KPMG
cutting through complexity

IT-Sicherheit in Deutschland

Handlungsempfehlungen für eine zielorientierte Umsetzung des IT-Sicherheitsgesetzes

kpmg.de

INHALT

Tabellen- und Abbildungsverzeichnis

Abkürzungsverzeichnis

BIGS	Brandenburgisches Institut für Gesellschaft und Sicherheit
BITKOM	Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V.
BMBF	Bundesministerium für Bildung und Forschung
BMI	Bundesministerium des Innern
BMWi	Bundesministerium für Wirtschaft und Energie
BNetzA	Bundesnetzagentur
BSI	Bundesamt für Sicherheit in der Informationstechnik
CASED	Center for Advanced Security der Universität Darmstadt
CISPA	Center for IT-Security, Privacy and Accountability
EC-SPRIDE	European Center for Security and Privacy by Design
EITO	European Information Technology Observatory
ENISA	Europäische Agentur für Netz- und Informationssicherheit
FOKUS	Fraunhofer-Institut für offene Kommunikationssysteme
HPI	Hasso-Plattner-Institut
INSI	Institution im besonderen staatlichen Interesse
ITK	Informationstechnik und Kommunikation
KASTEL	Kompetenzzentrum für angewandte Sicherheitstechnologie
KMU	Kleine und mittlere Unternehmen
KRITIS	Kritische Infrastrukturen
MINT	Mathematik, Informatik, Naturwissenschaft und Technik
SaaS	Security as a Service
SIEM	Security Information and Event Management System
SKM	Standardkosten-Modell
SPOC	Single Point of Contact
TK	Telekommunikationsdiensteanbieter und Netzbetreiber
TKG	Telekommunikationsgesetz
UP Bund	Umsetzungsplan für die Gewährleistung der IT-Sicherheit in der Bundesverwaltung

EXECUTIVE SUMMARY

Das Bundesministerium des Innern (BMI) hat am 12. März 2013 den Referentenentwurf eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme vorgestellt (im Folgenden auch IT-Sicherheitsgesetz), mit dem das Ministerium das Ziel einer Verbesserung der IT-Sicherheit in Deutschland verfolgt. Zu den wesentlichen Regelungsinhalten des Referentenentwurfs gehören insbesondere eine Pflicht zur Meldung von IT-Sicherheitsvorfällen durch Betreiber kritischer Infrastrukturen und Telekommunikationsanbieter sowie die Einführung von IT-Mindestsicherheitsstandards. Der Referentenentwurf löste eine bis heute anhaltende Debatte bzgl. seiner juristischen und organisatorischen Implikationen für die potentiell betroffenen Unternehmen aus. Die Einbringung des Referentenentwurfs in das parlamentarische Verfahren wird für dieses Jahr erwartet.

Vor diesem Hintergrund zielt die von KPMG im Auftrag des Bundesverbandes der Deutschen Industrie (BDI) durchgeführte Studie darauf ab, zum einen den Aufwand abzuschätzen, der sich vor allem aus der Umsetzung der geplanten Meldepflicht auf Seiten der betroffenen Unternehmen ergeben wird. Zum anderen sollen Empfehlungen zur inhaltlichen Ausgestaltung der Meldepflicht und IT-Mindestsicherheitsstandards formuliert werden. Hierfür wurden Unternehmensvertreter aus den Bereichen der kritischen Infrastruktur und der Telekommunikationsindustrie befragt. Daneben wurden auch Unternehmen der Zulieferer und Ausrüsterindustrie in die Erhebung einbezogen und die aus der Meldepflicht resultierendem Bürokratiekosten quantitativ abgeschätzt.

FINANZIELLE BELASTUNG DER UNTERNEHMEN DURCH DIE MELDEPFLICHT

Die Berechnungen zeigen, dass die Umsetzung der Meldepflicht, so wie sie im Referentenentwurf vom 12. März 2013 ausgestaltet ist, zu signifikanten Erhöhungen der Personal- und Sachkosten für die betroffenen Unternehmen führen kann. Finanzielle Belastungen könnten sich zudem auch aus dem Risiko möglicher Reputationsschäden ergeben, die aus einem fehlerhaften Umgang mit den Meldedaten entstehen kann. In Anlehnung an die Methode des Standardkostenmodells wurden zudem die Bürokratiekosten abgeschätzt, die sich unmittelbar aus der Meldepflicht für die betroffenen Unternehmen ergeben. Diese spezifischen Kosten summieren sich auf Grundlage der für diese Studie getroffenen Annahmen auf insgesamt rund 1,1 Milliarde Euro pro Jahr.

Da der vorliegende Referentenentwurf in wesentlichen Punkten – etwa bei der Frage, welche Unternehmen konkret betroffen sind und welche IT-Sicherheitsvorfälle in welchem Detailgrad tatsächlich gemeldet werden müssen – einen erheblichen Interpretationsspielraum erlaubt, erscheint eine weitergehende Präzisierung dieser Punkte im Rahmen der Weiterentwicklung des Referentenentwurfs angezeigt. Auf Grundlage einer solchen Konkretisierung könnten auch die der Abschätzung zugrunde gelegten Annahmen weiter präzisiert oder angepasst werden.

EMPFEHLUNGEN FÜR EINE ZIELORIENTIERTE WEITERENTWICKLUNG DER VORGESEHENEN MAßNAHMEN

Im Rahmen dieser Studie wurden Empfehlungen entwickelt, die die zielgerichtete Umsetzung des Referentenentwurfs unterstützen können. Die Empfehlungen lassen sich dabei in drei Themenfelder unterteilen: Meldepflicht, IT-Mindestsicherheitsstandards sowie Kommunikation und Transparenz.

EMPFEHLUNGEN ZUR MELDEPFLICHT

- **Definition der Tatbestände:**
  Es ist zu definieren, welche IT-Sicherheitsvorfälle über welchen Meldeweg, in welcher Qualität und Detailtiefe und innerhalb welchen Zeitraums gemeldet werden müssen.

- **Definition der meldepflichtigen Unternehmen:**
  Die Definition des BMI, auf die sich der Referentenentwurf bezieht, erlaubt lediglich eine sektorale Festlegung. Sinnvoller erscheint eine Erstellung transparenter und eindeutiger Kriterien, auf deren Grundlage für die Betreiberunternehmen erkennbar ist, ob sie den gesetzlichen Vorlagen unterliegen.

- **Pseudonymisierung der Meldepflicht via Treuhänder:**
  IT-Sicherheitsvorfälle sind pseudonymisiert abzugeben. Diese Art der Übermittlung ermöglicht es dem BSI uneingeschränkt ein Lagebild zu erstellen und minimiert zugleich das Risiko von Reputationsschäden für die meldenden Unternehmen. Ein unabhängiger Treuhänder könnte dabei die vermittelnde Rolle annehmen und bei Bedarf auch einen gesicherten Rückkanal zum meldenden Unternehmen zur Verfügung stellen

- **Aktive Informationspolitik des BSI:**
  Die vom BSI gesammelten und ausgewerteten Meldungen sollten unmittelbar und aktiv für die Unternehmen nutzbar gemacht werden.

- **Herstellung von Transparenz bzgl. Nutzung und Verwendung der Meldedaten:**
  Zur Erhöhung der Akzeptanz der Meldepflicht sollte transparent und eindeutig dargestellt werden, wo und wie die Meldungen gespeichert, wie sie weiterverarbeitet und an wen sie in welchen Fällen und in welchem Umfang weitergegeben werden.

- **Vermeidung von Doppelregulierung:**
  Der aktuelle Referentenentwurf birgt die Gefahr einer Doppelregulierung, insbesondere für Unternehmen aus dem ITK-Sektor. Eine eindeutige Zuordnung der unterschiedlichen Sicherheitsvorfälle würde den Meldeprozess vereinfachen und Mehraufwand vermeiden.

- **Schaffung von Rechtssicherheit für meldende Unternehmen:**
  Zahlreiche Unternehmen sind unsicher, ob ihnen im Rahmen einer möglichen Meldung Rechtsfolgen drohen könnten. Im Rahmen des Gesetzgebungsverfahrens sollte daher der Wunsch der Unternehmen nach Rechtssicherheit adäquat berücksichtigt werden.

EMPFEHLUNGEN ZU IT-MINDESTSICHERHEITSSTANDARDS

- **Unterstützung der branchenorientierten Selbstorganisation:**
  Die Möglichkeit, branchenspezifische IT-Mindestsicherheitsstandards zu entwickeln, ist sinnvoll. Eine branchenorientierte Selbstorganisation von Mindeststandards ist zielführend und sollte ein ausreichendes Maß an Flexibilität gewährleisten.

- **Berücksichtigung der Internationalität der Unternehmen:**
  Bei der Entwicklung und Anerkennung branchenspezifischer IT-Mindestsicherheitsstandards sollte die starke Ausrichtung der häufig europäisch und global operierenden deutschen Unternehmen an international geltenden Standards berücksichtigt und auf nationale Insellösungen verzichtet werden.

- **Beachtung der Rolle der Zulieferer und Ausrüster:**
  Es sollte berücksichtigt werden, dass die gesetzlichen Vorgaben über den Kreis der eigentlich betroffenen Betreiberunternehmen hinaus Folgewirkungen auch auf andere Unternehmen haben können. Während Zulieferer und Ausrüster, etwa aus der Elektro- und der Maschinenbauindustrie mit Belastungen durch ein mögliches „Durchreichen" von Mindeststandards" belastet werden können, können sich für Hersteller und Dienstleister aus dem Bereich der IT-Sicherheit Potentiale ergeben.

EMPFEHLUNG ZU KOMMUNIKATION UND TRANSPARENZ

- **Kommunikation der Ziele des geplanten Gesetzes:**
  Eine transparente Kommunikation der Ziele der Meldepflicht ist dringend angezeigt, um ein besseres Verständnis auf Seiten der Unternehmen zu fördern und Vertrauen für den Umgang mit signifikanten Sicherheitsvorfällen auszubauen.

- **Fortführung des konstruktiven Dialogs zwischen Industrie, Verwaltung und Politik:**
  Der kontinuierliche und konstruktive Austausch zwischen Unternehmen, Industrievertretern, Verwaltung und Politik hat sich bewährt. Da IT-Sicherheit für die Unternehmen und für die öffentliche Hand auch in den kommenden Jahren ein zentrales Thema darstellen wird, sollte der Dialog und die Zusammenarbeit vertrauensvoll weitergeführt und weiter ausgebaut werden.

KAPITEL 1
Einführung

BEDEUTUNG DER IT UND DER INFORMATIONSSICHERHEIT FÜR WIRTSCHAFT UND GESELLSCHAFT

Vernetzung und Digitalisierung haben zunehmend Einfluss auf Wirtschaft und Gesellschaft. IT-Lösungen sind in unterschiedlichste Produktionsprozesse vieler Branchen integriert und damit bedeutende Produktionsfaktoren der Industrie. Somit leistet IT einen erheblichen Beitrag zur Wettbewerbsfähigkeit der Unternehmen in Deutschland. Gesellschaftlich bedeutsame Dienste wie Energieversorgung, Transport oder Telekommunikation sind von IT-Lösungen abhängig und ein Leben ohne das Internet ist in der heutigen Gesellschaft nicht mehr vorstellbar.

Laut Statistischem Bundesamt nutzen 87% der deutschen Unternehmen einen Internetzugang[1] und davon 37% soziale Medien für die Interaktion mit Privatkunden[2]. Etwa 40% der Unternehmen setzen Cloud-Dienste ein[3], und allein für 2013 weist die Industrie 4.0 eine Bruttowertschöpfung von 76,8 Mrd. Euro auf.[4]

Ebenso sind Verbraucher zunehmend in vielen Bereichen ihres Lebens auf das Informations- und Kommunikationstechnik angewiesen. 76% der Deutschen besitzen einen privaten Internetanschluss,[5] 40,4 Mio. Menschen sind Nutzer von Smartphones[6] und 29,7 Mio. Menschen nutzen mobile Internetdienste.[7]

Auch in der öffentlichen Verwaltung spielt IT eine zentrale Rolle. So gibt der Bund jährlich etwa drei Milliarden Euro für IT aus.[8] Informationstechnik und Kommunikation (ITK) schaffen aus Sicht des Bundes neue Möglichkeiten der Verwaltungsarbeit und bilden ein wichtiges Instrument zur Modernisierung der Verwaltung.[9]

Der hohe Durchdringungsgrad von IT in allen Bereichen des gesellschaftlichen und wirtschaftlichen Lebens ist allerdings nicht nur mit Chancen verbunden, sondern birgt auch Risiken in den Bereichen Sicherheit und Datenschutz. Das Thema IT-Sicherheit im Sinne von umfassenden IT-Sicherheitsvorkehrungen und einer verbesserten Handlungsfähigkeit im Falle eines Angriffs wird daher immer präsenter und bedeutender.

Laut einer Umfrage des Bundesverbandes Informationswirtschaft, Telekommunikation und neue Medien e.V. (BITKOM) sind 38% der Deutschen 2013 Opfer von Computer- und Internetkriminalität geworden, jeder Zehnte hat einen finanziellen Schaden durch Cyberangriffe davongetragen.[10] Gemäß dem Verband muss eine Verbesserung des Sicherheitsniveaus auf drei Ebenen stattfinden: IT-Produkte und Online-Dienste sollten sicherer und Strafverfolgung verbessert werden. Zudem sollten Nutzer über mögliche Risiken aufgeklärt werden, um entsprechend handeln zu können[11]

Die Anzahl der Cyberattacken steigt und Angriffe werden zunehmend anspruchsvoller. Im Zuge dessen sind sie oft schwieriger zu entdecken und zu verhindern, sodass sie nachhaltige Schäden anrichten. Auch die Cyberkriminalität steigt und 2012 wurden fast 64.000 Fälle polizeilich erfasst.[12] Hinzu kommen nicht erfasste und abgefangene Angriffe.

---

[1] Statistisches Bundesamt 2013b
[2] Statistisches Bundesamt 2013a
[3] BITKOM 2014d
[4] BITKOM 2013a, S. 36
[5] Initiative D21 2013, S. 10
[6] Netzökonom 2014
[7] Statistisches Bundesamt 2014b
[8] Bundesministerium des Innern 2014a
[9] Bundesregierung 2010, S. 8
[10] BITKOM 2014a
[11] BITKOM 2014a
[12] Bundeskriminalamt 2012, S. 3

„IT-Sicherheit wird zu einer wesentlichen Voraussetzung zur Wahrung der Freiheitsrechte".[13] Diese in Bedeutung und Tragweite vor dem Hintergrund der aktuellen Diskussion um staatliche Ausspähung zu verstehende Aussage aus dem Koalitionsvertrag der derzeitigen Bundesregierung verdeutlicht in klaren Worten das gestiegene öffentliche Bewusstsein, sondern weist auch auf den in den letzten Jahre erheblich gestiegenen Bedeutungszuwachs der IT-Sicherheit für Wirtschaft und Gesellschaft hin.

Für Unternehmen stellt IT-Sicherheit dementsprechend eine neue Herausforderung dar. Laut einer Studie des European Information Technology Observatory (EITO) aus dem Jahr 2013 hat IT-Sicherheit bei europäischen Unternehmen die höchste Priorität im Bereich Technologie.[14] Ebenso ist IT-Sicherheit laut einer BITKOM-Umfrage der wichtigste IT-Trend des Jahres 2014 für deutsche Unternehmen der Branche Informationstechnologie und Kommunikation.[15]

WACHSENDER HANDLUNGSBEDARF

Angesichts der wirtschaftlichen Bedeutung von IT-Risiken besteht erhöhter Handlungsbedarf. Die deutsche Wirtschaft ist von kleinen und mittleren Unternehmen (KMU) geprägt, 99,3% der deutschen Unternehmen zählen zu dieser Kategorie und mehr als 60% der Beschäftigten arbeiten in KMU[16.] Trotz eines erhöhten Bewusstseins für IT-Sicherheit[17] spiegelt sich dieser Trend laut dem Bundesministerium für Wirtschaft und Energie (BMWi) aktuell noch nicht in der technischen Ausstattung der KMU wieder. Sowohl personell als auch organisatorisch besteht aus diesem Grund aus Sicht des BMWi Handlungsbedarf für deutsche Unternehmen.[18]

In Reaktion auf die steigende Bedrohung durch Cyberkriminalität versucht die Bundesregierung beispielsweise Standards (z.B. ISO 27001 oder den BSI IT-Grundschutz) verbindlich zu machen und regelmäßige Kontrollen einzuführen. Auch die Privatwirtschaft engagiert sich mit verschiedenen freiwilligen Initiativen für eine Stärkung der IT-Sicherheit.

Der **Referentenentwurf eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme** (IT-Sicherheitsgesetz) kann als weiterer Schritt aufgefasst werden, um das Lagebild der deutschen IT-Sicherheit zu verbessern. Dieser Entwurf, der öffentlich bereits intensiv debattiert wurde, soll in der vorliegenden Studie analysiert werden.[19]

In dem Entwurf nehmen sogenannte „kritische Infrastrukturen" [20] eine gesonderte Stellung ein, da sie für das Funktionieren von Staat, Wirtschaft und Gesellschaft essentiell sind. IT-Angriffe auf kritische Infrastrukturen stellen aus dem Grund eine besondere Bedrohung dar, da ihr Ausfall weitreichende Folgen für das Gemeinwohl hätte. Sie stehen daher verstärkt unter Schutz.

Der Sektor ITK nimmt eine Schlüsselrolle ein. Er zählt einerseits zu den Sektoren mit kritischen Infrastrukturen und ist andererseits bedeutend für das Funktionieren der übrigen Sektoren mit kritischen Infrastrukturen, da seine Produkte und Dienstleistungen heute Grundlage vieler Geschäftsprozesse sind.

Neben Kommunikationsdiensten ermöglicht ITK auch den Zugang zu Daten und Informationen und trägt dazu bei, Geschäftsprozesse zu vereinfachen. Ausfälle können daher wesentliche Beeinträchtigungen der Geschäftsabläufe verschiedenster Branchen mit sich bringen. Der Verbreitungsgrad moderner Kommunikation und Informationstechnik ist darüber hinaus auch in zahlreichen Privathaushalten hoch. Inzwischen ist dies zu einem elementaren Bestandteil des öffentlichen Lebens geworden und oftmals Schnittstelle zu verschiedenen Unternehmensdienstleistungen (z.B. Navigation, Banktransfers, etc.).

---

[13] Bundesregierung 2013, S. 97
[14] European Information Technology Observatory 2013, S. 28
[15] BITKOM 2014c
[16] Statistisches Bundesamt o. J.b
[17] BITKOM 2014a
[18] Bundesministerium für Wirtschaft und Energie, S. 2
[19] Vgl. FAZ 2013, Spiegel 2013, Handelsblatt 2013
[20] Die Definition für kritische Infrastrukturen folgt in Kapitel 2 und basiert auf der Nationalen Strategie zum Schutz Kritischer Infrastrukturen des Bundesministeriums des Innern (Bundesministerium des Innern 2009).

ZIELE DER STUDIE

Im Zentrum der Studie stehen zwei zentrale Elemente des am 12. März 2013 durch das BMI vorgelegten Referentenentwurfs: Meldepflicht und IT-Mindestsicherheitsstandards. Ziel ist es, vor allem eine erste Abschätzung des Aufwandes durchzuführen, der auf die betroffenen Unternehmen durch die Umsetzung dieser beiden Elemente zukommen kann. Zugleich sollen Handlungsempfehlungen zur Ausgestaltung der Meldepflicht und der IT-Mindestsicherheitsstandards als Diskussionsbeitrag formuliert werden.

Die Erkenntnisse der Studie stützen sich insbesondere auf drei Säulen:

1. Eine inhaltliche Analyse des Referentenentwurfs

2. Eine Befragung potentiell betroffener Unternehmen

3. Eine an das Standardkostenmodell angelehnte Schätzung der potentiell entstehenden Bürokratiekosten.

Die Studie gliedert sich wie folgt:

In **Kapitel 2** werden aktuelle Entwicklungen im Bereich der IT-Sicherheit in Deutschland dargestellt, um den Referentenentwurf in die allgemeinen Entwicklungslinien einzuordnen.

Im Fokus von **Kapitel 3** steht der aktuelle Referentenentwurf. Zentrale Maßnahmen, wie die vorgesehenen Meldepflichten und IT-Mindestsicherheitsstandards, werden hier detailliert analysiert. Daneben werden auch legislative Entwicklungen auf europäischer Ebene berücksichtigt.

In **Kapitel 4** folgt die quantitative Analyse möglicher Folgen des Gesetzes. In Anlehnung an das Standardkostenmodell wird hier eine quantitative Einschätzung der direkt aus der vorgesehenen Meldepflicht Kosten für die Unternehmen vorgenommen. Daneben erfolgt eine qualitative Einschätzung weiterer sich ggf. aus der Umsetzung des Referentenentwurfs ergebenden monetären Belastungen der Unternehmen.

In **Kapitel 5** werden die Ergebnisse der Studie zusammengefasst und für zielgerichtete Umsetzung des Referentenentwurfs vorgestellt.

Die Studie wurde im Auftrag des Bundesverbands der Deutschen Industrie von März bis Juni 2014 erstellt. Der Inhalt und die Empfehlungen wurden unabhängig durch die KPMG AG Wirtschaftsprüfungsgesellschaft erarbeitet und reflektieren nicht notwendigerweise die Meinung des BDI oder seiner Mitgliedsverbände.

KAPITEL 2

IT-Sicherheit in Deutschland: Aktuelle Entwicklungen

2.1 Entwicklungen der gesetzgebenden Ebene

Als Antwort auf die gestiegene IT-Gefährdungslage haben Bundesregierung und Bundestag in den zurückliegenden Jahren eine Reihe von Maßnahmen auf den Weg gebracht, die zu einer Erhöhung der IT-Sicherheit in Deutschland beitragen sollen. Dabei wird IT-Sicherheit häufig im Kontext der besonderen Schutzwürdigkeit kritischer Infrastrukturen (KRITIS) betrachtet. Gemäß der KRITIS-Strategie des Bundesministeriums des Innern handelt es sich bei KRITIS um „Organisationen und Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen [handelt], bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden".[21]

Die erwähnten Maßnahmen, zu denen auch der zurzeit im BMI in der Erstellung befindliche Referentenentwurf des Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme[22] (IT-Sicherheitsgesetz) zählt, reichen dabei von der klaren Zuweisung behördlicher Verantwortlichkeiten über die Verabschiedung gesetzlicher Regelungen und politischer Strategien bis zur Einrichtung neuer Gremien und Strukturen. Die wichtigsten dieser Maßnahmen und Initiativen sollen im Folgenden kurz dargestellt werden, um eine bessere Einordnung des aktuellen Referentenentwurfs zu ermöglichen.

POLITISCHE STRATEGIEN UND GESETZLICHE REGELUNGEN ZUR ERHÖHUNG DER IT-SICHERHEIT

Aufbauend auf dem im Jahre 2005 verabschiedeten „**Nationalen Plan zum Schutz der Informationsinfrastrukturen**"[23] verabschiedete die Bundesregierung im Jahr 2009 die „Nationale Strategie zum Schutz kritischer Infrastrukturen".[24] Diese „**KRITIS-Strategie**" identifiziert insbesondere terroristische Handlungen und Naturereignisse als wesentliche Gefährdungsquellen und hebt dabei die besonderen „Risiken und Gefährdungen für Informationsinfrastrukturen"[25] hervor. Zur Erhöhung der Sicherheit kritischer Infrastrukturen befürwortet die KRITIS-Strategie einen kooperativen Ansatz aller Beteiligten, der die Zusammenarbeit zwischen öffentlichen Stellen und den privaten KRITIS-Betreibern umfasst und freiwillige Selbstverpflichtungen der Unternehmen zur Erhöhung des KRITIS-Schutzes ermöglicht. Für den Fall, dass die Unternehmen trotz freiwilliger Selbstverpflichtungen festgestellte Sicherheitsmängel nicht beseitigen, behält sich die Bundesregierung gesetzgeberische Maßnahmen vor.[26]

Ebenfalls 2009 verabschiedete der Deutsche Bundestag, das „**Gesetz zur Stärkung der Sicherheit in der Informationstechnik des Bundes**"[27], mit dem die Aufgaben und Befugnisse des BSI neu geregelt und erweitert wurden. Das BSI ist nunmehr die zentrale Behörde für Meldungen von IT-Sicherheitsvorfällen. Die Behörde wurde 1991 gegründet und gehört zum Geschäftsbereich des BMI, tritt jedoch als unabhängige und neutrale Stelle auf. [28] Das BSI hat die Aufgabe, die IT-Sicherheit in Deutschland zu stärken und fungiert dabei sowohl als IT-Sicherheitsdienstleister des Bundes als auch als Ansprechpartner von Herstellern und Nutzern von Informationstechnik.[29]

---

[21] Bundesministerium des Innern 2009, S. 4
[22] Bundesministerium des Innern 2013a
[23] Bundesministerium des Innern 2005
[24] Bundesministerium des Innern 2009
[25] Bundesministerium des Innern 2009, S. 8
[26] Bundesministerium des Innern 2009
[27] Deutscher Bundestag
[28] Bundesamt für Sicherheit in der Informationstechnik o. J.b
[29] Bundesamt für Sicherheit in der Informationstechnik o. J.a

Um der gestiegenen Bedeutung und der ebenfalls erhöhten Gefährdungslage der Informationsinfrastrukturen in Deutschland gerecht zu werden und mit dem Ziel, die Sicherheit im Cyber-Raum[30] zu erhöhen, verabschiedete die Bundesregierung im Februar 2011 die „**Cyber-Sicherheitsstrategie für Deutschland**“[31] (Cyber-Strategie). Die Cyber-Strategie formuliert insgesamt zehn strategische Ziele und Maßnahmen, zu denen u.a.

