06.15

ZIR

Zeitschrift Interne Revision

50. Jahrgang
Dezember 2015
Seiten 241–292

www.ZIRdigital.de

Fachzeitschrift für Wissenschaft und Praxis

Herausgeber:
DIIR Deutsches Institut für Interne Revision e.V.

Standards · Regeln · Berufsstand

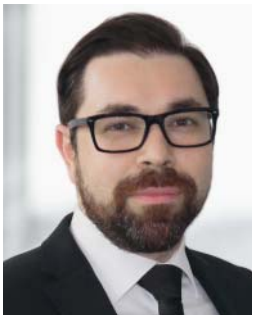
Management · Best Practice · Arbeitshilfen

ESV ERICH SCHMIDT VERLAG

20380

MICHAEL GOLDSHTEYN · MICHAEL ADELMEYER

Die Auswirkungen des IT-Sicherheitsgesetzes auf die Interne Revision



Michael Goldshteyn, *Diplom-Wirtschaftsjurist (FH), CISA, ist als Manager bei der Baker Tilly Roelfs AG Wirtschaftsprüfungsgesellschaft, Düsseldorf tätig.*

Michael Adelmeyer, *M.Sc., CISA, ist als IT-Revisor bei der Baker Tilly Roelfs AG Wirtschaftsprüfungsgesellschaft, Düsseldorf tätig.*

Die Sicherheit und der Schutz von IT-Systemen gewinnen in der heutigen Unternehmenslandschaft zunehmend an Bedeutung. Aus diesem Grund hat der Gesetzgeber das IT-Sicherheitsgesetz verabschiedet. Hierdurch soll eine signifikante Verbesserung der Sicherheit informationstechnischer Systeme herbeigeführt und Kritische Infrastrukturen besser vor Cyberangriffen geschützt werden. Nach einer Darstellung der Änderungen und ihrer kritischen Würdigung wird der Frage nachgegangen, welche Auswirkungen die Gesetzesnovelle auf die Unternehmen selbst und die Arbeit der Internen Revision entfaltet. Anschließend werden Handlungsempfehlungen ausgesprochen.
Dieser Beitrag spiegelt die persönliche Auffassung der Autoren wider.

1. Einleitung

Der Deutsche Bundestag hat am 17. Juli 2015 das IT-Sicherheitsgesetz verabschiedet[1]. Es soll Mindeststandards für die IT-Sicherheit setzen und hierdurch eine erhebliche Verbesserung der Sicherheit informationstechnischer Systeme herbeiführen. Um dieses Ziel zu erreichen, sind zahlreiche Prüfungs- und Meldepflichten bei Betreibern sog. „Kritischer Infrastrukturen" vorgesehen. Hierbei handelt es sich um Unternehmen aus den Branchen Transport und Verkehr, Gesundheit, Wasser, Ernährung sowie dem Finanz- und Versicherungswesen. Sie müssen angemessene organisatorische und technische Vorkehrungen treffen, um Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu vermeiden. Damit einhergehend sind die Betreiber auf die Einhaltung demnächst zu veröffentlichender Branchenstandards sowie der Erbringung eines regelmäßigen Nachweises über die getroffenen Maßnahmen verpflichtet. Sofern dabei sog. „erhebliche Störungen" der Systeme festgestellt werden, sind sie an das Bundesamt für Sicherheit in der Informationstechnik zu melden.

Im Rahmen dieses Aufsatzes werden zunächst die gesetzlichen Anforderungen dargestellt. In dem Zusammenhang werden etwaige Konkretisierungen und Ergänzungen zur Gesetzeslage bzw. zum Regelungsstand näher beleuchtet. Aufgrund des begrenzten Umfangs der Ausarbeitung wird die Gesetzesänderung nicht in all ihren Ausprägungen besprochen. Spezialgesetzliche Regelungen (z. B. für die Telekommunikationsbranche) und die Pflichten des BSI bleiben außen vor. Darauf aufbauend werden abschließend Hinweise auf kurzfristigen Handlungsbedarf aufgezeigt. Hierbei werden auch die Auswirkungen auf die Interne Revision analysiert und gewürdigt.

2. Das IT-Sicherheitsgesetz

2.1 Anwendungsbereich

Die Novelle betrifft primär sog. Kritische Infrastrukturen (KRITIS). Gemäß § 2 Abs. 10 S. 1 BSIG handelt es sich bei einer Kritischen Infrastruktur um eine Einrichtung, eine Anlage oder Teile eines Unternehmens, die zu einem der nachfolgend aufgeführten Sektoren bzw. Bereiche zählen.

Sektor Energie

- Stromversorgung (Branche: Elektrizität)
- Versorgung mit Erdgas (Branche: Gas)

1 Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz), BGBl. I 2015, S. 1324 ff.

- Versorgung mit Mineralöl (Branche: Mineralöl)

Sektor Informationstechnik und Telekomunikation
- Sprach- und Datenkommunikation (Branchen: Telekommunikation, Informationstechnik)
- Verarbeitung und Speicherung von Daten (Branche: Informationstechnik)

Sektor Transport und Verkehr
- Transport von Gütern (Branchen: Luftfahrt, Seeschifffahrt, Binnenschifffahrt, Schienenverkehr, Straßenverkehr, Logistik)
- Transport von Personen im Nahbereich (Branchen: Seeschifffahrt, Binnenschifffahrt, Schienenverkehr, Straßenverkehr, Logistik)
- Transport von Personen im Fernbereich (Branchen: Luftfahrt, Seeschifffahrt, Binnenschifffahrt, Schienenverkehr, Straßenverkehr, Logistik)

Sektor Gesundheit
- Medizinische Versorgung (Branchen: medizinische Versorgung, Labore)
- Versorgung mit Arzneimitteln und Medizinprodukten (Branchen: medizinische Versorgung, Labore, Arzneimittel und Impfstoffe)

Sektor Wasser
- Trinkwasserversorgung (Branche: öffentliche Wasserversorgung)
- Abwasserbeseitigung (Branche: öffentliche Abwasserbeseitigung)

Sektor Ernährung
- Versorgung mit Lebensmitteln (Branchen: Ernährungswirtschaft, Lebensmittelhandel)

Sektor Finanz- und Sicherheitswesen
- Zahlungsverkehr, Zahlungsdienstleistungen durch Überweisung, Zahlungskarten und E-Geld (Branchen: Banken, Finanzdienstleister)
- Bargeldversorgung (Branche: Banken)
- Kreditvergabe (Branche: Banken, Finanzdienstleister)
- Geld- und Devisenhandel (Branche: Börsen, Banken, Zahlungsdienstleister)
- Wertpapier- und Derivatehandel (Branche: Börsen, Banken, Zahlungsdienstleister)
- Versicherungsleistungen (Branche: Versicherungen)

