Dennis-Kenji Kipker, David Pfeil

IT-Sicherheitsgesetz in Theorie und Praxis

Was Betreiber (wirklich) beachten müssen – Eine interdisziplinäre Fallstudie

Vor mittlerweile über einem Jahr, im Juli 2015, wurde das IT-Sicherheitsgesetz vom Deutschen Bundestag erlassen, das vor allem für die Betreiber Kritischer Infrastrukturen Vorgaben zur Verbesserung der IT-Security enthält. In diesem Beitrag soll anhand einer exemplarischen Fallstudie am Beispiel eines Betreibers Kritischer Infrastrukturen untersucht werden, welche technisch-organisatorischen Maßnahmen konkret zur möglichst effektiven Implementierung der Cyber-Sicherheitsstrategie beitragen können und wo besondere Probleme in der Umsetzung zu verorten sind.

1 Problemstellung und Zielsetzung

In den letzten Jahren hat die Technisierung, Digitalisierung und Vernetzung der Gesellschaft erhebliche Fortschritte erzielt. Damit verbunden wächst auch das Angriffs- und Schadenspotenzial, das durch den Ausfall oder Missbrauch von IT-Systemen ausgelöst werden kann.[1]

Das deutsche IT-Sicherheitsgesetz (IT-SiG) ist eine Reaktion des Gesetzgebers auf diese Entwicklung. Im Schwerpunkt sieht es zwei Maßnahmen zur Verbesserung der Sicherheitslage vor: die Einführung eines technisch-organisatorischen Mindeststandards (TOM) für Betreiber Kritischer Infrastrukturen gem. § 8a BSIG sowie eine Meldepflicht an das BSI im Falle sicherheitskritischer Vorfälle gem. § 8b BSIG. Vergleichbare Anforderungen gelten für Spezialgesetze wie dem AtG, EnWG und TKG.

Die Umsetzung dieser abstrakten gesetzlichen Anforderungen ist in technischer Hinsicht zurzeit noch nicht zweifelsfrei konkretisiert. Insbesondere stellen sich für die Betreiber Kritischer Infrastrukturen zwei Fragen:

1. Kann ein dem „Stand der Technik" im Sinne des IT-SiG entsprechender Mindest-Sicherheitsstandard durch etablierte Methoden eines Managementsystems für Informationssicherheit (ISMS) realisiert werden?
2. Welche zusätzlichen Anforderungen entstehen durch die Verpflichtung, sicherheitskritische Vorfälle zu melden und wie kann diesen entsprochen werden?

Zur Beantwortung dieser Fragen wird die aktuelle IT-Organisation eines Betreibers aus dem Wasser-Sektor beispielhaft untersucht. Als Maßstab der Fallstudie dienen die Anforderungen der ISO 27000-Normenreihe[2], die den international etablierten Standard für ISMS wiedergibt.

2 Der Mindestsicherheitsstandard nach dem IT-SiG

§ 8a Abs. 1 BSIG verpflichtet die in § 2 Abs. 10 BSIG definierten und durch die BSI-KritisV weiter konkretisierten Betreiber Kritischer Infrastrukturen zur Einhaltung von IT-Mindestsicherheits-

1 BSI, Die Lage der IT-Sicherheit in Deutschland 2014, S. 7.

2 Ein Standard der International Organization for Standardization (ISO) zum Aufbau und Betrieb eines Informationssicherheitsmanagementsystems (ISMS). Soweit auf das ISMS Bezug genommen wird, betrifft dies auch die deutsche Norm DIN ISO/IEC 27001:2015-03.