- der verstärkte Schutz kritischer Infrastrukturen vor IT-Angriffen,
- die Stärkung der IT-Sicherheit in der öffentlichen Verwaltung,
- die Errichtung eines Nationalen Cyber-Abwehrzentrums unter Federführung des BSI,
- die Einrichtung eine Nationalen Cyber-Sicherheitsrates unter Beteiligung verschiedener Bundesministerien sowie Vertretern der Länder,
- der Schutz der IT-Systeme in Deutschland,
- sowie die Forderung nach stärkerer internationaler Zusammenarbeit

gehören.

Ähnlich wie die KRITIS-Strategie hebt die Cyber-Strategie die Bedeutung der Zusammenarbeit zwischen staatlichen Stellen und privaten Unternehmen bei dem Schutz des Cyberraums hervor. Zugleich unterstreicht sie jedoch auch den staatlichen Anspruch, immer dort Regelungen vorzugeben und Befugnisse zu erweitern, wo dies aus staatlicher Sicht notwendig ist, um die Cyber-Sicherheit zu erhöhen.

STAATLICHE FÖRDERUNG DER IT-SICHERHEIT

Begleitend zu den gesetzlichen Regelungen und politischen Strategien bietet der Bund verschiedene öffentliche Förderprogramme an, die die Umsetzung der freiwilligen und gesetzlich geforderten Initiativen erleichtern sollen. Insbesondere das Bundesministerium für Bildung und Forschung (BMBF) und das BMWi fördern Formate für die Entwicklung innovativer IT-Sicherheitslösungen in Deutschland. Förderschwerpunkte bilden dabei vor allem der Datenschutz und der Schutz der Privatsphäre von Bürgerinnen und Bürgern.[32] Das BMBF fördert vor diesem Hintergrund eine Reihe von „Kompetenzzentren“:

- CISPA: Center for IT-Security, Privacy and Accountability in Saarbrücken[33]
- EC-SPRIDE: European Center for Security and Privacy by Design in Darmstadt[34]
- KASTEL: Kompetenzzentrum für angewandte Sicherheitstechnologie in Karlsruhe[35]

Ziel dieser Einrichtungen ist es, die IT-Sicherheitskompetenzen innerhalb Deutschlands zu bündeln und interdisziplinär zu verbinden.

Die Kompetenzzentren widmen sich verschiedenen Aspekten der IT-Sicherheit. Ein Beispiel dafür ist der gemeinsam von ihnen veröffentlichte Bericht „Entwicklung sicherer Software durch Security by Design“.[36] **Security by Design** widmet sich Sicherheitslücken in der Anwendungssoftware, die durch existierende reaktive Methoden wie Firewalls und Virenscanner und nachträglich implementierte Sicherheitslösungen unzureichend abgedeckt werden. Sicherheitsanforderungen werden hier bereits bei der Softwareentwicklung berücksichtigt, damit Angriffe frühzeitig verhindert werden können.

---

[30] „Der Cyber-Raum umfasst alle durch das Internet über territoriale Grenzen hinweg weltweit erreichbaren Informationsinfrastrukturen. In Deutschland nutzen alle Bereiche des gesellschaftlichen und wirtschaftlichen Lebens die vom Cyber-Raum zur Verfügung gestellten Möglichkeiten. Staat, Kritische Infrastrukturen, Wirtschaft und Bevölkerung in Deutschland sind als Teil einer zunehmend vernetzten Welt auf das verlässliche Funktionieren der Informations- und Kommunikationstechnik sowie des Internets angewiesen.“ Bundesministerium des Innern 2011

[31] Bundesministerium des Innern 2011

[32] Bundesministerium für Bildung und Forschung o. J.a

[33] Weitere Informationen: https://www.cispa-security.de/

[34] Weitere Informationen: http://www.ec-spride.tu-darmstadt.de/ec-spride/

[35] Weitere Informationen: http://www.kastel.kit.edu/

[36] Fraunhofer-Institut für Sichere Informationstechnologie 2013

Eine weitere Initiative des BMBF ist das EUREKA-Forschungsprojekt „**Safe and Secure European Routing – SASER**“.[37] In diesem Projekt arbeiten Partner aus fünf europäischen Ländern an wissenschaftlichen, technischen und systemischen Lösungen für einen problemlosen Transport von Daten. Im Resultat sollen optisch-elektronische Technologien den Einsatz robuster und energiesparender Router ermöglichen, die einen sicheren, zuverlässigen und energieeffizienten Transport von Daten ermöglichen.

In dem Projekt „**SIEM für KMU**“[38] untersucht das BMBF die Nutzbarkeit von Sicherheitssystemen für kleine und mittlere Unternehmen (KMU). KMU sind häufig Opfer von Cyber-Angriffen. Sie schützen sich davor z.B. mit Firewalls und Virenscannern, die aber unabhängig voneinander arbeiten und somit keine Informationen austauschen. So können nicht alle Angriffe identifiziert werden. Die Integration der eingesetzten Systeme findet in sogenannten Security Information and Event Management (SIEM)-Systemen statt. Diese sind jedoch sehr kostenaufwendig und erfordern technische Fachkenntnisse, weshalb sie häufig nur von großen Unternehmen eingesetzt werden können. Das Projekt untersucht Möglichkeiten zum verbesserten Einsatz bei KMU.

Zusätzlich hat das BMBF die Forschungsschwerpunkte **sicheres Cloud Computing**[39] und **Sicherung der Privatsphäre**[40] aufgegriffen. Gemeinsam mit der Akademie der Technikwissenschaften acatech wurde eine Analyse zum Thema Internet Privacy durchgeführt und Handlungsempfehlungen entwickelt sowie ein interdisziplinärer wissenschaftlicher Beraterkreis „Privacy“ eingerichtet.

Um dem Fachkräftemangel entgegenzuwirken, fördert das BMBF spezialisierte Ausbildungen in IT-Sicherheit an den oben genannten Kompetenzzentren. So können Studierende ein dem Master gleichwertiges Zertifikat zur Spezialisierung in IT-Sicherheit erwerben (KASTEL) oder den Studiengang IT-Security belegen (TU Darmstadt). Berufstätige können in Darmstadt ebenfalls ein Zertifikat zur IT-Sicherheit erwerben (CASED). Bereits an Schulen fördert die Bundesregierung zudem die sogenannten MINT-Fächer (Mathematik, Informatik, Naturwissenschaft und Technik).[41]

Weitere Initiativen zur Förderung der IT-Sicherheitsindustrie des BMBF schließen beispielsweise Themen der **Quantenkommunikation** zur abhörsicheren Übertragung von Nachrichten oder gezielte Nachwuchsförderprogramme für Studenten und Berufstätige ein.[42] Zusätzlich wird der Sektor durch das BMWi beispielsweise durch die Initiative „**IT-Sicherheit in der Wirtschaft**“[43] oder mit der Aktion „**Trusted Cloud**“[44] gefördert.

2.1 Existierende Austauschformate und Initiativen der Privatwirtschaft

Parallel zum Auf- und Ausbau staatlicher Stellen und Förderung sowie der Verabschiedung politischer Leitlinien wurden in den vergangenen Jahren auch zahlreiche private Initiativen und Aktivitäten unterhalb der Gesetzesebene zur Erhöhung der IT-Sicherheit in Deutschland ins Leben gerufen. Diese umfassen u.a. Konferenzen, Expertenforen, Vereine und Austauschplattformen. Damit existieren bereits heute zahlreiche Möglichkeiten für öffentliche wie private Stellen, sich über aktuelle Entwicklungen, Risiken und Gefahrenszenarien auszutauschen und gemeinsame Lösungen zu entwickeln. Im Folgenden werden die wichtigsten dieser Initiativen kursorisch dargestellt.

ALLIANZ FÜR CYBER-SICHERHEIT

Die Allianz für Cyber-Sicherheit wurde 2012 gemeinsam vom BSI und dem Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (BITKOM) gegründet. Nach

[37] Weitere Informationen: http://www.vdivde-it.de/KIS/sichere-ikt/safe-and-secure-european-routing-saser
[38] Weitere Informationen: http://www.vdivde-it.de/KIS/foerderbekanntmachungen/kmu-innovativ
[39] Weitere Informationen: http://www.vdivde-it.de/KIS/sichere-ikt/sicheres-cloud-computing
[40] Weitere Informationen: http://www.vdivde-it.de/KIS/leben-in-der-digitalen-welt
[41] Bundesministerium für Bildung und Forschung o. J.b
[42] Weitere Informationen: http://www.vdivde-it.de/KIS/sichere-ikt/quantenkommunikation
[43] Weitere Informationen: http://www.it-sicherheit-in-der-wirtschaft.de/
[44] Weitere Informationen: http://www.trusted-cloud.de/

Angaben der Allianz engagieren sich aktuell mehr als 740 Organisationen aus Verwaltung und Wirtschaft in diesem Rahmen für IT-Sicherheit.[45]

Die Allianz hat das Ziel, die IT-Sicherheit in Deutschland zu erhöhen und den Standort Deutschland in Bezug auf Cyber-Angriffe sicherer zu machen. Zur Erreichung ihrer Ziele setzt die Allianz bei ihrem Angebotsportfolio zwei Schwerpunkte: Informationspool und Erfahrungsaustauch.

Der Informationspool bietet zahlreiche Dokumente und Publikationen zum Thema IT-Sicherheit. Ein Teil dieser Informationen ist öffentlich zugänglich (z.B. Basisdokumente) und andere nicht-öffentliche Informationen stehen nur registrierten Teilnehmern zur Verfügung (z.B. aktuelle Lageberichte). Vertrauliche Informationen sind dagegen nur Unternehmen zugänglich, die als „Institution im besonderen staatlichen Interesse" (INSI) registriert sind. Bei dieser Gruppe handelt es sich zumeist um KRITIS-Betreiber wie etwa Finanzdienstleister, ITK-Betreiber oder Energieversorger.[46]

Der zweite Schwerpunkt der Allianz liegt auf dem Erfahrungsaustausch. Im Rahmen von Workshops und Kongressen können Teilnehmer sich über ihre Erfahrungen im Bereich IT-Sicherheit austauschen. Weitere Angebote umfassen z.B. Schulungen und Webinare, diese sind nur für Teilnehmer zugänglich.[47]

Die Allianz gibt in regelmäßigen Abständen ein aktuelles Lagebild für Deutschland heraus, in das u.a. auch Informationen einfließen, die von Unternehmen und Organisationen an die auf dem Internetportal angebotene Meldestelle für Cyber-Angriffe gemeldet werden können.[48]

EXPERTENKREISE DES BUNDESAMTS FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK

Als Teil der Allianz für Cyber-Sicherheit nahm 2013 der vom BSI ins Leben gerufene „Expertenkreis Cyber-Sicherheit" seine Arbeit auf.[49] Der Expertenkreis dient zum einen dem Austausch und der Diskussion aktueller Entwicklungen und Herausforderungen im Bereich der IT-Sicherheit. Zum anderen gehört es zu den Aufgaben des Expertenkreises, Empfehlungen des BSI auf ihre praktische Umsetzbarkeit zu prüfen und zu bewerten sowie geeignete Maßnahmen zur Abwehr von Cyber-Gefahren zu identifizieren.[50]

Daneben betreibt das BSI auch den „Expertenkreis Internetbetreiber", der insbesondere die aktuelle Gefährdungslage der kritischen Infrastruktur analysiert und Empfehlungen zur Gewährleistung der Sicherheit der Internetinfrastruktur formuliert sowie den „Expertenkreis IT-Forensik".[51] Die Ergebnisse der Expertenkreise fließen in das Lagebild oder Veröffentlichungen zur Cyber-Sicherheit ein.

INITIATIVE IT-SICHERHEIT IN DER WIRTSCHAFT

Die 2011 vom BMWi ins Leben gerufene Initiative „IT-Sicherheit in der Wirtschaft" verfolgt das Ziel, die Sicherheitslage in KMU zu verbessern. Dafür bündelt sie bestehende Initiativen und ergänzt sie durch spezifische Maßnahmen zur Förderung der IT-Sicherheit in KMU.[52] So führt sie eine Sensibilisierungskampagne für IT-Sicherheit in Unternehmen durch, stellt einen IT-Sicherheitsnavigator mit umfassenden und strukturierten Informationsangeboten zum Thema IT-Sicherheit bereit und bietet sowohl einen Webseiten-Check, als auch einen IT-Sicherheitscheck für KMU an.[53]

[45] Allianz für Cyber-Sicherheit o. J.a
[46] Allianz für Cyber-Sicherheit 2013, S. 3
[47] Bundesamt für Sicherheit in der Informationstechnik o. J.d
[48] Allianz für Cyber-Sicherheit o. J.d
[49] Allianz für Cyber-Sicherheit o. J.b
[50] Bundesamt für Sicherheit in der Informationstechnik 2013
[51] Allianz für Cyber-Sicherheit o. J.c,
[52] Bundesministerium für Wirtschaft und Energie o. J.a
[53] IT Sicherheit in der Wirtschaft o. J.

NATIONALER IT-GIPFEL

Der Nationale IT-Gipfel wird jährlich vom BMWi ausgerichtet. Zu dem eintägigen Kongress kommen Vertreter der Politik, Wirtschaft und Wissenschaft zusammen, um gemeinsam Konzepte zur Stärkung der Bundesrepublik Deutschland als ITK-Standort zu entwickeln.[54]

Die Vorbereitung des Nationalen IT-Gipfels findet in Arbeitsgruppen statt, welche sich mit zentralen und aktuellen Herausforderungen der IT in Deutschland befassen. Die Arbeitsgruppen geben im Anschluss an den Gipfel Ergebnispapiere heraus, die sich mit den möglichen Auswirkungen dieser Herausforderungen und den damit verbundenen Chancen auseinandersetzen sowie mögliche Konsequenzen und Handlungsfelder aufzeigen.[55]

CYBER SECURITY SUMMIT

Der Cyber Security Summit ist ein seit 2012 gemeinsam von der Münchner Sicherheitskonferenz und der Deutschen Telekom organisiertes Treffen von Vertretern aus der Wirtschaft und mit Sicherheitsthemen befassten Politikern.[56]

Ziel der Konferenz ist es, Herausforderungen der IT-Sicherheit zu analysieren und präventive Ansätze in Unternehmen und Politik zu verankern. Die Teilnehmer arbeiten nicht nur auf nationaler Ebene an sektorübergreifenden Lösungsansätzen, sondern setzen sich Angaben des Summit zufolge auch auf internationaler Ebene für Sicherheitslösungen ein.

2012 wurde ein Acht-Punkte Plan für Cyber-Sicherheit[57] vorgestellt, in dem u.a. ein vertiefter Informationsaustausch und gezielte Handlungen von Wirtschaft, Politik und Gesellschaft gefordert wurden.[58]

POTSDAMER KONFERENZ FÜR NATIONALE CYBERSICHERHEIT

Die Potsdamer Konferenz für Nationale Cybersicherheit wurde 2013 vom Hasso-Plattner-Institut (HPI) und dem Brandenburgischen Institut für Gesellschaft und Sicherheit (BIGS) initiiert.

Ziel der Konferenz ist es, Akteuren und Multiplikatoren der deutschen Sicherheitswirtschaft den Austausch zu relevanten Themen zu ermöglichen und eine stärkere Vernetzung herzustellen. Themen der Veranstaltung von 2013 waren beispielsweise Cyberkriminalität, -spionage, -schutz und -defence. In diesem Jahr zählten u.a. Cyber-Sicherheit und Industrie 4.0 sowie der Schutz kritischer Infrastrukturen zu den Themenschwerpunkten.[59]

DEUTSCHLAND SICHER IM NETZ

Der Verein „Deutschland sicher im Netz“ e.V. wurde 2006 als ein Ergebnis des ersten IT-Gipfels der Bundesregierung (vgl. oben) gegründet. Der Verein stellt Angebote zu sicherheitsrelevanten Themen für Unternehmen, insbesondere für KMU und Privatpersonen zur Verfügung. Ein weiterer Schwerpunkt der Arbeit liegt auf der Aufbereitung von Informationen für Kinder, Jugendliche und Eltern.[60] Zu den Angeboten des Vereins gehören z.B. Sicherheitschecks, Lehr- und Lernpakete und eine Vielzahl an Informationsformaten.[61]

Zu den Vereinsmitgliedern gehören sowohl Privatunternehmen als auch Verbände und gemeinnützige Organisationen[62]. Der Verein kooperiert mit dem BSI und wird auch vom BMI als Schirmherr unterstützt. Weitere Kooperationen bestehen mit dem Fraunhofer-Institut für offene Kommunikationssysteme (FOKUS) sowie mit der Stiftung Digitale Chancen.[63]

---

[54] Bundesministerium für Wirtschaft und Energie o. J.b
[55] Beispiel: Nationaler IT-Gipfel (2014): Ergebnispapier "Arbeit in der digitalen Welt" Bundesministerium für Wirtschaft und Energie 2014
[56] Cyber Security Summit 2014
[57] Stiftung Münchner Sicherheitskonferenz 2012
[58] Stiftung Münchner Sicherheitskonferenz o. J.
[59] Hasso-Plattner-Institut 2014
[60] Bundesministerium des Innern o. J.
[61] Deutschland sicher im Netz o. J.c
[62] Deutschland sicher im Netz o. J.b
[63] Deutschland sicher im Netz o. J.a

SELBSTREGULIERUNG INFORMATIONSWIRTSCHAFT

Nach eigenen Angaben dient der 2011 gegründete Verein „Selbstregulierung Informationswirtschaft e.V." als organisatorisches Dach für unterschiedliche Selbstregulierungsansätze der digitalen Wirtschaft. Ziel ist es, den Verbraucher- und Datenschutz im Rahmen der gesetzlichen Regelungen des Telemediengesetzes und des Telekommunikationsgesetzes zu fördern.[64]

Mitglieder des Vereins sind beispielsweise der Branchenverband BITKOM, die Deutsche Post AG, die Deutsche Telekom AG, Google Deutschland, Microsoft Deutschland und die Nokia GmbH.[65]

Der Verein veröffentlicht Verhaltenskodizes und entwickelt Selbstregulierungsmaßnahmen für die digitale Wirtschaft, deren Einhaltung er auch evaluiert und prüft. Zudem werden für Unternehmen und Privatpersonen, Informationen zur Anwendung von technischen Schutzmaßnahmen und zum verantwortungsbewussten Umgang mit Telemedien bereitgestellt.[66]

2.2 Überblick IT-Sicherheitsindustrie in Deutschland

Die kontinuierliche Bedeutungszunahme der IT-Sicherheit in Politik, Gesellschaft und Wirtschaft hat sich in den letzten Jahren auch in Form eines spürbaren Wachstums der IT-Sicherheitsindustrie ausgedrückt. Durch die gestiegene Sensibilität für Cyber-Attacken, E-Crime und Datendiebstahl ist die Nachfrage nach IT-Sicherheitsgütern über alle Branchen der deutschen Wirtschaft hinweg gestiegen.[67]

Die Nachfrage nach Unterstützung bei der IT-Sicherheit ist daher hoch und wird von der wachsenden IT-Sicherheitsindustrie zunehmend bedient. In den vergangenen Jahren wurde das Angebot für IT-Sicherheitsprodukte und vor allem -dienstleistungen in Deutschland stark ausgebaut.[68] Das folgende Kapitel gibt einen Überblick über die IT-Sicherheitsindustrie und deren jüngste Entwicklungen.

DER IT-SICHERHEITSMARKT IN DEUTSCHLAND

In Deutschland wurden 2012 IT-Sicherheitsgüter, also Produkte und Dienstleistungen der IT-Sicherheit, im Wert von 6,6 Milliarden Euro erworben.[69] Dieser Wert ergibt sich aus der inländischen Produktion, abzüglich der Exporte und zuzüglich der Importe. Nach Angaben des Bundesministeriums für Wirtschaft und Energie wurde der Bedarf an IT-Sicherheitsgütern 2012 zu ca. 80% durch die inländische Produktion und zu etwa 20% durch aus dem Ausland eingeführte Produkte und Dienstleistungen bedient.[70]

Das Produkt- und Dienstleistungsspektrum der IT-Sicherheitsindustrie in Deutschland setzt sich aus Dienstleistungen, Software und Hardware zusammen. Dienstleistungen schließen z.B. Sicherheitsanalysen, Sicherheitstrainings und Zertifizierungen ein. Software dient beispielsweise dem Schutz vor Viren oder bietet VPN- und Sicherheitslösungen für mobile Endgeräte. Unter Hardware fallen dagegen Produkte wie Bandlaufwerke und andere mechanische Bauteile.

Den größten Anteil am Marktvolumen haben Dienstleistungen (45% Marktanteil), gefolgt von Software (41% Marktanteil) und Hardware (13% Marktanteil, alle Zahlen für 2012).[71] Als Ursache für den hohen Anteil von IT-Sicherheitsdienstleistungen und Software kann eine zunehmende Vernetzung und die damit einhergehende wachsende Komplexität von IT-Sicherheitsgütern genannt werden. Diese fordert spezialisierte Software und Dienstleistungen für intelligente IT-Sicherheitslösungen. Noch vor wenigen Jahren besaß Hardware mit 38% einen größeren Anteil am Marktvolumen als Software und Dienstleistungen (27% bzw. 35%).[72]

---

[64] Selbstregulierung Informationswirtschaft o. J.b
[65] Selbstregulierung Informationswirtschaft o. J.a
[66] Selbstregulierung Informationswirtschaft o. J.b
[67] BITKOM 2013b
[68] Bundesministerium für Wirtschaft und Energie 2013a, S. 17
[69] Bundesministerium für Wirtschaft und Energie 2013b, S. 21
[70] Bundesministerium für Wirtschaft und Energie 2013b, S. 16
[71] Bundesministerium für Wirtschaft und Energie 2013b, S. 22
[72] Bundesministerium für Wirtschaft und Energie 2013b, S. 21

Die gestiegene Nachfrage nach Software und Dienstleistungen wird von IT-Sicherheitsunternehmen erfolgreich bedient. Gleichzeitig sinken mit der Nachfrage nach Produkten für Hardware-Sicherheit auch deren Marktpreise. [73]

DIE BEDEUTUNG DER IT-SICHERHEIT FÜR DIE DEUTSCHE INDUSTRIE

Abnehmer für IT-Sicherheitsgüter finden sich in Deutschland vor allem in den technologieintensiven Branchen. Die größten Abnehmer mit einem Anteil von 20,7% sind Anbieter von IT- und Informationsdienstleistungen. Hersteller von digitalen Videogeräten, elektronischen Bauelementen und Erzeugnissen für Telekommunikation und Unterhaltung stellen 11,9% der Nachfrage für IT-Sicherheitsgüter. Telekommunikationsdienstleister nehmen 7,2% ein. Weitere bedeutende Abnehmer sind vor allem Hersteller von Maschinen (5,7%) und Finanzdienstleister (4,1%). Die übrigen Abnehmer verzeichnen jeweils nur einstellige Anteile am Gesamtkonsum.[74]

IT-Sicherheit wird auch in den folgenden Jahren mit hoher Wahrscheinlichkeit für die deutsche Industrie an Bedeutung gewinnen. Besonders im Hinblick auf den Auf- und Ausbau der sogenannten Industrie 4.0 wird das Thema zunehmend den wirtschaftlichen Erfolg vieler Branchen beeinflussen.

„Industrie 4.0" beschreibt die vierte industrielle Revolution, eine neue Stufe der Organisation und Steuerung der gesamten Wertschöpfungskette über den Lebenszyklus von Produkten. Dieser Zyklus orientiert sich an den zunehmend individualisierten Kundenwünschen und erstreckt sich von der Idee, über die Entwicklung und Fertigung, die Auslieferung eines Produkts an den Endkunden bis hin zum Recycling, einschließlich der damit verbundenen Dienstleistungen.

