Institut der deutschen Wirtschaft Köln

IW policy paper · 6/2017

Aktuelle politische Debattenbeiträge aus dem Institut der deutschen Wirtschaft Köln

Wirtschaftliche Kosten der Cyberspionage für deutsche Unternehmen

Cybersicherheit als Grundvoraussetzung der digitalen Transformation

Autoren:

Barbara Engels
Telefon: 0221 4987-703
E-Mail: engels@iwkoeln.de

17. Mai 2017

Inhalt

JEL-Klassifikation:
L20, O30, O31

Zusammenfassung

Cybersicherheit ist entscheidend für eine erfolgreiche digitale Transformation. Das volle Potenzial digitaler Technologien kann nur ausgeschöpft werden, wenn Institutionen, Unternehmen und Privatpersonen sich auf die Sicherheit ihrer Daten und Systeme verlassen können. Bislang ist das nicht der Fall, wie zahlreiche Cybersicherheitsvorfälle belegen. Insbesondere die Cyberspionage, also der Diebstahl von relevanten Unternehmensdaten und geistigem Eigentum, macht Unternehmen zu schaffen. Auch deutsche Unternehmen sind aufgrund ihrer innovativen Produkte, besonders auch im Bereich Industrie 4.0, und ihrer starken Position auf den Weltmärkten ein lukratives Ziel für Hacker. Cybercrime wird deshalb von vielen deutschen Unternehmen als die größte Bedrohung für deutsche Unternehmen und den Wirtschaftsstandort Deutschland gesehen. Tatsächlich zieht Cyberspionage enorme Kosten nach sich. Neben den direkten Kosten durch den Verlust des geistigen Eigentums und die Behebung des Schadens kommt es zu diversen indirekten Kosten wie Umsatzausfällen und Reputationsschäden. Das vorliegende Paper bietet eine qualitative und quantitative Einschätzung dieser Kosten für deutsche Unternehmen. Angesichts der Vielfalt der Kostenarten und der Höhe der Kosten ist es essentiell, Cybersicherheit als Grundvoraussetzung für alle unternehmerischen Tätigkeiten zu verstehen, um die Wettbewerbsfähigkeit und die Stabilität der deutschen Wirtschaft zu schützen.

Abstract

Cybersecurity is crucial for a successful digital transformation. The full potential of digital technologies can only be tapped if institutions, companies and individuals can rely on the security of their data and systems. This has so far not been the case, as numerous cyber security incidents prove. Cyber espionage, the theft of relevant company data and intellectual property, is especially harmful to companies. German companies are an attractive target for hackers due to their innovative products, especially in the industrial sector, and their strong position on the world markets. Many German companies therefore cybercrime as the greatest threat to German companies and Germany as a business location. In fact, cyber espionage causes enormous costs. In addition to the direct costs of the loss of intellectual property and the elimination of the damage, there are various indirect costs, such as turnover losses and the damage to reputation. This paper provides a qualitative and quantitative assessment of these costs for German companies. Given the diversity of cost types and the high amount of costs, it is essential to regard cyber security as a prerequisite for all entrepreneurial activities in order to protect the competitiveness and stability of the German economy.

1. Einleitung

Die wichtigste Ressource der digitalen Transformation sind Daten. Je mehr und je intensiver Produkte, Prozesse, Maschinen und Menschen miteinander verbunden sind, desto mehr Angriffspunkte gibt es und desto eher können sie angegriffen und Daten abgeschöpft werden. Der Sicherheit und Verfügbarkeit von Daten kommt eine strategische Bedeutung zu. Cybersicherheit, also die Sicherheit von Datennetzen, die Sicherheit in der Informations- und Kommunikationstechnik, ist entscheidend für eine erfolgreiche digitale Transformation. Das volle Potenzial digitaler Technologien kann nur ausgeschöpft werden, wenn Institutionen, Unternehmen und Privatpersonen sich auf die Sicherheit ihrer Daten verlassen können. Bislang ist das nicht der Fall, wie zahlreiche Cybersicherheitsvorfälle belegen, die fast täglich von den Medien berichtet werden. Unternehmen berichten, dass die Anforderungen an die IT-Sicherheit neben den hohen Kosten das zentrale Digitalisierungshemmnis sind (Demary et al., 2016, 36). Besonders die Cyberspionage, also der Diebstahl von relevanten Unternehmensdaten und geistigem Eigentum (Intellectual Property, IP), macht Unternehmen zu schaffen.

Viele deutsche Unternehmen sind aufgrund ihrer innovativen Produkte, besonders auch im Bereich Industrie 4.0, und ihrer starken Position auf den Weltmärkten ein lukratives Ziel für Hacker. Cybercrime wird deshalb nach Einschätzung vieler Unternehmen als die größte Bedrohung für Unternehmen und den Wirtschaftsstandort Deutschland gesehen (Allianz, 2017). Mehr als jedes dritte Unternehmen in Deutschland ist laut KPMG (2017) in den vergangenen beiden Jahren von Computersabotage, digitaler Erpressung oder einer anderen Form von Cyberkriminalität betroffen gewesen. Die tatsächliche Quote dürfte noch deutlich höher liegen, da es eine hohe Dunkelziffer gibt. Laut Branchenverband Bitkom (2016) sind zwei von drei Industrieunternehmen (69 Prozent) in Deutschland im Zeitraum 2014/2015 Opfer von Datendiebstahl, Wirtschaftsspionage oder Sabotage geworden, darunter vor allem kleine und mittlere Unternehmen (KMUs; siehe auch Bitkom (2015)). KMUs sind begehrte Ziele und verfügen im Gegensatz zu großen Konzernen ressourcenbedingt tendenziell nicht über ganzheitliche Sicherheitskonzepte, haben aber schützenswertes Know-how oder Zugriff auf dieses.

Die digitale Transformation im Sinne von Industrie 4.0 verschärft diese Bedrohungslage. Dadurch, dass immer mehr Daten verfügbar gemacht werden, die Vernetzung intensiviert wird und die Grenzen der internen IT-Infrastrukturen aufweichen, entstehen neue Angriffsmöglichkeiten. Cyberangriffe können sich durch die Vernetzung verschiedener Standorte und Unternehmen kaskadierend fortsetzen. Etwa drei Viertel der Unternehmen gehen davon aus, dass das Risiko, angegriffen zu werden, für deutsche

Unternehmen in Zukunft steigen wird (KPMG, 2017, 13). 73 Prozent schätzen das Risiko des Ausspähens oder Abfangens von Daten bereits jetzt als hoch oder sehr hoch ein (KPMG, 2017, 14).

Das vorliegende Papier bietet eine qualitative und quantitative Einschätzung der Kosten der Cyberkriminalität und insbesondere der Cyberspionage für deutsche Unternehmen. Cyberspionage zieht vielfältige direkte und indirekte Kosten für die betroffenen Unternehmen sowie Kosten für die Volkswirtschaft nach sich. Eine genaue Quantifizierung der Schäden für die deutsche Wirtschaft ist schwierig, denn viele Vorfälle werden erst spät oder gar nicht bemerkt und die vorhandenen Studien liefern kein umfassendes Bild. Allerdings kann als Untergrenze pro Jahr von einem zweistelligen Milliardenbetrag ausgegangen werden.

2. Ziele und Methoden der Cyberspionage

In diesem Kapitel wird Cyberspionage als Teil der Cyberkriminalität inklusive ihrer Ziele und Methoden erläutert. Generell zählen in der engeren Definition Straftaten zur Cyberkriminalität, die sich gegen das Internet, Datennetze, informationstechnische Systeme oder deren Daten richten. In der weiteren Definition zählen Straftaten dazu, die mittels dieser Informationstechnik begangen werden (Tatmittel Internet).

Cyberspionage ist eine externe Bedrohung für Unternehmen und Institutionen. Akteure infiltrieren Unternehmensnetzwerke auf der Suche nach geistigem Eigentum und anderen sensiblen Daten. Werden Daten aus dem Unternehmen heraus gestohlen, spricht man nicht von Cyberspionage. Vorfälle, bei denen zum Beispiel ein Mitarbeiter die Kundendatenbank stiehlt, fallen unter den Tatbestand des Privilegienmissbrauchs.

2.1 Ziele der Cyberspionage

Die Informationen, die im Fokus der Cyberspionage stehen, lassen sich in geistiges Eigentum (IP), sensible Unternehmensdaten sowie Kunden- und Mitarbeiterdaten unterteilen. IP umfasst jede Arbeit oder Erfindung kreativen Ursprungs, darunter Quellcodes, Produktdesigns, Formeln und Blaupausen (z.B. WTO, 2017). Der Ressourcenaufwand für die Entwicklung komplexer Produkte und Konzepte ist hoch, daher ist der Verlust dieser Informationen durch Cyberspionage finanziell schwerwiegend. Industriebranchen wie Pharma, Chemie oder der Technologiesektor sind beliebte Ziele der Angreifer, weil das gestohlene geistige Eigentum für den Dieb oft leicht reproduzierbar ist und schnell monetarisiert werden kann (siehe dazu auch 4.1). Aber auch Unternehmen aus anderen Branchen sowie kleine Unternehmen sind stark von Cyberspionage

betroffen. Wettbewerbsrelevantes, geschäftskritisches Wissen ist in allen Unternehmensbereichen vorhanden und unabhängig von der Unternehmensgröße ein wertvoller Vermögensgegenstand (Bundesamt für Verfassungsschutz, 2015). Sensible Unternehmensdaten umfassen Investitionsdaten, Kooperations- und Transaktionspläne, operative Informationen, Verträge und Geschäftsgeheimnisse. Durch den Zugang zu diesen Informationen können Cyberkriminelle Geschäftsvorgänge, Produktankündigungen und Investitionsnachrichten vorwegnehmen oder anderweitig ausnutzen.

KPMG (2017) teilt risikobehaftete Informationen in Kundendaten, Bank- und Finanzdaten des Unternehmens, Preis- und Konditionsinformationen, Patente, Produktinformationen und Konstruktionszeichnungen, Strategiepapiere, Entscheidungsgrundlagen, Gremienprotokolle, Personaldaten, IT-Daten und Gesundheitsdaten ein. Mehr als drei Viertel der in dieser Studie befragten deutschen Unternehmen nehmen Kunden- sowie Bank- oder Finanzdaten als besonders risikobehaftet wahr (KPMG, 2017, 16). Preis- und Konditionsinformationen werden vor allem im Handel (72 Prozent) und Patente, Produktinformationen und Konstruktionszeichnungen hauptsächlich in der Industrie (69 Prozent) als besonders risikobehaftet angesehen (KPMG, 2017, 17). Große Unternehmen mit einem Umsatz von mehr als drei Milliarden Euro nennen vor allem Wettbewerber und organisierte Kriminelle als potenzielle Angreifer (KPMG, 2017, 22).