Dr. Dennis-Kenji Kipker

Wissenschaftlicher Assistent am Institut für Informations-, Gesundheits- und Medizinrecht (IGMR) der Universität Bremen, Mitglied im Vorstand der Europäischen Akademie für Informationsfreiheit und Datenschutz (EAID) Berlin
E-Mail: kipker@uni-bremen.de

David Pfeil

B.Sc., studierte Informatik an der Universität Bremen und arbeitet als Softwareentwickler bei der Hollmann IT GmbH

E-Mail:
revolver@informatik.uni-bremen.de

standards. Dazu sollen organisatorische und technische Vorkehrungen, die dem „Stand der Technik" entsprechen, getroffen werden. Daneben haben Betreiber gem. § 8a Abs. 2 BSIG die Möglichkeit, branchenspezifische Sicherheitsstandards zu erarbeiten und dem BSI vorzuschlagen, diese müssen in technischer Hinsicht mit den Vorgaben nach § 8a Abs. 1 BSIG vergleichbar sein. Damit ist die Realisierung des gesetzlich verlangten Mindeststandards der IT-Sicherheit in allen Fällen an den Stand der Technik geknüpft. Hierbei handelt es sich um einen so genannten „unbestimmten Rechtsbegriff" bzw. um eine Generalklausel.[3] Diesen gesetzgeberisch intendierten Instrumenten ist zu eigen, dass sie zwar eine bestimmte zu erfüllende Anforderung beschreiben, jedoch nicht näher festlegen, wie diese im Einzelnen auszugestalten ist. Im Zusammenhang mit technischen Regeln, die einer steten Weiterentwicklung unterliegen, mag dies zwar sinnvoll sein,[4] kann aber in der außerjuristischen Praxis gerade im Falle neuer gesetzlicher Regelungen, die noch nicht durch Rechtsprechung und Behörden konkretisiert werden konnten, zu Umsetzungsproblemen führen.

Die Erfahrung hat gezeigt, dass mit derlei Schwierigkeiten auch die Betreiber Kritischer Infrastrukturen bei der Realisierung der IT-Sicherheitsanforderungen nach § 8a BSIG aktuell konfrontiert sind. Zwar wird in der Gesetzesbegründung zum IT-SiG der Stand der Technik weiter konkretisiert: So sind zu dessen Bestimmung insbesondere einschlägige internationale, europäische und nationale Normen und Standards heranzuziehen sowie vergleichbare Verfahren, Einrichtungen und Betriebsweisen, die mit Erfolg in der Praxis erprobt wurden. Ebenso schließt die Verpflichtung zur Berücksichtigung des Stands der Technik solche Vorkehrungen nicht aus, die einen gleichermaßen effektiven Schutz wie die anerkannten Vorkehrungen nach dem Stand der Technik bieten. Weiter heißt es für die Zertifizierung der getroffenen Maßnahmen, dass geprüft werden soll, ob ein Betreiber die für seine Branche und Technologie geeigneten und wirksamen Maßnahmen und Empfehlungen befolgt, etwa ein Information Security Management betreibt und ein Business Continuity Management (BCM) implementiert hat sowie darüber hinaus die branchenspezifischen Besonderheiten beachtet.[5] Die branchenspezifischen Sicherheitsstandards betreffend erfolgt die Erarbeitung unter anderem unter Einbeziehung des UP KRITIS. Hier referenziert die vom BSI veröffentlichte Orientierungshilfe auf den BSI-IT-Grundschutz.[6] Dieser Maßnahmenkatalog bezieht sich auf die organisatorischen, technischen, personellen und infrastrukturellen Abläufe einer Organisation, um die IT-Sicherheit zu verbessern und die vom BSI durchgeführte Zertifizierung nach IT-Grundschutz zu erlangen.[7] Mit Blick auf die internationale Vergleichbarkeit besteht die Möglichkeit, die BSI-Standards den Anforderungen der ISO 27000-Normenreihe zuzuordnen, sodass auch hier wieder ein Bezug zum ISMS nach ISO 2700X hergestellt ist.[8]