Basis ist die Verfügbarkeit aller relevanten Informationen in Echtzeit durch Vernetzung aller an der Wertschöpfung beteiligten Instanzen sowie die Fähigkeit aus den Daten den zu jedem Zeitpunkt optimalen Wertschöpfungsfluss abzuleiten. Durch eine vertikale und horizontale Vernetzung von Menschen, Maschinen, Objekten und ITK-Systemen werden echtzeitoptimierte, selbstorganisierte, unternehmensübergreifende Wertschöpfungsnetzwerke gebildet, die dem zunehmenden Wunsch der Verbraucher nach intelligenten und individualisierten Produkten nachkommt. Beispiele für die Technologiefelder der Industrie 4.0 sind Embedded Systems, Smart Factories, Robuste Netze und Cloud Computing.[75]

Die zunehmende Integration von Informationen, Daten und Systemen rückt die Bedeutung von IT-Sicherheit in den Vordergrund. Sie ist essentiell, um Personen, Unternehmen und Prozesse zu schützen und beispielsweise Sabotage oder Systemmanipulationen zu verhindern. Eine besondere Rolle kommt in diesem Zusammenhang Zulieferern und Ausrüstern zu, die wesentliche Komponenten und Produkte für kritische Infrastrukturen und Fabrikautomation, auch im Kontext von Industrie 4.0, liefern.

2.3 Fazit

Die Entwicklungen der letzten Jahre machen deutlich, dass sich in Deutschland sowohl die Bundesregierung als auch die Privatwirtschaft verstärkt für einen Ausbau von IT und IT-Sicherheit engagieren.

Auf staatlicher Ebene wurden wichtige gesetzliche und politische Maßnahmen zum Ausbau und der Verbesserung des Schutzes vor Cyberkriminalität auf den Weg gebracht. Das BSI ist als nationale Sicherheitsbehörde in Europa einmalig und nimmt damit im internationalen Vergleich eine Vorreiterstellung im staatlichen Vorgehen für IT-Sicherheit ein. Mit der Nationalen Cybersicherheitsstrategie und der Einrichtung eines Cyber-Sicherheitsrates wurde die Bedeutung des Themas öffentlich thematisiert und wirksam adressiert.

---

[73] Bundesministerium für Wirtschaft und Energie 2013b, S. 19
[74] Bundesministerium für Wirtschaft und Energie 2013b, S. 30
[75] Vgl. Plattform Industrie 4.0 und BITKOM 2013a

Auf privatwirtschaftlicher Ebene existieren eine Reihe an Initiativen, Austauschformaten und Kooperationen zur Stärkung der IT-Sicherheit. Diese finden zum Großteil auf freiwilliger Basis statt und dienen dem Informationsaustausch zu Entwicklungen im Bereich IT-Sicherheit sowie gleichzeitig dem Austausch innerhalb einzelner Branchen.

KAPITEL 3

Das IT-Sicherheitsgesetz und die EU-Richtlinie

Das BMI reagiert mit dem Referentenentwurf eines Gesetzes „zur Erhöhung der Sicherheit informationstechnischer Systeme“ auf die zunehmende gesellschaftliche und wirtschaftliche Abhängigkeit von informationstechnischen Systemen und des Cyberraums. Laut Entwurf existiert zwischen den verschiedenen Betreibern kritischer Infrastrukturen ein nicht weiter tolerierbarer Zustand unterschiedlicher Niveaus in der IT-Sicherheit, weshalb entsprechende gesetzliche Regelungen notwendig erscheinen.[76]

3.1. Inhalte des IT-Sicherheitsgesetzes

Der am 12. März 2013 vorgestellte Entwurf formuliert eine Reihe unterschiedlicher Maßnahmen, deren Ziel es ist, „den Schutz der Integrität und Authentizität datenverarbeitender Systeme zu verbessern und der gestiegenen Bedrohungslage anzupassen.“[77] Die im Referentenentwurf vorgeschlagenen Maßnahmen zielen dabei besonders auf eine Steigerung und einheitliche Nivellierung der IT-Sicherheit bei Betreibern kritischer Infrastrukturen (KRITIS) ab.

Der Referentenentwurf bezieht sich auf die KRITIS-Sektoren Energie, Informations- und Kommunikationstechnik, Gesundheit, Wasser, Ernährung, Transport und Verkehr sowie Finanz- und Versicherungswesen. Die KRITIS-Sektoren Medien und Kultur sowie Staat und Verwaltung sind von dem Referentenentwurf nicht betroffen.

Für Anbieter von Telekommunikationsdiensten und Netzbetreiber, die jeweils dem KRITIS-Sektor Informations- und Kommunikationstechnik zugeordnet werden können, sieht der Referentenentwurf zudem zusätzliche Anforderungen und Pflichten vor.

Die staatlichen Institutionen werden währenddessen im „Umsetzungsplan für die Gewährleistung der IT-Sicherheit in der Bundesverwaltung“ (UP Bund) adressiert[78]. Der UP Bund ist „die verbindliche interne IT-Sicherheitsleitlinie für den Schutz der Informationsinfrastrukturen in allen Behörden des Bundes.“ Um ein hohes Niveau der IT-Sicherheit in der Bundesverwaltung zu gewährleisten, werden im Rahmen des UP Bund Mindestanforderungen umgesetzt und regelmäßige Revisionen der IT-Sicherheit durchgeführt.[79]

Zu den wesentlichen Inhalten des Referentenentwurfs, die Unternehmen betreffen, gehören u.a.:

- Die **Einführung einer Meldepflicht für KRITIS-Betreiber**:
  Betreiber kritischer Infrastrukturen haben „schwerwiegende Beeinträchtigungen“ ihrer informationstechnischen Systeme, Komponenten oder Prozesse „unverzüglich“ an das BSI zu melden.[80]

- Die **Ausweitung der Meldepflicht für Anbieter von Telekommunikationsdiensten und Netzbetreiber an die Bundesnetzagentur (BNetzA):**
  Zusätzlich zu der bestehenden und im Telekommunikationsgesetz[81] festgelegten Meldepflicht für Anbieter von Telekommunikationsdiensten und Betreiber von Telekommunikationsnetzen haben diese „Beeinträchtigungen von Telekommunikationsnetzen und -diensten, die zu einer Störung der Verfügbarkeit der über diese Netze erbrachten Dienste oder zu einem unerlaubten Zugriff auf Telekommunikations- und Datenverarbeitungssystemen der Nutzer oder Teilnehmer führen können und von denen der Netzbetreiber oder der

[76] Bundesministerium des Innern 2013a, S. 1
[77] Bundesministerium des Innern 2013b, S. 1
[78] Bundesamt für Sicherheit in der Informationstechnik o. J.c
[79] Bundesamt für Sicherheit in der Informationstechnik o. J.c
[80] Bundesministerium des Innern 2013a
[81] Bundesministerium für Verkehr und digitale Infrastruktur

Telekommunikationsdiensteanbieter Kenntnis erlangt, der BNetzA unverzüglich mitzuteilen".[82]

- Die **Ausweitung der Meldepflicht der TK-Diensteanbieter und Netzbetreiber an ihre Nutzer:**
  TK-Anbieter haben Störungen, die von Datenverarbeitungssystemen der Nutzer ausgehen, an diese zu melden und die Nutzer auf angemessene technische Mittel zur Behebung der Störung hinzuweisen.[83]

- Die **Einführung von IT-Sicherheitsstandards:**
  Betreiber kritischer Infrastrukturen und ihre Branchenverbände können branchenspezifische Sicherheitsstandards erarbeiten, die auf Antrag durch das BSI anerkannt werden können.[84]

- Die **Einführung verpflichtender IT-Audits:**
  Betreiber kritischer Infrastrukturen werden verpflichtet, mindestens alle zwei Jahre einen Sicherheitsaudit durchzuführen, um ihre organisatorischen und technischen Vorkehrungen zur IT-Sicherheit überprüfen zu lassen. Die Auditergebnisse werden dem BSI übermittelt.[85]

Sowohl in der öffentlichen Debatte als auch innerhalb der Bundesregierung wurde der Referentenentwurf nach seiner Veröffentlichung zum Teil kontrovers diskutiert. Während die übergeordnete Stoßrichtung des Entwurfes, die Verbesserung der IT-Sicherheit in Deutschland, allgemein wohlwollend kommentiert wurde, stießen die Teile der Maßnahmen auf heftige Kritik.[86] Diese bezieht sich insbesondere auf die nach Ansicht der Industrie unzureichenden Definitionen und fehlenden Präzisierungen des Entwurfes. Dies betrifft vor allem die Frage des genauen Anwendungsbereichs (welche Unternehmen fallen unter die Regelungen, insbesondere unter die vorgesehenen Meldepflichten?) und der genauen Tatbestände (was ist zu melden?).

Aus diesem Grund fokussiert sich die vorliegende Studie auf diese beiden Elemente des Referentenentwurfs. Weitere Gesetzesinhalte, wie beispielsweise verpflichtende Sicherheitsaudits, stehen nicht im Fokus der Studie, werden dagegen nicht behandelt.

[82] Bundesministerium des Innern 2013a, S. 11
[83] Bundesministerium des Innern 2013a, S. 11–12
[84] Bundesministerium des Innern 2013a, S. 7
[85] Bundesministerium des Innern 2013a, S. 7–8
[86] Vgl. bspw.:
Stellungnahme DIHK: Deutscher Industrie- und Handelskammertag o. J.
Stellungnahme BITKOM: BITKOM 2012
Stellungnahme der Bundesärztekammer: Bundesärztekammer
Stellungnahme VKU: Verband kommunaler Unternehmen 2013
Stellungnahme DIN: Deutsches Institut für Normung o. J.

NÄHERE BETRACHTUNG DER GEPLANTEN MELDEPFLICHTEN

Im Referentenentwurf werden, wie oben dargestellt, drei Meldepflichten angesprochen, welche im Folgenden näher betrachtet werden:

Art der Änderung	Sender	Empfänger	Anlass
Neueinführung	Unternehmen der kritischen Infrastruktur	BSI – Bundesamt für Sicherheit in der Informationstechnik	Schwerwiegende Beeinträchtigungen informationstechnischer Systeme.
Ausweitung	Telekommunikationsdiensteanbieter und Netzbetreiber	BNetzA – Bundesnetzagentur	Störungen und unerlaubte Zugriffe auf Systeme der Nutzer und Teilnehmer.
Ausweitung	Telekommunikationsdiensteanbieter und Netzbetreiber	Nutzer von öffentlich zugänglichen Telekommunikationsdiensten	Störungen, die von Datenverarbeitungssystemen der Nutzer ausgehen.

Tabelle 1: Übersicht der Meldepflichten des Referentenentwurfs für IT-Sicherheit

Der Referentenentwurf sieht eine **Neueinführung der Meldepflicht für Unternehmen der KRITIS-Sektoren** vor:

> *„Betreiber kritischer Infrastrukturen haben über die Warn- und Alarmierungskontakte nach Absatz 3 schwerwiegende Beeinträchtigungen ihrer informationstechnischen Systeme, Komponenten oder Prozesse, das heißt Beeinträchtigungen, die Auswirkungen auf die Funktionsfähigkeit der von ihnen betriebenen kritischen Infrastrukturen haben können, unverzüglich an das Bundesamt zu melden."*[87]

Des Weiteren ist eine **Ausweitung der bereits nach §109a des Telekommunikationsgesetzes (TKG)[88] bestehenden Meldepflicht** an die BNetzA vorgesehen:

> *„Wer ein öffentliches Telekommunikationsnetz betreibt oder öffentlich zugängliche Telekommunikationsdienste erbringt, hat Beeinträchtigungen von Telekommunikationsnetzen und –diensten, die zu einer Störung der Verfügbarkeit der über diese Netze erbrachten Dienste oder zu einem unerlaubten Zugriff auf Telekommunikations- und Datenverarbeitungssystemen der Nutzer oder Teilnehmer führen können und von denen der Netzbetreiber oder der Telekommunikationsbetreiber Kenntnis erlangt, der Bundesnetzagentur unverzüglich mitzuteilen."*[89]

Zuvor war eine Meldung an die BNetzA nur „im Fall einer Verletzung des Schutzes personenbezogener Daten" notwendig.[90]

Die dritte Meldepflicht ist ebenfalls eine **Ausweitung der Meldepflicht an die Nutzer der Telekommunikationsdienstleistungen** im Sinne des TKG:

> *„Werden Störungen bekannt, die von Datenverarbeitungssystemen der Nutzer ausgehen, sind diese vom Dienstanbieter unverzüglich zu benachrichtigen. Soweit technisch möglich und zumutbar, müssen die Nutzer auf angemessene, wirksame*

[87] Bundesministerium des Innern 2013a, S. 9
[88] Bundesministerium für Verkehr und digitale Infrastruktur
[89] Bundesministerium des Innern 2013a, S. 11
[90] Bundesministerium für Verkehr und digitale Infrastruktur, §109a

und zugängliche technische Mittel hingewiesen werden, mit deren Hilfe die Nutzer Störungen […] erkennen und beseitigen können".[91]

Bisher war eine Meldung an die Betroffenen nur notwendig, sofern anzunehmen war, „dass durch die Verletzung des Schutzes personenbezogener Daten Teilnehmer oder andere Personen schwerwiegend in ihren Rechten oder schutzwürdigen Interessen beeinträchtigt werden".[92]

In dem Referentenentwurf werden an unterschiedlichen Stellen die Begriffe „Teilnehmer", „Nutzer" und „Endnutzer" verwendet. Um eine Aussage über die angesprochenen Gruppen zu treffen, folgt eine Definition der drei verwendeten Begriffe nach dem Telekommunikationsgesetz, welches laut Referentenentwurf ausgeweitet werden soll.[93]

Laut dem Referentenentwurf zur Erhöhung der IT-Sicherheit sollen Störungen, die vom Datenverarbeitungssystem der **Nutzer** ausgehen, genau an diese gemeldet werden. Die Rede ist demnach von Personen, die Telekommunikationsdienste in Anspruch nehmen, also auch selbst diejenigen, die keinen Vertrag mit dem Dienstleister abgeschlossen haben.

Teilnehmer	Nutzer	Endnutzer
„jede natürliche oder juristische Person, die mit einem Anbieter von öffentlich zugänglichen Telekommunikationsdiensten einen Vertrag über die Erbringung derartiger Dienste geschlossen hat"	„jede natürliche oder juristische Person, die einen öffentlich zugänglichen Telekommunikationsdienst für private oder geschäftliche Zwecke in Anspruch nimmt oder beantragt, ohne notwendigerweise Teilnehmer zu sein"	„ein Nutzer, der weder öffentliche Telekommunikationsnetze betreibt noch öffentlich zugängliche Telekommunikationsdienste erbringt"

Tabelle 2: Teilnehmer, Nutzer und Endnutzer laut TKG

3.2. Analyse des Entwurfs für das IT-Sicherheitsgesetz

DEFINITIONEN DES ANWENDUNGSBEREICHS

Bei der Festlegung des Anwendungsbereichs nimmt der Referentenentwurf keine eindeutigen Abgrenzungen etwa zwischen betroffenen Sektoren, Branchen oder Unternehmen vor. Stattdessen spricht der Entwurf von „Betreibern kritischer Infrastrukturen" und nennt dabei folgende sieben KRITIS-Sektoren:

- Energie
- Gesundheit
- Wasser[94]
- Ernährung
- Transport und Verkehr
- Finanz- und Versicherungswesen
- Informationstechnik und Telekommunikation[95]

[91] Vgl. Bundesministerium des Innern 2013a
[92] Bundesministerium für Verkehr und digitale Infrastruktur, §109a
[93] Bundesministerium für Verkehr und digitale Infrastruktur, §3
[94] Das Bundesministerium des Innern definiert nur die Öffentliche Wasserversorgung und Abwasserbeseitigung als KRITIS. Ob und inwieweit private Wasserwirtschaftsunternehmen hier auch gemeint sind, ist nicht eindeutig formuliert.
[95] Im Referentenentwurf ausgenommen ist die Kommunikationstechnik des Bundes, vgl. Bundesministerium des Innern 2013a, S. 6.

Der Verweis auf die Definition des BMI für Betreiber kritischer Infrastrukturen führt dazu, dass zum jetzigen Zeitpunkt keine eindeutige Identifikation der betroffenen Unternehmen und Telekommunikationsdienstleister möglich ist. Derzeit werden vom BMI nur die genannten Sektoren und die diesen zugeordneten Branchen definiert. Präzise Auswahlkriterien für KRITIS-Unternehmen wurden bisher nicht publiziert.

Obgleich der Referentenentwurf darauf verweist, dass die betroffenen Einrichtungen und Anlagen bzw. Teile davon im Rahmen der Rechtsverordnung nach § 10 Absatz 2[96] näher bestimmt werden, so werden keine Angaben über den Inhalt dieser Rechtsverordnung gemacht. Dementsprechend wird die Definition der unter KRITIS gefassten Unternehmen vollständig dem Verordnungsgeber überlassen.

Die Ausführungen des Referentenentwurfs erschweren auch die Abschätzung des von den betroffenen Unternehmen zu leistenden Erfüllungsaufwandes deutlich.

DEFINITION DER TATBESTÄNDE

Definitorische Spielräume lassen sich im Entwurf auch bzgl. der im Rahmen der vorgesehenen Meldepflicht zu meldenden Tatbestände erkennen. So finden sich nur wenige Hinweise darauf, welche Art von IT-Sicherheitsvorfällen bzw. welche Schadensdimension tatsächlich gemeldet werden sollen.

Angesichts der hohen Anzahl und der unterschiedlichen Arten an IT-Angriffen, denen deutsche Unternehmen täglich ausgesetzt sind, erscheint eine Präzisierung der IT-Sicherheitsvorfälle, die „schwerwiegende Beeinträchtigungen" verursachen, allerdings sachlich geboten. – so schätzt das BKA, dass täglich ca. 30.000 Cyberangriffe auf Unternehmen in Deutschland stattfinden. Eine Aussage darüber, welche dieser Angriffe eine „schwerwiegende Beeinträchtigung" auslösen und dementsprechend meldepflichtig wären, könnte auf Grundlage des Referentenentwurfs aktuell nicht getroffen werden.

Speziell für Anbieter von Telekommunikationsdiensten und Betreiber von Telekommunikationsnetzen sieht der Referentenentwurf eine weitere Meldepflicht vor, die an die BNetzA zu richten ist. Gemeldet werden müssen „Beeinträchtigungen von Telekommunikationsnetzen und -diensten, die zu einer Störung der Verfügbarkeit der über diese Netze erbrachten Dienste oder zu einem unerlaubten Zugriff auf Telekommunikations- und Datenverarbeitungssystemen der Nutzer oder Teilnehmer führen können und von denen der Netzbetreiber oder der Telekommunikationsdiensteanbieter Kenntnis erlangt […]".[97]

Ohne weitere Abgrenzung dessen, was hier unter „Störung" und „Verfügbarkeit" gemeint ist, ist der vorliegende Passus so zu verstehen, dass auch geringfügige Störungen der Verfügbarkeit an die BNetzA gemeldet werden müssen. Dies könnte zu einem erheblichen Anstieg der Meldungen an die BNetzA führen. Mit dieser Regelung tritt der Referentenentwurf auch klar hinter die Vorgaben bereits existierender Meldepflichten an die BNetzA zurück, die auf definierte Störungen mit „beträchtlichen Auswirkungen"[98] fokussieren. Neben diesen neuen Kriterien führt auch eine weitere Formulierung des Gesetzestextes zu einer Erhöhung der meldepflichtigen Sicherheitsvorfälle. Bisher mussten ausschließlich Vorfälle mit tatsächlichen beträchtlichen Auswirkungen gemeldet werden. Der aktuelle Referentenentwurf sieht darüber hinaus vor, dass auch Sicherheitsvorfälle gemeldet werden müssen, „die zu einer Störung der Verfügbarkeit der über diese Netze erbrachten Dienste oder zu einem unerlaubten Zugriff auf Telekommunikations- und Datenverarbeitungssystemen der Nutzer oder Teilnehmer führen **können**"[99] (eigene Hervorhebung). Anders als bisher sollen Sicherheitsfälle also nicht mehr nach ihrer tatsächlichen Konsequenz, sondern nach ihrem Potential bewertet werden. Diese Änderung der Meldekriterien könnte eine weitere Steigerung der Meldezahlen und des damit verbundenen Aufwands in Wirtschaft und öffentlichem Dienst mit sich bringen.

---

[96] „Das Bundesministerium des Innern bestimmt nach Anhörung der betroffenen Wirtschaftsverbände und im Einvernehmen mit dem Bundesministerium für Wirtschaft und Technologie durch Rechtsverordnung das Nähere über das Verfahren der Erteilung von Sicherheitszertifikaten und Anerkennungen nach § 9 und deren Inhalt". (§10 Abs. 1 BSI-Gesetz, Deutscher Bundestag)

[97] Bundesministerium des Innern 2013a, S. 11

[98] Bundesministerium für Verkehr und digitale Infrastruktur, §109, Abs. 5

[99] Bundesministerium des Innern 2013a, S. 11

Über die Meldung an die BNetzA hinaus sieht der Referentenentwurf für Telekommunikationsdiensteanbieter und Betreiber von Kommunikationsnetzen auch eine Meldung an ihre Nutzer[100] vor, wenn die Unternehmen Störungen, die von Datenverarbeitungssystemen der Nutzer ausgehen, erkennen. In einem solchen Falle sollen die Nutzer zudem auf „angemessene, wirksame und zugängliche Mittel" hingewiesen werden, mit denen die entsprechenden Störungen behoben werden können.[101] Was als Störung einzustufen wäre, bleibt ebenso offen wie die Frage, ob ein Hinweis an die Nutzer ausreicht oder ob auch entsprechende Soft- und Hardware zur Verfügung gestellt werden muss.

RISIKO VON MEHRAUFWAND/ DOPPELMELDUNG

Der vorliegende Referentenentwurf birgt insbesondere für Telekommunikationsdiensteanbieter und Betreiber von Kommunikationsnetzen das Risiko von Mehraufwand durch Doppelmeldungen. Bereits heute müssen Telekommunikationsdiensteanbieter nach § 109 Abs. 5 TKG Sicherheitsverletzungen und Störungen an die BNetzA melden, sobald diese beträchtliche Auswirkungen auf den Betrieb der Telekommunikationsnetze oder das Erbringen von Telekommunikationsdiensten haben. Da Telekommunikationsdiensteanbieter und Betreiber von Kommunikationsnetzen zugleich auch KRITIS-Betreiber sind, gilt für sie die Pflicht, (schwerwiegende) Beeinträchtigungen oder Störungen auch an das BSI zu melden. Eine eindeutige Zuordnung, welche Meldungen die Netzbetreiber und Telekommunikationsdiensteanbieter an das BSI, die BNetzA oder an beide vorgenommen werden muss, ist im Referentenentwurf nicht enthalten. Im Falle einer vollständigen oder teilweisen Überschneidung entstünde hier eine vermeidbare Doppelmeldung der gleichen Information. Da die BNetzA die bei ihr eingehenden Meldungen ohnehin schon heute an das BSI weitergibt, entstünde hier kein erkennbarer Mehrwert.

VERWENDUNG UND SPEICHERUNG DER MELDEDATEN

Zurzeit ungeklärt bleibt auch die Frage, wie die zu meldenden Informationen auf Seiten der Behörden weiterverarbeitet und ausgewertet werden. Da die Meldung nicht anonymisiert erfolgt und für das BSI zudem eine jährliche Berichtspflicht vorgesehen ist, ist davon auszugehen, dass behördenseitig hinreichende Vorkehrungen getroffen werden, um eine Offenlegung der Unternehmensidentitäten zu verhindern. Ob und wie diese Daten geschützt werden, wird im Referentenentwurf allerdings nicht spezifiziert. Dies gilt auch für die Frage, welche spezifischen Sicherheitsvorkehrungen amtsseitig getroffen werden, sollten die Meldungen zentral gespeichert werden.

ERSTELLUNG EINES LAGEBILDES

Im Referentenentwurf wird auf die Erstellung und Veröffentlichung eines Lageberichts als Grundlage für abgestimmte Reaktionen auf Cybersicherheitsvorfälle hingewiesen.[102] Zugleich wird eine jährliche Berichtspflicht des BSI formuliert – aktuell veröffentlicht das BSI seine Lageberichte in einem Abstand von zwei Jahren.

Während ein solcher jährlicher Bericht insbesondere der breiten Öffentlichkeit wichtige Entwicklungen und besondere Beispiele aus dem Bereich der IT-Sicherheit vermitteln kann, erscheint er für Unternehmen und Industrie nur von geringem Nutzen. Da das BSI durch die zu erwartenden Meldungen in die Lage versetzt wird, das Lagebild weiter zu verbessern und die Landkarte der IT-Sicherheit weiter auszudifferenzieren und das Lagebild eine abgestimmte Reaktion auf Cyberangriffe ermöglichen soll, erscheint es zweckmäßig, das Lagebild zeitnah auch mit den Unternehmen auszutauschen.