Aber auch fremde Nachrichtendienste haben Interesse an den Daten. Das Bundesamt für Verfassungsschutz (2015) kategorisiert die Hacker beziehungsweise deren Kunden in hochentwickelte Staaten, Staaten mit Technologierückstand und konkurrierende Unternehmen (Abbildung 1). Für hochentwickelte Staaten sind vor allem wirtschaftspolitische Strategien relevant. Rückständige Staaten stehlen vor allem technisches Know-how, um Kosten für eigene Entwicklungen zu sparen. Sie beschaffen sich Informationen über Fertigungstechniken, um auf dem Markt mit kostengünstiger gefertigten Nachbauten wettbewerbsfähig zu sein. Konkurrierende Unternehmen besorgen sich unter anderem Informationen über Wettbewerb und Kunden sowie Know-how zur Produktentwicklung und Produktionstechnik. Oft beauftragen diese Unternehmen über das Darknet kriminelle Gruppen mit der Spionage („Cybercrime as a Service“). Laut dem Sicherheitstacho (2017), der eine Übersicht über die aktuellen Cyberangriffe auf Sensoren der Deutschen Telekom gibt, kommen die meisten Angriffe aus China – dabei gibt es seit Juni 2016 eine gemeinsame Erklärung Deutschlands und Chinas, wonach Verletzungen von geistigem Eigentum sowie Handels- und Geschäftsgeheimnissen unter Verwendung des Cyberraums zur Erlangung von Wettbewerbsvorteilen für Unternehmen weder betrieben noch wissentlich unterstützt werden dürfen (Landwehr, 2016).

Abbildung 1: Angreifergruppen und deren Motive
Kategorisierung der Herkunft der Hacker beziehungsweise deren Kunden und deren Motive

Quelle: eigene Darstellung basierend auf Bundesamt für Verfassungsschutz, 2015

2.2 Methoden der Cyberspionage

Die Methoden der Cyberspionage sind vielfältig, da das Internet als offenes Netzwerk und dementsprechend auch die daran angegliederten Systeme der Unternehmen viele verschiedene Angriffspunkte bieten. Jeder kann im Detail Kenntnis erlangen vom Internet und von den Protokollen, vermittels derer die Kommunikation technisch bewältigt wird. Prinzipiell kann jeder, der sich mit dem Internet verbindet, mit entsprechenden Kenntnissen und Werkzeugen auf potenziell alle im Internet kommunizierten Daten zugreifen (Meinel/Sack, 2014). Deshalb sind Cyberangriffe eine effektive und von den betroffenen Stellen nur schwer aufzuklärende Methode der Informationsbeschaffung, die kostengünstig, in Echtzeit durchführbar und oft erfolgreich ist.

Die Anzahl der Einfallstore ins Netzwerk eines Unternehmens steigt ständig. Unternehmen müssen immer mehr Standorte, Remote-Mitarbeiter, cloudbasierte Anwendungen und einzelne Geräte schützen. Dementsprechend wird im Rahmen von Cyberkriminalität von einer asymmetrischen Bedrohung gesprochen: Die Angreifer müssen nur ein Schlupfloch finden, während die Unternehmen eine Vielzahl von Systemen mit zahlreichen Schwachstellen absichern müssen (Bitkom, 2016, 60).

Ein Großteil der Infrastruktur des Internets ist laut einer Untersuchung des Fraunhofer-Instituts für Sichere Informationstechnologie leicht anzugreifen. Demnach waren Ende 2016 92 Prozent des World Wide Web durch Manipulationen des Domain Name System (DNS) verwundbar (siehe BMBF, 2017). Das System sorgt dafür, dass Anfragen an eine bestimmte Webadresse den richtigen Webserver erreichen. Manipulationen

des Systems können Abhör- und Phishing-Angriffe ermöglichen. Auch 68 Prozent der von Telekommunikationsunternehmen betriebenen Netze und über 73 Prozent der Unternehmensnetze sind laut der Studie anfällig.

Die Schwachstellen sind auf technologischer, organisatorischer sowie personeller Ebene zu suchen. Falsche Anreize sind laut Anderson (2001) entscheidend an Problemen der Informationssicherheit beteiligt. Netzwerkexternalitäten, asymmetrische Information, Moral Hazard, Adverse Selektion sowie die Tragik der Allmende befördern Sicherheitsprobleme.[1] Cybersicherheitstechnologien sind daher effektiver, wenn sie das Verhalten der Nutzer berücksichtigen (Caputo/Pfleeger, 2011). Ein hoher Prozentsatz von Cybersicherheitsvorfällen wird direkt oder indirekt von den Menschen innerhalb einer Organisation verursacht. Nutzer sind unter Umständen achtlos und leichtsinnig im Umgang mit sensiblen Daten oder ihnen fehlt das Wissen für eine angemessene Datensicherheit. Auf technologischer Ebene sind Geräte wie Computer, Laptops, Tablets und Smartphones oft falsch konfiguriert oder ihre Software ist nicht upgedatet. Die Anzahl der angreifbaren Geräte dürfte mit dem Internet of Things, also der Vernetzung zwischen smarten Gegenständen sowohl untereinander als auch nach außen hin mit dem Internet, noch deutlich zunehmen: Schätzungen zufolge werden bis zum Jahr 2020 etwa 20 bis 50 Milliarden Geräte im Internet of Things (IoT) über das Internet verbunden sein. Aufgrund fehlender Sicherheitsvorkehrungen sind sie besonders gefährdet, Teil von sogenannten Botnetzen zu werden, einem Verbund von Systemen, die von einem fernsteuerbaren Schadprogramm befallen sind.

Schadprogramme (Malware) sind eine der häufigsten Angriffsarten bei unternehmerischen Cyberangriffen (vgl. BSI, 2016). Sie führen unerwünschte Funktionen auf einem oft per Email-Anhang oder durch den Besuch von infizierten Webseiten (Drive-by-Downloads) infizierten Gerät aus. Täglich werden etwa 380.000 neue Schadprogrammvarianten gesichtet. Inzwischen sind mehr als 600 Millionen verschiedene Varianten bekannt (AV-Test, 2017). Ein Schadsoftwaretyp ist Ransomware. Ransomware schränkt den Zugriff auf Dateien oder Systeme ein und gibt diese nur gegen Zahlung eines Lösegeldes wieder frei.

Wo Angreifer dank aktueller Software, Firewalls und Virenscannern abgewehrt werden, versuchen sie, die Nutzer auszutricksen. Vergleichbar mit dem Trickbetrug an der Haustür täuschen sie eine persönliche Beziehung oder Gewinnversprechen vor. Wenn das Opfer dann unter Druck einen infizierten E-Mail-Anhang öffnet oder eine entsprechende Webseite aufruft, kann das Nutzersystem mit Schadsoftware infiziert werden

---

[1] Netzwerkexternalitäten entstehen, wenn die Nachfrage eines Gutes durch die Anzahl der anderen Konsumenten beeinflusst wird. Asymmetrische Informationen bestehen, wenn nicht alle Marktteilnehmer die gleichen Informationen beispielsweise über ein Produkt haben. Eine Folge aus der Informations-asymmetrie ist adverse Selektion, d.h. eine Negativauslese, beispielsweise der Geschäftspartner. Moral Hazard bedeutet, dass sich Individuen aufgrund ökonomischer Fehlanreize verantwortungslos oder leichtsinnig verhalten und damit ein Risiko verstärken. Bei der Tragik der Allmende übernutzen Individuen ein öffentlich verfügbares Gut.

(BSI, 2016, 22). Hier wird konkret der Mensch als schwächstes Glied der Kette ausgenutzt.

Eine besonders gefürchtete Angriffsmethode sind Advanced Persistent Threats (APT). Die Angreifer suchen die Ziele dabei sorgfältig aus und bewegen sich unter hohem Aufwand teilweise über Jahre unerkannt im Nutzersystem. Die Täter versuchen, sich im Netzwerk des angegriffenen Unternehmens auszubreiten und sich einen langfristigen Zugang zu sichern (BSI (2016, 22); für eine Übersicht der bekannten APTs siehe Kaspersky Lab (2017)).

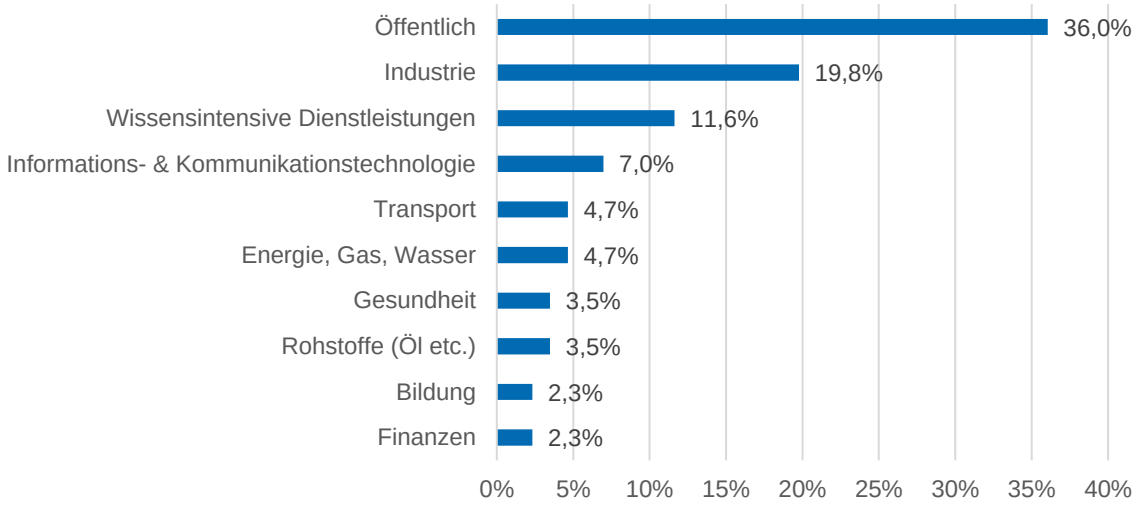
3. Bedrohungslage

Die Anzahl der Cyberangriffe und damit der Cyberspionagefälle wächst dramatisch. Nahezu täglich werden neue Fälle von Datendiebstahl, Computerbetrug, Computersabotage und anderen Datendelikten bekannt. Die von diesen Delikten ausgehenden Gefahren werden voraussichtlich in ihrem Ausmaß und in ihren Ausprägungen weiter zunehmen (siehe unter anderem KPMG, 2017). Zahlreiche Studien versuchen, das Ausmaß der Cyberkriminalität zu quantifizieren, aber die Dunkelziffer ist hoch. Nur ein kleiner Teil der Straftaten in diesem Bereich wird zur Anzeige gebracht oder gemeldet – zum einen, weil Verluste nicht bemerkt werden, zum anderen, weil Unternehmen eine Rufschädigung fürchten (siehe auch Kapitel 4.2). In einigen Bundesstaaten der USA ist es hingegen für Unternehmen verpflichtend, Hackerangriffe zu melden. OAG (2017) etwa listet alle Angriffe auf Daten kalifornischer Unternehmen auf, die mehr als 500 Personen betreffen. Eine Studie des LKA Niedersachsen (2013) kommt zu dem Ergebnis, dass lediglich neun Prozent aller Cyberkriminalitätsvorfälle angezeigt werden. Die Angriffe sind wegen dezentraler IT-Strukturen, auf die staatliche Stellen keinen Zugriff haben, nur schwer zu erkennen und aufzuklären (BMI, 2016).