Über die Zugehörigkeit zu einem der aufgeführten Bereiche hinaus muss die Kritische Infrastruktur auch von hoher Bedeutung für das Funktionieren des Gemeinwesens sein. Dies ist der Fall, wenn ihr totaler bzw. partieller Ausfall Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit nach sich zieht. Das gleiche gilt auch für die Beeinträchtigung der vorgesehenen Aufgabenerfüllung. Sollten diese Tatbestandsmerkmale zutreffen, ist davon auszugehen, dass der Kritischen Infrastruktur eine besondere Bedeutung bei der Sicherung von Grundbedürfnissen der Bevölkerung beizumessen ist und sie hierdurch eines Schutzes bedarf.[2] Die Abgrenzung folgt grundsätzlich der Definition des Bundesamtes für Bevölkerungsschutz und Katastrophenhilfe und war notwendig, da bislang keine Legaldefinition des Begriffes existierte und damit einhergehend keine Abgrenzung der Normadressaten erfolgen konnte.[3]

Kritische Infrastrukturen haben eine besondere Bedeutung für die Sicherung von Grundbedürfnissen der Bevölkerung und bedürfen daher eines besonderen Schutzes.

Im Verlauf des Gesetzgebungsverfahrens musste auch der Umstand berücksichtigt werden, dass technische Entwicklungen, kulturelle und gesellschaftliche Einflussfaktoren sowie die während der Umsetzung der Vorgaben noch zu sammelnden Erfahrungen weitere Modifikationen und Anpassungen der Definition einer Kritischen Infrastruktur nach sich ziehen könnten. Aus diesen Gründen wurde das Bundesministerium des Innern mit § 10 Abs. 1 BSIG ermächtigt, eine Rechtsverordnung zu erlassen. Sie flankiert zukünftig die Gesetzesnovelle und konkretisiert die Vorgehensweise zur Identifikation Kritischer Infrastrukturen und ihrer Betreiber durch objektive Beurteilungskriterien, um hierdurch dem Erfordernis der hinreichenden Bestimmtheit der Normadressaten Rechnung zu tragen.[4] Über die bloße Konkretisierung der systemischen Definition Kritischer Infrastrukturen hinaus, soll sie insb. auch Kriterien zur Bestimmung von Einrichtungen, Anlagen oder Teilen eines Unternehmens

2 Vgl. BT-Drs. 18/4096, S. 23.
3 Vgl. BT-Drs. 18/4096, S. 23.
4 Vgl. BT-Drs. 18/5121, S. 16.

enthalten, um sie als Kritische Infrastruktur im Sinne des BSI-Gesetzes einzuordnen. Die Verabschiedung soll zeitnah erfolgen und bedarf keiner Zustimmung des Bundesrates. Bei ihrer Abfassung sind jedoch Vertreter der Wissenschaft, die betroffenen Betreiber und die entsprechenden Wirtschaftsverbände sowie die zuständigen Bundesministerien anzuhören.

Sicherungsmechanismen sind zu implementieren, wenn die Informationstechnik Einfluss auf die Erbringung der kritischen Dienstleistung entfaltet.

Als Maßstab für die Einordnung dienen die Bedeutung der als kritisch anzusehenden Dienstleistung sowie die mit ihrem Ausfall oder einer Beeinträchtigung einhergehenden Konsequenzen für die Funktionsfähigkeit des Gemeinwesens. Eine Dienstleistung soll zukünftig als kritisch im Sinne des BSIG gelten, wenn sie Folgen für die Sicherheit von Leib, Leben, Gesundheit und Eigentum der vom Ausfall unmittelbar oder mittelbar betroffenen Teile der Bevölkerung entfaltet.[5] Um die aus der Beeinträchtigung resultierenden Konsequenzen festzulegen, soll ein branchenspezifischer Schwellenwert, welcher sich an der Anzahl betroffener Personen ausrichtet, für jede kritische Dienstleistung im entsprechenden Sektor ermittelt werden. Die Schwellenwerte werden in Zusammenarbeit mit Vertretern der betroffenen Kritischen Infrastrukturen sowie durch Konsultation externer Sachkundiger, insb. der Verwaltung, Wirtschaft und Wissenschaft, erarbeitet werden.

2.2 Anforderungen an die IT-Sicherheit

Wie im Abschnitt 2.1 ausgeführt, werden Kritische Infrastrukturen erst mit dem Inkrafttreten der Rechtsverordnung abschließend definiert. Daran anknüpfend wird ihren Betreibern im § 8a Abs. 1 BSIG eine zweijährige Frist gewährt, um angemessene organisatorische und technische sowie im Einzellfall auch infrastrukturelle und personelle Vorkehrungen zur Vermeidung von Störungen zu treffen. Die Vorkehrungen werden als angemessen angesehen, wenn die eingesetzten Mittel und insb. mit der Umsetzung zusammenhängende Kosten, in einem hinnehmbaren Verhältnis zu den Folgen eines Ausfalls oder einer Beeinträchtigung stehen. Bezweckt werden der ordnungsgemäße Betrieb und die kontinuierliche Verfügbarkeit der angebotenen Dienstleistung.[6] Als störungsanfällige und somit zu schützende Bereiche zählen die Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit der informationstechnischen Systeme, Komponenten oder Prozesse. Die Vorgabe erstreckt sich also nicht nur auf die informationstechnischen Systeme, sondern darüber hinaus auch auf zugehörige Komponenten und insbesondere die Prozesse in der Informationsverarbeitung, welche für die Funktionsfähigkeit der jeweiligen Kritischen Infrastrukturen ausschlaggebend sind. Somit sind Sicherungsmechanismen immer zwingend zu implementieren, wenn die Informationstechnik Einfluss auf die Erbringung der kritischen Dienstleistung entfaltet. Neben Maßnahmen zur Vermeidung von Störungen sind auch entsprechende Vorkehrungen zu ihrer rechtzeitigen Aufdeckung und Behebung zu treffen. Dies gilt auch dann, wenn der Betrieb der Kritischen Infrastruktur an einen Dritten ausgelagert wurde und von ihm wahrgenommen wird.[7]

Überdies soll bei der Konzeption und Umsetzung der Vorkehrungen der Stand der Technik berücksichtigt werden. Mit der Anforderung wird sichergestellt, dass die getroffenen Maßnahmen sowohl zeitgemäß als auch tatsächlich geeignet sind, die Funktionsfähigeit der KRITIS aufrecht zu erhalten.[8] Die Vorgabe ist seitens des Gesetzgebers bewusst als eine Soll- und nicht als eine Mussvorschrift verfasst worden, um in begründeten Ausnahmefällen, bspw. wenn die Einhaltung unverhältnismäßige Kosten nach sich ziehen sollte, ein adäquates Handeln zu ermöglichen.[9] Hierdurch können die Betreiber flexibler auf bestimmte technische Änderungen und Anpassungen reagieren und z. B. die Auswirkung neuer Softwareupdates auf alle betroffenen Prozesse vor dem Einspielen in Produktivsysteme testen.

