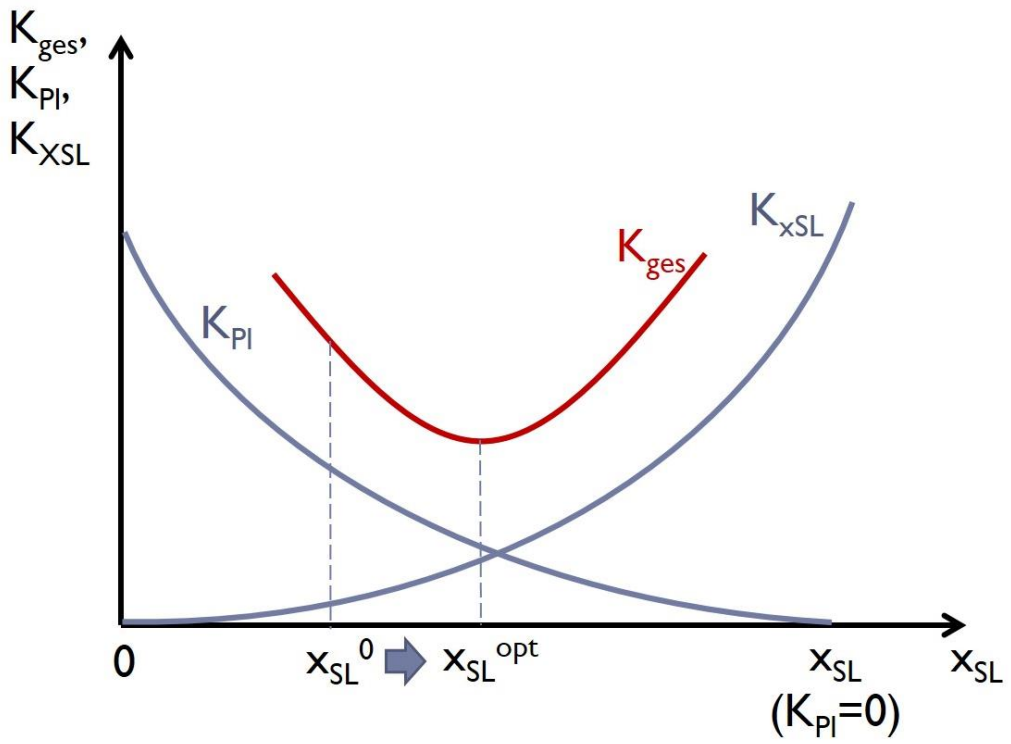


Abbildung 4 Optimaler Einsatz von Schutzleistungen
Quelle: Eigene Darstellung.

Die Abszisse zeigt den Umfang der umgesetzten Menge an Schutzleistungen (x_{SL}). Auf der Ordinate sind die Kosten abgetragen. Wenn man sich auf der Abszisse vom Koordinatenursprung aus immer weiter nach rechts bewegt, also die Menge der Schutzleistungen X_{SL} steigert, so ergeben sich zwei gegenläufige Kosteneffekte. Die Ausgaben für die Schutzleistungen (K_{xSL}) steigen an. Die Kosten aber, die als Verluste durch die entstehenden Schäden durch Angriffe entstehen (K_{Pl}), nehmen ab. Dabei bildet die Stelle x_{SL} (K_{Pl} = 0) den Gedanken einer „absoluten Sicherheit“ ab. Abgesehen davon, dass dies in der Realität quasi nicht zu erreichen wäre, wird mit dieser Darstellung deutlich, dass, selbst wenn möglich, so doch gesellschaftlich nicht wünschenswert wäre. Die (rote) Kurve der Gesamtkosten (K_{ges}) stellt die Summe dieser beiden Kostenarten dar. Das Optimum in der Bereitstellung von Schutzleistungen x_{SL} ergibt

sich dort, wo die Gesamtkosten ein Minimum ausweisen. Diese Stelle ist in Abbildung 3 als x_{SL}^{opt} ausgezeichnet.

Wenn in der Debatte zur Cybersicherheit gesagt wird, das Niveau an Cyberschutz reiche nicht aus, dann stellt sich dies in der Abbildung dar wie folgt. Die mit der These verbundene Annahme ist, dass wir uns derzeit in einer gesellschaftlich suboptimalen Situation x_{SL}^{0} (vgl. wiederum Abbildung 4) bezüglich des Schutzes bewegen, indem nämlich die Akteure (Schutzgut-eigentümer bzw. Staat) *zu wenig* Schutzleistungen x_{SL} nachfragen. Das führt zu suboptimal hohen Kosten („zu hohe Kosten") durch Schäden

$$K_{P\cdot l}(x_{SL}^{0}) > K_{P\cdot l}(x_{SL}^{opt}) \qquad (2\text{-}8)$$

und suboptimal geringen Kosten (Ausgaben) („zu geringe Ausgaben") für Schutzleistungen x_{SL}

$$K_{x_{SL}}(x_{SL}^{0}) < K_{x_{SL}}(x_{SL}^{opt}) \qquad (2\text{-}9),$$

besonders aber zu suboptimal hohen („zu hohen") gesellschaftlichen Gesamtkosten:

$$K_{ges}(x_{SL}^{0}) > K_{ges}(x_{SL}^{opt}) \qquad (2\text{-}10).$$

Die These ist also, dass in der Wirtschaft und Gesellschaft im Umgang mit Cyberbedrohungen eine Bewegung auf der Abszisse nach rechts nötig ist, um ein gesellschaftliches Optimum zu erreichen. Die Ursachen liegen besonders in **umfassenden Informationsdefiziten von Schutzguteigentümern.** Insbesondere liegen zu wenige Informationen über Bedrohung bzw. zu erwartenden Kosten des Schadens vor. Umgekehrt bestehen Informationsdefizite bezüglich des Schutzeffekts von Schutzleistungen. Schließlich sind auch **externe Effekte** zu berücksichtigen. All dies wird in den Abschnitten 3.1 und 3.2, weiter unten, eingehend diskutiert.

Diese Größen empirisch zu bestimmen, ist schwer. Will man den Wert der Schäden (K_{Pl}) durch Auskunft des Geschädigten (Schutzguteigentümers) ermitteln, dann stellt sich die Frage, inwieweit er Auskunft geben *kann* und inwieweit er es *will*. Bei **Könnens-Defiziten** ist zu berücksichtigen, dass Angriffe zuweilen durch die Opfer selbst gar nicht festgestellt werden. Wenn es sie feststellt, steht das Opfer vor der Frage, inwieweit es selbst den Schadensumfang ermittelt bzw. ermitteln kann.

Der Wert von geistigem Eigentum lässt sich zuweilen, gerade, wenn es sich um die „Kronjuwelen" handelt, kaum ermessen, da er ja für lange Zeiträume in der Zukunft Erträge abwirft

oder abwerfen sollte. Ferner wären etwa indirekte Schäden und Fremdschäden zu berücksichtigen. Mit anderen Worten: Bereits bei der unternehmensindividuellen Schadensermittlung geht es um die Produktion von Informationen – und die ist kostenträchtig und muss unweigerlich ab einem bestimmten Punkt aus Kostengründen (inkl. Zeitaufwand, begrenzt verfügbarem Personal usw.) abgebrochen werden.

Bei **Wollens-Defiziten** werden von den Unternehmen einerseits mögliche Reputationskosten einer Schadenspublikation in Rechnung gestellt. Andererseits ist etwa eine Meldung oder Publikation von Schäden oder Vorkommnissen selbst ein kostenträchtiger Vorgang, der somit jedenfalls nicht unter beliebigen Umständen vorgenommen wird.[96] All dies ist für die Erfassung der Cybersicherheit hochrelevant und wird im Abschnitt 4.1 weitergehend informationsökonomisch betrachtet.

Der Bitkom hat sich bei allen Unwägbarkeiten, im Studienbericht 2018 dieser Aufgabe gestellt. Für die Jahre 2016 und 2017 kommt er dabei zu einem errechneten Gesamtschaden von 43,4 Mrd. EUR.[97] Bei einer Vorgängerstudie aus dem Jahr 2015 lag dieser Wert allerdings noch deutlich höher, bei insgesamt 102,4 Mrd. EUR für die Jahre 2013 und 2014.[98] Aus diesen Ergebnissen sind keine generellen Trends abzuleiten, da sich die Bedrohungslandschaft zu dynamisch und agil zeigt. Werden bspw. systemkritische Schwachstellen identifiziert und ausgenutzt, die weitverbreitet in der Industrie vorkommen, würden Fallzahlen nach oben schnellen.

[96] Informationsökonomisch kann man hier von Kosten des *screening* sprechen (vgl. etwa Fritsch 2018, S. 265 f.). Dies ist auch ein Grund warum etwa bei Umfragen die Rücklaufquote typischerweise weit unter 100 Prozent liegt.

[97] Vgl. Bitkom 2018a, S. 24 f.

[98] Vgl. Bitkom 2015, S.17.

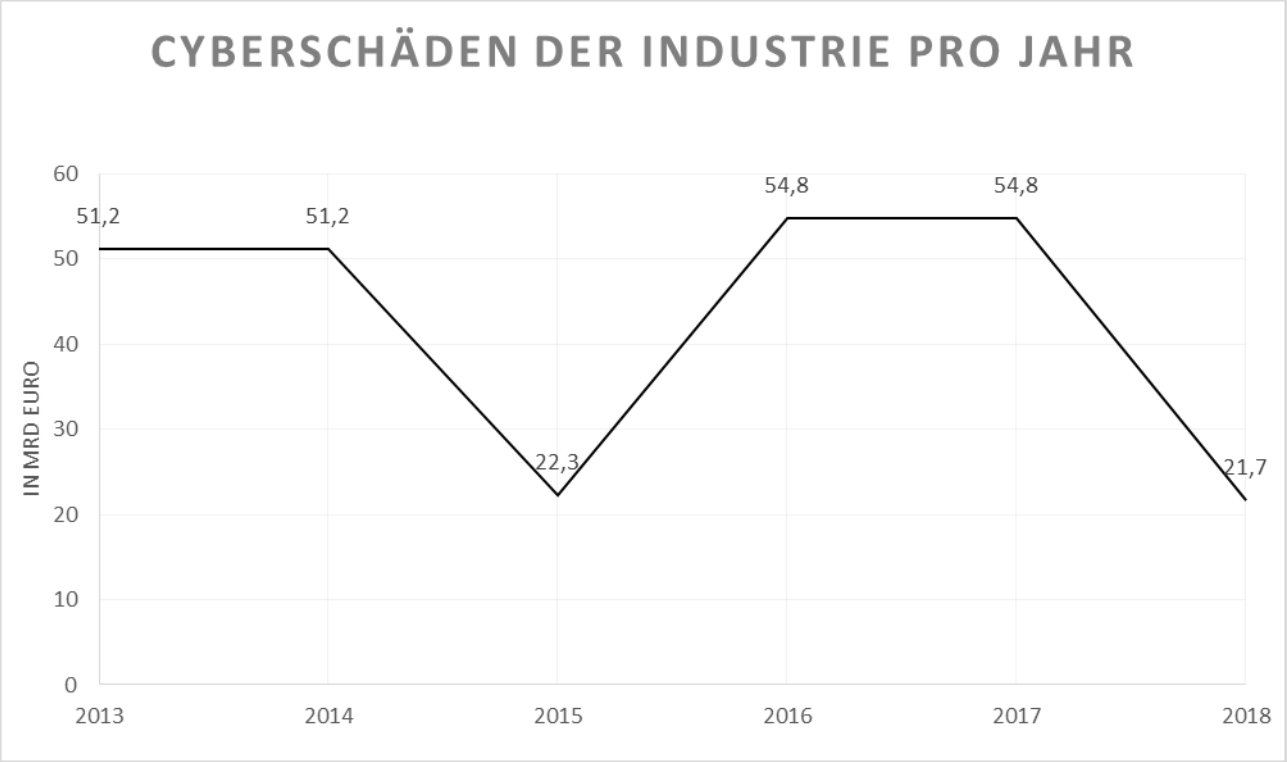


Abbildung 5 Cyberschäden der Industrie pro Jahr
Quelle: Eigene Berechnungen auf der Grundlage von Bitkom (2013, 2014, 2015, 2016, 2017, 2018a).

Das Bundeskriminalamt (BKA) kommt in seinen Veröffentlichungen hingegen auf viel geringere Werte (vgl. Abbildung 6). Hier belaufen sich die festgestellten Schadenssummen lediglich auf zweistellige Millionenbeträge. Sie entstammen den vom Bundeskriminalamt (BKA) jährlich herausgegebenen *Cybercrime Reports*. Darin wird jedoch festgestellt, dass diese Zahlen nur eine eingeschränkte Aussagekraft haben, weil eine hohe Dunkelziffer vorliegt.[99] Mit Verweis auf Umfrageergebnisse von der Bitkom begründet das BKA[100], dass nur etwa 18 Prozent aller Schadensfälle der Polizei gegenüber angezeigt werden.[101] Sie schreiben weiterhin,[102] dass Cyberangriffe und Cyberspionage auch für die deutsche Wirtschaft von Bedeutung sind und weisen auf die hohe Dunkelziffer in diesem Bereich hin.

[99] Vgl. BKA, 2017, S. 3.

[100] Ebd. S. 7.

[101] Hierbei könnte man feststellen, dass dies nur einen Multiplikator von gut 5 erklärt. Der Multiplikator im Vergleich von BKA-Zahlen und Bitkom-Zahlen beträgt aber größenordnungsmäßig 1.000. Zu den Erklärungen für diese Diskrepanz mag gehören, dass einerseits Fallzahlen, andererseits Schadensumfänge betrachtet sind. Jedenfalls wird hierbei auch deutlich, dass der staatlichen Strafverfolgung im Cyberbereich wohl eher eine untergeordnete Rolle zukommt. Für die Rolle öffentlicher Bereitstellung von Schutzleistungen vgl. auch Abschnitt 2.3.

[102] Vgl. BKA 2017, S. 28.

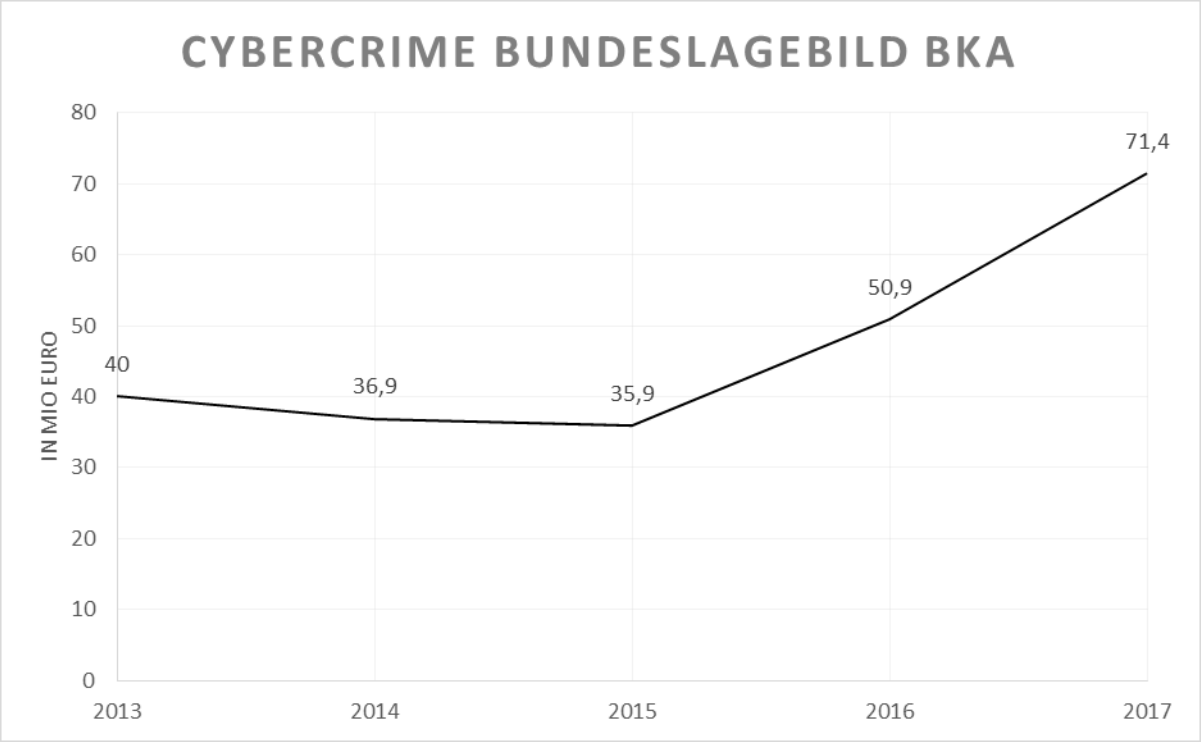


Abbildung 6 Schäden durch Cybercrime gem. Bundeslagebild des BKA
Quelle: BKA (2013, 2014, 2015, 2016, 2017).

Die Erfassung von Kosten für Schutzleistungen ist nicht trivial. Zum einen gibt es Maßnahmen, deren pekuniärer Preis diffus bleibt, etwa bei innerbetrieblichen organisatorischen Maßnahmen. Besonders aber ist Sicherheit eine Komponente von Hardware und Software-Produkten, die nicht nur oder noch nicht in erster Linie Sicherheit zum Ziel haben (PSK). Dennoch hat auch hier der Bitkom eine empirische Erhebung vorgenommen, deren Ergebnis in Abbildung 7 dargestellt ist.

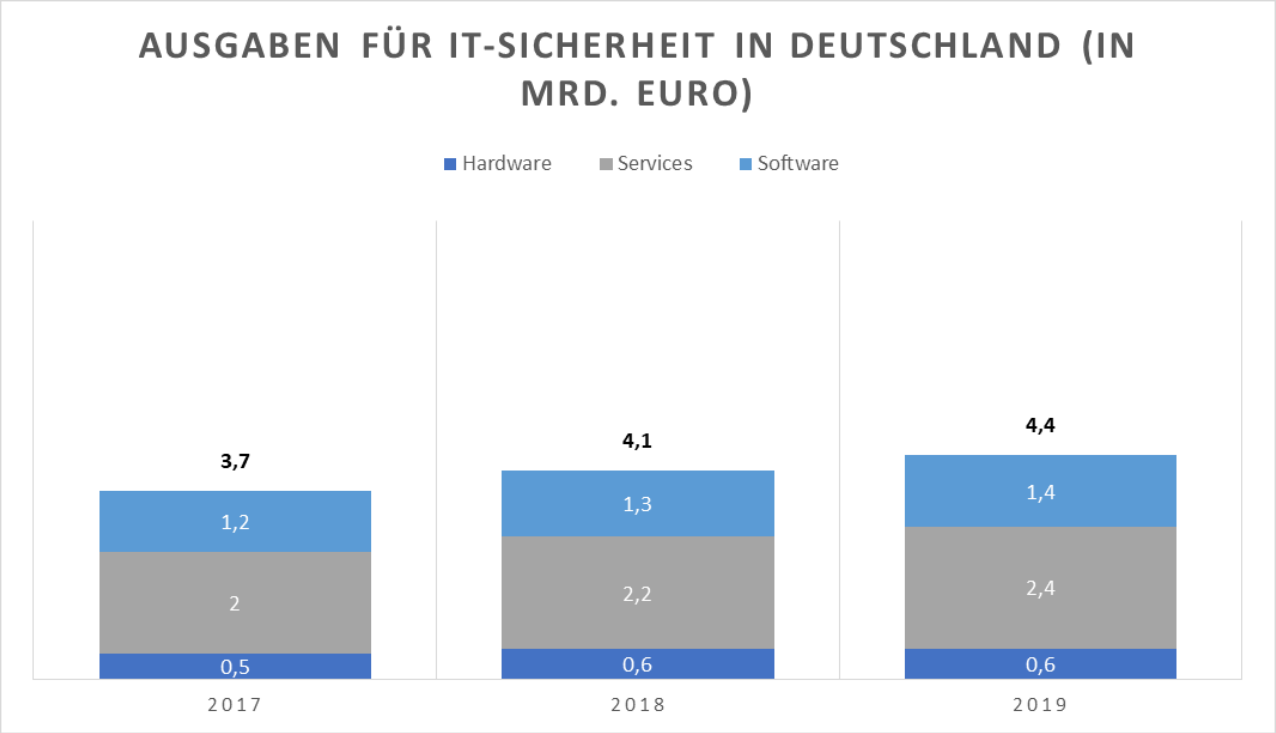


Abbildung 7 Ausgaben für IT-Sicherheit in Deutschland (in Mrd. EUR)
Quelle: Bitkom 2018b.

Demnach kann man monoton steigende Ausgaben für IT-Sicherheit beobachten. Dabei wurde im Jahr 2018 der Betrag von 4 Mrd. EUR überschritten.

Richtet man den Blick in die USA, dann ist dort ebenso – allerdings auf ganz anderem Niveau – ein monotoner Anstieg der Ausgaben zu beobachten.[103] Vergleicht man die Werte für 2018 pro Einwohner, dann werden allerdings in den USA umgerechnet knapp 180 EUR pro Einwohner,[104] in Deutschland knapp 50 EUR pro Einwohner für IT-Sicherheit ausgegeben.

[103] Vgl. Abbildung 8 bzgl. der Gesamtausgaben.

[104] Eigene Berechnung: Bei zugrunde gelegten 327 Millionen Einwohnern in den USA und einem aktuellen Wechselkurs von 0,90EUR/USD.

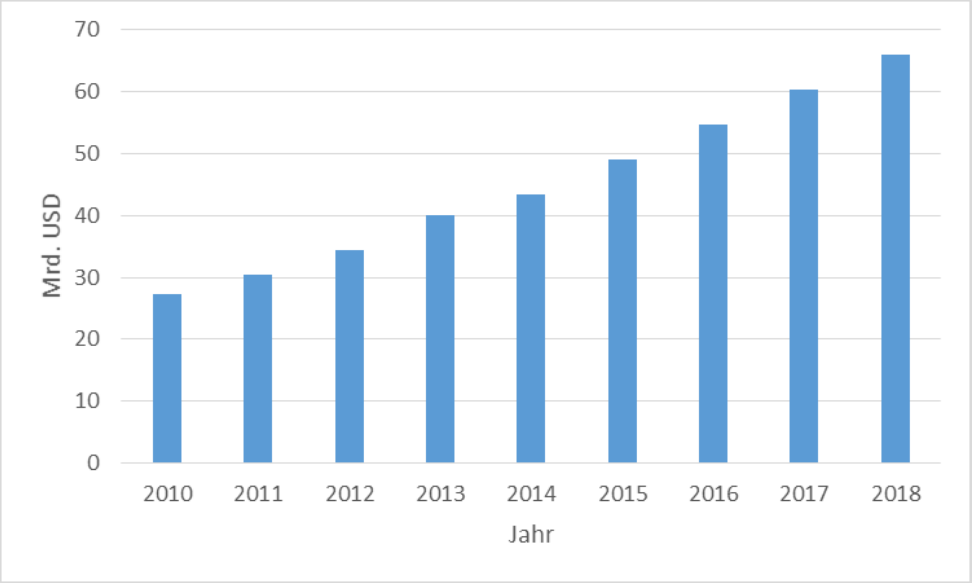


Abbildung 8 Gesamtausgaben für Cybersecurity in den USA von 2010 bis 2018 (in Mrd. USD)
Quelle: Sen 2018, S. 24, mit Berufung auf den Identity Theft Resource Center, o.J.

In jedem Fall aber lässt sich beobachten: Auch diese Entwicklung entspricht mit Blick auf die Abbildung 8 einer Bewegung von links nach rechts auf einer Ausgabenkurve mit (monotoner) Steigung.

Wenn die Annahme stimmt, dass gegenwärtig ein Schutzleistungsniveau vorliegt, das kleiner als das optimale Schutzleistungsniveau ist (also $x_{SL}^{0} < x_{SL}^{opt}$), dann ergeben sich in doppelter Weise Wachstumschancen durch Anpassungen und eine Bewegung in Richtung von x_{SL}^{opt} :

1. mit Blick auf vermiedene Schäden bei Nachfragern von Schutzleistungen bzw. IT-SP/PSK (Reduzierung von $K_{P.l}$) zzgl. Wachstumschancen in mit weniger Schutzleistungen vermiedenen Geschäftsmodellen und Teilmärkten (*Enabler*-Perspektive).

2. mit Blick auf Wachstumschancen von Anbietern von IT-SP/PSK (Erhöhung der Ausgaben für SL, *Driver*-Perspektive).

Dabei zielt die Perspektive „Wachstum“ im Kontext der Cybersicherheit auf eine wirtschaftliche Entwicklung im Rahmen eines angemessenen, also gesellschaftlich effizienten Einsatzes von Schutzleistungen.[105]

[105] Mit Blick auf Abbildung 4 geht es um Erreichung des Optimums x_{SL}^{opt}.

2.7 Mehrstufigkeit des Schutzes

Es gibt viele unterschiedliche Formen von Schutzleistungen. In Abbildung 1 wurde in 3 Kategorien a) Technologie, b) Humankapital und c) Risikotransfer unterschieden. Schutzleistungen können auf unterschiedlichen Stufen der Bedrohung begegnen. Sie stehen typischerweise wechselseitig in einem Verhältnis unvollständiger Substituierbarkeit[106] und weisen einen jeweils unterschiedlichen Grad an Präventivität auf.[107] Im Anschluss an Abbildung 1 zeigt Abbildung 9 drei idealtypische Stufen von Schutzleistungen im Problemfeld Cybersicherheit. Dabei handelt es sich auf Stufe 1 typischerweise um öffentliche Güter, die also nicht der jeweilige Schutzgut-eigentümer individuell nachfragt. Auf den Stufen 2.1 bzw. 2.2 hingegen handelt es sich um marktgängige bzw. private Güter.[108] Dabei lässt sich Dreistufigkeit im Prinzip auch im Bereich der offline-Sicherheit finden.[109]

[106] Dies ist ein Begriff aus der mikroökonomischen Entscheidungstheorie (vgl. statt vieler nur Gawel 2009).

[107] Vgl. Bretschneider et al. 2018, S. 9 f.

[108] Die Begrifflichkeit öffentliche und private Güter wird hier im Sinne der ökonomischen Fachbegriffe gebraucht, besonders gemessen am Kriterium der Exkludierbarkeit. Diese Definition unterscheidet sich von der Begriffsnutzung in nicht-ökonomischen bzw. öffentlichen Debatten. Da wird unter einem „öffentlichem Gut“ ein Gut verstanden, welches der Staat bereitstellt oder bereitstellen soll. Im letzten Fall entspricht das einer Bedeutung, der in der ökonomischen Begrifflichkeit beispielsweise auch das *meritorische* Gut entspricht.

[109] Vgl. Bretschneider et. al. 2020, S. 104 ff.

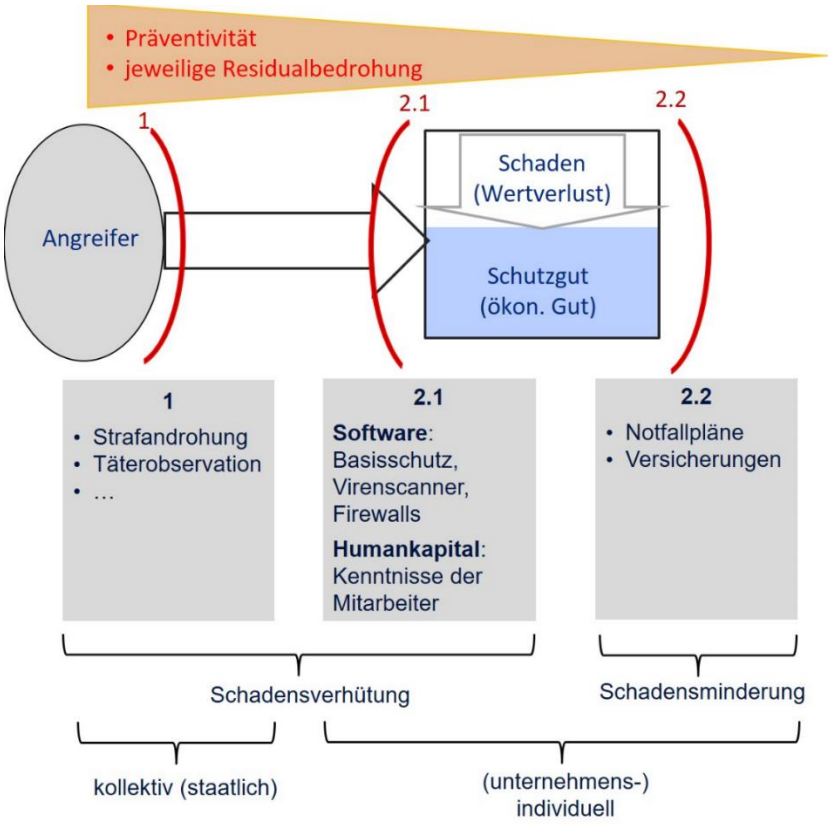


Abbildung 9 Angriff und Schutz auf Stufen unterschiedlicher Präventivität
Quelle: Eigene Darstellung.

Auf einer ersten Stufe (1) können Schutzleistungen als öffentliche Güter „nahe am Täter“ oder jedenfalls jenseits eines einzelnen Schutzgutes ansetzen. Sie sind also „weiter weg“ vom einzelnen Schutzgut und bieten Schutz für eine Vielzahl von Schutzgütern. Sie besitzen in Bezug auf die Bedrohung eine geringe Spezifität.[110] Die prominenteste Schutzleistung auf dieser Stufe ist die Strafverfolgung bzw. Bestrafung, sog. *repressive* Schutzleistungen, die in ihrer Präventionsfunktion potenzielle Täter abschrecken, indem sie den Erwartungswert der Bestrafung in ihr Kalkül einbeziehen.[111] Eine Vielzahl von Schutzguteigentümern profitiert dabei von dieser Schutzleistung. Entsprechend werden Schutzleistungen dieser Art, wegen des Trittbrettfahrerproblems bei Exklusionsdefiziten, typischerweise kollektiv und idealtypisch vom Staat bereitgestellt.

Auf der Stufe (2.1) kann für ein bestimmtes Schutzgut ein Schutz zwecks Schadensverhütung und Abwehr von Eindringlingen eigenverantwortliche Schutzleistungen in Form von Produkten

[110] Vgl. Stuchtey und Skrzypietz 2014, S. 203.

[111] Dies entspricht der Argumentation der *economics of crime*, die auf den bahnbrechenden Artikel von Gary S. Becker (1968) zurückgeht.

aus der Privatwirtschaft zum Tragen. Dies geschieht in der *offline*-Sicherheit etwa durch Türen und Türschlössern, im Cyberbereich etwa durch Virenscanner oder Firewalls. Neben diesen technischen Möglichkeiten lässt sich aber auch im Cyberbereich zwecks Schadensverhütung auch in das Humankapital investieren. So kann ein Unternehmen bestimmte Verhaltensregeln für Mitarbeiter einführen, um z.B. Angriffe mittels *social engineering* zu verhindern.

Schließlich kann auf einer Stufe (2.2) ein Schutzguteigentümer (insbes. auch Unternehmen) eine Schadensminderung anstreben, gleichsam in der „letzten Verteidigungslinie" der genannten drei. Hierzu gehört die „Härtung" des Schutzguts zur Steigerung der Resilienz. Ebenso gehört dazu das Aufstellen von Notfallplänen und der Abschluss von Cyberversicherungen.[112]

Im Gegensatz zur Stufe (1) hat für die beiden Stufen (2.1) und (2.2) der einzelne Schutzguteigentümer (Unternehmen) die individuelle Verantwortung. Dabei hat er nicht nur zu entscheiden, in welchem Umfang er überhaupt in (Cyber-)Schutzleistungen investiert; und auch nicht nur, welcher Art die Schutzgüter im Allgemeinen sein sollen; sondern schließlich auch, wie hoch der Präventionsgrad der unterschiedlichen individuell nachgefragten Schutzleistungen sein bzw. wie sein optimaler Mix ausgestaltet sein soll.[113][114]

Gesellschaftlich stellt sich wiederum die Frage nach der angemessenen (effizienten) Balance zwischen öffentlichen (Stufe 1) und privaten Schutzleistungen (Stufe 2). Neben der allgemeinen Frage nach der Substituierbarkeit von privaten und öffentlichen Gütern,[115] wurde diese Frage in der Literatur bereits auch für den Bereich der Sicherheit diskutiert.[116] Unstrittig dürfte dabei jedenfalls sein, dass die private Nachfrage nach Schutzleistungen steigt, wenn die öffentliche Bereitstellung von Schutzleistungen, mithin die Durchsetzung des Rechts, abnimmt oder die Bedrohung zunimmt.[117]

Im Vergleich zwischen den Bereichen der *offline*- und der Cybersicherheit gilt nun die allgemeine Einschätzung, dass in der Cybersicherheit die privat nachgefragten Schutzleistungen der Stufe 2 im Vergleich zu den öffentlich bereitgestellten Schutzleistungen eine größere relative

---

[112] Vgl. statt vieler BIGS 2017, Wrede et al. 2018.

[113] Vgl. Ehrlich und Becker 1972.

[114] Die hier dargestellte Dichotomie von Schadensabwehr und Schadensminderung ist natürlich sehr grob. Zum tatsächlich von Entscheidungsträgern in einem Experiment gewählten Mix vgl. Yaakov et al. 2019.

[115] Vgl. Bergstrom und Goodman 1973.

[116] Vgl. Clotfelter, 1977; Tulkens und Jacquemin, 1971.

[117] Ein prominentes historisches Beispiel ist die sizilianische Mafia, die Ende des 19. Jahrhunderts als „privater Sicherheitsdienstleister" bei geringer *rule of law* und plötzlich steigender Bedrohung nachgefragt wurde (vgl. Dimico et al. 2017).

Bedeutung haben. Das ist vor allem darin begründet, dass für Cyberangreifer Geografie unerheblich ist, für hoheitliches Handeln von Strafverfolgungsbehörden dagegen schon. Für Polizeibehörden enden die Befugnisse an der territorialen Grenze. Vor diesem Hintergrund werden sich die weiteren Überlegungen im Rahmen dieser Studie auf privat, durch die Schutzguteigentümer, nachgefragte Schutzleistungen fokussieren.[118]

Bevor der Bereich der öffentlichen Güter bzw. öffentlicher Schutzleistungsbereitstellung abgeschlossen wird, sei noch auf einige Aspekte in diesem Zusammenhang aufmerksam gemacht. Zunächst besteht bei der Strafverfolgung neben der Frage des Hoheitsgebietes weiterhin das Problem der genauen Attribution/Feststellung der Täter. In vielen Fällen ist es besonders aufwändig oder gar unmöglich, den Urheber einer Attacke zu identifizieren.

Öffentliche Güter bzw. Schutzleistungen höherer Präventivität gibt es nicht nur im Rahmen der Strafverfolgung. Die Deutsche Telekom etwa füttert ihr Netz mit „Anti-Viren“ um hier eine erste Stufe eines Schutzes gegenüber einschlägigen Bedrohungen bereitzustellen. Dabei mag sich die Frage stellen, ob hierfür eine staatliche Regulierung nötig ist, dass alle Netzanbieter derartige Anti-Viren bereitstellen. Es mag sich hier aber auch ein spontaner Marktstandard durchsetzen. Der institutionelle Zugriff für eine staatliche Regulierung wäre wohl die Eigenschaft dieser Netze als KRITIS („Sektoren […] Informationstechnik und Telekommunikation“, § 2 Abs. 10 Nr. 1 BSIG).

2.7.1 Rolle des Staates

Eine Rolle der öffentlichen Hand – wiederum als Regulierer oder Marktteilnehmer – ist aus ordnungspolitischer Sicht angebracht, wenn öffentliche Güter oder Allmende-Güter betroffen sind. Letztere spielen im Kontext von Forschung und Innovation im Zusammenhang mit Cybersicherheit keine Rolle, öffentliche Güter hingegen schon. Diese liegen dann vor, wenn einerseits keine Rivalität in der Nutzung vorliegt, und andererseits keine Ausschließbarkeit von der Nutzung (technisch oder organisatorisch) zu verhältnismäßigen Kosten realisierbar ist. Trifft beides zu, so ist davon auszugehen, dass keine Organisierbarkeit der Ressourcenallokation über Marktmechanismen vorliegt.

[118] Dies ist unbenommen der Tatsache, dass der Staat für seine eigenen Institutionen, Prozesse und Systeme selbst Schutzleistungen nachfragt. Und es ist auch unbenommen der Tatsache, dass der Staat gerade bei KRITIS-Unternehmen als Regulierer auftritt.

Wenn zum Beispiel aufgrund der **Nichtausschließbarkeit** ein ausgeprägtes Trittbrettfahrer-Problem verhindert, dass sich ein ausreichender Anteil der privaten Unternehmen (oder auch der privaten Haushalte) wirkungsvoll mit qualitativ hochwertigen und tendenziell kostspieligen Virenscannern gegen Schadsoftware-Befall ihrer IT-Systeme schützt, so könnte der Staat als Regulierer oder Subventionierer auftreten. Mit anderen Worten, wenn sich allzu viele Unternehmen darauf verlassen, dass schon andere Unternehmen mit Investitionen in technische Cybersicherheit für eine ausreichende Herdenimmunisierung sorgen, kann der Staat entweder ein Mindestmaß solcher Investitionen vorschreiben und die Einhaltung kontrollieren, oder aber die von Unternehmen zu zahlenden Preise für derartige Investitionen mit Hilfe von Zuschüssen absenken und so die finanzielle Hemmschwelle senken. (Ähnliche Effekte wie eine staatliche Regulierung könnten die Geschäftsbedingungen von Cyberversicherungsgesellschaften erzielen, welche dann als Quasi-Regulierer fungieren würden.)

Es könnte auch jenseits von öffentlichen Gütern – also bei privaten Gütern oder Klubkollektivgütern – Gründe für Marktversagen in verschiedener Form geben, die eine staatliche Einflussnahme rechtfertigen oder gar ratsam erscheinen lassen können. Dies wäre etwa dann der Fall, wenn der Markt für Cybersicherheits-Produkte und Dienstleistungen durch ausgeprägte Informationsasymmetrien geprägt ist. Hier könnten staatliche Stellen die Rolle eines unabhängigen und neutralen Bereitstellers von Informationen zu Quantität und Qualität von Bedrohungen sowie zur Qualität von Schutz-Angeboten (bspw. mittels von Zertifizierungen) einnehmen. Auch das Vorliegen erheblicher (negativer) externer Effekte kann zwecks Internalisierung der Kosten eine staatliche Einflussnahme erfordern.

Aus ordnungspolitischer Sicht – aus fiskalischen Gründen sowie zwecks Minimierung vermeidbarer Wettbewerbsverzerrungen – abzulehnen sind hingegen Eingriffe des Staates in Märkte privater Güter, in denen kein Marktversagen vorliegt. Denkbar ist ein solcher Fall zum Beispiel beim Schutz von Produktionsprozessen eines herkömmlichen Industrieunternehmens. Wird dieses Unternehmen Opfer einer erfolgreichen Cyberattacke, und muss daraufhin seine Produktion für eine gewisse Zeit zurückfahren oder unterbrechen, so ist das zunächst aus volkswirtschaftlicher Sicht nur das Problem dieses Unternehmens.

Grundsätzlich kann es darüber hinaus aus Sicht der Wirtschafts- und **Industriepolitik** Ziel der Maßnahmen der öffentlichen Hand sein, Wettbewerbsvorteile der deutschen Cybersicherheitsbranche im Bereich Forschung und Innovation erstens zu identifizieren, und sie zweitens – ggf. im Einklang mit multilateralen Regel- und Vertragssystemen – zu schützen oder gar auszuweiten.

Die für staatliche Eingriffe denkbaren Instrumente unterscheiden sich je nach betrachteter Gruppe der Unternehmen etwas. Im Bereich der als *Driver* klassifizierten Unternehmen (sowie nicht privatwirtschaftlicher Forschungs- und Entwicklungseinrichtungen) sind Eingriffe in Form von Regulierung, Subvention und Marktteilnahme möglich. Reguliert werden kann bspw. in Form von Transparenz- und Kennzeichnungsvorschriften. Forschung und Entwicklung kann mit Zuschüssen gefördert werden. Am Markt kann der Staat in zwei Rollen eingreifen: Einerseits als Nachfrager von Schutzprodukten und Dienstleistungen, andererseits als Anbieter öffentlicher Güter.

Im Bereich der *Enabler* sind vor allem Regulierung und Subventionen denkbar. Reguliert werden kann bspw. in Form von Regelungen zu Mindestschutz und Haftung. Investitionen in Produkte und Dienstleistungen der Cybersicherheit könnten in Form von staatlichen Krediten und Zuschüssen unterstützt werden, wie dies etwa die staatseigene Kreditanstalt für Wiederaufbau (KfW) ähnlich mit Investitionszuschüssen im Bereich (analogen) Einbruchschutzes tut.

Für die weitergehenden Analysen erscheint es sinnvoll, auf Grundlage des betrachteten Sicherheitsproblems und möglicher Lösung nun Märkte und dessen Akteure sowie die staatlichen Institutionen für Cybersicherheit in Deutschland zu betrachten.

2.7.2 Märkte für Cybersicherheit

Im Zentrum dieses Kapitels steht hier der Markt für Schutzleistungen bzw. IT-SP/PSK, für den *cum grano salis* im Abschnitt 2.4 für Deutschland ein Umsatz von nunmehr über 4 Mrd. EUR im Jahre 2018 festgestellt wurde.[119] Auf der einen Seite sind hier die Nachfrager dieser Güter und Leistungen zu betrachten ((a) in nachfolgender Abbildung 10). In der *Enabler*-Perspektive sind dies Unternehmen, die sich durch angemessene Cybersicherheits-Investitionen hinreichend schützen wollen, um im Kontext zunehmender Digitalisierung ihr Potenzial ausschöpfen zu können. In der *Driver*-Perspektive und auf der Anbieterseite stehen Unternehmen, die durch Dienste und Produkte in diesem Bereich genau diese Nachfrage adressieren können und somit ihrerseits einen Wachstumsimpuls erfahren ((b) in Abbildung 10). Die Abbildung 10 und dieser Abschnitt sollen deutlich machen, dass über die Bilateralität dieser beiden Marktseiten hinaus noch weitere relevante Akteure und (Teil-)Märkte in den Blick zu nehmen sind, wenn je eine *Enabler*- oder *Driver*-Perspektive eingenommen werden soll. Denn auch dort werden jeweiligen Wachstumsmöglichkeiten determiniert.

[119] Vgl. Abbildung 7.

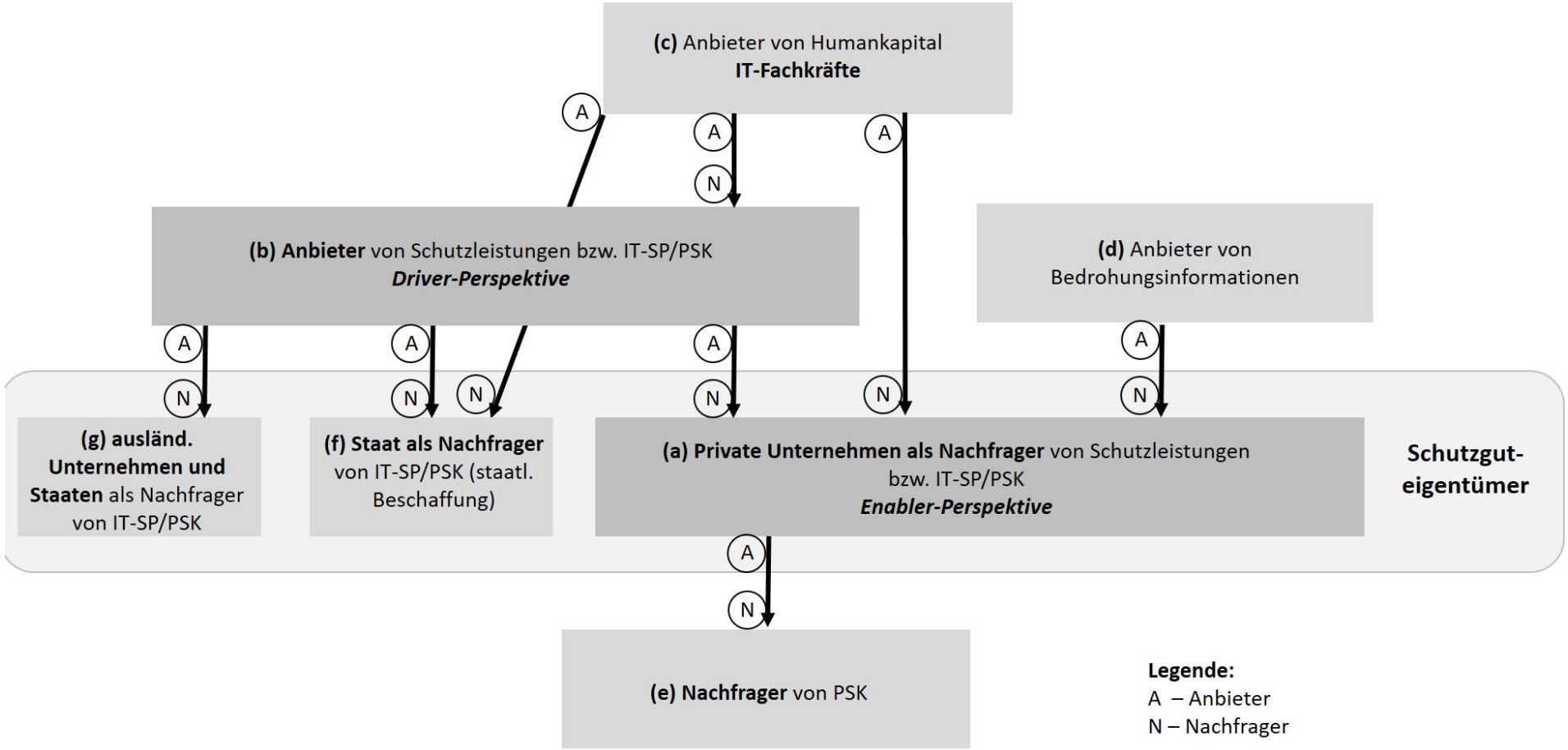


Abbildung 10 Akteure auf den Märkten um den Markt für IT-SP/PSK
Quelle: Eigene Darstellung.

