Hanna Lurz, Barbara Scheben, RAin, und Wilhelm Dolle

Das IT-Sicherheitsgesetz: Herausforderungen und Chancen für Unternehmen – vor allem für KMU

Am 25.7.2015 ist das IT-Sicherheitsgesetz in Kraft getreten. Es soll den Schutz der Bürgerinnen und Bürger sowie die Sicherheit von Unternehmen im Internet verbessern. Ziel ist, die digitalen Infrastrukturen Deutschlands zu den sichersten weltweit zu machen. Gerade bei kleinen und mittleren Unternehmen, zu denen 99,3 % der deutschen Unternehmen zählen, bleiben aber noch viele Fragen offen.

I. Historie

Im Juni 2010 hat der Europäische Rat das auf zehn Jahre angelegte Wirtschaftsprogramm „Europa 2020" verabschiedet, das intelligentes, nachhaltiges und integratives Wachstum verfolgt. Das Programm strebt fünf Kernziele an: Beschäftigung, Forschung und Entwicklung, Klimawandel und nachhaltige Energiewirtschaft, Bildung sowie die Bekämpfung von Armut und sozialer Ausgrenzung. Diese Kernziele sollen durch insgesamt sieben Flaggschiffinitiativen erreicht werden, zu der auch die Digitale Agenda zählt.

Ein Baustein der Digitalen Agenda ist das „Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz)". Es stellt im eigentlichen Sinne kein neues Gesetz dar, sondern ist vielmehr eine Sammlung von Änderungsgesetzen für bestehende Gesetze. Konkret betroffen sind das BSI-Gesetz, das Atomgesetz, das Energiewirtschaftsgesetz, das Telemedien- und Telekommunikationsgesetz sowie das Bundesbesoldungs- und Bundeskriminalamtgesetz. Mehr als zwei Jahre sind vergangen, seit der erste Entwurf im März 2013 unter dem damaligen Innenminister *Hans-Peter Friedrich* veröffentlicht wurde. Es folgten neue Entwürfe im August und November 2014 sowie im Februar 2015; letzterer wurde am 12.6.2015 inkl. Änderungsantrag der Koalitionsfraktionen verabschiedet und trat nach Zustimmung durch den Bundesrat, Prüfung und Unterzeichnung durch den Bundespräsidenten sowie Veröffentlichung durch das Bundesjustizministerium am 25.7.2015 in Kraft.

II. Zielsetzung

Aufgrund der hohen IT-Durchdringung von Geschäftsprozessen und Abläufen über alle Branchen hinweg sowie der allseits diskutierten, nicht abzustreitenden rasant voranschreitenden Vernetzung der IT-Infrastrukturen und der Wirtschaftsakteure wird die Abhängigkeit von IT weiter steigen. Dass der IT-Sicherheit und deren Gefährdungen in Form von Cyberangriffen und Ähnlichem mehr Aufmerksamkeit geschenkt werden muss, ist daher unbestritten.

Das erklärte Ziel des IT-Sicherheitsgesetzes ist „eine signifikante Verbesserung der Sicherheit informationstechnischer Systeme (IT-Sicherheit) in Deutschland […]. Die vorgesehenen Neuregelungen dienen dazu, den Schutz der Systeme im Hinblick auf die Schutzgüter der IT-Sicherheit (Verfügbarkeit, Integrität, Vertraulichkeit und Authentizität) zu verbessern, um den aktuellen und zukünftigen Gefährdungen der IT-Sicherheit wirksam begegnen zu können. Ziel des Gesetzes ist die Verbesserung der IT-Sicherheit von Unternehmen, der verstärkte Schutz der Bürgerinnen und Bürger im Internet und in diesem Zusammenhang auch die Stärkung von Bundesamt für Sicherheit in der Informationstechnik (BSI) und Bundeskriminalamt (BKA)".[1] Diese Zielsetzung unterstreicht auch das übergeordnete Ziel von Innenminister *Thomas de Maizière*, „dass das Netz sicherer wird und die digitalen Infrastrukturen Deutschlands künftig zu den sichersten weltweit gehören".[2] Die angestrebte Erhöhung der IT-Sicherheit soll durch Aufklärung, den Schutz der sogenannten Kritischen Infrastrukturen (KRITIS) sowie durch erweiterte Befugnisse und höhere Anforderungen erreicht werden.

III. Geltungsbereich

Das IT-Sicherheitsgesetz hat mehrere Adressaten. In erster Linie betrifft es die Betreiber Kritischer Infrastrukturen in den Sektoren Energie, Finanz- und Versicherungswesen, Ernährung, Wasser, Gesundheit, Transport und Verkehr sowie Informationstechnik und Telekommunikation. Indirekt sind auch Dienstleister von KRITIS-Betreibern betroffen, die zum Betrieb kritischer Dienstleistungen beitragen. Bundes-, Landes- und Kommunalverwaltung sowie Ministerien und Sicherheitsbehörden unterliegen nicht dem IT-Sicherheitsgesetz; ebenso wenig Branchen und Betreiber des KRITIS-Sektors „Medien und Kultur", die durch entsprechende Vorgaben auf Landesebene reguliert werden sollen.

Bislang löst das IT-Sicherheitsgesetz nicht auf, wer Betreiber einer „Kritischen Infrastruktur" im Sinne des Gesetzes ist. Als weiterer Schritt zur Umsetzung muss daher durch Verabschiedung der noch zu erstellenden Rechtsverordnung festgelegt werden, welche Unternehmen den Regelungen des Gesetzes unterliegen. „Die Rechtsverordnung wird messbare Kriterien wie bspw. den Marktanteil an der Versorgung einer bestimmten Region mit einer bestimmten Leistung festlegen. Wer diese Kriterien erfüllt, betreibt eine Kritische Infrastruktur im Sinne des Gesetzes."[3] Bis zum Erlass der klärenden Rechtsverordnungen hilft nur die offizielle, aber wenig konkrete KRITIS-Definition: „Kritische Infrastrukturen im Sinne dieses Gesetzes sind Einrichtungen, Anlagen oder Teile davon, die 1. den Sektoren Energie, Informationstechnik und Telekommunikation, Transport

1 BMI: Gesetzentwurf der Bundesregierung, Entwurf eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz), http://www.bmi.bund.de/SharedDocs/Downloads/DE/Nachrichten/Kurzmeldungen/entwurf-it-sicherheitsgesetz.pdf?__blob=publicationFile (Abruf: 8.9.2015), Abschn. A.

2 Die Bundesregierung: IT-Sicherheitsgesetz, Schutz für die digitale Infrastruktur, 25.7.2015. https://www.bundesregierung.de/Content/DE/Artikel/2014/12/2014-12-17-kabinett-it-sicherheitsgesetz.html (Abruf: 8.9.2015).

3 BSI: Fragen und Antworten zum Inkrafttreten des IT-Sicherheitsgesetzes, https://www.bsi.bund.de/SharedDocs/FAQs/DE/BSI/IT-SiGesetz/faq_node.html (Abruf: 8.9.2015).

und Verkehr, Gesundheit, Wasser, Ernährung sowie Finanz- und Versicherungswesen angehören und 2. von hoher Bedeutung für das Funktionieren des Gemeinwesens sind, weil durch ihren Ausfall oder ihre Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit eintreten würden."[4] Das Bundesamt für Sicherheit in der Informationstechnik (BSI) gibt an, dass der Gesetzesbegründung zufolge von insgesamt nicht mehr als 2000 Betreibern Kritischer Infrastrukturen in den regulierten sieben Sektoren auszugehen ist.[5]

Zusätzlich zu KRITIS-Betreibern verpflichtet das IT-Sicherheitsgesetz auch Anbieter gewerblicher Telemediendienste, d. h. Betreiber von Webangeboten wie zum Beispiel Online-Shops, zum Handeln. Für diese gelten mit Inkrafttreten erhöhte Anforderungen an Maßnahmen zum Schutz von Kundendaten und den genutzten IT-Systemen. Daher müssen Anbieter geeignete technische und organisatorische Maßnahmen nach dem Stand der Technik ergreifen, um sowohl unerlaubte Zugriffe auf ihre technischen Einrichtungen und Daten als auch Störungen zu verhindern.