2.3 Branchenspezifische Sicherheitsstandards

Um die Sicherheitsstandards möglichst praxisnah und den spezifischen Bedürfnissen des jeweiligen Sektors angemessen auszugestalten, können so-

5 Vgl. BT-Drs. 18/4096, S. 31.

6 Vgl. BT-Drs. 18/4096, S. 25.
7 Vgl. BT-Drs. 18/4096, S. 26.
8 Vgl. BT-Drs. 18/5121, S. 17.
9 Vgl. BT-Drs. 18/5121, S. 15.

wohl die Betreiber Kritischer Infrastrukturen als auch ihre Interessenvertretungen und Verbände branchenspezifische Sicherheitsstandards zur Umsetzung von Anforderungen an die IT-Sicherheit ausarbeiten. Die Vorschrift ermöglicht den brancheninternen Zusammenschluss mehrerer Betreiber. Zudem entfällt die Notwendigkeit, bereits etablierte Verfahren und Sicherungssysteme kostspielig zu überarbeiten und neu auszurichten. Die Ausarbeitungen werden auf Antrag vom Bundesamt für Bevölkerungsschutz und Katastrophenhilfe sowie im Einvernehmen mit der zuständigen Aufsichtsbehörde des Bundes oder im Benehmen mit der sonst zuständigen Aufsichtsbehörde im Hinblick auf die Erfüllung der Anforderung des § 8a Abs. 1 BSIG bewertet.[10]

2.4 Durchführung von Audits

Damit die organisatorischen und technischen Vorkehrungen zur Vermeidung von Störungen nicht ins Leere laufen, ist über ihre Implementierung hinaus auch der Nachweis der Funktionsfähigkeit zu erbringen. Hierfür sind mindestens alle zwei Jahre Sicherheitsaudits, Prüfungen oder Zertifizierungen durch die KRITIS-Betreiber vorzunehmen. Gemäß § 8a Abs. 4 BSIG kann das Bundesamt für Sicherheit in der Informationstechnik die Art und Weise der Prüfungsvornahme, die zu erstellenden und vorzulegenden Nachweise sowie fachliche und organisatorische Anforderungen an den Prüfer festlegen. Dem geht jedoch eine Anhörung von Vertretern der betroffenen Betreiber und ihrer Interessenvertretungen und Wirtschaftsverbände voran. Weil Art und Umfang der Prüfungen nicht nur von den Vorgaben des BSI, sondern auch von branchenspezifischen Sicherheitsstandards, dem jeweiligen informationstechnischen Umfeld sowie bereits implementierten Prüfungs- und Zertifizierungsprozessen abhängig gemacht wird, wurde auf eine detaillierte gesetzliche Reglementierung des Verfahrens verzichtet. Grundsätzlich bedarf es im Verlauf von Prüfungen der Feststellung, ob branchentypische und technisch geeignete sowie wirksame Vorkehrungen getroffen wurden. Der Gesetzesbegründung folgend zählen hierzu im Wesentlichen die Einrichtung und der Betrieb eines Information Security Managements, die Identifikation und das Management von kritischen Cyber-Assets, die Implementierung von Maßnahmen zur Angriffsprävention und -erkennung sowie eines Business Continuity Managements.[11] Überdies sind branchenspezifische Anforderungen, welche bspw. aus den zukünftigen Sicherheitsstandards resultieren können, zu beachten.

Die Prüfungsvornahme kann sowohl durch den Betreiber selbst als auch einen beauftragten Dritten erfolgen. In beiden Fällen muss die zu prüfende Stelle über eine angemessene Qualifikation verfügen und hierüber entsprechende Nachweise führen können. Eine Qualifikation gilt als gegeben, wenn sie in einem fachlichen Zusammenhang mit der Überprüfung der Einhaltung der Sicherheitsstandards steht und glaubhaft gemacht werden kann.

Eine Aufstellung der erfolgten Prüfungen oder Zertifizierungen ist mitsamt den Ergebnissen und den aufgedeckten Sicherheitsmängeln an das BSI zu übermitteln. Wurden Sicherheitsmängel fest-

10 Vgl. BT-Drs. 18/4096, S. 26.

11 Vgl. BT-Drs. 18/4096, S. 27.

gestellt, kann das BSI die Übermittlung der gesamten Audit-, Prüfungs- oder Zertifizierungsergebnisse verlangen. Darüber hinaus kann im Einvernehmen mit der zuständigen Aufsichtsbehörde des Bundes oder im Benehmen mit der sonst zuständigen Aufsichtsbehörde die Beseitigung der Sicherheitsmängel gefordert werden.

Nach der Feststellung von Sicherheitsmängeln kann der Staat ihre Beseitigung einfordern.

2.5 Einrichtung einer Meldestelle

Innerhalb von sechs Monaten nach Inkrafttreten der Rechtsverordnung haben die Betreiber Kritischer Infrastrukturen eine Kontaktstelle einzurichten und sie gegenüber dem BSI zu benennen. Die Kontaktstelle dient primär dem Informationsaustausch mit dem Bundesamt und soll eine jederzeitige Erreichbarkeit der Betreiber sicherstellen. Insb. sind die Prüfungsergebnisse und vorgefundenen Sicherheitsmängel über die Kontaktstelle zu übermitteln. Gleiches gilt für die Wahrnehmung von im folgenden Abschnitt aufgeführten Meldepflichten. Im Zuge der Umsetzung eines kooperativen Ansatzes zwischen Staat und Bürger stellt das BSI den KRITIS-Betreibern Informationen zu Sicherheitslücken, zu Schadprogrammen, zu erfolgten oder versuchten Angriffen auf die Sicherheit in der Informationstechnik und zu der dabei beobachteten Vorgehensweise sowie potentielle Auswirkungen auf die Verfügbarkeit der Kritischen Infrastrukturen zur Verfügung. Hierdurch werden die Betreiber in die Warn- und Alarmierungsmechanismen einbezogen, so dass bei einer Störung der informationstechnischen Systeme, Komponenten oder Prozesse ein ausreichender Informationsfluss sichergestellt wird.

Es steht den Betreibern jedoch frei, über die eigene Kontaktstelle hinaus auch eine gemeinsame Ansprechstelle für einen bestimmten Sektor zu benennen. In dem Fall soll der Informationsaustausch zwischen den Kontaktstellen und dem Bundesamt in der Regel über die gemeinsame Ansprechstelle stattfinden. Ungeachtet dessen, ob der Informationsaustausch und die Übermittlung von Informationen über die eigene oder die gemeinsame Kontaktstelle erfolgt, muss der gesamte Prozess nachvollziehbar und überprüfbar sein.