Aus der *Enabler*-Perspektive stehen **Unternehmen als Schutzguteigentümer (a)**, und damit als Nachfrager auf Märkten für IT-SP/PKS im Zentrum des Interesses. Dies sind vielfach private oder öffentliche Unternehmen, für die die Digitalisierung von Prozessen und Produkten vor allem Produktivitätswachstum zum Ziel hat. Damit einher geht aber unwillentlich auch, sich stärker der Cyberbedrohung auszusetzen. Es sind Unternehmen, die unterschiedliche Dinge produzieren bzw. Dienstleistungen erbringen. Die Digitalisierung verspricht eine Produktivitätssteigerung in nahezu allen Wirtschaftsbereichen. Für diese Unternehmen wird die Cyberbedrohung zur Wachstums- und Innovationsbremse, weil sie die Profitabilität von Investitionen in die Digitalisierung der Produktion reduziert. Abschnitt 4.1, weiter unten, widmet sich ausführlicher Unternehmen als Schutzguteigentümer (*Enabler*-Perspektive) mit Blick auf *innovative* Unternehmen (IU).

Derartige Unternehmen haben in jedem Fall auf ihrem jeweiligen Absatzmarkt mit den **Nachfragern ihrer jeweiligen Produkte und Dienste (e)** umzugehen. Hierbei stellt sich etwa auch die Frage, inwieweit die Unternehmen gegenüber ihren Nachfragern die Vorteilhaftigkeit ihrer Investitionen in Cybersicherheit glaubhaft vermitteln und dies entsprechend als Wettbewerbsparameter einsetzen können. Das ist für das Nachfrageverhalten auf dem (Faktor-) Markt für IT-SP-PSK sehr relevant, da (jedenfalls bei privaten Unternehmen) *nur hier* der Erlös generiert werden kann, mit dem auf den für Cybersicherheit relevanten Faktormärkten nachgefragt wird.[120]

In vielen Fällen benötigen Unternehmen als Schutzguteigentümer **IT-Fachpersonal (c)**, um effizient am Markt für IT-SP/PSK zu investieren und um ein cybersicheres Umfeld zu etablieren. Dabei handelt es sich gleichsam um ein Komplement zu IT-SP/PSK.[121]

Eher wenig Aufmerksamkeit erhält in der Debatte bislang der Markt für **Bedrohungsinformationen (d)**; jedenfalls wird er als solcher bislang nicht explizit gemacht. Um ein rationales Risikomanagement durchführen zu können, hat der Schutzguteigentümer jedoch ein substanzielles Interesse an Informationen zu Art und Umfang der Bedrohung bzw. den zu erwartenden Schäden. Ferner stehen genau diese Informationen im Zentrum, wenn das „Bewusstsein“ (*awareness*) für die Herausforderung gesteigert und das Thema – wie vielfach gefordert – in Unternehmen „zur Chefsache“ gemacht werden soll.[122]

[120] Vgl. hierzu Kapitel 3.1.3.
[121] Vgl. hierzu Kapitel 5.
[122] Vgl. hierzu Kapitel 3.1.2.

In der *Driver*-Perspektive stehen die **Anbieter von IT-SP/PSK (b)** im Zentrum. Diese Art von Unternehmen bieten Leistungen für in Schutzguteigentümer in dessen Schutz-/Sicherheitsinteresse an. Dabei kann es sich um Software (Virenschutzprogramme), um Hardware oder um Dienstleistungen handeln. Hierunter fallen zudem auch Cyberversicherungen, die für den Schutzguteigentümer ebenfalls eine Möglichkeit sind, mit dem Risiko umzugehen.[123] Auch sie fragen auf dem Arbeitsmarkt **Humankapital bzw. IT-Fachkräfte (c)** nach und stehen damit auf diesem Markt in Konkurrenz mit ihren Nachfragern.

Für den Absatzmarkt der Anbieter von IT-SP/PSK ist herauszuheben, dass dort nicht nur private Unternehmen und nicht nur Organisationen aus Deutschland auftreten. Hier ist vielmehr einerseits auch der (deutsche) **Staat ein Nachfrager (f)**, im Rahmen seines eigenen Bedarfs nach IT-SP/PSK. Insofern hat gerade auch das staatliche Beschaffungswesen einen Einfluss auf Wachstumschancen von IT-SP/PSK-Anbietern. In dieser Rolle fragt im Übrigen auch der Staat IT-Fachkräfte am Arbeitsmarkt nach und konkurriert dabei folglich mit Anbietern wie anderen Nachfragern von IT-SP/PSK. Und andererseits sind im Rahmen des internationalen Handels auch **Nachfrager (private wie staatliche) aus dem Ausland (g)** zu berücksichtigen. Auch sie bilden eine Determinante für die Wachstumschancen der IT-SP-PSK-Anbieter.

Abschließend ist bei dem Blick auf die Akteure noch auf eine wichtige Uneindeutigkeit hinzuweisen. Eine eindeutige Zuordnung von Unternehmen zu einer der beiden Seiten, Anbieter und Nachfrager von IT-SP/PSK, ist nicht immer oder ohne weiteres möglich. Das liegt darin, dass IT-Sicherheit eben vielfach als eine Komponente eines Gutes vorkommt, daher die Rede von Produkten mit Sicherheitskomponente. Auch die Nachfrager auf den Märkten für IT-SP/PSK (*Enabler*-Perspektive) verkaufen ja wiederum auf ihrem Absatzmarkt ein Gut, das seinerseits die „Komponente Sicherheit“ aufweist. Auch gibt es zahlreiche Unternehmen, die einen starken IT-Sicherheitsdienst zum Eigenschutz aufgebaut haben, deren Dienstleistungen aber auch Dritten anbieten.

[123] Auf Stufe 2.2 in Abbildung 9.

2.7.3 Institutionen der Cybersicherheit in Deutschland

Die staatliche Cybersicherheits-Architektur ist aufgrund ihrer föderalen Struktur durch eine Vielzahl von Behörden auf Landes- und Bundesebene gekennzeichnet. Dazu gehören Strafverfolgungs-, Ordnungs- und Gefahrenabwehrbehörden, genauso wie Nachrichtendienste sowie die Bundeswehr.[124]

Der nationale **Cybersicherheitsrat** ist eine übergeordnete Instanz, der zum einen die politische Zusammenarbeit innerhalb der Bundesregierung organisieren und bei der Koordinierung einer kohärenten Cybersicherheitsstrategie unterstützen, und zum anderen die Verbindung zwischen Staat und Wirtschaft herstellen soll.

Zu den wichtigsten Behörden im Bereich der Cybersicherheit gehören das BSI, die Zentrale Stelle für Informationstechnik im Sicherheitsbereich (ZITiS), die Cyberagentur (die ursprünglich Agentur für Disruptive Innovation in der Cybersicherheit und Schlüsseltechnologien, kurz ADIC hieß) bzw. Cyberagentur des Bundes sowie die militärische Organisationseinheit Kommando Cyber- und Informationsraum (KdoCIR). Dem Bundesministerium des Inneren, für Bau und Heimat (BMI) unterstellt sind dabei BSI, ZITiS sowie ADIC, wobei sich das BMI die Zuständigkeit bei der Cyberagentur mit dem Bundesministerium der Verteidigung (BMVg) teilt.

Auf Bundesebene ist das **BSI**, als zuständige zivile Behörde, für die IT-Sicherheit in Deutschland verantwortlich.[125] Im Geschäftsbereich des BMI ist die Bundesbehörde zudem der zentrale IT-Sicherheitsdienstleister des Bundes und gestaltet durch Detektion, Prävention und Reaktion für Staat, Wirtschaft und die Gesellschaft, die Informationssicherheit im digitalisierten Raum. Des Weiteren ist das BSI für Standardsetzung und Zertifizierung zuständig und mit 940 Stellen (2018) das operative Schwergewicht der zivilen Cybersicherheitslandschaft.[126] Dem BSI unterstellt sind mehrere Lagebildzentren, wie das **nationale Cyberabwehrzentrum** (Cyber-AZ) als Informationsplattform für die verschiedenen Sicherheitsorgane; sowie das nationale IT-Lagezentrum, welches Schwachstelleninformationen für Behörden und Wirtschaft zur Verfügung stellt und bei Bedarf in das IT-Krisenreaktionszentrum umgewandelt wird. Das ***Computer Emergency Response Team*** des Bundes (CERT-Bund) ist ebenfalls beim BSI angesiedelt und kann bei akuten Bedrohungslagen mit einem Notfall-Einsatzteam eingreifen und das weitere Vorgehen koordinieren.

---

[124] Vgl. https://www.bmi.bund.de/DE/themen/it-und-digitalpolitik/it-und-cybersicherheit/.

[125] Vgl. https://www.bsi.bund.de/DE/DasBSI/Leitbild.

[126] Vgl. https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2018/Stellungnahme_Kohlekommission_25102018.html.

ZITiS mit Sitz in München soll bis zum Jahr 2022 eine Größe von 400 Stellen haben und hat zur Aufgabe, die Sicherheitsbehörden des Bundes bei der kontinuierlichen Weiterentwicklung ihrer technischen Fähigkeiten zu unterstützen, sowie den Sicherheitsbehörden als Dienstleister für technische Lösungen und Methoden zur Verfügung zu stehen.[127]

Die neugeschaffene **Cyberagentur** mit dem Standortbeschluss in Halle/Leipzig soll analog zum Vorbild der US-amerikanischen *Defense Advanced Research Projects Agency* (DARPA), Innovationen fördern, finanzieren und insbesondere disruptive Technologien und Prototypen hervorbringen. Es geht um das ambitionierte Ziel, die technologische Innovationsführerschaft Deutschlands sicherzustellen.[128] Hier sind bis 2022 etwa 100 Stellen zu besetzen.[129]

Kritik gab es bereits nicht nur wegen der Standortwahl. Der Bundesrechnungshof bemängelte die dürftige und bisher nur z.T. geleistete Finanzierung und stellte fest, dass die Personalgewinnung äußerst schwierig werden würde (Besserstellungsverbot).[130] Darüber hinaus sieht der Bundesrechnungshof ein viel größeres und kritischeres Problem, die staatliche Mehrfachförderung. Es ist nicht klar inwiefern sich die Cyberagentur klar von anderen „Cyber-Behörden" abgrenzt und somit auch beim Personal in Konkurrenz zu den anderen Behörden steht, da auf dem Arbeitsmarkt für IT-Fachleute bereits jetzt die Nachfrage das Angebot übersteigt.

Der **Cyber- und Informationsraum** (CIR) der Bundeswehr ist ein seit 2017 bestehender eigenständiger militärischer Organisationsbereich mit dem Auftrag Deutschland im Cyber- und Informationsraum zu verteidigen. Während die Legitimität der Abwehr von Cyberangriffen auf die Netze der Bundeswehr als Aufgabenbereich unumstritten ist, gibt es seit der Gründung kontroverse Diskussionen darüber, ob und auf welcher rechtlicher Basis offensivere Aufgaben wahrgenommen werden können.[131] Das **Kommando Cyber- und Informationsraum** (KdoCIR) in Bonn ist das Führungskommando, welches alle IT-Kompetenzen und -Kapazitäten der Bundeswehr bündeln soll und sowohl für die truppendienstliche Führung, als auch für angestellte zivile Fachkräfte zuständig ist. Zum Organisationsbereich CIR gehören ca. 13.500 Dienstposten, der 2021 vollkommen einsatzbereit sein soll.[132]

---

[127] Vgl. https://www.bmi.bund.de/SharedDocs/pressemitteilungen/DE/2017/01/zitis-vorstellung.html.

[128] Vgl. Koalitionsvertrag 2018, S. 159.

[129] Vgl. https://www.bmi.bund.de/SharedDocs/pressemitteilungen/DE/2019/07/20190703-cyberagentur.html.

[130] Vgl. Meister und Biselli 2019a.

[131] Vgl. Meister und Biselli 2019b.

[132] Vgl. https://www.bmvg.de/de/themen/cybersicherheit/cyber-verteidigung/entwicklung-des-org-bereich-bei-der-bw

Neben der Etablierung des Studiengangs Cybersicherheit an der Bundeswehruniversität in München wurde mit einer ministeriellen Entscheidung das Forschungsinstitut CODE gegründet, um fachliche Expertise im Bereich *Cyber Defence* aufzubauen und weiterzuentwickeln. Im BMVg sind somit Kompetenzen in den Bereichen Ausbildung, Forschung, operative Maßnahmen und Innovation gebündelt. Die inhaltliche Abgrenzung zu den zivilen Behörden, zumindest in den Bereichen Forschung und Innovation, ist nicht klar geregelt und kann somit zu Doppelstrukturen führen, die finanzielle Mittel binden und zu Konkurrenz bei der Personalanwerbung führen können. Aus einer ordnungspolitischen Perspektive wäre ein regelmäßiger und institutionalisierter Austausch der Behörden zu den verschiedenen Forschungs- und Innovationszielen wünschenswert, um Innovationsdoppelungen zu vermeiden.

Das Bundesministerium für Bildung und Forschung (BMBF) fördert seit 2011 die drei Kompetenzzentren **CISPA** (Saarbrücken), **CRISP** (Darmstadt) und **KASTEL** (Karlsruhe), die Informationssicherheitsforschung und Wissenstransfer vereinen. Die Kompetenzzentren vereinen dabei vor allem universitäre Grundlagenforschung mit der angewandten Forschung verschiedener Fraunhofer-Institute.

Die Strafverfolgung bei Cyberangriffen gegen Wirtschaftssubjekte wird nicht vom BSI wahrgenommen, sondern von den **Zentralen Ansprechstellen Cybercrime** (ZAC), die jeweils nach Bundesländern gegliedert sind und dort den Ermittlungsbehörden der Staatsanwaltschaft und der Polizei unterstellt sind.

Darüber hinaus gibt es vom Bundesministerium für Wirtschaft und Energie (BMWi) finanzierte Förderprogramme, die Cybersicherheitsberatung im Mittelstand fördern.[133] Erwähnenswert sind auch die Standardisierungsbemühungen der unabhängigen Plattform für Normung und Standardisierung, das Deutsche Institut für Normung (DIN), im Bereich der Cybersicherheit. Hier werden insbesondere mit Blick auf die *Enabler*-Funktion gemeinsame Standards mit anderen Regelsetzern (nationale, europäische und internationale, branchenübergreifende und branchenspezifische Verbände, Vereine, Behörden) entwickelt, um die Cybersicherheits-Architektur besser aufeinander abzustimmen und Konzepte wie *Security by Design*, *Usability* und sog. ubiquitäre Vernetzung in einen allgemeinen Wissenstransfer einzubinden.[134]

[133] Vgl. BMWi 2019b.
[134] Vgl. DIN/DKE Roadmap 2017.

Kooperation auf Bundes- und Landesebenen

Auf Grundlage der Cybersicherheitsstrategie von 2011, wurde als ressortgemeinsame Informations- und Kooperationsplattform das **Cyberabwehrzentrum** (Cyber-AZ) innerhalb des BSI gegründet.[135] Das Cyber-AZ koordiniert Schutz- und Abwehrmaßnahmen basierend auf der operativen Zusammenarbeit der beteiligten Behörden. Dazu werden verfügbare Informationen zu Cyberangriffen zwischen den Behörden ausgetauscht, bewertet und für entsprechenden Gegenmaßnahmen genutzt. Die durch permanente oder anlassbezogene Verbindungspersonen vertretenen Behörden im Cyber-AZ, verwerten die Informationen aus ihrem jeweiligen Zuständigkeitsbereich heraus.[136]

Als erstes Bundesland hat Bayern eine eigene IT-Sicherheitsbehörde aufgebaut. Das **Landesamt für Sicherheit in der Informationstechnik** (LSI) ist dem Staatsministerium der Finanzen und für Heimat unmittelbar nachgeordnet und zählt zu seinen Kernaufgaben die Gefahrenabwehr des staatlichen Behördennetzes (BayernServer und BayernNetz) sowie auf Ersuchen, die Bereitstellung von Beratungs- und Unterstützungsleistungen für Kommunen, Unternehmen, Bürger sowie Betreiber Kritischer Infrastrukturen.[137]

Während sich das anfänglich aufgrund der unzureichenden Kapazitäten, der eingeschränkten Handlungskompetenzen, der konträren Vorstellungen im Umgang mit Cybervorfällen, und nicht zuletzt der unausgewogenen Informationsteilung, in der Kritik stehende Cyber-AZ auf den Informationsaustausch konzentriert und versucht, diese in gezielte Maßnahmen umzusetzen, liegt der Schwerpunkt der sogenannten ***Computer Emergency Response Teams*** (CERT) der Länder darauf, bei sicherheitsrelevanten IT-Vorfällen schnell zu reagieren und den betroffenen Einrichtungen mit technischer Expertise zur Seite zu stehen.[138]

Vor diesem Hintergrund ist die Bund-Länder Zusammenarbeit essentiell für eine schnelle und adäquate Zusammenarbeit. Zum einen gilt es die Netzwerke der fortschreitenden digitalisierten Verwaltung der Länder und die IT-Strukturen des Bundes, technisch zu sichern, und zum anderen dafür Sorge zu tragen, dass der Informationsaustausch über Bedrohungen und die Zusammenarbeit sowohl zwischen Bund und Länder, als auch zwischen Behörden und Unternehmen besser funktioniert. Damit soll sichergestellt werden, dass Maßnahmen einheitlich und

[135] Vgl. https://www.bmvg.de/de/themen/cybersicherheit/partnerschaften-zur-cybersicherheit/nationales-cyber-abwehrzentrum.

[136] Vgl. Herpig und Bredenbrock 2019, S. 6.

[137] Vgl. Bayrisches E-Government-Gesetz 2015, Artikel 10.

[138] Ebd. Fußnote 108, S. 8.

zielgerichtet erfolgen, um identifizierte Schwachstellen in allen betroffenen Bereichen synchron zu adressieren.

Der CERT-Verbund ist eine Allianz deutscher Sicherheits- und Computernotfallteams bestehend aus akademischen, kommerziellen, sowie Unternehmens- und Verwaltungs-CERT Teams.[139] Ziel ist es, Informationen auszutauschen, um die nationalen IT-Netze zu schützen und auf Bedrohungsszenarios schnell und simultan reagieren zu können. Die einzelnen Bundesländer haben entweder eigene Länder-CERT der Verwaltung etabliert oder sich zusammengeschlossen, um ein gemeinsames CERT Team zu betreiben, wie es z.B. beim CERT Nord der Verwaltungen von Bremen, Hamburg, Schleswig-Holstein und Sachsen-Anhalt der Fall ist.[140]

Zu unterscheiden ist der vom BSI betriebene CERT-Bund, der ausschließlich an Bundesbehörden berichtet und für präventive wie auch reaktive Maßnahmen bei IT-Sicherheitsvorfällen zuständig ist. Die Kooperation im CERT-Verbund, dem auch der CERT-Bund angehört, ist laut BSI eng und wird dazu genutzt, in regelmäßigen Abständen Informationen und Erfahrungen in einer integren und vertrauensvollen Atmosphäre auszutauschen.[141] Dabei hat sich ein noch engerer Kreis gebildet der zusätzlich einen *Code of Conduct* unterzeichnet und sich damit zu einer Vertraulichkeitsvereinbarung verpflichtet hat.[142] Auf europäischer Ebene besteht ein informeller Zusammenschluss zur Kooperation und simultanen Reaktion bei IT-Sicherheitsvorfällen in der sogenannten *European Governmental CERTs Group* (EGC).[143]

Neben der Bund-Länder CERT Zusammenarbeit, steht auch ein Austausch im Bereich der Informationssicherheit und der Unterstützung und Beratung durch das BSI bei der Gefahrenabwehr und bei der Umsetzung des Informationssicherheitsmanagements (ISMS). Dazu ist ein umfangreiches IT-Sicherheits-Lagebild notwendig, welches vom nationalen IT-Lage- und Analysezentrum im BSI erstellt wird. Das nationale IT-Lagezentrum ist rund um die Uhr besetzt und dient sowohl den Bundesbehörden, Kritische Infrastrukturen, als auch Partnern als Anlaufstelle, um IT-Sicherheitsvorfälle schnell und kompetent einzuordnen und auf mögliche Bedrohungen hinzuweisen.[144] Dabei steht das Lagezentrum im ständigen Kontakt zu nationalen und

---

[139] Vgl. https://www.cert-verbund.de/.

[140] Vgl. http://certnord.de/.

[141] Vgl. https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/Aktivitaeten/CERT-Bund/Zusammenarbeit/zusammenarbeit_node.html.

[142] Ebd.

[143] Ebd.

[144] Vgl. https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/Aktivitaeten/IT-Lagezentrum/itlagezentrum.html.

internationalen Partnern und kann bei schwerwiegenden Vorfällen, zur technischen Analyse und Koordinierung der Gegenmaßnahmen, zum IT-Krisenreaktionszentrum erweitert werden.

Kooperation auf EU-Ebene

Der am 27. Juni 2019 in Kraft getretene europäische Rechtsakt zur Cybersicherheit (*Cybersecurity Act*), hat der europäischen Cybersicherheits-Agentur ENISA (*European Network and Information Security Agency*) ein dauerhaftes Mandat verliehen und die Agentur mit deutlich mehr personellen wie auch finanziellen Mitteln ausgestattet.[145] Darüber hinaus soll die europäische Cybersicherheitsagentur ein einheitliches EU-weites Zertifizierungsverfahren für Informations- und Kommunikationstechnikprodukte, -dienstleistungen und -prozesse einführen. Bestehende nationale Zertifizierungsrahmen werden dabei berücksichtigt und im Hochsicherheitsbereich behalten die Mitgliedsstaaten ihre Rolle im Zertifizierungsprozess.[146] Dies ist ein Schritt zur Harmonisierung von Cybersicherheitsstandards innerhalb der EU, um die Bewertungskriterien der Vertrauenswürdigkeit von Produkten und Dienstleistungen von Herstellern und deren technische Überprüfung zu vereinheitlichen.

In Kooperation mit den nationalen Behörden werden u.a. Sicherheitsrichtlinien auf der Grundlage von Rechtsvorschriften, wie z.B. der Richtlinie zur Gewährleistung einer hohen Netzwerk- und Informationssicherheit (NIS-Richtlinie) umgesetzt, die Zusammenarbeit im Meldewesen von Cybervorfällen intensiviert und Rahmenwerke für Audits erstellt.[147] Die NIS-Richtlinie besteht aus drei Teilen: Dem Aufbau eines nationalen CERT-Teams in jedem Mitgliedsstaat, dem Ausbau der Kooperation in Fragen der Cybersicherheit über Ländergrenzen hinweg, und der Aufsicht Kritischer Infrastrukturen und digitaler Service Provider.[148] Die vollständige Umsetzung der NIS-Richtlinie in nationale Rechtvorschriften ist noch nicht in allen EU-Staaten geschehen. Bulgarien, Ungarn und Belgien befinden sich noch in der Umsetzungsphase und haben bereits einen erheblichen Verzug.[149]

Eine weitere Form der Kooperation findet in Form von Übungen beteiligter EU-Mitgliedsstaaten statt, in denen IT-Sicherheitsvorfälle simuliert werden, um Abläufe zu testen, zuverlässige

---

[145] Vgl. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2019.151.01.0015.01.ENG&toc=OJ:L:2019:151:TOC

[146] Vgl. https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2019/Cybersecurity_Act_270619.html

[147] Vgl. https://eur-lex.europa.eu/eli/dir/2016/1148/oj.

[148] Vgl. https://www.enisa.europa.eu/topics/nis-directive.

[149] Vgl. Grad der Umsetzung (Stand Oktober 2019) https://ec.europa.eu/digital-single-market/en/state-play-transposition-nis-directive.

Kommunikationskanäle zu etablieren und ein länder- sowie bereichsübergreifendes Krisenmanagement zu entwickeln.[150]

Privatwirtschaftliche Initiativen und staatliche Schnittstellen

Neben den staatlichen Akteuren haben sich in den letzten Jahren auch private Initiativen zum Schutz vor Cyberangriffen in der deutschen Wirtschaft gegründet. Dazu gehören z.B. die *Charter of Trust* und die Deutsche Cybersicherheitsorganisation (DCSO)[151]. Darüber hinaus haben sich staatlich-privatwirtschaftliche Kooperationen herausgebildet, die zum einen den aktiven Informationsaustausch zur Bedrohungslage forcieren und zum anderen die Resilienz der deutschen Wirtschaft als Kernelement und als eine gesamtgesellschaftliche Aufgabe betrachten. Dazu gehören u.a. das Bündnis für Cybersicherheit zwischen dem Innenministerium und dem Bundesverband der deutschen Industrie (BDI)[152], die Sicherheitskooperation Cybercrime zwischen Bitkom und einigen Landeskriminalämtern[153], die Koordinierungsstelle IT-Sicherheit (KITS) beim DIN als Fachbeirat für den Informationsaustausch zwischen Behördenvertretern, Unternehmen, Verbänden und den verschiedenen Bereichen und Domänen die sich mit der Normung von IT-Sicherheitskomponenten beschäftigen[154], sowie die Arbeitsgruppe „Sicherheit vernetzter Systeme“ der Plattform Industrie 4.0, die Lösungsansätze für ein erhöhtes Sicherheitsniveau der vernetzten Industrie entwickelt[155].

[150] Vgl. https://www.bsi.bund.de/DE/Themen/KRITIS/Aktivitaeten/IT-Krisenreaktionszentrum/Uebungen/Beispiele/beispiele_node.html.

[151] Vgl. https://dcso.de/de/about-us/.

[152] Vgl. https://www.bmi.bund.de/SharedDocs/pressemitteilungen/DE/2018/09/mou-mit-bdi.html.

[153] Vgl. https://sicherheitskooperation-cybercrime.de/.

[154] Vgl. https://www.din.de/de/din-und-seine-partner/din-e-v/organisation/koordinierungsstellen/kits.

[155] Vgl. https://www.plattform-i40.de/PI40/Navigation/DE/Plattform/Arbeitsgruppen/AG03/sicherheit-vernetzter-systeme.html.

	Gründung	Hauptsitz	Struktur	Aufgaben	Budget
BSI – Bundesamt für Sicherheit in der Informationstechnik	1991	Bonn	Gehört zum Geschäftsbereich des Bundesministeriums des Inneren. In 8 Abteilungen organisiert; jede Abteilung setzt sich aus ein bis drei Fachbereichen zusammen; Fachbereiche in verschiedene Referate unterteilt. Unabhängige und neutrale Stelle mit hoher technischer Expertise	Stärkung der IT-Sicherheit; zuständig für den Schutz der IT-Systeme des Bundes	€117,9 Millionen (2018)
ADIC – Agentur für Innovationen in der Cybersicherheit (Cyberagentur)	2019	Region Halle-Leipzig	Federführung BMI und BMVg, Dual-Use Technologie	Technologische Innovationsführerschaft Deutschlands fördern; Forschungs- und Innovationsvorhaben im Bereich der Cybersicherheit identifizieren, anstoßen, fördern und finanzieren; disruptive Technologien	€365 Millionen (geplant 2019-2022)
ZITiS – Zentrale Stelle für Informationstechnik im Sicherheitsbereich	2017	München	Gründung durch BMI; 6 Bereiche, 22 Referate, Leitung (Präsident, Leitungsstab, Vizepräsident/CTO)	Forschungs- und Entwicklungsdienstleister der Sicherheitsbehörden für technische Lösungen im Cyberbereich (Digitale Forensik, Telekommunikationsüberwachung, Krypto- und Big-Data-Analyse wie auch technische Fragen der Kriminalitätsbekämpfung, Gefahren- und Spionageabwehr). Keine Eingriffsbefugnisse und keine Beschaffungsorganisation (laut eigener Definition)	€36,7 Million (im Bundeshaushalt für 2019)
KdoCIR – Kommando Cyber- und Informationsraum	2017	Bonn	BMVg, Führungskommando des CIR	Erstellung eines konsolidierten Cyber-Lagebildes, strategische Aufklärung, operative Kommunikation. Das KdoCIR dient zudem in Fragen der Cybersicherheit als Schnittstelle für andere Ressorts des Bundes, für die Wirtschaft und für internationale Verbündete	-
CODE – Forschungsinstitut Cyber Defence	2013	München	Gründung durch BMVg; an der UniBw angesiedelte; Cybercluster Forschungsfelder: Cyber Defence, Smart Data, Mobile Security, e-Health, Kritische Infrastrukturen	Entwicklung von innovativen technischen Neuerungen und Konzepten zum Schutz von Daten, Software und Systemen unter Beachtung gesetzlicher und betriebswirtschaftlicher Rahmenbedingungen, ganzheitlich, integrativ und interdisziplinär; „Forschungsinstitut für Cyber Defence und Smart Data der Bundeswehr und des Bundes“; Interaktion zwischen Industrie, Forschung und Behörden weiter stärken	-

Kompetenz- und Forschungszentren für IT-Sicherheit	2011	Dezentral; CISPA in Saarbrücken; CRISP in Darmstadt; KASTEL in Karlsruhe	Zentrale Bausteine der Digitalen Agenda des BMBF; interdisziplinär	Forschung und Entwicklung in IT-Sicherheitsforschung und Datenschutz	-

Tabelle 3 Relevante Behörden und Institute der Cybersicherheitsarchitektur
Quelle: Eigene Darstellung.

2.8 Risikomanagement und Cyberversicherung

Selbst beim Einsatz bester IT-Sicherheitstechnik und Experten sowie regelmäßiger Sicherheitsschulungen der Anwender ist es unmöglich, die Bedrohung durch Cyberangriffe auf null zu reduzieren. Wie bereits aufgezeigt wurde, ist es auch ökonomisch nicht sinnvoll, übermäßig Ressourcen in Schutzleistungen zu investieren. Daher verbleibt in jedem Fall ein Restrisiko, dass ein Cyberangriff erfolgreich sein kann und es zu entsprechenden Schäden kommt. Unternehmen und ihre Führung sind dann gefragt, zu entscheiden, ob sie finanziell und rechtlich in der Lage und willens sind, dieses Risiko selbst zu tragen oder im Rahmen eines Risikomanagements an Dritte gegen einen Preis weiter zu reichen.

Vereine auf Gegenseitigkeit und Versicherungen sind seit Jahrhunderten die institutionelle Lösung, um aus einem unkalkulierbaren Schicksalsschlag ein berechenbares Risiko zu machen. Ende des 16. Jahrhunderts entstandenen in Deutschland erste Brandkassen als kollektive Absicherungsmechanismen.[156] Durch das Gesetz der großen Zahlen, also das *pooling* von Risiken, nähert sich die relative Häufigkeit der theoretischen Wahrscheinlichkeit eines Ereignisses an und wird somit für die Versicherung, anders als für den Einzelnen, berechenbar.

Ähnlich wie beim Feuerrisiko Ende des 16. Jahrhunderts ist das Cyberrisiko für das einzelne Unternehmen (insbesondere KMU) kaum berechenbar und gleicht bei seiner Realisierung einem Schicksalsschlag. Viele Unternehmer und Führungskräfte kapitulieren daher vor dem Cyberrisiko und geben sich der Apathie hin. Gerade in solchen Fällen kann eine Cyberversicherung eine betriebswirtschaftliche Lösung sein. Das finanzielle Risiko eines Schadens durch einen erfolgreichen Cyberangriff wird dabei gegen einen Preis (Versicherungsprämie) verkauft und geht damit an die Versicherung über. Für das einzelne Unternehmen wird somit das Cyberrisiko berechenbar und beherrschbar. Aus den höchst unsicheren Schadenskosten werden sichere und kalkulierbare Prämienzahlungen.

[156] Vgl. Koch 2012, S. 29.

Gleichzeitig profitieren die Versicherungen über die Zeit von dem Wissen, das sie durch die einzelnen Schadensfälle und deren Analyse erlangen. Angriffsmethoden sowie Schwächen beim Cyberschutz können durch sie ausgewertet werden und zum einem für eine bessere Kalkulation des Risikos und damit der Versicherungsprämie herangezogen werden. Zum anderen können aber auch die Versicherungsbedingungen über die Zeit angepasst und somit die Kunden zu einem besseren Cyberschutz angereizt werden. Über die Versicherungsbedingungen und deren Veränderung über die Zeit wirkt der Cyberversicherer zumindest für seine Kunden wie ein Quasi-Regulierer.[157] Nur bei Einhaltung der Versicherungsbedingungen gilt auch der Versicherungsschutz für den Versicherungsnehmer.

Nicht nur durch den Schaden ihrer Kunden werden die Versicherer klug. Cyberversicherungspolicen beinhalten regelmäßig nicht nur die Kompensation des monetären Schadens eines Cyberangriffs. Daneben werden auch sog. Assist-Leistungen angeboten, die im Wesentlichen darauf abzielen, den Schadensumfang zu begrenzen: Den Datenabfluss zu stoppen, Daten oder die Funktionsfähigkeit der IT-Systeme wiederherzustellen, oder Kommunikationsdienstleistungen mit Kunden und dem Kapitalmarkt zu erbringen. Hierzu bedienen sich die Versicherer in der Regel eines externen IT-Sicherheitsdienstleistungsunternehmens, das im Schadensfall dieses in der Schadensbegrenzung und -behebung unterstützt. Die hierfür anfallenden Kosten sind durch die Cyberpolice gedeckt. Auch und gerade über diese Assist-Dienstleistungen lernen die Versicherer etwas über Schwachstellen in IT-Sicherheitssystemen und sich wandelnde Angriffsmethoden. Hierüber könnten sie andere, bislang nicht betroffene Kunden im wohlverstandenen Eigeninteresse informieren. Eine weite Verbreitung von Cyberversicherungen kann so helfen, Informationsasymmetrien abzubauen.[158]

Die Besonderheit der Cyberversicherung ist: Versicherer gehen aus Eigeninteresse mit ihren Assistenzleistungen über den reinen Risikotransfer hinaus. Die Einhaltung von Sicherheitsstandards wie ISO 27001, regelmäßige Audits und Awareness-Schulungen wirken auf eine Risikoreduzierung *ex ante* hin. Krisenmanagement, Notfallkundenservice und Öffentlichkeitsarbeit helfen, Schäden *ex post* zu begrenzen. Eine flächendeckende Cyberversicherungspflicht könnte durch diesen Mechanismus dabei helfen, das aggregierte Cyberschutzniveau in Deutschland anzuheben.[159]

---

[157] Vgl. Camillo 2017.
[158] Vgl. BIGS 2017, S. 61.
[159] Interview 1, Verband.

Blickt man auf den deutschen Markt für Cyberversicherungen, so kann man feststellen, dass das oben beschriebene Idealbild eines Risikomanagements über Versicherungen bislang noch nicht der Realität entspricht. Der Cyberversicherungsmarkt in Deutschland ist noch weitestgehend unterentwickelt.[160] Dies liegt zu aller erst daran, dass das Risiko, das sich der Versicherer über den Abschluss einer Police in die Bilanz holt, bislang noch nicht hinreichend kalkulierbar ist. Dies wiederum liegt an unzureichenden Informationen über die Bedrohungssituation einerseits, als auch an den Schwierigkeiten, die Wirksamkeit der IT-Schutzleistungen eines Unternehmens einschätzen zu können, andererseits.[161] Um trotzdem das Risiko für den Versicherer kalkulierbar zu machen, werden in den Policen regelmäßig die Schadenshöhen nach oben begrenzt. Das Tempo und die Komplexität der Risiko-Gemengelage in der technologischen Entwicklung ist eine permanente Herausforderung für die nacheilenden Aktuare.[162] Eine weitere Wachstumsbremse ist auch hier der Mangel an hinreichend qualifiziertem Personal als *Underwriter* auf Seiten der Versicherer.[163]

Gänzlich ausgeschlossen in den Versicherungsbedingungen ist, wie bei anderen Vermögensversicherungen auch, das Kriegs- und Terrorrisiko. Dies ist theoretisch zwar völlig einleuchtend, setzt aber voraus, dass in einer wohl geordneten „westfälischen Welt“, ein Kriegs- oder Terrorakt im Cyberraum auch als solcher erkannt und gerichtsfest anerkannt wird. Ein prominentes Beispiel hierfür ist die Weigerung der Versicherungen von Mondelez und Merck, Schäden im hohen dreistelligen Millionenbereich durch die NotPetya-Attacke zu kompensieren, weil hinter dem Angriff die russische Regierung vermutet wird. Merck und Mondelez waren demnach nur Kollateralschäden in einem staatlich initiierten Cyberkrieg.[164] Da aber die Attribution von Angriffen regelmäßig große Schwierigkeiten bereitet, herrscht hier sowohl für Versicherungsanbieter als auch für die Nachfrager von Cyberpolicen hohe Unsicherheit. Unsicherheit wiederum hemmt die Marktentwicklung für Cyberversicherungen.

In den USA besteht daher eine Regelung, dass das US-Finanzministerium in Absprache mit dem Außen- und dem Justizministerium den Kriegsfall im Cyberraum feststellt und damit die Versicherer aus der Haftung entlässt; und der Staat als eine Art Rückversicherer für Schäden

[160] Vgl. BIGS 2017, S. 59.
[161] Vgl. Biener et al. 2015.
[162] Vgl. GDV 2019b.
[163] Vgl. BIGS 2017, S. 31.
[164] Vgl. Marvan 2017; BSI 2019, S. 17.

oberhalb von 100 Mio. US-Dollar einspringt.[165] In Ergänzung zu dieser staatlichen Rückversicherung hat „(…) das Department of Homeland Security (DHS) die Möglichkeit, bestimmte Technologien als „Qualified Anti-Terrorism Technology“ zu zertifizieren. Dadurch wird die Haftung für eventuelle Schäden vom Nutzer der Technologie auf den Hersteller übertragen. Dieser kann wiederum sein Haftungsrisiko durch die „Government Contractor Defense”-Klausel reduzieren, die eine Haftung nur vorsieht, wenn die von der Regierung spezifizierten Anforderungen nicht eingehalten wurden.”[166] Eine vergleichbare Regelung fehlt in Deutschland.

Äußerst hilfreich für den deutschen Markt für Cyberversicherungen war die Einigung im April 2017 auf Allgemeine Versicherungsbedingungen für die Cyberrisikoversicherung, durch den GDV.[167] Hier wurden Definitionen vorgenommen und Standards für Versicherungspolicen geschaffen, die das bestehende Angebot vergleichbar machen und die Informationskosten für potentielle Versicherungsnehmer reduzieren. Diese Versicherungsbedingungen gilt es regelmäßig fortzuschreiben, an den Stand der technischen Entwicklung anzupassen und insbesondere auf die bislang noch unzureichend abgedeckten Bereiche der industriellen Cybersicherheit auszudehnen.[168]

Man könnte nun meinen, dass eine Cyberversicherungspflicht eine Lösung für Unternehmen sein könnte, sich des Cybersicherheitsproblems bei der Digitalisierung zu entledigen. Hier gilt es aber zu berücksichtigen, dass die Schadenskosten durch eine Versicherung nur verteilt werden. Werden die Schäden nicht zumindest teilweise verhindert, so spiegelt sich dies in den Prämien wieder. Somit ist die Cyberversicherung nur ein (wenngleich wichtiger) Baustein im betrieblichen Schutz vor Cyberangriffen.

---

[165] Vgl. BIGS 2017, S. 49; Terrorism Risk Insurance Act https://www.treasury.gov/resource-center/fin-mkts/Pages/program.aspx.

[166] Vgl. BIGS 2017, S. 49; Support Anti-Terrorism by Fostering Effective Technologies (SAFETY) Act https://www.safetyact.gov/.

[167] Vgl. GDV 2017.

[168] Vgl. BIGS 2017, S. 29.

3 Allokatives Marktversagen auf privaten Märkten für IT-SP/PSK

Allokatives Marktversagen auf Märkten für IT-SP/PSK führt zu Effizienzverlusten und schmälert die Möglichkeiten eines langfristig tragfähigen, mithin eines sicherheits-nachhaltigen Wachstums. Das betrifft sowohl die Angebots- als auch die Nachfrageseite dieses Marktes, und im Ergebnis auch die gesellschaftliche Versorgung mit Schutzleistungen. Gemeinsam mit dem Problem des Fachkräftemangels[169] dürften gerade diese Effizienzverluste dazu beitragen, dass ein volkswirtschaftlich effizientes Niveau (in Menge und Qualität) an IT-SP/PSK verfehlt wird. Dabei werden zwei grundsätzliche Arten des Marktversagens betrachtet.

In Abschnitt 3.1 wird mit den umfassenden Informationsdefiziten das wohl überragende Problem der Cyberbedrohung diskutiert. Informationsdefizite erschweren, dass optimale Entscheidungen getroffen werden können. In der Folge ergibt sich auch ein gesellschaftlich suboptimales Marktergebnis.

In Abschnitt 3.2 werden daraufhin externe Effekte beim Konsum von IT-SP/PSK diskutiert. Bei ihnen kommt es trotz individuell rationaler Entscheidungen zu gesellschaftlich suboptimalen Ergebnissen. Grund dafür sind technische Wechselwirkungen.

In beiden Abschnitten wird das Entscheidungskalkül der Nachfrageseite von IT-SP/PSK besonders thematisiert (*Enabler*-Perspektive). Dennoch ergibt sich daraus auch ein Effekt auf die Angebotsseite (*Driver*-Perspektive). Folglich führt eine Überwindung von Marktversagen zu Wachstumschancen auf beiden Marktseiten.

3.1 Informationsdefizite

In der Literatur zur Ökonomie der Cybersicherheit (*Economics of Cybersecurity*) werden unter den relevanten Arten von Marktversagen besonders Informationsdefizite in den Mittelpunkt gerückt.[170] [171] Laut Moore gilt hierbei: *"Unreliable information takes many forms"*.[172] Dabei wird hier vorgeschlagen, Informationsdefizite in zwei Typen einzuteilen, denen sich jeweils ein

[169] Vgl. Kapitel 5.

[170] Vgl. Anderson 2001; Anderson und Moore 2006 und 2007; Moore 2010a und 2010b.

[171] Man findet dies öfter unter dem Begriff der „Informationsasymmetrie". Allerdings ist dies ein engerer Begriff, da er davon ausgeht, dass es jemanden gibt, der über die Information verfügt, während jemand anderes (i.d.R. die andere Marktseite) nicht über diese Information verfügt. Dieses Phänomen soll hier als Teilmenge des Begriffs „Informationsdefizit" betrachtet werden. Hinzukommen aber auch Defizite über Informationen, bei denen u.U. *niemand* über die aggregierte Information verfügt, da nur einzelne Bestandteile in der Volkswirtschaft dezentral verteilt sind (vgl. von Hayek 1945). In diesem Sinne schreibt auch Walker (2012, S. 10): „There is an asymmetry of information problem […] or more correctly an *absence of information* problem." (Herv. d. Verf.)

[172] Moore 2010a, S. 8.

Markt zuordnen lässt: Der Markt für Bedrohungsinformationen und den Markt für IT-SP/PSK (vgl. Abschnitt 2.4, weiter oben). So geht es also um

- Informationen über **Bedrohung** und damit des zu erwartenden Schadens ohne Abwehr; und um
- Information über **Qualität bzw. Effektivität von IT-Schutzmaßnahmen**.

Vor diesem Hintergrund wird im nun folgenden Abschnitt 3.1.1 einführend, die Entscheidungssituation von Schutzguteigentümern bei einer möglichen Investition in Bedrohungsinformationen sowie in IT-SP/PSK als ökonomische (kostenträchtige) Güter vorgestellt. Daraufhin wird das doppelte Informationsproblem betrachtet: Im Abschnitt 3.1.2 wird das Problem der Bedrohungsinformation und im Abschnitt 3.1.3 das Problem der Qualitätsinformation beleuchtet.

3.1.1 Zur Entscheidungssituation über Cybersicherheits-Investition von Schutzguteigentümern

Das soeben vorgestellte *doppelte* Informationsproblem wird deutlich, wenn man sich die Entscheidungssituation des Schutzguteigentümers mit Blick auf mögliche IT-SP/PSK vor Augen führt.[173]

[173] Vgl. Abbildung 11.

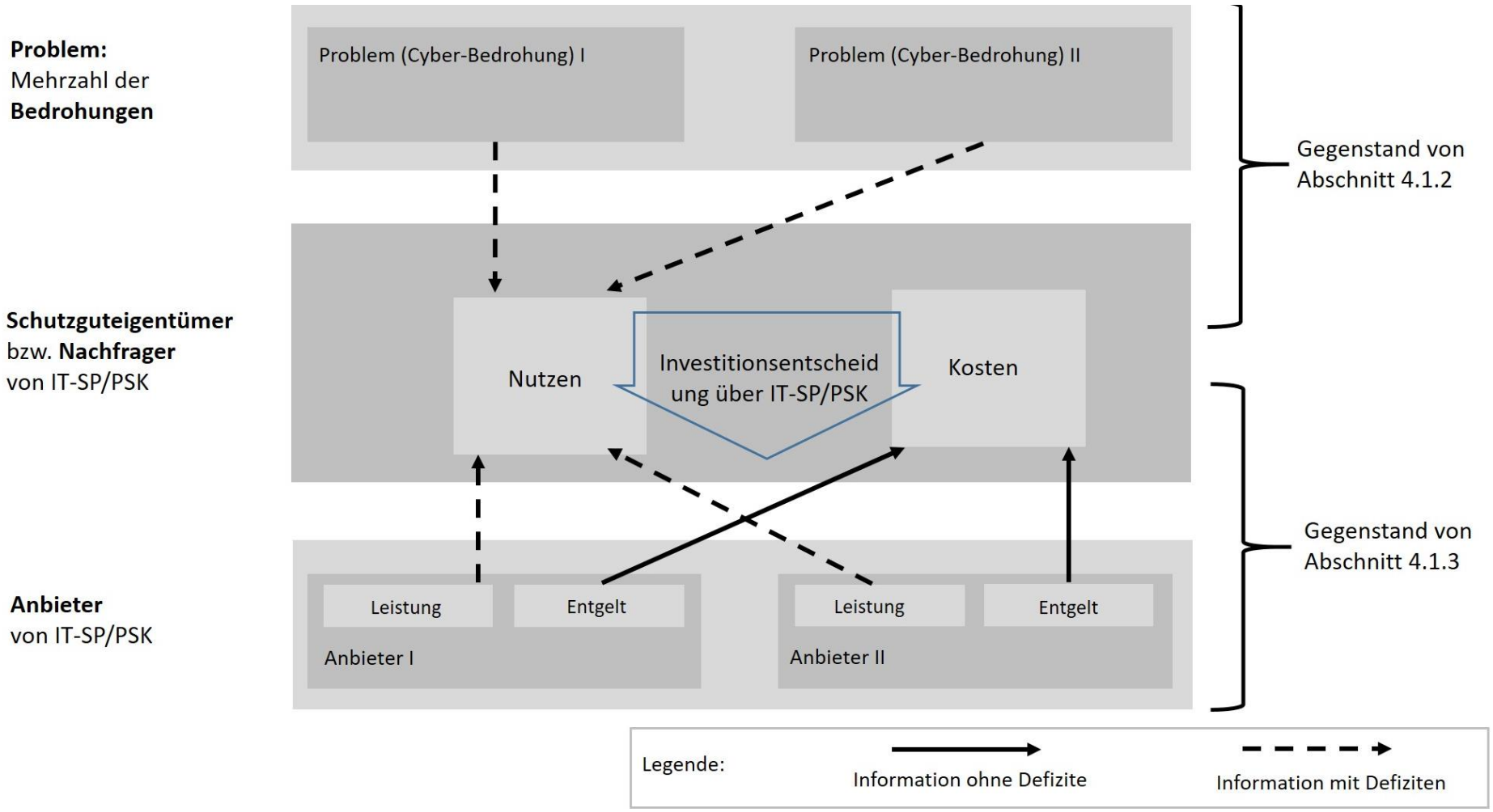


Abbildung 11 Schutzguteigentümer zwischen Cyberproblemen und Anbietern von Sicherheitsmaßnahmen / Versicherungen
Quelle: Eigene Darstellung.