Der Breach Level Index (2017) geht davon aus, dass täglich knapp vier Millionen Datensätze weltweit verloren gehen oder gestohlen werden. Laut einer Studie der Allianz (2017) sehen deutsche Unternehmen Cybervorfälle als größtes Geschäftsrisiko noch vor Betriebsunterbrechungen etwa durch Brände oder Naturkatstrophen und Marktveränderungen wie neue Wettbewerber. Deutschland ist aufgrund der großen Masse wertvoller Daten im Rahmen von Industrie 4.0 besonders attraktiv für Cyberkriminelle, die auf die Branchen Fertigung und Produktion zielen. Die globale Sicherheitsstudie von Verizon (2016) zeigt, dass 2015 vor allem der öffentliche Sektor betroffen war, dann die Industrie und wissensintensive Dienstleister (Abbildung 2). Laut dem Bundesamt für Verfassungsschutz (2015, 6) sind vor allem technologieorientierte und innovative Unternehmen aus den Bereichen Informations- und Kommunikationstechnologie (IKT), Biotechnologie, Optoelektronik, Automobil- und Maschinenbau, Luft- und Raumfahrttechnik sowie Energie- und Umwelttechnologie beliebte Spionageziele. Industrieanlagen sind leicht angreifbar, denn viele von ihnen

sind mehr als 30 Jahre alt und werden lediglich nachträglich mit Sensoren bestückt, die ihre Daten in unterschiedlichen Sprachen (Protokollen) übermitteln, manchmal sogar unverschlüsselt.

Abbildung 2: Weltweite Cyberspionagevorfälle nach Branchen
Prozentuale Verteilung der Cyberspionagevorfälle (weltweit), 2015, in Prozent



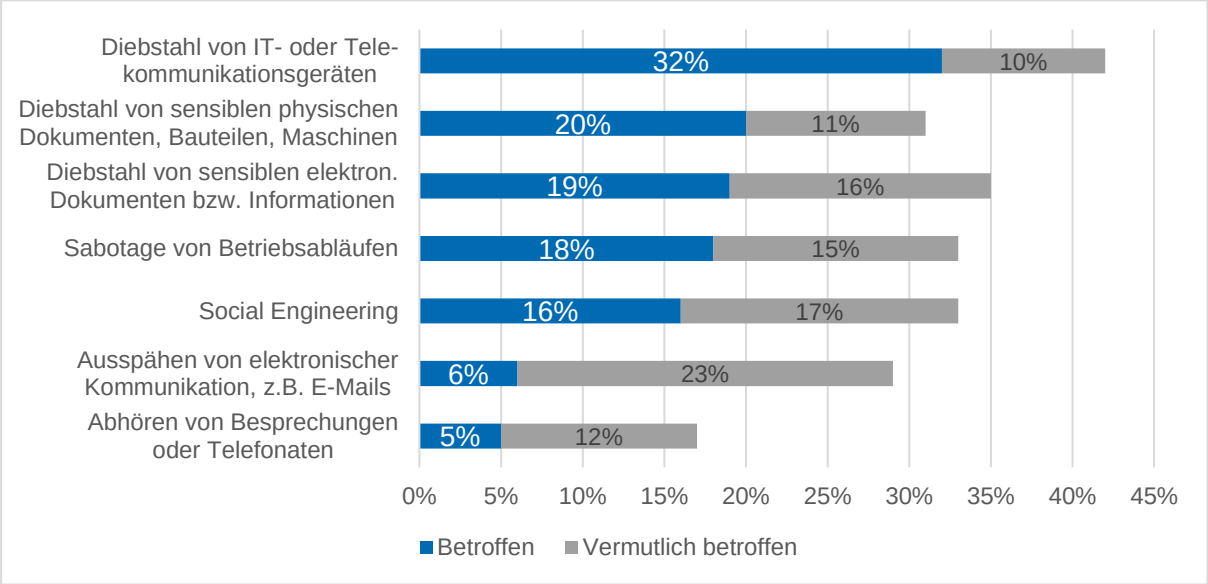
Quelle: Verizon, 2016, 53; eigene Darstellung

Vor allem kleinere Firmen haben oft die falsche Vorstellung, dass ihnen keine Gefahr von Hackern drohe, weil sie dafür zu uninteressant seien (Rixecker, 2017). Laut Branchenverband Bitkom (2015) sind gut 50 Prozent aller Unternehmen in Deutschland im Zeitraum 2013/2014 Opfer von IT-Kriminalität geworden – Tendenz steigend. Mittelständler sind mit über 60 Prozent besonders stark von Spionage- und Sabotageakten sowie von Datendiebstahl betroffen. Laut der ähnlichen 2016er-Auflage der Studie sind zwei von drei Industrieunternehmen (69 Prozent) in Deutschland im Zeitraum 2014/2015 Opfer von Datendiebstahl, Wirtschaftsspionage oder Sabotage geworden, darunter vor allem kleine und mittlere Unternehmen (Bitkom, 2016). In einer anderen Studie geben fast 60 Prozent der befragten Unternehmen an, in den vergangenen fünf Jahren einen Cybersicherheitsvorfall erlebt zu haben (Cebr, 2016, 14). Das Softwareunternehmen Check Point (2016, 17) hat ausgerechnet, dass an einem durchschnittlichen Tag in einem Unternehmen alle 81 Sekunden eine bekannte Malware und alle vier Sekunden eine unbekannte Malware heruntergeladen wird. Alle fünf Sekunden greift ein Nutzer auf eine schadhafte Webseite zu, alle 32 Minuten werden sensible Daten aus dem Unternehmen herausgeschickt.

Die Befragung des Bitkom (2016) unter deutschen Industrieunternehmen zeigt, dass nahezu alle Fälle von Sabotage oder Spionage im wirtschaftlichen Umfeld auf digitale Daten oder die Informations- und Kommunikationsinfrastruktur der Unternehmen abzielen (siehe Abbildung 3). Ein Drittel der Unternehmen berichtet vom Diebstahl von IT- oder Telekommunikationsgeräten, ein Fünftel vom Diebstahl sensibler Informationen. Der Anteil der vermuteten Angriffe ist beim Ausspähen von Emails am höchsten.

Große Unternehmen haben laut der Studie eine bessere Übersicht über die Vorfälle als kleinere Unternehmen: Der Anteil vermuteter Vorfälle ist geringer (13 Prozent zu 22 Prozent). Viele Mittelständler verfügen nicht über das notwendige Wissen und die Ressourcen, um zu identifizieren, wo Sicherheitsprobleme liegen und wie sie sich schützen können. Die hohen Anforderungen an die IT-Sicherheit sind ein zentrales Digitalisierungshemmnis, wie die Metastudie zum Thema digitale Transformation im Mittelstand von Demary et al. (2016) zeigt.

Abbildung 3: Sicherheitsvorfälle in deutschen Unternehmen
Antworten auf die Frage: „Von welchen Handlungen war Ihr Unternehmen in den vergangenen zwei Jahren betroffen/vermutlich betroffen?“, in Prozent
Basis: Umfrage unter 504 Industrieunternehmen



Quelle: Bitkom, 2016; eigene Darstellung

Geht man davon aus, dass die zunehmende Vernetzung zu steigenden Sicherheitsrisiken führt, müssten stärker digitalisierte Unternehmen auch stärker von Cyberkriminalität betroffen sein. Laut Bitkom (2016) ist das Gegenteil der Fall: Der Anteil betroffener Unternehmen, die ihren Digitalisierungsgrad als hoch einschätzen, ist um 11 Prozentpunkte geringer als bei denjenigen, die sich einen niedrigen Digitalisierungsgrad zuschreiben. Die Auseinandersetzung mit der Digitalisierung ruft offensichtlich auch das Thema IT-Sicherheit auf den Plan. Dies ist ein weiterer Hinweis darauf, dass Digitalisierung und IT-Sicherheit Hand in Hand gehen müssen und es auch tatsächlich tun.

4. Kosten der Cyberspionage

Cyberangriffe und besonders Cyberspionage ziehen oft enorme materielle und immaterielle Schäden nach sich. Die Kosten sind kaum quantifizierbar, da Unternehmen viele Angriffe und damit Kosten nicht oder erst Jahre später erkennen oder aus Angst vor Reputationsschäden geheim halten. Laut Armin et al. (2015) führt die Vielzahl der teilweise widersprüchlichen Studien zu den wirtschaftlichen Kosten der Cyberkriminalität sogar dazu, dass keine Cybersicherheitsmaßnahmen ergriffen werden, weil deren Kosteneffektivität nicht klar beurteilt werden kann. Eine Quantifizierung ist oft auch irreführend, weil vorhandene Studien von Unternehmen oder Institutionen erstellt wurden, die eine bestimmte Agenda haben, darunter etwa IT-Sicherheitsanbieter. Anderson et al. (2013) verzichten in ihrer Cyberkriminalitätskosten-Studie ganz auf die Berechnung der Kosten von Cyberspionage, da es keine verlässliche Beweislage für Ausmaß und Kosten der Spionage gebe. In diesem Kapitel werden vor diesem Hintergrund zunächst die qualitativen Ausmaße der Kosten durch Cyberspionage thematisiert. Unterschieden wird zwischen direkten Kosten und indirekten Kosten für die Unternehmen sowie gesamtwirtschaftliche Kosten. In einem letzten Teil wird ein Überblick verschiedener Ergebnisse zur Quantifizierung der Kosten in Deutschland gegeben.