2.6 Meldepflichten

Wird eine erhebliche Störung der Verfügbarkeit, Integrität, Authentizität oder Vertraulichkeit der informationstechnischen Systeme, Komponenten oder Prozesse festgestellt, ist sie unverzüglich – ohne schuldhafte Verzögerung – über die Kontaktstelle an das BSI zu melden. Der Begriff „Störung" orientiert sich an der Rechtsprechung zu § 100 Abs. 1 des Telekommunikationsgesetzes. Demnach liegt eine Störung vor, „... wenn die eingesetzte Technik die ihr zugedachte Funktion nicht mehr richtig oder nicht mehr vollständig erfüllen kann oder versucht wurde, entsprechend auf sie einzuwirken ...".[12] Die Gesetzesbegründung führt hierzu beispielhaft Sicherheitslücken, Schadprogramme und erfolgte, versuchte oder erfolgreich abgewehrte Angriffe auf. Auch außergewöhnliche technische Fehlfunktionen (z. B. Ausfall der Serverkühlung) sind unter dem Begriff der „Störung" zu subsumieren. Eine weitere Voraussetzung für die Auslösung der Meldepflicht ist die Erheblichkeit. Die Störung ist als erheblich einzustufen, wenn sie entweder zu einem Ausfall oder einer Beeinträchtigung der Funktionsfähigkeit der jeweiligen Kritischen Infrastruktur führen könnte oder bereits geführt hat. Als Beispiele sind neuartige oder außergewöhnliche Vorfälle oder gezielte Angriffe aufzuführen. Eine erhebliche Störung ist aber auch bei Vorfällen, die nur durch einen hohen Ressourcenaufwand bewältigt werden können, anzunehmen. Unerheblich hingegen sind regelmäßige Ereignisse (bspw. Spam-Emails oder wartungsbedingte Hardwareausfälle), welche ohne Aufwand und Probleme gelöst werden können. Sollte die Störung von öffentlichem Interesse sein, kann eine entsprechende Benachrichtigung der Betroffenen erfolgen, sofern dem die schutzwürdigen Interessen der KRITIS-Betreiber nicht entgegenstehen.

Der Gesetzesbegründung folgend ist für die Meldung ein zweistufiges Verfahren vorgesehen. Zunächst sollen die KRITIS-Betreiber schnellstmöglich die unmittelbar zur Verfügung stehenden Informationen übersenden. Die Ausgangs-

12 BT-Drs. 18/4096, S. 27.

meldung ist im weiteren Verlauf um, sofern relevant, neue Informationen zu ergänzen. Um eine sachgerechte Auswertung vornehmen zu können, muss die Meldung neben allgemeinen Angaben zu der Störung auch weitere Informationen beinhalten. Hierzu gehören die technischen Rahmenbedingungen, insb. die vermutete oder tatsächliche Ursache, die betroffene Informationstechnik, die Art der betroffenen Einrichtung oder Anlage sowie die jeweilige Branche. Hat die Störung zu keinem Ausfall oder keiner Beeinträchtigung geführt, bedarf es keiner Übermittlung unternehmensspezifischer Angaben oder einer namentlichen Nennung des Betreibers. Allgemeine Angaben, wie bspw. zum Zweck und Funktionalität der Anlage, reichen daher zur Erfüllung der Meldepflicht aus. Die Nennung des Betreibers ist dann vonnöten, wenn die Störung tatsächlich zu einem Ausfall oder einer Beeinträchtigung der Funktionsfähigkeit der Kritischen Infrastruktur geführt hat. Anderenfalls kann in einem tatsächlichen Schadensfall weder eine angemessene Reaktion noch eine Kontaktaufnahme mit dem Meldenden erfolgen. Um die Meldepflichten zu konkretisieren, wird das BSI zukünftig und unter Mitwirkung der KRITIS-Betreiber und zuständiger Aufsichtsbehörden Kriterien für meldepflichtige Vorfälle definieren und sie fortlaufend anpassen.

2.7 Mitwirkung an der Behebung von Sicherheitslücken

Die Anforderung, bei der Behebung von Sicherheitslücken mitzuwirken, richtet sich primär an die Hersteller informationstechnischer Produkte und Systeme, an deren Mithilfe es in der Praxis oft mangelt.[13] Daher kann das BSI, sofern es der Behörde erforderlich scheint, eine Mitwirkung des Herstellers (z. B. durch die Bereitstellung von Sicherheits-Updates) an der Beseitigung oder Vermeidung einer Störung fordern. Hierdurch wird die Position der KRITIS-Betreiber bei der Auswahl und dem Einsatz sicherer IT-Produkte und IT-Systeme gestärkt. Die Mitwirkung muss dem Hersteller jedoch zuzumuten sein. Daher sind willkürliche oder unverhältnismäßige Forderungen vom Gesetzeswortlaut nicht erfasst.

2.8 Erleichterungsregelung

Die Vorgaben bezüglich der Implementierung organisatorischer und technischer Vorkehrungen zur Vermeidung von Störungen, der Vornahme von Audits, Prüfungen und Zertifizierungen sowie zur Einrichtung einer Meldestelle und der Wahrnehmung der Meldepflichten sind grundsätzlich ohne die Rücksichtnahme auf die Organisationsform der Betreiber Kritischer Infrastrukturen umzusetzen. Um dem Grundsatz der Verhältnismäßigkeit Genüge zu tun, wurde eine Erleichterungsregelung für Kleinstunternehmen im Sinne der Empfehlung 2003/361/EC der Kommission vom 6. Mai 2003 geschaffen. Die §§ 8a und 8b BSIG müssen von Unternehmen, die weniger als 10 Personen beschäftigen und deren Jahresumsätze bzw. Jahresbilanzen unter 2 Millionen Euro liegen, nicht umgesetzt werden. Dies gilt auch für Unternehmen, die aufgrund der Anzahl der Mitarbeiter oder der Jahresumsätze als Kleinstunternehmen anzusehen sind und deren Kapital oder Stimmrechte zu mind. 25 % direkt oder indirekt von öffentlichen Stellen oder Körperschaften des öffentlichen Rechts kontrolliert werden.

Die Erleichterungsvoraussetzungen sind dem BSI auf Anforderung in angemessener Weise, bspw. durch die Vorlage einer Selbsterklärung mit entsprechenden Belegen, nachzuweisen. Zudem müssen die Voraussetzungen bei dem KRITIS-Betreiber selbst vorliegen. Eine (auch teilweise) Auslagerung der Kritischen Infrastruktur oder die organisatorische Übertragung der Verantwortung hat keinen Einfluss auf die Erleichterungsregelung. Auch bleiben die sonstigen Verpflichtungen der KRITIS-Betreiber hiervon unberührt.