In der mittleren Ebene der Abbildung ist die Situation einer Investitionsentscheidung eines Schutzguteigentümers hinsichtlich IT-SP/PSK als Kosten-Nutzen-Kalkül dargestellt. Die untere Ebene stellt die unterschiedlichen (hier: zwei) Angebote an IT-SP/PSK dar, zwischen denen er im Rahmen der Investitionsentscheidung zu wählen hat.[174] Dabei ist jede Option durch eine bestimmte Leistung und durch ein bestimmtes Entgelt (Preis) charakterisiert, die sich für den Nachfrager als Kosten der IT-SP/PSK niederschlagen. Und hinsichtlich der Informiertheit des Entscheiders lässt sich pointiert sagen: Diese Kosten sind für sein Entscheidungskalkül die einzige Information, über die er (bestenfalls) Klarheit hat. Dies ist also eine sichere Information in seinem Kosten-Nutzen-Kalkül (durchgezogene Pfeile). Über die Leistung und Qualität des IT-SP/PSK aber, z.B. einer Schutzsoftware, besteht in vielen Fällen mindestens teilweise Unklarheit. Es liegt eine Situation mit Informationsdefiziten vor (durchbrochene Pfeile). Die Leistung bestimmt aber den Nutzen des Schutzguteigentümers, einzig anhand dessen sich die Inkaufnahme von Kosten begründen und messen lässt.

Gerade aber mit Blick auf die Bewertung des Nutzens von IT-SP/PSK kommt nun das Problem der Bedrohungsdiagnose hinzu (in der oberen Ebene in Abbildung 11). Selbst wenn der Entscheider volle Information über die Qualität der Schutzleistung hat, so kann er doch den Nutzen, den er daraus zieht, nur dann identifizieren, wenn er seine individuelle Bedrohungslage in hinreichendem Umfang kennt.[175] Dabei sind in Abbildung 11 zwei unterschiedliche Bedrohungen abgebildet. Auch in der Einschätzung der Bedrohung sind Informationsdefizite (gestrichelte Pfeile) anzunehmen. Dies vervielfacht ggf. das Problem der richtigen Kosten-Nutzen-Einschätzung, und damit eines angemessenen Risikomanagements. Dieses doppelte Informationsdefizit lässt sich vereinfacht und (für den Extremfall) zugespitzt so ausdrücken:

Der Schutzguteigentümer weiß nicht nur nicht, inwieweit eine Schutzleistung (IT-SP/PSK) sein Sicherheitsproblem effektiv zu adressieren vermag, sondern auch nicht, welches Sicherheitsproblem er überhaupt hat.

Damit dürfte die allgemein beobachtete Verunsicherung bei Unternehmen im Umgang mit der Cyberbedrohung gut beschrieben sein. Im Übrigen dürften diese Defizite nicht nur auf Seiten der privaten

[174] Eine weitere Wahlmöglichkeit besteht natürlich immer darin, in gar keine Schutzleistung zu investieren. Dementsprechend ist eine solche Entscheidung stets dreidimensional: Der Schutzguteigentümer hat zu entscheiden, (1) ob er eine Schutzleistung nachfragen soll, (2) welcher Art die Schutzleistung sein soll und (3) in welchem Umfang er diese Schutzleistung beziehen will.

[175] Diese Einschränkung bezieht sich auf ein Problem, das in der Lehrbuchliteratur – allgemeiner – unter dem Begriff der Nutzenunkenntnis behandelt wird (vgl. Fritsch 2018, S. 270 ff.).

Unternehmen bzw. privater Nachfrager vorliegen. Auch der Staat besitzt über die Qualität und Wirksamkeit von Schutzleistungen in vielen Fällen lediglich unvollständige Informationen. Die Debatte über den Ausschluss chinesischer Anbieter beim Aufbau von 5G-Netzen liefert hierfür einen Hinweis.

Betrachtet man Information als ökonomisches Gut, so wird deutlich, dass es nicht darum geht, ob eine Information „da ist“ oder „nicht da ist“. Sinnvoller Weise sollte Information nicht derartig binär, sondern graduell verstanden werden: Dass sie sich unter Einsatz von Kosten generieren bzw. akquirieren lässt und der (optimale) Umfang der Informiertheit zumindest theoretisch anhand eines Kosten-Nutzen-Kalküls bestimmt werden kann.

In diesem Sinne macht nachfolgende Abbildung 12 deutlich, dass Informationen nicht üppig und kostenlos verfügbar, sondern knapp und damit kostspielig sind.[176]

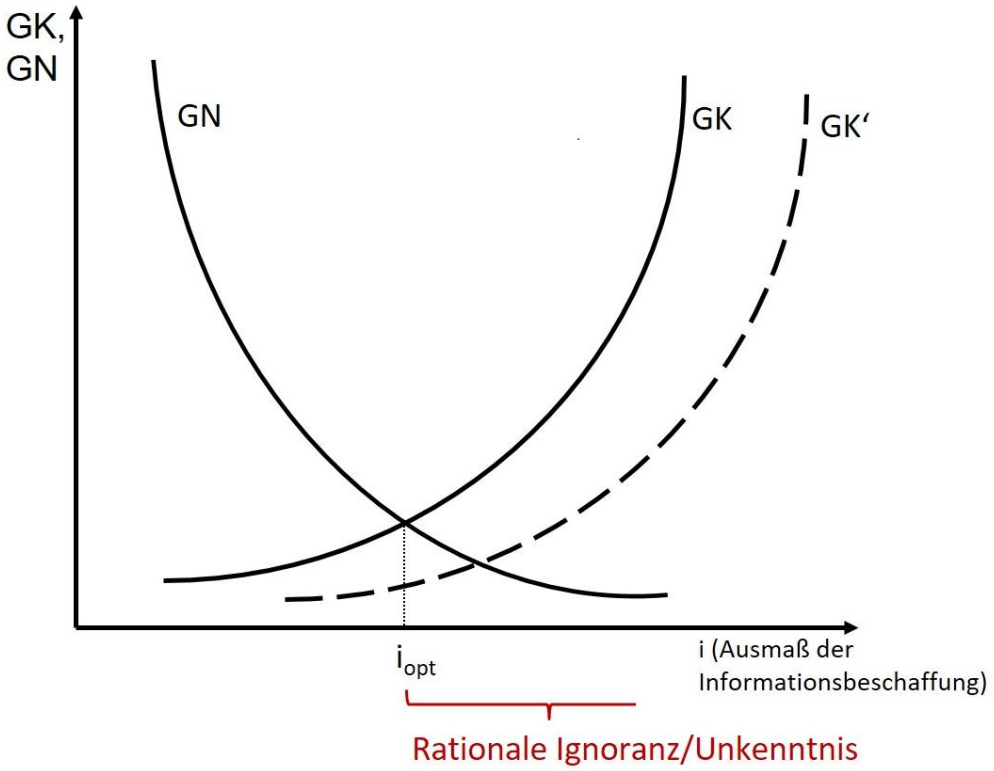


Abbildung 12 Optimale Informiertheit bzw. Unwissenheit als Funktion aus GK und GN der Informationsbeschaffung
Quelle: Eigene Darstellung in Anlehnung an Donges und Freytag 2009, o.S.).

Auf der Abszisse ist das Ausmaß der Informationsbeschaffung *i* dargestellt. Je weiter man sich darauf nach rechts bewegt, umso größer ist der Umfang der beschafften Information. Auf der Ordinate sind GN

[176] Diese fundamentale informationsökonomische Feststellung wird für den Bereich der *Cybersecurity* durch folgende Einschätzung von Moore (2010a) – unbenommen einer notwendigen Unterscheidung zwischen Mangel und Knappheit – gestützt: “*Many industries report a deluge of data. Some even complain of being overwhelmed. However, in the security space there is a dearth of relevant data needed to drive security investment.* “ (Moore 2010a, S. 7).

und GK der Informationsbeschaffung abgetragen. Dahinter steckt die Überlegung, dass sich für ein Wirtschaftssubjekt als Entscheider mit steigender Informationsbeschaffung zwei gegenläufige Effekte ergeben. Zum einen steigt der Nutzen der Information, da so die darauffolgende Entscheidung auf einer besseren Informationsgrundlage fußt.[177] Zum anderen aber steigen auch die Kosten der Informationsbeschaffung. Dementsprechend wird angenommen, dass die ersten Ableitungen von Kosten und Nutzen, also Grenzkosten und Grenznutzen, positiv sind.

Ferner wird jedoch angenommen, dass der *Grenz*nutzen abnimmt, während die *Grenz*kosten zunehmen.[178] Ein optimaler Umfang der Informationsbeschaffung ergibt sich nun an der Stelle auf der Abszisse, an der Grenzkosten und Grenznutzen gleich groß sind (GK = GN). Das ist die Stelle, an der die Summe aus den Kosten der Informationsbeschaffung und den Kosten der Ignoranz (d.h. des Nicht-Informiert Seins) am geringsten ist.

Gerade im Lichte eines Interesses an einer effizienten Allokation von IT-SP/PSK sei betont, dass sich die Bedingungen der optimalen Informiertheit über die Zeit ändern können. Insbesondere können auch die (Grenz-)Kosten der Informationsbeschaffung sinken (Verschiebung der Grenzkostenkurve nach unten auf GK‘), sodass dann ein höheres Informationsniveau das effiziente Informationsniveau ist.

3.1.2 Zur Bedrohungsinformation

Eine weitreichende Problematik im Zusammenhang mit Cybersicherheit besteht darin, dass ein Schutzguteigentümer die Bedrohung, der er ausgesetzt ist, nach Art und Umfang überhaupt erst einmal erkennen muss. Scheinbar nehmen viele Unternehmen bislang noch sehr unsystematisch oder gar keine Bedrohungsanalysen vor und agieren eher reaktiv als präventiv.[179] Der aktuell in der Debatte vorgetragene Ruf nach mehr *awareness*[180] (Bewusstsein) kann nur der erste Schritt sein.[181] Denn es stellt sich grundsätzlich die Frage: Auf welchen Informationen kann oder soll eine unternehmerische Risikoanalyse denn nun beruhen?

---

[177] Und nur deswegen holt man ja überhaupt Informationen ein.

[178] Vgl. Abbildung 12.

[179] Vgl. z.B. Interview 12, Driver International.

[180] *Awareness*-Kampagnen laufen allerdings seit Jahren ohne durchschlagenden Erfolg. Darüber hinaus ist in einer zunehmend stark vernetzten Umgebung das schwächste Glied ausschlaggebend für den Gesamtschutz eines Systems. Ein Klick auf einen Link durch einen achtlosen Mitarbeiter reicht unter Umständen aus, ein ganzes System zu kompromittieren.

[181] Wiederkehrend wird in der Literatur ein „mangelndes Risikobewusstsein für Cyberbedrohungen“ (Wrede et al. 2018, S. 405) beklagt. In einer Umfrage schätzen Unternehmen den Schutzbedarf ihrer Daten im Jahr 2017 als höher ein als im Jahr 2011/12 (vgl. Hillebrand 2017, S. 4). Zu den Ursachen steigender Awareness gehören etwa Ereignisse wie die bekanntgewordenen Fälle von Daten-*leak*s oder wahrnehmbare Infektionen mit Schadprogrammen (vgl. ebd.).

Hier kommt es für ein Unternehmen auf zielführende Entscheidungsrundlagen an. Neben der Frage nach einem auf messbaren Kennzahlen (etwa *return on security investment*, ROSI) beruhenden Entscheidungsmechanismus, der Frage nach der Qualität der Sicherheitsinvestitionen (IT-SP/PSK) bzw. der Frage nach der Reaktion des eigenen Absatzmarktes ist gerade auch die Information über die Bedrohung in punkto Art, Umfang, Wahrscheinlichkeit und erwartetem Schaden maßgeblich.

Wie auf Märkten für IT-SP/PSK, so ist auch auf den Märkten für Bedrohungsinformationen der Schutzguteigentümer der Nachfrager. Dabei kann diese Information grundsätzlich entweder als privates oder aber als öffentliches (hier damit dann typischerweise als veröffentlichtes[182]) Gut bereitgestellt werden. Einen Überblick bietet Tabelle 4.

Bedrohungsinformation als **privates** Gut	Bedrohungsinformation als **öffentliches (veröffentlichtes)** Gut
• eigene Viktimisierungserfahrungen • Penetrationstests	• medial diskutierte Angriffe • Veröffentlichung von „Lagebildern“ aufgrund von … - Meldepflichten (Lagebericht des BSI) - Unternehmensumfragen (Cybersicherheits-Umfrage von BSI/ACS, Studienbericht des Bitkom) - Anzeigen bei Polizeibehörden (Bundeslagebild des BKA) - Einschätzungen von IT-SP/PSK-Anbietern

Tabelle 4 Bedrohungsinformationen als privates und als öffentliches Gut
Quelle: Eigene Darstellung.

Eigene Viktimisierungserfahrungen. Eine exklusive Information über die eigene Bedrohungslage erhält man, wenn man selbst Opfer eines Angriffs geworden ist. Unter der sprichwörtlichen Maßgabe „aus Schaden wird man klug“ erhält man so ggf. eine „anschauliche“ Information darüber, welche Art Bedrohungen unter anderem existieren und wie groß der Schaden sein kann. Einschränkend ist hier zu vermerken, dass es möglich ist, dass der Angriff vom Opfer unbemerkt bleibt. Selbst bei Kenntnisnahme des Angriffs mag eine Abschätzung des Schadens in Geldeinheiten zusätzlichen Aufwand und Kosten verursachen. Daher werden Schäden oftmals nur geschätzt. Vor allem aber dürfte die Information durch

[182] Als Beispiel seien die veröffentlichten und an die breite Allgemeinheit gerichteten Meldungen des Warn- und Informationsdienstes (WID) des BSI genannt, die kostenfrei online abrufbar oder per E-Mail zu abonnieren sind.

eigene Opfererfahrung für das einzelne Unternehmen wie auch volkswirtschaftlich als alleinige Informationsquelle aufgrund der Inkaufnahme von Schäden zu teuer sein. Deswegen wird unternehmensindividuell, in Verbänden, Initiativen und staatlichen Behörden versucht, Bedrohungsinformationen auch jenseits der äußerst kostenintensiven „Erfahrung am eigenen Leibe“ zu generieren.

So hat auch eine nicht-repräsentative Umfrage des BIGS unter Cybersicherheitsexperten ergeben, dass knapp zwei Drittel („trifft zu“, „trifft eher zu“) der Befragten sich ein jährliches, detailliertes und anonymisiertes Lagebild wünschen würden.[183]

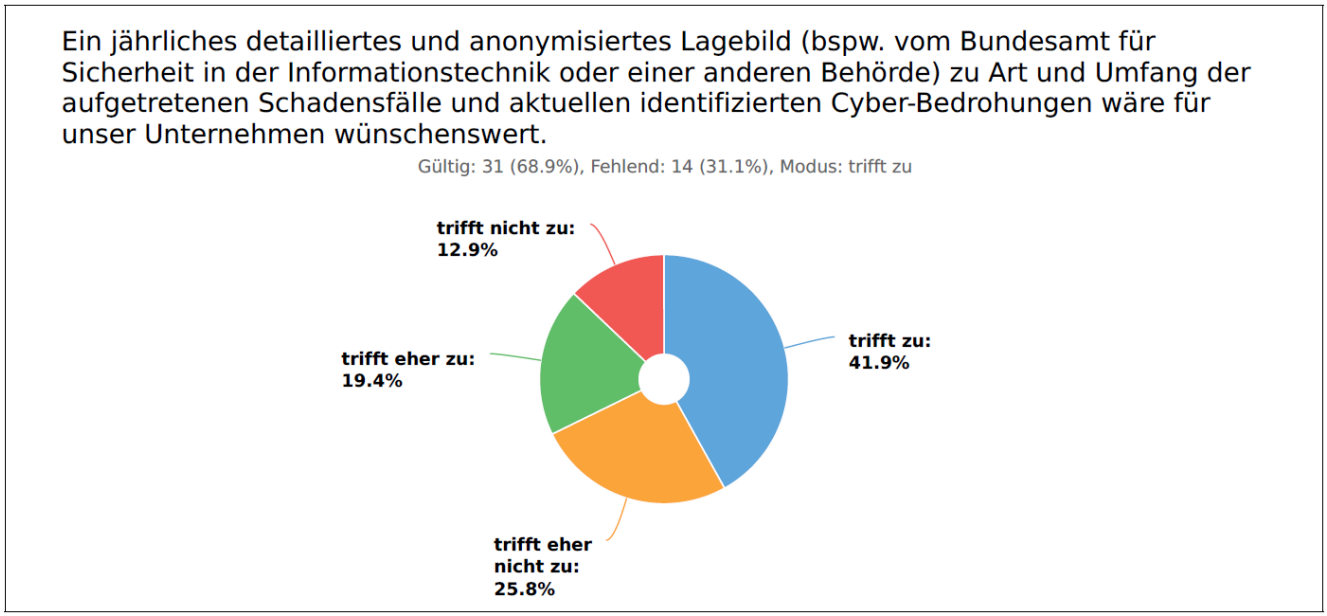


Abbildung 13 Wunsch nach einem genaueren periodischen Lagebild
Quelle: Eigene Darstellung auf Grundlage der Ergebnisse der Onlinebefragung des BIGS 2019.

Ebenso gaben bei der gleichen Befragung mehr als die Hälfte (56,2 Prozent) der Befragten an, dass die Bereitstellung der zugrunde liegenden Informationen (über bestehende Regelungen für Betreiber kritischer Infrastrukturen hinaus) verpflichtend geregelt werden müsse.[184]

***Penetrationstests*:** Eine Form, unternehmensindividuelle Informationen über Schwachstellen und somit die Qualität der Schutzleistungen zu generieren, sind beauftragte bzw. ausgeschriebene Penetrationen der eigenen Systeme. Es handelt sich dabei um bewusst provozierte und kontrollierte Angriffe durch nicht böswillige Akteure. Der Vorteil liegt hier darin, dass damit der Dynamik und Agilität auf Seiten der Angreifer entsprochen wird. Darauf basierend können geeignete Schutzmaßnahmen ergriffen werden, um die identifizierten Schwachstellen zu schließen. Penetrationstest könne zugleich aber auch als

[183] Vgl. Abbildung 13.
[184] Vgl. Ebd.

Schutzleistung verstanden werden. Mit ihrer Hilfe erhält ein Unternehmen Informationen über die Qualität der eingesetzten Schutzmaßnahmen.

***Öffentliche / Veröffentlichte Bedrohungsinformationen*:** Hier ist zunächst festzuhalten, dass es sich, gemessen an der Dynamik des Gegenstandes und angesichts meist jährlicher Berichte, um einen eher langsamen Transfer von Informationen handelt. Ferner handelt es sich nicht um unternehmensindividuelle, sondern um „allgemeine" Bedrohungsinformationen. Aber auch diese Berichtstätigkeit dürfte im Informationsgeschehen ihren Platz haben, beispielsweise bezüglich der allgemeinen Allokationsentscheidungen öffentlicher Mittel.

Akzeptiert man diese Voraussetzungen, so stellt sich die Frage nach der Qualität der Information. Diese wird maßgeblich davon bestimmt, wie sich die Akteure dieses Informationstransfers verhalten. Dabei ist die Information als öffentliches (*veröffentlichtes*) Gut dadurch charakterisiert, dass hier mehrere Akteure in Produktion und Bereitstellung der Information eingebunden sind, da ein „Vermittler" die einzelnen Informationen sammelt, verarbeitet und bereitstellt.[185]

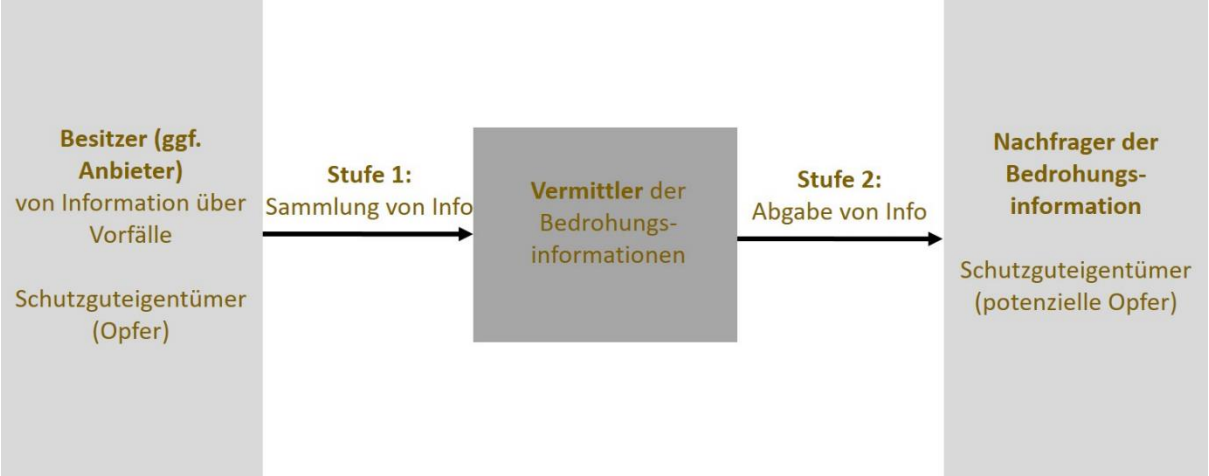


Abbildung 14 Transfer der Bedrohungsinformation über zwei Stufen
Quelle: Eigene Darstellung.

Vermittler und Bereitsteller von Bedrohungsinformationen sind hier etwa das BSI, die ACS, der Bitkom, und das BKA; oder auch private Anbieter von IT-SP/PSK.[186] Besitzer der Informationen (links in der Abbildung) sind Unternehmen bzw. Institutionen, die ihrerseits bereits Opfer von Angriffen wurden und ihrer ggf. bestehenden Meldepflicht beim BSI nachgekommen sind, eine Anzeige bei Polizeibehörden aufgegeben oder an einer Umfrage teilgenommen haben.

[185] Vgl. Abbildung 14.
[186] Vgl. Bartsch und Frey 2017, S. 14.

Mit Blick auf die Informationsqualität für den Nachfrager (rechts in der Abbildung) sind grundsätzlich

- Wollen (Interesse) und Können (Restriktionen) bezüglich der
- Informationsproduktion und -distribution
- beim Informationsbesitzer (links in der Abbildung) wie auch beim Vermittler

zu berücksichtigen. Eine ausführliche Analyse dessen steht noch aus und kann im Rahmen dieser Studie nicht geleistet werden. An dieser Stelle sollen die folgenden kursorischen Überlegungen genügen.

a) Informationsbesitzer

Informationsbesitzer sind Unternehmen, die Opfer von Cyberangriffen geworden sind (unabhängig davon, ob der Angriff erfolgreich verlaufen ist, oder zumindest teilweise abgewehrt werden konnte). Hier stellt sich die Frage, ob und unter welchen Umständen sie bereit sind, Informationen preiszugeben. Dabei dürften in ihr Kalkül die folgenden Überlegungen einfließen.

Für die Preisgabe spricht:

- das eigene Interesse an der reziproken Preisgabe von derartigen Informationen von anderen Unternehmen, da tatsächliche Opfer (in der Vergangenheit) ja immer auch potenzielle Opfer (in der Zukunft) sind. Damit besteht ein Interesse in der Sache und erhöht zumindest die Akzeptanz von Regelungen, die auf die Meldung hinwirken (Pflicht). Der Akzeptanz auch förderlich ist die Erwartung einer (erfolgreichen) Strafverfolgung und eines Schadensausgleichs.

- ein i.e.S. ökonomischer Anreiz, wie die Zahlungsbereitschaft von Informationsnachfragern oder Sanktionen bei einer bestehenden Meldepflicht.

Zu beachten ist bei einer Konstruktion von Anreizen durch die öffentliche Hand, inwieweit die Informationseigentümer im Lichte des Arrangements dazu tendieren könnten, unzutreffende Angaben zu machen.[187]

Gegen eine Preisgabe spricht:

- der mögliche Reputationsschaden, wenn die Informationen mit Nennung des betroffenen Unternehmens öffentlich werden. Hier hat allerdings das wachsende gesellschaftliche Verständnis für Cybersicherheits-Problematik für eine gewisse Entlastung gesorgt.[188]

[187] Vgl. zu rechtspolitischen Überlegungen im Rahmen von Informationspreisgaben etwa Tonner, Schlacke, und Alt 2015.
[188] Vgl. BSI 2019, S. 60 ff.

- der Umstand, dass u.U. auch potenzielle Angreifer sich die Informationen zunutze machen könnten.
- die bloßen Kosten der Informationsabgabe (Wer ist zuständig? Was darf die Person? Welche Unterlagen sind dafür nötig? Usw.)

b) Vermittler

Vermittler können nur Informationen weiterreichen, die sie zuvor erhalten haben. Qualitätsdefizite aus der ersten Stufe (Sammeln der Informationen) können in dieser zweiten Stufe nicht wieder kompensiert werden. Das etwa bedingt die begrenzte Aussagekraft von Schadensinformationen, wie sie das BKA veröffentlicht.[189] Unbenommen dieses Umstandes lässt sich festhalten:

Sind private Anbieter von IT-SP/PSK die Vermittler von Bedrohungsinformationen, so liegt dem typischerweise ein Geschäftsinteresse zugrunde, was den Wert der hier vermittelten Information schmälert. Ein gegenläufiger Effekt ergibt sich durch die in vielen Fällen jahrelange Expertise, die bei in diesem Geschäft tätigen Anbietern vorliegt. Sind Behörden die Vermittler, kommt es auf die gesetzlichen Vorgaben und das Selbstverständnis der Behörde an, wie die Bedrohungsinformationen weitergegeben werden. Schließlich sind dabei auch die Interessen der Opfer und staatliche Sicherheitsinteressen zu berücksichtigen. Hier zeigt sich der grundsätzliche Konflikt, dass aus Sicht der Wohlfahrtsökonomie der Wert des Wissens durch Teilung steigt, während sein sicherheitspolitischer Wert abnimmt, wenn Exklusivität nicht mehr gewahrt wird.[190]

Allianz der Guten: Neben den Bedrohungsinformationen, die von staatlichen Stellen und Cybersicherheitsunternehmen (direkt oder indirekt) zur Verfügung gestellt werden, haben sich auch Allianzen aus privatwirtschaftlichen Unternehmen gebildet. Die Initiative *Charter of Trust*, die sich 2018 auf Betreiben von einigen Industrieunternehmen u.a. Siemens gegründet hat, will die Zusammenarbeit der beteiligten

[189] Vgl. Abschnitt 2.2.

[190] Das BSI etwa scheint sich gegenwärtig nicht in erster Linie, als (Informations-)Vermittler dieser Art zu verstehen. Dies würde auch bedeuten, sich als *Service*-Institution für die Wirtschaft zu verstehen. Interessant ist in diesem Zusammenhang, dass gem. § 3 Abs. 1 Nr. 14 BSIG zu den Aufgaben bislang (lediglich) „Beratung und Warnung […] der Anwender“ gehören, wobei die „Anwender“ ganz am Schluss genannt werden. Der neue Referentenentwurf („IT-Sicherheitsgesetz 2.0“) sieht nun immerhin „Beratung, *Information* und Warnung“ (Herv. d. Verf.) vor.

Unternehmen im Bereich der Cybersicherheit intensivieren, um Vertrauen zu schaffen, Resilienzen aufzubauen und von den individuellen Erfahrungen im Kollektiv zu profitieren.[191] Darüber hinaus sind verbindlichen Anforderungen an die Cybersicherheit der Zulieferer, die in digitalisierten (internen und externen) Lieferketten/Prozessen eng mit den Industrieunternehmen verzahnt sind, als eines der zentralen Themen ausgemacht worden.[192]

Die Sorge vor negativen Auswirkungen durch die Bekanntmachung von Cyberangriffen auf die Reputation scheint zunehmend der Erkenntnis zu weichen, dass der Nutzen solcher Kooperationen größer ist. Durch die Internalisierung der Prinzipien solcher Allianzen, basierend auf dem gegenseitigen Vertrauen und der Übernahme von Verantwortung, entsteht ein Klubkollektivgut, bei dem mit Informationen über Angriffe auf das eigene Unternehmen eingezahlt wird, und bei dessen Nutzung innerhalb des Kreises keine Rivalität besteht. Dahinter steckt die Logik einer Plattform, die aus vielen einzelnen (direkt und indirekt) verbundenen Teilen besteht, auf der die (positiven wie auch negativen) Erkenntnisse/Erfahrungen des Einzelnen, dem Kollektiv dabei helfen, Resilienzen aufzubauen.

3.1.3 Zur Qualitätsinformation

Defizienter Transfer von Qualitätsinformationen zwischen den Marktseiten wird in den Wirtschaftswissenschaften spätestens seit Akerlofs *"Market for Lemons"*[193] diskutiert.[194] Anderson hat diese Überlegung auf Märkte für IT-SP/PSK übertragen.[195]

Akerlofs Theorie befasst sich mit der Frage, welche Folgen sich auf einem Markt ergeben, auf dem die Qualität eines Gutes durch die Nachfrager nicht vorvertraglich feststellbar ist.[196] Um die Wirkung dieser vorvertraglichen Nicht-Feststellbarkeit zu kontrastieren, ist es hilfreich, das Marktergebnis zu betrachten, das sich bei unterschiedlichen Qualitäten, allerdings ohne das Problem asymmetrischer Information, ergibt.[197] In diesem Fall lässt sich die Qualität also durchaus vorvertraglich feststellen.

---

[191] Vgl. https://assets.new.siemens.com/siemens/assets/api/uuid:405ff71f-fbd5-4131-b664-beed66500655/version:1560753163/charteroftrust-2019-de-online.pdf.

[192] Vgl. Höpner und Kerkmann 2019.

[193] Vgl. Akerlof 1970.

[194] In der Literatur wird das unter dem Begriff der asymmetrischen Information (zu Lasten des Nachfragers), der verborgenen Eigenschaften (*hidden characteristics*) oder der adversen Auslese (*adverse selection*) diskutiert.

[195] Vgl. Anderson 2001, S. 7 ff.

[196] Dies ist einschlägig besonders für sog. Erfahrungsgüter (d. h. Güter, bei denen die Qualität erst nach dem Konsum des Gutes vollständig bekannt wird), aber auch für sog. Vertrauens- bzw. Glaubens-Güter (d.h. Güter, bei denen die Qualität weder vor Vertragsschluss eingeschätzt werden kann, noch nach dem Konsum bekannt ist, vgl. etwa Fritsch 2018, S. 255). – In der ökonomischen Neoklassik wurden Fragen der Güterqualität zugunsten der Fragen um Gütermengen vernachlässigt. Hier hat die moderne Informationsökonomik, von der Akerlof einer der bekanntesten Vertreter ist, einen „Aufholprozess" eingeleitet, wobei aber die ökonomische Analysemethode beibehalten wird.

[197] Vgl. Abbildung 15.

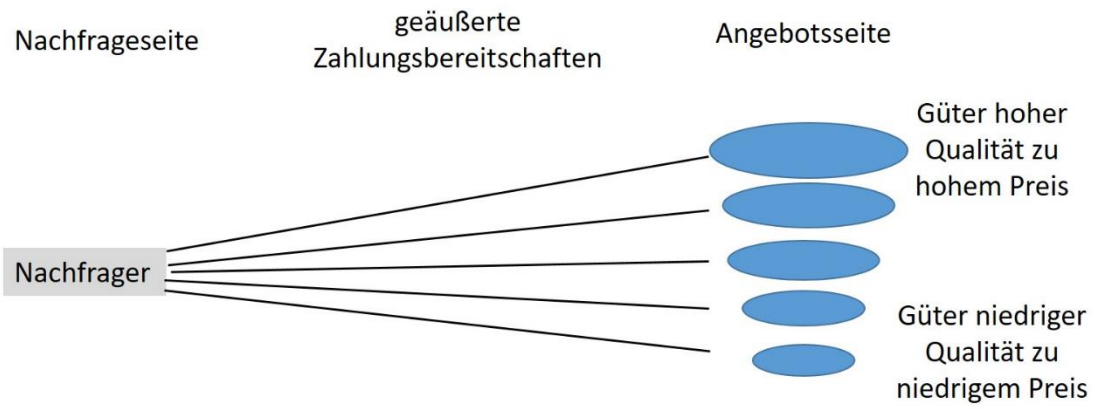


Abbildung 15 Nachfrageverhalten ohne asymmetrische Informationsverteilung
Quelle: Fritsch 2018, S. 252.

Hier stehen Nachfrager (auf der linken Seite) mehreren unterschiedlichen Preis-Qualität-Kombinationen der Angebotsseite (auf der rechten Seite) gegenüber. So gibt es etwa Güter zu hoher Qualität bei hohem Preis oder aber Güter zu geringer Qualität bei geringem Preis. Man kann sich dabei im Prinzip ein Kontinuum mit gewissen Abstufungen vorstellen. Je nach Zahlungsbereitschaft können die Nachfrager auf eine bestimmte Preis-Qualitäts-Kombination zugreifen. In der Folge bestehen nebeneinander unterschiedliche qualitätsbezogene Marktsegmente.

Anders liegt der Fall bei asymmetrisch verteilter Information bzw. vorvertraglich nicht feststellbarer Güterqualität vor.[198]

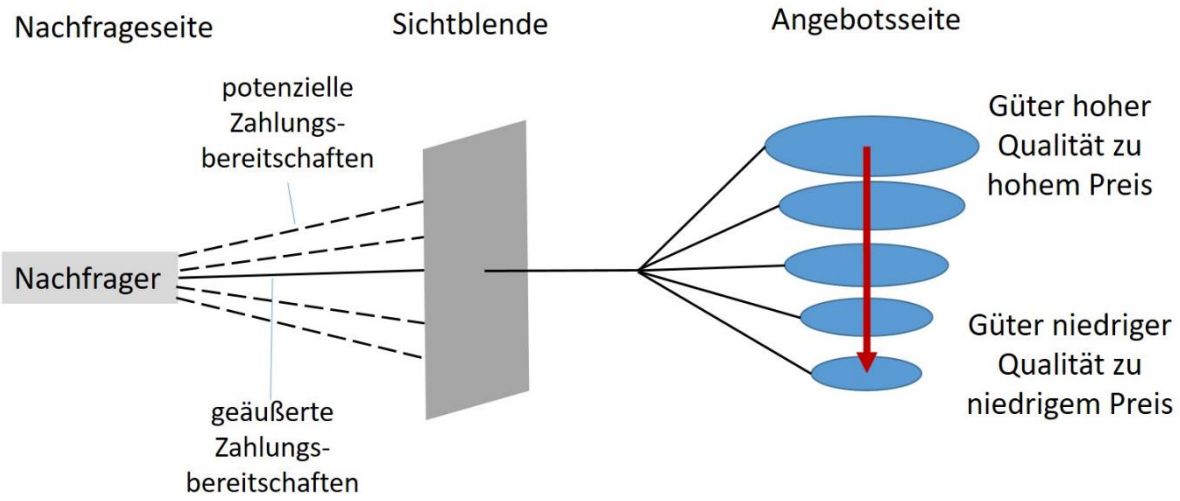


Abbildung 16 Nachfrageverhalten mit asymmetrischer Informationsverteilung
Quelle: Fritsch 2018, S. 252.

[198] Vgl. Abbildung 16.

Aufgrund einer mit Blick auf die Produktqualität bestehenden Sichtblende können die Nachfrager zwar den Preis, nicht aber die Qualität erkennen. Wenn sich die Nachfrager nun hinsichtlich der Qualität an einem stochastischen, „durchschnittlichen“ Erwartungswert orientieren, reicht ihre Zahlungsbereitschaft nicht mehr aus, um die Herstellungskosten von Produkten höherer Qualität abzudecken. Damit werden sich Anbieter höherer Preis-Qualitäts-Kombinationen vom Markt zurückziehen. Wenn man annimmt, dass sich in der Folge ein derartiges Wechselspiel zwischen Nachfrage und Angebot fortsetzt, werden im Ergebnis eines solchen Prozesses der sog. adversen Auslese nur noch Güter zu geringem Preis und geringer Qualität am Markt umgesetzt. Gesellschaftliche Wohlfahrtseinbußen entstehen dadurch, dass *potential gains from trade* im Bereich höherer Qualitäten ausbleiben. Auf den Märkten für IT-SP/PSK ist genau dies nun auch zu beobachten: *”[S]ecurity vendors may assert their software is secure, but buyers refuse to pay a premium for protection and so vendors become disinclined to invest in security measures.“*[199]

Als Beispiel können Viren-Scanner dienen, deren Basis-Versionen von vielen Herstellern kostenfrei angeboten werden. Hier besteht ein Problem in der Anreizstruktur, da die tatsächliche Wirksamkeit und Schutzwirkung für viele Nutzer intransparent ist, und bei Ausbleiben merklicher Zwischenfälle kein Bewusstsein für die Notwendigkeit höherer Investitionen in qualitativ bessere Scanner entstehen wird. Funktioniert ein Virenscanner besonders gut, ist das Problem besonders ausgeprägt, da wenige oder keine Schadensfälle auftreten. Dies ist ein Problem, das Anbieter von Schutzleistungen auch im analogen Bereich betrifft: Ist die Qualität hoch, wird die Schutzleistung als überflüssig und zu teuer empfunden, ist sie zu niedrig, wird sie aufgrund ihres Versagens als zu teuer empfunden. In der Konsequenz werden die qualitativ besten Virenscanner schwer verkäuflich, und in ihre Weiterentwicklung kann tendenziell weniger investiert werden.

Zu berücksichtigen ist, dass sich derartige Probleme asymmetrischer Information auf dem Absatzmarkt der Schutzguteigentümer fortpflanzen. Denn auch deren Leistungen sind in der einen oder anderen Form stets Produkte mit Sicherheitskomponente. Diese Perspektive erscheint jedoch gerade deswegen lohnend, da die Sicherheitsinvestitionen eines solchen Unternehmens gerade auch davon abhängen, in welchem Umfang die Kunden dieses Unternehmens diese Investitionen in IT-SP/PSK honorieren. Wenn man diese Überlegung fortsetzt, dann kommt es entlang einer Wertschöpfungskette darauf an, dass die Endnutzer eines bestimmten Produkts diese Investitionen hinreichend honorieren. Voraussetzung dafür ist, dass Qualitätsunterschiede hinsichtlich Sicherheitseigenschaften durch die Nachfrager bzw. Endkunden erkannt werden können.

[199] Moore 2010a, S. 8.

Dass das erläuterte Problem der Akerlofschen asymmetrischen Information bzw. versteckter Eigenschaften (*hidden characteristics*) durchaus praxisrelevant ist, lässt sich durch eine Interpretation der sog. Cybersicherheits-Umfrage unterlegen. Hierin untersucht das BSI in Kooperation mit der Allianz für Cybersicherheit seit 2014 in jedem Jahr „die Gefährdungslage und Betroffenheit deutscher Institutionen durch Cyberangriffe sowie den Umsetzungsstand entsprechender Schutzmaßnahmen".[200] Für die Umfrage zum Jahr 2018 wurden die Befragungen im Februar/März 2019 durchgeführt. Von den 1.039 teilnehmenden Institutionen waren 57 Prozent kleine und mittlere Unternehmen bzw. Institutionen (1 bis 249 Beschäftigte) und 43 Prozent große Unternehmen bzw. Institutionen (250 oder mehr Beschäftigte). Dabei kommen die befragten Institutionen etwa aus den Branchen Information und Kommunikation (18 Prozent), Energieversorgung (17 Prozent) oder öffentliche Verwaltung (11 Prozent).[201] Mit Blick auf die Grundlagen aus Abschnitt 2 wurden hier also – jedenfalls im Kern – Schutzguteigentümer befragt. Innerhalb dieser Institutionen/Unternehmen wurden wiederum die IT-Fachleute befragt.[202]

Im Zusammenhang mit dieser Cybersicherheits-Umfrage wird hier nun die These aufgestellt, dass ein strukturelles Spannungsfeld besteht, zwischen

i. einerseits einem durchaus **vorhandenen und sogar zu guten Teilen handlungsleitenden Problembewusstsein** und

ii. andererseits der Herausforderung für die Unternehmen, dass sich der Wert dieser Investition (höhere Sicherheit) **nicht hinreichend als Wettbewerbsparameter gegenüber den Nachfragern auf den Absatzmärkten kommunizieren lässt** und somit im Rahmen des Wettbewerbsgeschehens eher als „Bremse", mithin als Wachstumsbremse wirkt.

In Abbildung 17 verbindet sich der erste Teil (i) mit den Unterabbildungen a, b und c und die der zweite Teil (ii) mit der Unterabbildung d.

Zu (i): Es wurde bspw. erfragt (Unterabbildung a), ob Cyberangriffe als relevante Gefährdung betrachtet werden. Dem können gut drei Viertel der befragten Institutionen (76 Prozent) zustimmen. Weiterhin wurde (Unterabbildung b) – in dynamischer Hinsicht und im Zusammenhang mit den Digitalisierungsprozessen – gefragt, ob sich hierbei aus Sicht der Befragten die Angriffsflächen für Bedrohungen aus dem Cyberraum vergrößern. Das betrachten sogar nicht weniger als 88 Prozent der Befragten als zutreffend, also noch einmal zwölf Prozentpunkte mehr als bei der ersten Frage. Mit Blick auf den eigenen

[200] BSI und ACS 2019, S.3.

[201] Vgl. Ebd.

[202] Vgl. Ebd., S. 26. Die genaue Auffächerung lautet hier: IT-Sicherheitsverantwortliche (77 Prozent), IT-Spezialisten (42 Prozent) und IT-Anwender/innen (27 Prozent).

Handlungsbedarf (Teilabbildung c) wurde in der vorangegangenen Cybersicherheits-Umfrage[203] ermittelt, inwieweit die Befragten Handlungsbedarf für die betreffende Institution sehen bzw. inwieweit Verbesserungen geplant sind. Hier sind es immerhin 71 Prozent der Institutionen, die Verbesserungen planen. Interessant ist nun, dass weitere 7 Prozent der Befragten zwar Handlungsbedarf sehen, dies aber nicht umsetzen. Dies könnte gerade auch mit dem zweiten Teil (ii) der o. g. These zusammenhängen.

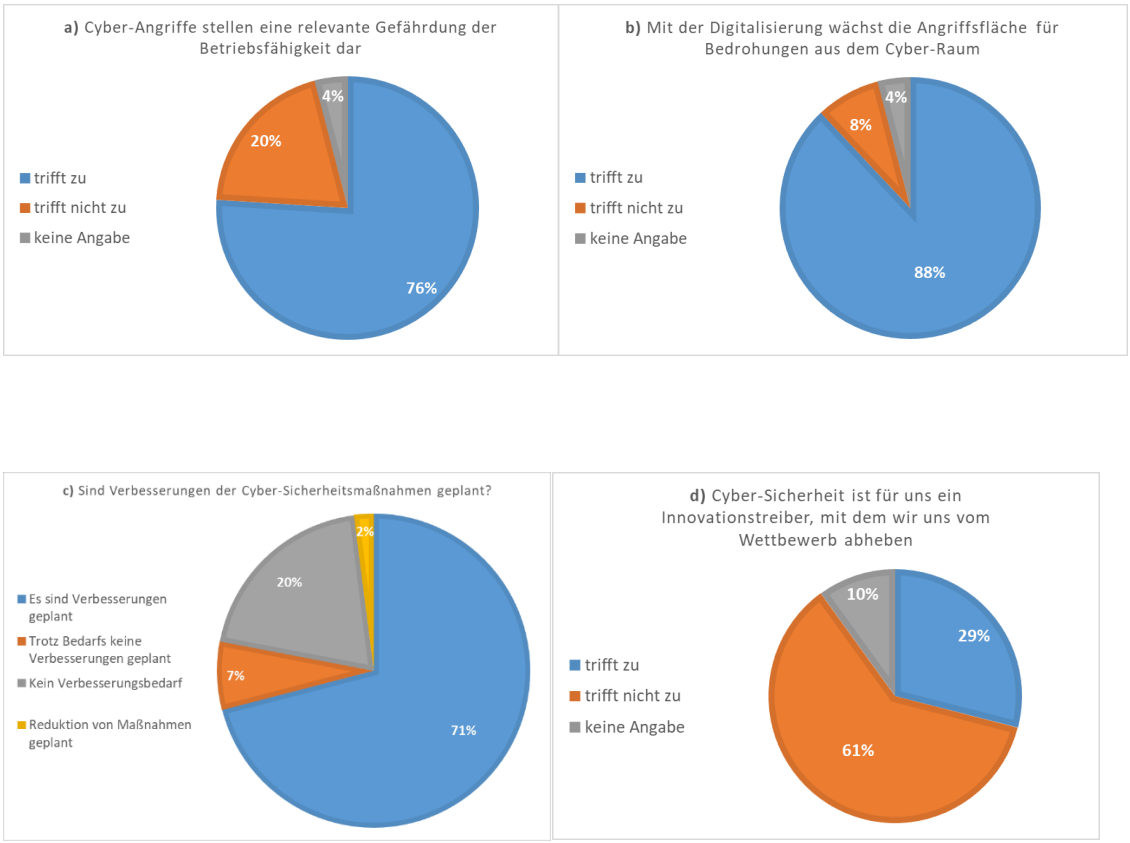


Abbildung 17 Ergebnisse der Cybersicherheits-Umfrage
Quellen: BSI und ACS 2018 und 2019.[204]

Zu (ii): In der Cybersicherheits-Umfrage (Unterabbildung d) wurden die Teilnehmer zudem mit der Aussage konfrontiert, die es zu bewerten galt: „Cybersicherheit ist für uns ein Innovationstreiber, mit dem wir uns vom Wettbewerb abheben." Der Anteil derer, die dem zustimmen konnten, ist hier weit geringer als bei allen anderen Aussagen. Lediglich 29 Prozent betrachten dies als zutreffend. Hingegen

[203] Vgl. BSI und ACS 2018, S. 11.
[204] Im Einzelnen: Abbildung a) BSI und ACS 2019, S. 6; Abbildung b) BSI und ACS 2019, S. 7; Abbildung c) BSI und ACS 2018, S. 11; Abbildung d) BSI und ACS 2019, S. 8. Dabei entstammen die Abbildungen a, b und d aus der jüngsten Umfrage, die Abbildung c aus der Umfrage davor. Hintergrund ist hier, dass in den jährlichen Cybersicherheitsumfragen den Unternehmen nicht in jedem Jahr die gleichen Fragen gestellt werden.

halten 61 Prozent der Befragten für unzutreffend. Dementsprechend wird in BSI und ACS getitelt: „Weniger als ein Drittel der Institutionen verstehen Cybersicherheit als Chance für Innovationen.“[205]

In Abbildung 18 sei diese Diskrepanz noch einmal in einer Übersicht verdeutlich. Auf der linken Seite die drei Säulen, die je über 70 Prozent indizieren, auf der rechten Seite eine dem gegenüber stark abfallende Zustimmung in der Frage, inwieweit Cybersicherheit als Wettbewerbsparameter eingesetzt werden kann.