DEFINITIONEN DER SICHERHEITSSTANDARDS

Als eine weitere Maßnahme zur Steigerung der IT-Sicherheit in Deutschland sieht der Referentenentwurf die Einhaltung eines IT-Mindestsicherheitsstandards für KRITIS-Betreiber vor. KRITIS-Betreiber und ihre Branchenverbände können diese Sicherheitsstandards selbstständig und branchenspezifisch erarbeiten. Die erarbeiteten Vorschläge werden durch das BSI in Abstimmung mit den zuständigen Aufsichtsbehörden der entsprechenden Branchen geprüft und

[100] Der Referentenentwurf unterscheidet nicht zwischen Teilnehmern und Nutzern. Diese Distinktion ist aber durchaus relevant. Während Teilnehmer in einer vertraglich geregelten Beziehung zu dem Telekommunikationsanbieter stehen, sind Nutzer den Betreibern von Telekommunikationsnetzen teilweise unbekannt, wenn Sie diese über den Zugang eines Teilnehmers nutzen. Siehe Kapitel 4 für weitere Ausführungen.
[101] Bundesministerium des Innern 2013a, S. 12
[102] Bundeministerium des Innern 2013a, S. 2-3

bei festgestellter Eignung zugelassen.[103] Mit dieser Regelung knüpft der Referentenentwurf an den kooperativen Ansatz der in Kapitel 2.1. dargestellten Strategien und Initiativen an. Der Referentenentwurf gibt bisher allerdings keinen Aufschluss darüber, wie der vorgeschlagene Anerkennungsprozess geplant ist. Eine transparente und klare Regelung dieses Prozesses sollten die Gestaltungsräume der Unternehmen definieren und damit eine flexible und zielorientierte Erstellung der IT-Sicherheitsstandards unterstützen.

3.3. Die aktuelle europäische Gesetzgebung und mögliche Einflüsse auf das deutsche Gesetzesvorhaben

Auch auf europäischer Ebene wird das Thema IT-Sicherheit legislativ behandelt, insbesondere in dem derzeit von der Europäischen Kommission entwickelten Vorschlag für eine „Richtlinie[104] des europäischen Parlaments und des Rates über Maßnahmen zur Gewährleistung einer hohen gemeinsamen Netz- und Informationssicherheit in der Union“[105] (kurz Richtlinie zur Informationssicherheit).

Im Folgenden werden die Aspekte der europäischen Richtlinie zur Informationssicherheit aufgegriffen, deren Inhalte für die Ausgestaltung des deutschen Referentenentwurfs relevant sind.

DEFINITION DES ANWENDUNGSBEREICHS

Der aktuelle Stand der Richtlinie zu Informationssicherheit definiert sieben Sektoren als kritische Infrastruktur und somit als Zielgruppe des Vorschlags. Im Einzelnen werden folgende Bereiche genannt:

- Energie (Strom, Gas und Öl)
- Elektronische Kommunikationsdienste
- Verkehr (Luftfahrt, Seeverkehr, Schienenverkehr, Wasserverkehr, unterstützende Logistikdienste)
- Gesundheitswesen (Einrichtungen der medizinischen Versorgung und Gesundheitsfürsorge)
- Bankwesen (Kreditinstitute)
- Finanzinfrastrukturen (Börsen und Clearingstelle)
- Öffentliche Verwaltung

Aus sektoraler Betrachtungsweise liegen die wesentlichen Unterschiede zwischen dem deutschen und dem europäischen Entwurf darin, dass der deutsche Entwurf die Sektoren Wasser und Ernährung mit einbezieht. Diese sind nicht Teil des europäischen Entwurfs. Die öffentliche Verwaltung hingegen ist, anders als im deutschen Entwurf, auf europäischer Ebene im Entwurf enthalten. Meldepflichten und andere Auflagen würden also auch für öffentliche Organisationen gelten. Eine spätere Inkludierung der öffentlichen Verwaltung könnte also die Folge einer Verabschiedung der europäischen Richtlinie zur Informationssicherheit sein. Der Vorschlag betont zudem, dass die Liste der aufgeführten Sektoren nicht erschöpfend ist.[106] Weitere Sektoren oder Branchen könnten also der Liste hinzugefügt werden.

Ein weiterer Unterschied besteht in der Ausweitung der betroffenen Unternehmen im Bereich der Informations- und Kommunikationstechnologie. In der europäischen Richtlinie werden auch sogenannte „Anbieter von Diensten der Informationsgesellschaft“ als Teile der kritischen Infrastruktur verstanden. Dazu zählen laut Entwurf

- Plattformen des elektronischen Geschäftsverkehrs
- Internet-Zahlungs-Gateways

[103] Bundesministerium des Innern 2013a, S. 7
[104] Europäische Richtlinien müssen von den europäischen Mitgliedsstaaten in nationales Recht umgewandelt werden um gültig zu sein.
[105] Europäische Kommission
[106] Europäische Kommission Art. 8.3

- Soziale Netze
- Suchmaschinen
- Cloud-Computing-Dienste und
- Application-Stores.

Auch diese Liste wird in dem Vorschlag als nicht erschöpfend bezeichnet. Hard- und Software-Hersteller werden hingegen explizit ausgenommen und nicht Anbieter von Diensten der Informationsgesellschaft verstanden. Falls diese Anbieter auf europäischer Ebene zur Meldung verpflichtet werden, müsste auch der deutsche Gesetzgeber eine entsprechende Erweiterung der betroffenen Unternehmen vornehmen.

Welche Unternehmen aus den genannten Sektoren Sicherheitsvorfälle melden müssen, lässt sich dem Vorschlag nicht eindeutig entnehmen. Wie auch im deutschen Entwurf lässt die gewählte Definition Konkretisierungsbedarf erkennen. Meldepflichtig sind „Betreiber kritischer Infrastrukturen, die für die Aufrechterhaltung zentraler wirtschaftlicher und gesellschaftlicher Tätigkeiten in den Bereichen Energie, Verkehr, Banken, Börsen und Gesundheit unerlässlich sind".[107] Genauere Kriterien zur Identifikation dieser Marktteilnehmer sind nicht genannt. Derzeit werden lediglich Kleinstunternehmen grundsätzlich von der Meldepflicht ausgenommen.[108] Ohne eine Konkretisierung zur Identifizierung auf deutscher und europäischer Ebene, lässt sich kein sinnvoller Vergleich herstellen. Allerdings erscheint die Ausgrenzung von Kleinstunternehmen auf europäischer Ebene als sinnvolle erste Maßnahme, um entstehende Verunsicherungen zu vermeiden.

DEFINITION DER TATBESTÄNDE

Die oben definierten Marktteilnehmer und die öffentliche Verwaltung werden dazu verpflichtet, alle Sicherheitsvorfälle zu melden, die erhebliche Auswirkungen auf die Sicherheit der von ihnen bereitgestellten Kerndienste haben" (Artikel 14 §2). Diese Definition erlaubt einen ähnlich großen Interpretationsspielraum wie der deutsche Referentenentwurf. Die europäische Kommission behält sich vor, eine genauere Spezifikationen der Umstände bei Sicherheitsvorfällen durch spätere delegierte Rechtsakte zu erlassen.[109] Bis diese europäischen Rechtsakte erfolgt sind, ist nicht einzuschätzen, inwiefern sich diese Definition der Tatbestände mit der deutschen Regelung decken wird, ober ob wesentliche Unterschiede und daraus entstehender Anpassungsbedarf der deutschen Regulierung bestehen werden.

Nach der europäischen Richtlinie zur Informationssicherheit verbleibt die Verantwortung für die Meldung von Sicherheitsvorfällen in ausgegliederten Netz- und Informationssystemen bei den jeweiligen Marktteilnehmern oder der öffentlichen Verwaltung. Dieser Aspekt ist im deutschen Referentenentwurf derzeit noch ungeklärt und könnte für Verunsicherung im Bereich der extern bereitgestellten IT und IT-Sicherheit sorgen. An dieser Stelle könnte eine Orientierung an der europäischen Richtlinie für Informationssicherheit vorteilhaft sein

RISIKO VON MEHRAUFWAND/ DOPPELMELDUNG

Der deutsche Referentenentwurf sieht drei Meldepflichten vor, die von unterschiedlichen Akteuren an unterschiedliche Zielstellen gemeldet werden sollen. Auf europäischer Ebene ist eine Meldung an die national zuständige Behörde verpflichtend vorgesehen.

Anders als auf deutscher Ebene wird das Risiko einer Doppelmeldung auf europäischer Ebene umgangen. Anbieter von Kommunikationsdiensten werden explizit von der Meldepflicht ausgenommen, da diese bereits durch andere Richtlinien zur Meldung verpflichtet sind.[110] An dieser Stelle schafft die europäische Richtlinie zur Informationssicherheit Klarheit und vermeidet somit Verunsicherung. Dies gibt es im deutschen Referentenentwurf so noch nicht.

---

[107] Europäische Kommission Art. 8.3
[108] Europäische Kommission Art. 14.8
[109] Europäische Kommission Art. 14.5 und 14.6
[110] Elektronische Kommunikationsdienste werden bereits separat in der Richtlinie 2002/114/EG zu der Meldung von Sicherheitsvorfällen verpflichtet. Artikel 2 § 3 des aktuellen Vorschlags, befreit solche Organisationen daher von zusätzlichen Meldepflichten. Die anderen Bestandteile der Richtlinie bleiben unberührt geltend.

DEFINITIONEN DER SICHERHEITSSTANDARDS

Der Vorschlag der Europäischen Kommission definiert nur wenige Eckpunkte über die Ausgestaltung von Sicherheitsstandards. Ähnlich wie im deutschen Referentenentwurf wird allerdings gefordert, dass die zuständigen Behörden befugt sind, Informationen über den Stand der Sicherheit der betroffenen Organisationen einzuholen und sich diese einer Sicherheitsprüfung unterziehen müssen. Ob es sich um eine einmalige oder periodische Sicherheitsprüfung handelt, geht aus dem Vorschlag nicht eindeutig hervor. Diese Prüfung der Sicherheit dieser Netz- und Informationssysteme soll entweder durch eine Behörde selbst oder eine qualifizierte unabhängige Stelle durchgeführt werden.[111] An dieser Stelle ist derzeit kein späterer Anpassungsbedarf der deutschen Gesetzgebung festzustellen.

VERWENDUNG UND SPEICHERUNG DER MELDEDATEN

Die europäische Richtlinie sieht vor, jeweils eine nationale Behörde zu benennen, die für die Umsetzung der Inhalte in dem jeweiligen Mitgliedsstaat zuständig ist. Die nationale Behörde sammelt Meldungen von Sicherheitsvorfällen und gibt diese unter bestimmten Bedingungen an unterschiedliche Stakeholder weiter. So ist eine Unterrichtung der Öffentlichkeit vorgesehen, sobald dies nach Einschätzung der zuständigen Behörde im öffentlichen Interesse liegt. Es läge ebenfalls im Ermessen dieser nationalen Behörde, ob die Informierung der Öffentlichkeit durch die nationale Behörde selbst oder durch den Marktteilnehmer bzw. die betroffene öffentliche Verwaltung geschieht.[112] An dieser Stelle gehen die auf europäischer Ebene zugeschrieben Kompetenzen über die Regelungen im aktuellen Referentenentwurf hinaus. Falls die europäische Richtlinie umgesetzt wird, wäre also mit einer Erweiterung der Kompetenzen der zuständigen deutschen Behörde zu rechnen.

Der Vorschlag der Europäischen Kommission enthält weiterhin konkrete Informationen über ein europäisches Frühwarnsystem zwischen den national zuständigen Behörden. Bei der Erfüllung bestimmter Kriterien (Potential schnellerer Ausweitung, Übersteigung nationaler Reaktionskapazitäten oder Betroffenheit mehrerer Mitgliedsstaaten) werden „alle in ihrem Besitz befindlichen relevanten Informationen“[113] über nationale Sicherheitsvorfälle an andere europäische Sicherheitsbehörden übertragen. Die nationale Behörde würde Informationen zu Sicherheitsfällen also nicht nur speichern und verwerten, sondern auch auf europäischer Ebene weiterleiten. Auch Geschäftsgeheimnisse der meldenden Unternehmen könnten, allerdings nur wenn unbedingt notwendig, zwischen den Behörden auf europäischer Ebene ausgetauscht werden.[114]. Die Richtlinie der Europäischen Kommission sieht zudem Sanktionen vor, die durch die national verantwortlichen Behörden umzusetzen sind. Diese sollen gegen Marktteilnehmer und die öffentliche Verwaltung verhängt werden, falls diese nicht mit den Forderungen der Richtlinie einhergehen.[115] Über die Ausgestaltung dieser Sanktionen enthält der Vorschlag keine Informationen. Die europäische Richtlinie zur Informationssicherheit geht an dieser Stelle über die deutsche Gesetzgebung hinaus und räumt den nationalen Behörden weitreichendere Kompetenzen ein. Des Weiteren sind die national ernannten Sicherheitsbehörden laut Artikel 14.4 dafür verantwortlich, Sicherheitsvorfälle mit „schwerwiegendem kriminellen Hintergrund an die jeweils zuständigen Strafverfolgungsbehörden zu melden. Sicherheitsvorfälle, die über das Frühwarnungssystem verbreitet werden und mutmaßlicher Weise einen kriminellen Hintergrund haben, sollen zudem an das bei Europol angesiedelte Europäische Zentrum zur Bekämpfung der Cyberkriminalität gemeldet werden.

3.4. Fazit

Der vorliegende Referentenentwurf für das IT-Sicherheitsgesetz dokumentiert den Anspruch der Bundesregierung einer Förderung der IT-Sicherheit in Deutschland nachzukommen und diese aktiv mitzugestalten. Das BMI, als Institution für Bevölkerungsschutz und Sicherheitsaufgaben, übernimmt eine federführende Rolle in der Verfolgung der Entwicklungen in diesem für Wirtschaft und Gesellschaft bedeutenden Bereich.

Es wird deutlich, dass die Erfahrung und das Know-how der betroffenen Branchen und Branchenverbände anerkannt werden. Die Branchen und Branchenverbände werden in diesem Zuge

[111] Europäische Kommission Art. 15.2a
[112] Europäische Kommission Art. 14.4
[113] Europäische Kommission Art. 10.2
[114] Europäische Kommission, S. 18 (38)
[115] Siehe Europäische Kommission Art. 17

an verschiedenen Stellen des Gesetzes integriert, etwa bei der Entwicklung branchenspezifischer Sicherheitsstandards.

Vor dem Hintergrund der möglichen Tragweite des Gesetzes und seiner inhaltlichen Ziele wäre jedoch ein noch stärkerer und frühzeitigerer Austausch mit dem Betroffenen bzw. Beteiligten zielführend und empfehlenswert, um zentrale Elemente des Referentenentwurfs zu schärfen und dessen Umsetzbarkeit und Wirksamkeit zu gewährleisten. Besonders die Notwendigkeit klarer Definitionen und die Rechtssicherheit für Unternehmen sprechen für eine stärkere Beteiligung der Branchen und Branchenverbände.

Klärungsbedarf besteht besonders bei Fragestellungen zu möglichen Doppelregulierungen und etwaigen, nicht beabsichtigten Auswirkungen des Gesetzes. Diese sollten ausführlich beleuchtet und wenn möglich beseitigt oder ausgeglichen werden, um eine effiziente und effektive Umsetzung zu gewährleisten.

KAPITEL 4

Quantitative Analyse möglicher monetärer Folgen des IT-Sicherheitsgesetzes

Für die Studie wurden zwölf Interviews mit Unternehmen unterschiedlicher Branchen durchgeführt. Bei der überwiegenden Mehrheit der befragten Unternehmen handelte es sich um Betreiber kritischer Infrastrukturen und Telekommunikationsdiensteanbieter. Diese Unternehmen wären direkt von dem Referentenentwurf betroffenen. Daneben wurden auch Zulieferer und Ausrüster, z.B. aus der Maschinenbauindustrie, der Luftfahrtindustrie und der Elektroindustrie, von KRITIS-Betreibern in die Befragung aufgenommen. Die (qualitativen) Interviews wurden auf Grundlage eines standardisierten Interviewleitfadens mit offenem Antwortformat durchgeführt, der neben inhaltlichen Fragen u.a. zur Meldepflicht und IT-Sicherheitsstandards auch einen Teil zur Abschätzung des unternehmensseitigen Aufwands durch den Meldeprozesses umfasste. Dieser Leitfaden wurde im Vorfeld der Gespräche mit dem Auftraggeber abgestimmt. Daneben wurden im Rahmen der Studie auch eine Reihe weiterer, informeller Gespräche zu verschiedenen Aspekten des Themas der IT-Sicherheit mit Vertretern der Branchen, der Behörden und anderer Institutionen geführt, um den Fokus der Studie zu kontextualisieren und die aktuelle Debatte adäquat zu berücksichtigen.

Aufgrund der nicht eindeutigen Definitionen des Referentenentwurfs und einer begrenzten Stichprobe sind die Ergebnisse dieses Kapitels als indikativ zu verstehen, um ein Verständnis für die Größenordnung der erwarteten Kosten zu erlangen. Dieses Vorgehen macht den Bedarf nach einer eindeutigen Eingrenzung der betroffenen Unternehmen und meldepflichtigen Tatbestände deutlich.

4.1 Bürokratiekostenschätzung

Mit den geplanten Meldepflichten kommen, wie im vorigen Kapitel bereits angedeutet, Kosten auf die betroffenen Unternehmen zu. Jede Meldung ist mit einem bürokratischen Aufwand für das Unternehmen verbunden, es entstehen Kosten durch die Bearbeitung und Erstellung der einzelnen Meldungen. Um eine Einschätzung darüber treffen zu können, welches Ausmaß die Bürokratiekosten annehmen, wird in diesem Kapitel eine Methode angewendet, die sich am Standardkosten-Modell (SKM) orientiert.

METHODIK

Gesetze und Verordnungen enthalten unterschiedlichste Verpflichtungen für Unternehmen. Jene Verpflichtungen, die Kosten verursachen, lassen sich grob in zwei Kategorien unterteilen. Zum einen werden den Unternehmen durch Gesetze so genannte inhaltliche Verpflichtungen – wie beispielsweise der Einsatz von Schadstofffiltern in Kraftfahrzeugen oder die Zahlung von Steuern – auferlegt, die vor allem der Realisierung öffentlicher Interessen dienen. Zum anderen entstehen Kosten durch die Erarbeitung und Bereitstellung von Informationen, also durch Informationsverpflichtungen, wie das Erstellen von Berichten, das Beibringen von Nachweisen und Belege oder das Ausfüllen von Anträgen. Das Standard-Kosten-Modell beschränkt sich bei der Messung rein auf diese Informations- bzw. Bürokratiekosten.[116]

Das SKM wurde in den Niederlanden zur Messung von Bürokratieaufwänden und der Identifikation von Kostentreibern entwickelt. Seitdem wurde es sowohl international als auch in Deutschland mehrfach erfolgreich angewendet, um den bürokratischen Kostenaufwand für eine gesetzliche Informationspflicht „ex-post“ zu messen. Das Modell ermöglicht aber auch eine „ex-ante“-Schätzung der zu erwartenden Kosten verschiedener Regulierungsalternativen.

Das SKM ist eine pragmatische Schätzmethode. Sein Kern ist die Identifizierung von Informationspflichten in den Regulierungsalternativen und die Zuordnung sowie die Bewertung der zuge-

[116] Bertelsmann Stiftung

hörigen Standard-Aktivitäten. Die Bewertung erfolgt durch das Produkt aus Anzahl der meldepflichtigen Vorgänge, Bearbeitungsdauer und Stundensatz. Diese Herangehensweise beruht auf der Erkenntnis, dass sich die Tätigkeiten unterschiedlicher Meldeprozesse stark ähneln, selbst wenn sich die Meldeinhalte erheblich unterscheiden.

BERECHNUNGSVERFAHREN

Die Berechnung der Bürokratiekosten für die Meldepflichten des Referentenentwurfs für IT-Sicherheit ist ein schrittweiser Prozess. Zunächst werden die Standardaktivitäten definiert und der Zeitaufwand für jede dieser Aktivitäten geschätzt, um so den Zeitaufwand pro Meldung zu ermitteln. Daraufhin werden die Kosten pro Zeiteinheit ermittelt und mit dem Zeitaufwand multipliziert, um die Kosten pro Meldung festzustellen (Kosten pro Verwaltungstätigkeit). Im Anschluss daran wird die Fallzahl ermittelt. Diese ergibt sich aus der durchschnittlichen Zahl der Meldungen eines Unternehmens in einem Jahr, multipliziert mit der Anzahl der von der Meldepflicht betroffenen Unternehmen. Anhand dieser Daten können sowohl die Kosten für ein einzelnes Unternehmen als auch für die Gesamtwirtschaft abgeschätzt werden, wenn der Referentenentwurf in seiner aktuellen Form umgesetzt werden würde.[117]

Die Schätzung der Bürokratiekosten ist demnach das Produkt der folgenden vier Faktoren:[118]

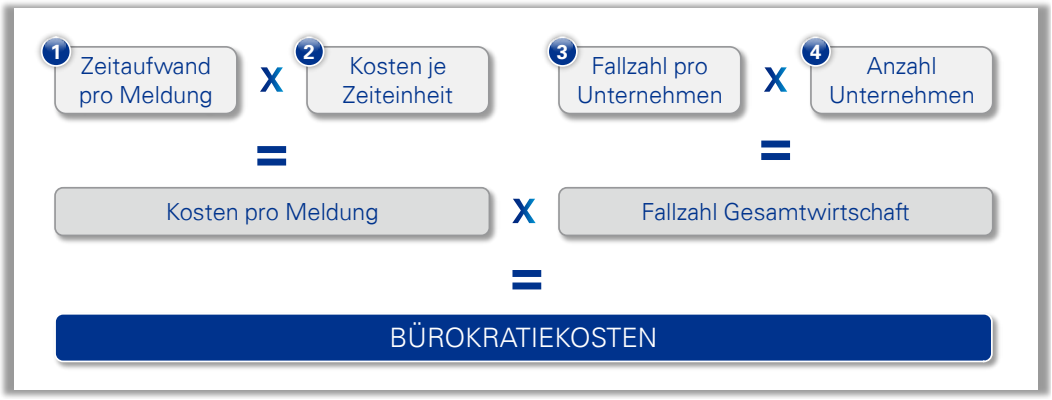

Abbildung 1: Berechnung der Bürokratiekosten

Faktor 1: Zeitaufwand pro Meldung

Eine Meldung wird im Rahmen des SKM als Prozess verstanden, der in einzelne standardisierte Verwaltungstätigkeiten unterteilt wird. Zur Berechnung des Zeitaufwandes einer Meldung werden also die Zeitaufwände für die einzelnen Verwaltungstätigkeiten ermittelt und addiert. Diese Tätigkeiten sind dabei für alle Meldeprozesse einheitlich und umfassen jeweils die folgenden 14 Aktivitäten:

[117] Für eine ausführliche Beschreibung des SKM siehe Statistisches Bundesamt 2006
[118] Bertelsmann Stiftung

1	Einarbeitung in die Informationspflicht	**2**	Datenübermittlung an zuständige Stellen oder Veröffentlichungen
3	Beschaffung der Daten	**4**	Interne Sitzung
5	Formulare ausfüllen, Beschriftung, Kennzeichnungen oder Etikettierungen durchführen	**6**	Externe Sitzungen
7	Berechnungen durchführen	**8**	Kopieren, archivieren, verteilen, ggf. löschen (wenn gesetzlich vorgeschrieben)
9	Überprüfung der Daten und Einträge	**10**	Korrekturen, die aufgrund der öffentlichen Prüfung durchgeführt werden müssen
11	Fehlerkorrektur	**12**	Weitere Informationsbeschaffung im Falle von Schwierigkeiten mit den zuständigen Behörden
13	Aufbereitung der Daten	**14**	Fortbildungs- und Schulungsteilnahmen

Tabelle 3: Standardisierte Verwaltungstätigkeiten nach dem Standardkosten-Modell

Hierfür wurden im Rahmen der Befragung auch die notwendigen Informationen zu den Bürokratiekosten abgefragt. Die Befragten gaben zunächst an, welche der 14 Tätigkeiten für die Erstellung der Meldung notwendig sind. Für alle notwendigen Tätigkeiten wurde von den Befragten bewertet, ob der Aufwand der Tätigkeit als „leicht", „mittel" oder „komplex" einzustufen ist.

Hinter jeder Aufwandseinstufung liegt ein standardisierter Minutenwert, der im SKM für jede Tätigkeit statistisch erhoben und in einer Zeitwerttabelle festgehalten wurde. Wenn etwa die Tätigkeit „Berechnungen durchführen" als leicht bewertet wird, ist damit laut der Zeitwerttabelle ein Aufwand von 3 Minuten verbunden. Bei einer Einschätzung als „komplex" werden hingegen 120 Minuten veranschlagt.[119] Die hinterlegten Zeitwerte unterscheiden sich für die einzelnen Aktivitäten.