Obgleich die gesetzgeberischen Ausführungen, verbunden mit den fachspezifischen Auslegungsquellen, somit eine bestimmte Stoßrichtung vorgeben, werden sie nicht zweifelsfrei konkret, welche technisch-organisatorischen Maßnahmen tatsächlich und branchenspezifisch getroffen werden müssen. Diese Entscheidung wird den Betreibern überantwortet. Durch die Ausgestaltung der Einhaltung des Standes der Technik als Soll-Vorschrift werden die Vorgaben weiter verwässert, indem dem Betreiber für begründete Ausnahmefälle eine Abweichungsmöglichkeit eingeräumt wird.[9] Um den mit der Umsetzung von IT-Sicherheit Verantwortlichen eine Orientierungshilfe an die Hand zu geben, ist deshalb zu klären, ob die Einrichtung eines ISMS im tatsächlichen Sinne ausreichend ist, um dem „Stand der Technik" zu genügen und damit als universell ausreichender Nachweis zur Erfüllung der Vorgaben des § 8a BSIG zu dienen. Die Zertifizierung nach ISO 27001 wäre folglich dann ausreichend, wenn der Betreiber nachweisen kann, dass mit dem Betrieb des ISMS alle für ihn wesentlichen IT-Schutzziele erreicht sind.

3 Untersuchung der IT-Organisation eines Betreibers Kritischer Infrastrukturen

3.1 Vorüberlegungen und Methodik

Zur Konkretisierung der Anforderungen aus dem IT-SiG wird ein Versorgungsdienstleister des vom Gesetz nach § 2 Abs. 10 BSIG grundsätzlich betroffenen Wasser-Sektors durch ein Sicherheitsaudit untersucht. Dieser Untersuchung liegen die Anforderungen der ISO 27000-Normenreihe zum ISMS zu Grunde. Die Tätigkeiten zum Erfassen des Sicherheitsniveaus beim Betreiber werden unter dem Begriff „IT-Sicherheitsaudit" zusammengefasst. In Vorbereitung des Audits ist es zunächst erforderlich, den Zweck und Umfang der Untersuchung (sogenannter „Scope") festzulegen.[10] Ferner fordert ISO 27001 die Bewertung der erbrachten IT-Sicherheitsleistungen durch Methoden, die zu „vergleichbaren und reproduzierbaren Ergebnissen führen".[11] Gerade für das Management eines Unternehmens ist es von hoher Bedeutung, die Entwicklung von Geschäftsprozessen zu vergleichen und zu bewerten. Hieraus folgt die Notwendigkeit, die Umsetzung von Maßnahmen im Rahmen eines ISMS durch Kennzahlen abzubilden.

Eine solche Möglichkeit zur Abbildung des Entwicklungsstandes eines Prozesses liefert das Reifegradmodell. In dessen Rahmen wird die Reife eines Prozesses über verschiedene Stufen ihres Erfüllungsgrads abgebildet. Die Kriterien, ab wann eine Stufe als erreicht gilt, müssen je nach Untersuchungsgegenstand definiert und dokumentiert werden. Anhand eines Zielreifegrads können Maßnahmen zu dessen Erreichen zielgerichtet geplant und eingesetzt werden.[12] Eine Konkretisierung des Reifegradmodells wird durch die ISO 15504 oder SPICE-Norm (Software Process Impro-

3 Dazu schon *Kipker*, DuD 2016, S. 610.

4 Vgl. BMJV, Handbuch der Rechtsförmlichkeit, S. 84 f.

5 BT-Drs. 18/4096, S. 26 f.

6 BSI, Orientierungshilfe zu Inhalten und Anforderungen an branchenspezifische Sicherheitsstandards (B3S) gemäß § 8a (2) BSIG, S. 4, abrufbar unter: http://www.kritis.bund.de/SharedDocs/Downloads/Kritis/DE/B3S_Orientierungshilfe.pdf (Stand: 16.9.2016).