> **Eine erhebliche Störung liegt vor, wenn Kritische Infrastrukturen ausfallen oder beeinträchtigt werden. Darauf erfolgt eine Meldung der relevanten Informationen.**

Die Erleichterungsvoraussetzungen gelten jedoch nicht nur für Kleinstunternehmen, sondern partiell auch für Unternehmen bestimmter Branchen. Wird ein öffentliches Telekommunikationsnetz betrieben oder werden öffentlich zugängliche Telekommunikationsdienste erbracht, bedarf es keiner Implementierung von Vorkehrungen und der Durchführung von Prüfungen. Ebenso entfällt die Verpflichtung zur Einrichtung einer Kontakt-

13 Vgl. BT-Drs. 18/5121, S. 16.

stelle sowie der Meldung erheblicher Störungen. Dies gilt auch für Betreiber von Energieversorgungsnetzen oder Energieanlagen im Sinne des Energiewirtschaftsgesetzes, für Genehmigungsinhaber nach § 7 Absatz 1 des Atomgesetzes sowie sonstige Betreiber Kritischer Infrastrukturen, soweit sie auf Grund von Rechtsvorschriften Anforderungen erfüllen müssen, die mit den Anforderungen nach § 8a und § 8b BSIG vergleichbar oder gar weitergehend sind.

Werden die Gesetzesanforderungen von den Betreibern Kritischer Infrastrukturen nicht erfüllt, kann dies (auch mehrfach) mit einem Bußgeld von bis zu 100.000 € sanktioniert werden.

2.9 Sanktionen

Um eine vollumfängliche Umsetzung der Gesetzesnovelle sicherzustellen, wurden bußgeldbewehrte Sanktionen eingeführt. Werden dem BSI keine oder unvollständige Audit-, Prüfungs- oder Zertifizierungsergebnisse übermittelt oder wird der geforderten Beseitigung von Sicherheitsmängeln gem. § 8a Abs. 3 S. 4 Nr. 2 BSIG nicht entsprochen, kann ein Bußgeld bis zu 100.000 Euro verhängt werden. In allen anderen Fällen kann ein Bußgeld bis zu 50.000 Euro verhängt werden. Hierbei handelt es sich um die unterlassene Implementierung angemessener organisatorischer und technischer Vorkehrungen, die nicht oder nicht rechtzeitige Benennung einer Kontaktstelle sowie die unrichtige, unvollständige oder die nicht rechtzeitige Meldung von Störungen und Sicherheitsvorfällen. Gleiches gilt, wenn die Meldung ausbleibt. Der Verstoß ist dabei jedoch nur dann bußgeldbewehrt, wenn Meldungen unterlassen wurden oder nicht im Einklang mit dem Gesetzeswortlaut erfolgten und die betreffende Störung tatsächlich zu einem Ausfall oder einer Beeinträchtigung der Funktionsfähigkeit der Kritischen Infrastruktur geführt hat.[14] Die Bußgelder können auch kumulativ bei mehreren Verstößen verhängt werden.

14 Vgl. BT-Drs. 18/5121, S. 16.

3. Auswirkungen und kurzfristiger Handlungsbedarf für die Unternehmen

3.1 Vorbereitende Tätigkeiten

Bezogen auf die Anforderungen aus dem IT-Sicherheitsgesetz bedarf es zunächst der Klärung, ob die Zugehörigkeit des eigenen Unternehmens zu den im Abschnitt 2.1 genannten Sektoren bzw. Bereichen gegeben oder es folglich (vorbehaltlich der noch zu erlassenen Rechtsverordnung) potentiell als solches einzustufen ist. Hierauf aufbauend sind entsprechende technische sowie organisatorische Vorkehrungen zur vorbereitenden Umsetzung der sich aus dem IT-Sicherheitsgesetz ergebenden Anforderungen zu treffen. In der Praxis hat sich die Ausarbeitung eines Umsetzungsplans in Abstimmung mit der Geschäftsführung bewährt. Dieser beinhaltet eine Ist-Aufnahme und eine anschließende Bewertung der Lage der IT-Sicherheit im Unternehmen. In dem Zusammenhang sollten bereits implementierte Prozesse sowie vorhandene Dokumente, Richtlinien und Anweisungen eruiert und hinsichtlich ihrer Konformität zu den geforderten Mindestanforderungen an die IT-Sicherheit überprüft werden. Als Orientierung können hierbei etablierte Standards, wie bspw. die IT-Grundschutzkataloge des BSI[15], dienen. Auf Basis dieser Erstaufnahme kann in einem zweiten Schritt bereits die teilweise Umsetzung der Mindestanforderungen durchgeführt werden. Eine sachgerechte Dokumentation der Umsetzung kann durch die Aufnahme in Sicherheits- und Notfallkonzepte erfolgen.[16]

Aufgrund der fehlenden Transparenz und der Unmöglichkeit der nachträglichen Einflussnahme auf das Verfahren zur Definition der Kritischen Infrastrukturen sollte sich jeder Betreiber einer solchen, sofern er bereits heute davon ausgehen kann, dass er von der Gesetzesänderung betroffen ist bzw. potentiell betroffen sein kann, rechtzeitig an das BSI wenden und sein Interesse an der Mitarbeit in entsprechenden Gremien bekunden.[17] Alternativ sind die Interessenverbände bzw. -vertreter zu informieren. Selbiges gilt für die nach § 8a Abs. 2 BSIG noch zu erarbeitenden branchenspezifischen Sicherheitsstandards, die

15 https://www.bsi.bund.de/DE/Themen/ITGrundschutz/StartseiteITGrundschutz/startseiteitgrundschutz_node.html, abgerufen am 14.08.2015.
16 Vgl. BT-Drs. 18/4096, S. 26.
17 Nach § 10 Abs. 1 ITSG wird „Zugang zu Akten, die die Erstellung oder Änderung dieser Verordnung betreffen, [...] nicht gewährt."

von den Betreibern und ihren Branchenverbänden vorgeschlagen werden können.

Als zentrale organisatorische Vorkehrung sollten vorbereitende Maßnahmen zur Implementierung eines Informationssicherheitsmanagementsystems (ISMS) getroffen werden. Auch wenn die Pflicht zur Errichtung eines ISMS bislang durch den geänderten § 11 Abs. 1a EnWG lediglich für Strom- und Gasnetzbetreiber unmittelbare Anwendung findet, liegt eine verpflichtende Umsetzung für KRITIS-Betreiber aufgrund der Gesetzesnovelle nahe.[18] Eine freiwillige Selbstverpflichtung im Rahmen der IT-Compliance ist – zumindest in Teilen – aufgrund der steigenden gesetzlichen Anforderungen an die Informationssicherheit, bspw. das nötige Vorliegen eines Datensicherheitskonzeptes nach den GoBD,[19] ohnehin zu begrüßen. Auch hierbei können einschlägige Standards (BSI-Standard 100 – 1: Managementsysteme für Informationssicherheit (ISMS) bzw. ISO 27001) als Orientierung dienen.