4.1 Direkte Kosten

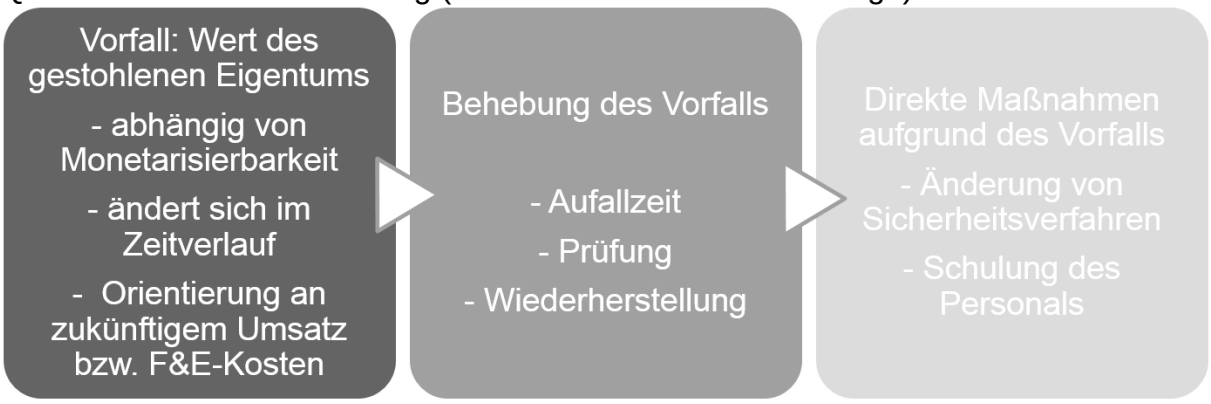
Die direkten Kosten der Cyberspionage sind in Abbildung 4 zusammengefasst. Die unmittelbarste Komponente der direkten Kosten ist der Wert des gestohlenen Eigentums. Diese ist allerdings sehr schwierig zu schätzen. Beim Verkauf oder der Fusion eines Unternehmens ist es normale Praxis, den Wert des IP zu berechnen – an diesem Wert können Unternehmen sich auch bei einem Cyberspionagevorfall orientieren. Diese Berechnungen beruhen oft auf einer Vorhersage über die künftigen Erträge aus der Verwendung des IP oder auf den zugehörigen Forschungs- und Entwicklungskosten (vgl. McAfee, 2014). Beide Werte können sehr unterschiedlich ausfallen. Die Nutzbarkeit der Daten für den Angreifer schränkt die Validität dieser Schätzung ein, denn nicht alle Daten sind gleich nutzbar für die Diebe.

Die Fähigkeit des Datenempfängers, die Daten zu nutzen, kann sehr unterschiedlich ausfallen. Je nutzbarer und monetarisierbarer die gestohlenen Daten für den Angreifer, desto höher der Wert (vgl. McAfee, 2014, 12). In der Chemiebranche reicht der Verlust einer chemischen Formel für ein bestimmtes Produkt, damit ein Wettbewerber schnell ein potentiell kostengünstigeres Produkt auf den Markt bringen kann. Deshalb sind Chemieunternehmen beliebte Ziele der Cyberspionage. In Sektoren, in denen fortgeschrittene Fertigungskapazitäten genutzt werden, wie etwa in der Halbleiterindustrie, kann es Jahre dauern, bis der Diebstahl von geistigem Eigentum ein konkurrierendes

Produkt erzeugt. Der Wert des gestohlenen IP könnte in den ersten Jahren nach dem Diebstahl null betragen und dann dramatisch zuzunehmen, wenn der Erwerber die Möglichkeit hat, die Daten gewinnbringend zu nutzen (McAfee, 2014, 13). Bei Technologieprodukten kann die Verzögerung zwischen Diebstahl der Daten und Nutzung der Daten in der Produktion des Konkurrenten Jahre betragen.

Oft werden die direkten Kosten auch falsch eingeschätzt, weil der Verlust der Daten spät oder gar nicht auffällt. Ein Fahrraddiebstahl wird bei der nächsten geplanten Nutzung bemerkt. Ein Unternehmen, dem die Pläne für ein E-Bike gestohlen wurden, bemerkt dies oft nicht, bis sein Konkurrent ein baugleiches Rad auf den Markt bringt (vgl. McAfee, 2014, 13).

Abbildung 4: Komponenten der direkten Kosten von Wirtschaftsspionage
Qualitative Zusammenstellung (Indikation der zeitlichen Abfolge)



Quelle: Eigene Darstellung

Der zweite Kostenblock der direkten Kosten ist mit der Behebung des Spionagevorfalls verbunden. Oft müssen die betroffenen sowie mit ihnen verbundene Systeme für eine Zeit vom Netz genommen, auf Infektionen geprüft, von Malware gereinigt und eventuell aus Backups wiederhergestellt werden. Auch die Backups müssen auf Schwachstellen überprüft werden. Analyse, Reparatur und Härtung (Beschränkung auf notwendigen Funktionsumfang) der kompromittierten Systeme sind oft mit erheblichen Ausfallzeiten verbunden, die gerade in der industriellen Produktion sehr kostenintensiv sind.

Der dritte Kostenblock der direkten Kosten speist sich aus den direkten Maßnahmen, die sich aus dem Vorfall ergeben. Neue Schutzmechanismen bezüglich Überwachung und Verschlüsselung werden implementiert. Mitarbeiter müssen sensibilisiert und weitergebildet werden. Die Maßnahmen können oft langwierig und kostenintensiv sein. Gerade dieser dritte Kostenblock überschneidet sich partiell mit den indirekten Kosten, die sich aus einem Cyberspionagevorfall ergeben. Diese werden im Folgenden beschrieben.

4.2 Indirekte Kosten

Indirekte Kosten oder nachgelagerte Kosten der Cyberspionage sind komplexer und in der Regel schwerer quantifizierbar als direkte Kosten (Abbildung 5).

Abbildung 5: Komponenten der indirekten Kosten der Wirtschaftsspionage
Qualitative Zusammenstellung (Indikation der möglichen zeitlichen Abfolge)

Quelle: Eigene Darstellung

Sie speisen sich vor allem aus Umsatzverlusten. Mit gestohlenen Daten lässt es sich einfacher und schneller produzieren. Umsatzausfälle werden vor allem durch von Wettbewerbern auf den Markt gebrachte Plagiate verursacht, die auf der gestohlenen IP basieren. Die bestohlenen Unternehmen verlieren Wettbewerbsvorteile, unter anderem durch Patentenrechtsverletzungen. Generell investiert ein Unternehmen in Forschung und Entwicklung, um IP zu schaffen und aus dieser IP eine gewisse Rendite zu erwirtschaften. Dieser Return on Investment (ROI) sinkt, wenn auf dem Markt ein konkurrierendes Produkt auf der Grundlage von gestohlenem IP erscheint. Neue Produkte ziehen Kunden an, bis die Konkurrenten aufholen. Wenn IP gestohlen wird, kann es sein, dass dieser sogenannte Lead in stark gekürzter Form auftritt. Beispielsweise dauert er dann nur drei Monate statt einem Jahr und die Investitionsrendite ist maximal ein Viertel der potenziellen Rendite ohne den Cyberspionagevorfall.

Eine softe, schwer messbare Komponente der indirekten Kosten sind Marken- und Reputationsschäden. Diese sind besonders erheblich, wenn bei dem Cyberspionagevorfall Geschäftspartnerdaten ausspioniert wurden. Sowohl bei Kunden als auch bei Lieferanten und anderen Geschäftspartnern führen Reputationsschäden zu einem Verlust von Vertrauen – und vice versa. Das kann gerade für kleine Unternehmen verheerend sein (Check Point, 2016, 41), insbesondere wenn Kunden nicht nur verunsichert sind, sondern dem Unternehmen ganz den Rücken kehren. Auch für Digital- und Online-Unternehmen, die mit ihrem auf Netzwerkeffekten basierendem Geschäftsmodell auf einen großen Kundenstamm angewiesen sind, sind Rufschäden besonders

kritisch. Laut Campbell et al. (2003) hat die öffentliche Bekanntgabe des Verlusts vertraulicher Informationen negative Auswirkungen auf den Aktienkurs des betroffenen Unternehmens. Auch Jahre später können Cybersicherheitsvorfälle noch zu einer niedrigeren Bewertung des Unternehmens führen, so geschehen etwa im Fall des Verkaufs des Kerngeschäfts von Yahoo an Verizon, der wegen Datendiebstählen zu einem Bruchteil des einstigen Werts stattfand (Lunden, 2017).

Der Verlust des Vertrauens unter Kunden und Lieferanten macht oft kosten- und zeitintensive Abhilfemaßnahmen nötig. Ihnen müssen zumindest temporär zusätzliche Anreize geliefert werden, deren Kosten schwer abschätzbar sind. Neben der tatsächlichen Sicherheit muss vor allem auch in die gefühlte Sicherheit investiert werden. Schätzungen legen nahe, dass der Markenwert als Folge eines Datenlecks um etwa ein Fünftel fällt und es acht Monate dauert, um den Ruf wiederherzustellen (Experian, 2011, 5). Ein Cyberspionagevorfall kann also auch strategisch von Konkurrenten zur Rufschädigung eingesetzt werden. Auch intern kann die Rufschädigung enormen Schaden verursachen, etwa indem sie demotivierend auf Mitarbeiter wirkt und die Mitarbeiterfluktuation begünstigt (vgl. Bitkom, 2016, 15).

Opportunitätskosten sind die dritte massive Komponente der indirekten Kosten. Cyberspionage verringert die Innovationstätigkeit von Unternehmen. Aufgrund des geringeren ROI sinkt der Anreiz, innovativ zu agieren und in Forschung und Entwicklung zu investieren. Außerdem entstehen Opportunitätskosten dadurch, dass sich Unternehmen als Folge eines Cyberspionagevorfalls unter Umständen risikoaverser verhalten und weniger innovative, webbasierte Technologien anwenden. Das kann dazu führen, dass dem betroffenen Unternehmen ganze Geschäftszweige verschlossen bleiben oder sich verschließen. Selbst wenn das Unternehmen in der Folge weniger IT-basiert arbeitet, können die Ausgaben für IT-Sicherheit durch zusätzlich nötig gewordenen Schutzmaßnahmen massiv steigen. Nicht selten sind Cyberattacken Pilotangriffe, die Schwachstellen für nachfolgende Angriffe identifizieren und offenlegen sollen (Cebr, 2016, 22). Des Weiteren kommt es durch Cyberspionage zu umfassenden, kostenintensiven Rechtsstreitigkeiten, die den Kostenapparat weiter aufblähen und die Opportunitätskosten treiben.

Das Verhältnis der direkten zu den indirekten Kosten ist je nach Art und Branche des Unternehmens und des Spionagevorfalls (betroffene Daten, Umfang, Zeitablauf) unterschiedlich. Eine generelle Aussage darüber, welche Kostenkomponente größer ist, ist nicht möglich. Generell ist davon auszugehen, dass das Ausspionieren von Kundendaten besonders die indirekten Kosten über die Reputationsschäden erhöht, während das Ausspionieren von Forschungsdaten über den Wert des geistigen Eigentums eher die direkten Kosten fördert. Allerdings sind die direkten und indirekten Kosten über den Umsatzausfall auch kaum trennbar miteinander verbunden.

4.3 Volkswirtschaftliche Kosten

Der dritte Kostentyp, die volkswirtschaftlichen Kosten, aggregiert die Schäden von der mikroökomischen Unternehmensebene auf die makroökonomische Ebene. So führt eine reduzierte Innovationstätigkeit der Unternehmen zu einer generell weniger innovativen Volkswirtschaft, was die Wettbewerbsfähigkeit mindert und den Standort Deutschland unattraktiver macht. Die Handelsbilanz verschlechtert sich, da Cyberspionage meist aus dem Ausland initiiert wird und ausländische Unternehmen in der Folge im Markt relativ bessergestellt sind. Der Diebstahl von IP fungiert als unmittelbare Subvention für den Erwerber (McAfee, 2014, 13). Insgesamt wird geschätzt, dass Cyberkriminalität etwa 15 bis 20 Prozent des Gesamtwertes der Internetökonomie kostet, was als eine Steuer auf Innovation und Wachstum in der IT betrachtet werden kann (McAfee, 2014, 3).