Ferner sind Telekommunikationsunternehmen durch das IT-Sicherheitsgesetz „verpflichtet, ihre Kunden zu warnen, wenn sie bemerken, dass der Anschluss des Kunden […] für IT-Angriffe missbraucht wird. Gleichzeitig sollen die Provider ihre Kunden auf mögliche Wege zur Beseitigung der Störung hinweisen."[6]

IV. Inhalte

Im Kern enthält das IT-Sicherheitsgesetz drei Verpflichtungen, denen Unternehmen und die öffentliche Hand[7] nachkommen müssen: verpflichtende Mindestanforderungen an die IT-Sicherheit durch die Umsetzung allgemeiner und branchenspezifischer Mindeststandards, regelmäßige Sicherheitsüberprüfungen zum Nachweis der Umsetzung der Anforderungen sowie eine Meldepflicht für Vorfälle unter Nennung von Warn- und Alarmierungskontakten an das BSI.

1. Allgemeine und branchenspezifische Mindeststandards

Durch Ergänzung von § 8a „Sicherheit in der Informationstechnik Kritischer Infrastrukturen" im BSI-Gesetz (BSIG) werden Betreiber Kritischer Infrastrukturen dazu verpflichtet, angemessene Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen, die für die Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen maßgeblich sind. Dies betrifft indirekt auch Dienstleister der KRITIS-Betreiber, wenn z. B. für den Betrieb der Kritischen Infrastruktur notwendige Dienstleistungen im Rahmen von Outsourcing durch externe Parteien erbracht werden.

Die zu treffenden Vorkehrungen sollen sowohl technische als auch organisatorische Maßnahmen (TOM) beinhalten. Beispiele hierfür sind das Betreiben eines Informationssicherheitsmanagementsystems (ISMS), die Identifikation und das Management kritischer Cyber-Assets, Maßnahmen zur Angriffsprävention und -erkennung sowie die Implementierung eines Business Continuity Managements (BCM). Dabei soll der Stand der Technik eingehalten werden. Als „angemessen" gelten Vorkehrungen, wenn der dafür erforderliche Aufwand nicht außer Verhältnis zu den Folgen eines Ausfalls oder einer Beeinträchtigung der betroffenen Kritischen Infrastruktur steht.

KRITIS-Betreiber und ihre Branchenverbände können branchenspezifische Sicherheitsstandards zu technischen und organisatorischen Maßnahmen ableiten und dem BSI vorschlagen. Dieses stellt auf Antrag fest, ob die vorgeschlagenen Standards geeignet sind, die gesetzlichen Anforderungen zu gewährleisten. Die Feststellung erfolgt dabei im Einvernehmen des Bundesamts für Bevölkerungsschutz und Katastrophenhilfe, der zuständigen Aufsichtsbehörde des Bundes oder der sonst zuständigen Aufsichtsbehörde.

2. Nachweispflicht

Die Erfüllung der im IT-Sicherheitsgesetz geforderten organisatorischen und technischen Vorkehrungen zum Schutz Kritischer Infrastrukturen muss dem BSI mindestens alle zwei Jahre nachgewiesen werden. Der Nachweis kann durch Sicherheitsaudits, Prüfungen oder Zertifizierungen erfolgen, wobei bislang keine feste Form des Nachweises definiert ist. Die Betreiber übermitteln dem BSI eine Aufstellung der durchgeführten Überprüfungen einschließlich der dabei aufgedeckten Sicherheitsmängel. Liegen Sicherheitsmängel vor, kann das BSI die Übermittlung der gesamten Überprüfungsergebnisse sowie im Benehmen mit der zuständigen Aufsichtsbehörde die Beseitigung der Mängel verlangen.

Zur Ausgestaltung des Prüfverfahrens kann das BSI Anforderungen an die Art und Weise der Durchführung, an die auszustellenden Nachweise sowie fachliche und organisatorische Anforderungen an die prüfende Stelle festlegen. Dabei sind Vertreter der betroffenen Betreiber und Wirtschaftsverbände anzuhören.[8]

3. Meldepflicht

Mit der Änderung des BSI-Gesetzes durch Art. 1 des IT-Sicherheitsgesetzes sind Betreiber Kritischer Infrastrukturen ferner dazu verpflichtet, IT-Sicherheitsvorfälle unverzüglich zu melden. Dies betrifft erhebliche Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit von informationstechnischen Systemen, Komponenten oder Prozessen der Betreiber. Dabei wird eine Störung als erheblich eingestuft, wenn sie zu einem Ausfall oder einer Beeinträchtigung der Funktionsfähigkeit der betriebenen Kritischen Infrastrukturen führen könnte oder geführt hat.

Die Meldung muss über eine zuvor genannte Kontaktstelle an das BSI erfolgen. Betreiber öffentlicher Telekommunikationsnetze und Anbieter von Telekommunikationsdiensten sowie Betreiber von Energieversorgungsnetzen und Energieanlagen, die unter Aufsicht der Bundesnetzagentur (BNetzA) stehen, melden Störungen statt an das BSI an die BNetzA.[9]

Grundsätzlich kann die Meldung von Störungen zweistufig verlaufen. Dabei sollen zunächst alle ohne Rechercheaufwand erhobenen Umstände gemeldet und im Verlauf der weiteren Bearbeitung des Vorfalls weitere Informationen nachgereicht werden. Die Meldung muss Angaben zur Störung sowie zu den technischen Rahmenbedingungen, insbesondere der vermuteten oder tatsächlichen Ursache, der betrof-

4 § 2 Abs. 10 BSIG.
5 BSI Fragen und Antworten zum Inkrafttreten des IT-Sicherheitsgesetzes, https://www.bsi.bund.de/SharedDocs/FAQs/DE/BSI/IT-SiGesetz/faq_node.html (Abruf: 8.9.2015).
6 BSI Fragen und Antworten zum Inkrafttreten des IT-Sicherheitsgesetzes, https://www.bsi.bund.de/SharedDocs/FAQs/DE/BSI/IT-SiGesetz/faq_node.html (Abruf: 8.9.2015).
7 Vom Gesetz grundsätzlich ausgenommen sind lediglich Kleinstunternehmen mit weniger als zehn Mitarbeitern. Darunter fallen gemäß der im Gesetz zitierten EG-Empfehlung (2003/261/EC) jedoch keine Unternehmen, die zu 25 % oder mehr in öffentlicher Hand sind.
8 § 8a BSIG.
9 § 11 EnWG sowie § 109 TKG.