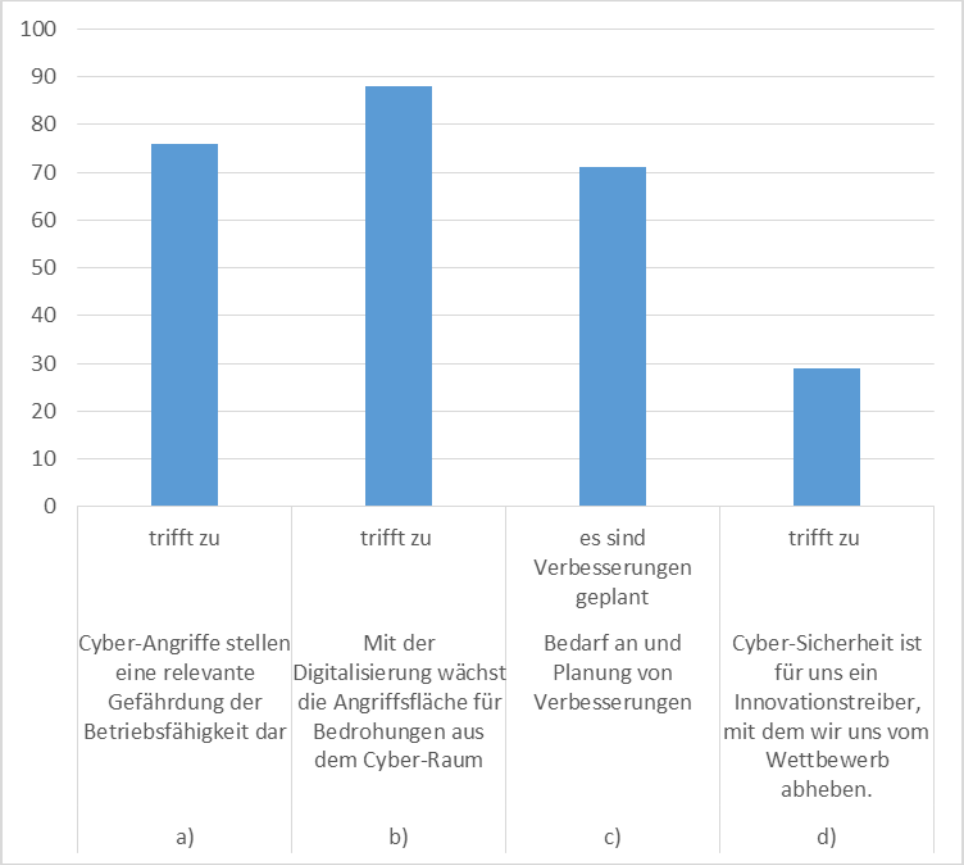


Abbildung 18 Direkter Vergleich der Antworten
Quelle: BSI und ACS 2018 und 2019.[206]

Worin liegt die Ursache für eine solche Diskrepanz zwischen den Ergebnissen einerseits a) bis c) und andererseits d)? Es erscheint dafür die Erklärung überzeugend, dass für die betrachteten Institutionen/Unternehmen Schwierigkeiten bestehen, den Nutzen, der sich aus Sicherheitsinvestitionen ergibt, den Nachfragern *ex ante* auf ihren Absatzmärkten zu kommunizieren. Dass man entgegen dieser Schwierigkeit gleichwohl Verbesserungen plant, lässt sich u. U. damit erklären, dass man *ex post*-Wirkungen

[205] BSI und ACS 2019, S. 8.

[206] Die einzelnen Zuordnungen der Quellen gelten wie in vorangegangener Fußnote 195.

antizipiert, die erheblich sind; namentlich eine tatsächliche Belastung für die Betriebstätigkeit[207] bis hin zur Existenzgefährdung sowie Reputationsschäden bei Vorfällen. Mit Letzteren ergibt sich auf Seiten der Nachfrager auf den Absatzmärkten gleichsam ein ineffizient später Lerneffekt.

Die Zustimmungsdifferenzen zwischen den Fragen a) bis c) könnten wie folgt erklärt werden. Die Zustimmung zur Aussage a) könnte als eine Referenz über die *awareness* zur aktuellen Bedrohungslage fungieren, und wäre abhängig von Informationen, wie sie in Unterabschnitt 3.1.1 diskutiert wurden. Frage b) hat hingegen einen allgemeineren, in die Zukunft gerichteten Charakter, der von der konkret-gegenwärtigen eigenen Bedrohung abstrahiert. Dem können noch einmal deutlich mehr Unternehmen bzw. Institutionen zustimmen. In Frage c) geht es in die andere Richtung. Hier wird die Einsicht aus der Beantwortung von Frage a) mit Blick auf tatsächliche Maßnahmen für die Praxis herausgefordert. Hier aber dürfte der Aspekt der mangelnden Wirksamkeit von Sicherheit als Wettbewerbsparameter (sichtbare Qualitätseigenschaft) die Ursache sein. Die Lücke, um die hier vertretende Interpretation abzurunden, die sich zwischen den positiven Antworten aus zu den Fragen a) (76 Prozent) und c) (71 Prozent) ergibt, wird im Rahmen von Frage c) durch die Antwortoption „Trotz Bedarfs keine Verbesserungen geplant“ (über-) kompensiert, was die Situation von 7 Prozent der Befragten widerspiegelt.

3.1.4 Vorläufige Schlussfolgerungen und Handlungsempfehlungen

Die Überlegungen aus diesem Abschnitt machen über die einzelnen Marktversagensprobleme hinaus deutlich, wie „dünn“ die informationelle Entscheidungsbasis für Unternehmen (als Schutzguteigentümer) in ihrem Risikomanagement sein dürfte. Es zeigt auf, dass man wohl über die bloße appellative Intervention hinausgehen muss, wie sie etwa im Zusammenhang mit *Cybersecurity* von Bartsch und Frey vorgetragen wird: Unternehmen und Schutzguteigentümer mögen Qualitätsaspekte bei derartigen Investitionsentscheidungen stärker in den Mittelpunkt stellen und „weniger kostenorientiert“ agieren.[208] Wenn die Probleme in der beschriebenen Weise existieren, lassen sich Informationsdefizite kaum durch ein bloßes „Plädoyer pro Qualität“ überwinden.

Es wird vielmehr darauf ankommen, effiziente, teils marktbasierte, teils institutionelle Wege zu finden und zu optimieren, um einen Informationsfluss herzustellen, der Entscheidungen für Cyberschutz auf eine rationale Basis stellt. Bei dem Marktversagenstatbestand der Informationsdefizite im Allgemeinen

[207] Vgl. Frage a – Gefährdung der Betriebstätigkeit.
[208] Bartsch und Frey 2017, S. 33.

und bei dieser komplexen Sachlage im Besonderen kommt es darauf an, dass die Gesellschaft, insbesondere Wirtschaft und Politik, zügig einen gemeinsamen Lernprozess generiert. Auf der Grundlage lässt sich durchaus unterstützen, was in der letzten Bitkom-Studie empfohlen wurde:

> „Besonders wichtig bei der Bekämpfung von Cybercrime ist aber auch der Austausch von Informationen und Erfahrungen. Dies sollten Unternehmen zum einen untereinander tun, aber auch mit den staatlichen Behörden. Bestehende Kooperationen, wie beispielsweise die Sicherheitskooperation Cybercrime zwischen Bitkom und sieben Landeskriminalämtern oder die Allianz für Cybersicherheit, sind Plattformen, auf denen der Austausch funktioniert. Solche Organe sollten fortgeführt und ausgebaut werden.“[209]

Eine solche „weiche“ Handlungsempfehlung, die auf Kommunikation, Kooperation und auch weitere institutionen- und informationsökonomische Forschung hinweist, ist bei Informationsdefiziten angemessen. Denn bei ihnen sind in vielen Fällen durchaus effiziente Marktlösungen zu erwarten, da die Wirtschaftssubjekte gerade bei Qualitätsinformationen ein Interesse haben, die Asymmetrie zu überwinden. Beispiele dafür sind:

- Produkte und Dienstleistungen, die ihrerseits die Qualität von IT-SP/PSK prüfen,[210]
- kostenlose Basisversionen von IT-SP/PSK oder
- privatvertragliche Haftungsverpflichtungen innerhalb von Wertschöpfungsketten.

Für die Politik kommt es darauf an, ein wachsamer Begleiter dieser Prozesse zu sein, um ggf. flankierend – etwa mit Zertifikaten – oder aber letztlich regulierend – mit Standards oder Haftungsregelungen zu agieren.

Im Bereich des Transfers von Bedrohungsinformationen scheint eine wiederkehrende Evaluation der Entstehung von Lagebildern, insbes. des BSI, unter Effizienz- und anreizökonomischen Aspekten sinnvoll.

[209] Bitkom 2018a, S. 57.

[210] Vgl. Berke 2019. So gibt es *Software*, die andere *Software* auf ihre Sicherheitseigenschaften hin überprüfen.

3.2 Externe Effekte

Zu den gängigen Theorien des Marktversagens gehört auch die Theorie der sog. externen Effekte.[211] Hier ist nun *nicht* das Problem, dass Entscheider wegen Informationsdefiziten ihr individuell optimales Schutzniveau verfehlen. Das Problem ist vielmehr, dass ein *gesellschaftlich optimales* Schutzniveau trotz individueller Optima verfehlt wird, da die Entscheidungen der einzelnen Akteure durch technologische Wechselwirkungen auf Kosten- bzw. Nutzenniveaus anderer Akteure Einfluss nehmen, ohne dass dies durch den Marktmechanismus erfasst bzw. preislich ausgeglichen wird.[212] [213] Institutionenökonomisch betrachtet spricht man davon, dass die Eigentumsrechte der einzelnen ökonomischen Akteure nicht klar abgegrenzt sind.

Die Lehrbuchliteratur zu externen Effekten bezieht sich zu weiten Teilen auf *negative* externe Effekte in der *Produktion*, im Zusammenhang mit den paradigmatischen Beispielen aus der Umweltpolitik. Im Zusammenhang mit IT-SP/PSK geht es nun um **Netzwerkeffekte**, die sich im Zusammenhang mit mehr oder weniger sicherer Software ergeben. Hier spielen mögliche *positive* wie *negative* externe Effekte im *Konsum* eine Rolle, wie man es etwa vom Bereich der Impfungen bzw. Infektionskrankheiten kennt. Ein Internetznutzer, der durch eine Investition in einen Virenscanner seinen Rechner erfolgreich gegen Befall durch Schadsoftware schützt und damit als Glied im Infektionsweg ausfällt, schützt „automatisch" andere Unternehmen und Privatnutzer von Rechnern. Abbildung 19 stellt schematisch dar, dass mit steigendem Umfang bzw. Qualität der Sicherheitsmaßnahmen der externe Nutzen steigt. Dabei sei angenommen, dass der externe Grenznutzen (erste Ableitung) sinkt, sich der Effekt also zusehends abschwächt.

[211] Vgl. statt vieler Donges und Freytag 2009; Fritsch 2018, S. 84 ff.

[212] Vgl. Fritsch 2018, S. 85.

[213] Vor diesem Hintergrund wird der ökonomische Fachbegriff der „externen Effekts" zuweilen auch als „technologischer" externer Effekt präzisierend bezeichnet. Damit kann dieses Phänomen von sog. pekuniären oder psychologischen externen Effekten abgegrenzt werden (vgl. etwa Fritsch 2018, S. 85). Nur der technologische externe Effekt aber stellt innerhalb der ökonomischen (Allokations-)Theorie einen Tatbestand eines Marktversagens dar.

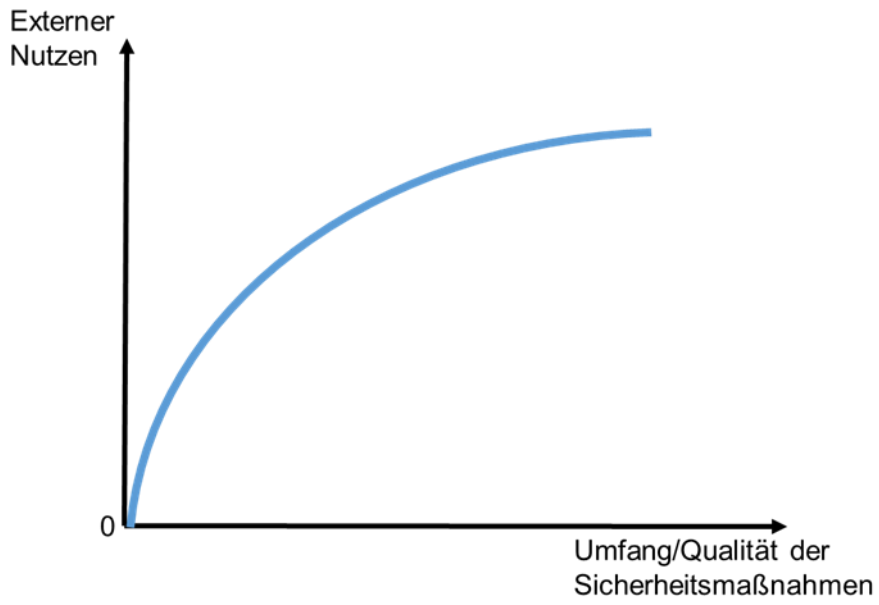


Abbildung 19 Umfang/Qualität der Sicherheitsmaßnahmen und externer Nutzen
Quelle: Eigene Darstellung.

Für diesen „gemeinnützigen“ Effekt wird der Käufer des Virenscanners nicht finanziell entschädigt. Folglich kommt es gesellschaftlich zu einer unter-effizienten Versorgung mit qualitativ hochwertigen Virenscannern.

Ist aber ein Gerät unzureichend geschützt, dann kommt es nicht zu positiven, sondern zu negativen Externalitäten. Ein in der Praxis relevantes Beispiel dafür ist die Kaperung von schlecht abgesicherten Alltagsprodukten des sog. *Internet of Things* durch Hacker, die diese dann zu einem *Botnet* zusammenschließen und andere Nutzer angreifen. Ein anderes Beispiel sind schlecht abgesicherte Personal Computer und der darauf installierten Software, von denen aus sich nach einer Infektion Computerviren über die Adressbücher der Emailprogramme eigenständig weiterverbreiten. Das Versäumnis der Nutzer, ihre Geräte ausreichend zu schützen, macht diese zu Gliedern der Infektionswege, und schädigt damit andere Nutzer.

Das Prinzip dahinter ist, dass ein nicht-konsolidiertes, also mit Blick auf die Sicherheit nicht nachhaltiges, Wachstum (Erschließung von Geschäftsfeldern) zu negativen externen Effekten führen kann; dann also, wenn die Sicherheitsmaßnahmen nicht proportional ansteigen. Schematisch ist dies in Abbildung 20 dargestellt. Bei gegebenen (konstanten) Sicherheitsmaßnahmen führt eine Ausweitung der Digitalisierung zu externen Kosten (negativen externen Effekten). Dabei sei angenommen, dass die externen Grenzkosten (erste Ableitung) steigen.

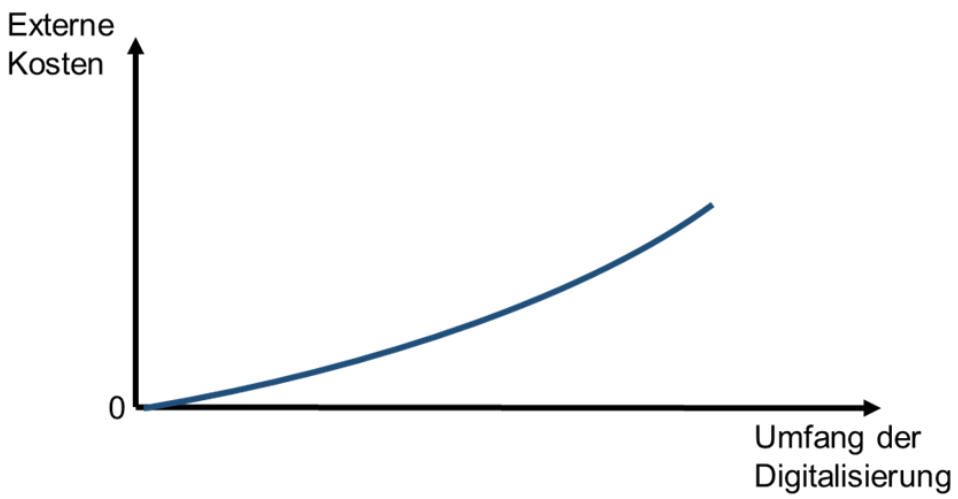


Abbildung 20 Umfang der Digitalisierung und externe Kosten
Quelle: Eigene Darstellung.

In der Zusammenschau von positiven und negativen externen Effekten lässt sich konstatieren, dass das Bestehen von Externalitäten und seine saldierte Richtung von zwei Determinanten abhängt, nämlich von:

- Umfang bzw. Qualität an Schutzmaßnahmen: Hier kann eine Erweiterung c. p. (bei konstantem Digitalisierungsniveau) zu positiven externen Effekten führen.
- Umfang der Digitalisierung: Hier kann eine Erweiterung c. p. (bei konstantem Niveau an Schutzmaßnahmen) zu negativen externen Effekten führen.

In Abbildung 21 ist dieser Zusammenhang in einem *dreidimensionalen* Koordinatensystem dargestellt. Die Ordinate stellt die Externalitäten da, die entweder positiv (externer Nutzen) oder aber negativ (externe Kosten) ausfallen können. Für die Determinanten Digitalisierungsumfang und Umfang bzw. Qualität der Schutzmaßnahmen gibt es nur positive Achsenabschnitte.

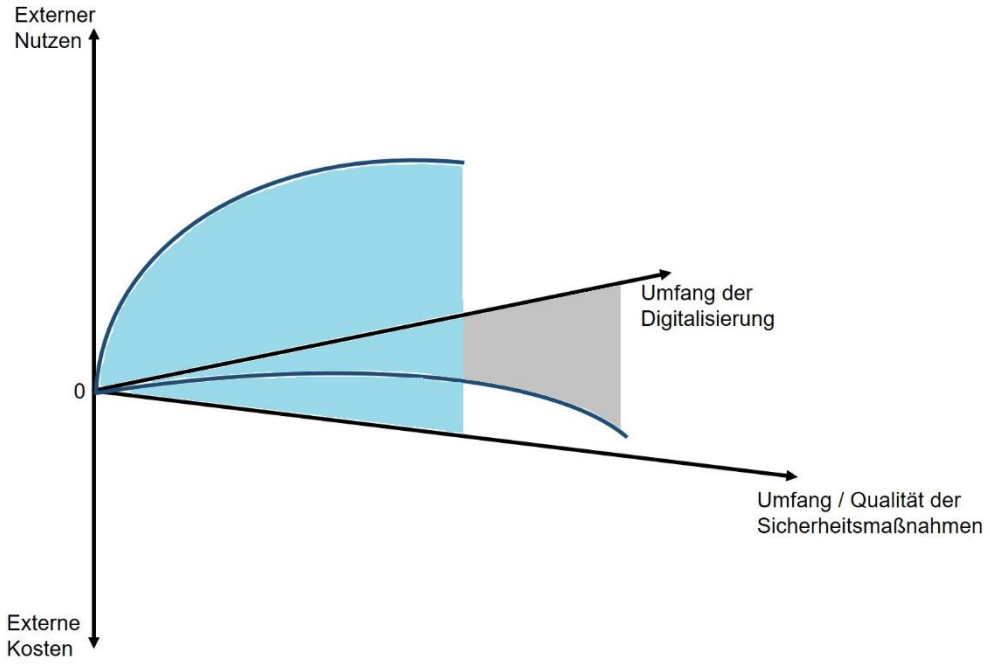


Abbildung 21 Digitalisierungsumfang und Sicherheitsmaßnahmen als Determinanten für Externalitäten
Quelle: Eigene Darstellung.

Damit ergibt sich ein *Externalitätengebirge*, das in den positiven wie negativen Bereich hineinreicht. Bei partieller Variation gilt, was bereits im Zusammenhang der Abbildungen 21 genannt wurde: Steigt c.p. die Digitalisierung, so verändern sich die Externalitäten negativ (auf dem Gebirge „abwärts"); steigen c.p. die Sicherheitsmaßnahmen, so verändern sich die Externalitäten positiv (auf dem Gebirge „aufwärts").

Im Rahmen eines solchen Modells ist jedes Unternehmen bzw. jedes Geschäftsfeld durch einen bestimmten Digitalisierungs-Sicherheitsvektor charakterisiert. Entsprechend ergibt sich ein positiver oder negativer externer Effekt. Allerdings kann der externe Effekt auch genau „null" sein. Das wäre der Fall, wenn es sich um eine stetige, an jeder Stelle ableitbare Funktion handelt würde.[214] Das ist an all den Stellen der Fall, an denen das Externalitätengebirge die Ebene schneidet. Damit ist konzeptionell ein Wachstumspfad vorstellbar, an dem keinerlei externe Effekte (EE) bestehen (EE = 0). Er ist in Abbildung 22 dargestellt, in einem „Grundriss" des Externalitätengebirges aus Abbildung 21.

[214] Eine weitere notwendige Bedingung für Differenzierbarkeit ist die Eindeutigkeit der Ableitung an einer gegebenen Stelle, es muss also genau eine Tangente geben. Das ist nicht der Fall, wenn die (stetige) Kurve Knicks oder Spitzen enthält. In der Praxis muss außerdem Stetigkeit nicht unbedingt gegeben sein. Hier ist es vielmehr auch vorstellbar, dass an einem bestimmten Punkt eine infinitesimale Verbesserung der Sicherheitsqualität zu einem Sprung bei den externen Effekten führt.

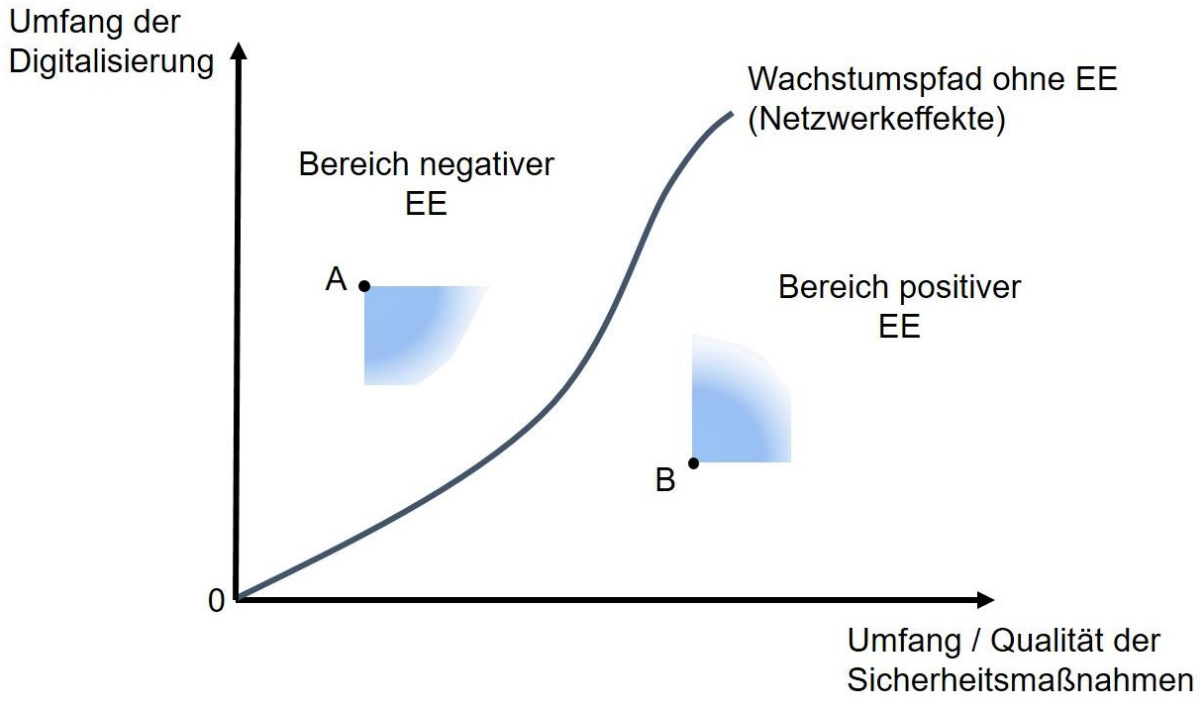


Abbildung 22 Positive und negative externe Effekte zwischen Digitalisierungs- und Sicherheitswachstum
Quelle: Eigene Darstellung.

In der Abbildung wird deutlich, dass sich links und rechts des Wachstumspfads ohne externe Effekte ein Bereich negativer (links) und positiver (rechts) externer Effekte ergibt. Jedes Unternehmen liegt mit seiner Wachstums-Sicherheits-Kombination mutmaßlich in einem der beiden Bereiche, etwa im Punkt A oder im Punkt B. Eine Politik der Internalisierung würde nun auf folgendes abzielen:[215]

- Im Bereich **negativer externer Effekte** geht es darum, das sicherheitsneutrale Digitalisierungswachstum stärker zu belasten (im Lichte relativer Preise zu verteuern). Dies wäre ein Anreiz, das Sicherheitsniveau zu erhöhen und/oder den Digitalisierungsumfang zu verringern (blaue Fläche am Punkt A).
- Im Bereich **positiver externer Effekte** geht es darum, das digitalisierungsneutrale Sicherheitswachstum zu begünstigen (im Lichte relativer Preise günstiger zu machen). Dies gäbe Anreiz, das Sicherheitsniveau und/oder das Digitalisierungsniveau zu erhöhen (blaue Fläche am Punkt B).

Wie sollte Angesichts dieser Zusammenhänge reguliert werden? Im Gegensatz zu Informationsdefiziten ist bei externen Effekten eine stärkere regulatorische Entschlossenheit gefragt. Das liegt darin begründet**,**

[215] Vgl. blaue Flächen in Abbildung 22.

dass bei externen Effekten, anders als bei Informationsdefiziten, die Interessen der Marktteilnehmer nicht darauf hinwirken, das Effizienzdefizit zu überwinden. Dabei stehen grundsätzlich zwei regulatorische Instrumente bereit, einerseits der Standard, andererseits die Subvention/Sanktion.

Beim **Standard** erscheint es sinnvoll, ihn möglichst mit Blick auf das Sicherheits*ziel* zu formulieren, um bezüglich der technischen Mittel eine effizienzfördernde Technologieoffenheit zu gewährleisten. Hier ist ferner zu klären, wer (Hersteller, Händler) dem Standard verpflichtet wird und wie sich dies auf Importe (denkbar wären sogar Einfuhrverbote) auswirken kann.

Bei einer **Subvention** wären die folgenden institutionellen Fragen zu klären:

- Soll die Förderung institutionell über die Nachfrage oder über die Anbieter organisiert werden? (in der Theorie ist beides gleichermaßen möglich und für den Effekt unerheblich)
- Welche Form soll die Subvention genau erhalten? (Absetzungen für Abnutzung, Steuererleichterungen usw.)
- Welche Produkte/Leistungen sollen gefördert werden? Man müsste diese Festlegungen wohl mit einem Zertifizierungs- bzw. Standardisierungssystem verbinden.
- Was ist die Bemessungsgrundlage für eine Subvention? Der Preis des Produktes? Der Qualitäts- bzw. Sicherheitsstandard?
- Wie wird der Umfang der Subvention festgelegt? (Subventionssatz s)
- Gibt es einen erforderlichen Mindestumsatz/ eine Obergrenze (Deckelung)? usw. (Spezifizierungsparameter des Subventionsbetrages)

Analogie zur Herdenimmunität

Das Sicherheitsniveau eines Netzwerks aus einzelnen unterschiedlichen Komponenten und Systemen wird von der Absicherung der Einzelteile bedingt. Schwachstellen in einzelnen Teilen dieser Netze – man kann sie als Glieder einer Kette verstehen – sind die häufigsten Einfallstore für Eindringlinge und bringen somit das gesamte Netzwerk in Gefahr. Die stark interdependente Komponente ist für die Sicherheitsinfrastruktur insofern eine Herausforderung, als dass ein Netzwerk nur so stark ist, wie das schwächste Glied in der Kette. Punkt- und Insellösungen können nur Löcher stopfen und ein erster Schritt auf dem Weg zu einem höheren Cybersicherheitsniveau sein, aber sie können keine ausreichende Gesamtstrategie in einer hochvernetzten Umgebung darstellen. Die Sicherheitsanstrengungen aller Netzwerkmitglieder müssen auf ein vertretbares Mindestniveau angehoben werden und mit dem „Stand der Technik“, permanent auf die Aktualität hin untersucht werden.

Ausgehend von diesem Grundgedanken findet sich in der Literatur zur Cybersicherheit das Modell der **Herdenimmunität**.[216] Cybersicherheit wird in diesem Modell mit der öffentlichen Gesundheit verglichen: Den Mechanismen der Cybersicherheit eines Netzwerks entspricht der Seuchenschutz einer Population. Der individuelle Grundschutz in Form von Impfungen ist notwendig, um die Population vor dem großflächigen Ausbruch von Seuchen zu bewahren. Bei bestimmten Infektionskrankheiten gibt es eine kritische Grenze, die nach Erreichen der Schwelle die Ausbreitung der Krankheit verhindert.

Dieser Analogie folgend könnten Schwellenwerte für ein festgelegtes Cybersicherheitsniveau errechnet werden und entsprechende Vorgaben gemacht werden, um Ausbreitungsschäden zu minimieren. Bei hohen Schutzleistungen der kritischen Masse kann Cybersicherheit (als Sicherheit der Netzwerke) eine positive Netzwerkexternalität darstellen. Ein Netzwerk mit geringen Schutzleistungen dagegen stellt eine negative Netzwerkexternalität dar.

Die von Eneken Tikk aufgestellte "*Duty of Care Rule*“ (Sorgfaltspflichtregel) besagt, dass jeder die Verantwortung hat, ein angemessenes Sicherheitsniveau in seiner Informationsstruktur umzusetzen.[217] Diese Regel wird aufgrund fehlender wirtschaftlicher Anreize bislang oft nicht berücksichtigt. Es gelten ähnliche Grundsätze für die Cybersicherheit wie für die öffentliche Gesundheit. Obwohl nicht kongruent, lassen sich Parallelen zwischen den Risiken einer Infektion mit Krankheitserregern und der nachfolgenden Ausbreitung von Epidemien einerseits, und der Infektion mit Computerviren mit anschließender Proliferation in Netzwerken andererseits ziehen. Insofern kann ein verbindlicher Sicherheitsstandard

[216] Vgl. Mulligan und Schneider 2011; Sales 2012.
[217] Vgl. Tikk 2011, S. 125.

im IKT-Sektor ebenso wie eine Impfpflicht im Gesundheitssektor eingeführt werden. Beide, Standard und Pflicht, sollen die Ausbreitung verhindern.

Während die unmittelbare Umgebung eines Individuums durch den *spill-over*-Effekt geschützt ist, wird die Bevölkerung durch eine große Masse geimpfter Menschen geschützt (Herdenimmunität). Bei den meisten Krankheiten trägt die kritische Masse von etwa 85 Prozent[218] geimpfter Menschen dazu bei, das Risiko einer unkontrollierten Verbreitung zu minimieren. Ein ähnlicher Ansatz könnte im Bereich der Cybersicherheit verfolgt werden, um das Sicherheitsniveau in verschiedenen lokalen oder gar globalen Netzwerken zu verbessern (ganzheitlicher Ansatz).[219] Hierbei kann es sich auch um eine lokale Herdenimmunität handeln, bei der sich einzelne Mitglieder des Netzwerks (bspw. Rechner in einem Konzern) infizieren können, ohne dass dies lokal zu einem Befall einer größeren Anzahl anderer Mitglieder führen würde. Grundsätzlich gilt: je höher die IT-Sicherheit (analog zur Impfung) der einzelnen Netzwerkmitglieder, desto höher ist die Netzwerk- bzw. Cybersicherheit.

Wie im Gesundheitswesen erfordert diese Sicherheit in einem Netzwerk eine Form der Überwachung. Institutionen wie das Robert Koch Institut (Bundesinstitut für Infektionskrankheiten) können ähnlich wie eine Kontroll- und Überwachungsstelle handeln, um die Einhaltung der Meldepflichten zu überwachen und im Notfall die Isolation und Quarantäne durchzuführen. Ein Schritt in diese Richtung wurde auf EU-Ebene mit der Richtlinie zur Netzwerk- und Informationssicherheit (NIS-Richtlinie) sowie der Ausweitung des Meldewesens für kritische Infrastrukturen und der Stärkung der Agentur der Europäischen Union für Cybersicherheit (ENISA), bereits unternommen. Auf nationaler Ebene ist das BSI für die zivile IT-Sicherheit verantwortlich.

[218] Vgl. Sales 2012, S. 1540.

[219] Es handelt sich hierbei um generelle Überlegungen zur Verbesserung des Cybersicherheitsniveaus, die bisher wenig erforscht sind. Die kritische Masse der Herdenimmunität im Bereich der Cybersicherheit ist nach wie vor Gegenstand der Forschung. Dabei ist wichtig zu betrachten, welche technischen und politischen Maßnahmen realisierbar sind, sowie zwischen lokalen und globalen Handlungsmöglichkeiten zu unterscheiden.

4 *Enabler*- und *Driver*-Analyse im Lichte von Innovation und Wachstum

Im Folgenden soll die Bedeutung von Cybersicherheit für deutsche Unternehmen im Allgemeinen und deutsche IT-Sicherheitsunternehmen im Besonderen analysiert werden. In der *Enabler*-Perspektive ist eine hinreichende Cybersicherheit Voraussetzung für Unternehmen, erfolgreich die Digitalisierung ihrer Wertschöpfungskette (i.e. Industrie 4.0) vorzunehmen. Cybersicherheit und die Anbieter von technischen Lösungen und Dienstleistungen ermöglichen eine erfolgreiche Digitalisierung, indem sensitive Daten und Produktionsprozesse vor den Bedrohungen im Cyberraum geschützt werden.

Cybersicherheit ist ein fast weltweit wachsender Markt. Anbieter von technischen Lösungen (Hardware und Software) sowie von Dienstleistungen (inkl. Instrumenten zum Risikomanagement -z.B. Cyberversicherungen und Bildungseinrichtungen) wachsen deutlich stärker, als die Volkswirtschaft im Durchschnitt. Dies ist auch in Deutschland der Fall. Auffallend ist aber, dass wenige auf Cybersicherheit spezialisierte und international tätige Unternehmen aus Deutschland kommen. Ein Indiz hierfür kann sein, dass kaum deutsche Unternehmen in den auf Cybersicherheit spezialisierten Investmentfonds in relevanter Größe vertreten sind.[220] Gelänge es, deutschen Unternehmen aus dem Bereich der IT-Sicherheit einen größeren Marktanteil im In- und Ausland zu erlangen, dann würden diese selbst einen größeren Beitrag zum volkswirtschaftlichen Wachstum beitragen. Sie würden damit selbst zum Treiber (*Driver*) des Wirtschaftswachstums.

4.1 *Enabler*-Analyse im Lichte von Innovation und Wachstum

In dieser Studie wird Cybersicherheit im Lichte von Innovation und Wachstum analysiert. In der *Enabler*-Perspektive richtet sich damit der Blick auf Schutzguteigentümer, die Innovationskraft besitzen. Dabei soll der Innovationsbegriff mit seinen unterschiedlichen Reichweiten verstanden werden. In einem engeren, technischen Sinne bezieht er sich auf *Intellectual Property* (IP, geistiges Eigentum) und damit gerade auch auf Unternehmen, die selbst FuE betreiben. In einem weiteren Sinne bezieht er sich auf die innovative Idee, auf denen das Kerngeschäft eines Unternehmens beruht und die nicht notwendigerweise eng technisch gefasst ist. In der *Cyberdomain* gilt es also genau wie in der "realen" Welt das zu schützen, was den spezifischen Wettbewerbsvorteil eines bestimmten Unternehmens ausmacht.

Unterschiedliche empirische Kennzahlen bietet etwa das Mannheimer Innovationspanel: Innovationsausgaben, Innovationsintensität, Innovationserfolg, Anzahl der Unternehmen mit kontinuierlicher FuE, und Innovatorenquote. Zentral darunter ist die Innovationsintensität, bei der die Innovationsausgaben am Umsatz gemessen werden.

[220] Vgl. ETFMG 2019.

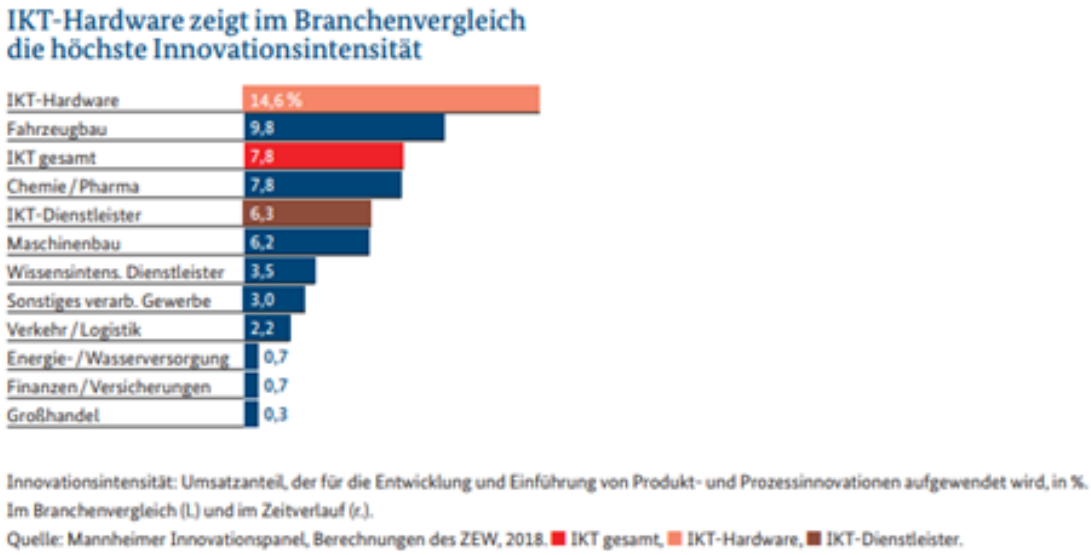


Abbildung 23 Innovationsintensität nach Branche
Quelle: Mannheimer Innovationspanel.

Demnach sind die Branchen Fahrzeugbau, Informations- und Kommunikationstechnologie und Chemie/ Pharma besonders innovationsintensiv. Gleicht man Zahlen zu Cyberangriffen der unterschiedlichen Branchen ab, so lässt sich feststellen, dass die genannten drei Branchen jeweils einem erhöhten Bedrohungsniveau ausgesetzt sind. So wurde in der jüngsten Bitkom-Studie den Branchen Chemie/ Pharma und dem Automobilbau, die umfangreichste Betroffenheit durch Cyberangriffe bescheinigt.

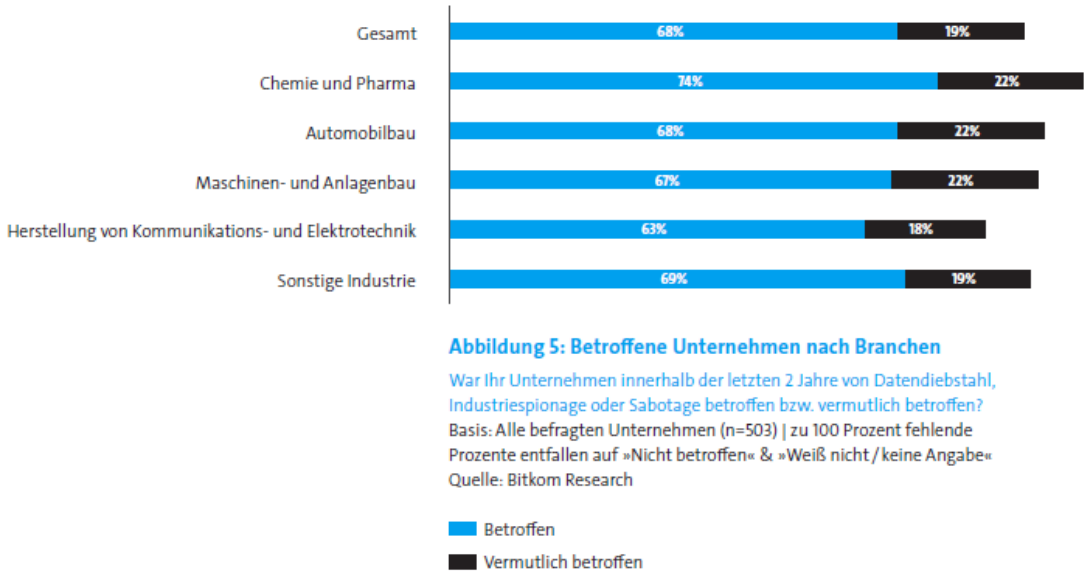


Abbildung 24 Betroffene Unternehmen nach Branchen
Quelle: Bitkom 2018a, S. 17.

Die Informations- und Kommunikationstechnik (IKT) ist Teil der sog. Kritischen Infrastruktur. Daher besteht hier bei Angriffen und besonderen Vorkommnissen eine Meldepflicht beim BSI. Die Meldungen wurden dort im Lagebericht den Branchen zugeordnet. Dabei ergibt sich ein Bild wie in Abbildung 25.

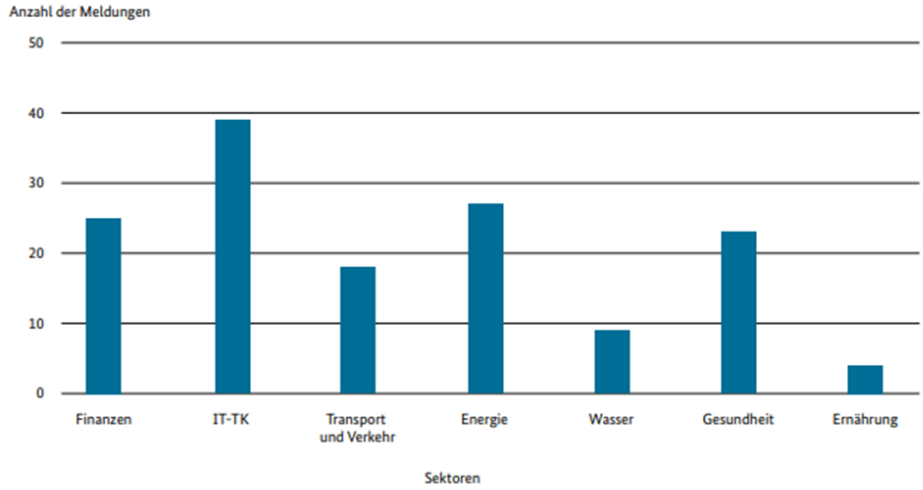


Abbildung 02 Meldeaufkommen von KRITIS-Betreibern (freiwillige und verpflichtende Meldungen nach § 8b BSIG) im Berichtszeitraum vom 01.06.2017 bis 31.05.2018

Abbildung 25 Meldeaufkommen von KRITIS-Betreibern
Quelle: BSI 2018.

Demnach ist die Informationstechnologie und Telekommunikation (IKT) mit knapp 40 Meldungen im Berichtszeitraum der relativ höchsten Anzahl an (in erster Linie meldepflichtigen) Angriffen ausgesetzt.

Eine im Zusammenhang mit der Herausforderung der Cybersicherheit relevante Unterscheidung ist die zwischen großen Unternehmen einerseits und kleinen und mittelständischen Unternehmen (KMU) andererseits. Dabei ist Großunternehmen eine etwas größere Innovationskraft zuzurechnen. Jedenfalls weisen Großunternehmen (>250 MA) eine höhere Innovatorenquote (67,7 Prozent) auf als kleine und mittelständische Unternehmen (KMU) mit 35 Prozent.[221] Ferner geben Großunternehmen mehr Geld (138,9 Mrd. EUR, 2017) für Innovationen aus, bspw. für eine interne, kontinuierlich arbeitend FuE-Abteilung, als KMU (27,9 Mrd. EUR).[222] Schließlich halten 40,8 Prozent der Großunternehmen eine kontinuierlich arbeitende FuE-Abteilung vor, gegenüber lediglich 9,9 Prozent bei den KMU.[223]

Wie aber ist die Situation im Bereich von Digitalisierung und Cybersicherheit? Hier zeigt die Bitkom-Studie 2018 interessante Ergebnisse. Zunächst einmal ergeben die Umfragen, dass gerade mittelgroße

[221] Vgl. ZEW 2018, S. 6.
[222] Vgl. Ebd., S. 5.
[223] Vgl. Ebd., S. 6.