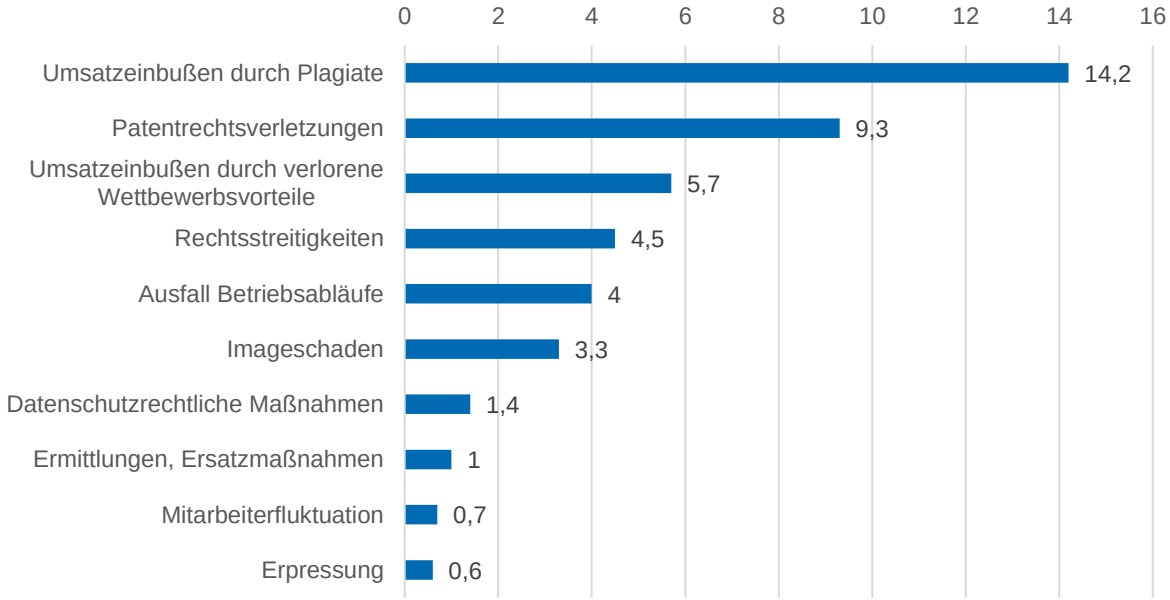
Auch auf dem Arbeitsmarkt führt Cyberspionage zu erheblichen Kosten. So musste eine Firma ihre Mitarbeiterschaft von 800 auf 400 halbieren, nachdem Hacker IP gestohlen und ein konkurrierendes Produkt eingeführt hatten (McAfee, 2014, 13). Laut Detica (2011) kommt es durch Cybercrime zu erheblichen Steuerrückgängen und Verlusten durch das verringerte Vertrauen von ausländischen Investoren in die Sicherheit der heimischen Unternehmen.

4.4 Versuche der Quantifizierung

Die Kosten von Cyberspionage zu quantifizieren ist ein komplexes Unterfangen und führt eher zu verzerrten Schätzungen als zu präzisen Aussagen. Zahlreiche Studien von Auftraggebern mit unterschiedlicher Agenda und variantenreichen Kostendefinitionen geben ein recht unscharfes Bild von den tatsächlichen Schäden durch Cyberspionage ab. In vielen Studien werden Spionagevorfälle auch nicht sauber von anderen Arten der Cyberkriminalität unterschieden. Dennoch werden an dieser Stelle zumindest Versuche der Quantifizierung unternommen, indem verschiedene Umfrage- und Schätzergebnisse vorgestellt werden.

Die OECD geht davon aus, dass Fälschung und Piraterie (nicht nur basierend auf Cyberspionagevorfällen) Unternehmen weltweit 638 Milliarden US-Dollar pro Jahr kosten. Das US-amerikanische Handelsministerium schätzt die Schäden durch IP-Diebstahl aller Art allein für amerikanische Unternehmen auf 200 bis 250 Milliarden US-Dollar pro Jahr (beides McAfee, 2014). McAfee (2014) selbst spricht von 445 Milliarden US-Dollar an Schäden weltweit und 100 Milliarden US-Dollar für amerikanische Unternehmen.

Abbildung 6: Aufgetretene Schäden nach Delikttyp
in Milliarden Euro (konservative Berechnung)
Basis: Alle befragten Industrieunternehmen, die in den vergangenen zwei Jahren von Datendiebstahl, Industriespionage oder Sabotage betroffen waren (n=349); Antworten um Ausreißer (2,5 Prozent der größten und kleinsten Werte) bereinigt und hochgerechnet



Quelle: Bitkom, 2016; eigene Darstellung

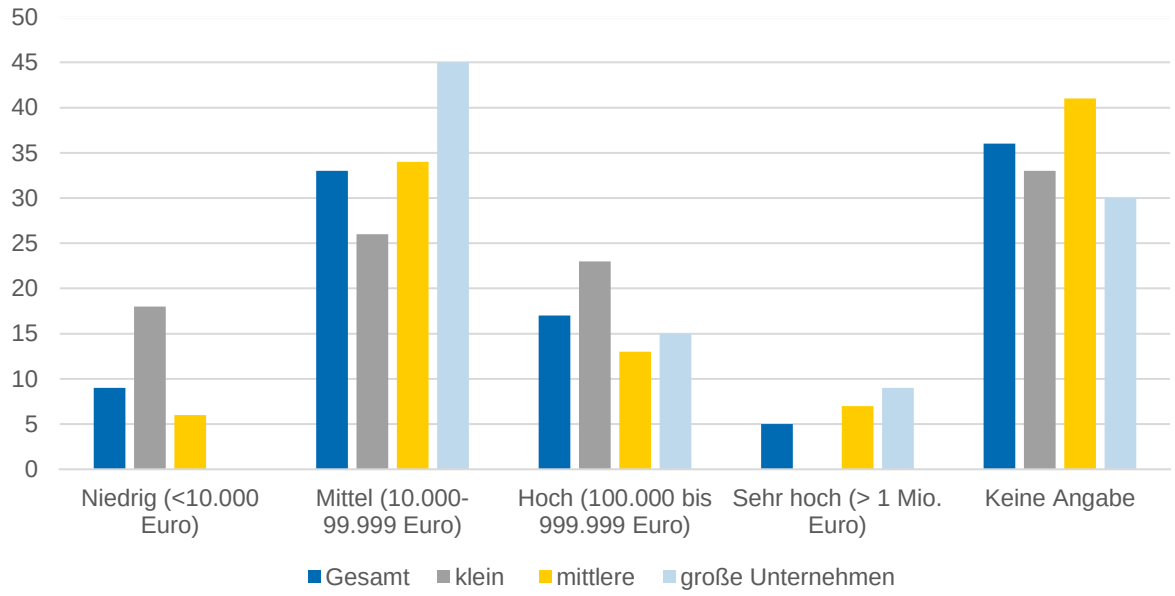
Eine nichtrepräsentative Studie des Ponemon Institute (2016) berechnet, dass der Diebstahl eines Kundendatensatzes deutsche Unternehmen insgesamt etwa 154 Euro kostet. Durchschnittlich werden laut der Studie bei einem Spionagevorfall etwa 24.000 Datenschätze gestohlen. Bitkom (2015) schätzt die Schäden für die deutsche Wirtschaft auf 51 Milliarden Euro jährlich. Bitkom (2016, 26) schlüsselt die aufgetretenen Schäden in einer repräsentativen Studie nach Delikttyp auf (Abbildung 6) und errechnet jährliche Schäden von 22,35 Milliarden Euro für die deutsche Industrie. Mehr als ein Viertel des Schadens geht auf Umsatzverluste durch Plagiate zurück. Es folgen Umsatzverluste durch Patentrechtsverletzungen, welche ähnliche Folgen wie Plagiate haben. Umsatzeinbußen durch verlorene Wettbewerbsvorteile, etwa durch einen verlorenen Vorsprung bei der Einführung neuer Produkte, der es Industrieunternehmen erlaubt, höhere Preise zu verlangen und damit Entwicklungskosten zu amortisieren, sind relativ wenig kostspielig. Cebr (2016, 10) geht von Schäden in Höhe von 13 Milliarden Euro jährlich über die vergangenen fünf Jahre für große deutsche Unternehmen aus. Zusammenfassend sind jährliche Schäden in hoher zweifacher Milliardenhöhe zu erwarten, die Dunkelziffer ist hoch.

KPMG (2017, 24) berücksichtigt, dass Schadenssummen schwer gemittelt werden können, da sie oft sehr unterschiedlich ausfallen und durch Extremwerte geprägt sind, indem die Kosten in Größenkategorien aufgelistet werden, ohne einen allgemeinen

Durchschnitt zu bilden. Die Schadenssumme bezieht sich auf den Zeitraum der vergangenen zwei Jahre und beinhaltet laut KPMG den eingetretenen Verlust, den entgangenen Gewinn, Ermittlungs- und Folgekosten, Bußgelder, Geldstrafen und eventuelle Gewinnabschöpfungen. Der realisierte Schaden nimmt mit der Unternehmensgröße zu (Abbildung 7). Die meisten Fälle fielen in die Kategorie der mittleren Schäden bis unter 100.000 Euro. Drei Viertel der Unternehmen nannten Schäden im Bereich bis zu 250.000 Euro. Die Hälfte der Angaben bewegt sich im Bereich zwischen 15.000 und 120.000 Euro. Jedes zwanzigste Unternehmen hat mehr als eine Million Euro an Schäden in den Büchern, unter größeren Unternehmen sogar jedes zehnte (KPMG, 2017, 9).