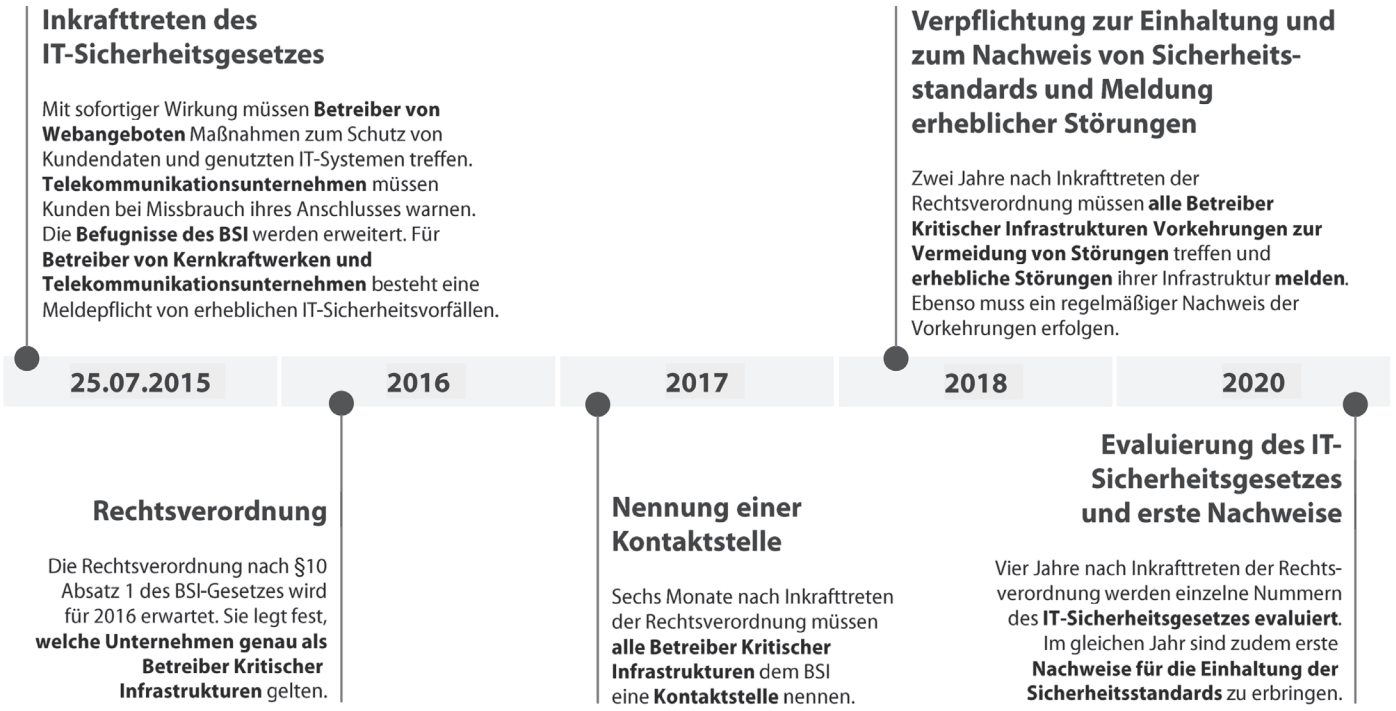

Abbildung 1: **Zeitliche und inhaltliche Agenda des IT-Sicherheitsgesetzes**

fenen Informationstechnik, der Art der betroffenen Einrichtung oder Anlage sowie zur Branche des Betreibers enthalten. Sofern die Störung nicht tatsächlich zu einem Ausfall oder einer Beeinträchtigung der Funktionsfähigkeit der Kritischen Infrastruktur geführt hat, kann die Meldung pseudonym (also etwa über einen Branchenverband) erfolgen; in sonstigen Fällen ist die Nennung des Betreibers erforderlich. Generell sind die Regelungen des Bundesdatenschutzgesetzes anzuwenden.[10]

Aus Sicht der Regierung ist die Meldepflicht eine sinnvolle Sache. Zum einen führt sie dazu, dass sich die betroffenen Unternehmen strukturiert mit den Sicherheitsvorfällen beschäftigen. Zum anderen können die Meldungen dazu dienen, ein Lagebild der Angriffe sowie Informationen über besonders betroffene Technologien oder Branchen zu erhalten. Eine zentrale Koordination kann so möglicherweise helfen, die Ursache für Angriffe zu finden, insbesondere wenn mehrere Unternehmen betroffen sind. Die Meldepflicht bildet jedoch nach wie vor einen großen Unsicherheitsfaktor für Unternehmen, vor allem im Hinblick auf die Frage, wie viele Meldungen tatsächlich vorgenommen werden müssen und welche Kosten dadurch entstehen. KPMG hat diesen Punkt im Rahmen der Studie „IT-Sicherheit in Deutschland" analysiert: Je nach Auslegung der Vorfallsdefinition kann demnach die Meldepflicht über alle Betreiber gesehen mehrere hunderttausend Meldungen im Jahr zur Folge haben. Auf Basis der vorgesehenen Meldepflichten im ersten Referentenentwurf des IT-Sicherheitsgesetzes schätzten die Studienautoren die Bürokratiekosten für die betroffenen Unternehmen auf bis zu 1,1 Mrd. Euro.[11]

Die im IT-Sicherheitsgesetz beinhalteten Meldepflichten sind von anderen gesetzlich festgeschriebenen Informationspflichten abzugrenzen. Das gilt insbesondere für § 42a BDSG, die „Informationspflicht bei unrechtmäßiger Kenntniserlangung von Daten". Die dort genannten meldepflichtigen Vorfälle dürften vielfach als IT-Sicherheitsvorfall im Sinne des IT-Sicherheitsgesetzes zu klassifizieren sein. Dabei muss berücksichtigt werden, dass es sich bei den Meldungsempfängern um unterschiedliche Adressaten handelt. So ist die Meldung gem. § 42a BDSG gegenüber der zuständigen Datenschutzaufsichtsbehörde sowie gegenüber dem Kreis der Betroffenen abzugeben. Bei einer Meldung nach den Vorgaben des IT-Sicherheitsgesetzes können dies hingegen – je nach Tatbestand – das BSI, der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, die Bundesnetzagentur bzw. die für Telemedienangebote zuständigen Landesbehörden sein.

Daher müssen betroffene Unternehmen sorgfältig prüfen, ob nicht in Einzelfällen mehrere Meldepflichten tangiert sind. Kommen die Unternehmen ihren Meldepflichten nicht nach, handeln sie ordnungswidrig und sind somit bußgeldpflichtig. Im Falle des § 42a BDSG kann die Geldbuße gem. § 43 II Nr. 7 BDSG in Verbindung mit § 43 II 1 BDSG bis zu 300 000 Euro betragen.[12]

4. Evaluierung

Das IT-Sicherheitsgesetz sieht nach Art. 10 die Evaluierung mehrerer Passagen vier Jahre nach Inkrafttreten der Rechtsverordnung vor. Konkret werden hierbei Art. 1, Nr. 2, 7 und 8 des IT-Sicherheitsgesetzes überprüft, was die Definition und Festlegung Kritischer Infrastrukturen, die Anforderungen an KRITIS-Betreiber sowie die Zuständigkeiten der einzelnen Bundesbehörden betrifft. Die Evaluierung wird unter Einbeziehung eines wissenschaftlichen Sachverständigen stattfinden, der im Einvernehmen mit dem Deutschen Bundestag bestellt wird.

5. Telemedien- und Telekommunikationsgesetz

Neben den Änderungen am BSI-Gesetz entfaltet das IT-Sicherheitsgesetz Wirkung auf einige spezialgesetzliche Regelungen. Dazu zählen

10 § 8a BSIG.

11 KPMG AG Wirtschaftsprüfungsgesellschaft: IT-Sicherheit in Deutschland, Handlungsempfehlungen für eine zielorientierte Umsetzung des IT-Sicherheitsgesetzes, 2014. http://www.bdi.eu/download_content/KPMG_IT-Sicherheit_in_Deutschland.pdf (Stand: 8.9.2015), S. 27–34.

12 Vgl. zu den ansonsten anfallenden Bußgeldern die Abschnitte „Telemedien- und Telekommunikationsgesetz" sowie „IT-Sicherheit und das Bußgeldrecht".

u. a. das Telemediengesetz (TMG) und das Telekommunikationsgesetz (TKG).

So sind gem. § 13 Abs. 5 TMG Anbieter gewerblicher Telemediendienste verpflichtet, durch technische und organisatorische Maßnahmen sicherzustellen, dass kein unerlaubter Zugriff auf die angebotenen Dienste möglich ist und dass diese gegen die Verletzung personenbezogener Daten sowie gegen Störungen gesichert sind. Diese Maßnahmen müssen unter Berücksichtigung des Stands der Technik implementiert werden. Einschränkend gilt jedoch, dass die Implementierung der Vorkehrungen dem Diensteanbieter auch technisch möglich und wirtschaftlich zumutbar sein muss. Laut Gesetz gilt dies z. B. für die Anwendung eines als sicher anerkannten Verschlüsselungsverfahrens.