7 BSI, IT-Grundschutz-Kataloge, S. 2.

8 Für eine einfache Zuordnung der Maßnahmen des IT-Grundschutzes und deren Entsprechungen zur ISO 27001-Norm hat das BSI eine Zuordnungstabelle veröffentlicht, abrufbar ist diese unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Hilfsmittel/Doku/Vergleich_ISO27001_GS.html (Stand: 16.9.2016).

9 BT-Drs. 18/5121, S. 15.

10 *Harich*, IT-Sicherheitsmanagement, S. 327 ff.

11 DIN ISO/IEC 27001, S. 14.

12 *Mangiapane/Büchler*, Modernes IT-Management, S. 13.

vement and Capability Determination) aufgestellt.[13] SPICE sieht dabei eine Abbildung über 6 Stufen (Level 0 bis 5) vor:[14]

Tabelle 1 | Reifegradstufen nach SPICE

Level	Übersetzung	Bedeutung
0	Unvollständig	Ein Prozess wird nicht durchgeführt oder ist nicht vorhanden.
1	Durchgeführt	Der Prozess erfüllt seinen Zweck.
2	Gesteuert	Der Prozess wird systematisch geplant und kontrolliert.
3	Etabliert	Der Prozess wird über die gesamte Organisation einheitlich durchgeführt.
4	Vorhersagbar	Der Prozess wird systematisch gemessen und kontrolliert.
5	Optimiert	Es gibt Ziele zur Prozessverbesserung und die Auswirkungen der Optimierung werden gemessen.

Für das IT-Sicherheitsaudit wird das SPICE-Modell zur Ermittlung des individuellen Reifegrads genutzt. Dabei werden für jeden zu untersuchenden Prozess jeweils nach SPICE zu erfüllende Kriterien aufgestellt, anhand derer dessen Reifegrad beurteilt werden kann.

3.2 Durchführung des IT-Sicherheitsaudits

Im Rahmen des Audits werden die allgemeinen Anforderungen an das ISMS und insbesondere die vorhandenen technischen und organisatorischen Maßnahmen untersucht. Technische Maßnahmen können zum Beispiel die Mittel zum physischen Schutz des IT-Systems, sowie die Sicherheit in Soft- und Hardware betreffen. Organisatorische Maßnahmen umfassen beispielsweise Handlungsanweisungen innerhalb von Betrieben und Organisationen. Das Audit besteht aus insgesamt vier miteinander zusammenhängenden Arbeitsschritten, die in folgender Reihe durchgeführt werden:

- initiale Befragung des IT-Verantwortlichen beim Betreiber der Infrastruktur,
- Begehung der Räumlichkeiten des zentralen Verwaltungsgebäudes,
- Begehung der Räumlichkeiten der eigentlichen Versorgungsanlage,
- Besprechung des Audits mit dem IT-Verantwortlichen, Fixierung der Ergebnisse.

Besondere Berücksichtigung für den gesamten Auditierungsprozess findet die Tatsache, dass das ISMS als flexibles Rahmenwerk die IT-Sicherheit als fortlaufenden Prozess beschreibt, der den Aufbau, die Umsetzung sowie die regelmäßige Kontrolle und Anpassung des IT-Sicherheitskonzepts erfordert.[15]