Unternehmen das Ziel von Angreifern sind.[224] Sowohl kleinere als auch große Unternehmen waren in geringerem Ausmaß von Angriffen betroffen.

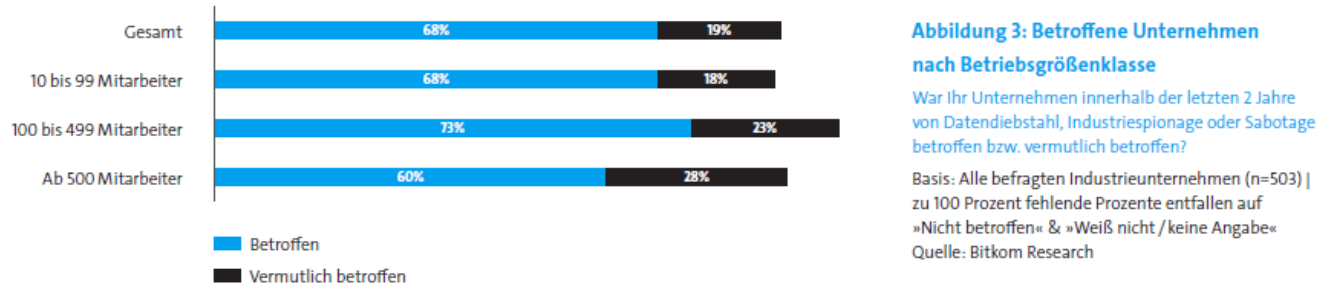


Abbildung 26 Betroffene Unternehmen nach Betriebsgrößenklassen
Quelle: Bitkom 2018a, S. 14.

Weiterhin wurde in der Bitkom Studie 2018 nach dem Grad der Digitalisierung im jeweiligen Unternehmen gefragt. Hier wurde deutlich, dass kleine Unternehmen den geringsten, mittelgroße Unternehmen einen mittleren, und große Unternehmen einen hohen Grad an Digitalisierung aufweisen.

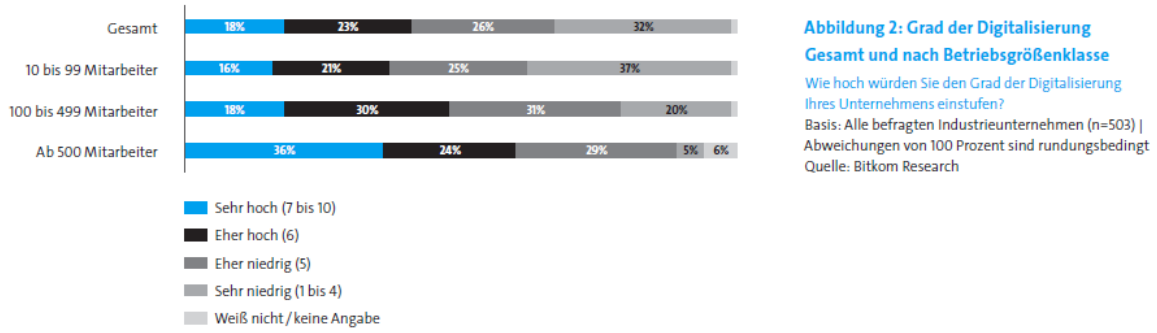


Abbildung 27 Grad der Digitalisierung – gesamt und nach Betriebsgrößenklasse
Quelle: Bitkom 2018a, S. 11.

Unternehmen mittlerer Größe liegen bei der Digitalisierung auf mittlerem, bei den Angriffen aber auf dem höchsten Niveau. Eine mögliche Erklärung wäre, dass im Zusammenspiel von Digitalisierung eine Art Kuznets-Kurven-Effekt vorliegt.[225]

[224] Vgl. Abbildung 26.
[225] Vgl. Abbildung 28.

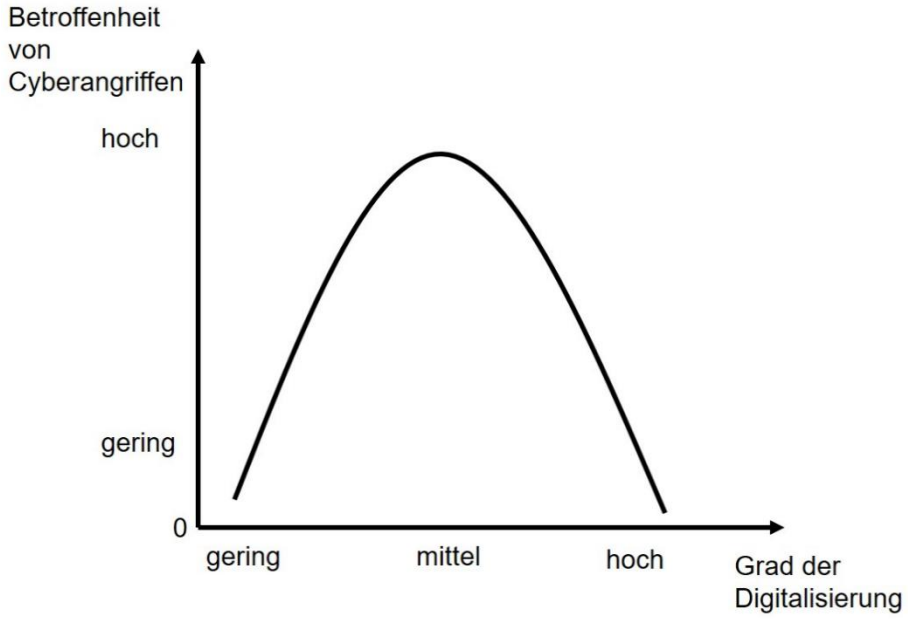


Abbildung 28 Kuznets-Kurve beim Zusammenhang von Digitalisierungsgrad und Betroffenheit von Cyberangriffen
Quelle: Eigene Darstellung in Anlehnung an die vom Ökonomen Simon Kuznets in den 1950er-Jahren formulierte hypothetische Kurve zum Zusammenhang ökonomischer Ungleichheit und Pro-Kopf-Einkommen.

Die Hypothese lautet, dass man in zweierlei Weise vor Cyberangriffen relativ geschützt ist. Entweder ist der Digitalisierungsgrad der Wertschöpfungskette gering, und damit ist es auch die Angriffsfläche bzw. der anzurichtende Schaden. Oder aber die Digitalisierung der Wertschöpfungskette ist fortgeschritten, und damit einhergehend sind es auch die Kompetenzen und Instrumente zum Schutz der digitalen Systeme. Eine hohe Gefährdung ergibt sich dazwischen, wenn Unternehmen zwar schon einzelne Glieder ihrer Wertschöpfungskette digitalisiert haben, das Bewusstsein für die damit einhergehende Bedrohung und die Fähigkeiten zum Schutz jedoch noch wenig ausgeprägt sind. Hier böte sich ein politischer Ansatzpunkt, Hilfestellung mit dem Ziel zu geben, dass Digitalisierung der Produktion und Cyberschutz sich komplementär und parallel in angemessenem Tempo miteinander fortentwickeln.[226]

Dabei gilt es auch zu berücksichtigen, dass, wie in allen Bereichen der Digitalisierung, **Cyberschutzleistungen in hohem Maße mit Skaleneffekten verbunden** sind. Die relativen Kosten des Schutzes nehmen also mit der Unternehmensgröße ab. Die finanzielle Hürde für kleine und mittelständische Unternehmen, in einen adäquaten Cyberschutz zu investieren und entsprechende Kompetenzen im Unternehmen aufzubauen oder extern durch Dienstleister einzukaufen, ist also ungleich höher als für große Unternehmen.

[226] Vgl. *security by design* und *security by default*

Für einen Organisationsbereich oder Geschäftsprozess eingekaufte bzw. entwickelte und eingerichtete Cyberschutzleistungen lassen sich zu geringen Grenzkosten auf andere Bereiche und Prozesse ausweiten, da innerhalb des Unternehmens regelmäßig nur überschaubare Anpassungen notwendig sein werden. Der finanzielle Mehraufwand ist also klein, die zusätzliche Schutzwirkung für das Unternehmen als Ganzes dagegen groß. Daher profitieren große Unternehmen – mit vielen Abteilungen und Geschäftsprozessen – relativ in stärkerem Ausmaß von solchen Investitionen als KMU.

Das mittelgroße Unternehmen offenbar besonders Cyberangriffen ausgesetzt sind, kann aber auch eine andere Ursache haben. So formuliert Bitkom: „Der Mittelstand in Deutschland ist besonders innovativ und stark in die Lieferketten von großen Konzernen eingebunden. Insofern liegt es nahe, dass es Angreifer zum einen auf das Spezialwissen der KMU abgesehen haben. Und zum anderen KMU als Einfallstore nutzen, um an die Daten großer Konzerne zu kommen. In der Regel schützen sich Großkonzerne besser.“[227] Dabei sahen Interviewpartner in der Expertenbefragung Handlungsbedarf für KMU: „Bei Industriespionage als relevante Gefahr ist die beste Option für das Unternehmen in IT-Sicherheit zu investieren, um Innovationsfähigkeit und Wettbewerbsfähigkeit langfristig zu sichern.“[228] Entsprechend muss es im vitalen Interesse der großen Unternehmen sein, dass bei ihren Zulieferern (i.d.R. KMU, auf deren Absatzmärkten sich die großen Unternehmen befinden) ein ausreichendes Maß an Schutz gegeben ist.

Große Unternehmen unterhalten heute in der Regel eine IT- oder gar eine IT-Sicherheitsabteilung, und betreiben erheblichen Aufwand zum Schutz ihrer Daten, Informationen und Prozesse. Anders sieht es oft bei mittleren und kleineren Unternehmen aus. So formulierte ein Gesprächspartner im Rahmen der Expertenbefragung das Grundproblem: „Cybersicherheit ist sehr ressourcenaufwendig.“ Neben vergleichsweise geringeren Ressourcen sind dafür möglicherweise vor allem auch Informationsdefizite ursächlich, die tendenziell nur in großen Unternehmen mit dem entsprechenden Ressourceneinsatz behoben werden (können).

Informationsdefizite können Unternehmen daran hindern, die Bedrohungslage richtig einzuschätzen. Eine Gefahr, die nicht erkannt wird, kann in aller Regel auch schlecht gebannt werden. Informationsdefizite anderer Art können aber selbst bei qualitativ und quantitativ zutreffender Einschätzung der Bedrohung die Investition in einen effektiven Schutz be- oder verhindern. Wenn nämlich die Qualität der Angebote von Unternehmen aus der Gruppe der *Driver* aufgrund unsichtbarer Qualität und technischer Komplexität nicht eingeschätzt werden kann, unterbleibt die Investition entweder ganz (da sie intern

[227] Bitkom 2018a, S.14.

[228] Interview 5, Experte.

nicht belastbar gerechtfertigt werden kann), oder es werden tendenziell minderwertige (zu wenige/ zu schlechte) Produkte und Dienstleistungen beschafft.[229]

Ebenfalls eine Rolle spielen **positive externe Effekte**, die KMU in stärkerem Maße von Investitionen in eigene Schutzmaßnahmen absehen lassen als Großunternehmen. Schließlich fällt der positive externe Effekt mit zunehmender Unternehmensgröße relativ immer weniger ins Gewicht. Eher ist zu erwarten, dass stattdessen KMU aufgrund einer geringeren Ausnutzung von **Skaleneffekten** sowie geringerer unternehmensinterner Synergieeffekte leichtfertiger eine Trittbrettfahrer-Rolle einnehmen werden. Sie werden dies in der Hoffnung tun, dass einerseits die von Großunternehmen und Behörden ergriffenen Schutz- und Gegenmaßnahmen die KMU ohne Kostenbeteiligung indirekt ebenfalls vor Schaden bewahren, sowie dass andererseits eine ausreichend große Zahl anderer Unternehmen durch ihre Schutzmaßnahmen bereits einen Herdenimmunisierungseffekt schaffen.

Die Annahme, dass das eigene KMU im Vergleich zu Großunternehmen aufgrund der größenbedingt geringeren Anzahl an Schnittstellen zur Außenwelt und der geringeren Bekanntheit eine geringere Angriffsfläche böte, sowie aufgrund vergleichsweise geringerer Umsatzzahlen insgesamt ein weniger attraktives Ziel für Cyberkriminelle darstellen müsste, trägt das ihre dazu bei, dass Unternehmen kleinerer und mittlerer Größe ihren Schutz vor Cyberbedrohungen vernachlässigen. Wirtschaftspolitische Aktivitäten müssen also darauf abzielen, die hier beschriebenen Gründe für Marktversagen abzustellen oder auszugleichen. Darüber hinaus gibt es keinen Grund anzunehmen, dass es nicht im wohlverstandenen Eigeninteresse eines Unternehmens läge, seinen Wettbewerbsvorteil auch in der digitalen Welt hinreichend zu schützen, wie sie es in der analogen Welt ehedem tun.

Allerdings gibt es Grund zur Annahme, dass externe Effekte und Unternehmensgröße zukünftig beim Schutz vor Cyberangriffen eine geringe Rolle spielen werden. Neue **Plattformlösungen**, wie sie zum Beispiel von der Deutschen Telekom angeboten werden, sorgen mit einem quasi automatisierten und anonymen Wissenstransfer zwischen Unternehmen dafür, dass Lehren aus dem Schaden eines Kunden der Plattform nahezu in Echtzeit auch den anderen Kunden zu Gute kommen. Die Internalisierung der externen Effekte wird hier zum Geschäftsmodell des Cybersicherheitsanbieters, während KMU von Skaleneffekten profitieren, von denen sonst nur größere Unternehmen profitieren könnten. Aus Wettbewerbssicht besteht hier allerdings die Gefahr von *lock-in*-Effekten, die sich aufgrund hoher Wechselkosten für die Kunden ergeben.

[229] Vgl. das Konzept des *Market for Lemons*, Akerlof 1970, in Kapitel 3.1.3.

4.1.1 Beratungsangebote

Bereits heute gibt es Angebote des Staates, mit deren Hilfe insbesondere KMU einen Anreiz erhalten sollen, sich dem Thema Cybersicherheit stärker zu widmen. Die Kosten hierfür werden daher zumindest teilweise durch den Steuerzahler übernommen.

Das BMWi fördert z.B. mit den beiden Beratungsangeboten *go-Inno* und *go-digital* die Zusammenarbeit von KMU mit anderen Unternehmen und Forschungseinrichtungen, um erfolgsversprechende Innovationen bei Markteintritt zu unterstützen.[230] Die Programme zielen darauf ab, eine bessere Vernetzung in Innovationsnetzwerken und Clustern (siehe auch das Förderprogramm go-cluster) zu ermöglichen und die digitale Markterschließung sowie digitalisierte Geschäftsprozesse, in Einklang mit der IT-Sicherheit, voranzutreiben. Der Fokus der Förderung soll sich zunehmend auf die Stärkung der IT-/Cybersicherheit richten (erhöhter Zuschuss, wenn Investitionen in IT-Sicherheit erfolgen), da s*ecurity-by-design* nicht als staatliche Zwangsmaßnahme verstanden werden soll, sondern als ein Wettbewerbsvorteil (Wirkung sowohl auf *Enabler* als auch *Driver*-Ebene).[231]

Die Transferstelle *IT-Sicherheit in der Wirtschaft* soll zudem zukünftig für Unternehmen Unterstützungsangebote bündeln, Informationen und Handlungsempfehlungen verständlich und praxisnah aufbereiten, das Auffinden der passenden Angebote erleichtern und über *best practice* - Beispiele aus den mittelständischen Unternehmen konkrete Handlungsmöglichkeiten der breiten mittelständischen Wirtschaft bekannt machen.[232]

[230] Vgl. BMWi 2019b.

[231] Vgl. https://www.innovation-beratung-foerderung.de/INNO/Navigation/DE/go-digital/go-digital.html

[232] Aussagen des BMWi auf Anfrage zu den Förderprogrammen IT-Sicherheit in der Wirtschaft.

4.1.2 Standardisierung

Ein wichtiges Instrument Informationsdefizite für Unternehmen bei der Beschaffung adäquater IT-Sicherheitstechnik und Dienstleistung zu helfen, Informationskosten zu senken, sind die Einführung/Nutzung von Standards und Normen.

Normungsorganisationen wie das Deutsche Institut für Normung sind offiziell anerkannte Organisationen, die sich den Grundprinzipien der Normung – Unabhängigkeit von Einzelinteressen, Freiwilligkeit der Anwendung, Konsens, Kohärenz, Transparenz, Offenheit und Effizienz - verschrieben haben.[233] Das Institut hat in diesem Zusammenhang einen Staatsvertrag mit der Bundesrepublik Deutschland unterzeichnet und ist verpflichtet, Standards im Sinne des Gemeinwohls zu etablieren.

International werden Standards von der Vereinigung der Normungsorganisationen, der Internationalen Organisation für Normung (*International Organization for Standardization* - ISO), in allen Bereichen außer Elektrik, Elektronik und verwandte Technologien, die von der *International Electrotechnical Commission* (IEC), sowie Telekommunikation, die von der *International Telecommunication Union* (ITU) behandelt werden, erarbeitet.[234] Zur Stärkung der Standardisierungssysteme der drei Organisationen, wurde 2001 die *World Standards Cooperation* (WSC) gegründet. Die WSC soll die Umsetzung internationaler, auf Konsens basierender Standards, weltweit fördern. Das Europäische Komitee für Normung (*Comité Européen de Normalisation* - CEN) ist der Dachverband der nationalen Normungsorganisationen auf europäischer Ebene.

Standardisierungsorganisationen können von verschiedenen Interessengruppen gegründet werden und unterscheiden sich hinsichtlich ihrer Entscheidungsfindungsprozesse, der Transparenz und der Führung/Steuerung.[235] Standards haben vielfältige ökonomische Auswirkungen, die sich auch auf Innovationen auswirken. Sie können zum einen durch konsensuale Verhandlungen durch Unternehmen und interessierten Stakeholdern in einem fakulativen Prozess innerhalb von Standardisierungsorganisationen erreicht werden (marktgetriebener Prozess) oder durch staatliche Regulierung (top-down).[236] Sie sind Teil der technologischen Infrastruktur, die den Pfad subsequentieller Innovationen beeinflussen und bestimmen kann.

Standards können auf Innovationen wirken, indem sie Wissen einem breiteren Publikum zugänglich machen. Nach anfänglichen Implementierungsschwierigkeiten können insbesondere KMU von *best*

[233] Vgl. WTO 2000.
[234] Vgl. ISO Structure and Governance, https://www.iso.org.
[235] Vgl. Kleinhans 2018, S. 15.
[236] Vgl. Blind et al. 2017, S. 250.

practices und Lösungen auf dem Stand der Technik profitieren, da sie aufgrund zusätzlicher Entwicklungs- und Produktionskosten oft nicht in der Lage sind, verschiedene Anwendungen zu unterstützen.[237] Darüber hinaus kann der Einsatz verschiedener Systeme zu einer Kaufzurückhaltung der Verbraucher führen, die in Erwartung einer sich durchsetzenden Technologieinfrastruktur, den Kauf innovativer Produkte verschieben.[238]

Standards können jedoch auch in die andere Richtung wirken, indem sie den am Standardisierungsprozess beteiligten Unternehmen einen Wettbewerbsvorteil verschaffen. In einem heterogenen Markt mit unterschiedlichen technologischen Standards kann – abgesehen von Preis und Qualität der Produkte – die Implementierung von regulierenden (staatlichen) Standards dazu führen, dass sich Teile der Industrie durch auf die Standardsetzung einwirkende Lobbyarbeit einen Wettbewerbsvorteil verschaffen.[239] Dies kann zu Markteintritts-Hemmnissen (Mangel an qualifiziertem Personal und Kapital zur Umsetzung) führen und somit Innovationen durch andere Unternehmen verhindern.[240]

Standards können zudem für mehr Kohärenz sorgen, indem sie die Vielfalt der Möglichkeiten des Handelns sinnvoll einschränken. Dadurch können Ressourcen stärker gebündelt werden, was Innovationen zur notwendigen kritischen Masse verhelfen kann. Kompatibilitätsstandards sorgen für Interoperabilität und bilden die Grundlage, um komplementäre Produkte und Netzwerkeffekte zu etablieren. Sie können auch ein Qualitäts- oder ein Sicherheitsniveau festlegen und dadurch helfen, externe Effekte zu internalisieren.

Sicherheitsstandards

Sicherheitsstandards helfen, bei Fällen asymmetrischer Informationsverteilung zumindest ein Mindestmaß an Sicherheitsqualität sichtbar zu machen.

---

[237] Vgl. BMWi 2012, S. 52.

[238] Vgl. Blind et al. 2017, S. 251.

[239] Ebd. S. 258.

[240] In einem Markt mit einem hohen Grad an Unsicherheit (hohe Konkurrenz, Komplexität der Technologien, volatiles Kundenverhalten), charakterisiert durch ein instabiles und sich schnell veränderndes technisches Umfeld in dem unterschiedliche technologische Entwicklungen miteinander konkurrieren, kann staatliche Regulierung die Innovationskraft (gekennzeichnet durch das Verhältnis zwischen Input und Output; Unternehmen mit weniger Input - Menge der Ressourcen/Innovationsausgaben - für ein bestimmtes Output - erfolgreiche Einführung eines Produkts - sind effizienter) von Unternehmen stärker beeinträchtigen als ein marktgetriebener Standardisierungsprozess. Dies kann vor allem daran liegen, dass zwischen staatlichen Regulierern und Marktakteuren, eine Informationsasymmetrie besteht. Ein Standardisierungsprozess von Marktakteuren würde, dieser Logik folgend, geringere Konformitäts- und Innovationskosten verursachen als der top-down Ansatz von staatlichen Regulierern, in einem heterogenen Markt miteinander konkurrierender Technologien.

Sicherheitsstandards müssen für digitale Produkte konzeptionell verstanden werden: Sie sollten vor allem leistungsbezogen und auf die Lebensdauer eines Produktes zugeschnitten sein. Die ISO 27000 und insbesondere ISO 27001 Reihe hat einen anerkannten Standard zur Informations- und IT-Sicherheit in den Unternehmen geschaffen.[241]

Zertifikate dienen in erster Linie der Senkung einer bestimmten Art von Transaktionskosten, nämlich der von Informationskosten. Sie kennzeichnen Produkte und Dienstleistungen, die eine bestimmte (Mindest-)Qualität aufweisen. Dies ist dann von Bedeutung, wenn diese Qualität nicht ohne weiteres anhand anderer Merkmale zu erkennen ist, und somit die Kauf- und Zahlungsbereitschaftsentscheidung potenzieller Kunden erschwert wird. Nicht nur für individuelle Käufer, sondern gleich für ganze Märkte relevant ist dieses Transparenzproblem, wenn es zu Konzentrationen von Angebot und Nachfrage im Niedrigqualitäts-Segment führt.

Wie Akerlof bereits 1970 unter dem Begriff *Market for Lemons*[242] anhand des Beispiels des Gebrauchtwagenmarktes mit windigen Händlern beschreibt, kann derartige – im Bereich von Cyberschutz-Produkten und -Dienstleistungen der Cybersicherheit systematisch abträgliche – Intransparenz dazu führen, dass selbst Käufer mit einer eigentlich höheren Zahlungsbereitschaft, keine Angebote höherer Qualität mehr finden und kaufen können. Dieses Problem kann durch sogenanntes *signaling* behoben werden, in diesem Zusammenhang also einer vertrauenswürdigen Signalgabe durch ein Zertifikat bzgl. der Qualität dessen, was der Cyberschutz-Bedürftige zu erwerben gedenkt.

Aktuelle Entwicklungen

Die Deutsche Organisation für Normung hat 2017 eine Normungs-*Roadmap* herausgegeben, die verschiedene Branchen illustriert, in denen IT-Sicherheitsstandards erarbeitet werden: Industrie 4.0/ *Smart Factory*, *eMobility*, *eHealth*, *Smart Grid* und *Smart Home*.[243]

Insbesondere vor dem Hintergrund einer allgegenwärtigen Digitalisierung werden in zahlreichen Gremien Standards erarbeitet, die auch IoT-Geräte miteinschließen sollen. Eine Grundsatzfrage im aktuellen Standardisierungsprozess ist der potentielle Zielkonflikt zwischen Sicherheit und Benutzerfreundlich-

[241] Vgl. ISO 27001, https://www.iso.org/standard/54534.html
[242] Vgl. Akerlof 1970.
[243] Vgl. DIN/DKE Roadmap 2017.

keit (*usability)*. Bei zu geringer Nutzerfreundlichkeit, so ist zu befürchten, werden sich bestimmte Innovationen nicht durchsetzen können. Hier betont die Normungs-*Roadmap*, dass ein Ausgleich zwischen beiden Aspekten gefunden werden muss.

Von grundsätzlicher Natur ist das Problem, dass zunehmende Vernetzung bei Gleichförmigkeit der Systeme – trotz wünschenswerter und angestrebter Effizienzgewinne – jedoch auch zu einer Erhöhung der Anfälligkeit für Cyberrisiken führt. Problematisch ist, dass sich die oben genannten Standardisierungsgremien an verschiedenen sektoralen Lösungen abarbeiten, aber kein allgemeiner und grundsätzlicher IoT-Standard erarbeitet wird, der übergeordnet existiert.

4.2 *Driver*-Analyse im Lichte von Innovation und Wachstum

Im vorangegangenen Abschnitt wurde das Augenmerk auf die *Enabler*-Perspektive sowie die Entfaltungsmöglichkeiten der Innovationskraft der Schutzguteigentümer gerichtet. Im Folgenden soll die sogenannte *Driver*-Perspektive betrachtet werden. Also jenen Unternehmen, die selbst Produkte und Dienstleistungen zum Schutz vor Cyberbedrohungen anbieten und im Wettbewerb um Marktanteile und Gewinn versuchen, mit innovativen Angeboten erfolgreich zu sein. Durch ihre Geschäftstätigkeit tragen sie zum allgemeinen Wirtschaftswachstum bei. Konkret stellen sie die Cybersicherheitsprodukte und -dienstleistungen her, die sie als Schutzleistungen an andere Unternehmen – die somit zur gestörten Wahrnehmung ihrer eigenen Geschäftstätigkeit befähigt (*enabled*) werden – verkaufen. Aber auch staatliche Abnehmer sowie Privatleute gehören zum Kundenkreis.

Die Branche Cybersicherheit gehört in Deutschland, trotz überdurchschnittlichen Wachstums[244] einer starken IT-Wirtschaft, bislang nicht zu den in absoluten Zahlen – Umsatz und Beschäftigtenzahlen – wirtschaftlich wirklich bedeutenden. WifOR gibt für 2017 die Bruttowertschöpfung der IT-Sicherheitswirtschaft mit 15,5 Milliarden Euro[245] sowie die Beschäftigtenzahl als Näherungswert mit knapp 160.000 Erwerbstätigen[246] an. Bisweilen ist es schwierig, die IT-Sicherheitswirtschaft von anderen Bereichen der IT-Wirtschaft abzugrenzen. Betrachtet man die IT-Wirtschaft als Ganzes, liegt die Bruttowertschöpfung noch erheblich höher. So schreiben Weber et al.: ”*Therefore, the German ICT sector was able to increase its gross value added to €108bn – an increase of 4 % compared to the previous year. This shows that ICT is leaving traditional industrial sectors, such as mechanical engineering or the chemical and pharmaceutical industry, trailing far behind.”*[247]

Insbesondere im internationalen Vergleich fällt auf, dass trotz des überdurchschnittlichen Wachstums offenbar noch Entwicklungspotenzial besteht, wie auch mehrfach aus der Expertenbefragung hervorgeht.[248] Länder wie Israel, die Vereinigten Staaten und Großbritannien bspw. haben schon früh eine Standortpolitik betrieben, die die Privatwirtschaft, akademische Einrichtungen und Institutionen, staatliche Einrichtungen und in Teilen auch das Militär zusammenbringt, um ein Ökosystem zu schaffen, das Innovationen fördert und fordert.[249] Für die Wirtschaftspolitik stellt sich daher die Frage, was sie dazu beitragen kann, das Wachstum dieser Branche noch weiter zu erhöhen. Umso mehr, als das eine leistungsfähige (nationale) IT-Sicherheitswirtschaft auch eine sicherheitspolitische Komponente hat. Damit

[244] Vgl. Stuchtey und Rieckmann 2018, S.56.
[245] Vgl. WifOR 2019b, S. 15.
[246] Ebd. S. 26.
[247] Weber et al. 2018, S. 3.
[248] Interview 1, Verband; Interview 12, Driver international.
[249] Vgl. dazu auch den Abschnitt zu Clusterbildung.

stellt sich die Frage: Wie kann diese Branche mit möglichst geringen Eingriffen noch wettbewerbsfähiger gemacht werden – und was sind wirksame, aber möglichst schonende Eingriffe in den Markt?

Grundvoraussetzung und Bedingung *sine qua non* für eine innovations- und wachstumsfähige IT-Sicherheitswirtschaft ist ein ausreichendes Angebot von **Humankapital**. Diese muss derzeit als ein limitierender Faktor für das Branchenwachstum in der Bundesrepublik angesehen werden, wie im Rahmen der Expertenbefragung mehrfach deutlich wurde (rund 91 Prozent der Experten sind der Meinung, dass der Mangel an qualifizierten Arbeitskräften ein erhebliches Hemmnis für die Digitalisierung von Geschäftsprozessen, und rund 77 Prozent für das Wachstum der deutschen IT-Sicherheitswirtschaft ist[250]). Wie anhand der Entwicklung der Einstiegs- und Wechselgehälter von auf Cybersicherheit spezialisierten Programmierern und Entwicklern erahnt werden kann, hat eine Erhöhung der Nachfrage nach Personal ohne ausreichende gleichzeitige Erhöhung der Anzahl ausgebildeter Fachkräfte und Absolventen von spezialisierten Studiengängen einen mittelfristig wachstumsdämpfenden Effekt auf die Unternehmen der Branche.[251]

Auch staatliche Arbeitgeber stehen hier vor zunehmend gravierenden Schwierigkeiten – hier nicht, weil der Gewinn durchwachsende Personalkosten geschmälert wird, sondern weil sie in der Effektivität ihrer Aufgabenerfüllung beeinträchtigt werden. Staatliche Institutionen stehen hier im Wettbewerb um qualifiziertes Personal mit der häufig besser bezahlenden Privatwirtschaft, was zu zunehmenden Schwierigkeiten bei der Personalgewinnung führt. Behörden konkurrieren zusehends untereinander um ausreichend motiviertes Personal. Tendenziell werden im Sinne einer Auslese die vergleichsweise stärker sicherheitsorientierten und weniger innovativen Mitarbeiter die schlechter bezahlten, aber sicheren Stellen im Staatsdienst vorziehen.[252]

Ohne zunächst oder zumindest parallel das Problem der zu geringen Verfügbarkeit von Humankapital an der Wurzel zu packen, erscheint es für die Zielerreichung – Förderung von Innovation und Wachstum – also wenig sinnvoll, durch anderweitige staatliche Maßnahmen weiter das Wachstum in der Branche anzufeuern. Ein stärkeres Wachstum der Cybersicherheitsbranche würde unweigerlich eine erhöhte Nachfrage nach entsprechend qualifiziertem Humankapital nach sich ziehen. Bei einem zumindest kurz-

[250] Vgl. Kapitel 5.

[251] Vgl. u.a. Sawall 2019; Ilg 2019.

[252] Mit dem aktuellen Besoldungsstrukturenmodernisierungsgesetz soll hier über Prämien-Programme und zeitlich begrenzte Gehaltszuschüsse eine Attraktivitätsoffensive geführt werden. So erläuterte Bundesinnenminister Horst Seehofer (CSU): "Mit der Reform machen wir den Bund als Dienstherrn noch attraktiver: Mehr Geld für Anwärter, moderne Personalgewinnung und attraktive Zulagen sind nur einige Stichworte aus dem Maßnahmenpaket" (Haack, 2019).

fristig unelastischen Angebot käme es also nur zu einem *crowding out* auf dem Arbeitsmarkt entsprechend qualifizierten Personals. Von daher sind sowohl im akademischen wie auch im Bereich der beruflichen Bildung Anstrengungen von Hochschulen und anderen Ausbildungsstädten notwendig, mehr qualifiziertes Personal in diesem Bereich zu locken. Steigende Gehälter helfen hierbei, aber mindestens genauso notwendig ist ein wachsendes Angebot an Studien-und Ausbildungsplätzen sowie einer geistigen Bereitschaft junger Menschen, eine Karriere in diesem Bereich zu suchen.[253]

Die IT-Sicherheitsforschung[254] und **Forschungsförderung** im Cybersicherheitsbereich kann dazu beitragen, die Knappheit an Humankapital zu lindern. Und auch die mehrjährige Tätigkeit in Forschungseinrichtungen (wie einem der Fraunhofer-, Max Planck- oder Helmholtz-Zentren, dem Hasso-Plattner-Institut, politiknahen Forschungs- und Beratungsinstituten etc.), kann durch *learning by doing* und *training on the job* Kompetenzen für spätere Verwendungen auch bei solchen Mitarbeitern hervorbringen, die vorher etwa als Geistes- und Sozialwissenschaftler mit dem Thema Cybersicherheit kaum Berührungspunkte hatten.

Förderung insbesondere in der Grundlagenforschung erzeugt überdies positive externe Effekte. So konstatiert Fritsch[255], dass „(…) Erkenntnisse der Grundlagenforschung nach geltendem Recht nicht patentierbar sind (…).“ Er fährt fort: „Jedes Unternehmen, das (auf irgendeine Weise) in den Besitz von Ergebnissen der Grundlagenforschung gelangt, darf dieses Wissen für seine Zwecke einsetzen, ohne einen Beitrag zu den entsprechenden Kosten der Grundlagenforschung leisten zu müssen.“ Während es aus volkswirtschaftlicher Sicht zunächst wünschenswert erscheint, diese Effekte zu internalisieren (und die Unternehmen an den Kosten zu beteiligen), ist die angesprochene Wirkung aus Sektor- und Unternehmenssicht erfreulich. Die Cybersicherheitsbranche profitiert davon, und dies auch im Bereich der angewandten Forschung, insofern die Ergebnisse veröffentlich werden, was bei steuerfinanzierten nationalen und europäischen Förderprogrammen die Regel ist.

Verbesserungspotenzial besteht nach Aussage von Industrie- und Verbandsvertretern bei der Überführung von Forschungsergebnissen in marktnahe Produkte. Die fehlenden Anreize, Forschungsergebnisse national geförderter Projekte in marktreife Produkte zu entwickeln, wurden mehrfach in den Expertenbefragungen kritisiert.[256] Hier besteht dringend Handlungsbedarf. So schreibt der Vorstandsvorsitzende

[253] Interview 6 und 7, Verband; vgl. Kapitel 5.

[254] Tatsächlich existieren zahlreiche Förderprogramme und -Projekte. Bereits im Jahr 2011 stand die Intensivierung der IT-Sicherheitsforschung auf der Agenda des Bundesinnenministeriums, so beispielsweise betont durch den IT-Direktor BMI Schallbruch (https://www.youtube.com/watch?v=cbyg5dhmJ0s, Minute 36, zuletzt abgerufen 14.08.2019).

[255] Vgl. Fritsch 2014, S. 82 f.

[256] Interview 2, 4, 5, 7, Experte; Interview 2, Regulierer; Interview 4, staatliche Stelle; Interview 9, Driver.

des ASW Bundesverbandes[257] zur Erhöhung der Wirksamkeit von Forschungsausgaben: „Die Forschungsförderung im Bereich der Cyberabwehr führte bisher nicht zu konkreten Produktionsentwicklungen, die eine entsprechende Marktverbreitung in Deutschland erreichen konnten. Hier könnte sich Deutschland an Israel orientieren, wo die staatliche Förderung von Start-ups zentraler Bestandteil des Regierungsprogramms ist. Das BMI könnte sich wiederum an den Aktivitäten des BMVg zur zivilen Sicherheitsforschung orientieren. Positiv und weiter ausbaufähig sind die Entwicklungen der Cybersicherheitshubs in Berlin, München, Bonn und Darmstadt."

Trotz dieser Kritik, die Möglichkeiten für die zivile IT-Sicherheitsforschung sind in Deutschland recht ausgeprägt. Gerade KMU finden an Hochschulen und außeruniversitären Forschungseinrichtungen zahlreiche wissenschaftliche Partner, mit denen gemeinsam die Entwicklung von Sicherheitslösungen vorangetrieben werden können. Darüber hinaus dienen verschiedene Plattformen dazu, bei der Vernetzung von Forschungs- und Innovationsaktivitäten national wie auch international gezielt zu unterstützen.

Auf Bundesebene stehen Programme zur Finanzierung innovativer Projektideen bereit. Zusätzlich zu dem bereits bestehenden Sicherheitsforschungsprogramm[258] (*BMBF-Sifo*) hat das BMBF ein eigenes IT-Sicherheitsforschungsprogramm[259] aufgelegt. Regelmäßig werden hier Ausschreibungen für Projektideen in hinreichend weit gefassten Themengebieten aus dem Bereich der IT-Sicherheit veröffentlicht. Die Programmsäule „Schutz kritischer Infrastrukturen" findet sich bspw. in beiden benannten Förderprogrammen wieder. Dies hängt mit dem cyber-physischen Charakter des Themenspektrums zusammen und verdeutlicht, dass eine interdisziplinäre wie auch interinstitutionelle Herangehensweise unerlässlich ist.

Forschungsverbünde aus Wissenschaftseinrichtungen, Unternehmen und Anwendern können sich im Rahmen eines zweistufigen Bewerbungsprozesses (1. Projektskizze, 2. Vollantrag) um eine Förderung bewerben. Die grundsätzliche Entscheidung über die Förderfähigkeit eines Projektes wird hier auf der Grundlage einer ca. 25-seitigen Projektskizze getroffen. Ein übergreifendes Ziel solcher Verbundprojekte ist eine unternehmerische Verwertung der Forschungsergebnisse. Im Rahmen dieser Programme

[257] Vgl. Wagner 2018, S. 76.

[258] Das nationale Rahmenprogramm "Forschung für die zivile Sicherheit" ist in drei Säulen gegliedert: Schutz und Rettung von Menschen, Schutz Kritischer Infrastrukturen, Schutz vor Kriminalität und Terrorismus.

[259] Der offizielle Name des Programms lautet: Forschungsrahmenprogramm der Bundesregierung zur IT-Sicherheit „Selbstbestimmt und sicher in der digitalen Welt 2015 bis 2020".

soll eben nicht (nur) Grundlagenforschung betrieben, sondern vielmehr konkrete Lösungen für Anwender entwickelt werden. Nationale Programme ermöglichen in der Regel nur eine Förderung bis zu einem Technologiereifegrad[260] von TRL 5.

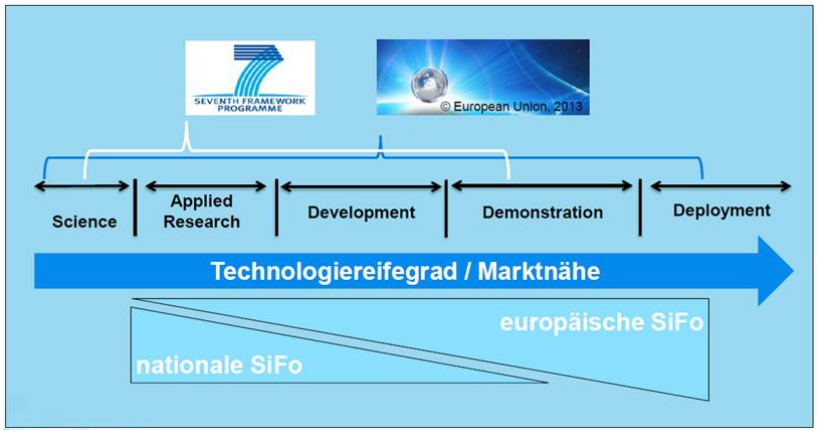


Abbildung 29 Nationale und europäische Sicherheitsforschung im Vergleich
Quelle: Nationale Kontaktstelle (NKS) für Sicherheitsforschung des BMBF.

Im Rahmen des Horizont 2020[261] Förderbereichs "Sichere Gesellschaften" handelt es sich bei den Ausschreibungen[262] meist um Forschungs- und Innovationsmaßnahmen (*Research and Innovation action*, RIA)[263] oder Innovationsmaßnahmen (*Innovation Action*, IA)[264]. Letzteres bezweckt die Erarbeitung von Plänen, Konzepten und Vorkehrungen für neue, verbesserte Produkte, Verfahren oder Dienstleistungen.[265] Allein der Prozess der geeigneten Partnerfindung für die Entwicklung eines europäischen Forschungsprojekts stellt Initiatoren einer Idee vor besondere Herausforderungen. Damit verbunden ist das Beantragungsverfahren deutlich aufwändiger und einstufig ausgelegt – d.h. von vornherein muss der Vollantrag gestellt werden, auf dessen Basis über eine Förderung entschieden wird. Die Vollanträge haben regelmäßig einen Umfang von mehr als 100 Seiten und sind von Beginn an in größeren Konsortien

[260] Das *Technology Readiness Level* (TRL) beschreibt die Entwicklungsstufe einer Technologie, eines Verfahrens oder einer Dienstleistung. In *Horizont 2020* wird der TRL vornehmlich in marktorientierten Ausschreibungsthemen verwendet. Ziel ist es, nur Produkte, Dienstleistungen und Verfahren zu fördern, die bei Projektstart bereits einen bestimmten TRL erreicht haben, bzw. bei Projektende erreichen werden.

[261] Eine Fortführung ist im Rahmen von *Horizont Europa* vorgesehen.

[262] Zu den Schwerpunkten zählen u.a. der Schutz und Stärkung der Widerstandsfähigkeit kritischer Infrastrukturen, Versorgungsketten und Verkehrsträger; die Verbesserung der Computer- und Netzsicherheit; Gewährleistung der Privatsphäre und der Freiheit, auch im Internet, sowie ein besseres Verständnis der gesellschaftlichen, rechtlichen und ethischen Zusammenhänge in Bezug auf alle Teilbereiche von Sicherheit, Risiko und Gefahrenabwehr; und Förderung der Normung und der Interoperabilität der Systeme, auch für Notfälle.

[263] Die Förderquote für Forschungs- und Innovationsmaßnahmen beträgt 100 Prozent.

[264] Die Förderquote für Innovationsmaßnahme beträgt grundsätzlich 70 Prozent. Gemeinnützige (non-profit) Einrichtungen erhalten auch hier eine Förderquote von 100 Prozent.

[265] Vgl. Tabelle 5.

von nicht selten über zehn Konsortialpartnern (aus mind. drei europäischen Mitgliedsstaaten oder assoziierten Ländern) abzustimmen und zu erstellen.

Die Erfolgschancen bei den europäischen Sicherheitsforschungsprogrammen (Secure Society, Digital Society) sind deutlich geringer als in den deutschen Programmen, d.h. liegen aktuell bei einer Erfolgsquote von 16,3 Prozent.[266] Daher ist es nicht verwunderlich, dass deutsche Antragsteller regelmäßig davor zurückschrecken, die Koordinatorenrolle einzunehmen. Auch sind deutsche Antragsteller hier relativ unterrepräsentiert, was nicht zuletzt auch an den vergleichsweise komfortablen nationalen Förderbedingungen liegen dürfte. Im Rahmen der europäischen Sicherheitsforschung können aufgrund anderer Beihilferegeln Projekte bis zu einem TRL 9, d.h. bis kurz vor der Marktaufnahme unterstützen.

Ziel-TRL		**Level**	**Bedeutung**
	Innovation Action	TRL 9	Eigentliches System hat sich in operativer Umgebung bewährt
		TRL 8	System vollständig und qualifiziert
Research and Innovation Action		TRL 7	System-Prototyp in operativer Umgebung demonstriert
		TRL 6	Technologie in einer relevanten Umgebung demonstriert
		TRL 5	Technologie in einer relevanten Umgebung validiert
		TRL 4	Technologie unter Laborbedingungen validiert
		TRL 3	Experimentelle Nachweisbarkeit der Anwendbarkeit
		TRL 2	Beschreibung des technologischen Konzepts
		TRL 1	Beobachtung des Funktionsprinzips

Tabelle 5 Technologiereifegrad
Quelle: Eigene Darstellung, in Anlehnung an NKS-KMU Nationale Kontaktstelle zum EU-Programm Horizont 2020.

[266] Vgl. BMBF 2019b, S. 5. Ergebnisse der Aufrufe aus dem Jahr 2018 im Bereich Sichere Gesellschaften des europäischen Forschungsprogramms Horizont 2020.

Zusammenfassend kann man feststellen, dass die deutschen Förderprogramme im Beantragungsprozess im Vergleich mit dem europäischen Programm weniger aufwendig sind und die Förderwahrscheinlichkeit höher liegt. In den europäischen Programmen kann die Entwicklung einer IT-Sicherheitslösung dagegen weiter in Richtung Marktreife im Rahmen eines Forschungsförderprojekts vorangetrieben werden. Wenn man also erst einmal eine europäische Förderung erlangt hat, dann macht es diese leichter, eine marktfähige Lösung zu entwickeln. Das zu durchreitende Tal des Todes (*valley of death*) für Innovationen ist mit einer deutschen Förderung länger.