Für Telekommunikationsanbieter ergibt sich aus dem IT-Sicherheitsgesetz u. a. eine erweiterte Befugnis zur Speicherung von Verkehrsdaten. Diese war vor Inkrafttreten des Gesetzes lediglich auf die Speicherung zur Bekämpfung von Störungen oder Fehlern an Kommunikationsanlagen beschränkt. Nun ist eine solche gem. § 100 Abs. 1 TKG ebenso zur Bekämpfung von Störungen und Fehlern zulässig, die zu einer Einschränkung der Verfügbarkeit von Informations- und Kommunikationsdiensten oder zu einem unerlaubten Zugriff auf Telekommunikations- und Datenverarbeitungssysteme der Nutzer führen können. Diese Neufassung sieht sich einiger Kritik ausgesetzt, da die Speicherung sogar im Falle potenzieller Störungen rechtmäßig ist. Kritische Stimmen sehen hierin eine versteckte Vorratsdatenspeicherung.[13]

Vergleichbar zu den Betreibern Kritischer Infrastrukturen wurden die Meldepflichten für Telekommunikationsanbieter erweitert. Insbesondere müssen gem. § 109 Abs. 5 Nr. 2 TKG sogar Störungen gemeldet werden, die potenziell zu beträchtlichen Funktionsbeeinträchtigungen führen können. Der Gesetzgeber betont dabei ausdrücklich, dass Störungen, die zu einer Einschränkung der Verfügbarkeit der über diese Netze erbrachten Dienste oder einem unerlaubten Zugriff auf Telekommunikations- und Datenverarbeitungssysteme der Nutzer führen können, ebenfalls von der Meldepflicht erfasst sind. Bleibt eine Meldung gem. § 109 Abs. 5 TKG aus, kann dies gem. § 149 Abs. 1 Nr. 21a TKG mit einer Geldbuße von bis zu 50 000 Euro geahndet werden.

Abschließend besteht nun gem. § 109a Abs. 4 TKG darüber hinaus die Pflicht, dass Diensteanbieter Nutzer unverzüglich zu benachrichtigen haben, wenn ihnen von Datenverarbeitungssystemen der Nutzer ausgehende Störungen bekannt sind. Darüber hinaus hat der Anbieter die Nutzer im Rahmen seiner Möglichkeiten auf angemessene, wirksame und technische zugängliche Mittel zur Beseitigung der Störung hinzuweisen.

V. Rolle des BSI

Das IT-Sicherheitsgesetz erweitert die Beratungsfunktion und Warnbefugnisse des BSI.[14] Rechtliche Grundlage hierfür sind entsprechende Änderungen des BSI-Gesetzes.

Das BSI fungiert als zentrale Meldestelle für die Sicherheit in der Informationstechnik des Bundes. Zu den vornehmlichen Aufgaben des BSI gehören insbesondere die zentrale Sammlung der zur Sicherstellung der Informationssicherheit erforderlichen Informationen sowie die Zusammenarbeit mit den anderen Bundesbehörden. Im Detail beinhaltet § 8b II BSIG die Verpflichtungen zur Sammlung und Auswertung von Informationen hinsichtlich von Gefahrenquellen für die IT-Sicherheit, die Analyse, inwieweit Betreiber Kritischer Infrastrukturen davon betroffen sind, die Erstellung eines Lagebilds zur Sicherheit in der Informationstechnik und die Unterrichtung betroffener Unternehmen sowie der zuständigen Behörden und Kontaktstellen. Die so gesammelten Informationen kann das BSI den übrigen Betreibern Kritischer Infrastrukturen in angemessener Form und unter Berücksichtigung von Quellen- und Geheimschutz sowie der Interessen des meldenden Betreibers zur Verfügung stellen. Somit erhalten auch die Betreiber durch die Meldung einen Mehrwert. Eine Meldung wird dabei lediglich öffentlich gemacht, wenn die Bekanntmachung im öffentlichen Interesse liegt und keine schutzwürdigen Interessen des Meldenden entgegenstehen. Zudem regelt § 8d BSIG, dass eine Weitergabe der gesammelten Informationen an Dritte nur auf Antrag und unter Berücksichtigung der Interessen der Betreiber Kritischer Infrastrukturen erfolgen darf. Zugang zu personenbezogenen Daten wird grundsätzlich nicht gewährt.

Darüber hinaus besitzt das BSI die Funktion eines Frühwarnsystems für die Öffentlichkeit bzw. die betroffenen Kreise. Als Anwendungsfälle dieser Funktion benennt § 7 Abs. 1 Nr. 1 BSIG die Warnung vor Sicherheitslücken in IT-Produkten und -Diensten, Schadprogrammen sowie im Falle des Verlusts oder unerlaubten Zugriffs auf Daten. Zur Bekämpfung dieser Gefahrenquellen kann das BSI zudem geeignete Sicherheitsmaßnahmen und -produkte empfehlen.

Abschließend ist das BSI befugt, auf dem Markt bereitgestellte bzw. dazu vorgesehene IT-Produkte und -Systeme zu untersuchen. Die daraus gewonnen Erkenntnisse dürfen vom BSI weitergegeben und veröffentlicht werden, soweit das zur Erfüllung seiner Aufgaben erforderlich ist und dem Hersteller des Produkts eine angemessene Frist zur Stellungnahmen eingeräumt wurde.

Kritische Stimmen befürchten diesbezüglich eine mangelnde Unabhängigkeit des BSI und fordern daher eine noch klarere Festlegung der Rolle des BSI.

VI. Weitere rechtliche Dimension

Da es sich beim IT-Sicherheitsgesetz lediglich um ein Änderungsgesetz handelt, kann es eine Vielzahl der rechtlichen Aspekte gar nicht erst abdecken. Vielmehr müssen schon bestehende Regelungen zusätzlich zum IT-Sicherheitsgesetz beachtet werden. Im Falle der Umsetzung etwaiger IT-Sicherheitsmaßnahmen gilt das insbesondere für das BDSG; aber auch „datenuntechnische" Gesetze, wie z. B. das OWiG, sind zu berücksichtigen.

1. IT-Sicherheit und das Bußgeldrecht

In den frühen Gesetzesentwürfen fehlte es dem IT-Sicherheitsgesetz gänzlich an originären Straf- und Bußgeldregelungen. Diese Tatsache gilt für Straftatbestände nach wie vor; jedoch wurden mit § 14 BSIG einige neue Bußgeldtatbestände konzipiert. Adressat der einzelnen Tatbestände sind jeweils die Betreiber Kritischer Infrastrukturen. Für die ebenfalls vom IT-Sicherheitsgesetz erfassten Anbieter von Teleme-

13 Vgl. dazu Deutscher Bundestag, PuK 2 – Parlamentsnachrichten: Kritik am IT-Sicherheitsgesetz, Innenausschuss/Öffentliche Anhörung, 20.4.2015, https://www.bundestag.de/presse/hib/2015_04/-/370702 (Abruf: 7.9.2015), S. 49 (C).

14 Zusätzlich werden auch die Ermittlungszuständigkeiten des BKA im Bereich der Computerdelikte gestärkt. Dies gilt insbesondere für den Fall von IT-Angriffen auf Einrichtungen des Bundes.

dien- bzw. Telekommunikationsdiensten gelten die jeweiligen Spezialregelungen des TMGs bzw. des TKGs.

§ 14 BSIG stellt vier Verstöße in den Vordergrund. Dazu gehören die fehlende oder mangelhafte Implementierung von Sicherheitsvorkehrungen, das Zuwiderhandeln gegenüber einer Anordnung des BSI im Falle von Sicherheitsmängeln, eine nicht vorschriftenkonforme Benennung einer Kontaktstelle gegenüber dem BSI sowie die ausbleibende oder mangelhafte Meldung von Störungen Kritischer Infrastrukturen, die zum Ausfall oder der Beeinträchtigung ihrer Funktionsfähigkeit geführt haben.