Bezüglich der zu treffenden technischen Vorkehrungen und sonstigen Maßnahmen bzw. der Einhaltung des Stands der Technik können aufgrund der noch zu erfolgenden abschließenden Definition durch den Gesetzgeber lediglich vorbereitende Tätigkeiten unternommen werden. Dies schließt bspw. die Aufnahme der IT-Landschaft im Unternehmen mit Fokus auf die Aktualität bzw. die Angemessenheit der im Einsatz befindlicher Hardware, ihrer Kritikalität und ihrer Rolle im Rahmen der IT-Sicherheit ein. Für die Feststellung des Stands der Technik sind nicht nur internationale und nationale Normen und Standards, sondern auch praxiserprobte und allgemein anerkannte Verfahrensweisen ausschlaggebend. Dies wiederum setzt eine regelmäßige Überprüfung seitens der KRITIS-Betreiber voraus (siehe hierzu Abschnitt 3.3), wozu sich aufgrund ihrer unabhängigen Stellung im Unternehmen die Internen Revision eignet.

Bei der generellen Umsetzung von Mindestanforderungen an die IT-Sicherheit durch Betreiber

18 Vgl. Weise/Brühl (2015), S. 290.
19 Vgl. hierzu BMF-Schreiben vom 14.11.2014–IV A 4–S 0316/13/10003, BStBl. I 2014, Rzn. 106.

Kritischer Infrastrukturen sind im Hinblick auf die Angemessenheit der für den Betreiber erforderliche Aufwand und insb. die Kosten zu berücksichtigen. Hierzu sollten intern auf Basis der initialen Ist-Aufnahme bereits Schwellenwerte bzw. grobe Kostenschätzungen bzw. die Einschätzung der Verhältnismäßigkeit vorgenommen werden. Als Modell zur Investitionsrechnung und der damit einhergehenden Einschätzung der Verhältnismäßigkeit kann hierbei bspw. das „Return on Security Investment"-Modell (ROSI) verwendet werden.[20]

3.2 Einrichtung einer zentralen Meldestelle

Die Meldepflicht von (potentiellen) Störungen bzw. Beeinträchtigungen nach § 8b BSIG stellt einen erheblichen Eingriff in die Datenverarbeitungsprozesse von betroffenen Unternehmen dar.[21] Zur Erfüllung der Anforderungen sind innerhalb von sechs Monaten nach Inkrafttreten der Rechtsverordnung entsprechende Kommunikationsstrukturen einzurichten. Hierzu gehört die Benennung einer Kontaktstelle, deren ständige Erreichbarkeit gewährleistet sein muss. Diese jederzeitige Erreichbarkeit wird insb. kleine und mittlere Unternehmen (KMU) aufgrund ihrer personellen Ressourcen vor erhebliche Herausforderungen stellen und erfordert aus diesem Grund eine frühzeitige Definition einer Umsetzungsstrategie zur Erfüllung der Anforderungen. Unklar ist bis jetzt zudem, ob die Funktion der Warn- und Alarmierungskontakte auch von Dritten übernommen werden kann, was besonders für Unternehmen von Relevanz ist, die den Betrieb und die Überwachung der IT-Infrastruktur vollständig an Dritte ausgelagert haben.[22] In diesem Zusammenhang gilt es auch zu klären, inwiefern Prüfungsrechte oder Möglichkeiten zur Prüfung bei Auslagerung bestehen, was sich bspw. bei Cloud-Umgebungen als kritischer Punkt darstellt.[23]

Das Erfordernis einer Kontaktstelle erweist sich insbesondere für KMU aufgrund der personellen Ressourcen als Herausforderung.

Meldepflichtige IT-Sicherheitsvorfälle nach § 8b Abs. 4 BSIG können in allen Bereichen im Unternehmen auftreten, die potentiell kritische bzw. zentrale Geschäftsprozesse beinhalten oder diese unterstützen. Daher erfordert eine effektive Überwachung dieser Bereiche eine Etablierung angemessener interner Prozesse. Hierzu gehören eine Vernetzung der Meldestelle im Unternehmen respektive die Ausstattung selbiger mit entsprechenden Weisungs- und Informationsbefugnissen zur Erfüllung der gesetzlichen Aufgaben. Für die potentiell kritischen Bereiche müssen demzufolge interne Verantwortlichkeiten benannt und funktionsfähige Eskalationsmechanismen bei Auftreten eines meldepflichtigen Vorfalls installiert werden. Dem liegt eine initiale unternehmensinterne Definition über die Kritikalität von meldepflichtigen (potentiellen) Störfällen, sprich die Festlegung der individuellen und unternehmensinternen Meldeschwelle von Störereignissen, zugrunde. Dieser Punkt ist relevant, da die Meldepflicht hinsichtlich der Schwelle von meldepflichtigen Ereignissen durch die Erarbeitung eines entsprechenden Kriterienkataloges noch zu konkretisieren ist[24] und je nach Ausgestaltung eine unverhältnismäßige und inflationäre Pflicht zur Meldung von Vorfällen droht.[25] Somit ist festzulegen, ob zunächst überhaupt die Voraussetzungen für die Meldepflicht eines Vorfalls erfüllt sind bzw. ob dieser in einem zweiten Schritt bei einer tatsächlich eingetretenen Beeinträchtigung namentlich oder anonym gemeldet werden muss. Die intern festgelegten Schwellenwerte können zudem in die Erarbeitung des Kriterienkataloges eingebracht werden.

Unternehmensinternen Einfluss hat die Umsetzung der Meldepflicht zudem auf die Tätigkeiten des Datenschutzbeauftragen. Da meldepflichtige Vorfälle potentiell personenbezogene Daten beinhalten können, ist bei der Einrichtung der Meldestelle bzw. bei der Implementierung entsprechender Prozesse der Datenschutzbeauftragte einzubeziehen.[26] Dies kommt insbesondere zum Tragen, wenn die Meldung bei einer tatsächlichen Beeinträchtigung oder einem Ausfall nicht anonym erfolgen darf. Mit Hinblick auf die Transparenz im Umgang mit personenbezogenen Daten könnten

20 Vgl. Sowa (2007), S. 443.
21 Vgl. Bräutigam/Wilmer (2015), S. 39.
22 Vgl. Roos (2014), S. 726.
23 Vgl. Weise/Brühl (2015), S. 294.
24 Vgl. Leisterer (2014), S. 575.
25 Vgl. Bräutigam/Wilmer (2015), S. 40.
26 Vgl. Roos (2014), S. 727.

die Meldeverfahren in das Verfahrensverzeichnis mit aufzunehmen und im Rahmen der Tätigkeit des Datenschutzbeauftragten zu kontrollieren sein.