Durch die Einschätzung des Aufwandes aller Tätigkeiten über alle Befragten hinweg, kann eine Einschätzung für die Höhe des Aufwandes je Aktivität getroffen werden. In Summe kann daraus der reguläre zeitliche Aufwand pro Meldung abgeleitet werden.

Faktor 2: Kosten je Zeiteinheit

In der Befragung wurde deutlich, dass die drei betrachteten Meldungen in der Regel von Fachexperten durchgeführt werden müssen (Annahme hier: ausgebildete Informatiker). Aus diesem Grund werden für die Berechnung der Meldekosten die durchschnittlichen Arbeitgeberkosten für einen Arbeitnehmer mit der hier angenommenen Qualifikation verwendet. Diese ergeben sich aus dem durchschnittlichen Bruttolohn für „Erbringung von Dienstleistungen der Informationstechnologie" (4626,25 Euro monatlich).[120] Zuzüglich der durch den Arbeitgeber zu leistenden Sozialabgaben, Gemeinkosten und Sachkosten ergibt sich eine monatliche Arbeitgeberbelastung von 7425,38 Euro.[121] Dies entspricht **einem Kostensatz von ca. 60,00 EUR pro Stunde**.[122]

Einige Unternehmen hielten es im Rahmen der Befragung für wahrscheinlich, dass durch die neuen Meldungen ein stärkerer Einsatz der Compliance- und Rechtsabteilung sowie des betrieblichen Datenschutzbeauftragten notwendig wäre, wodurch der Kostensatz deutlich höher ausfallen würde, da hier zusätzlich mit den Kosten für die juristische Expertise kalkuliert werden müsste.

[119] Diese 120 Minuten können sich aus Arbeitsvorgängen mehrerer Personen zusammensetzen.
[120] Dieser Satz ergibt sich aus der monatlichen Vergütung für die „Erbringung von Dienstleistungen der Informationstechnologie" vgl. Statistisches Bundesamt 2013c.
[121] Sozialabgabenberechnung: vgl. AOK. Es wird ein Gemeinkostensatz von 30% des Bruttogehalts angenommen, vgl. Bundesministerium der Finanzen. Die Sachkosten werden auf Basis des Sachkostenpauschale des Bundes berechnet, vgl. Bundesministerium der Finanzen.
[122] Der Stundensatz beruht auf eigenen Berechnungen unter der Annahme von 200 Arbeitstagen pro Jahr.

Faktor 3: Meldungen pro Unternehmen

Abhängig von der jeweiligen Definition der Tatbestände unterscheidet sich die Häufigkeit der Meldungen pro Unternehmen. Für die drei hier diskutierten Meldepflichten hat sich aus den Befragungen eine deutliche Unsicherheit ergeben, wie viele Meldungen tatsächlich vorgenommen werden müssen. Die aktuelle Ungewissheit bezüglich der Ausgestaltung der zum Referentenentwurf gehörenden Verordnung führt dazu, dass vielfach keine eindeutigen Zahlen zu der Häufigkeit der Meldungen ermittelt werden konnten, sondern dass vorerst mit einem geschätzten Wert an vorzunehmenden Meldungen als erste Schätzung gerechnet wurde.

Faktor 4: Anzahl der meldenden Organisationen

Bei der Anzahl der betroffenen Unternehmen muss zwischen den einzelnen Meldepflichten unterschieden werden. So ist einmal die Anzahl der Unternehmen zu definieren, die als KRITIS-Unternehmen eingestuft werden, und anderseits die Anzahl der Netzbetreiber und Telekommunikationsdiensteanbieter festzustellen. Die Betrachtung erfolgte demnach getrennt.

KRITIS-Unternehmen

Da der Referentenentwurf offen lässt, ob alle Unternehmen der jeweiligen KRITIS-Sektoren von den vorgesehenen Regelungen betroffen sind oder diese nur für einen bestimmten, sich z.B. durch besondere Kritikalität auszeichnenden Teil der Unternehmen gelten, ist eine Abschätzung der durch den Referentenentwurf betroffenen Unternehmen nur eingeschränkt möglich.

Um dennoch eine Abschätzung der möglichen quantitativen Effekte des IT-Sicherheitsgesetzes durchführen zu können, soll an dieser Stelle noch einmal die KRITIS-Definition der KRITIS-Strategie angeführt werden, der zufolge es sich bei KRITIS um „Organisationen und Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen [handelt], bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden".[123]

Auf Grundlage der in dieser Definition formulierten Anforderungen („erhebliche Störungen", „dramatische Folgen") erscheint es unwahrscheinlich, dass sämtliche Unternehmen der im Entwurf aufgeführten KRITIS-Sektoren unter die geplanten Regelungen fallen werden. Stattdessen ist davon auszugehen, dass lediglich Unternehmen besonderer Kritikalität betroffen sein werden.

Eine genaue Definition der betroffenen Unternehmen wird im Referentenentwurf nicht vorgenommen und kann daraus auch nicht abgeleitet werden. Im Sinne der Studie werden aus diesem Grund die im Folgenden erläuterten Annahmen getroffen. Diese Annahmen dienen als erste indikative Annäherung an die Zahl betroffener Unternehmen.

Für die Berechnung wird daher angenommen, dass diese besondere Kritikalität vor allem den Großunternehmen der jeweiligen unter KRITIS definierten Branchen zugewiesen werden kann. Als Großunternehmen gelten dabei gemäß Definition der Europäischen Kommission Betriebe mit mindestens 249 Mitarbeitern oder einem jährlichen Umsatz, der 50 Mio. € übersteigt.[124] Großunternehmen, so die Annahme, besitzen aufgrund ihrer Unternehmensgröße über eine tendenziell hohe strukturelle Reichweite (Kunden, Netze, Infrastrukturen, etc.), weshalb Störungen und Beeinträchtigungen ihrer Dienste besonders schwere Auswirkungen auf Wirtschaft und Gesellschaft hätten.

Auch wenn vermutet werden kann, dass sich in der Gruppe der Großunternehmen Unternehmen befinden, die als nicht „kritisch" eingeschätzt werde können, und in einzelnen KRITIS-Sektoren ggf. auch einzelne kleine und mittelständische Unternehmen eine besondere Kritikalität aufweisen können, folgen die zugrunde liegende Arbeitsannahmen einer pragmatischen und plausiblen Auslegung der KRITIS-Definition.

Die folgende Tabelle zeigt die Anzahl der in den einzelnen KRITIS-Sektoren zu verzeichnenden Großunternehmen. Hierfür wurden insbesondere Daten des Statistischen Bundesamtes aus dem Jahr 2011 herangezogen, da diese vollständig vorliegen. Teilweise basieren die Daten auf eigenen Berechnungen, die dem Schnitt der Sektoren, wie vom BBK und BSI definiert, best-

[123] Bundesministerium des Innern 2005, S. 4
[124] Die Zuordnung basiert auf der vom Statistischen Bundesamt verwendeten Methodik der Umsatz- und Beschäftigtengrößenklassen der Kommission der Europäischen Gemeinschaften.

möglich entsprechen. Für diese Studie ergibt sich damit eine Gesamtzahl von **18.466 Großunternehmen in den KRITIS-Sektoren**.

KRITIS-Sektor	Anzahl Großunternehmen
Energie	13.811
Gesundheit	1.108
Wasser	44
Ernährung	448
Transport und Verkehr	1.359
Finanz- und Versicherungswesen	780
Informationstechnik und Telekommunikation	916
Gesamtzahl	**18.466**

Tabelle 4: Anzahl Großunternehmen KRITIS-Sektoren

Die dargestellte Herangehensweise verdeutlicht, dass eine intensive Auseinandersetzung mit den einzelnen Branchen notwendig ist, um eine klare Definition der Kriterien, nach denen Unternehmen von dem IT-Sicherheitsgesetz betroffen sind, zu erarbeiten. Diese eindeutige Definition ist die Voraussetzung für eine konkrete Erfassung der betroffenen Unternehmen und damit für eine präzisere Abschätzung der Gesetzesfolgen.

Telekommunikationsdiensteanbieter und Netzbetreiber

Die Ausweitung der Meldepflichten für Telekommunikationsdiensteanbieter und Netzbetreiber sieht keine Eingrenzung auf KRITIS-Unternehmen vor. Betroffene Unternehmen sind laut Telekommunikationsgesetz alle Unternehmen, die öffentliche Telekommunikationsdienste erbringen.[125] Im selben Gesetz sind Telekommunikationsdienste wie folgt definiert:

> *„in der Regel gegen Entgelt erbrachte Dienste, die ganz oder überwiegend in der Übertragung von Signalen über Telekommunikationsnetze bestehen, einschließlich Übertragungsdienste in Rundfunknetzen.“*[126]

Das Statistische Bundesamt versteht unter Telekommunikationsdienstleistungen deckungsgleich die „Übertragung von Sprache, Daten, Text, Ton und Bild und alle […] damit verbundenen Dienstleistungen“.[127] Davon ausgehend zählt es in Deutschland 2.167 Telekommunikationsdienstleister.[128]

Auf Basis der hier ermittelten Unternehmenszahlen können die Bürokratiekosten für die Wirtschaft berechnet werden. Das Ergebnis der Kalkulation hängt in großem Maße von der Anzahl der hier inkludierten Organisationen ab.

ANWENDUNG DES STANDARDKOSTENMODELLS

Für jede der drei in Kapitel 3 vorgestellten Meldepflichten werden die potentiell entstehenden Kosten im Folgenden separat in Anlehnung an das SKM berechnet. Für einige der Berechnungen müssen an unterschiedlichen Stellen Annahmen getroffen werden. Diese werden an entsprechender Stelle deutlich gemacht.

Neueinführung einer Meldung von KRITIS-Betreibern an das BSI

Die Befragung der KRITIS-Betreiber ergab, dass alle der oben aufgeführten 14 Standardaktivitäten für die Meldung eines IT-Sicherheitsvorfalls an das BSI ausgeführt werden müssen. Nach

[125] Bundesministerium für Verkehr und digitale Infrastruktur § 109a
[126] Bundesministerium für Verkehr und digitale Infrastruktur § 3
[127] Statistisches Bundesamt (2013d), S. 2
[128] BITKOM 2014b

Anwendung der SKM-Zeitwerttabelle ergibt sich nach Einschätzung der befragten Unternehmen ein Zeitaufwand von insgesamt 11 Stunden pro Meldung.

Die Arbeitgeberkosten für die meldende Person pro Stunde sind wie oben erläutert auf 60 Euro festgelegt worden. Daraus ergeben sich **Kosten von etwa 660 Euro pro Meldung für die Unternehmen**.

Die Schätzung der anfallenden Meldungen hängt stark von der genauen Ausgestaltung der Meldepflicht hinsichtlich der zu meldenden Tatbestände ab. Laut Referentenentwurf müssen alle Vorfälle, die Auswirkungen auf die Funktionsfähigkeit der Unternehmen haben können, gemeldet werden. Das schließt selbst die Fälle ein, die im Endeffekt die Funktionsfähigkeit der von ihnen betriebenen kritischen Infrastrukturen nicht beeinflussen. Die Definition der zu meldenden Tatbestände bleibt dabei offen. Die Befragungen der Unternehmen ergaben, dass täglich teilweise hunderte Angriffe auf ihre Systeme eingehen, diese jedoch weder zielgerichtet noch schwerwiegend sind und i.d.R. erfolgreich abgefangen werden können. Sollten diese Angriffe unter die Meldepflicht fallen, so muss von einer Vielzahl von Meldungen pro Tag je Unternehmen ausgegangen werden.

Obwohl der Großteil der befragten Unternehmen keine größeren oder zielgerichteten Angriffe festgestellt hat, ist es in Folge von IT-Angriffen vereinzelt zu Produktionsverzögerungen z.B. in der Datenübertragung gekommen. Die Spanne für die Anzahl der zu leistenden Meldungen pro Jahr ist demnach sehr groß.

Für die Berechnung der Bürokratiekosten wurde von einem Durchschnittswert von einer Meldung pro Woche ausgegangen, dies bedeutet etwa **50 Meldungen pro Jahr pro Unternehmen**. Die Annahme beruht auf einer pragmatischen Schätzung, die aus der Beobachtung und Befragung der für die Behandlung von IT-Sicherheitsvorfällen eingesetzten Spezialisten basiert. Davon ausgehend, ist eine Schätzung von ungefähr einer Meldung pro Woche als realistische Basis anzunehmen. Die tatsächliche Anzahl der notwendigen Meldungen wird je nach konkreter Ausgestaltung der Meldepflicht niedriger oder deutlich höher ausfallen.

Auf Grundlage der weiter oben ermittelten **18.466 Unternehmen**, die von der Meldepflicht betroffen sind, ergibt sich eine **Anzahl von 923.300 durchzuführenden Meldungen pro Jahr.**

Werden die Kosten pro Meldung mit der Anzahl der zu erwartenden Meldungen multipliziert, ergeben sich für diese Meldepflicht zu erwartende **Bürokratiekosten von ca. 600 Millionen Euro**.

Abbildung 2: Bürokratiekosten Meldepflicht KRITIS-Betreiber an BSI

Ausweitung der Meldung von Telekommunikationsdiensteanbietern und Netzbetreibern an die BNetzA

Für die Ausweitung der Meldepflicht der Telekommunikationsdiensteanbieter und Netzbetreiber gelten ähnliche Meldevorgänge, weshalb der Aufwand pro Meldung dem der Meldung der KRITIS-Betreiber entspricht. Ebenso ergaben die Befragungen, dass der Meldevorgang größtenteils von ausgebildeten Informatikern durchgeführt werden muss. Somit können die **Kosten pro Meldung im Schnitt ebenfalls 660 Euro** abgeschätzt werden.

Meldungen an die BNetzA müssen laut Referentenentwurf dann erfolgen, sobald Beeinträchtigungen von TK-Netzen und -diensten vorliegen, die zu einer Störung der Verfügbarkeit der erbrachten Dienste oder zu einem unerlaubten Zugriff auf TK- und Datenverarbeitungssystemen der Nutzer oder Teilnehmer führen können. Die erneute „Kann-Regelung" lässt keine eindeutige Abschätzung der erwarteten Meldungen zu. Die Befragung der TK-Diensteanbieter ergab, dass die Meldung an die BNetzA häufiger stattfinden würde als die Meldung an das BSI, da TK-Diensteanbieter und Netzbetreiber häufiger Ziel eines Angriffes sind als KRITIS-Betreiber. In der folgenden Berechnung wird von einer Meldung pro Arbeitstag ausgegangen, also **250 Meldungen pro Jahr pro Unternehmen.** Diese Schätzung beruht darauf, dass ein TK-Diensteanbieter oft im Fokus von Angreifern stehen, da darüber die eigentlichen Angriffsziele leichter erreichbar sind. Durch die Bündelung mehrerer möglicher Angriffsziele bei den Kunden der TK-Diensteanbieter ist die Anwendung des Faktors 5 auf die Meldungen der Unternehmen hier vertretbar. Multipliziert mit der Zahl der **2.167 Telekommunikationsdienstleister und Netzbetreiber** ergeben sich damit **541.750 Meldungen pro Jahr.**

Die Bürokratiekosten dieser Meldepflicht betragen nach dieser Abschätzung **ca. 350 Millionen Euro im Jahr.**

Abbildung 3: Bürokratiekosten für TK-Meldepflicht an BNetzA

Ausweitung der Meldung von TK-Diensteanbietern und Netzbetreibern an die Nutzer von Telekommunikationsdiensten

Eine Meldung der Telekommunikationsdienstanbieter und Netzbetreiber an ihre Nutzer muss erfolgen, sobald Störungen bekannt werden, die von Datenverarbeitungssystemen der Nutzer ausgehen. Die Befragung der Netzbetreiber ergab, dass 13 der 14 Standardaktivitäten für eine solche Meldung an ihre Nutzer notwendig sind, da die weitere Informationsbeschaffung im Falle von Schwierigkeiten mit den zuständigen Behörden entfällt. Die Unternehmen schätzten den zeitlichen Aufwand jedoch mit **3 Stunden pro Meldung** geringer ein, da die Meldeinhalte weniger komplex sind. Anhand des bereits bei den anderen beiden Meldepflichten verwendeten Kostensatzes für Informatiker ergeben sich **Kosten von etwa 180 Euro pro Meldung**.

Diese Meldepflicht gilt, genau wie die Meldepflicht an die BNetzA, für alle 2.167 Telekommunikationsdienstanbieter und Netzbetreiber. Die Unternehmen konnten keine exakte Aussage zu der Anzahl der zu meldenden Störungen treffen. Ein Problem bei der Ermittlung dieser Zahl besteht darin, dass die Unternehmen, wie in Kapitel 3 erläutert, nicht zwingend in einem vertraglichen Verhältnis zu ihren Nutzern stehen müssen.

Die Befragung ergab, dass durchschnittlich pro 130 Nutzern eine Meldung im Jahr durchgeführt werden muss. Die in dieser Studie geschätzte Nutzerzahl wird über die Teilnehmerzahl ermittelt. Diese liegen vermutlich unter den tatsächlichen Nutzerzahlen liegen. Da lediglich Teilneh-

merzahlen der vier größten Netzbetreiber vorliegen, wurden nur diese und nicht die Zahlen aller 2.167 Unternehmen in die Rechnung einbezogen.

Die führenden Netzbetreiber Deutschlands geben quartalsweise ihre Nutzerzahlen für Mobiltelefonie bekannt und zählten im vierten Quartal 2013 gemeinsam **115.225.000 Mobilfunkteilnehmer**.[129] Zusammen mit der ermittelten durchschnittlichen Meldehäufigkeit und den Teilnehmerzahlen ergibt sich daraus eine Fallzahl von durchschnittlich **886.154 Meldungen pro Jahr insgesamt** allein für Mobilfunkdienste. Die Teilnehmerzahl inkl. Festnetztelefonie und ISP ist vermutlich deutlich noch höher, dazu liegen jedoch keine Daten vor. Dementsprechend betragen die erwarteten Bürokratiekosten dieser Meldepflicht **ca. 150 Millionen Euro.**

Abbildung 4: Bürokratiekosten für TK-Meldepflicht an Nutzer

Gesamtbürokratiekosten

Entsprechend der oben dargelegten Berechnungen ergeben sich durch die drei geplanten Meldepflichten **Gesamtbürokratiekosten in Höhe von ca. 1,1 Milliarde Euro.** Dieser Wert ist als Schätzung zu verstehen. Deutlich wird, dass Bürokratiekosten entstehen und diese nicht unerheblich sein werden.

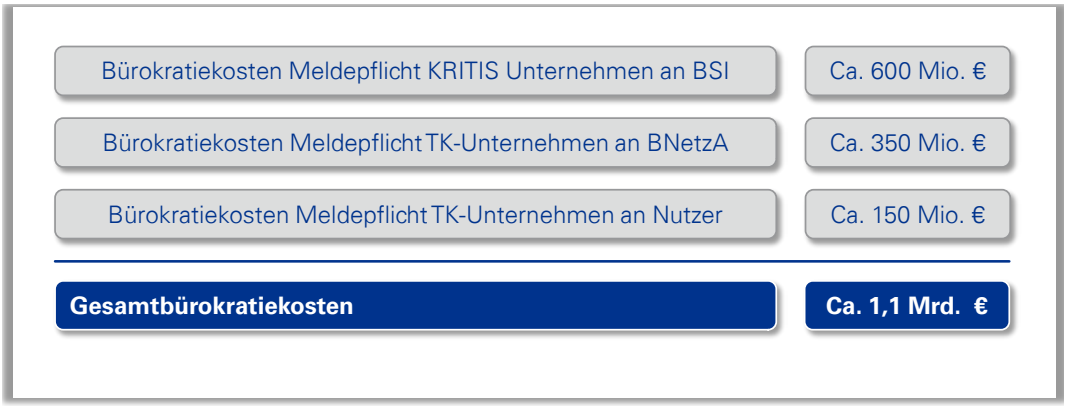

Abbildung 5: Bürokratiekosten gesamt

[129] Bundesnetzagentur 2014

4.2 Weitere Kosten des IT-Sicherheitsgesetzes

Bürokratiekosten stellen allerdings nur einen Kostenpunkt dar. Daneben gibt es noch verschiedene andere Kosten, die im Falle der Umsetzung des Referentenentwurfs auf die betroffenen Unternehmen zukommen könnten.

PERSONALKOSTEN

Wie die Befragung gezeigt hat, rechnen die Unternehmen durch die Umsetzung der Meldepflicht vor allem mit einem erhöhten Personalaufwand. Im Rahmen der Bürokratiekostenschätzung wurden Personalkosten bereits anteilig berücksichtigt. In der SKM-Rechnung wurde vom Qualifikationsniveau eines ausgebildeten Informatikers ausgegangen und die Bürokratiekosten wurden mit dem entsprechenden Kostensatz berechnet. Die Befragung der Unternehmen ergab jedoch, dass je nach Ausgestaltung der konkreten Anforderungen möglicherweise auch Juristen diese Aufgaben übernehmen müssten. In diesem Falle würde der Kostensatz deutlich höher ausfallen und somit auch die Personalkosten.

Weitere Personalkosten können durch die Einrichtung der im Referentenentwurf geforderten 15 Warn- und Alarmierungskontakte[130] pro Unternehmen entstehen, über die die Unternehmen eine jederzeitige Erreichbarkeit gewährleistet müssen.[131] Eine solche Erreichbarkeit lässt sich für Unternehmen nur durch die Einrichtung eines Schichtbetriebs sowie von Bereitschafts-, Wochenend- und Feiertagsdiensten sicherstellen. Diese Dienste sind mit Zusatzvergütungen für Arbeitnehmer und somit mit Zusatzkosten für die Arbeitgeber verbunden.

IT-INFRASTRUKTURKOSTEN

Auch die IT-Infrastruktur selbst muss nach Meinung der befragten Betreiber kritischer Infrastrukturen ggf. angepasst werden. Diese Anpassungen beziehen sich sowohl auf die Meldepflicht als auch auf Mindestsicherheitsstandards.

Bei der Meldepflicht geht es nicht nur um den sicheren Versand der Daten an das BSI und die dafür ggf. notwendige Hard- und Software, sondern auch um den Aufbau analytischer Kapazitäten. Sollten z.B. analog zur Meldung an die BNetzA genaue Nutzerzahlen oder eine regionale Eingrenzung gefordert sein, wären signifikante Anpassungen der Prozesse bei vielen Unternehmen notwendig.

Besonders könnte dies die TK-Dienstleister/Netzbetreiber treffen, da die Meldepflicht an die Kunden komplexe analytische Fähigkeiten (z.B. Identifikation einzelner Nutzer) voraussetzt.

Viele der befragten Unternehmen haben ihre Sicherheitsumgebungen auf das Erkennen und Abwehren von Angriffen ausgerichtet. Die darunterliegenden organisatorischen Prozesse sind nicht für eine strukturierte Weiterleitung der Meldung an eine Behörde ausgelegt. Hier bedarf es sowohl technischer, personeller und organisatorischer Anpassungen der Betriebsmodelle dieser Sicherheitsumgebungen. Diese Problematik ist auch für ausgelagerte Dienstleistungen vorhanden, da die Meldepflicht beim auslagernden Unternehmen liegt und nicht bei dem jeweils beauftragten Dienstleister.

KOSTENRISIKEN DURCH REPUTATIONSSCHÄDEN

Weitere finanzielle Belastungen könnten Unternehmen durch Reputationsschäden entstehen. Reputation kann definiert werden als das „auf Erfahrungen gestützte Ansehen und ggf. auch Vertrauen, das ein Individuum oder eine Organisation bei anderen Akteuren“[132] besitzt. Für Unternehmen bedeutet dies, dass Reputation von besonderer Bedeutung z.B. für die Herstellung von Vertrauen zu Kunden und Investoren ist. Wie auch in den Interviews deutlich wurde, stellt Reputation eine wertvolle Ressource für die Unternehmen dar.