Abbildung 7: Gesamtschaden durch Cyberkriminalität

Angaben in Prozent, Zeitraum 2015/2016



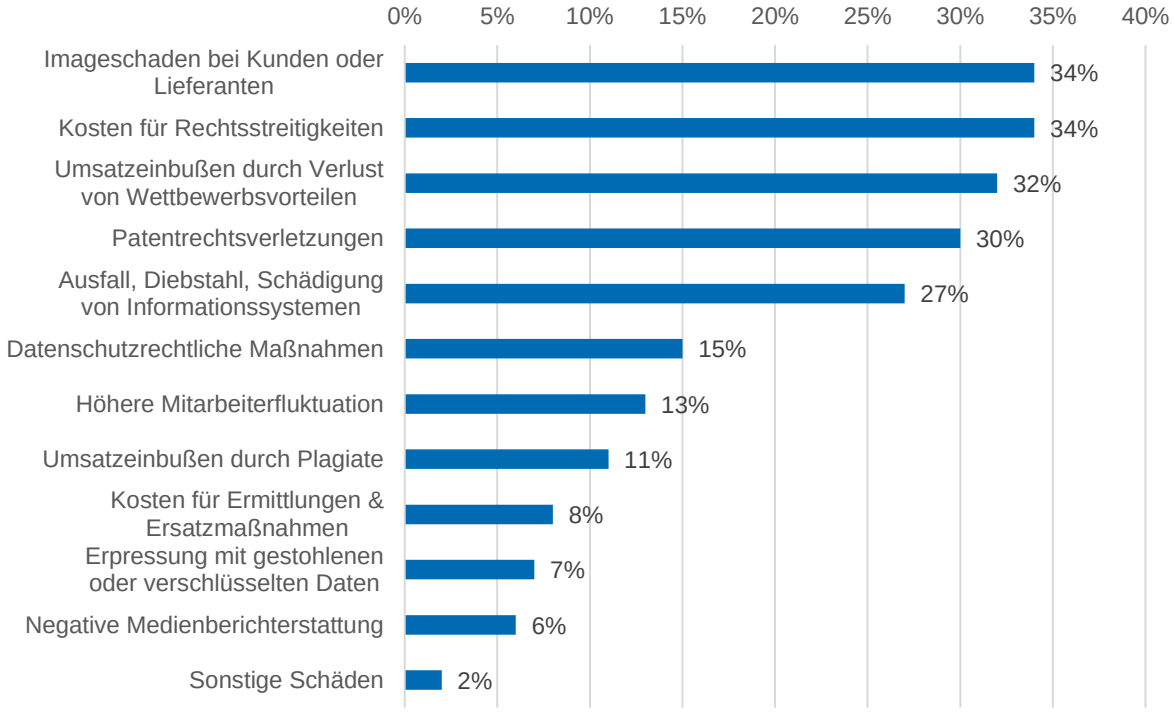
Klein: Unternehmen mit einem Umsatz unter 250 Mio. Euro; mittel: 250 Mio. bis unter 3 Mrd. Euro; groß: mehr als 3 Mrd. Euro

Quelle: KPMG, 2017, 24; eigene Darstellung

Auffallend viele Unternehmen wollten oder konnten keine Angabe zur Schadenssumme machen, was die Vermutung nahelegt, dass eine Bezifferung schwierig ist, etwa auch, weil die Kosten selten als eigenständige Summen verbucht werden. Es fällt ebenfalls auf, dass viele Befragte die Schadenssumme auf null beziffern, obwohl sie angeben, von Cybersicherheitsvorfällen betroffen zu sein. Eine mögliche Erklärung ist, dass die Aufarbeitung nicht als separater Kostenpunkt betrachtet wird (KPMG, 2017, 9). Delikte im Zusammenhang mit der Verletzung geistigen Eigentums verursachen im Vergleich zu den anderen abgefragten Arten der Cyberkriminalität deutlich größere Schäden, geschehen aber auch seltener als andere Arten. Für die Verletzung von Geschäfts- und Betriebsgeheimnissen liegen diese meist zwischen wenigen Tausend bis

zu 250.000 Euro, für die Verletzung von Urheberrechten zwischen 20.000 und 800.000 Euro. Ermittlungs- und Folgekosten haben dabei einen relativ geringen Anteil an den Gesamtkosten (KPMG, 2017, 25).

Abbildung 8: Aufgetretene Schadensfälle
Mehrfachnennungen der befragten Unternehmen, in Prozent
Basis: Alle befragten Industrieunternehmen, die in den vergangenen zwei Jahren von Datendiebstahl, Industriespionage oder Sabotage betroffen waren (n=349)



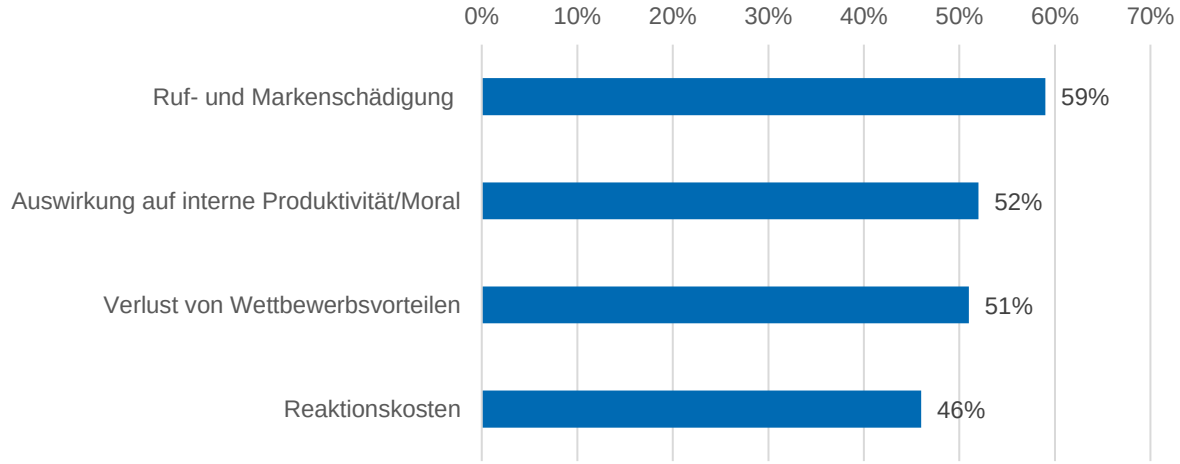
Quelle: Bitkom, 2016; eigene Darstellung

Ein anderer Versuch der Einschätzung der Kosten wird über die aufgetretenen Schadensarten geleistet (Abbildung 8). Basis der Untersuchung des Bitkom (2016) sind Industrieunternehmen in Deutschland, die innerhalb von zwei Jahren Opfer von Cyberkriminalität (darunter Cyberspionage) geworden sind. Die Arten der aufgetretenen Kosten sind mannigfaltig. Jeweils mehr als ein Drittel der angegriffenen Industrieunternehmen war mit Rechtsverfolgungskosten und Imageschäden konfrontiert. Dicht darauf folgen Umsatzeinbußen durch Wettbewerbsnachteile, welche nach Studiendefinition aus zwei Gründen entstehen: entweder indirekt, weil die Konkurrenz durch die Kenntnis neuer Fertigungsmethoden effizienter produziert, oder direkt, etwa durch Unterbieten bei Ausschreibungsverfahren und dem damit einhergehenden Auftragsverlust. An vierter Stelle stehen Patentrechtsverletzungen. Auch der Ausfall, Diebstahl und die Schädigung von Informationssystemen werden von knapp einem Drittel der betroffenen Unternehmen genannt. Weitere aufgetretene Schadenvorfälle sind divers, werden aber von deutlich weniger Unternehmen angeführt. Wettbewerbsnachteile betreffen mit 41 Prozent vor allem große Unternehmen mit mehr als 500 Mitarbeitern. Für

mittelständische Unternehmen waren in einem Viertel aller Fälle datenschutzrechtliche Maßnahmen ein Kostentreiber. Diese bestehen vor allem aus Informationskosten der Bevölkerung (Bitkom, 2016, 15).

Eine alternative Einschätzung der Kosten eines Cybersicherheitsvorfalls bietet eine Studie über die Befürchtungen der Unternehmen, welche Kosten auf sie zukommen könnten (Abbildung 9). Laut Cebr (2016) fürchten insgesamt 46 Prozent der Unternehmen die Kosten eines Cybersicherheitsvorfalles – relativ wenig gemessen an der hohen Anzahl der Betroffenen. Knapp 60 Prozent davon haben Angst vor einer Ruf- und Markenschädigung – Imageschäden spielen also ähnlich wie bei Bitkom (2015) eine große Rolle. Es ist zu erwarten, dass die Angst vor der Rufschädigung noch steigt, da das IT-Sicherheitsgesetz mehr und mehr Unternehmen aus mehr und mehr Branchen dazu verpflichtet, ernsthafte Cybersicherheitsverstöße zu melden: Neben Unternehmen aus den Sektoren Energie, Informationstechnik und Telekommunikation, Wasser sowie Ernährung sind mit dem zweiten Teil der sogenannten KRITIS-Verordnung auch Unternehmen aus den Sektoren Finanzen, Transport und Verkehr sowie Gesundheit betroffen (vgl. BSI, 2017). Gut die Hälfte der Unternehmen fürchtet Auswirkungen auf die Moral der Mitarbeiterschaft und damit auf die interne Produktivität. Der Verlust von Wettbewerbsvorteilen und Reaktionskosten spielen auch eine vergleichbar große Rolle.

Abbildung 9: Befürchtete Kosten
Anteil an Unternehmen, die jeweilige Kosten befürchten, in Prozent
Basis: 205 Unternehmen ab 1.000 Mitarbeitern mit Sitz in Deutschland

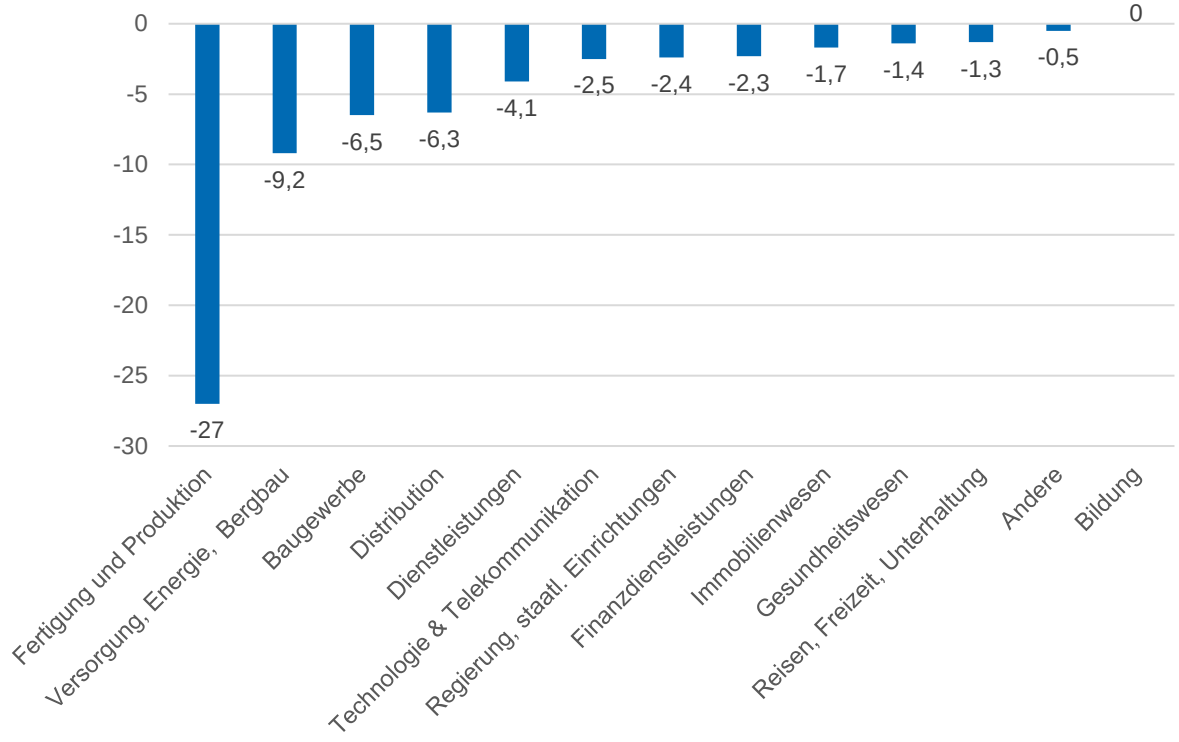


Quelle: Cebr, 2016; eigene Darstellung

Besonders betroffen vom Umsatzrückgang durch Cyberkriminalität sind laut Cebr (2016) die Bereiche Fertigung und Produktion sowie Versorgung, Energie und Bergbau (Abbildung 10). In Fertigung und Produktion gibt es zahlreiche attraktive Daten, die im Interesse der Hacker stehen. Manipulation und Sabotage fügen Konkurrenten

in diesem Bereich hohen Schaden zu. Die Energiebranche weist besonders stark vernetzte Prozesse auf und ist deshalb sehr kostspieligen Cyberangriffen ausgesetzt.