Eine anderweitige Maßnahme kann im Bereich der **staatlichen Beschaffung** von Produkten und Dienstleistungen aus dem Bereich Cybersicherheit gesehen werden. Ziel ist eine Erhöhung der Gesamtnachfrage (*c.p.*, also unter Vermeidung etwaiger Verdrängungs-Effekte, sowie mit möglichst gering ausfallender marktverzerrender Wirkung). Erreicht werden soll mittelbar eine Verlagerung der Lernkurve innerhalb der Unternehmen der Branche auf ein gesellschaftlich effizientes Niveau, sowie Skaleneffekte innerhalb der Unternehmen. In Deutschland fehlt es den Unternehmen der Branche oft an einer kritischen Größe. So stellt WifOR in seiner Studie fest: „Die vorherrschende Stellung übernehmen mit 89,3 Prozent die kleinen Unternehmen mit bis zu 9 sozialversicherungspflichtigen Beschäftigten",[267] um im internationalen Vergleich wettbewerbsfähig zu sein. Ungeachtet der beachtlichen *Start-up*-Szene gibt es nur wenige Unternehmen[268] in Deutschland, die in diesem Punkt vergleichbar mit den bekanntesten internationalen Wettbewerbern beispielsweise aus den Vereinigten Staaten sind. Europäische Staaten, u.a. auch Deutschland, versuchen bisher erfolglos das amerikanische Modell zu replizieren, was auch daran scheitert, dass Unternehmen auf dem Heimatmarkt keine kritische Größe erreichen, Skaleneffekte ausbleiben und somit nicht mit amerikanischen und anderen Anbietern konkurrieren können.[269]

Eine überzeugende Kritik, die in den Experteninterviews und auch im Rahmen des vom BIGS durchgeführten Workshops mit IT-Sicherheitsexperten geäußert wurde, bezieht sich auf den **Umfang von Ausschreibungen** im Bereich der IT-Sicherheitsdienstleistungen. Das Volumen der ausgeschriebenen Personentage sei so hoch, dass nur die wenigen internationalen großen Beratungsgesellschaften (die sog. *big four*: PwC, EY, KPMG, Deloitte) solche Aufträge schultern könnten. Damit deutsche Anbieter hier zum Zuge kommen und wachsen können, sollten die Losgrößen verkleinert werden.

[267] WifOR 2019b, S. 14.
[268] Beispiele für Ausnahmen im Sinne einer unvollständigen und nicht wertenden Aufzählung wären die Deutsche Telekom AG, die Rohde & Schwarz GmbH & Co. KG sowie SAP SE.
[269] Interview 12, Driver International.

Die Auftragsgröße ist nicht nur bei IT-Dienstleistungen ein Problem. Auch bei der Beschaffung von Systemlösungen im Cybersicherheitsbereich hat die eher mittelständisch strukturierte Cybersicherheitsbranche Probleme, konkurrenzfähige Angebote abzugeben. Internationale Großunternehmen haben hier einen Vorteil, auch ohne dass die von ihnen angebotenen Lösungen technisch einer denkbaren inländischen Variante überlegen wären. Warum es also in der Konsequenz auf dem deutschen Markt nicht zu einer **Konsolidierung** kommt, wurde im Rahmen dieser Studie nicht tiefer untersucht. Vereinzelt wird von Brancheninsidern die Vermutung geäußert, dies könne daran liegen, dass es sich häufig um eigentümergeführte Unternehmen handele. Eine andere Erklärung ist die hohe bestehende Profitabilität, die keinen Veränderungsdruck erzeuge.

Natürlich wäre es denkbar, dass sich KMU für Großprojekte zu Bietergemeinschaften zusammenschlössen. Wie auch in anderen Bereichen der Sicherheitswirtschaft fehlt es in Deutschland aber an einem **Systemintegrator**, der die notwendige Abstimmung und Koordinierung vornimmt, ohne dass dabei zu hohe Transaktionskosten anfallen.

Während es bei der Unternehmensgröße zunächst keine kurzfristig wirksamen direkten Ansatzpunkte für staatliches Handeln gibt, könnte jedoch beispielsweise die Übernahme der Rolle des **Systemintegrators** durch eine deutsche Institution staatlicherseits inzentiviert werden. Dieser könnt dann bei großen Ausschreibungsverfahren, an denen sich ansonsten und bislang nur große, internationale Cybersicherheitsunternehmen beteiligen konnten, gezielt kleine und mittlere Unternehmen zu konkurrenz- und leistungsfähigen Konsortien zusammenführen.

In den BIGS-Experteninterviews wurde immer wieder bemängelt, dass der Staat selbst es aufgrund seiner **Beschaffungspolitik** den Anbietern innovativer Lösungen schwermache, zu einem Markterfolg zu kommen. Regelmäßig würden Produkte mit speziellen Eigenschaften nachgefragt – und nicht die Lösung eines Problems, wodurch eben auch innovative Ideen zum Einsatz kommen könnten. Zudem werde im Zweifel immer das billigste Angebot den Zuschlag bekommen und nicht hinreichend Innovationsgrad und Lösungserreichung bei der Auftragsvergabe berücksichtigt.[270] Damit vertue der Staat selbst die Chance, innovative Cybersicherheitslösungen in den Markt zu ziehen. Dabei wäre es gerade für einheimische Anbieter wichtig, deutsche Behörden als bereits gewonnene **Schlüsselkunden** im internationalen Wettbewerb präsentieren zu können. Wer es eben geschafft hat, seine Lösung an das BSI oder das KdoCIR zu verkaufen, dem fällt es leichter, auch Dritte von seinem Angebot zu überzeugen.

[270] Interview 1, 4, 10, Experte; Interview 3 und 6, Verband; Interview 6 und 9, Driver; Interview 8, Staatliche Stelle schriftlich.

Die Kritik an der wenig innovationsfreundlichen Beschaffung öffentlicher Auftraggeber ist nicht spezifisch für den Bereich der Cybersicherheit. Das BMWi hat daher schon vor geraumer Zeit ein Kompetenzzentrum für innovative Beschaffung eingerichtet, dass es staatlichen Einrichtungen erleichtern soll, von Standardausschreibungen abzuweichen. Offensichtlich wird von diesem Angebot bislang bei der öffentlichen Beschaffung von IT-SP und -Dienstleistungen noch unzureichend Gebrauch gemacht. Hier scheinen noch Anstrengungen insbesondere der politischen Leitung notwendig zu sein, diesen alternativen Beschaffungswegen zum Durchbruch zu verhelfen.

Gerade im Hochsicherheitsbereich bietet sich eine Beschaffung von Lösungen mithilfe der vorkommerziellen Auftragsvergabe (***Pre-Commercial Procurement*** – PCP) an. So formuliert auch das Bundeswirtschaftsministerium: „PCP ist kein Beschaffungsverfahren im eigentlichen Sinne, aber ein Instrument zur Förderung innovativer, effizienter und nachhaltiger öffentlicher Leistungserbringung.“[271] Bei diesem Verfahren begleitet der öffentliche Auftraggeber die Entwicklung einer Lösung, um sicherzustellen, dass diese genau seinen Anforderungen entspricht. Diese Lösung wird dann am Ende auch ohne weitere Ausschreibung beschafft. Dieses Beschaffungsverfahren kommt insbesondere im Rahmen von Horizont 2020- Förderungen zum Einsatz.

Diese spezifische **Änderung des Nachfrageverhaltens** des Staates, nämlich eine verstärkte und gezielte Nutzung der Instrumente der innovativen Beschaffung, kann einen bedeutenden Anreiz für Unternehmen darstellen, in bestimmten Innovations- und Entwicklungsvorhaben überhaupt erst Ressourcen zu investieren. Solche Programme der Industriepolitik können der Überbrückung des v*alley of death* zwischen Entwicklung und Vermarktung von Produkten und Dienstleistungen dienen, wie auch aus einigen Expertenbefragungen deutlich wurde.[272]

Vorsichtiger sollte aufgrund zu erwartender marktverzerrender Wirkungen allerdings mit der **Beeinflussung des Nachfrageverhaltens** auf (*Enabler*-)Unternehmensseite verfahren werden. Hier sollten nur Maßnahmen und Anreize in Frage kommen, die in gleicher Weise und möglichst gleichermaßen auf alle Unternehmen wirken. In Frage kommen hier Regulierungen zu Haftung und Versicherung, Normung, Zertifikate und Qualitätsstandards sowie Datenschutzrecht[273], jedoch auch Förder- und Finanzierungsprogramme.

[271] Vgl. BMWi 2017.

[272] Interview 3, 11, 13 (schriftlich) Driver; Interview 1 und 7, Verband.

[273] Vgl. hierzu auch ENISA (2018) in Bezug auf die Auswirkungen der europäischen Datenschutz-Grundverordnung: “*It may be argued that fear of punishment of itself is the driver for more care in the design of processing but it might offer an economic incentive to minimize the risk.*”

Bezüglich der Schaffung von günstigen **Rahmenbedingungen** im Sinne eines innovations- und wachstumsfreundlichen Ökosystems für Cybersicherheitsunternehmen lassen sich bisherige Ansätze weiter optimieren. Hier erscheint es sinnvoll, im Sinne von „Stärken stärken" mehr als bisher auf die Förderung bereits in Grundzügen vorhandener Wettbewerbs- und Standortvorteile abzustellen. So sind nach Aussage der vom BIGS befragter Experten in den Technologiefeldern **Kryptologie, Künstliche Intelligenz** sowie **Blockchain**, im internationalen Vergleich, sehr wettbewerbsfähige Kompetenzen in der Bundesrepublik vorhanden.[274] Dennoch sind die in Frage kommenden Unternehmen in der Regel keine Marktführer in ihrem jeweiligen Segment. Eine gezielte Förderung von öffentlicher Forschung in diesen ehedem starken Feldern sowie der Einsatz innovativer Beschaffungsverfahren für die Schaffung von Referenzkunden könnten dazu beitragen, dass mehr deutsche Cybersicherheitsunternehmen in Einzelbereichen zur Weltspitze aufschließen oder diese bilden könnten.

Sektorübergreifend und zum **Markenkern "*Sicherheit Made in Germany*"** zugehörig kommt die Förderung grundrechtskonformer und vertrauenswürdiger Produkte und Dienstleistungen der Cybersicherheit in Frage. Angebotene Produkte (und Dienstleistungen) mit der glaubhaften Versicherung „ohne Hintertür für Sicherheitsbehörden", sind ein aus Sicht eines erheblichen und mutmaßlich wachsenden Anteils der Abnehmer von Cybersicherheitsprodukten ein kaufentscheidendes Qualitätskriterium. Eine solche Zusicherung könnte zukünftig zwar möglicherweise nicht als weltweites Alleinstellungsmerkmal, jedoch zumindest als maßgebliche Differenzierung von den Angeboten der derzeitigen Marktführer aus den bedeutenden Herstellerländern dienen. Insbesondere der Punkt **Datenschutz kann zu einem Wettbewerbsvorteil werden.**[275]

Während Unternehmen etwa aus Märkten wie China, Russland, aber auch den USA und Israel in punkto Vertraulichkeit und Datenschutz einen geringeren Vertrauensvorschuss bei den Nachfragern haben, gelten deutsche Hersteller als bislang in Bezug auf die Datensouveränität als vertrauenswürdig. **Das hohe Datenschutzniveau und die scheinbare Zurückhaltung der Sicherheitsbehörden sowie der Glaube an ordnungspolitische Grundsätze können gerade im Bereich der Sicherheitstechnik und Dienstleistungen beim internationalen Markterfolg helfen.** Dies setzt aber voraus, dass zum einen dieses Vertrauen gerechtfertigt ist und zum andern, dass deutsche Unternehmen ihre Produkte und Dienstleistungen im Ausland auch anbieten können. Dies wiederum setzt Reziprozität voraus, also ein Offenhaltung des deutschen Markts für Sicherheitsprodukte aus dem Ausland. Gerade bei digitalen Produkten spielt die **Marktgröße** aufgrund der hohen Skaleneffekte eine wesentliche Rolle beim Markterfolg.

[274] Interview 4, 8, staatliche Stelle; Interview 7, Verband; Interview 3, 9, 14, Driver.
[275] Interview 3 und 7, Verband; Interview 8, Experte.

Abstand sollte daher von Bestrebungen genommen werden, **Autarkie** über die gesamte Wertschöpfungskette zu erreichen.[276] Dies betrifft abgesehen von hochsensiblen Aspekten der nationalen Sicherheit insbesondere den Versuch einer durchgängigen nationalen oder europäischen Herstellung von Infrastrukturkomponenten (Hardware), insofern hier kein Wettbewerbsvorteil besteht. Da eine leistungsfähige digitale Infrastruktur Voraussetzung für viel andere Branchen und deren Wettbewerbserfolg ist, können zweitbeste nationale Lösungen einen hohen Preis nach sich ziehen. Protektionistischen Argumenten (verkleidet als sicherheitspolitische Notwendigkeit) sollte daher mit Vorsicht begegnet werden, nicht zuletzt, weil Wachstumsförderung im Bereich Cybersicherheit nur einen kleinen Teilbereich der Industrie- und Handelspolitik darstellt, und ein möglichst uneingeschränkter Waren- und Dienstleistungsverkehr ein übergeordnetes Ziel darstellt.

Stattdessen erscheint – auch aus Sicht der Unternehmen der Branche – die Vertiefung eines **einheitlichen europäischen Binnen- und** hier insbesondere **Nachfragermarktes** für Produkte und Dienstleistungen der Cybersicherheit erfolgsversprechend, wenn es darum geht, in einzelnen Bereichen der Cybersicherheitsbranche, innovative und international wettbewerbsfähige Unternehmen zu fördern. Beschaffungen staatlicher Stellen könnten europaweit einheitlicher als bislang ausgeschrieben und vergeben werden, um Skalen- und Synergieeffekte zu erzielen.[277]

Außerhalb der EU, der NATO und wenigen gleichgestellten Drittstaaten wird die Marktgröße für deutsche Unternehmen oftmals durch die **Exportkontrolle** beschnitten. Dies gilt auch für das NATO-Mitglied Türkei. Da dies bei ihrer internationalen Konkurrenz in der Regel nicht der Fall ist, bedeutet die *dual use* - Problematik bei vielen Cybersicherheitsprodukten einen Wettbewerbsnachteil für deutsche Unternehmen, der mit dem sicherheitspolitischen Nutzen abzuwägen ist.

Wenig sinnvoll erscheint zudem die im Cyberbereich oftmals künstlich erscheinende **Unterscheidung** zwischen **ziviler und militärischer Sicherheit**. Die westfälische Trennung zwischen innerer und äußerer Sicherheit an der Landesgrenze existiert in der Cyberdomäne kaum. Das macht potenziell jedes Sicherheitsprodukt im IT-Bereich zu einem *dual use* - Fall. Die Halbleiterplatte aus Deutschland kann natürlich auch in einem ausländischen Waffensystem verbaut werden, wie auch in einem Fernseher aus dem gleichen Staat. Bei einer strengen Auslegung der *dual use* - Problematik wäre die Marktgröße für deutsche Cyber Sicherheitsunternehmen auf die EU, die NATO- Mitgliedstaaten und sog. Drittstaaten beschränkt. Dies würde den Markterfolg im internationalen Wettbewerb gegen französische, amerikanische oder israelische Konkurrenten sehr schwer machen.

[276] Vgl. hierzu auch Stuchtey 2015, bzgl. von Fragen technologischer Souveränität.
[277] Interview 3, 6, Verband; Interview 11, Driver international.

Neben Regulierung, Marktkonsolidierung und -öffnung sowie den bereits angesprochenen Fördermöglichkeiten kommt im Rahmen der rechtlichen Möglichkeiten innerhalb der europäischen Union die Option einer gezielten Subventionspolitik oder beschleunigte Abschreibungsmöglichkeiten hinzu.[278]

Empirisch ist das Wachstum der IT-Sicherheitswirtschaft nur schwer nachzuverfolgen. Die Branche wird in vielen Untersuchungen entweder in die Sicherheitswirtschaft oder IT-Branche subsumiert. Auch fällt die definitorische Abgrenzung zwischen den Branchen, wie auch von Geschäftsaktivitäten innerhalb eines Unternehmens nicht leicht.

Abbildung 30[279] zeigt beobachtetes bzw. für das laufende Jahr erwartetes Umsatzwachstum derjenigen Bereiche der Sicherheitswirtschaft, die einen direkten Bezug zu IT, Digitalisierung und Elektronik haben, sowie der klassischen Sicherheitsdienstleistungen (wie bspw. Wachschutz) und der Gesamtwirtschaft in Deutschland. Letztere wird am realen Bruttoinlandsprodukt gemessen.

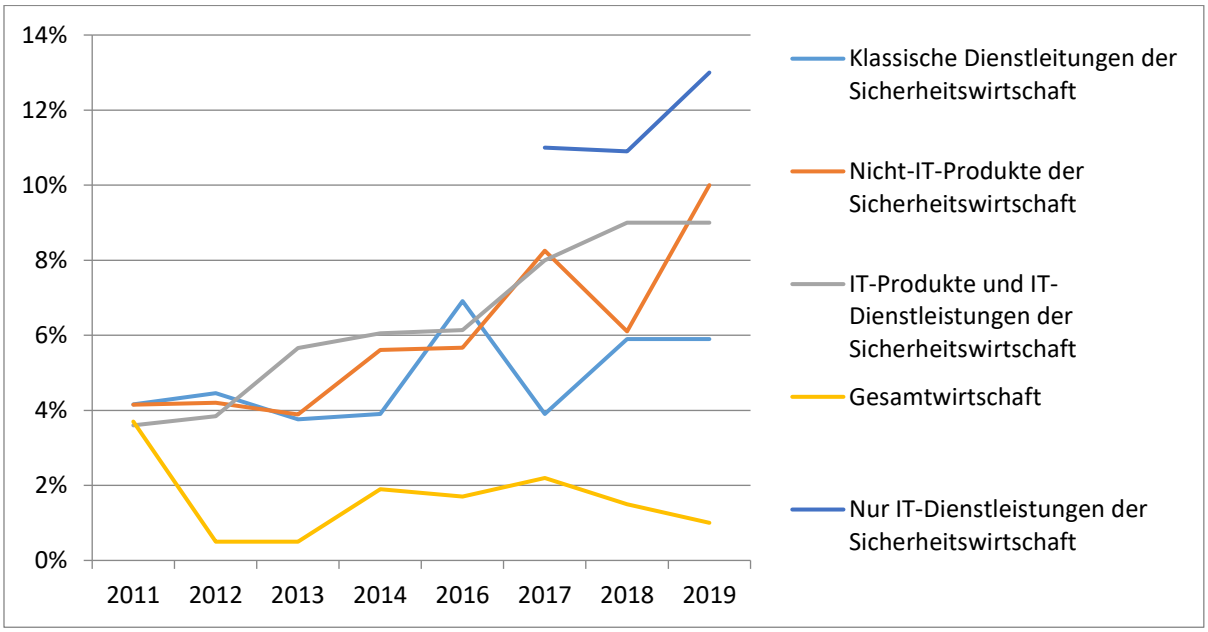


Abbildung 30 Angaben zu Wachstumsentwicklung und -erwartung bis 2019, nach Angebotsportfolio, im Vergleich zur Gesamtwirtschaft
Quelle: Eigene Darstellung.

Wie aus der Zeitreihe ersichtlich ist, wächst der Umsatz der Sicherheitswirtschaft mit Bezug zu Informationstechnologie (IT) und Digitalisierung inklusive elektronischer Nicht-IT-SP, seit Jahren deutlich

[278] Interview 2 und 4, Experte; Interview 3, 9, 11, Driver.
[279] Quelle: Fortgeschriebene Abbildung auf Basis von *Stuchtey, Rieckmann (2018) Die Vermessung der Sicherheitswirtschaft – Wachstum und Veränderung im Zeichen der Digitalisierung. In: Kompendium Sicherheit – Gesellschaft – Digitalisierung von Günter Calaminus (Hrsg.), TCC Verlagsgesellschaft, 2018,* S. 56 Abbildung 2. Zugrunde liegende Datenquellen: BIGS (2011-2017), Bitkom (2018a), Heuer (2018), ISG Information Services Group (2018), Security Essen (2018), Statista (2018), BMWi (2019b). Daten für die Kurve „Nur IT-Dienstleistungen der Sicherheitswirtschaft“ liegen nicht für die gesamte Zeitreihe vor.

stärker als das reale Bruttoinlandsprodukt. So wird deutlich, dass die Sicherheitswirtschaft ab dem Jahr 2011 in allen Bereichen deutlich überdurchschnittlich wächst. Das steile Umsatzwachstum der klassischen Sicherheitsdienstleistungen ab 2015 muss im Rückblick als Sondereffekt betrachtet werden, der maßgeblich auf die Flüchtlingskrise zurückzuführen ist. Nach einer Schrumpfung in 2017 ist hier mittlerweile eine Verstetigung zu beobachten.

Heute sind es vor allem die Bereiche der hauptsächlich elektronischen Sicherheitstechnik sowie der IT-Produkte und IT-Dienstleistungen, die das stärkste Umsatzwachstum vermelden. Für letztere werden in 2019 gar bis zu 13 Prozent Wachstum erwartet. Da allerdings für den Bereich der IT-Dienstleistungen der Sicherheitswirtschaft keine separaten Angaben verfügbar sind, können in der vorliegenden Zeitreihe nur Daten ab 2017 dargestellt werden.

Das aktuell starke Wachstum der „Nicht-IT"-Sicherheitsprodukte wird trotz ihrer Zuordnung stark durch elektronische Produkte getrieben, eine Trennung von solchen elektronischen sowie von IT-SP wird zunehmend schwierig und fragwürdig. In anderen Worten: Die Grenze zwischen elektronischer Nicht-IT-Sicherheitstechnik sowie IT-Sicherheitstechnik verschwimmt zusehends. Neben Brandmeldetechnik sind Zugangskontroll- und Überwachungssysteme unter den wachstumsstärksten Sicherheitstechniksparten, die auch von der derzeitig ausgeprägten Bautätigkeit und dem Trend zu "smarter" Gebäudetechnik profitieren. Deutlich wird unabhängig von der Zuordnung dieser technischen Grenzfälle eines: Der Markt für Produkte und Dienstleistungen der Sicherheitswirtschaft mit direktem Bezug zu Elektronik und/oder Informationstechnik wächst überdurchschnittlich und seit Jahren konsistent.

Qualitative Veränderungen in der Sicherheitswirtschaft sind zu großen Teilen auf technische Entwicklungen aus den Bereichen Elektronik und Informationstechnik zurückzuführen. Vereinfachend lassen sich diese in Komplementär- und Substitutionseffekte unterscheiden.[280] Ein Beispiel für einen Komplementäreffekt „wäre die Unterstützung der Sicherheitsfirma eines Shopping Centers durch „intelligente", auf Algorithmen basierende Videoanalyse z.B. im zugehörigen Parkhaus."[281] Um einen Substitutionseffekt hingegen handelte es sich, „wenn durch auf Algorithmen basierende Videoanalyse die Stelle des menschlichen Bildschirmbeobachters entfiele. Ein solcher Substitutionseffekt bedeutet eine Änderung der Kombination aus Inputfaktoren (Humankapital/Arbeit und Kapital /Technik) zur Produktion des gleichen Outputs. Arbeit wird teilweise und zusehends durch Kapital ersetzt."[282]

[280] Vgl. Stuchtey und Rieckmann 2018.
[281] Ebd. S. 45.
[282] Ebd.

Sowohl Komplementär- als auch Substitutionseffekte können dabei Effizienz- und Effektivitätsgewinne mit sich bringen und als Wachstumstreiber fungieren. Substitutionseffekte gehen mittelfristig allerdings auch mit einem negativen Beschäftigungseffekt einher, insofern es nicht gelingt, die frei werdenden Arbeitskräfte in anderer Funktion oder an anderer Stelle einzusetzen. Im Prinzip handelt es sich hier um schöpferische Zerstörung im Verständnis Schumpeters.[283] Beobachtet man die aktuelle Entwicklung der Sicherheitsdienstleistungsunternehmen, so fällt eine allmähliche Teilung in zwei Gruppen ins Auge. Die erste Gruppe hält an der Erbringung klassischer und wenig humankapitalintensiven Wachschutz- und Bestreifungs-Dienstleistungen fest, und zeichnet sich durch eine „vergleichsweise geringe Arbeitsproduktivität und Innovationskraft aus.“[284] Diese Gruppe wies im Rahmen der der Flüchtlingskrise 2015 ein erhöhtes Wachstum auf, stagniert allerdings seitdem bzw. verliert wieder an Bedeutung. Die zweite und wachsende Gruppe „passt sich den neuen technischen Möglichkeiten dahingehend an, dass sie nicht mehr primär Mann- oder besser Personenstunden verkaufen. Vielmehr werden vermehrt integrierte Sicherheitslösungen vermarktet. Ein ergebnisorientierter Ansatz tritt hier an die Stelle eines prozessorientierten.“[285]

Clusterbildung

Um die Bildung wettbewerbsfähiger Industrien und die gestiegene Produktion/Leistung einer bestimmten Region erklären zu können, hat sich ein Zweig der Entwicklungstheorie auf die positiven Einflüsse und Externalitäten der Agglomerationsökonomie konzentriert, die auch mit dem Begriff der Cluster bezeichnet wird. Dabei unterstützt die Konzentration von Unternehmen die Entwicklung regionaler Cluster (a) durch die Produktivitätssteigerung durch den hohen Informationsaustausch und *knowledge spillover* (jedes Unternehmen produziert mehr Einheiten *output* pro Einheit *input*) und (b) durch die Senkung der Investitionskosten wie Kapital, qualifizierte Arbeitskräfte und Technologien (Größenvorteile).[286]

Insofern unterscheidet sich die Cybersicherheitsbranche nicht von anderen Sektoren, wenn es darum geht, erfolgreiche Beispiele der Cluster Bildung anzuwenden. Die Open-Source Bewegung und die starken Tendenzen der Informationsteilung, die auf die 1960er Jahre zurückgehen, sollten bei einer Betrachtung jedoch nicht außer Acht gelassen werden.[287] Dabei spielt Vertrauen eine besondere Rolle, die sich häufig erst über persönliche Beziehungen entwickelt. Es scheint als würde der hohe Grad an Vernetzung

[283] Vgl. Schumpeter 1912, S. 157.
[284] Stuchtey und Rieckmann 2018, S. 45.
[285] Ebd. S. 45 f.
[286] Vgl. Porter 1985; und Porter 2000.
[287] Vgl. Tozzi 2017.

und die Dezentralität sowie die Virtualität dazu führen, dass Akteure in der Cybersicherheitsbranche großen Wert auf den persönlichen Kontakt legen. Informationen die besonders relevant und kritisch sind, werden oftmals privat zwischen Cybersicherheitsexperten ausgetauscht, zu denen man eine vertrauenswürdige Beziehung aufgebaut hat.[288] Die Bedeutung der geografischen Lage bzw. räumlichen Nähe zwischen diesen Akteuren, insbesondere beim Aufbau vertrauenswürdiger Beziehungen, die sich zu starken Partnerschaften, einem intensiven Informationsaustausch und einem wesentlichen Wissenstransfer entwickeln sollen, sollte nicht unterschätzt werden.

Für eine interessante Tätigkeit mit guten Verdienstmöglichkeiten gibt es insofern bei vielen Menschen die Bereitschaft zur geographischen Mobilität. Aus der Forschung zu **Wirtschaftsclustern** ist bekannt, dass gerade die Ansammlung einer großen Menge an ähnlich qualifiziertem Personal Ansiedlung neuer Unternehmen in einem bestimmten Bereich wahrscheinlicher macht. Die Hürde für einen Jobwechsel sinkt, wenn dadurch kein Umzug für die gesamte Familie notwendig wird. Dies gilt umso mehr, wenn mehrere Personen in einem Haushalt erwerbstätig sind.

So zeigt sich dann auch in Abbildung 31, dass sich in Deutschland einige Regionen herausgebildet haben, in denen es zu einer Häufung von Unternehmen und Einrichtungen aus dem Bereich der IT-Sicherheit gekommen ist. Im Umfeld großer und erfolgreicher Forschungseinrichtungen siedeln sich Unternehmen an oder gründen sich direkt aus den Wissenschaftseinrichtungen aus. Von daher spricht viel dafür, dass sich innovative Institutionen im Umfeld eines solchen Clusters ansiedeln, um es Talenten einfach zu machen, ihnen beizutreten. Die Clusterbildung in Israel wurde im Rahmen der Expertenbefragung als ein Erfolgsfaktor für die dortige Cybersicherheitsbranche genannt.[289]

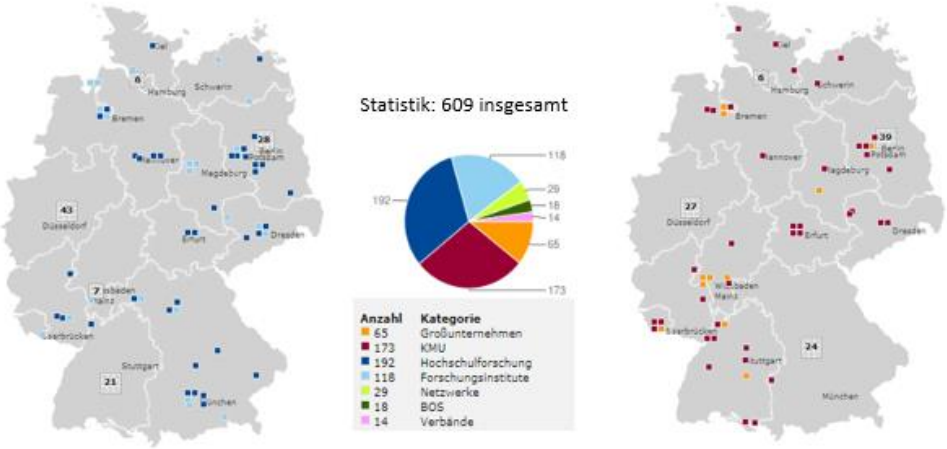
Aus dieser Perspektive erscheint daher eine Clusterförderung gegenüber einer Regionalförderung vorzugswürdig. Bei letzterer profitieren Innovation und Forschung nur als Beiprodukt einer primär auf Beschäftigungs- und Multiplikatoreffekte abzielenden Mittelallokation in strukturschwachen Regionen, und aufgrund fehlender Synergie- und Skaleneffekte weniger stark, als bei Förderung bestehender Cluster.

Die nachfolgende Abbildung zeigt, wo sich in Deutschland bereits gehäuft Unternehmen und Wissenschaftseinrichtungen aus dem Bereich Informations- und Kommunikationstechnik befinden. Wie diese Häufungen zu echten Clustern weiterentwickelt werden können, zeigen internationale Erfolgsmodelle.

[288] Vgl. Zhao und White 2017.
[289] Interview 3, Verband.

KMU (107) und Großunternehmen (40) (165)

Hochschulen (104) und Forschungsinstitute



Dem interaktiven Kompetenzatlas zur Sicherheitsforschung in Deutschland zufolge sind derzeit 349 der insgesamt 609 registrierten Institutionen in der Informations- und Kommunikationstechnik (IKT) aktiv. Darunter fallen die Anwendungs- und Technologiefelder Informationssicherheitstechnik und Cybersicherheit, Informationssysteme, Integrierte Plattformen, KI oder Robotik.

Abbildung 31 KMU/Großunternehmen und Hochschulforschung/Forschungsinstitute in der IKT im Vergleich
Quelle: BMBF (2019a) Kompetenzatlas zur Sicherheitsforschung in Deutschland, unter: www.securityresearchmap.de.

Die New America Studie *Cybersecurity as an Engine for Growth* hat sich drei Cluster angeschaut, die sich alle durch unterschiedliche Förderung und Konstellationen erfolgreich entwickelt haben.[290] Neben dem bekannten Be'er Scheva - Cluster in Israel betrachteten die Wissenschaftler die Stadtregionen Malvern im Vereinigten Königreich und San Antonio in den Vereinigten Staaten. Dabei stellten sie vier Merkmale heraus, die sich trotz der unterschiedlichen Zusammensetzung der Cluster für eine erfolgreiche Entwicklung gleichen und sich z.T. auch mit den Erkenntnissen aus den Experteninterviews decken:

1. **Die Präsenz von staatlichen Einrichtungen**, in diesem Falle von Cybersicherheits-Behörden, insbesondere von Militär und anderen Sicherheitsbehörden, fördert die Entwicklung einer Region aus zwei Gründen:
    a. Durch die Ausbildung/Fortbildung wird der lokalen Wirtschaft ein Talentpool zur Verfügung gestellt, auf das sie z.T. zurückgreifen kann.

[290] Vgl. Cohen et al. 2017.

b. Die Nähe zu Auftragnehmer ist für den öffentlichen Sektor tendenziell wichtiger als für den privaten Sektor. Das Wachstum lokaler Cluster kann dadurch gefördert werden, wobei sowohl etablierte Unternehmen als auch Start-ups davon profitieren können und sich Effekte letztlich auch auf den Privatsektor auswirken.

Die Kooperation von Unternehmen mit Behörden kann sich von der Projekt- hin zu einer strategischen Ebene entwickeln und dazu führen, dass technologische Entwicklungen nicht als Auftrag, sondern in Zusammenarbeit durchgeführt werden. Die geographische Nähe ermöglicht einen intensiveren Informationsaustausch und somit ein besseres Verständnis für Bedürfnisse, Probleme und zukünftige Entwicklungen.

2. **Universitäten/Hochschulen** spielen eine wichtige Rolle bei der Entwicklung eines lokalen Talentpools. Durch Kooperationsprogramme zwischen Cybersicherheitsunternehmen, den Behörden, Forschungseinrichtungen sowie Hochschulen, können duale (theoretische und praktische) Qualifikationen gefördert werden und regionalen Cluster ein Talentpool zur Verfügung stellen. Bildungsprogramme sollten dabei nicht nur auf akademische Bereiche beschränkt sein, sondern einen holistischen Ansatz verfolgen. Das Fundament dafür muss bereits im frühen schulischen Stadium gelegt werden.

3. **Technologietransferprogramme** sollten sowohl die Forschungsaktivitäten als auch die Monetarisierung von Technologieentwicklungen berücksichtigen. Studierende, Forscher und Unternehmen, gestützt von Behörden, sollten potenzielle Absatzmärkte in der Forschungspartnerschaft mit einbeziehen. In San Antonio z.B. hat die lokale Handelskammer einen Inkubator mit Vorständen bestehend aus lokalen Geschäftsleuten und Mitarbeitern der Handelskammer gegründet, der neu gegründete Cybersicherheitsunternehmen bei den ersten Schritten unterstützen soll und dabei hilft, langfristige Partnerschaften mit lokal ansässigen Einrichtungen aus dem Cybersicherheitsbereich zu entwickeln.[291] In diesem Milieu soll der Wissenstransfer erleichtert werden, wovon letztlich alle Beteiligten direkt profitieren.

4. **Fachkenntnisse von Entscheidungsträgern** (interdisziplinär) und eine starke Führungsrolle (unterschiedliche Stakeholder) sind von entscheidender Bedeutung, um finanzielle Mittel und Förderprogramme zielgerichtet einzusetzen, ein Bewusstsein für die Herausforderungen und

[291] Vgl. Petersen und Writer 2016.

Entwicklungen zu erzeugen und strategische Entscheidungen, die nicht nur kurzfristige Absichten verfolgen, treffen zu können. Dabei sind organisationsübergreifende Beziehungen und die Institutionalisierung von Kooperationen und der Zusammenarbeit notwendig, um Synergieeffekte zu schaffen.

5 Humankapital: Mangel an IT-Fachkräften als Wachstumshemmnis

Der IT-Fachkräftemangel wird in Deutschland schon seit vielen Jahren beklagt. Der Mangel wird sich in den kommenden Jahren noch erhöhen, auch wenn die Veränderung regional unterschiedlich verläuft. Besonders gravierend wird es aber gerade dort, wo schon heute die Industriearbeitsplätze oder die IT-Cluster beheimatet sind.[292]

In den BIGS-Experteninterviews wurde der Mangel an qualifizierten Arbeitskräften als erhebliches Hemmnis für die Digitalisierung von Geschäftsprozessen angesehen. Dieser Aussage stimmten 20 Teilnehmer zu, bei nur einer Ablehnung und einer Enthaltung. Das gilt einerseits für die Nachfrageseite von IT-SP/PSK-Märkten (*Enabler*-Perspektive), aber auch für die Anbieterseite (*Driver*-Perspektive). Damit verbunden, waren 15 der interviewten Experten der Meinung, dass dieser Mangel das Wachstum der deutschen IT-Sicherheitswirtschaft maßgeblich negativ beeinflusst. Das verwundert kaum, fragt ja zudem auch der Staat IT-Arbeitskräfte nach.

Von einem Fachkräftemangel in der IT-Sicherheitsbranche wird bereits seit längerer Zeit berichtet und vor ihm gewarnt. Bereits im Jahr 2020 sollen in Europa 350.000 Cybersecurity experten fehlen.[293] Auch Deutschland ist von diesem Fachkräftemangel betroffen. Und in Anbetracht der steigenden Bedeutung der IT-Sicherheitsbranche und dem damit einhergehenden Wachstum der Nachfrage nach IT-Sicherheitsexperten, stellt dieser Mangel ein ernstzunehmendes Wachstumshemmnis für die Branche dar.

Dieses Kapitel befasst sich mit dem obengenannten Problem, dessen Konsequenzen und bietet mögliche Lösungsvorschläge, um dem Fachkräftemangel entgegenzuwirken. Zunächst wird der *status quo* dargestellt, um einen Überblick über den bestehenden Fachkräftemangel zu bekommen; dies beinhaltet eine Aufführung der offenen Stellen, sowie eine Betrachtung der Qualifikation der Arbeitskräfte in dieser Branche. Darauf folgt eine Aufstellung der bereits existierenden und der zukünftigen Studiengänge im Bereich der Cybersicherheit. Abschließend werden mögliche Lösungsvorschläge und Handlungsempfehlungen präsentiert.

[292] Vgl. WifOR 2019a, S. 38.
[293] Vgl. Frost und Sullivan 2017, S. 8.

5.1 Zum Status quo

Die IT-Sicherheitsbranche Deutschlands ist innerhalb der letzten 10 Jahre deutlich gewachsen. Die Bundesagentur für Arbeit vermerkt einen Zuwachs von 177.000 beschäftigten IT-Fachleuten innerhalb von fünf Jahren (2012 bis 2017),[294] welcher auf die fortschreitende Digitalisierung zurückzuführen ist. Insgesamt ist die IT-Branche seit 2008 um 284.000 sozialversicherungspflichtige IT-Fachleute gewachsen.[295] Dabei war die Entwicklung in den letzten fünf Jahren besonders dynamisch. Allein im Vergleich zum Vorjahr gibt es 2018 6 Prozent mehr IT-Fachleute.[296] Obwohl dies die Zahl der gesamten IT-Fachkräfte abbildet, und daher nicht exklusiv die IT-Sicherheitskräfte aufführt, wird ersichtlich, dass die Branche schon heute stark wächst und mit der fortschreitenden Digitalisierung weiterhin wachsen wird.

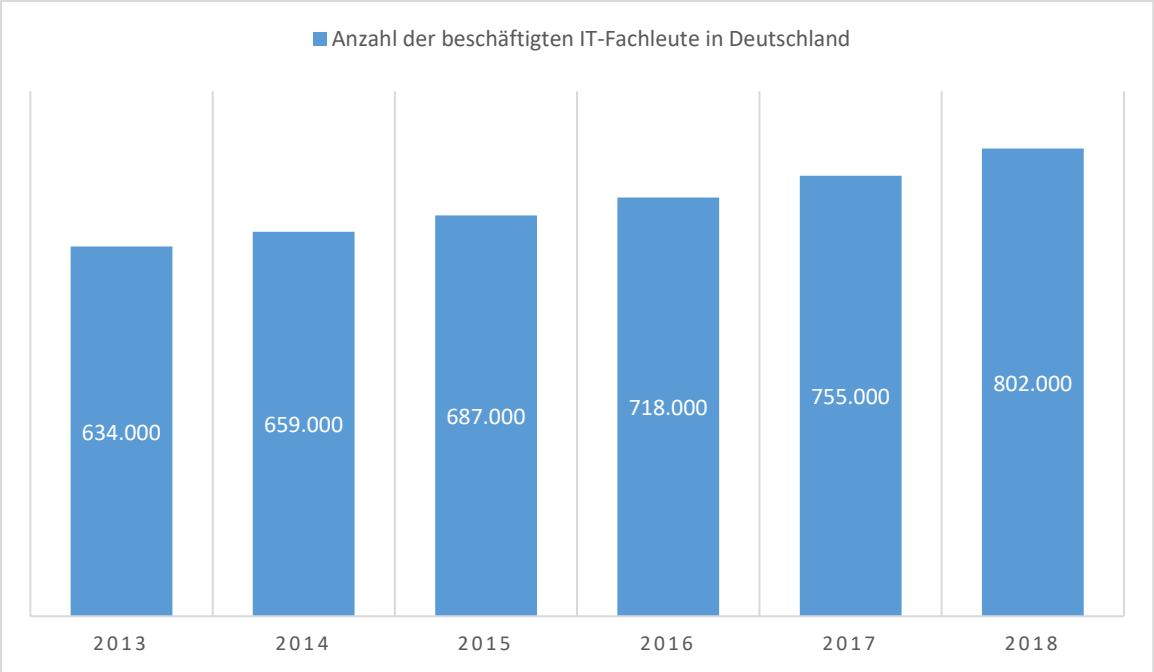


Abbildung 32 Anzahl der beschäftigten IT-Fachleute in Deutschland
Quelle: Bundesagentur für Arbeit 2019, S. 4.

Die Gesamtzahl von 802.000 beschäftigten IT-Fachleuten in Deutschland im Jahr 2018 setzt sich folgenderweise zusammen. 47 Prozent haben einen Fach- oder Hochschulabschluss, auch diese Zahl ist innerhalb von 5 Jahren um 5 Prozent gewachsen (2013-2018).[297] Hinzu kommen 38 Prozent, die einen

[294] Vgl. Bundesagentur für Arbeit 2019, S. 5.
[295] Vgl. Ebd. S. 5.
[296] Vgl. Ebd. S. 4.
[297] Vgl. Ebd. S. 5.

anderen anerkannten Abschluss haben.[298] Somit haben 85 Prozent der IT-Fachleute einen Berufsabschluss, was zeigt, dass eine abgeschlossene Ausbildung innerhalb dieser Branche erwünscht und gefordert ist.

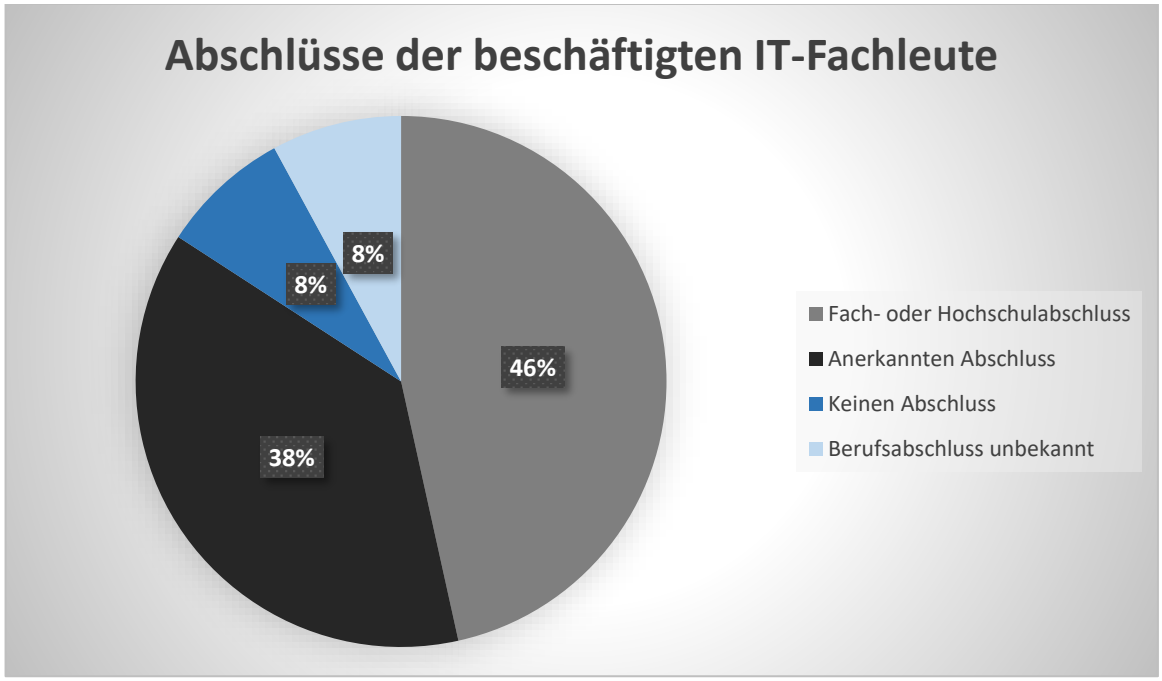


Abbildung 33 Abschlüsse der beschäftigten IT-Fachleute
Quelle: Bundesagentur für Arbeit 2019, S. 5.

Es wird deutlich, dass ein Berufsabschluss durchaus von Vorteil ist, um in der IT-Branche angestellt zu werden. Nur 8 Prozent der in der Branche tätigen Personen haben keinen Berufsabschluss und bei 8 Prozent der sozialversicherungspflichtig Beschäftigten IT-Fachleuten ist dieser unbekannt.[299]

78.000 der in Deutschland angestellten IT-Fachkräfte kommen aus dem Ausland.[300] Hiervon wiederum kommen 41 Prozent aus Ländern innerhalb der EU, am meisten aus Italien und Spanien.[301] Die anderen 59 Prozent kommen aus dem außereuropäischen Ausland, hauptsächlich aus Indien (11.000).[302] Es ist ebenfalls nennenswert, dass 4.000 der Fachkräfte aus außereuropäischen Ländern aus Asylzugangsländern kommen (dies umfasst Afghanistan, Eritrea, Irak, Iran, Nigeria, Pakistan, Somalia und Syrien).[303]

[298] Vgl. Ebd. S. 6.
[299] Vgl. Ebd.
[300] Vgl. Ebd. S. 9.
[301] Vgl. Ebd.
[302] Vgl. Ebd.
[303] Vgl. Ebd.

Die IT-Branche kann in mehrere Tätigkeitsbereiche aufgeteilt werden. Diese beinhalten Informatik, IT-Netzwerktechnik, Softwareentwicklung, Systemanalyse, sowie Beratung und Vertrieb. Prozentual arbeiten die meisten IT-Fachkräfte innerhalb der Informatik (30 Prozent) und der Softwareentwicklung (28 Prozent).[304] IT-Sicherheitsexperten werden allerdings in allen Tätigkeitsbereichen, obgleich weniger in Beratung und Vertrieb, gebraucht. Demnach werden IT-Sicherheitsfachkräfte innerhalb der gesamten Branche benötigt, was die Nachfrage deutlich erhöht.