Geht Reputation verloren, etwa durch Bekanntwerden der Folgen eines IT-Sicherheitsvorfalles, kann sich dies u.a. in einem Rückgang von Kundenzahlen, Umsatzeinbußen oder einem veränderten Investorenverhalten ausdrücken und damit auch finanziell spürbar werden. Auch wenn

[130] Bundesministerium des Innern 2013a, S. 9
[131] Bundesministerium des Innern 2013a, S. 9
[132] Springer Gabler Verlag

ein solcher Mechanismus nicht in jedem Fall erfolgen muss, verdeutlichen verschiedene Beispiele die mögliche Tragweite von Reputationsschäden: Nachdem der etwa eine US-amerikanische Einzelhandelskette im Dezember 2013 einen Datenverlust von über 40 Millionen Kundendaten bekanntgab, verzeichnete er im ersten Quartal 2014 ein Umsatzeinbruch von 16%.[133] Zeitgleich ging das Kundengeschäft um 5,5% zurück.[134] Im Mai diesen Jahren wurde ein Diebstahl von Kundeninformationen bei einem Internetmarktplatz bekannt, in dessen Folge der Aktienkurs absackte.[135]

Obgleich der vorliegende Referentenentwurf nicht auf den Begriff der Reputation verweist, lassen sich einige Inhalte bzw. Elemente identifizieren, die unter Umständen die Reputation der betroffenen Unternehmen berühren können. Dies gilt insbesondere für die geplante Meldepflicht und die damit verbundene Möglichkeit der Weitergabe bzw. Veröffentlichung von IT-Sicherheitsvorfällen.

Laut Referentenentwurf wird die vorgesehene Meldepflicht offen, also mit Nennung der Identität des meldenden Unternehmens, durchgeführt. Vor dem Hintergrund des Risikos möglicher Reputationsschäden für die Unternehmen durch das öffentliche Bekanntwerden eines IT-Sicherheitsvorfalls kann eine offene Meldung aus Unternehmenssicht durchaus als kritisch beurteilt werden. Es besteht die Gefahr, dass erst durch das Bekanntwerden einer entsprechenden Meldung der Schaden eintritt.

Eine mögliche Alternative wäre es, die Meldepflicht so zu gestalten, dass das Risiko eines Reputationsschadens für die Unternehmen gesenkt wird, die Erstellung eines Lagebilds durch das BSI aber dennoch uneingeschränkt gewährleistet wird.

Gleichzeitig sollte transparent gemacht werden, wie die gemeldeten Daten im Nachgang genutzt bzw. ob, und wenn ja unter welchen Auflagen sie ggf. weitergegeben werden.

KOSTEN DURCH IT-MINDESTSICHERHEITSSTANDARDS

Wie die Befragung zeigte, rechnen die Unternehmen mehrheitlich mit einem monetären Mehraufwand durch die Einführung gesetzlicher IT-Mindestsicherheits-standards. Dabei wurden mehrheitlich zwei Kostentreiber genannt: Zum einen gaben die Unternehmen an, die eigenen Standards an die neuen Vorgaben anpassen zu müssen – auch dann, wenn bereits hohe eigene Sicherheitsstandards implementiert wären. Zum anderen wiesen vor allem die international tätigen Unternehmen darauf hin, dass die Einführung nationaler Standards zu erhöhten unternehmensinternen Kosten führen können, um die eigenen, internationalen IT-Sicherheitsstruktur zu harmonisieren. Auf Grundlage des vorliegenden Referentenentwurfs lassen sich diese Kostenrisiken augenblicklich jedoch nicht quantifizieren.

In einer Gesamtschau sollte allerdings auch darauf hingewiesen werden, dass die Einführung der Mindeststandards für IT-Sicherheit für eine Reihe von Unternehmen, namentlich Zulieferern und Dienstleistern von IT-Sicherheit, auch Wertschöpfungspotentiale bietet. Damit eröffnet der Referentenentwurf möglichen Raum zur Verbesserung der Kompetenzen im IT-Sicherheitsbereich in Deutschland.

[133] USA Today
[134] Quartz
[135] Die Welt 2014

KAPITEL 5

Zusammenfassung, Handlungsempfehlungen und Alternativen

5.1 Zusammenfassung

IT-Sicherheit ist sowohl für die öffentliche Hand als auch für die Unternehmen in Deutschland ein Thema von besonderer Bedeutung und Tragweite. Beide Bereiche haben in den letzten Jahren mit zahlreichen, auch gemeinsamen Initiativen dazu beigetragen, die öffentliche Sensibilität für dieses Thema zu erhöhen und die IT-Sicherheitslage zu verbessern.

Mit dem Referentenentwurf eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme liegt aktuell ein vom BMI vorgestellter Maßnahmenkatalog vor, mit dem das BMI als federführendes Ressort das Ziel einer Verbesserung der IT-Sicherheit in Deutschland verfolgt. Die vorliegende Studie hat sich in ihrer Analyse auf zwei wesentliche Elemente des Referentenentwurfs konzentriert: Die Pflicht zur Meldung von IT-Sicherheitsvorfällen durch Betreiber kritischer Infrastrukturen und Telekommunikationsanbieter sowie die Einführung von IT-Mindestsicherheitsstandards.

Im Rahmen der Studie wurde eine Analyse des Referentenentwurfs vorgenommen, die folgende Elemente enthält:

- Eine inhaltliche **Analyse des vorliegenden Referentenentwurfs** in Bezug auf Stärken und Schwächen

- Eine **Befragung der potentiell vom Referentenentwurf betroffenen Unternehmen** in Bezug auf die IT-Sicherheit im allgemeinen und möglichen Folgen einer Umsetzung des bestehenden Referentenentwurfs

- Eine indikative **Bürokratiekostenschätzung** in Bezug auf den vorliegenden Entwurf, die angelehnt an die SKM-Methode mögliche Kosten, die durch den Referentenentwurf entstehen, schätzt

Die Analyse zeigt, dass im Referentenentwurf in der aktuellen Form noch Interpretationsspielräume bezüglich der betroffenen Unternehmen und relevanten Sicherheitsvorfälle erkennbar sind. Die im Rahmen der Studie durchgeführte Befragung sowie die Bürokratiekostenschätzung zeigen darüber hinaus, dass das Gesetz potentiell zu einer hohen finanziellen und organisationalen Belastung von Unternehmen führen kann.

Hinsichtlich der Meldepflichten lassen sich u.a. folgende Beobachtungen festmachen:

- Sie sind aktuell so formuliert, dass unklar bleibt, welche Unternehmen melden und welche Tatbestände gemeldet werden müssen.

- Neben den direkt durch die Meldepflicht verursachten Bürokratiekosten von etwa 1,1 Mrd. Euro entstehen für die Unternehmen möglicherweise weitere mittelbare Kosten. Diese schließen Personal- und Infrastrukturaufwände ein, zudem können mögliche Reputationsschäden finanzielle Belastungen für die Unternehmen verursachen.

- Aktuell bleibt unklar ob bzw. wie die Unternehmen an dem sich aus den Meldungen ergebenden Erkenntnisgewinn bzgl. des Lagebildes partizipieren können.

- Da es sich bei KRITIS-Betreibern und Telekommunikationsdiensteanbietern um bereits regulierte Unternehmen handelt, ist eine Doppel- bzw. Mehrfachregulierung zu vermeiden.

Die Einführung von Mindeststandards stößt bei den befragten Unternehmen grundsätzlich auf Akzeptanz. Allerdings ist der mit ihrer Implementierung verbundene Aufwand spürbar. Hier sollte daher auf Flexibilität und bereits funktionierende privatwirtschaftliche Regelungen geachtet werden.

Auf Basis der in dieser Studie durchgeführten Analyse werden im folgenden Abschnitt Empfehlungen und mögliche Alternativen zum Referentenentwurf aufgeführt.

5.2 Empfehlungen und Alternativen

Zu den wesentlichen Zielen der vorliegenden Studie zählt die Identifizierung von Empfehlungen, die einen konstruktiven, zielorientierten und auch umsetzbaren Beitrag zur Diskussion um die geplante Meldepflicht und die IT-Mindestsicherheitsstandards leisten sollen. Auf Grundlage der Analyse des Referentenentwurfs, der Erkenntnisse aus den Interviews und der Bürokratiekostenschätzung wird im Folgenden eine Auswahl von 12 Empfehlungen vorgestellt, die verschiedene Handlungsfelder adressieren. Zugleich erfüllen sie drei wichtige Kriterien:

1. **Kompatibilität mit dem Ziel einer verbesserten IT-Sicherheit**: Die Empfehlungen richten sich konsequent an dem Ziel eines höheren IT-Sicherheitsniveaus aus. Sie nehmen Bezug zu wesentlichen Elementen des Referentenentwurfs und können dazu beitragen, deren Wirkung weiter zu verstärken.
2. **Umsetzungsfähigkeit:** Die Empfehlungen zeichnen sich durch einen ausbalancierten Ansatz aus, der eine hohe Umsetzbarkeit ermöglicht. Der Umsetzungsaufwand der einzelnen Empfehlungen ist unterschiedlich hoch, ohne dabei jedoch das Inkrafttreten des Gesetzes zu verzögern.
3. **Akzeptanz auf Seiten der Betroffenen**: Die Empfehlungen reflektieren die Anregungen und Diskussionspunkte der interviewten Unternehmen, sodass eine hohe Akzeptanz durch die betroffenen Unternehmen zu erwarten ist.

Abbildung 6 gibt einen Überblick über die 12 Empfehlungen, die dort nach übergeordneten Handlungsfeldern strukturiert sind. Nachfolgend werden die einzelnen Empfehlungen näher beschrieben.

Abbildung 6: Überblick Empfehlungen

EMPFEHLUNGEN ZUM HANDLUNGSFELD MELDEPFLICHT

1. Definition der Tatbestände

Wie in Kapitel 3 dargestellt ist der Referentenentwurf vom 12. März 2013 dahingehend zu präzisieren, welche IT-Sicherheitsvorfälle konkret gemeldet werden müssen. Auch aus Sicht der befragten Unternehmen stellt dies eine besondere Schwäche des vorliegenden Referentenentwurfs dar. Angesichts der enormen Bandbreite der IT-Sicherheitsvorfälle, denen sich Unternehmen ausgesetzt sehen könnten, und im Hinblick auf das damit potentiell verbundene hohe Meldeaufkommen erscheint eine genaue Definition der meldepflichtigen IT-Sicherheitsvorfälle erforderlich. Zugleich könnte der unternehmensseitig entstehende Aufwand präziser eingeschätzt werden.

Im Rahmen der Abgrenzung, welche IT-Sicherheitsvorfälle zu melden sind, sollten sinnvollerweise auch damit eng verknüpfte Fragestellungen adäquat beantwortet werden. Dies betrifft sowohl die Frage nach dem genauen Meldeweg, der für die Übermittlung vorgesehen ist, als auch die Frage nach der Qualität und Detailtiefe der abzugebenden Meldung. Schließlich ist hier auch der Zeitraum zu definieren, innerhalb dessen die Behörden über die entsprechenden IT-Sicherheitsvorfälle informiert werden sollen. Dieser sollte den Umfang und die Dauer unternehmensinterner Prozesse berücksichtigen und zu enge zeitliche Vorgaben vermeiden. Schließlich sollte auch diskutiert werden, welchen Aufwand Unternehmen zu leisten haben, um IT-Sicherheitsvorfälle zu erkennen.

2. Definition der meldepflichtigen Unternehmen

Wie in Kapitel 4 dargestellt ist aktuell noch unklar, welche Unternehmen als kritische Infrastruktur verstanden werden und damit von der Meldepflicht und den IT-Mindestsicherheitsstandards betroffen sein könnten. Angesichts des mit der Implementierung beider Vorgaben verbundenen Aufwands, der für die betroffenen Unternehmen insbesondere durch Personalkosten oder Umstellungen interner Prozesse entsteht, erscheint eine klare Eingrenzung der aktuellen Schwankungsbreite geboten. Zugleich würde die unternehmerische Planungs- und Rechtssicherheit verbessert.

3. Pseudonymisierung der Meldpflicht via Treuhänder

In ihrer bisher geplanten Ausgestaltung sieht die Meldepflicht eine Übermittlung der Meldungen unter Offenlegung der Identität des jeweils meldenden Unternehmens vor. Insbesondere angesichts des Risikos möglicher Reputationsschäden wird dieses Verfahren von den befragten Unternehmen abgelehnt. Demgegenüber steht das behördliche Interesse, durch die Meldepflicht „eine Verbesserung des Lagebildes zur IT-Sicherheit zu erreichen".[136] Die Erstellung und kontinuierliche Pflege eines aktuellen Lagebildes gehört naturgemäß zu den wesentlichen Aufgaben des BSI als zuständige Behörde für die Sicherheit der Informationstechnik in Deutschland. Dies wird auch uneingeschränkt von den befragten Unternehmen anerkannt. Gleichwohl erscheint es zulässig zu hinterfragen, ob die Erstellung eines Lagebildes zwingend einer verpflichtenden Offenlegung der Identität des meldenden Unternehmens bedarf.

Ein Alternativverfahren ist die Einrichtung eines anonymen Meldeprozesses, der von einigen der befragten Unternehmen präferiert wird, und den Behörden die Identität des meldenden Unternehmens nicht anzeigt. Ein solches Verfahren lässt die Erstellung eines Lagebildes weiterhin zu. Gleichzeitig könnte das Risiko möglicher Reputationsschäden minimiert werden. Allerdings ist ein anonymisiertes Verfahren auch mit Herausforderungen verbunden. So würde eine vollständige Anonymisierung die Herstellung eines direkten und bidirektionalen Kommunikationsweges unmöglich machen. Dies wäre insbesondere von Nachteil, wenn das BSI akute Risikowarnungen an den Melder zurückspielen wollte. Eine weitere Herausforderung bestünde darin, dass keine Überprüfung möglich ist, ob die erfolgten Meldungen tatsächlich von einem der Meldepflicht unterliegenden Unternehmen getätigt wurden.

Um die Zielkonflikte abzumildern, wird ein pseudonymisiertes Meldeverfahren empfohlen. Pseudonymisierung kann dabei gemäß der Definition des Bundesdatenschutzgesetzes „als das Ersetzen des Namens und anderer Identifikationsmerkmale durch ein Kennzeichen" verstanden werden, das den Zweck hat „die Bestimmung des Betroffenen auszuschließen oder wesentlich zu erschweren".[137] Anders als im Rahmen einer vollständigen Anonymisierung bliebe der Mel-

[136] Bundesministerium des Innern 2013a, S. 25
[137] Bundesdatenschutzgesetz, § 3 (6a), vgl. Bundesbeauftragter für den Datenschutz und die Informationsfreiheit

dende etwa im Falle eines schwerwiegenden Störungsfalles für die Behörden identifizierbar. Auch bliebe die Möglichkeit, ein die unterschiedlichen Branchen berücksichtigendes Lagebild zu erstellen, uneingeschränkt erhalten. Aber auch das Risiko eines Reputationsschadens für die meldenden Unternehmen würde dabei deutlich reduziert.

Zur effektiven Ausgestaltung eines pseudonymisierten Meldeverfahrens wird empfohlen eine neutrale Stelle – einen unabhängigen Treuhänder – einzurichten, die im Meldeprozess zwischen den die Meldung abgebenden Unternehmen und den die Meldung annehmenden Behörden geschaltet ist. Um eine hohe Akzeptanz für den Treuhänder sicherzustellen, sollte dessen Auswahl im gemeinsamen Dialog aller beteiligten Akteure erfolgen.

Das pseudonymisierte Meldeverfahren könnte wie folgt ausgestaltet werden: Es beginnt mit der verschlüsselten Versendung der Meldung des betroffenen Unternehmens an den Treuhänder. Diesem ist die Identität des Meldenden bekannt, aber durch die Verschlüsselung kann er den Inhalt der Meldung von Dritten nicht einsehen. In einem nächsten Schritt entfernt der Treuhänder die Unternehmensidentität und fügt eine Pseudoidentität etwa im Sinne eines Kennzeichens ein. Danach erfolgt der Versand der weiterhin verschlüsselten Meldung an das BSI, das mithilfe eines entsprechenden Schlüssels Zugriff auf den Meldeinhalt erlangt. Eine potentiell notwendige Kommunikation zwischen den Teilnehmern erfolgt auf dem umgekehrten Wege und damit ebenfalls über den Treuhänder. Der ganze Übermittlungsprozess muss vom Ablauf nachvollziehbar und auch auditierbar sein.

Insgesamt trägt eine pseudonymiserte Meldepflicht den Anliegen der Unternehmen und den Interessen der für IT-Sicherheit in Deutschland verantwortlichen Behörden gleichermaßen Rechnung, ohne dabei die jeweils möglichen Nachteile einer offenen und einer vollständig anonymisierten Meldung zu besitzen. Eine offene Diskussion und Prüfung dieses Verfahren erscheint daher im Sinne der IT-Sicherheit ebenso zielführend wie sachorientiert.

4. Aktive Informationspolitik des BSI

Der Referentenentwurf spricht davon, dass die durch die Meldepflicht beim BSI zusammenlaufenden Informationen dort nicht nur gesammelt und ausgewertet werden. Vielmehr sollen die daraus resultierenden Erkenntnisse den meldenden Unternehmen zur Verfügung gestellt werden.[138] Mit diesem Hinweis spricht der Referentenentwurf ein zentrales Anliegen der im Rahmen dieser Studie befragten Unternehmen an, nämlich die Forderung nach einem aktiven Austausch der sich aus der Meldepflicht amtsseitig ergebenden Informationen und nach Teilhabe an dem dadurch verbesserten Lagebild.

Insbesondere die Angaben der befragten KRITIS-Betreiber machen deutlich, dass ein wesentlicher Mehrwert der Meldepflicht durch einen aktiven, gezielten und schnellen Informationsaustausch zwischen BSI und Unternehmen erzielt werden kann. Durch eine aktive Rolle des BSI könnten vorhandene Austauschplattformen sinnvoll ergänzt und wichtige Informationen etwa zur Bedrohungslage und neuen Angriffsformen zeitnah an die Unternehmen zurückgespielt werden. Die Mehrheit der befragten Unternehmen zeigte ein klares Interesse daran, in einen von beiden Seiten aktiv geführten Dialog mit dem BSI zu treten und das Lagebild zur IT-Sicherheit kooperativ zu verbessern.

Die Informationspolitik des BSI sollte sich nicht auf die Veröffentlichung von Halbjahres- oder Jahresberichten erschöpfen, sondern sollte kontinuierlich und zeitnah erfolgen. Dabei könnten beispielsweise praktische Erfahrungen in der Prävention oder der Abwehr von IT-Sicherheitsvorfällen oder die Aufklärung über neuartige oder besonders entwickelte Angriffsmuster an die Unternehmen kommuniziert werden. Denkbar wären darüber hinaus aber auch die Erstellung und der Austausch branchenspezifischer Lagebilder. Auf diese Weise könnte das BSI zu einer Informationsdrehscheibe werden und seine besondere Rolle für IT-Sicherheit in Deutschland unterstreichen. Internationale Beispiele wie etwa die schweizerische Melde- und Analysestelle Informationssicherung (MELANI) oder das britische Centre for the Protection of National Infrastructure (CPNI) könnten hier als Orientierungspunkte für einen aktiven Austausch zwischen Behörden und Unternehmen dienen.

[138] Bundesministerium des Innern 2013a, S. 2

5. Transparenz bzgl. Nutzung und Verwendung der Meldungen

Die im Rahmen der Meldepflicht von den Unternehmen an die Behörden übermittelten Daten besitzen naturgemäß einen besonders sensiblen Charakter. Die Daten erlauben Rückschlüsse auf Schwachstellen oder Risikobereiche der jeweiligen Unternehmen und bergen daher das Potential, Wettbewerbsnachteile zu generieren und Reputationsschäden zu verursachen. Es überrascht daher nicht, dass die befragten Unternehmen mehrheitlich auf die Notwendigkeit eines vertrauensvollen Umgangs mit den Meldedaten durch Seiten der Behörden verweisen. Zugleich spricht sich eine deutliche Mehrheit der Unternehmen für eine hohe behördenseitige Transparenz bezüglich der Speicherung, Verarbeitung und Weitergabe der Meldungen aus.

Der Referentenentwurf gibt zu diesem für die Unternehmen ausgesprochen bedeutsamen Punkt allerdings keine Auskunft. Umso wichtiger erscheint es, dass BMI und BSI zeitnah deutlich machen, wie die Nutzung und Verwendung der Meldungen konkret ausgestaltet sein wird. Die Relevanz einer solchen Transparenz ist auch vor dem Hintergrund der europäischen Richtlinie zu betonen, die explizit die Möglichkeit eines Austausches der Meldungen innerhalb der zuständigen europäischen Behörden vorsieht.

Um die Akzeptanz der Meldepflicht durch die Unternehmen zu erhöhen und die vertrauensvolle Zusammenarbeit zwischen Behörden und Unternehmen weiter zu stärken, sollten die Speicherung und die Aufbereitung der gemeldeten Daten transparent dargestellt und ihrer Verbreitung enge Grenzen gesetzt werden. Im Falle der Weitergabe an dritte Stellen (national und europäisch) wäre zu dem die Möglichkeit einer Vorabinformation der jeweils betroffenen Unternehmen zu prüfen. Im Sinne eines Qualitätsmanagements wäre zudem ein regelmäßiges und unabhängiges Audit des Verfahrens und des Umganges mit den Meldungen denkbar.

6. Vermeidung von Doppelregulierung

Die Analyse des deutschen Referentenentwurfs und des europäischen Vorschlags einer Richtlinie zur Informationssicherheit offenbart eine unterschiedliche Herangehensweise an die Regulierung von Telekommunikationsdiensteanbietern und Netzbetreibern. Der aktuelle Referentenentwurf sieht wie beschrieben drei Meldepflichten vor, bei denen es sich teilweise um Neueinführungen und teils um Ausweitungen handelt. Für einige Unternehmen aus dem ITK-Sektor gelten alle drei Meldepflichten. Die derzeit nur vage formulierten Definitionen der jeweils zu meldenden Tatbestände sind nicht überschneidungsfrei und könnten deshalb zu vermeidbarem Mehraufwand führen. Insbesondere sind hier die Meldungen von „schweren Beeinträchtigungen“ an das BSI und potentiellen „Störungen“ an die BNetzA gemeint. Nach aktuellem Stand könnten bestimmte Sicherheitsvorfälle eine Meldung an beide Behörden verpflichtend machen. Da die BNetzA eingehende Informationen und Meldungen schon heute an das BSI weiterleitet, wäre hier Mehraufwand ohne erkennbaren Informationsgewinn bei den beteiligten Akteuren die Folge.

Auf europäischer Ebene wird diese Problematik aufgelöst, indem die Anbieter von Kommunikationsdiensten von der neu eingeführten Meldepflicht ausgenommen werden. Diese Regelung schafft Klarheit für die betroffenen Unternehmen und vermeidet Doppelregulierung sowie daraus resultierenden Mehraufwand.

7. Berücksichtigung der Bedeutung von Rechtssicherheit für die meldenden Unternehmen

In den Interviews wurde deutlich, dass in zahlreichen Unternehmen Unsicherheit darüber herrscht, ob, und wenn ja unter welchen Umständen ihnen im Rahmen einer möglichen Meldung Rechtsfolgen drohen könnten. Eine vollumfängliche Bewertung dieser facettenreichen und für die Unternehmen zentralen Frage bedarf einer genauen juristischen Prüfung, die an dieser Stelle allerdings nicht geleistet werden kann. Umso wichtiger erscheint es, dass dieses unternehmerische Anliegen Eingang in die Diskussion findet und im Rahmen des Gesetzgebungsverfahrens adäquat berücksichtigt wird.

EMPFEHLUNGEN ZU IT-MINDESTSICHERHEITSSTANDARDS

8. Unterstützung der branchenorientierten Selbsorganisation von IT-Mindestsicherheitsstandards

Der Referentenentwurf eröffnet den Unternehmen und ihren Branchenverbänden die Möglichkeit, branchenspezifische IT-Mindestsicherheitsstandards zu entwickeln. Diese Regelung zeigt den staatlichen Willen, das in den Unternehmen und Branchen vorhandene Sicherheits-Know-how auszuschöpfen und für die Erhöhung der IT-Sicherheit nutzbar zu machen. Es verwundert

daher auch nicht, dass die branchenorientierte Selbstorganisation von den befragten Unternehmen mehrheitlich als der sachgerechteste Ansatz begrüßt wird.

Die branchenspezifische Selbstorganisation wird durch die Vorgabe begrenzt, dass die von Unternehmen und Branchen entwickelten Standards vor ihrer Implementierung durch das BSI abgenommen werden müssen. Wie dieser Abnahmeprozess ausgestaltet ist, wird im Referentenentwurf nicht weiter dargestellt. Die Einbindung des BSI entspricht der gewachsenen Verantwortung der Behörde – sie sollte jedoch die Branchenexpertise der Unternehmen ausreichend erfassen und berücksichtigen. Gleichzeitig sollte sie ggf. notwendige Anpassungen an den Stand der Technik zeitnah zulassen.