Die Verletzung dieser Regelungen ist gem. § 14 II BSIG mit Bußgeldern bis zu 50 000 Euro bewehrt. Lediglich wenn festgestellte Sicherheitsmängel trotz Aufforderung durch das BSI nicht beseitigt werden, kann die Geldbuße bis zu 100 000 Euro betragen. Neben diesen neu konzipierten Vorschriften beinhaltet das IT-Sicherheitsgesetz lediglich geringfügige Änderungen der Bußgeldtatbestände des TMG und des TKG, welche die mit dem IT-Sicherheitsgesetz verbundenen Änderungen berücksichtigen und ein Zuwiderhandeln gegen die jeweiligen Regelungen in den Bußgeldkatalog aufnehmen.

2. Haftung des Unternehmens und seiner Organe

Wie bereits dargestellt, sind neben den Bußgeldvorschriften des IT-Sicherheitsgesetzes insbesondere auch die Regelungen des OWiG zu berücksichtigen, da es sich bei Verstößen gegen die „originären" Bußgeldtatbestände des IT-Sicherheitsgesetzes um Ordnungswidrigkeiten handelt. Vor diesem Hintergrund sind in der Praxis insbesondere die §§ 30, 130 OWiG von Bedeutung.

§ 30 OWiG behandelt die Problematik der Verbandsgeldbuße. Grundsätzlich ist im deutschen Recht keine Kriminalstrafe für das Handeln von Unternehmen vorgesehen; jedoch kann eine Verbandsgeldbuße verhängt werden, wenn eine Leitungsperson des Verbands eine Ordnungswidrigkeit oder eine Straftat begangen und damit die den Verband betreffenden Pflichten verletzt hat. Das jeweilige Handeln wird dann dem Verband zugerechnet. § 30 OWiG erfasst unter dem Begriff der Leitungspersonen insbesondere Mitglieder der Organe juristischer Personen. Gem. § 30 I Nr. 5 OWiG sind zudem sonstige Leitungspersonen erfasst, die u.a. für die Überwachung der Geschäftsführung oder die Ausübung von Kontrollbefugnissen in leitender Stellung zuständig sein können. Die Ausübung von Kontrollbefugnissen ist so zu verstehen, dass die jeweilige Person durch diese Befugnis eine Führungsposition in der juristischen Person innehat.[15] Das kann auch für den Compliance-Officer (CO),[16] den Chief Information Officer (CIO) oder den IT-Sicherheitsbeauftragten gelten.

Da es sich bei § 30 OWiG nicht um einen eigenen Bußgeldtatbestand handelt, setzt die Sanktionierung eine Anknüpfungstat voraus. Hier kommen bspw. Verstöße gegen die Vorschriften des IT-Sicherheitsgesetzes in Betracht. Solche Verstöße sind als Verletzung einer den Verband betreffenden, sogenannten „betriebsbezogenen" Pflicht zu qualifizieren, da sie den Verband konkret als Normadressat betreffen.[17] Schließlich handelt es sich bei diesen Regelungen speziell um Vorschriften für Betreiber Kritischer Infrastrukturen bzw. Anbieter von Telemedien- bzw. Telekommunikationsdiensten. COs, CIOs oder IT-Sicherheitsbeauftragte müssen daher entsprechende Sorgfalt bei der Ausübung der mit dem IT-Sicherheitsgesetz verbundenen Pflichten walten lassen, da ansonsten Bußgelder drohen.

Die Geldbuße bemisst sich nach Charakter und Umständen der Tat. Hinsichtlich von Ordnungswidrigkeiten richtet sich das Höchstmaß der Geldbuße nach dem dort angedrohten Höchstmaß. Verweist das verletzte Gesetz jedoch auf § 30 OWiG, verzehnfacht sich das genannte Höchstmaß. Im Falle von Verstößen gegen das IT-Sicherheitsgesetz bliebe es somit bei den dort genannten 50 000 bzw. 100 000 Euro, da nicht auf § 30 OWiG verwiesen wird.

Vergleichbar zu § 30 OWiG befasst sich § 130 OWiG mit der Verletzung betriebsbezogener Pflichten, jedoch aus einem anderen Blickwinkel, da er auf die Aufsichtspflicht des Inhabers eines Unternehmens oder Betriebs abzielt. Inhaber im Sinne des § 130 OWiG sind etwa der Vorstand oder die Geschäftsführung eines Unternehmens oder Betriebs. Der Inhaber muss die erforderlichen Aufsichtsmaßnahmen treffen, um im Unternehmen oder Betrieb Zuwiderhandlungen gegen betriebsbezogene[18] Pflichten zu verhindern. Wie zuvor dargestellt, kommt in diesem Zusammenhang die Verletzung von im IT-Sicherheitsgesetz begründeten Pflichten in Betracht.

Die Aufsichtspflichten des Inhabers lassen sich vereinfacht in die Fallgruppen der Leitungspflichten, der Koordinations- und Organisationspflichten sowie der Kontroll- und Sanktionspflichten einteilen.[19] Die tatsächliche Zuwiderhandlung gegen eine betriebsbezogene Pflicht stellt eine sogenannte „objektive Bedingung der Ahndbarkeit" dar.[20] Ohne Gesetzesverstoß kann keine Strafe wegen Aufsichtspflichtverletzung erfolgen.

VII. Zulässigkeit von Logging- und Monitoringmaßnahmen – datenschutzrechtliche Aspekte

Bei der Implementierung von technischen und organisatorischen Maßnahmen im Sinne des IT-Sicherheitsgesetzes haben die Betreiber Kritischer Infrastrukturen die datenschutzrechtliche Relevanz einzelner Maßnahmen zu berücksichtigen, da in den meisten Fällen personenbezogene Daten tangiert sein werden. Dies gilt insbesondere für Logging- und Monitoringmaßnahmen, die zum Standardkanon der IT-Sicherheitsmaßnahmen zählen. Hier muss auf die personenbezogenen Daten Beschäftigter oder ggf. externer Administratoren zurückgegriffen werden.

Daher ist das datenschutzrechtliche Prinzip des Verbots mit Erlaubnisvorbehalt zu beachten. Dies bedeutet, dass die verantwortliche Stelle, also der Betreiber der Kritischen Infrastruktur, seine Maßnahme entweder auf die Einwilligung des Betroffenen oder einen Erlaubnistatbestand stützen können muss, um die Zulässigkeit der Maßnahme zu gewährleisten.

1. Die Einwilligung

Die Einwilligung ist in § 4a BDSG geregelt. Grundsätzlich kann sie für jede Art des Umgangs mit Daten eingeholt werden, solange sie auf der freien Entscheidung des Betroffenen beruht. Der Aspekt der Frei-

15 Vgl. *Rogall*, in: Karlsruher Kommentar zum OWiG, 4. Aufl. 2014, § 30, Rn. 84.
16 Vgl. *Meyberg*, in: Beck'scher Online-Kommentar zum OWiG, 8. Edition, § 30, Rn. 53.
17 Vgl. *Meyberg*, in: Beck'scher Online-Kommentar zum OWiG, 8. Edition, § 30, Rn. 80.
18 Eine Tat gilt dann als betriebsbezogen, wenn das Delikt z.B. aus „vermeintlich" betrieblichem Anlass, unter Ausnutzung betrieblicher Infrastruktur oder als Ausdruck von Handlungen in Wahrnehmung der Interessen und Aufgaben des Unternehmens verübt wurde.
19 Vgl. dazu detaillierter *Rogall*, in: Karlsruher Kommentar zum OWiG, 4. Aufl. 2014, § 130, Rn. 53 ff.
20 Vgl. *Rogall*, in: Karlsruher Kommentar zum OWiG, 4. Aufl. 2014, § 130, Rn. 77 f.

willigkeit ist jedoch bei Einwilligungen im Beschäftigungsverhältnis umstritten.[21] Daher muss im Einzelfall sorgsam geprüft werden, ob die Einwilligung tatsächlich freiwillig erfolgt und damit wirksam ist.