Das rasante Wachstum der Branche spiegelt die fortschreitende Digitalisierung der Industrie wider und es wird projiziert, dass die Branche auch in den nächsten Jahren weiterhin stark wachsen wird. Seit 2010 beträgt das jährliche Wachstum rund 5 Prozent. Zeitgleich mit dem Wachstum der Branche steigt die Nachfrage nach IT-Fachkräften. Trotz, oder gerade wegen, des schnellen Expandierens der Branche gibt es eine hohe Anzahl an Stellenausschreibungen und seit mehreren Jahren ist von einem Fachkräftemangel die Rede.[305]

Der Bitkom zufolge gab es 2018 in Deutschland 82.000 offene Stellen in der IT-Branche, was einen Anstieg von 49 Prozent Anstieg zum Vorjahr bedeutet.[306] Die meisten dieser Stellenangebote verzeichnen hohe Anforderungen an die Qualifikationen der Bewerber, und folglich der Arbeitskräfte. Ein Großteil verlangt nachweisbare Qualifikationen, die einem mindestens dreijährigen Studium oder einer Weiterbildung entsprechen. Einige Stellen setzen auch eine Berufsausbildung voraus, allerdings sind diese im Vergleich mit Stellenausschreibungen, welche traditionelle Hochschulqualifikationen verlangen, seltener. Auch hier wird deutlich, dass nachweisbare Qualifikationen einen hohen Stellenwert in der IT-Branche haben, und in den meisten Fällen eine Einstellungsvoraussetzung darstellen. Es zeigt sich, dass hauptsächlich Fachkräfte gefragt werden, die sich über eine längere Zeit mit IT-Sicherheit auseinandergesetzt haben. Deshalb wird bei vielen Stellenangeboten auch eine (mehrjährige) Berufserfahrung in diesem Bereich vorausgesetzt.

Obgleich die oberen Beobachtungen die gesamte IT-Branche umfassen, setzen sich die Trends in dem spezifischeren Cybersicherheitsfeld fort. Auch hier gibt es einen deutlichen Fachkräftemangel – besonders KMU melden „Mangel an einschlägigem Personal“ in der IT-Sicherheit.[307]

[304] Vgl. Ebd. S. 6.
[305] Vgl. Bitkom 2018a. S. 46 ff.
[306] Vgl. Bitkom 2018c.
[307] Hillebrand et al. 2017, S. 11.

Die Anzahl der Stellenausschreibungen für IT-Sicherheitsfachkräfte hat deutlich zugenommen, und sich innerhalb von vier Jahren mehr als verdoppelt. Zugleich stiegen auch die Suchanfragen nach Cybersecurity-Stellenausschreibungen um 30 Prozent.[308] Stellenausschreibungen für diese Positionen richten sich an die folgenden Studiengänge: Am meisten gesucht werden Informatikabsolventen, dicht gefolgt von Wirtschaftsinformatik, oder anderen MINT-Studiengängen. Allerdings werden auch manchmal Absolventen anderer Studiengänge, wie zum Beispiel Rechtswissenschaften, nachgefragt. Dies beruht auf dem Anliegen, Interdisziplinarität in der IT-Sicherheit zu fördern. Besonders in Verbindung mit einer Berufsausbildung, oder auch als Quereinsteiger mit Interesse an IT-Sicherheit, sind Absolventen mit einem Abschluss in Fächern außerhalb der Informatik gefragt.

5.2 Studiengänge in IT-Sicherheit

In einer Erfassung des Statistischen Bundesamtes über alle Studiengänge in Deutschland kann das Wachstum der Informatik-Studiengänge beobachtet werden. Das Statistische Bundesamt klassifiziert in einer Studie nach dem folgenden Prinzip: Fächergruppe (hier geht es um Ingenieurswissenschaften), dann Studienbereich (Informatik) und letztendlich in Studienfach (auch wieder Informatik, allerdings abgegrenzt von Computer- und Kommunikationstechniken, Technische Informatik, Medieninformatik, Medizinische Informatik, Wirtschaftsinformatik, und Bioinformatik). Da sich diese Analyse mit den Absolventen von Informatik- bzw. IT-Sicherheitsstudiengängen befasst, widmet sich die folgende Diskussion hauptsächlich den Zahlen bezüglich des Studienbereiches sowie des Studienfachs Informatik.

Demnach gibt es im Sommersemester 2018 insgesamt 205.601 Studierende des Studienbereichs Informatik, sowie den dazugehörigen Studienfächern.[309] Von denen sind wiederum 110.360 Studierende in Informatik an sich eingeschrieben.[310] Diese Zahl setzt sich wie folgt zusammen: im ersten Hochschulsemester sind insgesamt 3.148, während sich insgesamt 10.551 im ersten Fachsemester befinden.[311] Die letzteren haben sich demnach explizit für Informatik als Prüfungsfach entschieden und werden danach Absolventen des Studienfachs Informatik. Von den insgesamt 110.360 Informatikstudierenden kommen 19.926 aus dem Ausland.[312] Die Anzahl der Studierenden des Studienfaches Informatik hat sich innerhalb der letzten Jahre vergrößert, und spiegelt somit das anhaltende Wachstum der IT-Branche wider. Die steigende Anzahl der Informatikstudierenden der letzten acht Jahre kann in der folgenden Tabelle nachvollzogen werden.

[308] Vgl. Hering 2018.
[309] Vgl. DESTATIS 2019, S. 24.
[310] Vgl. Ebd. S. 106.
[311] Vgl. Ebd.
[312] Vgl. Ebd.

	Deutsche			Ausländer			Insgesamt		
	m	**w**	**i**	**m**	**w**	**i**	**m**	**w**	**i**
2010/11	52 283	6 377	58 660	8 353	2 546	10 899	60 636	8 923	69 559
2011/12	57 398	7 401	64 799	8 577	2 722	11 299	65 975	10 123	76 098
2012/13	61 235	8 785	70 020	9 261	2 992	12 253	70 496	11 777	82 273
2013/14	64 710	10 219	74 929	10 030	3 306	13 336	74 740	13 525	88 265
2014/15	68 429	11 970	80 399	10 862	3 655	14 517	79 291	15 625	94 916
2015/16	72 664	13 061	86 265	12 050	4 231	16 281	84 714	17 832	102 546
2016/17	76 858	15 258	92 116	13 303	4 689	17 992	90 161	19 947	110 108
2017/18	79 219	15 954	95 173	14 680	5 152	19 832	93 899	21 106	115 005

Tabelle 6 Anzahl der Informatikstudierenden an deutschen Hochschulen 2010 bis 2018
Quelle: Erstellt anhand von Daten, die bei einer Abfrage des Genesis Archivs auf der Website des Statistischen Bundesamtes (DESTATIS) generiert wurden, bezogen auf das Studienfach Informatik.
(m = männlich, w = weiblich, i = insgesamt)

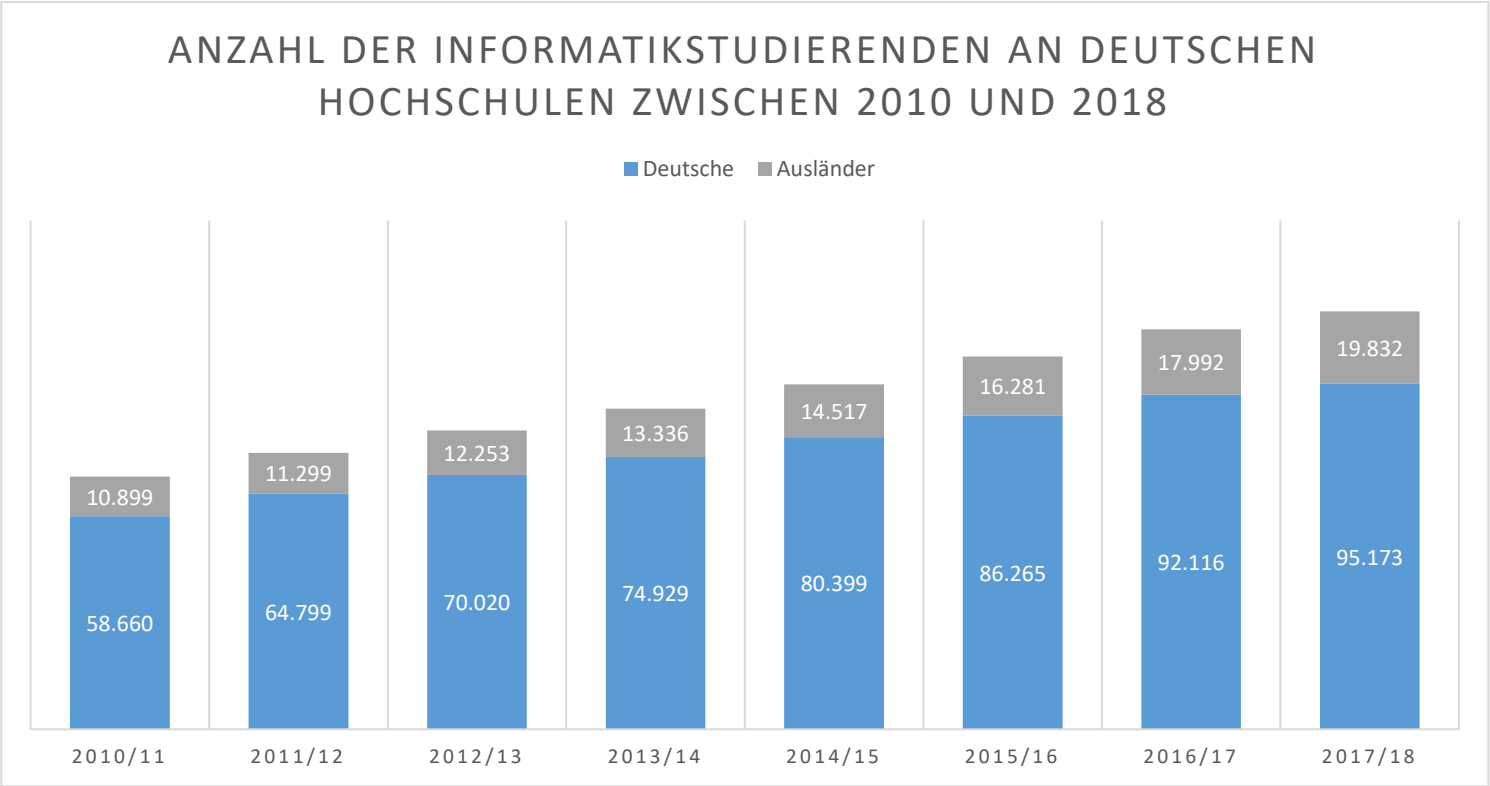


Abbildung 34 Anzahl der Informatikstudierenden an deutschen Hochschulen zwischen 2010 und 2018
Quelle: Eigene Darstellung. Erstellt anhand von Daten, die bei einer Abfrage des Genesis Archivs auf der Website des Statistischen Bundesamtes (DESTATIS) generiert wurden, bezogen auf das Studienfach Informatik.

Wie bereits angemerkt, beziehen sich die oben genannten Daten auf das Studienfach Informatik, und deshalb nicht nur auf Studiengänge, die sich explizit mit Cybersicherheit beschäftigen. Die Erfassung bei DESTATIS hat keine eigene Kategorie für *Cybersecurity*. Es wird hier angenommen, dass sich diese Studiengänge, obwohl es zur jetzigen Zeit noch relativ wenige gibt, innerhalb des Studienfaches Informatik subsumiert werden. Demnach wäre ein Teil der oben genannten 110.360 Studierenden des Sommersemesters 2018 in IT-Sicherheitsstudiengänge eingeschrieben.

Allerdings ist das Angebot der IT-Sicherheitsstudiengänge in Deutschland noch sehr begrenzt. Eine im Jahr 2019 veröffentlichte Studie von PricewaterhouseCoopers (PwC) erfasst zwar, dass es in Deutschlands Universitäten inzwischen 38 Professuren für IT-Sicherheit gibt.[313] Aber im europäischen Vergleich (allein im Vereinigten Königreich gibt es 34 M.Sc. Cybersecurity Studiengänge) und hinsichtlich des andauernden Fachkräftemangels, scheint dies nicht ausreichend zu sein. Auch die große Mehrheit der interviewten Experten wies darauf hin, dass noch vermehrt Masterstudiengänge in Deutschland eingerichtet werden müssten.[314] Sie waren aber gleichzeitig auch der Meinung, dass bestehende und zukünftige Cybersicherheits-Masterstudiengänge nicht nur aus technischer Sicht gelehrt werden sollten und dass genauso stark Ausbildungsberufe für den Bereich Cybersicherheit angeboten werden sollten. Multidisziplinäre Masterstudiengänge oder Ausbildungen könnten dadurch eine breitere Masse für das Thema begeistern.

Ein Großteil dieser Professuren hat ihren Sitz an einer geringen Zahl von Universitäten. Diese liegen zumeist an jenen Orten, die auch sonst durch ein starkes Cluster an Unternehmen, und Forschungseinrichtungen und staatlichen Einrichtungen aus dem Cybersicherheitsbereich auffallen. Die Frage der Kausalität konnte im Rahmen dieser Studie nicht untersucht werden. Obwohl das Studienfach Informatik in Deutschland weit verbreitet ist, gibt es von 68 Universitäten, die Informatik lehren, nur neun mit einem IT-Sicherheitsstudiengang.[315]

Eine vom BIGS durchgeführte Recherche in den öffentlich zugänglichen Websites der Universitäten und Fachhochschulen in Deutschland hat gezeigt, dass es an mehreren dieser Institutionen mittlerweile Studiengänge gibt, die sich explizit mit IT-Sicherheit befassen. Die zusammengetragenen Ergebnisse werden in der nachfolgenden Tabelle aufgeführt – mit dem Namen

[313] Vgl. PwC 2019.

[314] 14 der Befragten Experten sehen die Einrichtung von Masterstudiengängen als ein Mittel zur Milderung des Fachkräftemangels. Die verbliebenen Experten konnten oder wollten sich dazu nicht explizit äußern.

[315] Vgl. PwC 2019.

der jeweiligen Studienfächer, der Institution, die zu erreichende Qualifikation und, falls vorhanden, Angaben zu der Anzahl der Absolventen.

Lfd.	Institution	Studienfach	Qualifi-kation	Weitere Informationen
1.	Arden Universität Berlin	IT-Security Management	M.Sc.	
2.	BTU Cottbus	Cybersecurity	M.Sc.	Noch keine Absolventen
3.	Fachhochschule Wedel	IT-Sicherheit	M.Sc.	20 Studierende pro Jahrgang
4.	Friedrich-Alexander-Universität Erlangen Nürnberg	Informatik / IT-Sicherheit	B.Sc.	Neu; erste Absolventen im WS19/20
5.	Hochschule Aalen	IT-Sicherheit	B.Sc.	
6.	Hochschule Albstadt-Sigmaringen	IT-Security	B.Sc.	36 Studierende
7.	Hochschule für Angewandte Wissenschaft Ansbach	Datenschutz und IT-Sicherheit	M.Sc.	
8.	Hochschule für Technik, Wirtschaft und Medien Of-fenbach	Unternehmens- und IT-Sicherheit	B.Sc.	Neu; Start WS 19/20
9.	Hochschule Mannheim	Cybersecurity	B.Sc.	Neu; läuft seit zwei Semestern
10.	Hochschule Mittweida	IT-Sicherheit	B.Sc.	Noch keine Absolventen
11.	Hochschule Mittweida	Cybercrime / Cybersecurity	M.Sc.	Noch keine Absolventen
12.	Hochschule Stralsund	IT-Sicherheit und mobile Systeme	B.Sc.	
13.	Hochschule Wismar	IT-Sicherheit und Forensik	M.Eng.	
14.	Hasso-Plattner-Institut Potsdam	Cybersecurity	M.Sc.	Neu; Start WS19/20
15.	Ruhr-Universität Bochum	IT-Sicherheit / Informationstechnik	B.Sc.	35 Absolventen pro Semester
16.	Ruhr-Universität Bochum	IT-Sicherheit / Informationstechnik	M.Sc.	20 Absolventen pro Semester

17.	Ruhr-Universität Bochum	IT-Sicherheit / Netze und Systeme	M.Sc.	13 Studierende pro Semester
18.	Ruhr-Universität Bochum	Applied IT-Security	M.Sc.	6 Studierende pro Semester
19.	SRH Hochschule Berlin	Cybersecurity Consulting	B.Sc.	Neu; Start WS18/19
20.	Technische Hochschule Brandenburg	Security Management	M.Sc.	
21.	TU Darmstadt	IT-Security	M.Sc.	
22.	Universität der Bundeswehr München	Cybersecurity	M.Sc.	
23.	Universität des Saarlandes	Cybersecurity	B.Sc.	
24.	Universität des Saarlandes	Entrepreneurial Cybersecurity	M.Eng.	
25.	Universität zu Lübeck	IT-Security	B.Sc.	60 Studierende pro Semester
26.	Universität zu Lübeck	IT-Security	M.Sc.	
27.	Wilhelm Büchner Hochschule	IT-Sicherheit	B.Sc.	Noch keine Absolventen, frühestens 2020
28.	Universität Bonn	Cybersecurity	B.Sc.	58 Studierende; Start WS 19/20

Tabelle 7 Studiengänge im Bereich IT-/Cybersicherheit an Universitäten und Fachhochschulen in Deutschland
Quelle: Erstellt anhand von Daten, die durch eine Nachfrage bei den jeweiligen Institutionen bzw. auf öffentlichen Websites gesammelt wurden. Wo keine Absolventenzahl aufgeführt ist, gibt es keine Daten, oder diese dürfen nicht kommuniziert werden.
(B.Sc. = Bachelor of Science; M.Sc. = Master of Science; M.Eng. = Master of Engineering)

Anhand der Tabelle ist nachzuvollziehen, dass zwar schon einige IT-Sicherheitsstudiengänge angeboten werden, aber viele hiervon sich noch in der Anfangsphase befinden. Neun der aufgeführten 28 Studiengänge, und damit über 30 Prozent, werden entweder erst seit wenigen Semestern angeboten oder werden frühestens mit dem Wintersemester 2019/2020 beginnen. Dies bedeutet, dass es noch keine Absolventen dieser Studiengänge gibt, bzw. dass es noch einige Semester dauern wird bevor Absolventen der IT-Sicherheit dem Arbeitsmarkt zur Verfügung stehen und letztendlich den Fachkräftemangel abmildern können.

Um dem Fachkräftemangel weiterhin entgegenzuwirken, gibt es ein Angebot von verschiedenen Fort- und Weiterbildungsmaßnahmen, die genutzt werden können. Damit können sich IT-Kräfte, die keine Hochschulausbildung haben, in ihrem Arbeitsbereich weiterbilden und anspruchsvollere Arbeiten übernehmen. Ein Beispiel dieser ist die von Bitkom angebotene Ausbildung zum IT-Sicherheitsbeauftragten (ITSiBe). Innerhalb von vier Tagen lernen Teilnehmer „das nötige Fachvokabular, rechtliche Rahmenbedingungen und die Grundsätze der Informationssicherheit";[316] nach einer abschließenden Prüfung bekommen die Teilnehmer ein Personenzertifikat welches für zwei Jahre gültig ist. Obwohl solch ein Zertifikat natürlich keine dreijährige Hochschulausbildung ersetzten kann, haben sie ihren Wert, da sie die bestehenden Arbeitskräfte innerhalb der IT-Sicherheitsbranche unterstützen können und so die geringe Zahl der IT-Sicherheitsfachkräfte entlasten können.

Eine kürzlich veröffentlichte Studie der amerikanischen IT-Sicherheitsfirm Symantec bestätigt den andauernden Fachkräftemangel in Deutschland und erörtert dessen Ausmaße. Es sagen z.B. 48 Prozent der befragten deutschen C*ybersecurity*-Anbieter, dass die Kenntnisse ihrer Teams nicht mit den Kenntnissen der Cyberkriminellen mithalten können[317]; folgerichtig sagen 45 Prozent der befragten deutschen Sicherheits-Experten, „dass ihre Teams nicht ausreichend qualifiziert sind, um Cyberthreats zu bekämpfen."[318] Hinzu kommt, dass mehr als die Hälfte der Sicherheitsexperten angeben, dass herkömmliche Tagesaufgaben zu viel Arbeitszeit und Arbeitskräfte beanspruchen.

[316] Vgl. Bitkom 2019.
[317] Vgl. Kroker 2019.
[318] Ebd.

5.3 Handlungsempfehlungen

Es ist deutlich geworden, dass der Mangel an IT-Sicherheitskräften sowohl für die IT-Sicherheitswirtschaft als auch für herkömmliche Unternehmen ein Wachstumshemmnis darstellt. Diesen Mangel zu mildern ist Aufgabe von Staat, Unternehmen und ganz besonders von (Aus-)Bildungseinrichtungen. Ohne Fortschritte in diesem Bereich kann das Wachstumspotential durch Digitalisierung nicht voll ausgeschöpft werden.

Obwohl mittlerweile mindestens 28 Cybersicherheitsstudiengänge angeboten werden, gibt es noch viel zu wenig Absolventen, um den Fachkräftemangel wirksam zu bekämpfen. Der Mangel wird daher noch einige Jahre andauern, da viele dieser Studiengänge erstmalig Studierende immatrikulierten. In der Zwischenzeit lohnt es sich, IT-Sicherheit in andere Studienfächer zu integrieren, um auch nicht-Informatikstudierende für dieses Fach und Berufsfeld zu interessieren. Insbesondere auch in der Betriebswirtschaftslehre gäbe es eine gute Möglichkeit, Grundkenntnisse der IT-Sicherheit zu integrieren. Dadurch könnte ein größeres Verständnis für das Thema in den Unternehmen geschaffen werden. Zusätzlich muss innerhalb der Wissenschaftsdisziplin ein Wissenstransfer angeregt werden – Cybersicherheit gelingt nur ganzheitlich; und ein breiteres Bewusstsein für die Notwendigkeit der IT-Sicherheit ist angebracht, um das Thema und die Branche intensiv zu fördern.

Eine weitere mögliche Maßnahme wäre es, parallel zum weiteren Ausbau des Angebots der Cybersicherheitsstudiengänge in Deutschland, explizite IT-Sicherheitsmodule in breiter angelegte IT-Studiengänge zu integrieren. Dies geschieht auch schon teilweise. So haben zum Beispiel einige Hochschulen im Studienfach Informatik spezielle IT-Sicherheitsmodule integriert – IT-Sicherheitsmodule außerhalb des Studienbereiches Informatik sind allerdings nicht bekannt. Hiermit könnte gewährleistet werden, dass eine erhöhte Anzahl von Studenten mit IT-Sicherheit in Kontakt kommen und sich in diesem Themenfeld, zumindest grundlegend, ausbilden und qualifizieren lassen können. Dadurch würde die Interdisziplinarität von IT-Sicherheitsstudien gesteigert und die Hintergründe der IT-Sicherheitsexperten erweitert werden. Es muss des Weiteren dafür gesorgt werden, dass vertiefende IT-Sicherheitsstudiengänge (z.B. M.Sc.) auch vermehrt für Studierende ohne expliziten IT-Sicherheitshintergrund angeboten werden.

Langfristig sollten MINT-Fächer im Allgemeinen, und Informatik im Besonderen, in Schulen gefördert werden. Hierdurch kann das Interesse junger Menschen an dem Thema angeregt werden. Eine Mehrzahl der vom BIGS befragten Experten waren der Meinung, dass dies ein sehr

guter Ansatz wäre, um langfristig dem Fachkräftemangel zu begegnen.[319] Einige von ihnen wiesen auch daraufhin, dass *digital skills*, Cyberhygiene und *hacking* bereits in der Schule unterrichtet werden sollte.[320]

Des Weiteren sollten nichtakademische Berufslaufbahnen in der IT-Sicherheitsbranche besser angeboten und genutzt werden. Das beinhaltet lebenslanges Lernen und Weiterbilden der bestehenden IT-Sicherheitskräfte, um auf dem aktuellen Stand der Technikentwicklung zu bleiben. Außerdem sollten die Auszubildenden sowie die IT-Sicherheitsstudierenden Möglichkeiten haben, ihr praktisches Wissen und Erfahrungen auszubauen. Hierfür können realistische Umgebungen genutzt werden, in denen die Studierenden realitätsnahe Szenarien lösen müssen. Dies wird in Hochschulen in Frankreich in Kooperation mit Cybersicherheitsunternehmen angeboten, was nebenbei auch der Rekrutierung von Fachkräften zu Gute kommt.[321] Insbesondere sog. Cyberranges sind hier ein sinnvolles Vehikel, um Mitarbeiter von Unternehmen zu schulen.

Zuletzt bleibt noch das Mittel der qualifizierten Einwanderung. Gerade in Ländern mit einer soliden mathematisch-natur-wissenschaftlichen Ausbildung kann man auf die Suche nach migrationswilligen Fachpersonal gehen. Sprachprobleme dürften in diesem weitgehend auf Englisch operierenden Umfeld ein geringeres Problem sein.

[319] 16 der Befragten Experten sehen die Ausweitung der schulischen Ausbildung in den MINT-Fächern als ein Mittel zur Milderung des Fachkräftemangels. Bei einer Ablehnung, konnten oder wollten sich die verbliebenen Experten dazu nicht explizit äußern.

[320] Interview 2, Regulierer; Interview 3, Verband; Interview 12, Driver international.

[321] Interview 12, Driver international.

6. Zusammenfassung & Handlungsempfehlungen

Der Prozess der Digitalisierung ist ein Wachstumstreiber für die gesamte Volkswirtschaft. Ursache dafür ist, dass sich mit der Digitalisierung in quasi allen Bereichen gesellschaftlichen Handelns und Wirtschaftens, erhebliche Produktivitätssteigerungen erreichen lassen. Dies ist ein langfristiger Wachstumsimpuls, der in der Literatur als Kondratjew-Zyklus bezeichnet wird.[322] Es handelt sich also um einen lang andauernden, nachhaltigen Wachstumsimpuls und damit verbundener Wohlstandssteigerung.

Es ist fast schon selbstverständlich, dass die neuen technischen Möglichkeiten und der neue Wohlstand auch Begehrlichkeiten seitens krimineller Elemente wecken. Deswegen nun auf die Wachstumsmöglichkeiten durch Digitalisierung zu verzichten, wäre allerdings nicht zielführend. Vielmehr gilt es, dem Rechtsstaat auch in der Cyberdomäne zum Durchbruch zu verhelfen und sich darüber hinaus hinreichend selbst vor den Bedrohungen im Cyberraum zu schützen.

Während Cybersicherheit und die damit in Verbindung stehenden Ausgaben und organisatorischen Maßnahmen auf den ersten Blick als Restriktion, mithin als „Bremse“, auf den Digitalisierungsprozess wirken, ist Cybersicherheit tatsächlich die notwendige Bedingung, das Wachstumspotenzial der Digitalisierung auszuschöpfen. In dieser Logik ergibt sich eine konzeptionelle Nähe zur Umweltpolitik: Es kommt darauf an, dass die Nachhaltigkeitsdefizite von den Wirtschaftssubjekten und ggf. von der staatlichen Regulierung erkannt werden. Kurzfristig ist also eine durchaus kostenträchtige Konsolidierung herzustellen. Langfristig aber führt dies auf einen Wachstumspfad mit größerem gesellschaftlichem Wohlstand. Diese Überlegung sei schematisch dargestellt in Abbildung 35.

[322] Vgl. etwa Kurz et al. 2018.

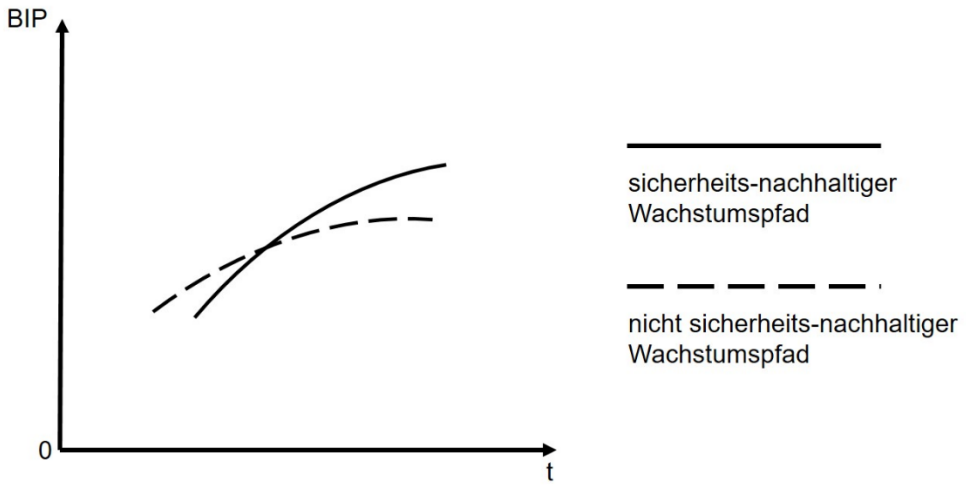


Abbildung 35 Sicherheitsnachhaltiger und nicht-sicherheitsnachhaltiger Wachstumspfad
Quelle: Eigene Darstellung.

Abgebildet ist ein Vergleich zwischen einen sicherheits-nachhaltigen Wachstumspfad (durchgezogene Linie) und einem nicht-sicherheits-nachhaltigem Wachstumspfad (gestrichelte Linie). Beim letzterem ergeben sich *kurzfristig* höhere Zuwächse. So kann man, angetrieben durch kurzfristige Digitalisierungsrenditen, schneller und zu geringen Kosten in neue Geschäftsfelder vordringen, mit denen sich Wachstum generieren lässt. Langfristig aber treten die Sicherheitsprobleme zu Tage und dämpfen das Wachstum. Diese Dämpfung ist ggf. erheblich, da nicht ausgeschlossen ist, dass Schäden durch Cyberangriffe für Unternehmen existenzgefährdend sein können. Eine Dämpfung ergibt sich zudem auch dann, wenn aufgrund von Cyberrisiken bzw. Sicherheitsdefiziten, Digitalisierungsprojekte zurückgehalten werden müssen, weil der mögliche (erwartete) Schaden den erwarteten Gewinn übertrifft. Es kommt also darauf an, dass mit dem Umfang der Digitalisierung, die Cybersicherheit „mitwächst“. Denn das Wachstum der Digitalisierung führt mit der damit einhergehenden zunehmenden Vernetzung in exponentieller Steigerung zu neuen Angriffspunkten, also zur Erleichterung von Zugängen für Angreifer und Kriminelle.[323]

Die vorangegangene Analyse hat gezeigt, dass es erhebliche **Marktversagenstatbestände** im Bereich der Cybersicherheit gibt. Damit also Unternehmen und Haushalte hinreichend in Cyberschutzleistungen investieren und somit der Cyberschutz mit der Digitalisierung mitwächst, ist es Aufgabe des Staates, durch geeignete Maßnahmen dieses Marktversagen zu korrigieren.

[323] Vgl. Abschnitt 2.

Damit Unternehmen und Haushalte die Nachfrage nach Cyberschutzleistungen und den notwendigen Umfang richtig abschätzen können, brauchen sie **verlässliche Informationen** über den Umfang und die Art der Bedrohung im Cyberraum. Das Angebot an Informationen ist heute noch unzureichend. Zwar gibt es zahlreiche Studien und einige staatliche Berichte zu diesem Thema, die aber alle für sich genommen ungenügend sind, wenn es darum geht, die Informationsdefizite zu beseitigen und ein holistisches Bild zu kreieren. Cybersicherheit benötigt Zeitreihendaten, um Korrelationen zwischen der Angriffsmethode und dem Angriffsziel ableiten zu können. Nur so lässt sich die Bedrohung realistisch einschätzen, um darauf basierend geeignete Gegenmaßnahmen zum Schutz zu treffen.

Während einerseits für Unternehmen und Haushalte nicht hinreichend Informationen über die Bedrohung im Cyberraum zur Verfügung stehen, haben diese, wenn sie selbst von Cyberattacken betroffen sind, kaum einen Anreiz, einen Angriff den zuständigen staatlichen Stellen zu melden. Die **Meldepflicht** beim BSI, die für bestimmte Betreiber von Kritischen Infrastrukturen gilt, hat hier Milderung geschaffen, ohne dass dies bereits ausreichend wäre.

Der jährlich veröffentlichte **BSI-Lagebericht** ist eine gute Quelle für Informationen zur Bedrohung im Cyberraum und zu möglichen Schutzmaßnahmen. Der Lagebericht sollte aber weiterentwickelt werden, um Unternehmen und Wissenschaft besser über Trends bei der Cyberbedrohung aufzuklären.[324] Nur dann kann die Privatwirtschaft hinreichend informiert, die richtigen Schutzmaßnahmen treffen. Wenn die Kernbotschaft aber wiederkehrend lautet, dass alles stetig immer nur schlimmer wird, dann droht eine resignierende Apathie die notwendigen Gegenmaßnahmen zu verdrängen.

Gerade die Meldungen auf Grundlage des IT-Sicherheitsgesetzes für KRITIS-Betreiber dürften eigentlich eine gute Datenbasis für Trendanalysen bieten. Anders als bei Umfragen besteht hier die Pflicht zur Meldung. Bislang bietet der BSI-Lagebericht gute Hinweise, wie sich gerade Unternehmen besser vor Cyberattacken schützen können. Bei der Bedrohungslage liegt der Schwerpunkt bei Fallbeispielen und qualitativer Beschreibung. Für die Aufteilung eines IT-Sicherheitsbudgets bietet er Ideen, aber kaum quantitative Entscheidungsunterstützung.

Nicht nur über den Umfang der Bedrohung im Cyberraum besteht ein Informationsdefizit, sondern auch über die **Effektivität** einzelner **Schutzmaßnahmen**, in die Unternehmen und Haus-

[324] Vgl. BSI 2019.

halte investieren können. Es bedarf eines vorhandenen vertieften Expertenwissens oder der Inkaufnahme hoher Informationskosten zwecks Einholung dieser Expertise von außen, wenn man dieses Informationsdefizit überwinden will. Die Ausweitung des Einsatzes von Standards und Zertifikaten als Signalgeber für bestimmte Qualitätsniveaus kann hier Abhilfe schaffen.

Im Bereich der IoT-Produkte gilt es, deren Sicherheit und sicheren Gebrauch im Internet für Nutzer und Hersteller überhaupt erst zu einem Entscheidungskriterium zu machen. Bislang haben beide Seiten im Grunde keinen Anreiz, bei der Entwicklung oder der Kaufentscheidung dieses Thema stark zu gewichten. Auch muss man konstatieren, dass es Teilen der Bevölkerung (z.B. Senioren) nicht zumutbar ist, regelmäßige Updates von Firmware vorzunehmen. Hier bietet sich daher zum einen analog zu anderen technischen Geräten die Einführung einer Anbieterhaftung an, und zum anderen eine möglichst weite Umsetzung des Prinzips *security by design*.

Ein wesentlicher Grund für zu geringe Investitionen in IT-Schutzleistungen ist das Vorhandensein von zum Teil erheblichen **externen Effekten**. Zahlreiche Maßnahmen schützen eher Dritte als das die Maßnahme ergreifende Individuum bzw. die Organisation selbst; und der unzureichende Schutz des einen hat schnell auch negative Konsequenzen für andere. Ähnlich wie bei der Impfung gegen Krankheiten gilt es, eine Art **Herdenimmunität** durch ausreichende Schutzleistungen im Gesamtsystem herbeizuführen. Neben einer klaren Zuteilung von *Pro*perty *Rights* (z.B. durch Produkthaftung) ist hier der Ansatzpunkt für staatliche Unterstützungsprogramme und Subventionen.

Eine Maßnahme könnte es sein, bestehende Förderprogramme auf das Thema IT-Sicherheit stärker auszurichten. So könnte etwa in den Programmen Go-inno und Go-digital des BMWi der Baustein Cybersicherheit gestärkt werden; zu Lasten von Bausteinen zur Markterschließung und/ oder durch einen Ausbau dieser Beratungsprogramme. Auch eine **Verkürzung der Abschreibungszeiten** (AfA) hilft, damit Unternehmen aktuelle Sicherheitsprodukte zum Einsatz bringen. Ähnlich wie in der Umwelt- und Klimaschutzdebatte kann man sich aber auch eine finanzielle Belastung von Nutzern schlecht abgesicherter IT-Systeme vorstellen. Im Extremfall kann das soweit reichen, dass ein IT-Grundschutz weitverbreiteter Konsumprodukte mit Internetanschluss – wie Computer oder Smartphones – ein öffentliches Gut darstellt. So könnte zum Beispiel ein Virenscanner kostenfrei vom BSI bereitgestellt werden, mit dessen Hilfe internetfähige Geräte einen solchen Grundschutz erhalten.[325]

[325] Dies heißt nicht, dass auch die Herstellung durch den Staat erfolgen muss.

Die **Forschungsförderung** im Bereich IT-Sicherheit ist in Deutschland bereits weit ausgeprägt. Auch wegen des Mangels an qualifiziertem Humankapital scheint eine weitere Ausweitung hier an Grenzen zu stoßen. Wichtig ist aber, dass nicht nur Spitzenforschung in diesem Bereich gefördert wird, sondern dass auch Projekte eine Förderung erhalten, die sich mit vermeintlich einfachen Fragen – wie einer sicheren, aber intuitiv zu bedienenden persönlichen Identifizierung im Internet – beschäftigen. Die Schwierigkeiten, die insbesondere wenig technikaffine Menschen bei der Umstellung im Rahmen der neuen Richtlinie für Zahlungsdienste Payment Services Directive 2 (PSD2) haben, zeigt, wie notwendig dies ist.

Beim Schutz vor Bedrohungen im Cyberraum bestehen zum Teil erhebliche **Skaleneffekte**. Daraus begründet sich auch der immer wieder kritisierte mangelnde Schutz von KMU, da diese zu klein für erwähnte Skaleneffekte sind. Neue Cloudbasierte Plattformlösungen schaffen aber die Möglichkeit, dass zukünftig solche Skaleneffekte internalisiert werden können. Auch kleine Unternehmen könnten dann durch ein zumindest teilweises Pooling ihres IT-Schutzes von den gleichen Skaleneffekten wie große Unternehmen profitieren. Auch der Austausch von Angriffsdaten und Abwehrmaßnahmen innerhalb von „Selbsthilfegruppen“ der IT-Sicherheitsverantwortlichen ist eine geeignete Maßnahme, Skaleneffekte auch unter KMUs auszunutzen.

Die Nachfrage nach qualifizierten IT Fachkräften ist in Deutschland hoch und wachsend. Schon heute gibt es hier einen erheblichen **Mangel an qualifiziertem Personal** und zahlreiche Vorschläge, wie durch gezielte Zuwanderung und eine bessere Bleibeperspektive für ausländische Studierende hier zumindest teilweise Abhilfe geschaffen werden kann. Dies gilt äquivalent für den Arbeitsmarkt für spezialisierte IT-Sicherheitsfachleute. Ca. 80.000 Stellen sind hier unbesetzt, und die Zahl steigt laufend. Allerdings ist auch nicht jeder Informatiker gleich ein qualifizierter IT-Sicherheitsexperte. Bisher gibt es nur wenige Studiengänge, die sich in diesem Feld spezialisiert haben. Die meisten dieser Studiengänge sind noch sehr jung, somit in der Etablierungsphase, und werden selbst im voll ausgebauten Zustand wenige Absolventen in den Arbeitsmarkt entlassen.

Es muss davon ausgegangen werden, dass der Arbeitskräftemangel die nächsten Jahre überdauern wird. Der Nachfrageüberhang lässt sich nur durch eine Senkung der Einstiegshürden mildern, und ferner, indem ein größerer Anteil von Studienanfängern und Masterstudierenden in dieses Feld gelockt wird. Hierbei gilt es auch ungewöhnliche Wege zu beschreiten. Zum Beispiel könnte eine **gezielte Studienförderung**, vergleichbar mit dem Deutschlandstipendium, die Attraktivität einer solchen Studienrichtung erhöhen. Auch das frühe Angebot von Stellen

für Werkstudenten kann hier helfen. Zudem muss der nichtakademische Aus- und Weiterbildungsbereich adressiert werden. Der IT-Arbeitsmarkt benötigt nicht nur Akademiker. Auch Nicht-Akademiker mit guten IT-Kenntnissen müssen im Prozess berücksichtigt werden. An dieser Schnittstelle kommt es häufiger zur Diskrepanz zwischen gesetzlichen Vorgaben zur schulischen und akademischen Qualifikation einerseits, und den vorhandenen Kenntnissen - vor allem ausländischer - Bewerber/ Anwärter andererseits.

Ohne eine Adressierung des Mangels an Humankapital kann eine staatliche Förderung der IT-Sicherheitswirtschaft in Deutschland kaum erfolgreich sein. Verstärktes Wachstum der Branche würde durch steigende Löhne des Fachpersonals gebremst. Schon heute kann man durch die stark gestiegene staatliche Nachfrage nach IT-Fachpersonal einen *crowdingout*-Effekt erkennen.

Ein effizienter **Risikotransfer** ist als dritte Säule des Cyberschutzes von großer Bedeutung. Die Verfügbarkeit von transparenten Versicherungslösungen ist eine wichtige Nebenbedingung bei der Digitalisierung von Wertschöpfungsketten. Um Versicherer und ihre Kunden vor Rechtsunsicherheit zu schützen, ist eine klare Regelung für den Kriegs- und Terrorfall notwendig. Hier lohnt sich der Blick auf die in den USA und Großbritannien gefundenen regulatorischen Lösungen. Die Versicherungswirtschaft muss die durch die versicherten Schadensfälle gewonnenen Informationen nutzen, um über ihre Versicherungsbedingungen die Anforderungen an einen effizienten Cyberschutz im Zeitablauf zu verbessern.

Die deutsche IT-Sicherheitswirtschaft ist geprägt durch den hohen Anteil kleiner Unternehmen. Das Wachstum in der Branche ist schon heute hoch. Der Mangel an IT-Fachkräften bremst dieses Wachstum. Auch deshalb halten sich IT-Sicherheitsunternehmen bei der Beteiligung an staatlichen Forschungsprogrammen zurück. Ein weiterer Grund scheint in der Veröffentlichungspflicht der FuE-Ergebnisse in vielen Programmen zu liegen. Mit einer Privatisierung von Wissensvorsprüngen schafft man hier Innovationsanreize.

In der deutschen IT-Sicherheitswirtschaft fehlt es an einem **Systemintegrator**. Zwar bieten die Unternehmen häufig innovative Speziallösungen an, die geringe Unternehmensgröße führt aber dazu, dass Skaleneffekte und Verbundvorteile nicht ausgenutzt werden können. Auch ist die Kapitalkraft oftmals zu gering, um längerfristige Beschaffungs- und Betreiberprojekte durchhalten zu können. Gerade bei staatlichen Ausschreibungen sollte hierauf Rücksicht genommen werden.

In den vom BIGS geführten Experteninterviews wird oftmals kritisiert, dass bei öffentlichen Ausschreibungen vielfach zu detailliert das zu beschaffende Produkt oder die Dienstleistung beschrieben wird. Innovative Lösungen erfüllten dann häufig die Ausschreibungsbedingungen nicht. Auch die langwierigen Beschaffungsverfahren führen dazu, dass die **staatliche Beschaffung** in Deutschland als Wachstums- und Innovationstreiber bislang eine untergeordnete Rolle spielt. Des Weiteren führt die dezentrale Beschaffung dazu, dass das Auftragsvolumen oftmals keine kritische Größe erreicht, um eine Lösung zum Marktdurchbruch zu verhelfen.

Sowohl bei der Beschaffung durch den Staat als auch durch Unternehmen wird von der IT-Sicherheitswirtschaft kritisiert, dass die Entscheider oftmals selbst wenig kompetent sind, was Entscheidungen bezüglich von Unterschieden und Vorteilhaftigkeiten von Angeboten betrifft. Dies erscheint aber ein Problem zu sein, welches beide Marktseiten – Anbieter wie Nachfrager – angehen müssen. Der Anbieter einer Lösung muss eben auch selbst herausarbeiten, was an seiner Lösung anders und vermeintlich besser bzw. innovativer als bei Wettbewerbern oder bestehenden Lösungen ist.[326]

Gerade in dem sich schnell verändernden und innovativen Feld der IT-Sicherheit werden Methoden der **innovativen Beschaffung** (wie zum Beispiel PCP) bislang noch ungenügend angewandt. Sie durchzusetzen ist eine politische Leitungsaufgabe. Dies gilt auch für eine Öffnung zumindest europäischer Märkte für die deutsche IT-Sicherheitswirtschaft. Die Schaffung eines einheitlichen EU-Binnenmarktes, auch im Bereich von Cybersicherheits-Produkten und –Dienstleistungen wäre ein wichtiger Beitrag, um international wettbewerbsfähige Anbieter in Europa zu schaffen. Gerade in einem Feld, das so stark von Skaleneffekten geprägt ist, ist **Marktgröße** ein erheblicher Wettbewerbsfaktor. Dieser Gedanke muss auch bei der Umsetzung der *dual-use*-Exportkontrolle stärker Beachtung finden.

Auch wenn Digitalisierung die Bedeutung von Grenzen und geographischer Entfernung weitgehend verschwinden lässt, sind Forschung und Entwicklung in diesem Bereich weiter ein von Menschen getriebenes Geschäft. Der persönliche Austausch und Nähe spielen eine wichtige Rolle, da von ***Spillover*-Effekten** alle Mitglieder in IT-Clustern profitieren. Dies gilt in gleichem Maße auch für den Bereich der Cybersicherheit. Aus sicherheitspolitischer Perspektive, wie aus Gründen der internationalen Wettbewerbsfähigkeit, sind die bestehenden Cluster in Deutschland zu stärken, statt neue Institutionen aus strukturpolitischen Erwägungen räumlich

[326] Vgl. Informationsasymmetrien bei IT-SP

fern von diesen anzusiedeln. Dies gilt umso mehr aufgrund des ohnehin bestehenden Mangels an qualifiziertem Personal.