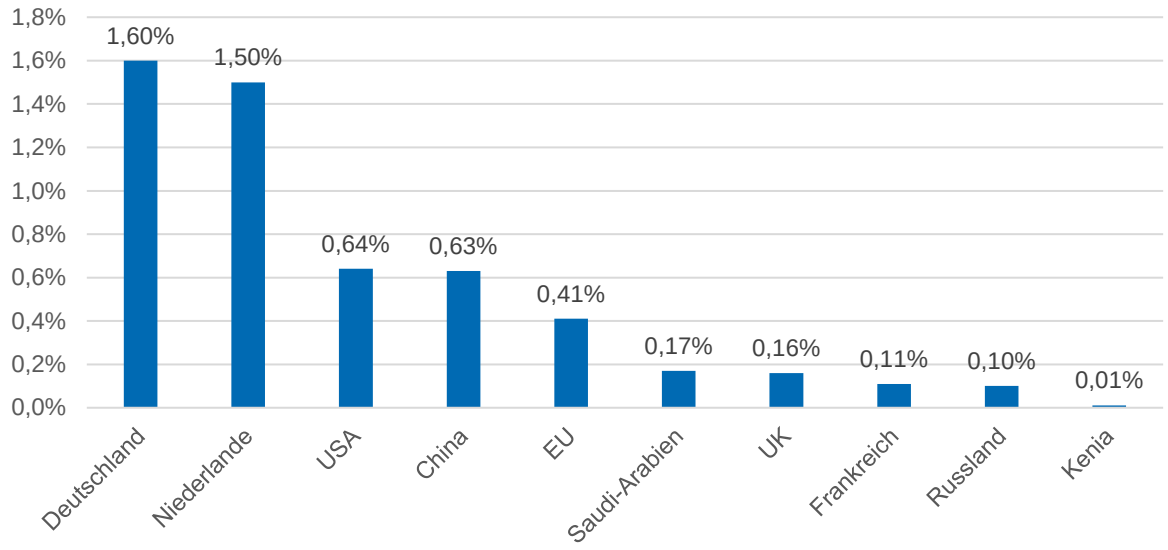
Abbildung 10: Geschätzter Umsatzrückgang als Folge von Cyberattacken in den vergangenen fünf Jahren nach Branchen, in Mrd. Euro



Quelle: Cebr, 2016; eigene Darstellung

Im weltweiten Vergleich ist Deutschland überdurchschnittlich von Cyberkriminalität betroffen. McAfee (2014, 8f.) hat Schätzungen zur Schadenshöhe für unterschiedliche Länder zusammengetragen, für die Studien verfügbar waren (Abbildung 11). In Deutschland und den Niederlanden liegt der Anteil der Schäden am BIP mit 1,6 bzw. 1,4 Prozent deutlich höher als in Ländern wie den USA, China oder der EU insgesamt. Dies zeigt wiederum, dass gerade deutsche Unternehmen mit ihrem IP-Reichtum im Zuge von Industrie 4.0 ein besonders lohnenswertes Ziel für Hacker sind. Da der BIP-Anteil jedoch noch unter zwei Prozent liegt, wird er gerne als „akzeptabel“ angenommen (McAfee, 2014, 11). Dies ist jedoch ein Trugschluss – zum einen, weil die Schätzungen nur eine Schadensuntergrenze sind und zum anderen, weil die Bedeutung von Cyberkriminalität und insbesondere auch Cyberspionage zunimmt.

Abbildung 11: Weltweiter Vergleich
Schäden durch Cyberkriminalität, in Prozent des Bruttoinlandsprodukts



Quelle: McAfee, 2014; eigene Darstellung

5. Empfehlungen an Unternehmen und Politik

In den vorangegangenen Kapiteln wurden der Umfang und die Vielfalt der Kosten von Cyberkriminalität im Allgemeinen und Cyberspionage im Besonderen dargestellt. Auch wenn eine eindeutige Quantifizierung der Kosten schwierig ist und Cyberkriminalität als wissenschaftliche Disziplin noch in ihren Kinderschuhen steckt (vgl. Armin et al. (2015, 708), wird die Relevanz von Cybersicherheit deutlich. Im Zuge der Digitalisierung und mit einer zunehmenden Anzahl an internetfähigen Produkten und Maschinen wird die Angreifbarkeit der Unternehmen und ihrer Daten zunehmen und das Thema Cyberspionage weiter an Brisanz gewinnen. Um die Wertschöpfung der deutschen Wirtschaft durch Vorsprung in Know-how und Technik zu schützen, müssen Unternehmen und Politik Maßnahmen zur Cybersicherheit ergreifen. Im Folgenden werden notwendige, aber keinesfalls hinreichende Maßnahmen erläutert.

IT-Sicherheitsstrategie im Unternehmen etablieren: Unternehmen müssen wettbewerbs- und geschäftskritische Daten eigenverantwortlich schützen und erforderliche Sicherheitsmaßnahmen wie Security-by-Design (integrierte Softwaresicherheit) und Privacy-by-Design (integrierter Datenschutz) berücksichtigen. Mit guter Technik, einem sauberen Updatemanagement und aktueller Software können Unternehmen bereits einen guten Basisschutz erreichen. Oftmals wird die vorhandene Sicherheitstechnologie noch zu wenig genutzt, weil sie nicht verstanden wird oder zu teuer ist. Eine IT-Sicherheitsstrategie in jedem Unternehmen hilft, sich über schützenswerte Daten und Sicherungsprozesse bewusst zu werden sowie Risiken und Sicherheitslücken zu

definieren und zu schließen. 2015 hatten laut Eurostat (2015) etwa 71 Prozent der deutschen Unternehmen keine formellen Cybersicherheitsrichtlinien wie beispielsweise ein sicheres Anwendungsentwicklungsprogramm. Nur knapp ein Fünftel der Unternehmen hat eine solche Strategie, die innerhalb der vergangenen 12 Monate definiert oder überprüft wurde. Der EU-28-Durchschnitt lag bei 32 bzw. 20 Prozent. In nur 19 Prozent der deutschen Unternehmen war die Geschäftsführung am Cyber-Risikomanagement beteiligt (regelmäßige Sicherheitsupdates, Risikomanagement-Meetings). Der präventive Ansatz der Schadensvorbeugung reicht für Cybersicherheit nicht aus. Eine wichtige Rolle kommt auch dem sogenannten Incident Management im Schadensfall zu, mit dem der entstandene Schaden minimiert wird. Immerhin planen laut Cebr (2016, 12) 89 Prozent der deutschen Unternehmen, ihre Ausgaben für Cybersicherheit zu erhöhen.

Mitarbeiter sensibilisieren: Allerdings hilft Technik nicht alleine. Zentral ist die Einbeziehung der Mitarbeiter, denn Mitarbeiter sind die wirkungsvollste Firewall – und die Sicherheit abhängig vom schwächsten Glied, dem einfachsten Einfallstor des Systems (Böhme/Moore, 2010). Laut KPMG (2017, 19) begünstigt vor allem Unachtsamkeit Cyberkriminalität. Das zwiespältige Verhältnis vieler Menschen zu Wissen und Technik, die irrationalen Ängste einerseits und das irrationale Vertrauen andererseits, müssen durch umfangreiche Aufklärungsmaßnahmen auch seitens der Politik beseitigt werden. Dann ist Mitarbeitern auch tendenziell eher bewusst, welche Daten besonders geschützt werden müssen. Diese sogenannten Kronjuwelen müssen klar von den Unternehmen definiert werden. Junge Menschen müssen in Schulen, Hochschulen und Ausbildungszentren Digitalkompetenzen wie IT-Sicherheits-Kompetenzen erlangen.

Informationen austauschen: Unternehmen müssen sich gegenseitig zeitnah und vertrauensvoll über Cyberattacken informieren, um die Cybersicherheit aller zu verbessern (Gal-Or/Ghose, 2005; Gordon et al., 2003). Eine Attacke gegen ein Unternehmen kann als Warnung für andere verstanden werden. Unternehmen können Angriffe leichter erkennen und abwehren. Auf diese Weise führt Nachlässigkeit eines Unternehmens nicht notwendigerweise dazu, dass viele andere auch Schäden verzeichnen, was angesichts großer Unternehmensnetzwerke besonders bedeutsam ist. Betroffene Unternehmen müssen Spionagesachverhalte sowie Verdachtsmomente gegenüber den Sicherheitsbehörden offensiv anzeigen, um gemeinsam Sicherheitsstrategien den Entwicklungen anpassen zu können.

Der Sinn für Kooperationen bei Angriffen sowie für mehr Transparenz bei den Abwehrstrategien scheint bislang allerdings nur wenig ausgeprägt zu sein. Viele Unternehmen wollen öffentlich keine Stellung zu möglichen Angriffen oder Verteidigungsstrategien nehmen. Aus Angst vor Reputationsschäden informieren Unternehmen oft

nicht über Vorfälle: Laut Armin et al. (2015, 703) werden 44 Prozent der Vorfälle weltweit nicht der Polizei gemeldet. Nur 43 Prozent der Unternehmen geben an, überhaupt Informationen über Cyberattacken zu teilen. Diese Informationsasymmetrie kann nur politisch geregelt werden. Das IT-Sicherheitsgesetz kann potentiell dazu führen, dass mehr Informationen über Vorfälle ausgetauscht werden. Bislang nimmt es jedoch vor allem die Betreiber kritischer Infrastrukturen in die Pflicht und umfasst bei allen anderen Unternehmen nicht die interne Kommunikation, weshalb die Reichweite in Bezug auf Industrie-4.0-Unternehmen begrenzt ist (Lehmann, 2017). Dennoch müssen Unternehmen dafür Sorge tragen, dass Angriffe von außen nicht in die innere Prozessstruktur eindringen können. Sicherungsmaßnahmen sollen dem „Stand der Technik" entsprechen und müssen laut Gesetzesbegründungen angemessen sein, womit sie von wirtschaftlichen Erwägungen abhängig sind. Angesichts der obigen Ausführungen über die schwere Einschätzbarkeit der Kosten und Folgen von Cyberspionagevorfällen könnten diese wirtschaftlichen Erwägungen jedoch fehlgeleitet sein. Die Politik muss deshalb besonders für KMU zusätzlich für ein Anreizmodell für Investitionen in Cybersicherheit eintreten, etwa indem sie Sicherheitsboni verteilt.