2. Die Erlaubnistatbestände des BDSG

Neben der Einwilligung sind verschiedene Erlaubnistatbestände des BDSG anwendbar.

Bei der Einrichtung von IT-Sicherheitsmaßnahmen, insbesondere der von technischen und organisatorischen Maßnahmen im Sinne des BDSG, ist zunächst § 28 Abs. 1 1 Nr. 2 BDSG zu berücksichtigen. Demnach ist die Verarbeitung personenbezogener Daten zur Wahrung berechtigter Interessen zulässig, solange kein Grund zur Annahme besteht, dass Interessen des Betroffenen an der Verarbeitung überwiegen. Berechtigtes Interesse ist dabei jedes von der Rechtsordnung gebilligte Interesse.[22] In diesem Fall dürfte dies auf die Beachtung von IT-Sicherheitsaspekten zutreffen. Da es sich sogar um gesetzlich geforderte Maßnahmen handelt, dürften keine überwiegenden Interessen der Betroffenen die Verarbeitung ausschließen. Selbiges gilt für Loggingmaßnahmen zur Datenschutzkontrolle, Datensicherung oder der Sicherstellung eines ordnungsgemäßen Betriebs.

Sofern die initial erhobenen Logging- und Monitoringdaten zu einem späterem Zeitpunkt bei Verdacht eines IT-Sicherheitsvorfalls ausgewertet werden, wäre ebenso § 28 I 1 Nr. 2 BDSG einschlägig, soweit es sich bei den Betroffenen, deren personenbezogene Daten zwecks Aufdeckung und Aufklärung genutzt werden, um Externe bzw. Unternehmensinterne handelt, die nicht vom Begriff des „Beschäftigten" gem. § 3 Abs. 11 BDSG erfasst sind.

Für Maßnahmen mit Bezug zu Beschäftigtendaten ist der Spezialtatbestand des § 32 BDSG zu beachten. Nach § 32 I 1 BDSG ist Erhebung, Verarbeitung und Nutzung personenbezogener Daten zulässig, wenn sie zu Zwecken des Beschäftigungsverhältnisses erforderlich ist. Im Falle von Logging- und Monitoringmaßnahmen wäre dies bspw. das Interesse an der Vorbeugung von Gesetzesverstößen durch die Beschäftigten. Zu nennen wären exemplarisch Maßnahmen zur Zugriffs- oder Weitergabekontrolle nach Anlage zu § 9 BSG, Nr. 3 und 4. Das Merkmal der Erforderlichkeit setzt eine Abwägung der Interessen des Arbeitgebers gegenüber denen des Beschäftigten voraus. Zudem ist der Arbeitgeber dazu verpflichtet, die Beeinträchtigung des Beschäftigten bspw. durch Anonymisierung oder Pseudonymisierung möglichst gering zu halten.

Satz 2 des § 32 Abs. 1 BDSG befasst sich mit der Verarbeitung von Beschäftigtendaten bei konkretem Straftatverdacht. Ein Beispiel wäre etwa der Verdacht des unbefugten Zugriffs auf Geschäfts- und Betriebsgeheimnisse zwecks Weitergabe an Dritte. In diesem Fall ist insbesondere der Verhältnismäßigkeitsgrundsatz zu beachten. Das Ausmaß der eingesetzten Aufklärungsmaßnamen hat sich an der Schwere der Tat des Verdächtigen zu orientieren. Die Beeinträchtigung des jeweils Betroffenen ist so gering wie möglich – und erforderlich – zu halten.[23]

3. Besondere Zweckbindung personenbezogener Daten gem. § 31 BDSG

Neben den genannten Erlaubnistatbeständen ist § 31 BDSG bei der Durchführung von Logging- und Monitoringmaßnahmen zu berücksichtigen, der den Grundsatz der besonderen Zweckbindung vorgibt. Demnach dürfen personenbezogene Daten, die ausschließlich zu Zwecken der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung des ordnungsgemäßen Betriebs einer Datenverarbeitungsanlange gespeichert werden, nur für diese Zwecke verarbeitet werden. Da zur Sicherstellung des ordnungsgemäßen Betriebs jedoch auch die Identifikation von Störern und Angreifern sowie unsachgemäßer Nutzung der Datenverarbeitungsanlagen zählt, dürften diese Protokolldaten in der Regel für Monitoringmaßnahmen genutzt werden, wenn sie aus diesen Gründen veranlasst wurden.

VIII. Das IT-Sicherheitsgesetz und KMU

Was kleine und mittlere Unternehmen (KMU) betrifft, so besteht bei der Implementierung von Sicherheitsmaßnahmen schon allein im Hinblick auf deren wirtschaftliche Bedeutung erhöhter Handlungsbedarf. 99,3 % der deutschen Unternehmen zählen in die Kategorie der KMU, und mehr als 60 % der Beschäftigten sind in KMU tätig. „Trotz eines erhöhten Bewusstseins für IT-Sicherheit 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."[24]

1. Sicherheitslage von KMU

Die Bedrohung, dass IT-bedingte Sicherheitsrisiken mittelfristig zunehmen, schätzt fast jedes zweite KMU als hoch oder sehr hoch ein. Auch die Einschätzung des Schutzbedarfs spiegelt ein hohes Bewusstsein für Cyberrisiken wider.[25] Dennoch sieht der größte Teil der KMU in Cyberkriminalität kein ernstzunehmendes Risiko. Dies geht aus einer von Zurich im Sommer 2014 durchgeführten Umfrage unter KMU hervor. Wie die Umfrage zeigt, gehören digitale Angriffe für nur 9 % der befragten KMU zur potenziellen Risikoeinschätzung (6 % in 2013). Damit zählt Cyberkriminalität weiterhin zu den als am geringsten eingestuften Risiken.

Hingegen hat die Angst vor Imageschäden deutlich zugenommen. So hat sich die Anzahl der KMU, die bspw. negative Schlagzeilen in den Medien als ihr größtes Risiko einschätzen, im Vergleich zum Vorjahr mit 16 % nahezu verdreifacht. Auch der Einsatz neuer Technologien wird durch KMU zunehmend als für den Unternehmenserfolg bedeutsam bewertet; nach der Strukturdatenerhebung des BMWi nutzt der Großteil der KMU IT-Anwendungen wie E-Mail, Online-Banking, kaufmännische Software für das Rechnungswesen und nutzt elektronische Kommunikationswege zur Übersendung von Steuer- und Beitragsdaten oder zum Datenaustausch mit Kunden und Lieferanten. Nicht nur im Bereich der Informationsverarbeitung, sondern auch in der Außendarstellung und der Marktkommunikation spielt IKT für KMU inzwischen eine un-

21 Vgl. dazu ausführlicher *Gola/Klug/Körffer*, in: Gola/Schomerus, Bundesdatenschutzgesetz, 12. Aufl. 2015, § 4a, Rn. 19 ff.
22 Vgl. *Wolff*, in: Beck 'scher Online-Kommentar Datenschutzrecht, 13. Edition, § 28, Rn. 59.
23 Zu weiteren Einzelheiten und m. w. N. *Scheben/Geschonneck/Klos*, CCZ 2012, 13, 15.
24 KPMG AG Wirtschaftsprüfungsgesellschaft: IT-Sicherheit in Deutschland, Handlungsempfehlungen für eine zielorientierte Umsetzung des IT-Sicherheitsgesetzes, 2014. http://www.bdi.eu/download_content/KPMG_IT-Sicherheit_in_Deutschland.pdf (Stand: 8.9.2015), S. 7.
25 Bundesministerium für Wirtschaft und Energie (BMWi): IT-Sicherheitsniveau in kleinen und mittleren Unternehmen, Studie im Auftrag des Bundesministeriums für Wirtschaft und Technologie, 2012. http://www.bmwi.de/BMWi/Redaktion/PDF/S-T/studie-it-sicherheit,property=pdf,bereich=bmwi2012,sprache=de,rwb=true.pdf (Abruf: 7.9.2015), S. 17–19.