Im politischen Umgang mit der Sicherheitswirtschaft besteht ein immer wiederkehrender Konflikt zwischen einer **sicherheitspolitischen Sicht** einerseits und einer **wirtschaftspolitischen Sicht** andererseits. Während letztere ihren Erfolg in Wachstum, Gewinn und Arbeitsplätzen misst, hat die Sicherheitspolitik immer das Problem, wie sie ihren Erfolg unter Beweis stellen kann. Hier besteht der eigentliche Erfolg darin, wenn eben nichts Messbares passiert. Es bleibt aber das grundlegende Problem des Risikomanagements: „there is no glory in prevention".[327]Aus sicherheitspolitischen Erwägungen gibt es ein Interesse an einer leistungsfähigen deutschen IT-Sicherheitswirtschaft in ihrer Funktion als vertrauensvoller Vorleister bzw. Zulieferer für die Arbeit der Behörden. Es gibt aber zugleich ein Interesse daran, dass der Zugriff auf diese Fähigkeiten begrenzt und kontrollierbar bleibt. Widersacher sollen möglichst nicht die gleichen Möglichkeiten haben, wie man selbst.

Für weit verbreitete IT-Lösungen wünschen sich Sicherheitspolitiker oft technische Hintertüren, um sie bei Bedarf für Kriminalitätsbekämpfung und Informationsbeschaffung einsetzen zu können. Für den internationalen Markterfolg sind hingegen gerade das im internationalen Vergleich besonders hohe deutsche Datenschutzniveau und die glaubhafte Kontrolle des Käufers über die eigenen Daten ein wichtiges Verkaufsargument, das deutschen IT-Sicherheitsanbietern einen Wettbewerbsvorteil gegenüber ausländischen Konkurrenten bietet. In dieser Frage erscheint eine politische Abwägung und Entscheidung bzw. grundsätzliche Weichenstellung derzeit noch möglich.

Zwingend erscheint für die Erschaffung einer innovativen, international konkurrenzfähigen IT-Sicherheitsbranche im Inland das Bestehen einer hinreichenden Marktgröße. Der deutsche Markt ist in vielen Produkt- und Softwarebereichen zu klein, um von Skaleneffekten ausreichend Gebrauch zu machen. Wer für den Hochsicherheitsbereich eine Lösung will, die sonst kein anderer haben soll, der muss den Maßanzug zum entsprechenden Preis bei der anwendungsorientierten Wissenschaft und den FuE-starken Unternehmen bestellen. Letztere gibt es aber nur, wenn sie in anderen Geschäftsfeldern der IT-Sicherheit ausreichend große Märkte finden, auf denen sie erfolgreich agieren können. Diese Studie liefert hoffentlich einen Beitrag und Impulse, damit dies in Zukunft besser gelingt.

[327] Gibbs & Duffy 2013.

Anhang

Methodisches Vorgehen

Für die Durchführung der Studie „Cybersicherheit als Katalysator für Innovationen“ wurde zunächst eine umfassende Literatur- und Dokumentanalyse vorgenommen. Zur Validierung und Vertiefung der so gewonnenen Ergebnisse wurde von unterschiedlichen Methoden Gebrauch gemacht:

1. 25 semi-strukturierte Experteninterviews;
2. ergänzende Online-Befragung;
3. Themenrelevante Workshops mit Experten zum Schließen verbleibender Wissenslücken.

Wir hoffen, dass viele der von uns berichteten Ergebnisse mit anderen Methoden untermauert werden können, z.B. durch die Durchführung strukturierterer Interviews, die auf Basis der hier vorliegenden vorläufigen Ergebnisse zielgerichtet weiterentwickelt werden können.

1. 25 Semi-strukturierte Experteninterviews

Im Rahmen der Studie wurden insgesamt **25 Experten aus Deutschland** befragt. Angesichts eines noch jungen Forschungsfelds, dem grundsätzlichem Mangel an Daten zum Forschungsgegenstand, der Orientierung an wissenschaftlichen Best-Practices sowie der höheren Aussagekraft von implizitem bzw. qualitativem Wissen, erschien diese Herangehensweise als besonders geeignet für die Untersuchung der vorher aus der Literatur- und Dokumentanalyse identifizierten Forschungsfragen.

Der Expertenpool wurde in drei Gruppen aufgeteilt:

A. Experten aus Wissenschaft sowie Anbieter von Cybersicherheitsprodukten und -dienstleistungen;
B. Privatwirtschaftliche Nachfrager von Cybersicherheitsprodukten und -dienstleistungen;
C. Regulierer, staatliche Stellen, Verbände, Initiativen privater Unternehmen.

Die Befragten wurden über das bestehende Netzwerk des BIGS identifiziert; anschließend wurde der Expertenpool um Empfehlungen weiterer Experten, insbesondere aus dem BDI-Ausschuss für Wirtschaftsschutz und Cybersicherheit ergänzt. Hierbei wurde eine möglichst gleichmäßige Verteilung der Gruppen angestrebt.

Die Fragen wurden mehreren **Themenblöcken** zugeteilt und je nach Expertengruppe (die Fragebögen entsprechend angepasst):

- Einordnung des Einflusses von Cybervorfällen
- Lokalisierung notwendiger Sicherheitsmaßnahmen
- Auswirkungen von Cybervorfällen auf die Investitionstätigkeit
- Wachstum des Cybersicherheitsmarktes
- Anreize, um Innovationen im Cybersicherheitsbereich zu fördern
- Beschaffungsstrategien von Behörden und Militär als Förderung des Wachstums der deutschen Branche
- Cybersicherheitsinnovationen in Israel, USA, UK

Die Interviews wurden entweder **persönlich oder telefonisch** von einem oder zwei BIGS-Mitarbeitern im Zeitraum vom 23. Mai bis 1. August 2019 durchgeführt, in Ausnahmefällen wurden auch schriftliche Antworten akzeptiert. Jedes Interview dauerte zwischen **30 Minuten und einer Stunde; die Identität der Gesprächspartner** wird vertraulich behandelt. Zu Beginn jedes Interviews wurde um eine Einverständniserklärung gebeten, die Ergebnisse anonymisiert für den genannten Studienzweck nutzen zu dürfen. Die Antworten wurden anschließend transkribiert und kodiert, um sie dann konsolidiert in die Studie einfließen lassen zu können.

Der **Vorteil** von semi-strukturierten Interviews besteht darin, dass gerade Kontextinformationen detailliert erörtert werden können, was mit einem strukturierten Befragungsinstrument nicht ohne Weiteres möglich ist. Es setzt nicht voraus, wie die Antworten auf Fragen strukturiert sein sollen, und ermöglicht somit eher, neue und unerwartete Erkenntnisse zu gewinnen. Der **Nachteil** der semi-strukturierten Methode besteht darin, dass die kontextuellen Ergebnisse nicht unbedingt auf den gesamten Tätigkeitsbereich der Interviewten übertragen werden können, sodass Ergebnisse eher als explorativ interpretiert werden müssen.[328] Somit werden zwangsläufig Abstriche bei der externen Validität in Kauf genommen.

[328] Vgl. Moore et al. 2015.

2. Online-Befragung (abgeschlossene Teilnahmen: n=34)

Da nach Abschluss der Experteninterviews die Perspektive der privatwirtschaftlichen Nachfrager von Cybersicherheits-Produkten und –Dienstleistungen nicht ausreichend Berücksichtigung fand, wurde im Zeitraum von einem Monat (5. bis 31. August 2019) eine ergänzende Online-Befragung mit diesem Personenkreis durchgeführt.

Im Rahmen der Online-Umfrage, wurden wie bei den semi-strukturierten Interviews, die Fragen in mehrere **Themenfelder** eingeteilt:

- Marktversagen und Regulierung
- Staatliche Betreiber als Treiber von Innovationen
- Staatliche Investitionen und öffentliche Beschaffungsstrategien
- Verbesserung und Anreize
- Forschungsförderung
- Humankapital
- Hemmnisse Einführung
- Verzögerung Digitalisierungsprojekte

Der Verzicht auf eine explorative und angepasste Interviewführung führte zu einem reduzierten Aufwand - im Vergleich zu den mündlichen Interviews - für die Befragten. Die Bearbeitung dauerte im Regelfall nicht länger als **15 Minuten**. Jeder Themenblock konnte auch schriftlich kommentiert werden, sodass die Kommentare anschließend, mit den Interviewergebnissen im Codierungsbericht entsprechend abgeglichen werden konnten. Die Online-Umfrage zielte insbesondere darauf ab, Thesen, die sich aus den Experteninterviews herauskristallisiert haben, einer größeren Gruppe zur Abstimmung vorzulegen.

Der **Vorteil** der strukturierten Befragungsform ist die geringere Bearbeitungszeit für die Befragten (und somit eine erhöhte Rücklaufquote), sowie die automatisierte Auswertung über das verwendete Befragungstool (*Sociolutions*). Der **Nachteil** besteht darin, dass bestimmten Aspekten nicht zielgerichtet nachgegangen werden kann und Ergebnisse viel Raum für Interpretation lassen. Bereits im Rahmen der semi-strukturierten Interviews konnte festgestellt werden, dass sich die Experten bei einigen Punkten nicht ganz einig waren bzw. binäre Ja-Nein Antworten nicht abzurufen waren. Dies spiegelte sich auch bei der nachfolgenden Erhebung über

das Befragungstool wider: Bei vielen der Fragekomplexe liegt im Rahmen einer gewissen Variation über mehrere Prozentpunkte, eine annähernd hälftige Verteilung von Zustimmung (trifft zu / trifft eher zu) und Ablehnung (trifft nicht zu / trifft eher nicht zu) der Fragestellungen vor. Die Deskriptivdaten laden bei diesen Fragen nicht zu belastbaren Schlussfolgerungen ein.

3. Workshops mit Experten zu Themenvertiefung

Nach Durchführung aller Experteninterviews und der Online-Befragung wurden die Ergebnisse in einem Workshop der Expertenkommission Forschung und Innovation, den Befragten und weiteren Experten präsentiert und diskutiert (Seminar mit der EFI-Kommission am 20. August 2019 in Berlin). Darüber hinaus wurden themenrelevante Workshops genutzt, um noch verbleibende Wissenslücken mit Hilfe von vertiefenden Fragebögen näher zu erörtern (Seminar "CyberFactory#1 – *Use and Misuse Cases*" am 23.10.2019 in Berlin).

Literaturverzeichnis

Ablon, L. und Libicki, M. (2015), Hackers' Bazaar: The Markets for Cybercrime Tools and Stolen Data. In: Defense Counsel Journal; Chicago Bd. 82, Ausg. 2, 143-152.

Akerlof, G. A. (1970), The Market of the Lemons: Quality, Uncertainty, and the Market Mechanism. In: Quarterly Journal of Economics 84, S. 488–500.

Anderson, R. (2001), Why Security is Hard. An Economic Perspective, Proceedings of 17th Annual Computer Security Applications Conference (ACSAC), New Orleans, La. Dec. 10–14.

Anderson, R. und Moore, T. (2006), The Economics of Information Security, *Science* (27 October 2006) 314, S. 610–613.

Anderson, R. und Moore T. (2007), The Economics of Information Security: A survey and open questions. In: Fourth bi-annual Conference on the Economics of the Software and Internet Industries, January 2007.

Anderson, R., Moore, T., Nagaraja, S. und Ozment, A. (2007), Incentives and Information Security, in: Nisan, N., Roughgarden, T., Tardos, E. und Vazirani, V. (Hg.), Algorithmic Game Theory, chapter 25. Cambridge University Press.

Arts, S. (2018), Offense as the New Defense: New Life for NATO's Cyber Policy. In: German Marshall Fund (GMF), vom 13.12.2018. URL: http://www.gmfus.org/publications/offense-new-defense-new-life-natos-cyber-policy, [zuletzt abgerufen am 01.08.2019].

Avast Threat Landscape Report 2019, Predictions, URL: https://press.avast.com/hubfs/media-materials/kits/2019-Predictions-Report/Avast%20Threat%20Landscape%20Report%202019.pdf?hsLang=en, 2019, [zuletzt abgerufen am 11.09.2019].

Barczok, A. (2017), Trojaner im OP - wie ein Krankenhaus mit den Folgen lebt. In: Heise Online, vom 05.02.2017. URL: https://www.heise.de/newsticker/meldung/Trojaner-im-OP-wie-ein-Krankenhaus-mit-den-Folgen-lebt-3617880.html, [zuletzt abgerufen am 22.08.2019].

Bartsch, M., und Frey St. (2017), Cyberstrategien für Unternehmen und Behörden, Wiesbaden: Springer Vieweg.

Bauer, J.M., und M. J. G. van Eeten (2009), Cybersecurity: stakeholder incentives, externalities, and policy options. Telecomm. Policy 33(10–11), S. 706–719.

Bayerisches E-Government-Gesetz – BayEGovG (2015), Gesetz über die elektronische Verfassung in Bayern vom 22. Dezember 2015, URL: https://www.gesetze-bayern.de/Content/Document/BayEGovG, [zuletzt abgerufen am 19.08.2019]

Becker, G. S. (1968), Crime and Punishment. An Economic Approach, *Journal of Political Economy* 76, S. 169–217.

Bendovschi, A. (2015), Cyber-attacks—trends, patterns and security countermeasures, Procedia Econ. Financ. 28, S. 24–31.

Bergstrom, T. C., und Goodman, R. P. (1973), Private Demands for Public Goods, *American Economic Review*, 63, S. 280–296.

Berke, J. (2019), Wie die Politik „made in Germany“ in der IT ausbremst. In: Wirtschaftswoche vom 30.06.2019, URL: https://www.wiwo.de/my/unternehmen/it/digitale-autarkie-wie-die-politik-made-in-germany-in-der-it-ausbremst/24498718.html?ticket=ST-45774905-Pr0za2VC6Sc0rsUGp5Ob-ap2, [zuletzt abgerufen am 19.07.2019].

Bertschek, I., Ohnemus, J., und Viete, S. (2018), The ZEW ICT survey 2002 to 2015: Measuring the digital transformation in German firms. Jahrbücher für Nationalökonomie und Statistik, 238(1), 87-99.

Biener, C., Eling, M., Wirfs, J. H. (2015), Insurability of cyber risk: an empirical analysis, Geneva Pap. Risk Insur. Issues Pract. 40(1), S. 131–158.

BIGS [Brandenburgisches Institut für Gesellschaft und Sicherheit] (2017), Cyberversicherungen als Beitrag zum IT-Risikomanagement – Eine Analyse der Märkte für Cyberversicherungen in Deutschland, der Schweiz, den USA und Großbritannien. Brandenburgisches Institut für Gesellschaft und Sicherheit (BIGS) – Standpunkt zivile Sicherheit Nr. 8.

Bitkom [Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V.] (2015), Spionage, Sabotage und Datendiebstahl – Wirtschaftsschutz im digitalen Zeitalter, Bitkom e. V., Berlin.

Bitkom (2018a), Spionage, Sabotage und Datendiebstahl – Wirtschaftsschutz in der Industrie, Bitkom e. V., Berlin.

Bitkom (2018b), Markt für IT-Sicherheit erstmals über 4 Milliarden Euro. In: Bitkom Pressebereich, vom 09.10.2018. URL: https://www.bitkom.org/Presse/Presseinformation/Markt-fuer-IT-Sicherheit-erstmals-ueber-4-Milliarden-Euro.html, [zuletzt abgerufen am 06.05.2019].

Bitkom (2018c), 82.000 freie Jobs: IT-Fachkräftemangel spitzt sich zu. In Bitkom Pressebereich, vom 13.12.2018. URL: https://www.bitkom.org/Presse/Presseinformation/82000-freie-Jobs-IT-Fachkraeftemangel-spitzt-sich-zu, [zuletzt abgerufen am 01.09.2019].

Bitkom (2019), Ausbildung zum IT-Sicherheitsbeauftragten (ITSiBe)/Chief Information Security Officer (CISO). In: Bitkom Akademie. URL: https://www.bitkom-akademie.de/seminare/it-sicherheitsbeauftragter-itsibe, [zuletzt abgerufen am 01.10.2019].

BKA [Bundeskriminalamt] (2015), Hacktivisten – Abschlussbericht zum Projektteil der Hebelforschung. Kriminalistisches Institut Forschungs- und Beratungsstelle Cybercrime KI 16.

BKA (2014), Cybercrime. Bundeslagebild 2013, Wiesbaden.

BKA (2015), Cybercrime. Bundeslagebild 2014, Wiesbaden.

BKA (2016), Cybercrime. Bundeslagebild 2015, Wiesbaden.

BKA (2017), Cybercrime. Bundeslagebild 2016, Wiesbaden.

BKA (2018), Cybercrime. Bundeslagebild 2017, Wiesbaden.

Blind, K., Petersen, S. S., und Riillo, C. A. F. (2017), The impact of standards and regulation on innovation in uncertain markets. Research Policy 46 (1) pp. 249-264.

BMBF [Bundesministerium für Bildung und Forschung] (2019a), Kompetenzatlas zur Sicherheitsforschung in Deutschland, URL: www.securityresearchmap.de [zuletzt abgerufen am 30.10.2019].

BMBF (2019b), Informationsbrief zur zivilen Sicherheitsforschung, URL: https://www.sifo.de/files/Informationsbrief_zur_zivilen_Sicherheitsforschung_04_2019.pdf, [zuletzt abgerufen am 30.10.2019].

BMWi [Bundesministerium für Wirtschaft und Energie] (2012), Analyse von Wachstumshemmnissen kleiner und mittlerer Unternehmen am Beispiel der IT-Branche, Studie im Auftrag des BMWi, Endbericht 2012, Berlin.

BMWi (2017), Innovative öffentliche Beschaffung, Leitfaden 2 Auflage 2017, Berlin.

BMWi (2019a), Soziale Marktwirtschaft stärken – Wachstumspotenziale heben, Wettbewerbsfähigkeit erhöhen, Jahreswirtschaftsbericht 2019, Berlin.

BMWi (2019b), Von der Idee zum Markterfolg: Programme für einen innovativen Mittelstand, Berlin.

Böhm, M. (2017), Telekom-Hacker zu Bewährungsstrafe verurteilt. In: Spiegel Online, vom 28.07.2017. URL: https://www.spiegel.de/netzwelt/netzpolitik/telekom-hack-brite-in-koeln-zu-bewaehrungsstrafe-verurteilt-a-1160149.html, [zuletzt abgerufen am 01.09.2019].

Bretschneider, W., Freytag, A., Rieckmann, J. und Stuchtey, T. (2018), Sicherheitsverantwortung zwischen Markt und Staat, BIGS-Studie 2018.

Bretschneider, W., Freytag, A., Rieckmann, J. und Stuchtey, T. (2020), Sicherheitsverantwortung zwischen Staat und Markt – eine institutionenökonomische Analyse, ORDO Band 70: Heft1.

BSI [Bundesamt für Sicherheit in der Informationstechnik] (2017), Die Lage der IT-Sicherheit in Deutschland 2017, URL: www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2017.pdf%3F__blob%3DpublicationFile%26v%3D4+&cd=1&hl=de&ct=clnk&gl=de, [zuletzt abgerufen am 07.07.2019).

BSI (2018), Die Lage der IT-Sicherheit in Deutschland 2018, URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2018.pdf;jsessionid=DD1BDC48FC3AB78118B32652671C926F.2_cid360?__blob=publicationFile&v=6, [zuletzt abgerufen am 07.07.2019].

BSI und ACS [Allianz für Cybersicherheit] (2018), Cybersicherheits-Umfrage 2017. Cyberrisiken, Meinungen und Maßnahmen, URL: https://www.allianz-fuer-Cybersicherheit.de/ACS/DE/Informationspool/Cybersicherheits-Umfrage/CybersicherheitsUmfrage_2018/umfrage_2018.html?nn=12243794&cms_pos=7, [zuletzt abgerufen am 03.07.2019].

BSI und ACS (2019), Cybersicherheits-Umfrage – Cyberrisiken & Schutzmaßnahmen in Unternehmen. Betrachtungszeitraum 2018, URL: https://www.allianz-fuer-Cybersicherheit.de/ACS/DE/Informationspool/Cybersicherheits-Umfrage/CybersicherheitsUmfrage_2018/umfrage_2018.html?nn=12243794&cms_pos=7, [zuletzt abgerufen am 02.07.2019].

BSI (2019), Die Lage der IT-Sicherheit in Deutschland 2019, URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2019.pdf?__blob=publicationFile&v=6, [zuletzt abgerufen am 28.10. 2019].

Bundesagentur für Arbeit (2019), IT-Fachleute, Berichte: Blickpunkt Arbeitsmarkt, April 2019.

Burgi, M. (2007), Vom Grundrecht auf Sicherheit zum Grundrecht auf Opferschutz, in: O. Depenheuer, M. Heintzen, M. Jestaedt und P. Axer (Hg), *Staat im Wort. Festschrift für Josef Isensee*, Heidelberg: C. F. Müller, S. 655–665.

Camillo, M. (2017), Cyber risk and the changing role of insurance, J. Cyber Policy 2(1), S. 53–63.

CAPEC (Common Attack Pattern Enumeration and Classification) List – 403: Social Engineering (Version 3.1), URL: https://capec.mitre.org/data/definitions/403.html, [zuletzt abgerufen am 01.10.2019].

Cisco Reihe zur Cybersicherheit 2019. URL: https://gblogs.cisco.com/de/neuer-cisco-cybersecurity-report-2019-was-sind-die-wirklichen-zukunftigen-trends/, [zuletzt abgerufen am 29.10.2019].

Clotfelter, Ch. T. (1977), Public Services, Private Substitutes, and the Demand for Protection against Crime, *The American Economic Review* 67 (5), S. 867–877.

Coase, R. H. (1937), The Nature of the Firm, *Economica* 4, S. 386–405.

Cohen, N., Hulvey, R., Mongkolnchaiarunya, J., und Novak, A., with Morgus, R., & Segal, A. (2017), Cybersecurity as an Engine for Growth. New America.

CyberPedia, What is Machine Learning?. In: Palo Alto Networks, URL: https://www.paloaltonetworks.com/cyberpedia/what-is-machine-learning, [zuletzt abgerufen am 02.10.2019].

Deloitte Cyber Security Report 2019, URL: https://www2.deloitte.com/de/de/pages/risk/articles/cyber-security-report.html, [zuletzt abgerufen am 15.10.2019].

Dimico, A., Isopi, A. und Olsson, O. (2017), Origins of the Sicilian Mafia. The Market for Lemons, *The Journal of Economic History* 77 (4), S. 1083–1115.

DIN/DKE Roadmap (2017), Deutsche Normungs-Roadmap IT-Sicherheit, Version 3, URL: https://www.dke.de/resource/blob/778258/44e2d336c2702f285ba669ee5cd47b10/deutsche-normungs-roadmap-it-sicherheit-version-3-0-data.pdf, [zuletzt abgerufen am 01.09.2019].

Donges, J. B., und Freytag, A. (2009), Allgemeine Wirtschaftspolitik, 3. A., Stuttgart: Lucius & Lucius.

DESTATIS [Statistisches Bundesamt] (2019), Bildung und Kultur Studierende an Hochschulen, Sommersemester 2018, Fachserie 11 Reihe 4.1.

Ehrlich, I. (1996), Crime, Punishment, and the Market for Offenses, Journal of Economic Perspectives 10 (1), S. 43–67.

Ehrlich, I., und Becker, G. S. (1972), Market-Insurance, Self-Insurance, and Self-Protection, *Journal of Political Economy* 80 (4), S. 623–648.

ENISA (2018), Analysis of the European R&D priorities in cybersecurity. Strategic priorities in cybersecurity for a safer Europe. ISBN: 978-92-9204-278-3, doi: 10.2824/14357.

ETFMG (2019), Hack: ETFMG Prime Cyber Security ETF, ISIN US26924G2012, vom 30.09.2019. URL: https://etfmg.com/wp-content/uploads/2019/03/HACK-FactSheet-2019-Q3-2019-10-21.pdf, [zuletzt abgerufen am 08.10.2019].

Fallick, B., Fleischman, C. A., and Rebitzer, J. B. (2006), Job-Hopping in Silicon Valley: Some Evidence Concerning the Micro-foundations of a High-Technology Cluster. The Review of Economics and Statistics 88, no. 3: 472–81.

FireEye M-Trends 2019, URL: https://content.fireeye.com/m-trends-de/rpt-m-trends-2019-de, [zuletzt abgerufen am 17.10.2019].

Fritsch, M. (2014), Marktversagen und Wirtschaftspolitik: Mikroökonomische Grundlagen staatlichen Handelns. Vahlen.

Fritsch, M. (2018), Marktversagen und Wirtschaftspolitik. Mikroökonomische Grundlagen staatlichen Handelns, 10. A., München: Vahlen.

Frost und Sullivan (2017), 2017 Global Information Security Workforce Study: Benchmarkin Workforce Capacity and Response to Cyber Risk, Center for Cyber Safety and Education, ISC. URL: https://www.isc2.org/-/media/B7E003F79E1D4043A0E74A57D5B6F33E.ashx, [zuletzt abgerufen am 01.10.2019].

Fruhlinger, J. (2017), What is Stuxnet, who created it and how does it work?. In: CSO vom 22.08.2017. URL: https://www.csoonline.com/article/3218104/what-is-stuxnet-who-created-it-and-how-does-it-work.html [zuletzt abgerufen am 01.08.2019].

Gawel, E. (2009), Grundzüge der mikroökonomischen Theorie, Lohmar.

GDV [Gesamtverband der deutschen Versicherungswirtschaft] (2017), URL: https://www.gdv.de/resource/blob/6100/d4c013232e8b0a5722b7655b8c0cc207/01-allgemeine-versicherungsbedingungen-fuer-die-Cyberrisiko-versicherung--avb-cyber--data.pdf, [zuletzt abgerufen am 01.10.2019].

GDV (2019a), URL: https://www.gdv.de/resource/blob/48506/a1193bc12647d526f75da3376517ad06/Cyberrisiken-im-mittelstand-2019-pdf-data.pdf, [zuletzt abgerufen am 01.10.2019].

GDV (2019b), URL: https://www.gdv.de/de/themen/news/-wir-werden-die-Cyberversicherung-als-einen-standard-sehen--44082, [zuletzt abgerufen am 01.10.2019].

Gibbs, N. und Duffy, M. (2013), The Presidents Club: Inside the World's Most Exclusive Fraternity. New York: Simon & Schuster.

Gill, M. (2017), Exploring Some Contradictions of Modern-Day Security (chapter 44). In: Ders. (Hg.), *Handbook of Security*, Basingstoke: Palgrave Macmillan, S. 980–1000.

Haack, A. (2019), Bund plant Einstiegsprämien und Zulagen für den IT-Bereich. In: Behörden-Spiegel, vom 23.07.2019. URL: https://www.behoerden-spiegel.de/2019/07/23/bund-plant-einstiegspraemien-und-zulagen-fuer-den-it-bereich/, [zuletzt abgerufen am 06.09.2019].

Hayek, F. A. von (1945), The Use of Knowledge in Society, *American Economic Review* 35 (4), S. 519–530.

Heuer, F. (2018), Deutscher Security-Markt wächst stark. In: Computerwoche, vom 12.11.2018. URL: https://www.computerwoche.de/a/deutscher-security-markt-waechst-stark,3546021, [zuletzt abgerufen am 06.05.2019].

Hering, A. (2018), Der Arbeitsmarkt für Fachkräfte in Bereich Cybersicherheit gewinnt weiter an Bedeutung. In: Indeed Hiringlab.org, vom 02.03.2018. URL: https://www.hiringlab.org/de/blog/2018/03/02/der-arbeitsmarkt-fur-fachkraefte-im-bereich-Cybersicherheit-gewinnt-weiter-an-bedeutung/, [zuletzt abgerufen am 15.05.2019].

Herpig, S. und Bredenbrock, C. (2019), Cybersicherheits-politik in Deutschland: Akteure, Aufgaben und Zuständigkeiten, Stiftung Neue Verantwortung, URL: https://www.stiftung-nv.de/sites/default/files/cybersicherheitspolitik_in_deutschland.pdf, [zuletzt abgerufen am 02.09.2019]

Hillebrand, A., Niederprüm, A., Schäfer S. und Thiele S. (2017), Aktuelle Lage der IT-Sicherheit in KMU. Kurzfassung der Ergebnisse der Repräsentativbefragung, Wissenschaftliches Institut für Infrastruktur und Kommunikationsdienste (wik). URL: https://www.wik.org/fileadmin/Sonstige_Dateien/IT-Sicherheit_in_KMU/Aktuelle_Lage_der_IT-Sicherheit_in_KMU_-_WIK.pdf, [zuletzt abgerufen am 05.09.2019].

Hirshleifer, J. (1980). Privacy: Its origin, function, and future. The Journal of Legal Studies, 9(4), 649-664.

Höpner, A. und Kerkmann, C. (2019), Siemens, Daimler, Airbus, Telekom, Tüv: Allianz für Cyber-Sicherheit findet immer mehr Mitglierder. In: Handelsblatt, vom 15.02.2019. URL: https://www.handelsblatt.com/unternehmen/it-medien/charter-of-trust-siemens-daimler-airbus-telekom-tuev-allianz-fuer-cyber-sicherheit-findet-immer-mehr-mitglieder/23988808.html?ticket=ST-62409488-sG47D7jdLRBTifbli0CG-ap3, [zuletzt abgerufen am 20.10.2019].

IBM (2019), X-Force Threat Intelligence Index 2019, URL: https://www.securindex.com/downloads/8b9f94c46a70c60b229b04609c07acff.pdf, [zuletzt abgerufen am 01.08.2019].

Institute of Risk Management (2014), Cyber Risk: Resources for Practitioners, URL: https://www.theirm.org/media/7237/irm-cyber-risk-resources-for-practitioners.pdf, [zuletzt abgerufen am 01.09.2019].

ISG Information Services Group (2018), Der deutsche IT-Security-Markt legt bis 2020 um mehr als 15 Prozent zu, URL: https://www.all-about-security.de/security-artikel/management-und-strategie/single/isg-der-deutsche-it-security-markt-legt-bis-2020-um-mehr-als/, 28.09.2018, [zuletzt abgerufen am 30.10.2019].

Ilg, P. (2019), IT-Gehälter: Security-Experten werden am besten bezahlt. In: Heise Online, vom 09.02.2019. URL: https://www.heise.de/newsticker/meldung/IT-Gehaelter-Chef-sollte-man-sein-4303057.html, [zuletzt abgerufen am 26.09.2019].

Isensee, J. (1983), Das Grundrecht auf Sicherheit. Zu den Schutzpflichten des freiheitlichen Verfassungsstaates, Berlin, New York: De Gruyter.

Johnston, L., und Shearing C. D., (2013), *Governing Security: Explorations of Policing and Justice*, London: Routledge.

Jouini, M., Rabai, L. B. A. und Aissa A. B. (2014), Classification of security threats. In: Information systems, Procedia Comput. Sci. 32, S. 489–496.

Jordan, T., und Taylor, P. (2004). Hacktivism and cyberwars: Rebels with a cause? Routledge.

Kim, W., Jeong, O. R., Kim, C. und So, J. (2011), The dark side of the Internet: attacks, costs and responses. Inf. Syst. 36(3), S. 675–705.

Kleinhans, J. P. (2018), Standardisierung und Zertifizierung zur Stärkung der internationalen IT-Sicherheit, Stiftung Neue Verantwortung, URL: https://www.stiftung-nv.de/sites/default/files/standardisierung_und_zertifizierung.pdf, [zuletzt abgerufen am 12.09.2019].

Koch, P. (2012), Die Geschichte der Versicherungswirtschaft in Deutschland, VVW GmbH.

Koalitionsvertrag (2018), Koalitionsvertrag zwischen CDU, CSU und SPD, Ein neuer Aufbruch für Europa. Eine neue Dynamik für Deutschland. Ein neuer Zusammenhalt für unser Land, 19. Legislaturperiode, URL: https://www.bundesregierung.de/resource/blob/975226/847984/5b8bc23590d4cb2892b31c987ad672b7/2018-03-14-koalitionsvertrag-data.pdf#page=159, [zuletzt abgerufen am 02.09.2019].

KPMG AG Wirtschaftsprüfungsgesellschaft (2017), e-Crime in der deutschen Wirtschaft 2017 – Computerkriminalität im Visier. URL: http://hub.kpmg.de/hubfs/LandingPages-PDF/e-crime-studie-2017-KPMG.pdf, [zuletzt abgerufen 07.05.2019].

KPN et al. (2018), European Cyber Security Perspectives 2017. URL: https://overons.kpn/content/downloads/news/European-Cyber-Security-Perspectives-2018.pdf, [zuletzt abgerufen am 01.09.2019].

Krämer, N. und Dahmen, U. (2017), Trojaner im KIS. In: BibliomedManager, vom 01.01.2017. URL: https://www.bibliomedmanager.de/zeitschriften/fw/heftarchiv/ausgabe/artikel/fw-1-2017-crime/31425-trojaner-im-kis/, [zuletzt abgerufen am 22.08.2019].

Kroker, M. (2019), Die Hälfte der IT-Security-Teams in Deutschland ist Cyberkriminellen nicht gewachsen. In: Kroker's Lool @ IT, vom 22.07.2019. URL: https://blog.wiwo.de/look-at-it/2019/07/22/die-haelfte-der-it-security-teams-in-deutschland-ist-Cyberkriminellen-nicht-gewachsen/, [zuletzt abgerufen am 01.08.2019].

Kubovič, O., (2019), Machine-Learning Era in Cybersecurity: A Step Towards a Safer World or the Brink of Chaos?. In: ESET, URL: https://www.welivesecurity.com/wp-content/uploads/2019/02/ESET_MACHINE_LEARNING_ERA.pdf, 2019, [zuletzt abgerufen am 09.10.2019].

Kurz, H. D., Schütz, M., Strohmaier, R. und Zilian, St. (2018), Riding a new wave of innovations. A long-term view at the current process of creative destruction, *Wirtschaft und Gesellschaft* 44 (4), S. 545–583.

Liedtke, D. (2017), Diagnose Hackerangriff: Wie Cyberattacken deutsche Kliniken lahmlegen. In: Stern, vom 27.11.2017. URL: https://www.stern.de/gesundheit/krankenhaus/hackerangriff--wie-Cyberattacken-deutsche-kliniken-lahmlegen-7762362.html, [zuletzt abgerufen am 22.08.2019].

Locke, J. (1689), Two Treatises of Government, hrsg. von *Peter Laslett*, Cambridge: Cambridge University Press 1988, S. 330-349.

Ludwig, K. (2016), Wenn Cyberkriminelle ein Krankenhaus lahmlegen. In: Süddeutsche Zeitung, vom 20.03.2016. URL: https://www.sueddeutsche.de/digital/angriff-auf-klinik-das-comeback-des-klemmbretts-1.2912255-0#seite-2, [zuletzt abgerufen am 01.09.2019].

Manky, D. (2013), Cybercrime as a service: A very modern business. In: Computer Fraud and Security 2013(6), 9–13.

Marvan, P. (2017), NotPetya-Attacke kostet Pharmakonzern Merck über 600 Millionen Dollar. In: Silicon, vom 30.10.2017. URL: https://www.silicon.de/41662161/notpetya-attacke-kostet-pharmakonzern-merck-ueber-600-millionen-dollar, [zuletzt abgerufen am 16.10.2019].

McAfee (2018). The Economic Impact of Cybercrime: No Slowing Down. Center for Strategic and International Studies.

Meister, A., und Biselli, A. (2019a), Bundesrechnungshof bezweifelt Sinn der neuen Cyberagentur. In: Netzpolitik.org, vom 03.07.2019, URL: https://netzpolitik.org/2019/bundesrechnungshof-bezweifelt-sinn-der-neuen-cyberagentur/#2019-06-18_Bundesrechnungshof_Cyberagentur, [zuletzt abgerufen am 26.09.2019].

Meister, A., und Biselli, A. (2019b), Geheimes Bundestagsgutachten attackiert Hackback-Pläne der Bundesregierung. In: Netzpolitik.org, vom 03.09.2019, URL: https://netzpolitik.org/2019/geheimes-bundestagsgutachten-attackiert-hackback-plaene-der-bundesregierung/, [zuletzt abgerufen am 26.09.2019].

Mirian, A., DeBlasio, J., Savage, S., Voelker, G.M., und Thomas, K. (2019), Hack for Hire: Exploring the Emerging Market for Account Hijacking. In: Proceedings of the World Wide Web Conference, S. 1273–1289, URL: https://www.sysnet.ucsd.edu/~voelker/pubs/hackforhire-www19.pdf, [zuletzt abgerufen am 16.10.2019].

Moore, T. (2010a), Introducing the Economics of Cybersecurity: Principles and Policy Options, Poceedings of a Workshop on Deterring CyberAttacks: Informing Strategies and Developing Options for U.S: policy.

Moore, T. (2010b), The economics of cybersecurity: principles and policy options, Int. J. Crit. Infrastruct. Prot. 3(3–4), S. 103–117.

Moore, T., Dynes, S., und Chang, F. R. (2015), Identifying how firms manage cybersecurity investment. In: Southern Methodist University, vom 28.10.2015. URL: http://blog.smu.edu/research/files/2015/10/SMU-IBM.pdf [zuletzt abgerufen am 14.08.2019].

Mulligan, D. K. und Schneider, F. B. (2011), Doctrine for cybersecurity. Daedalus, 140(4), 70-92.

Nagel, L. M. (2017), „Spiderman“ gesteht Cyberangriff. In: Handelsblatt, vom 21.07.2017. URL: https://www.handelsblatt.com/unternehmen/it-medien/1-2-millionen-telekom-router-angegriffen-spiderman-gesteht-Cyberangriff/20091186.html, [zuletzt abgerufen am 01.09.2019].

Peteranderl, S. (2019). Kims Dotcom. In: Spiegel Online, vom 08.03.2019. URL: https://www.spiegel.de/netzwelt/netzpolitik/kim-jong-un-nordkoreas-hacker-kims-geheimwaffe-a-1256354.html, [zuletzt abgerufen am 01.08.2019].

Petersen, M. und Writer, S. (2016), CyberSecurity San Antonio Creates New Tech Incubator Program. In: San Antonio Express-News, vom 23.06.2016. URL: http://www.expressnews.com/business/local/article/CyberSecurity-San-Antonio-creates-newtech-8320818.php, [zuletzt abgerufen am 04.10.2019].

Porter, M. E. (1985), Competitive advantage: Creating and sustaining superior performance, New York: Free Press.

Porter, M. E. (2000), Location, competition, and economic development: Local clusters in a global economy, Economic Development Quarterly 14 (February 2000): 15–34.

PwC [PricewaterhouseCoopers] (2019), PwC Untersuchung: Immer mehr IT-Studiengänge an deutschen Hochschulen. In: PwC Deutschland, vom 08.07.2019. URL: https://www.pwc.de/de/pressemitteilungen/2019/pwc-untersuchung-immer-mehr-it-studiengaenge-an-deutschen-hochschulen.html, [zuletzt abgerufen am 01.08.2019].

Radware (2017), Anatomy of a Hacker. In DDoS Chronicals, vom 03.10.2017. URL: https://security.radware.com/ddos-knowledge-center/ddos-chronicles/anatomy-of-a-hacker/, [zuletzt abgerufen am: 01.08.2019].

Reuter, M. (2019), Relevanz und Regulierung von Social Bots, erschienen in Dossier: Digitale Desinformation (Erstellt am 30.05.2019), Bundeszentrale für politische Bildung.

Rieckmann, J., und T. Stuchtey (2018), Die Vermessung der Sicherheitswirtschaft – Wachstum und Veränderung im Zeichen der Digitalisierung, in: G. Calaminus (Hg.), Kompendium Sicherheit – Gesellschaft – Digitalisierung von TCC Verlagsgesellschaft, S. 43–68.

Rosenbach, M. und Wagner, W. (2018), Nordkoreas Hackerarmee: Diktator Kims geheime Einnahmequelle - Banken ausrauben. In: Spiegel Online, vom 05.01.2018. URL: https://www.spiegel.de/politik/ausland/nordkoreas-cyberkrieger-rauben-weltweit-banken-aus-a-1186261.html, [zuletzt abgerufen am 01.08.2019].

Sales, N. A. (2012), Regulating Cyber-security. Northwestern University Law Review, 107(4), 1503-1568.

Sawall,A. (2019), Headhunter: Security-Experten können das dreifache Gehalt verlangen. In Golem.de, vom 21.01.2019. URL: https://www.golem.de/news/headhunter-security-experten-koennen-das-dreifache-gehalt-verlangen-1901-138866.html, [zuletzt abgerufen am 26.09.2019].

Scherschel, F. A. (2016), Großstörung bei der Telekom: Angreifer nutzten Lücke und Botnetz-Code. In: Heise Online, vom 29.11.2016. URL: https://www.heise.de/security/meldung/Grossstoerung-bei-der-Telekom-Angreifer-nutzten-Luecke-und-Botnetz-Code-3507088.html, [zuletzt abgerufen am 01.09.2019].

Schumpeter, J. A. (1912), Theorie der Wirtschaftlichen Entwicklung. Leipzig: Dunker & Humblot. The theory of economic development.

Security Essen (2018), Weiter starkes Wachstum im internationalen Sicherheitsmarkt. URL: https://www.security-essen.de/presse/pressetexte/detail-sec/weiter-starkes-wachstum-im-internationalen-sicherheitsmarkt-3767, [zuletzt abgerufen am 15.05.2019].

Seehofer (2019) Cyberbedrohungslage anhaltend hoch. Pressemitteilung 17.10.2019, URL: https://www.bmi.bund.de/SharedDocs/pressemitteilungen/DE/2019/10/bsi-bericht-Cyberbedrohungslage.html, [zuletzt abgerufen am 17.10.2019].

Sood, A. K. und Enbody, R. J. (2013), Crimeware-as-a-service - A survey of commoditized crimeware in the underground market. In: International Journal on Critical Infrastructure Protection, 6(1), 28-38.

Stadt Neuss (2015), Bilanz Lukaskrankenhaus 2015, URL: https://www.neuss.de/archiv/2016/08/bilanz-des-lukaskrankenhauses-2015, [zuletzt abgerufen am 22.08.2019].

Statista (2018), Statistiken zum Bruttoinlandsprodukt, https://de.statista.com.

Stuchtey, T. (2015), Souverän ist, wer selbstbestimmt entscheidet. In: griephan Edition 01/2015: Technologische Souveränität in der Wirtschaft. griephan / BDI.

Stuchtey, T. und Skrzypietz, T (2014), Das Gut Sicherheit und die Rolle der Sicherheitswirtschaft bei seiner Herstellung. In: Apolte, T. (Hg.), Transfer von Institutionen, Schriften des Vereins für Socialpolitik, Band 340, Berlin: Duncker & Humblot, S. 193 – 212.

Symantec Threat Report 2019, URL: https://www.symantec.com/de/de/security-center/threat-report, [zuletzt abgerufen am 20.10.2019].

Tikk, E. (2011). Ten rules for cyber security. Survival, 53(3), 119-132.

Tonner, K., Schlacke, S., und Alt, M. (2015), Stärkung eines nachhaltigen Konsums im Bereich der Produkt-Nutzung durch Zivil- und Öffentliches Recht. In: Obsoleszenz interdisziplinär (pp. 235-268). Nomos Verlagsgesellschaft mbH & Co. KG.

Tozzi, C. (2017), What the Hack? Tracing the Origins of Hacker Culture and the Hacker Ethic. In: Channel Futures, vom 13.03.2017. URL: https://www.channelfutures.com/open-source/what-the-hack-tracing-the-origins-of-hacker-culture-and-the-hacker-ethic, [zuletzt abgerufen am 10.10.2019].

Tulkens, H., und Jacquemin, A. (1971), The Cost of Delinquency: A Problem of Optimal Allocation of Private and Public Expenditures, CORE disc. paper no. 7133, Catholic Univ. Louvain.

Verizon (2019), Data Breach Investigations Report. URL: https://enterprise.verizon.com/de-de/resources/reports/dbir/, [zuletzt abgerufen am 01.08.2019].

Walker, S. (2012), Economics and the Cyber Challenge, *Information Security Technical Report* 17, S. 9–18.

Wagner, V. (2018), Handlungsfelder Cybersicherheit, in: G. Calaminus (Hg.), Kompendium Sicherheit – Gesellschaft – Digitalisierung von TCC Verlagsgesellschaft, S. 71–82.

Weber, T., Bertschek, I., Ohnemus, J., & Ebert, M. (2018), DIGITAL Economy Monitoring Report 2018-Compact. ZEW-Gutachten und Forschungsberichte.

WifOR (2019a), Aktuelle und zukünftige Einwanderungsbedarfe von IT-Fachkräften nach Deutschland. In: Friedrich-Ebert-Stiftung, WISO-Diskurs 09/2019.

WifOR (2019b), Der IT-Sicherheitsmarkt in Deutschland. Zweite Aktualisierung der Studie zu der aktuellen Lage der IT-Sicherheitswirtschaft, ihrer Entwicklung und zukünftigen Potenzialen in Deutschland, Studie im Auftrag des Bundesministeriums für Wirtschaft und Energie (BMWi). URL: https://www.bmwi.de/Redaktion/DE/Publikationen/Studien/it-sicherheitsmarkt-in-deutschland-studie-2019.pdf?__blob=publicationFile&v=8, [zuletzt abgerufen 19.08.2019].

World Economic Forum (2012), Partnering for Cyber Resilience: Risk and Responsibility in a Hyperconnected World—Principles and Guidelines. Report REF 270912, Cologny.

Wrede, D., Freers Th. und Graf von der Schulenburg, J. M. (2018), Herausforderungen und Implikationen für das Cyberrisikomanagement sowie Versicherung von Cyberrisiken – eine empirische Analyse, ZVersWiss 107, S. 405 – 434.

WTO [World Trade Organization] (2000), Second Triennial Review of the Operation and Implementation of the Agreement on Technical Barriers to Trade, Committee on Technical Barriers to Trade, 13. November 2000.

Yaakov, Y. B., Wang, X., Meyer, J., und An, B. (2019, October). Choosing Protection: User Investments in Security Measures for Cyber Risk Management. In: International Conference on Decision and Game Theory for Security (pp. 33-44). Springer, Cham.

Zetter, K. (2015). Countdown to zero day: Stuxnet and the launch of the world's first digital weapon, (Crown: New York).

ZEW [Leibniz-Zentrum für Europäische Wirtschaftsforschung] (2018), Innovationen in der Deutschen Wirtschaft - Indikatorenbericht zur Innovationserhebung 2018, Mannheim.

Zhao, W. und White, G. (2017), An Evolution Roadmap for Community Cyber Security Information Sharing Maturity Model, Paper presented at 50th Hawaii International Conference on System Sciences, Waikoloa, Hawaii, January 4–7, 2017. URL: https://scholarspace.manoa.hawaii.edu/bitstream/10125/41443/1/paper0294.pdf, [zuletzt abgerufen 19.08.2019].