9. Berücksichtigung der internationalen Geschäftstätigkeiten der Unternehmen

Eine große Anzahl der in KRITIS-Sektoren tätigen Unternehmen ist europäisch und auch global tätig. Infolgedessen orientieren sich zahlreiche Unternehmen im Bereich der IT-Sicherheit bzw. der Informationssicherheits-Managementsysteme an internationalen Standards. Dies gilt auch für die in dieser Studie befragten Unternehmen, die sich mehrheitlich an der internationalen Norm ISO 27001 orientieren. Als Gründe hierfür wurden u.a. eine größere, kundenspezifische Flexibilität, die Schaffung unternehmensweiter Synergien und der Vorteil eines einheitlichen und systematischen Risiko-Managements genannt. Vor diesem Hintergrund erscheint es sinnvoll, bei der Entwicklung und der behördenseitigen Anerkennung branchenspezifischer IT-Mindestsicherheitsstandards auf nationale Insellösungen zu verzichten und die internationale Ausrichtung der deutschen Unternehmen zu berücksichtigen. Eine solche Orientierung an internationalen Standards sollte auch dazu führen, dass sich Audits an internationalen Standards orientieren. Die Meldung von Auditberichten an das BSI sollte vor diesem Hintergrund kritisch hinterfragt werden.

10. Berücksichtigung der Rolle der Zulieferer und Ausrüster

Obwohl die Vorgaben des Referentenentwurfs aktuell nicht auf Zulieferer und Ausrüster zielen, ist zu erwarten, dass diese dennoch von der Vorgaben betroffen sein werden – und dies auf unterschiedliche Weise. Während die Gruppe der Zulieferer, die der Wertschöpfungskette vorgelagert sind, mit Kosten rechnen müssen, ergeben sich für Zulieferer und Hersteller von IT-Sicherheit Geschäftspotentiale.

Auf der einen Seite wiesen viele der befragten KRITIS- und TK-Unternehmen darauf hin, das IT-Mindeststandards auch für die gesamte Produktions- und Lieferkette zu gelten hätten. In der Folge unterstrichen einige der Befragten die hohe Wahrscheinlichkeit, ihre Zulieferer und Ausrüster, etwa aus den Bereichen Maschinenbau und Elektroindustrie, auf die Einhaltung etwaiger IT-Mindestsicherheitsstandards zu verpflichten. Im Rahmen der weiteren Ausgestaltung des Referentenentwurfs sollten daher mögliche Abstrahlungs- und Kosteneffekte der gesetzlichen Vorgaben über den Kreis der eigentlich betroffenen Unternehmen hinaus bedacht werden. Dies gilt umso mehr, da aktuell bereits eine Reihe privatwirtschaftlicher Vereinbarungen existieren, die erfolgreich umgesetzt werden, und die beispielsweise Fragen nach unternehmensübergreifender Kompatibilität von Mindeststandards regeln.

Auf der anderen Seite kann die spezifische Ausgestaltung der Standards für Zulieferer und Dienstleister von IT-Sicherheitsleistungen Raum für industrielle Wertschöpfung schaffen. Auch dieser Aspekt sollte im Rahmen der Weiterentwicklung des Referentenentwurfs, etwa durch die Förderung nationaler Kompetenzen bezüglich der IT-Sicherheit im Office- und Produktionsbereich in die Diskussion einfließen.

EMPFEHLUNGEN ZU KOMMUNIKATION UND TRANSPARENZ

11. Kommunikation der Ziele des Gesetzes

Eine transparente Kommunikation ist für jedes Gesetzesvorhaben von hoher Bedeutung, denn sie kann helfen, Vertrauen zu schaffen, Akzeptanz zu erhöhen und die jeweilige Debatte sach- und zielorientiert zu führen. Dies kann angesichts seiner politischen Bedeutung und des absehbaren Implementierungsaufwands auf Seiten der Unternehmen auch für den in dieser Studie beleuchteten Referentenentwurf gelten.

Wie die durchgeführten Interviews ergaben, fühlt sich die Mehrheit der befragten Unternehmen nicht ausreichend und transparent über die Ziele des Referentenentwurfs und insbesondere der Meldepflicht informiert. Dies betrifft sowohl die übergeordneten politisch-strategischen Leitli-

nien als auch die konkreten Ziele sowie Fragen nach der genauen inhaltlichen Ausgestaltung des Referentenentwurfs.

Die bevorstehende Einbringung des Referentenentwurfs in das parlamentarische Verfahren stellt einen geeigneten Augenblick dar, um die Ziele und die dem Referentenentwurf zugrunde liegenden Überlegungen und Annahmen insbesondere gegenüber den Unternehmen und Branchen zu kommunizieren und weiter zu verdeutlichen.

12. Fortführung des konstruktiven Dialogs zwischen Industrie, Verwaltung und Politik

IT-Sicherheit wird für die Unternehmen und die öffentliche Hand auch in den kommenden Jahren ein zentrales Thema darstellen. Wie im zweiten Kapitel aufgezeigt, existieren zahlreiche Austauschformate zwischen Unternehmen und staatlichen Stellen. Ergänzend gibt es unterschiedlichste Kontakte zwischen den Branchenvertretern und der administrativen Fachebene. Damit existiert bereits heute eine feste institutionelle Basis, auf der der Dialog und die Zusammenarbeit vertrauensvoll weitergeführt und weiter ausgebaut werden sollte.

ANHANG

Unternehmen KRITIS-Sektoren

In diesem Kapitel werden die vom IT-Sicherheitsgesetz betroffenen sieben KRITIS-Sektoren im Überblick vorgestellt und deren zugehörige Branchen aufgeführt. Anhand von Daten des Statistischen Bundesamtes werden die Sektoren zunächst mittels folgender Kennzahlen quantitativ erfasst:

- Anzahl der Unternehmen
- Anzahl der beschäftigten Mitarbeiter
- Umsatz

Mithilfe der Umsatz- und Beschäftigtengrößenklassen nach Empfehlung der Europäischen Kommission (2003/361/EG) und Erhebungen des Statistischen Bundesamtes wird anschließend der Anteil der Großunternehmen mit mehr als 249 Beschäftigten oder mehr als 50 Mio. Euro Jahresumsatz ermittelt. Dies bildet die Grundlage für die in Kapitel 4 durchgeführten Berechnungen.

ENERGIE

Energie ist eines der bedeutendsten Güter für das Funktionieren einer modernen Volkswirtschaft. Der Sektor ist von großer Bedeutung für das Funktionieren nahezu aller Prozesse und Aufgaben, die in Unternehmen, staatlichen Institutionen und privaten Haushalten ausgeführt werden. Störungen oder ein Ausfall der Energieversorgung haben weitreichende und direkte Folgen für das Wohlergehen der Bevölkerung. Dies würde insbesondere auch Auswirkungen auf andere kritische Infrastrukturen haben, da diese auf eine stabile Versorgung mit Energie angewiesen sind. Im Falle einer Beeinträchtigung könnte z.B. die Funktionalität des Transportsektors beeinträchtigt sein oder die medizinische Versorgung in Krankenhäusern nicht mehr gewährleistet werden.[139]

Der Sektor „Energie“ umfasst nach der Definition des BBK und BSI folgende Bereiche[140]:

- Elektrizität
- Gas
- Mineralöl

Dem Statistischen Bundesamt zufolge gibt es 48.292 Unternehmen in Deutschland, die der Energiebranche zugerechnet werden, wenngleich dies nur die Bereiche Elektrizität und Gas umfasst.[141] Diese beschäftigen insgesamt 247.291 sozialversicherungspflichtige Mitarbeiter und erwirtschafteten 2011 einen Umsatz von rund 494 Mrd. €.[142]Der Sektor Energie ist im Vergleich zu den übrigen Sektoren und im Vergleich zum gesamtdeutschen Durchschnitt in besonderem Maße von Großunternehmen geprägt. Diese machen 28,6% aller Energieunternehmen aus. Für das in dieser Studie verwendete Szenario wären dementsprechend **13.811 Unternehmen des Energiesektors vom Referentenentwurf betroffen**. Diese beschäftigen 215.637 Mitarbeiter und generieren 477 Mrd. Euro Umsatz, rund 97% des gesamten Branchenumsatzes.[143]

GESUNDHEIT

Gesundheit ist ein zentrales Gut, das in der Bundesrepublik Deutschland auf hohem Niveau gewährleistet wird. Die Versorgung der Bürger mit Dienstleistungen der Gesundheitswirtschaft ist für das Wohl der Bevölkerung von besonderer Bedeutung und kann in Krisen umso wichtiger

[139] Bundesamt für Bevölkerungsschutz und Katastrophenhilfe und Bundesamt für Sicherheit in der Informationstechnik o. J.a
[140] Bundesamt für Bevölkerungsschutz und Katastrophenhilfe und Bundesamt für Sicherheit in der Informationstechnik o. J.a
[141] Für den Bereich „Mineralöl“ liegen keine Daten vor.
[142] Statistisches Bundesamt 2011
[143] Statistisches Bundesamt o. J.a

sein. Ein Ausfall kann direkte Konsequenzen für die Bürger haben und das Wohl der Bevölkerung erheblich beeinträchtigen.

Der Sektor „Gesundheit" umfasst nach der Definition des BBK und BSI folgende Bereiche:[144]

- Medizinische Versorgung
- Arzneimittel und Impfstoffe
- Labore

Das Statistische Bundesamt zählt 196.129 Unternehmen im Gesundheitswesen, die insgesamt 2.051.355 sozialversicherungspflichtige Mitarbeiter beschäftigen; der Umsatz der Branche beläuft sich auf über 38 Mrd. €.[145]

Wie in vielen anderen Wirtschaftsbereichen ist auch die deutsche Gesundheitswirtschaft insgesamt stark mittelständisch geprägt.[146]Laut den Annahmen des in dieser Studie verwendeten Szenarios wären **1.108 Unternehmen aus dem Gesundheitssektor von dem Referentenentwurf betroffen**, das entspricht dem Anteil von rund 0,5% an Großunternehmen im Sektor. Diese beschäftigen zusammen rund 1,1 Mio. Mitarbeiter und erwirtschaften rund 23,7 Mrd. € Umsatz.[147]

WASSER

Der Zugang zu Wasser ist von essentieller Bedeutung für das menschliche Leben. Die Wasserversorgung erfolgt in Deutschland auf der Grundlage von hohen Standards, die rechtlich verbindlich festgeschrieben sind und deren Einhaltung regelmäßig überwacht wird. Diese garantieren eine zuverlässige Versorgung bei gleichzeitiger Gewährleistung von Sicherheit. Bei einem Ausfall der Wasserversorgung ist eine direkte Beeinträchtigung der Bevölkerung wahrscheinlich.

Der Sektor „Wasser" umfasst nach der Definition des BBK und BSI die folgenden Bereiche[148]:

- Öffentliche Wasserversorgung
- Öffentliche Abwasserbeseitigung

Dem Statistischen Bundesamt zufolge sind 4.331 Unternehmen in der Branche tätig, wobei sich dies nicht ausschließlich auf öffentliche Unternehmen bezieht. Die Branche beschäftigt 71.942 sozialversicherungspflichtige Mitarbeiter und hat einen jährlichen Umsatz von über 13 Mrd. €.[149]

Die Mehrzahl der Unternehmen in der Wasserwirtschaft in Deutschland sind kleinere Versorger, es gibt nur wenige große, zumeist privatwirtschaftliche Unternehmen. Unter den Annahmen des Szenarios dieser Studie sind **44 Unternehmen des Wassersektors von dem Referentenentwurf betroffen**, die entspricht dem Anteil an Großunternehmen im Sektor, welcher bei rund 1% liegt. Diese beschäftigen rund 27.925 Mitarbeiter und erzielen rund 4,2 Mrd. € Umsatz.[150]

ERNÄHRUNG

Die Versorgung der Menschen mit Nahrung ist von großer Bedeutung für das Wohlergehen der Bevölkerung. Die Versorgung erfolgt in Deutschland nahezu vollständig durch privatwirtschaftliche Unternehmen. Staatliche Institutionen beschränken sich weitestgehend auf die Funktion als Aufsichtsbehörde zur Sicherung der Lebensmittelqualität und Sicherstellung der Versorgung in Krisenfällen. Dies ist notwendig, da eine Unterbrechung der Versorgung erhebliche Auswirkungen auf die Bevölkerung zur Folge haben könnte.

---

[144] Bundesamt für Bevölkerungsschutz und Katastrophenhilfe und Bundesamt für Sicherheit in der Informationstechnik o. J.f
[145] Eigene Berechnungen, Daten: Statistisches Bundesamt 2014a
[146] Kartte und Neumann 2011
[147] Eigene Berechnungen, Daten: Statistisches Bundesamt 2014a
[148] Bundesamt für Bevölkerungsschutz und Katastrophenhilfe und Bundesamt für Sicherheit in der Informationstechnik o. J.e
[149] Eigene Berechnung, Daten: Statistisches Bundesamt 2014a
[150] Eigene Berechnung, Daten: Statistisches Bundesamt 2014a

Der Sektor „Ernährung“ setzt sich nach der Definition von BBK und BSI aus den folgenden Bereichen zusammen:

- Ernährungswirtschaft
- Lebensmittelhandel

Im Allgemeinen wird der Sektor Ernährung dahingehend unterschieden, dass Ernährungswirtschaft als die Industrie definiert wird, die „landwirtschaftliche Erzeugnisse be- und verarbeitet“[151], während der Lebensmittelhandel die „Schnittstelle zwischen den Verbrauchern und der Lebensmittelkette“ darstellt, durch die Nahrungsmittel verteilt werden.[152]

Der Sektor Ernährung zählt 76.906 Unternehmen mit 754.779 Beschäftigten und knapp 174 Mrd. € Umsatz. Die Ernährungswirtschaft ist in hohem Maße mittelständisch geprägt. Rund 0,5% der Unternehmen beschäftigten mehr als 250 Mitarbeiter und zählen damit zu den **Großunternehmen. Daraus ergeben sich für das betrachtete Szenario 448 betroffene Unternehmen im Sektor Ernährung**. Diese beschäftigen rund 270.000 Mitarbeiter und erwirtschaften mit 77 Mrd. € Umsatz etwa 44% des gesamten Umsatzes des Sektors.[153]

TRANSPORT UND VERKEHR

Ein funktionierendes Transport- und Verkehrssystem ist die Grundlage für eine moderne Gesellschaft, die auf die Mobilität von Gütern und Personen angewiesen ist. Diese Abhängigkeit nimmt durch die fortschreitende Globalisierung der Arbeitsteilung in modernen Volkswirtschaften weiter zu und festigt die zentrale Rolle des Sektors „Transport und Verkehr“ für die Produktion von Gütern und die Verrichtung von Dienstleistungen. Beeinträchtigungen oder Ausfälle des Transportwesens hätten gravierende Auswirkungen auf alle Teile der Bevölkerung und Lebensbereiche. Neben den Prozessen in der Wirtschaft, wäre auch die Ausführung der Aufgaben von Staat und Verwaltung erheblich beeinträchtigt.[154]

Der Sektor „Transport und Verkehr“ setzt sich der Definition von BBK und BSI zufolge aus den folgenden Bereichen zusammen[155]:

- Luftfahrt
- Seeschifffahrt
- Binnenschifffahrt
- Schienenverkehr
- Straßenverkehr
- Logistik

Dem Statistischen Bundesamt zufolge gibt es in Deutschland 123.531 Unternehmen, die im Bereich Verkehr und Lagerei tätig sind. In diesen Unternehmen sind 1.457.437 sozialversicherungspflichtige Beschäftigte angestellt, die einen Umsatz von rd. 260.2 Mrd. € erwirtschaften.[156]

Der Sektor „Transport und Verkehr“ ist geprägt von einer großen Anzahl an KMU. Diese haben im Bereich Verkehr und Lagerei einen Anteil von 98,9% an der gesamten Anzahl an Unternehmen. Großunternehmen machen etwa 1,1% der Unternehmen des Sektors aus und damit wären laut dem verwendeten Szenario **1.359 Unternehmen des Sektors Transport und Verkehr von dem Referentenentwurf betroffen**. Diese beschäftigen 724.346 Mitarbeiter und erwirtschaften über 159 Mrd. € Umsatz.

---

[151] Deutscher Bauernverband o. J.
[152] Bundesverband des Deutschen Lebensmittelhandels o. J.
[153] Eigene Berechnungen, Daten: Statistisches Bundesamt 2014a
[154] Bundesamt für Bevölkerungsschutz und Katastrophenhilfe und Bundesamt für Sicherheit in der Informationstechnik o. J.d
[155] Bundesamt für Bevölkerungsschutz und Katastrophenhilfe und Bundesamt für Sicherheit in der Informationstechnik o. J.d
[156] Statistisches Bundesamt 2011

FINANZ- UND VERSICHERUNGSWESEN

Das Finanz- und Versicherungswesen hat eine zentrale Bedeutung für das Funktionieren von Geschäftsprozessen in Deutschland. Die Aufrechterhaltung des Systems hängt ab von einigen zentralen Akteuren, wie z.B. der Europäischen Zentralbank und der Börse in Frankfurt. Bei einem Wegfall dieser Systemkomponenten wäre ein teilweiser Ausfall der Produkte und Dienstleistungen der Branche möglich, was direkte Auswirkungen auf Wirtschaft und Bevölkerung hat. Der Sektor „Finanz- und Versicherungswesen" ist zudem in hohem Maße von anderen KRITIS-Sektoren abhängig, insbesondere der Informations- und Kommunikationstechnologie.[157]

Der Sektor „Finanz- und Versicherungswesen" setzt sich gemäß der Definition von BBK und BSI aus den folgenden Bereichen zusammen:[158]

- Banken
- Börsen
- Versicherungen
- Finanzdienstleister

Dem Statistischen Bundesamt zufolge gibt es in Deutschland 72.737 Unternehmen, die im Finanz- und Versicherungswesen tätig sind. In diesen Unternehmen sind rund 1 Mrd. sozialversicherungspflichtige Beschäftigte angestellt, die einen Umsatz von rund 68 Mrd. € erwirtschaftet haben.[159]

Der Sektor „Finanz- und Versicherungswesen" ist geprägt von einer großen Anzahl an KMU. Großunternehmen machen einen Anteil von rund 1% des Sektors aus. Damit wären laut dem Szenario dieser Studie **780 Unternehmen des Sektors Finanz- und Versicherungswesen vom Referentenentwurf betroffen**. Diese Unternehmen zählen rund 733.000 Beschäftigten und erwirtschaften mit 38,5 Mrd. € mehr als die Hälfte des gesamten Umsatzes im Sektor.

INFORMATIONSTECHNIK UND TELEKOMMUNIKATION

Moderne Gesellschaften sind in zunehmendem Maße vom digitalisierten Informationsaustausch abhängig. Dieser Bedarf wird von den Unternehmen des Sektors ITK bedient, der zunehmend an Bedeutung gewinnt. Die von den ITK-Unternehmen bereitgestellten Produkte und Dienstleistungen stellen zentrale Ressourcen für die Funktionsfähigkeit von „Staat, Wirtschaft und Gesellschaft" dar. Sie bilden darüber hinaus die Grundlage für die Steuerung und Überwachung von Prozessen in vielen Bereichen einer modernen Wirtschaft und sind z.B. für die Automatisierung von Prozessen in Unternehmen bedeutsam, da hierdurch die Arbeit effizienter und effektiver gestaltet werden kann. Ein Ausfall der ITK hätte nicht nur Auswirkungen für die Dienstleistungen und Produkte der ITK-Branche, sondern würde auch Auswirkungen auf kritische Infrastrukturen anderer Sektoren haben.[160]

Der Sektor „ITK" umfasst nach der Definition des BBK und BSI folgende Bereiche:

- Telekommunikation
- Informationstechnik

Das Statistische Bundesamt zählt 130.842 Unternehmen in der ITK, die insgesamt 856.223 sozialversicherungspflichtige Mitarbeiter beschäftigen. Der Umsatz der Branche beläuft sich auf rund 218 Mrd. €.[161]

Die ITK-Wirtschaft in Deutschland ist extrem stark von kleinen Unternehmen geprägt. Nur 0,7% aller Unternehmen der ITK-Branche sind Großunternehmen.[162] Ausgehend von dem Szenario

[157] Bundesamt für Bevölkerungsschutz und Katastrophenhilfe und Bundesamt für Sicherheit in der Informationstechnik o. J.b
[158] Bundesamt für Bevölkerungsschutz und Katastrophenhilfe und Bundesamt für Sicherheit in der Informationstechnik o. J.b
[159] Statistisches Bundesamt 2011
[160] Bundesamt für Bevölkerungsschutz und Katastrophenhilfe und Bundesamt für Sicherheit in der Informationstechnik o. J.c
[161] Statistisches Bundesamt 2011

dieser Studie sind demnach **916 Unternehmen des ITK-Sektors von dem Referentenentwurf betroffen**. Diese beschäftigen zusammen knapp 400.000 Personen und generieren knapp 150 Mrd. € Umsatz.

[162] Statistisches Bundesamt o. J.a

LITERATUR VERZEICHNIS

Allianz für Cyber-Sicherheit (o. J.a): Einführung. Online verfügbar unter https://www.allianz-fuer-cybersicherheit.de/ACS/DE/Ueber_uns/ueber_uns.html, zuletzt geprüft am 12.06.2014.

Allianz für Cyber-Sicherheit (o. J.b): Expertenkreis Cyber-Sicherheit des BSI. Online verfügbar unter https://www.allianz-fuer-cybersicherheit.de/ACS/DE/Erfahrungsaustausch/Expertenkreise/Cyber-Sicherheit/expertenkreis_cybersicherheit.html, zuletzt geprüft am 12.06.2014.

Allianz für Cyber-Sicherheit (o. J.c): Expertenkreis Internetbetreiber. Online verfügbar unter https://www.allianz-fuer-cybersicherheit.de/ACS/DE/Erfahrungsaustausch/Expertenkreise/Betreiber-Internet/expertenkreis_betreiber.html, zuletzt geprüft am 12.06.2014.

Allianz für Cyber-Sicherheit (o. J.d): Über uns. Online verfügbar unter. https://www.allianz-fuer-cybersicherheit.de/ACS/DE/Ueber_uns/ueber_uns.html, zuletzt geprüft am 12.06.2014.

Allianz für Cyber-Sicherheit (2013): Jahresbericht 2012/1013. Online verfügbar unter https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_downloads/Jahresbericht_Allianz_2012_2013.pdf?__blob=publicationFile, zuletzt geprüft am 12.06.2014.

AOK (2014): Gehaltsrechner 2014. Online verfügbar unter http://www.aok-business.de/hessen/tools-service/gehaltsrechner/, zuletzt geprüft am 18.06.2014.

Arbeitskreis Industrie 4.0 (2013): Umsetzungsempfehlungen für das Zukunftsprojekt Industrie 4.0. Online verfügbar unter http://www.plattform-i40.de/sites/default/files/Abschlussbericht_Industrie4%200_barrierefrei.pdf, zuletzt geprüft am 12.06.2014.

Bertelsmann Stiftung (2006): Bürokratie messen, Belastung transparent machen. Das Standard-Kosten-Modell. Online verfügbar unter http://www.bertelsmann-stiftung.de/cps/rde/xbcr/SID-15683889-875B05C1/bst/SKM_Broschur_15020.pdf, zuletzt geprüft am 24.06.2014.

BITKOM (2012): Gesetz zur Verkürzung des Restschuldbefreiungsverfahrens, zur Stärkung der Gläubigerrechte und zur Insolvenzfestigkeit von Lizenzen; BITKOM-Stellungnahme. Online verfügbar unter http://www.bitkom.org/files/documents/BITKOM-Positionspapier_Software_in_der_Insolvenz.pdf, zuletzt geprüft am 12.06.2014.

BITKOM (2013a): Industrie 4.0 – Volkswirtschaftliches Potenzial für Deutschland. Online verfügbar unter http://de.statista.com/statistik/daten/studie/297992/umfrage/potentziale-von-industrie-40-fuer-den-deutschen-maschinen-und-anlagenbau/.

BITKOM (2013b): Nachfrage nach IT-Sicherheitstechnologien steigt um 5 Prozent. Online verfügbar unter http://www.bitkom.org/de/themen/54742_76716.aspx, zuletzt geprüft am 17.06.2014.

BITKOM (2014a): 38 Prozent der Internetnutzer Opfer von Cybercrime. Online verfügbar unter http://www.bitkom.org/de/presse/8477_79284.aspx, zuletzt geprüft am 12.06.2014.

BITKOM (2014b): Anzahl der ITK-Unternehmen in 2012. Online verfügbar unter http://www.bitkom.org/files/documents/Anzahl_ITK-Unternehmen_2012.pdf, zuletzt geprüft am 16.06.2014.

BITKOM (2014c): IT-Sicherheit ist das Hightech-Thema des Jahres. Online verfügbar unter http://www.bitkom.org/de/presse/8477_78713.aspx, zuletzt geprüft am 12.06.2014.

BITKOM (2014d): Nutzung von Cloud Computing in Unternehmen wächst. Online verfügbar unter http://www.bitkom.org/de/markt_statistik/64086_78524.aspx, zuletzt aktualisiert am 30.01.2014, zuletzt geprüft am 12.06.2014.