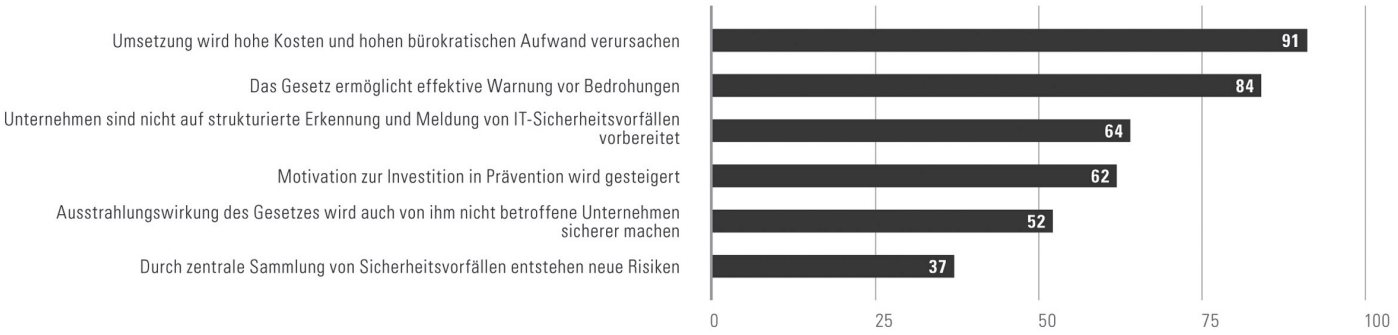

Abbildung 2: **Erwartungen an das IT-Sicherheitsgesetz, in % (Quelle: KPMG 2015, S. 38)**

entbehrliche Rolle. In Summe setzen 99,7 % aller KMU in Deutschland für ihre Geschäftsprozesse IT ein.[26]

Diese gegenläufigen Einschätzungen belegen, „dass das Risikobewusstsein in Bezug auf die Auswirkungen von Cyberangriffen bei deutschen KMU nur schwach ausgeprägt ist. […] Vielen Unternehmern ist das Ausmaß eines Cyberangriffs nicht bewusst“ [27]. Die fast vollständige Verbreitung von IT-Systemen in KMU führt jedoch dazu, dass technische Risiken, unbewusstes Fehlverhalten, Nachlässigkeit oder mangelnde IT-Kenntnisse mit Bezug auf die Verfügbarkeit und die Stabilität von Geschäftsprozessen existenzgefährdend sein können.[28] In Anbetracht der „hohen einzelwirtschaftlichen Bedeutung der IT erscheint das IT-Sicherheitsniveau der KMU in Deutschland als weiterhin stark verbesserungsbedürftig. Zwar ist ein hohes Bewusstsein für die Relevanz des Themas IT-Sicherheit vorhanden und ein gewisses Niveau von technischen Maßnahmen nahezu flächendeckend erreicht. Es mangelt aber an organisatorischen und personellen Maßnahmen sowie an der Einsicht, dass Vorfälle im IT-Bereich elementare Prozesse der Geschäftstätigkeit dauerhaft stören können und dass IT-Sicherheitsroutinen zwingend etabliert sowie definierte Abläufe bei Notfällen vorhanden sein sollten.“[29]

Daher sollten auch KMU vermehrt auf die Einführung einer geeignete IT-Sicherheitsorganisation setzen, z. B. im Rahmen eines ISMS. Dieses erweitert die vorhandenen technischen Maßnahmen um organisatorische und personelle Aspekte, welche aktuell in KMU kaum als defizitär wahrgenommen werden, obwohl sie häufig gar nicht oder nur rudimentär vorhanden sind. „Zwischen 30 % und 68 % aller KMU geben an, die jeweiligen Maßnahmen für nicht erforderlich zu halten.“[30] Das wird an zahlreichen Beispielen deutlich. So nutzen ca. 95 % der KMU Mobilfunkgeräte; doch nur in 36 % der Fälle erfolgt die Organisation durch ein zentrales Gerätemanagement. 70 % aller KMU haben noch nie eine IT-Sicherheitsanalyse durchgeführt. Notfallpläne sind nur in 43 % aller KMU vorhanden.

2. Auswirkungen und Herausforderungen des IT-Sicherheitsgesetzes

Aufgrund ihrer Größe und damit verbunden ihrer Kritikalität fallen KMU vermutlich nur in Ausnahmefällen direkt unter das IT-Sicherheitsgesetz. Daher müssen sie die Anforderungen an die IT-Sicherheit voraussichtlich auch nur in wenigen Fällen zwingend erfüllen.

Das IT-Sicherheitsgesetz verpflichtet Unternehmen oder Unternehmensverbünde, die einen maßgeblichen Anteil an der Verfügbarkeit einer Kritischen Infrastruktur halten. In vielen Szenarien wirkt sich dies faktisch auch auf KMU aus, die als Zulieferer oder Dienstleister für größere Unternehmen agieren, beispielsweise als IT-Dienstleister im Gesundheitssektor. Daher ist damit zu rechnen, dass KRITIS-Betreiber die per Gesetz entstehenden Anforderungen an ihre Dienstleister durchreichen, wodurch die Einhaltung gewisser Sicherheitsstandards aufgrund ihrer mittelbaren Funktion in Liefer- und Dienstleistungsketten auch von KMU gefordert wird.

Auch durch die im IT-Sicherheitsgesetz begründeten Änderungen des Telemediengesetzes (TMG) sind KMU betroffen. Die Änderungen betreffen dabei Anbieter von Telemedien, d. h. unter anderem Anbieter von Online-Angeboten, die über das Internet abrufbar sind. Diese müssen, soweit dies technisch möglich und wirtschaftlich zumutbar ist, durch technische und organisatorische Vorkehrungen sicherstellen, dass kein unerlaubter Zugriff auf die für ihre Telemedienangebote genutzten technischen Einrichtungen möglich ist und diese gegen Verletzungen des Schutzes personenbezogener Daten sowie gegen Störungen, auch soweit sie durch äußere Angriffe bedingt sind, gesichert sind. Das IT-Sicherheitsgesetz verweist an dieser Stelle insbesondere auf die Anwendung eines als sicher anerkannten Verschlüsselungsverfahrens.[31]

Konkret bedeuten die Änderungen des TMG, dass z. B. ein Mittelständler, der eine Webseite betreibt und diese nicht angemessen absichert, worauf in Folge die Vertraulichkeit personenbezogener Daten verletzt wird, gegen das TMG verstößt und mit entsprechenden Rechtsfolgen rechnen muss. Dies könnte insbesondere die Existenz kleiner Mittelständler bedrohen.

Bei der Angleichung von Risikobewusstsein und den entsprechenden Investitionen im Rahmen einer adäquaten Umsetzung von IT-Sicherheitsmaßnahmen sind die Höhe der Kosten, einschließlich des Zeitaufwandes sowie die Verfügbarkeit von qualifiziertem Personal, immer noch die größten Barrieren für KMU.[32] Sie stehen daher vor der Herausforderung, eine bedarfsgerechte und schlanke IT-Sicherheitsorganisation einzuführen. Abbildung 2 zeigt die Ergebnisse einer Umfrage durch KPMG im Rahmen der e-Crime-Studie 2015 (KPMG AG Wirtschaftsprüfungsgesellschaft: e-Crime, Computerkriminalität in der deutschen Wirtschaft, 2015, https://www.kpmg.com/DE/de/Documents/e-crime-studie-2015.pdf [Stand: 29.9.2015]), bei der Unternehmen nach ihren Erwartungen an das IT-Sicherheitsgesetz gefragt wurden. Dabei zeigt sich, dass das IT-Sicherheitsgesetz in erster Linie als bürokratisch und teuer beurteilt wird. Auch wird die Meldepflicht

26 BMWi (Fn. 25), S. 1, 14.
27 Zurich Gruppe Deutschland: Zurich Studie: KMU wähnen sich in Bezug auf Cyber-Kriminalität sicher, 25.11.2014. http://www.zurich.de/de-de/ueber-uns/presse/aktuell/aktuelle-veroeffentlichungen/2014/cyber-kriminalitaet (Stand: 8.9.2015).
28 BMWi (Fn. 25), S. 15.
29 BMWi (Fn. 25), S. 2.
30 BMWi (Fn. 25), S. 25.
31 § 13 Abs. 7 TMG.
32 BMWi (Fn. 25), S. 60.

in der aktuell vorgesehenen Form als nicht wirklich hilfreich bewertet: So ist nicht nachvollziehbar, was durch die Meldepflicht bezweckt wird und in welcher Relation dieser Zweck zum bei den betroffenen Unternehmen notwendigen Aufwand steht; die Meldepflicht wirkt zunächst vielmehr wie ein bürokratisches Monster. Wie dargestellt, wird sich insbesondere der IT-Mittelstand der Meldepflicht in vielen Bereichen nicht entziehen können, da er fest in Lieferketten von Krankenhäusern, Banken, Energieversorgern etc. eingebunden ist.