4. Vorbereitung und Durchführung von IT-Sicherheitsaudits

4.1 Anwendbare Standards

Wie bereits im Abschnitt 2.4 erörtert, haben die KRITIS-Betreiber die Implementierung und Aufrechterhaltung organisatorischer und technischer Vorkehrungen und sonstigen Maßnahmen mindestens alle zwei Jahre auf geeignete Weise nachzuweisen. Obwohl ohne die noch zu definierenden branchenspezifischen Standards ein konkreter Maßstab zur Durchführung von IT-Sicherheitsaudits fehlt,[27] können bereits existierende und in der Praxis anerkannte Standards eine Basis für die Durchführung von IT-Sicherheitsaudits bilden.[28] Ungeachtet der konkreten branchenspezifischen Ausprägungen ist folglich eine grundlegende Auseinandersetzung mit diesen Standards empfehlenswert. Als zentrale Rahmenwerke zur Identifikation und Umsetzung dem Stand der Technik entsprechender Sicherheitsmaßnahmen sind hierbei insb. folgende Standards zu nennen:

COSO-ERM (Enterprise Risk Management) Framework

Bei dem COSO-ERM Framework handelt es sich um eine allgemein anerkannte, strukturierte Vorgehensweise zur Identifikation und Analyse von Risiken aus einer gesamtheitlichen Perspektive. Hierdurch können Risiken adäquat beurteilt und priorisiert werden. Das Framework enthält auch Empfehlungen zur Risikosteuerung und einer damit einhergehenden Berichterstattung. Obwohl explizite Vorgaben an die Durchführung von IT-Sicherheitsaudits fehlen, bietet es doch einen übergreifenden und organisationsweiten Ansatz, mithilfe welchen das IT-Sicherheitsmanagement analog zu ISO/IEC 27001 als Teil eines unternehmensweiten Managementsystems umgesetzt werden kann.[29]

ISO/IEC 27000-Reihe

Die ISO/IEC 27000-Reihe vereint verschiedene Standards zur Informationssicherheit. ISO 27001 spezifiziert beispielsweise die Einführung eines Informationssicherheitsmanagementsystems, wie es durch das ITSG für Strom- und Gasnetzbetreiber verpflichtend ist.[30] Der ISO 27002-Standard enthält Vorgaben zur Risikoanalyse und beinhaltet teilweise sehr konkrete Handlungsanweisungen zu deren Bewältigung. Insbesondere die beiden vorgenannten Standards bilden die erforderliche Basis für die Durchführung von Revisionsprojekten im Bereich der IT-Sicherheit.

IT-Grundschutz-Kataloge/ IT-Grundschutz—Standards des BSI

Die IT-Grundschutz-Kataloge sind konkurrierend zu den ISO-27000 Standards eher technischer ausgelegt und stellen einen nationalen De-Facto Standard für IT-Sicherheit dar.[31] ISO 27001-Zertifizierungen auf der Basis von IT-Grundschutz weisen die Umsetzung internationaler Standards sowie die Bausteine des IT-Grundschutz-Kataloges mit Hinblick auf die Informationssicherheit nach und können von BSI-zertifizierten Auditoren durchgeführt werden.

IDW Prüfungsstandard 330

Der IDW PS 330 determiniert die Vorgehensweise des Wirtschaftsprüfers bei der Beurteilung von IT-Risiken mit Hinblick auf die Ordnungsmäßigkeit der Buchführung. Obwohl es sich hierbei um keinen originären Standard zur Beurteilung des generellen IT-Sicherheitsniveaus eines Unternehmens handelt, bietet er jedoch durch die Prüfung der Bereiche der IT-Infrastruktur, IT-Anwendungen, IT-Geschäftsprozesse sowie der IT-Organisation und des IT-Umfelds relevante Implikationen bei der Aufnahme der IT-Sicherheit eines Unternehmens bzw. ihrer initialen Beurteilung.

4.2 Einbindung der Internen Revision

Im Zuge der Wandlung des Aufgabengebietes der Internen Revision hin zu einer proaktiven Kontrolle der Umsetzung gesetzlicher Anforderungen ist in den letzten Jahren insb. der Bereich der Informationssicherheit respektive ihre Beurteilung in den Vordergrund gerückt. Die Interne Revision sollte hierbei als ein Teil des Maßnahmenbündels zur Erfüllung der Anforderungen, die sich aus dem IT-Sicherheitsgesetz ergeben, angesehen und zudem derart eingebunden werden, dass ihre Unabhängigkeit im Zuge der Umsetzung und Beurteilung gewahrt bleibt.[32]

27 Vgl. Heinickel/Feiler (2014), S. 712.
28 Vgl. Sowa (2007), S. 445.
29 Vgl. Brenner et al. (2011), S. 144
30 Vgl. Weise/Brühl (2015), S. 290.
31 Vgl. Lohre (2009), S. 187, Klett/Ammann (2014), S. 94.
32 Vgl. Lohre (2009), S. 180.

Die Entscheidung, ob die Auditierung der IT-Sicherheit durch interne Stellen oder externe Dritte erfolgen soll, obliegt den KRITIS-Betreibern. Bei einer internen Durchführung sind insb. zwei Aspekte maßgeblich. Zum einen darf bei der Durchführung kein Interessenkonflikt hinsichtlich des zu auditierenden Bereichs bestehen. Hierdurch scheiden grundsätzlich nicht nur die IT-Abteilung, sondern auch Abteilungen bzw. Beteiligte, welche sich mit den potentiell kritischen Prozessen befassen, aus. Aus diesen Gründen sowie aufgrund ihrer unabhängigen Stellung im Unternehmen, ist die Interne Revision geradezu für die Durchführung von IT-Sicherheitsaudits prädestiniert. Zu beachten ist jedoch, dass die grundsätzliche Verantwortung für die Erfüllung der Anforderungen des ITSG bzw. der IT-Compliance nicht bei der Internen Revision angesiedelt werden darf, da sie hierdurch ihre Unabhängigkeit verlieren würde und eine neutrale und objektive Beurteilung nicht mehr gewährleistet wäre.[33] Zum anderen besteht durch die Pflicht zum Nachweis entsprechender Qualifikationen bei interner Umsetzung die Frage nach vorhandenen Kapazitäten bzw. personellen Ressourcen im Unternehmen, die für die Durchführung der IT-Sicherheitsaudits in Frage kämen. Beim Aufbau von Ressourcen ist auf entsprechende Qualifikationen zu achten, die bspw.