Bundesamt für Bevölkerungsschutz und Katastrophenhilfe; Bundesamt für Sicherheit in der Informationstechnik (o. J.a): Sektor: Energie. Bundesamt für Bevölkerungsschutz und Katastro-

phenhilfe und dem Bundesamt für Sicherheit in der Informationstechnik. Online verfügbar unter http://www.kritis.bund.de/SubSites/Kritis/DE/Einfuehrung/Sektoren/Energie/Energie_node.html.

Bundesamt für Bevölkerungsschutz und Katastrophenhilfe; Bundesamt für Sicherheit in der Informationstechnik (o. J.b): Sektor: Finanz- und Versicherungswesen. Online verfügbar unter. http://www.kritis.bund.de/SubSites/Kritis/DE/Einfuehrung/Sektoren/FinanzundVersicherungswesen/FinanzundVersicherungswesen_node.html, zuletzt geprüft am 16.06.2014.

Bundesamt für Bevölkerungsschutz und Katastrophenhilfe; Bundesamt für Sicherheit in der Informationstechnik (o. J.c): Sektor: Informationstechnik und Telekommunikation. Online verfügbar unter http://www.kritis.bund.de/SubSites/Kritis/DE/Einfuehrung/Sektoren/ITK/ITK_node.html.

Bundesamt für Bevölkerungsschutz und Katastrophenhilfe; Bundesamt für Sicherheit in der Informationstechnik (o. J.d): Sektor: Transport und Verkehr. Bundesamt für Bevölkerungsschutz und Katastrophenhilfe; Bundesamt für Sicherheit in der Informationstechnik. Online verfügbar unter http://www.kritis.bund.de/SubSites/Kritis/DE/Einfuehrung/Sektoren/TransportundVerkehr/TransportundVerkehr_node.html.

Bundesamt für Bevölkerungsschutz und Katastrophenhilfe; Bundesamt für Sicherheit in der Informationstechnik (o. J.e): Sektor: Wasser. Online verfügbar unter http://www.kritis.bund.de/SubSites/Kritis/DE/Einfuehrung/Sektoren/Wasser/Wasser_node.html.

Bundesamt für Bevölkerungsschutz und Katastrophenhilfe; Bundesamt für Sicherheit in der Informationstechnik (o. J.f): Sektoren und Branchen Kritischer Infrastrukturen. Online verfügbar unter http://www.kritis.bund.de/SubSites/Kritis/DE/Einfuehrung/Sektoren/sektoren_node.html.

Bundesamt für Sicherheit in der Informationstechnik (o. J.a): Chancen nutzen – Risiken vermeiden. Online verfügbar unter https://www.bsi.bund.de/DE/DasBSI/dasbsi_node.html, zuletzt geprüft am 12.06.2014.

Bundesamt für Sicherheit in der Informationstechnik (o. J.b): Organisationsübersicht des BSI. Online verfügbar unter https://www.bsi.bund.de/DE/DasBSI/Aufgaben/aufgaben_node.html, zuletzt geprüft am 12.06.2014.

Bundesamt für Sicherheit in der Informationstechnik (o. J.c): Strategie & Aktivitäten. Online verfügbar unter https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/Strategie/cs_Strategie_node.html, zuletzt geprüft am 17.06.2014.

Bundesamt für Sicherheit in der Informationstechnik (o. Jd.): Allianz für Cyber-Sicherheit. Online verfügbar unter https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_downloads/ACS_Flyer_PDF.pdf?__blob=publicationFile, zuletzt geprüft am 12.06.2014.

Bundesamt für Sicherheit in der Informationstechnik (2013): Expertenkreis Cyber-Sicherheit des BSI nimmt seine Arbeit auf. Online verfügbar unter https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2013/Expertenkreis-Cyber-Sicherheit_22032013.html, zuletzt geprüft am 12.06.2014.

Bundesärztekammer (2013): Stellungnahme der Bundesärztekammer zum Entwurf eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz - ITSiG) 2013. Online verfügbar unter http://www.bundesaerztekammer.de/downloads/Stellungnahme_der_Bundesaerztekammer_zu_Entwurf_eines_Gesetzes_zur_Erhoehung_der_Sicherheit_informationstechnischer_Systeme.pdf, zuletzt geprüft am 12.06.2014.

Bundesbeauftragter für den Datenschutz und die Informationsfreiheit (2010): Bundesdatenschutzgesetz (BDSG). Online verfügbar unter http://www.bfdi.bund.de/cae/servlet/contentblob/409518/publicationFile/25234/BDSG.pdf, zuletzt geprüft am 12.06.2014.

Bundeskriminalamt (2012): Cybercrime - Bundeslagebild 2012. Online verfügbar unter http://www.bka.de/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrime__node.html?__nnn=true, zuletzt geprüft am 12.06.2014.

Bundesministerium des Innern (o. J.): Deutschland sicher im Netz. Online verfügbar unter http://www.bmi.bund.de/DE/Themen/IT-Netzpolitik/IT-

Cybersicherheit/Cybersicherheitsstrategie/sicher-im-Netz/sicher-im-netz_node.html, zuletzt aktualisiert am 12.06.2014, zuletzt geprüft am 12.06.2014.

Bundesministerium des Innern (2005): Nationaler Plan zum Schutz der Informationsinfrastrukturen (NPSI). Online verfügbar unter http://www.bmi.bund.de/cae/servlet/contentblob/121734/publicationFile/13577/Nationaler_Plan_Schutz_Informationsinfrastrukturen.pdf, zuletzt geprüft am 12.06.2014.

Bundesministerium des Innern (2009): Nationale Strategie zum Schutz Kritischer Infrastrukturen (KRITIS-Strategie). Online verfügbar unter http://www.bmi.bund.de/cae/servlet/contentblob/544770/publicationFile/27031/kritis.pdf, zuletzt geprüft am 12.06.2014.

Bundesministerium des Innern (2011): Cyber-Sicherheitsstrategie für Deutschland. Online verfügbar unter http://www.bmi.bund.de/SharedDocs/Downloads/DE/Themen/OED_Verwaltung/Informationsgesellschaft/cyber.pdf?__blob=publicationFile, zuletzt geprüft am 12.06.2014.

Bundesministerium des Innern (2013a): Referentenentwurf des Bundesministeriums des Innern. Entwurf eines Gesetzes zur Erhöhung der Sicherheit informations-technischer Systeme. ITSiG. Online verfügbar unter https://www.bmi.bund.de/SharedDocs/Downloads/DE/Gesetzestexte/Entwuerfe/Entwurf_it-sicherheitsgesetz.pdf?__blob=publicationFile, zuletzt geprüft am 12.06.2014.

Bundesministerium des Innern (2013b): Friedrich stellt Wirtschaft IT-Sicherheitsgesetz vor. BMI. Online verfügbar unter http://www.bmi.bund.de/SharedDocs/Kurzmeldungen/DE/2013/03/eco_mmr_itsicherheitsgesetz.html, zuletzt geprüft am 12.06.2014.

Bundesministerium des Innern (2014a): IT und Netzpolitik. IT-Steuerung des Bundes. BMI. Online verfügbar unter http://www.bmi.bund.de/DE/Themen/IT-Netzpolitik/IT-Bund/IT-Bund/it-bund_node.html;jsessionid=F687488C431854917DC50D62BBDA4D8F.2_cid364, zuletzt geprüft am 12.06.2014.

Bundesministerium des Innern (2014b): Rede von Bundesminister Dr. Thomas de Maizière, MdB, anlässlich der Einbringung des Bundeshaushalts 2014 (Innen, EP 06) am 08. April 2014 im Deutschen Bundestag. BMI. Online verfügbar unter http://www.bmi.bund.de/SharedDocs/Reden/DE/2014/04/haushalt.html, zuletzt geprüft am 12.06.2014.

Bundesministerium für Bildung und Forschung (o. J.a): Cybersicherheitsforschung für die Wettbewerbsfähigkeit Deutschlands. Online verfügbar unter http://www.bmbf.de/de/73.php, zuletzt aktualisiert am 03.06.2014, zuletzt geprüft am 12.06.2014.

Bundesministerium für Bildung und Forschung (o. J.b): Perspektive MINT-Berufe: Förderung von Technik und Naturwissenschaft. Online verfügbar unter http://www.bmbf.de/de/mint-foerderung.php, zuletzt geprüft am 12.06.2014.

Bundesministerium für Verkehr und digitale Infrastruktur (2004): Telekommunikationsgesetz. TKG. Online verfügbar unter http://www.bmvi.de/SharedDocs/DE/Anlage/Digitales/telekommunikationsgesetz-2012.pdf?__blob=publicationFile, zuletzt geprüft am 12.06.2014.

Bundesministerium für Wirtschaft und Energie (o. J.a): Initiative „IT-Sicherheit in der Wirtschaft“. Online verfügbar unter http://www.bmwi.de/DE/Themen/Digitale-Welt/sicherheit,did=362756.html, zuletzt geprüft am 12.06.2014.

Bundesministerium für Wirtschaft und Energie (o. J.b): Nationaler IT-Gipfel. Online verfügbar unter http://www.bmwi.de/DE/Themen/Digitale-Welt/nationaler-it-gipfel.html, zuletzt geprüft am 12.06.2014.

Bundesministerium für Wirtschaft und Energie (2012): IT-Sicherheitsniveau in kleinen und mittleren Unternehmen 2012. Online verfügbar unter http://www.bmwi.de/BMWi/Redaktion/PDF/S-T/studie-it-sicherheit,property%3Dpdf,bereich%3Dbmwi2012,sprache%3Dde,rwb%3Dtrue.pd, zuletzt geprüft am 12.06.2014.

Bundesministerium für Wirtschaft und Energie (2013a): Der IT-Sicherheitsmarkt in Deutschland. Online verfügbar unter http://www.bmwi.de/BMWi/Redaktion/PDF/Publikationen/Studien/it-sicherheitsmarkt-in-deutschland,property=pdf,bereich=bmwi2012,sprache=de,rwb=true.pdf, zuletzt geprüft am 17.06.2014.

Bundesministerium für Wirtschaft und Energie (2013b): Der IT-Sicherheitsmarkt in Deutschland. Online verfügbar unter.http://www.bmwi.de/BMWi/Redaktion/PDF/Publikationen/Studien/it-sicherheitsmarkt-in-deutschland,property=pdf,bereich=bmwi2012,sprache=de,rwb=true.pdf, zuletzt geprüft am 12.06.2014.

Bundesministerium für Wirtschaft und Energie (2014): Ergebnispapier "Arbeit in der digitalen Welt". Online verfügbar unter http://www.it-gipfel.de/IT-Gipfel/Navigation/mediathek,did=630874.html, zuletzt aktualisiert am 19.03.2014, zuletzt geprüft am 18.06.2014.

Bundesnetzagentur (2014): Teilnehmerentwicklung im Mobilfunk. Teilnehmerentwicklung im Mobilfunk nach Netzen pro Quartal. Online verfügbar unter http://www.bundesnetzagentur.de/cln_1432/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Marktbeobachtung/Deutschland/Mobilfunkteilnehmer/Mobilfunkteilnehmer_node.html, zuletzt geprüft am 16.06.2014.

Bundesregierung (2010): Regierungsprogramm Vernetzte und transparente Verwaltung, zuletzt geprüft am 12.06.2014.

Bundesregierung (2013): Deutschlands Zukunft gestalten. Koalitionsvertrag zwischen CDU, CSU und SPD, S. 97. Online verfügbar unter http://www.bundesregierung.de/Content/DE/_Anlagen/2013/2013-12-17-koalitionsver-trag.pdf;jsessionid=140DDFF643BB86430A1A3515F74FF396.s4t1?__blob=publicationFile&v=2, zuletzt geprüft am 12.06.2014.

Bundesverband des Deutschen Lebensmittelhandels (o. J.): Über uns. Schnittstelle zwischen Handel und Öffentlichkeit. Online verfügbar unter http://www.bvlh.net/ueber_uns.html, zuletzt geprüft am 16.06.2014.

Cyber Security Summit (2014): Cyber Security Summit. Online verfügbar unter http://www.cybersecuritysummit.de/, zuletzt geprüft am 12.06.2014.

Deutscher Bauernverband (o. J.): 1.4 Ernährungswirtschaft. Online verfügbar unter http://www.bauernverband.de/ernaehrungswirtschaft, zuletzt geprüft am 16.06.2014.

Deutscher Bundestag (2009): Gesetz zur Stärkung der Sicherheit in der Informationstechnik des Bundes. Online verfügbar unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/BSI/bsiges2009_pdf.pdf?__blob=publicationFile, zuletzt geprüft am 17.06.2014.

Deutscher Industrie- und Handelskammertag (o. J.): IT-Sicherheitsgesetz. Online verfügbar unter http://www.dihk.de/branchen/informations-und-kommunikationsbranche/it-multimedia-e-business/it-sicherheitsgesetz, zuletzt geprüft am 12.06.2014.

Deutsches Institut für Normung (o. J.): Stellungnahme des DIN Deutsches Institut für Normung e.V. zum Referentenentwurf eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme. Online verfügbar unter http://www.din.de/sixcms_upload/media/2896/KITS_N0149_Stellungnahme_des_DIN_zu_Referentenentwurf_eines_.149199.pdf, zuletzt geprüft am 12.06.2014.

Deutschland sicher im Netz (o. J.a): Kooperationen. Online verfügbar unter https://www.sicher-im-netz.de/kooperationen, zuletzt geprüft am 12.06.2014.

Deutschland sicher im Netz (o. J.b): Mitglieder. Online verfügbar unter https://www.sicher-im-netz.de/mitglieder, zuletzt geprüft am 12.06.2014.

Deutschland sicher im Netz (o. J.c): Online-Checks & Studien. Online verfügbar unter https://www.sicher-im-netz.de/unternehmen/online-checks-studien, zuletzt geprüft am 12.06.2014.

Die Welt (2014): Ebay ruft alle Nutzer zur Passwort-Änderung auf. Online verfügbar unter http://www.welt.de/wirtschaft/webwelt/article128279640/Ebay-ruft-alle-Nutzer-zur-Passwort-Aenderung-auf.html, zuletzt aktualisiert am 21.05.2014, zuletzt geprüft am 16.06.2014.

Europäische Kommission (2013): Vorschlag für eine RICHTLINIE DES EUROPÄISCHEN PARLAMENTS UND DES RATES über Maßnahmen zur Gewährleistung einer hohen gemeinsamen Netz- und Informationssicherheit in der Union. 2013/0027. Online verfügbar unter http://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:52013PC0048&from=EN, zuletzt geprüft am 12.06.2014.

European Information Technology Observatory (2013): ICT Market Report 2013/14 Germany. Online verfügbar unter http://www.eito.com/ICT-Market-Report-2013/14-Germany, zuletzt geprüft am 12.06.2014.

FAZ (2013): Was leistet das „IT-Sicherheitsgesetz"? Online verfügbar unter http://www.faz.net/aktuell/politik/fragen-und-antworten-was-leistet-das-it-sicherheitsgesetz-12647710.html

Fraunhofer-Institut für Sichere Informationstechnologie (2013): Entwicklung sicherer Software durch Security by Design. Online verfügbar unter https://www.kastel.kit.edu/downloads/Entwicklung_sicherer_Software_durch_Security_by_Design.pdf, zuletzt geprüft am 12.06.2014.

Freudenberg IT (2013): Maschinen- und Anlagenbauer verkennen Potenzial von Industrie 4.0. Online verfügbar unter http://www.freudenberg-it.com/de/it-innovation-readiness-index/teil-2.html, zuletzt aktualisiert am 19.11.2013, zuletzt geprüft am 12.06.2014.

Handelsblatt (2013): „Vorratsdatenspeicherung durch die Hintertür". Online verfügbar unter http://www.handelsblatt.com/politik/deutschland/kritik-an-it-sicherheitsgesetz-vorratsdatenspeicherung-durch-die-hintertuer/7912900.html

Hasso-Plattner-Institut (2014): Potsdamer Konferenz für Nationale Cybersicherheit. Online verfügbar unter http://www.potsdamer-sicherheitskonferenz.de/konferenz.html, zuletzt aktualisiert am 10.06.2014, zuletzt geprüft am 12.06.2014.

Initiative D21 (2013): D21 - Digital - Index. Auf dem Weg in ein digitales Deutschland?!, zuletzt geprüft am 12.06.2014.

IT Sicherheit in der Wirtschaft (o. J.): Angebote. Online verfügbar unter http://www.it-sicherheit-in-der-wirtschaft.de/IT-Sicherheit/Navigation/angebote.html, zuletzt aktualisiert am 09.01.2014, zuletzt geprüft am 12.06.2014.

Kartte, Joachim; Neumann, Karsten (2011): Weltweite Gesundheitswirtschaft - Chancen für Deutschland. Studie im Auftrag des Bundesministeriums für Wirtschaft und Energie. Roland Berger. Online verfügbar unter http://www.biodeutschland.org/tl_files/content/dokumente/biothek/Roland_Berger_Studie_Weltweite_Gesundheitswirtschaft.pdf, zuletzt geprüft am 16.06.2014.

Kommission der Europäischen Gemeinschaften (2013): EMPFEHLUNG DRE KOMMISSION vom 6. Mai 2013 betreffend die Definition der Kleinunternehmen sowie der kleinen und mittleren Unternehmen. 2003/361/EG. Online verfügbar unter http://www.esf.de/portal/generator/20314/property=data/vo__2003.pdf, zuletzt geprüft am 16.06.2014.

Netzökonom (2014): Samsung zieht Konkurrenz in Deutschland weiter davon. Online verfügbar unter http://netzoekonom.de/2014/04/13/samsung-zieht-konkurrenz-in-deutschland-weiter-davon/, zuletzt geprüft am 12.06.2014.

Plattform Industrie 4.0 (2014): Was Industrie 4.0 (für uns) ist. Online verfügbar unter http://www.plattform-i40.de/blog/was-industrie-40-f%C3%BCr-uns-ist, zuletzt geprüft am 26.06.2014.

Quartz (2014): Target's traffic still hasn't recovered from the giant data breach. Online verfügbar unter http://qz.com/212003/targets-traffic-still-hasnt-recovered-from-the-giant-data-breach/#212003/targets-traffic-still-hasnt-recovered-from-the-giant-data-breach/, zuletzt geprüft am 16.06.2014.

Selbstregulierung Informationswirtschaft (o. J.a): Mitgliederverzeichnis. Online verfügbar unter http://www.sriw.de/index.php/home/organisation/mitgliederverzeichnis, zuletzt geprüft am 12.06.2014.

Selbstregulierung Informationswirtschaft (o. J.b): Übersicht und Ziele. Online verfügbar unter http://www.sriw.de/index.php/home/uebersicht-und-ziele, zuletzt geprüft am 12.06.2014.

Spiegel (2013): Meldepflicht für Hackattacken: Ministerien wollen IT-Sicherheitsgesetz auf den Weg bringen. Online verfügbar unter http://www.spiegel.de/netzwelt/netzpolitik/ministerien-einigen-sich-ueber-it-sicherheitsgesetz-a-887292.html

Springer Gabler Verlag: Gabler Wirtschaftslexikon, Stichwort: Reputation. Online verfügbar unter: http://wirtschaftslexikon.gabler.de/Archiv/9313/reputation-v6.html, zuletzt geprüft am 12.06.2014.

Statistisches Bundesamt (o. J.a): Anteile kleiner und mittlerer Unternehmen an ausgewählten Merkmalen 2011. Energieversorgung. Online verfügbar unter https://www.destatis.de/DE/ZahlenFakten/GesamtwirtschaftUmwelt/UnternehmenHandwerk/KleineMittlereUnternehmenMittelstand/Tabellen/Energieversorgung.html.

Statistisches Bundesamt (o. J.b): Kleine & mittlere Unternehmen (KMU), Mittelstand . Online verfügbar unter https://www.destatis.de/DE/ZahlenFakten/GesamtwirtschaftUmwelt/UnternehmenHandwerk/KleineMittlereUnternehmenMittelstand/KleineMittlereUnternehmenMittelstand.html, zuletzt geprüft am 17.06.2014.

Statistisches Bundesamt (2006): Einführung des Standardkosten-Modells Methodenhandbuch der Bundesregierung. Online verfügbar unter https://www-skm.destatis.de/webskm/misc/Methodenhandbuch_SKM.pdf, zuletzt geprüft am 24.06.2014.

Statistisches Bundesamt (2011): Unternehmensregister . Unternehmen, Beschäftigte und Umsatz. Online verfügbar unter https://www.destatis.de/DE/ZahlenFakten/GesamtwirtschaftUmwelt/UnternehmenHandwerk/Unternehmensregister/Tabellen/UnternehmenBeschaeftigteUmsatzWZ08.html, zuletzt aktualisiert am 02.12.2013, zuletzt geprüft am 16.06.2014.

Statistisches Bundesamt (2013a): Soziale Medien halten Einzug in die Unternehmen. Online verfügbar unter https://www.destatis.de/DE/PresseService/Presse/Pressemitteilungen/2013/12/PD13_417_52911pdf.pdf?__blob=publicationFile, zuletzt geprüft am 12.06.2014.

Statistisches Bundesamt (2013b): Unternehmen und Arbeitsstätten. Nutzung von Informations- und Kommunikationstechnologien in Unternehmen. Online verfügbar unter https://www.destatis.de/DE/Publikationen/Thematisch/UnternehmenHandwerk/Unternehmen/InformationstechnologieUnternehmen5529102137004.pdf?__blob=publicationFile, zuletzt geprüft am 12.06.2014.

Statistisches Bundesamt (2013c): Verdienste und Arbeitskosten. Arbeitnehmerverdienste und Indizes der Arbeitnehmerverdienste - Lange Reihen -. Online verfügbar unter https://www.destatis.de/DE/Publikationen/Thematisch/VerdiensteArbeitskosten/Arbeitnehmerverdienste/ArbeitnehmerverdiensteLangeReihe.html, zuletzt geprüft am 24.06.2014.

Statistisches Bundesamt (2013d): Erzeugerpreisindizes für Dienstleistungen: Informationen zum Preisindex. Telekommunikation (WZ 2008: 61). Online verfügbar unter https://www.destatis.de/DE/ZahlenFakten/GesamtwirtschaftUmwelt/Preise/ErzeugerpreisindizesDienstleistungen/Tabellen/BrancheninfoTelekommunikation_Basis2010.pdf?__blob=publicationFile, zuletzt geprüft am 16.06.2014.

Statistisches Bundesamt (2014a): Statistisches Unternehmensregister. Unternehmen nach Wirtschaftsabschnitten und Größenklassen der sozialversicherungspflichtig Beschäftigten im Berichtsjahr 2011.

Statistisches Bundesamt (2014b): Zahl der mobilen Internetnutzer im Jahr 2013 um 43 % gestiegen. Internet. Online verfügbar unter https://www.destatis.de/DE/PresseService/Presse/Pressemitteilungen/2014/03/PD14_089_63931.html, zuletzt aktualisiert am 11.03.2014, zuletzt geprüft am 12.06.2014.

Stiftung Münchner Sicherheitskonferenz (o. J.): Cyber Security Summit. Online verfügbar unter https://www.securityconference.de/veranstaltungen/cyber-security-summit/, zuletzt geprüft am 12.06.2014.

Stiftung Münchner Sicherheitskonferenz (2012): Erster Cyber Security Summit 2012 in Bonn. Online verfügbar unter https://www.securityconference.de/fileadmin/user_upload/data/images/Cyber_Security_Summit/Fazit_CSS_2012.pdf, zuletzt geprüft am 12.06.2014.

Süddeutsche.de (2014): Rechnungsprüfer kritisieren Cyber-Abwehrzentrum. Online verfügbar unter http://www.sueddeutsche.de/digital/behoerde-in-bonn-rechnungspruefer-halten-cyber-abwehrzentrum-fuer-nicht-gerechtfertigt-1.1989433, zuletzt geprüft am 17.06.2014.

USA Today (2014): Target profit falls 16%, missing estimates. Online verfügbar unter http://www.usatoday.com/story/money/business/2014/05/21/target-earnings/9341321/?_ga=1.182493862.1485962042.1400750529, zuletzt geprüft am 16.06.2014.

Verband kommunaler Unternehmen (2013): VKU nimmt Stellung zum IT-Sicherheitsgesetz. VKU. Online verfügbar unter http://www.vku.de/wasser/ordnungspolitik/kommunale-daseinsvorsorge/vku-nimmt-stellung-zum-it-sicherheitsgesetz.html, zuletzt aktualisiert am 15.04.2013, zuletzt geprüft am 12.06.2014.

Kontakt

KPMG AG
Wirtschaftsprüfungsgesellschaft
Klingelhöferstraße 18
10785 Berlin

Wilhelm Dolle
Partner, Security Consulting
WDolle@kpmg.com

Alexander Geschonneck
Partner, Forensic
AGeschonneck@kpmg.com

Studienleiter:
Dr. Sebastian Chávez Wurm

www.kpmg.de