Eine weitere Auswirkung des IT-Sicherheitsgesetzes betrifft insbesondere IT-Mittelständler, die in der Entwicklung informationstechnischer Produkte und Systeme tätig sind. So erlangt das BSI per Gesetz die Berechtigung, sowohl bereitgestellte als auch zur Bereitstellung auf dem Markt vorgesehene Produkte und Systeme zu untersuchen und die aus den Untersuchungen gewonnenen Erkenntnisse weiterzugeben und zu veröffentlichen, sofern dies für die Abwehr von Gefahren für die Sicherheit der Informationstechnik des Bundes, die Beratung und Warnung der Stellen des Bundes, der Länder sowie der Hersteller, Vertreiber und Anwender in Fragen der Sicherheit in der Informationstechnik unter Berücksichtigung der möglichen Folgen fehlender oder unzureichender Sicherheitsvorkehrungen sowie die Aufgaben nach den §§ 8a und 8b als zentrale Stelle für die Sicherheit in der Informationstechnik Kritischer Infrastrukturen notwendig ist. Diese gesetzlich verankerte Berechtigung zur Prüfung von Produkten und Systemen mit Bewertung der IT-Sicherheit kann ggf. zu Reputationsschäden für die betroffenen Unternehmen führen.

Vor dem Hintergrund des aktuell debattierten Richtlinienentwurfs der Europäischen Kommission zur Netz- und Informationssicherheit (NIS Directive), deren Verabschiedung für Ende 2015 erwartet wird, bleibt weiterhin abzuwarten, ob das IT-Sicherheitsgesetz und die NIS-Richtlinie ausreichend aufeinander abgestimmt sein werden. Auch stellt sich die Frage nach der Notwendigkeit eines nationalen IT-Sicherheitsgesetzes. Da die NIS-Richtlinie das europäische Äquivalent zum IT-Sicherheitsgesetz darstellt, bestünde bei Widersprüchen insofern Anpassungsbedarf am IT-Sicherheitsgesetz. Diese befürchteten Änderungen würden vor allem KMU belasten, die aufgrund ihrer personellen und finanziellen Mittel nur schlecht mit unterschiedlichen Rechtsrahmen umgehen bzw. sich entsprechend aufstellen können.

IX. Fazit

Innenminister *Thomas de Maizière* hat ein ehrgeiziges Ziel: Er will Deutschlands IT-Systeme zu den sichersten der Welt machen. Eine verpflichtende Grundlage schafft in vielen Branchen die Notwendigkeit für die vielleicht längst überfälligen Detaildiskussionen zu mehr IT-Sicherheit. Dass der IT-Sicherheit und deren Gefährdungen in Form von Cyberangriffen und ähnlichem mehr Aufmerksamkeit geschenkt werden muss, ist unbestritten; der aktuelle Vorfall im deutschen Bundestag ist nur ein Beispiel hierfür.

Aus Sicht der Regierung ist auch die Meldepflicht eine sinnvolle Sache. So ließe sich mit den Meldungen ein umfassendes Bild der Gefährdungslage erstellen. Der deutschen Wirtschaft – und hier insbesondere den KMU mit eher wenig eigenem Know-how und Ressourcen – hilft die Pflicht jedoch nur, wenn das BSI Meldungen nicht nur entgegennimmt, sondern auch auswertet und den Betreibern von Kritischen Infrastrukturen zeitnah Informationen und Unterstützung zur Verfügung stellt. Dass das BSI dazu aktuell weder fachlich noch personell in der Lage ist, ist den meisten Beteiligten bewusst. Im Rahmen des Gesetzes werden nicht ohne Grund über 100 neue Stellen sowie Sachmittel für das BSI diskutiert.

Aus dem IT-Sicherheitsgesetz entstehende Mehrwerte für einzelne Unternehmen oder Unternehmensgruppen zu erwarten, ist grundsätzlich zunächst schwierig. Ein höheres Sicherheitsniveau bedeutet aber sowohl für Privatpersonen als auch für kleine oder große Wirtschaftsteilnehmer eine generelle Verbesserung. Dafür sollte das IT-Sicherheitsgesetz jedoch konkretisiert und näher an der Lebenswirklichkeit der Unternehmen ausgerichtet werden, was durch die noch zu erlassende Rechtsverordnung gelöst werden müsste.

Für KMU kann das IT-Sicherheitsgesetz als eine Hilfe zum Selbstschutz verstanden werden. Aktuell weisen KMU vor allem im Bereich der geschäftskritischen IT-Sicherheitsprozesse deutliche Schwächen auf, das heißt bei der Bewertung von Gefahrenbereichen, im Umgang mit Sicherheisfällen und beim Notfallmanagement. Ergreifen die Unternehmen präventive Maßnahmen zur Absicherung vor Cyberrisiken auf ganzheitlicher, d. h. sowohl technischer, organisatorischer als auch personeller Ebene, sind sie nicht nur gegen die Schäden von Cyberangriffen und Ausfällen geschützt, sondern auch gut aufgestellt bezüglich der aus dem IT-Sicherheitsgesetz entstehenden Anforderungen. Natürlich ist jedes Unternehmen selbst für die Umsetzung von angemessenen Sicherheitsmaßnahmen verantwortlich. Die Praxis zeigt allerdings, dass dieser Aspekt häufig entweder aus Unwissen oder aus Kalkül anderen Themen untergeordnet wird. Freiwillige Selbstverpflichtungen, sowohl der Wirtschaft als auch der öffentlichen Hand, haben in der Vergangenheit nicht den gewünschten Erfolg gebracht. Nachweisbare Sicherheit im Rahmen des IT-Sicherheitsgesetzes bietet nun die Chance, sowohl für Unternehmen als auch für den gesamten Standort Deutschland zu einem Aushängeschild werden.

Hanna Lurz ist Senior Consultant bei KPMG. Sie berät Unternehmen und Einrichtungen aus verschiedenen Sektoren und behandelt häufig interdisziplinäre Fragestellungen der Informationssicherheit. Ihre Schwerpunkte sind organisatorische IT-Sicherheit, Kritische Infrastrukturen (KRITIS) und Security Awareness.

Barbara Scheben, RAin, ist Partner bei KPMG. Ihr Tätigkeitsschwerpunkt liegt auf der Durchführung forensischer Sonderuntersuchungen sowie der Beratung zu Compliance, Datenschutz und der Unterstützung bei IT-Sicherheits- und Cybercrimevorfällen im Hinblick auf datenschutzrelevante Fragestellungen.

Wilhelm Dolle ist Partner bei KPMG. Zu seinen Arbeitsbereichen gehören IT-Strategie, Risiko- und Sicherheitsanalysen, Informationssicherheitsmanagementsysteme sowie Fragestellungen zu Penetrationstests und digitaler Forensik. Zudem beschäftigt er sich intensiv mit regulatorischen Anforderungen an die Informationssicherheit und das IT-Risikomanagement.