Aufgrund ihrer Unabhängigkeit ist die Interne Revision für die Durchführung von IT-Sicherheitsaudits prädestiniert.

durch (international) anerkannte Zertifikate (wie bspw. CISO, CISM, CISA o.Ä.) nachgewiesen werden können. Angesichts des komplexen und dynamischen Themengebiets der IT-Sicherheit ist bei der Rekrutierung in erster Linie auf ausgeprägte IT-Kompetenzen zu achten, wohingegen die Revisionskompetenz eher in den Hintergrund rückt und durch Seminare bzw. „on the job" erworben werden kann.[34] Bei einer externen Vergabe ist auf den Nachweis entsprechender Qualifikationen zu achten, die in der Regel von etablierten Anbietern von IT-Sicherheitsaudits erbracht werden können. Diese halten mit Hinblick auf das angesprochene nötige Know-how im Bereich der Informationssicherheit bzw. der Revision von IT-Systemen geeignetes Personal bereit.

Selbst wenn die Prüfung durch externe Dritte erfolgen sollte, ist die Involvierung der Internen Revision zu empfehlen. In dem Fall kann sich ihre Mitwirkung auf vorbereitende oder koordinierende Tätigkeiten erstrecken.[35] Bei erstmaligen Audits sind solche Vorbereitungen meist nicht vonnöten, bei Folgeprüfungen oder falls im Bereich der IT-Sicherheit bereits Zertifizierungen bestehen, können vorbereitende interne Audits kurz vor der angesetzten Prüfung durch einen Dritten zur Identifikation noch bestehender Abweichungen durchaus sinnvoll sein.[36]

Über die generellen und branchenspezifischen Sicherheitsstandards hinaus kann eine Kontrolle der Einhaltung der Erfordernisse nach § 8a Abs. 1 zudem über etablierte Prüfmechanismen, z. B. den jährlichen Revisionsplan, das Audituniverse und das Follow-Up-System der Internen Revision erfolgen. Auch Wirtschaftsprüfer prüfen bereits heute unter anderem im Rahmen der Jahresabschlussprüfung die für die Rechnungslegung relevanten IT-Systeme ebenso wie die Interne Revision.[37] Eine Kooperation mit dem Wirtschaftsprüfer oder der Internen Revision bei IT-Sicherheitsaudits ist vorbehaltlich entsprechender Qualifikationen mit Hinsicht auf die Synergieeffekte, die sich aus der Vertrautheit der Prüfungsgesellschaft mit den Systemen und den individuellen Anforderungen bzw. Besonderheiten des KRITIS-Betreibers ergeben, sinnvoll. Dies kommt insb. bei der Beachtung der Verhältnismäßigkeit im Zuge der Prüfung der Maßnahmen zur Einhaltung der IT-Sicherheit zum Tragen, die eine Kenntnis der unternehmensinternen Ziele und Strategien erfordert.[38] Die durchgeführten Sicherheitsaudits, Prüfungen oder Zertifizierungen, einschließlich der dabei aufgedeckten Sicherheitsmängel, sind dem BSI vorzulegen. Eine zentrale Rolle kommt der Internen Revision zudem bei der Überwachung bzw. Prüfung der Behebung potentiell im Rahmen der IT-Sicherheitsaudits identifizierten Feststellungen zu. Sollte das BSI aufgrund der festgestellten Sicherheitsmängel eine Übermittlung der gesamten Audit-, Prüfungs- oder Zertifizierungsergebnisse

33 Vgl. Lohre (2009), S. 183.
34 Vgl. Sowa (2007), S. 445.
35 Vgl. Lohre (2009), S. 187.
36 Vgl. Kilian (2007), S. 770.
37 Vgl. BT-Drs. 18/4096, S. 27.
38 Vgl. Sowa (2007), S. 443.

und deren unverzügliche Beseitigung verlangen, ist mit Hinblick auf mögliche Haftungsrisiken die objektive Sicherstellung der zeitgerechten Umsetzung der Feststellungen nötig.

5. Fazit

Das IT-Sicherheitsgesetz birgt weitreichende Konsequenzen für Betreiber Kritischer Infrastrukturen. Trotz der noch ausstehenden Konkretisierungen und der damit einhergehenden Unsicherheit bzgl. der genauen Ausprägung gesetzlicher Anforderungen sollten sich potentiell betroffene KRITIS-Betreiber frühzeitig mit möglichen Folgen des ITSG auseinandersetzen. Insb. bei der Erstaufnahme des Stands der IT-Sicherheit im Unternehmen auf Basis etablierter Rahmenwerke und Standards, der Erarbeitung von Branchenstandards und der darauf aufbauenden Auditierung des IT-Sicherheitsniveaus der betroffenen Unternehmen, kann der Internen Revision eine besondere Rolle zukommen. Im Hinblick auf die Durchführung der regelmäßigen Audits sollten bereits heute Einschätzungen zu einer internen Durchführung oder einer Vergabe an Dritte, wie bspw. Wirtschaftsprüfungsgesellschaften, vorgenommen und ggf. entsprechende Kompetenzen aufgebaut werden.

Literaturverzeichnis

Bräutigam, P. / Wilmer, S.: Big brother is watching you? – Meldepflichten im geplanten IT-Sicherheitsgesetz, in ZRP 2/2015, S. 38 – 42.

Brenner et al.: Praxisbuch ISO/IEC 27001: Management der Informationssicherheit und Vorbereitung auf die Zertifizierung, München, 2011.

Deutscher Bundestag, Drucksache 18/4096, vom 25.02.2015, Gesetzentwurf der Bundesregierung Entwurf eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz), S. 1 – 50.

Deutscher Bundestag, Drucksache 18/5121, vom 10.06.2015, Beschlussempfehlung und Bericht des Innenausschusses (4. Ausschuss) zu dem Gesetzentwurf der Bundesregierung–Drucksache 18/4096–Entwurf eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz), S. 1 – 18.

Heinickel, C. / Feiler, L.: Der Entwurf für ein IT-Sicherheitsgesetz–europarechtlicher Kontext und die (eigentlichen) Bedürfnisse der Praxis, in CR 11/2014, S. 708 – 714.

Kilian, D.: Vorbereitung und Durchführung von IT-Sicherheitsaudits (I), in IT-Sicherheit und Datenschutz 10/2007, S. 769 – 772.

Klett, D. / Ammann, T.: Gesetzliche Initiativen zur Cybersicherheit, in CR 2/2014, S. 93 – 99.

Leisterer, H. / Schneider, F.: Der überarbeitete Entwurf für ein IT-Sicherheitsgesetz, in CR 9/2014, S. 574 – 578.

Lohre, T.: Beitrag der Internen Revision zur IT-Compliance, in ZIR 4/2009, S. 179 – 189.

Roos, P.: Der neue Entwurf eines IT-Sicherheitsgesetzes–Bewegung oder Stillstand?, in MMR 11/2014, S. 723 – 730.

Sowa, A.: IT-Sicherheitsprüfungen durch die Interne Revision, in DuD 6/2007, S. 441 – 445.

Weise, M. / Brühl, S.: Auswirkungen eines künftigen IT-Sicherheitsgesetzes auf Betreiber Kritischer Infrastrukturen, in CR 5/2015, S. 290 – 294.