Cybersicherheit zum strategischen Faktor machen: Es ist wichtig zu erkennen, dass Unternehmen keine Wettbewerbsvorteile haben, wenn sie ihre Produkte und Prozesse mit weniger Sicherheitsfunktionen ausstatten. Sicherheit muss im Sinne von Security-by-Design verstärkt im Produktionsprozess mitgedacht werden. Die Bevölkerung muss aufgeklärt werden, sodass sie die Sicherheit eines Produktes bewerten und zu einem relevanten Faktor bei der Kaufentscheidung machen kann. Eine freiwillige Kennzeichnung für die Sicherheit von vernetzten Geräten erhöht die digitale Souveränität der Anwender: Ein informierter Konsument wird sich eher für das Produkt mit einem höheren Maß an Cybersicherheit entscheiden. Dennoch darf ein solches Gütesiegel nicht dazu führen, dass Cybersicherheit weiterhin als Feature statt als grundsätzliche Anforderung an ein Produkt gesehen wird (Kleinhans, 2017, 9). Verpflichtende Mindeststandards müssen auf europäischer Ebene insbesondere für IoT-Geräte durchgesetzt werden.

Cybersicherheit ist der Anschnallgurt der digitalen Gesellschaft: Autos wären zwar billiger, wenn man sie ohne Anschnallgurte baute, aber diese sind unerlässlich. Ebenso unerlässlich ist die Cybersicherheit für die deutsche Wirtschaft und damit den gesellschaftlichen Wohlstand. Die Analyse der Kosten durch Cyberspionagevorfälle zeigt, welches Schadenpotenzial in Cyberangriffen steckt. Eine erfolgreiche Digitalisierung von Staat, Wirtschaft und Gesellschaft kann es ohne Cybersicherheit nicht geben. Politik, Unternehmen und die Zivilgesellschaft sind angehalten, für Gefahren aus dem Netz zu sensibilisieren und Cybersicherheit zu fördern, denn zur Digitalisierung gibt es keine Alternative.

Literatur

Allianz, 2017, Allianz Risk Barometer – Die zehn wichtigsten Geschäftsrisiken 2017, http://www.agcs.allianz.com/insights/white-papers-and-case-studies/allianz-risk-barometer-2017/ [28.2.2017]

Anderson, Ross, 2001, Why Information Security is Hard – An Economic Perspective, Proceedings oft he 17th Annual Computer Security Applications Conference, S. 358 – 365, IEEE Computer Society

Anderson, Ross / **Baron**, Chris / **Böhme**, Rainer / **Clayton**, Richard / **van Eten**, Michel J.G. / **Levi**, Michael / **Moore**, Tyler / **Savage**, Stefan, 2013, Measuring the Cost of Cybercrime, in: Böhme, Rainer (Hrsg.), The Economics of Information Security and Privacy, S. 265 – 300, Heidelberg

Armin, Jart / **Thompson**, Bryn / **Ariu**, David / **Giacinto**, Giorgio / **Roli**, Fabio / **Kijewski**, Piotr, 2015, 10th International Conference on Availability, Reliability and Security (ARES), http://ieeexplore.ieee.org/document/7299982/?reload=true [2.5.2017]

AV-TEST, 2017, Malware, https://www.av-test.org/de/statistiken/malware/ [9.3.2017]

Bitkom, 2016, Datendiebstahl, Spionage und Sabotage in der Industrie, https://www.bitkom.org/Presse/Presseinformation/Industrie-im-Visier-von-Cyberkriminellen-und-Nachrichtendiensten.html [27.3.2017]

Bitkom, 2015, Digitale Wirtschaftsspionage, Sabotage und Datendiebstahl https://www.bitkom.org/Presse/Presseinformation/Digitale-Angriffe-auf-jedes-zweite-Unternehmen.html [4.4.2017]

BMBF – Bundesministerium für Bildung und Forschung, 2017, 92 Prozent der Infrastruktur des Internets sind verwundbar, https://www.bmbf.de/de/92-prozent-der-infrastruktur-des-internets-sind-verwundbar-3843.html [27.3.2017]

BMI – Bundesministerium des Innern, 2016, Cyberspionage, http://www.bmi.bund.de/DE/Themen/Sicherheit/IT-Cybersicherheit/Cyberspionage/cyberspionage_node.html [2.3.2017]

Böhme, Rainer / **Moore**, Tyler, 2010, The iterated weakest link, IEEE Security & Privacy, Jg. 8, Nr. 1, S. 53 – 55

BSI –Bundesamt für Sicherheit in der Informationstechnik, 2017, Das IT-Sicherheitsgesetz, https://www.bsi.bund.de/DE/Themen/Industrie_KRITIS/IT-SiG/it_sig_node.html [10.4.2017]

BSI –Bundesamt für Sicherheit in der Informationstechnik, 2016, Die Lage der IT-Sicherheit in Deutschland 2016, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2016.html [2.4.2017]

Bundesamt für Verfassungsschutz, 2015, Wirtschaftsspionage – Risiko für Unternehmen, Wissenschaft und Forschung, https://www.verfassungsschutz.de/download/broschuere-2014-07-wirtschaftsspionage.pdf [15.3.2017]

Campbell, Katherine / **Gordon**, Lawrence A. / **Loeb**, Martin P. / **Zhou**, Lei, 2003, The economic cost of publibly announced information security breaches: Empirical evidence from the stock market, Journal of Computer Security, Jg. 11, Nr. 3, S. 431 – 448

Cebr – Centre for Economics and Business Research, 2016, Konsequenzen unzureichender Cyber-Sicherheit für Unternehmen und Wirtschaft in Deutschland – Ein Bericht für Veracode, http://www.veracode.com/sites/default/files/Resources/AnalystReports/business-and-economic-consequences-of-inadequate-cybersecurity-the-case-of-germany-de.pdf [3.3.2017]

Check Point, 2016, 2016 Security Report, Tel Aviv/Israel

Breach Level Index, 2017, Data Breach Statistics, http://breachlevelindex.com/ [9.3.2017]

Caputo, Deanna D. / **Pfleeger**, Shari L., 2012, Leveraging behavioral science to mitigate cyber security risk, Computers and Security, Jg. 31, Nr. 4, S. 597 – 611

Demary, Vera / **Engels**, Barbara / **Röhl**, Klaus- Heiner / **Rusche**, Christian, 2016, Digitalisierung und Mittelstand – Eine Metastudie, IW-Analyse, Nr. 109, Köln

Detica, 2011, The Cost of Cybercrime: A Detica report in partnership with the Office of Cyber Security and Information Assurance in the Cabinet Office, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60943/the-cost-of-cyber-crime-full-report.pdf [28.04.2017]

Eurostat, 2015, ICT security in enterprises, http://ec.europa.eu/eurostat/statistics-explained/index.php/ICT_security_in_enterprises [20.4.2017]

Experian, 2011, https://www.experian.com/assets/data-breach/white-papers/reputation-study.pdf [10.3.2017]

Gal-Or, Esther / **Ghose**, Anindya, 2005, The Economic Incentives for Sharing Security Information, Information Systems Research, Jg. 16, Nr. 2, S. 186 – 208

Gordon, Lawrence A. / **Loeb**, Martin P. / **Lucyshyn**, William, 2003, Sharing information on computer systems security: An economic analysis, Journal of Accounting and Public Policy, Jg. 22, Nr. 6, S. 461 – 485

Kaspersky Lab, 2017, Targeted Cyberattacks Logbook, https://apt.securelist.com/#firstPage [9.3.2017]

Kleinhans, Jan-Peter, 2017, Strategische IT-Sicherheitspolitik für das Internet der Dinge – Handlungsoptionen für die Politik, Berlin

KPMG, 2017, e-Crime in der deutschen Wirtschaft 2017 – Computerkriminalität im Visier, https://home.kpmg.com/de/de/home/themen/2017/04/ecrime-studie.html [15.4.2017]

Landwehr, Andreas, 2016, Deutschland und China wollen Mechanismus gegen Cyber-Spionage schaffen, https://www.heise.de/newsticker/meldung/Deutschland-und-China-wollen-Mechanismus-gegen-Cyber-Spionage-schaffen-3377805.html [7.4.2017]

Lehmann, Hendrick, 2017, Chancen und Risiken von Industrie 4.0 – Von Anfang bis Ende, PROTECTOR 1-2/2017, S. 16 – 17

LKA Niedersachsen, 2013, Dunkelfeldstudie – Befragung zu Sicherheit und Kriminalität in Niedersachsen, http://www.lka.niedersachsen.de/forschung/dunkelfeldstudie/dunkelfeldstudie-befragung-zu-sicherheit-und-kriminalitaet-in-niedersachsen-109236.html [9.3.2017]

Lunden, Ingrid, 2017, After data breaches, Verizon knocks $350M off Yahoo sale, now valued at $4.48B, https://techcrunch.com/2017/02/21/verizon-knocks-350m-off-yahoo-sale-after-data-breaches-now-valued-at-4-48b/ [22.2.2017]

McAfee, 2014, Net Losses: Estimating the Global Cost of Cybercrime, https://www.mcafee.com/resources/reports/rp-economic-impact-cybercrime2.pdf [2.4.2017]

Meinel, Christoph / **Sack**, Harald, 2014, Sicherheit und Vertrauen im Internet – Eine technische Perspektive, Wiesbaden

OAG – Office of the Attorney General, 2017, Search Data Security Breaches, California Department of Justice, https://oag.ca.gov/ecrime/databreach/list [3.5.2017]

Ponemon Institute, 2016, 2016 Cost of Data Breach Study – Germany, http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEL03094DEEN [10.3.2017]

Rieckmann, Johannes / **Kraus**, Martina, 2015, Tatort Internet: Kriminalität verursacht Bürgern Schäden in Milliardenhöhe, DIW Wochenbericht Nr.12, S. 295 – 301

Rixecker, Kim, 2017, Safer Internet Day: Wir räumen mit 4 Mythen zur IT-Sicherheit auf, http://t3n.de/news/it-sicherheit-mythen-793041/ [7.2.2017]

Sicherheitstacho, 2017, Übersicht über die aktuellen Cyberangriffe auf DTAG-Sensoren, http://www.sicherheitstacho.de/ [9.3.2017]

Verizon, 2016, Data Breach Investigations Report, http://www.verizonenterprise.com/resources/reports/rp_Verizon-2016-executive-summary_xg_en.pdf [5.3.2017]

WTO – World Trade Organization, 2017, What are intellectual property rights?, https://www.wto.org/english/tratop_e/trips_e/intel1_e.htm [3.5.2017]