3.3 Ergebnisse des IT-Sicherheitsaudits

Im Folgenden werden die zentralen Ergebnisse des Auditierungsprozesses beim Wasserversorger dargestellt. Im Bereich der „Allgemeinen Informationen" zur IT-Infrastruktur wurde festgestellt, dass mit der Netzwerkbetreuung, Administration und IT-Beratung ein externer IT-Dienstleister beauftragt wurde und zusätzlich ein externer Datenschutzbeauftragter (DSB) bestellt wurde. Die zentrale Schnittstelle zwischen IT-Dienstleister, DSB und Betreiber der Infrastruktur ist der interne IT-Verantwortliche. Die Verantwortlichkeiten für die Organisation der IT-Sicherheit sind durch den Organisationsplan des Unternehmens festgelegt und allen Mitarbeitern bekannt. Eine Sammlung von Informationssicherheitsrichtlinien oder ein Betriebshandbuch ist nicht vorhanden. Alle Fragen, die das Wissen des IT-Verantwortlichen überschreiten, werden an den externen IT-Dienstleister weitergegeben. Auf Seiten der Mitarbeiter besteht mangels regelmäßiger Schulungen wenig Bewusstsein bezüglich der Bedeutung von IT-Sicherheit („Awareness"). Auch das Wissen des IT-Verantwortlichen beruht größtenteils auf Selbststudium.

Im Hinblick auf die Zugangssteuerung ist festzuhalten, dass die Nutzung des IT-Systems durch die Vergabe von passwortgeschützten User-IDs geregelt wird. Die System-Passwörter müssen alle drei Monate erneuert werden. Die Vergabe, Verwaltung und Löschung von Systemzugängen wird allein durch den IT-Verantwortlichen vorgenommen. Die Datensicherheit ist nicht durch ein etabliertes Verschlüsselungsverfahren geschützt, ebenso erfolgt keine digitale Signierung von E-Mails oder Dokumenten.

Die Betriebsabläufe des Unternehmens haben sich vor allem durch ihre wiederholte Anwendung und Nutzung etabliert. Das Verwaltungsnetzwerk wird durch eine Firewall geschützt. Der Serverraum verfügt über eine eigene Sicherungsschaltung und ist vom restlichen Netz getrennt. Auch findet eine automatisierte Datensicherung statt. Die Anschaffung, Entwicklung und Instandhaltung von Systemen wird in Absprache mit dem externen IT-Dienstleister erarbeitet und vorgenommen.

Es gibt kein dokumentiertes Vorgehen für den Umgang mit Informationssicherheitsvorfällen. Eine Verbesserung der IT-Sicherheit wurde durch den externen IT-Dienstleister in Bezug auf die Vernetzung der Steuerungsanlagen bereits angestoßen. Dabei wurde eine Umstellung auf die Nutzung eines gesicherten VPN-Tunnels je Anlage erreicht. Auffällig ist dabei, dass die Steuersysteme der eigentlichen Versorgungsanlagen nicht als echter Bestandteil der internen IT betrachtet werden. Eine Dokumentation der Systeme lag nicht vor, die Verantwortung wird vollständig auf die mit der Wartung beauftragten Anlagenhersteller übertragen.

Im Gesamtergebnis erreicht der Betreiber einen durchschnittlichen Reifegrad von 1,15 bei einem Zielreifegrad von 3,07. Daraus ergibt sich zusammenfassend, dass das derzeitige Sicherheitsmanagement des Versorgers den Anforderungen der ISO 27001 nicht genügt. Die im Einzelnen für das IT-Sicherheitsaudit erreichten Reifegradstufen sind in Tabelle 2 dargestellt.

3.4 Handlungsempfehlungen

Abgeleitet aus den Ergebnissen des IT-Sicherheitsaudits können verschiedene allgemeine Handlungsempfehlungen zur Vermeidung typischer Schwachstellen beim Betrieb Kritischer Infrastrukturen gegeben werden. Im Mittelpunkt der Betrachtung stehen vor allem solche Betreiber, die bisher kein definiertes Sicherheitskonzept besaßen, nunmehr aber durch die Anforderungen des IT-SiG erfasst werden. Daneben sind die Empfehlungen auch für KMUs interessant, die nach wie vor keine Informationssicherheit nach dem Stand der Technik vorweisen müssen, jedoch freiwillig ihren status quo zu verbessern gedenken.

Die Dokumentation von IT-Sicherheitsvorfällen ist nicht nur im Hinblick auf die Umsetzung der Anforderungen des IT-SiG

13 *Harich*, IT-Sicherheitsmanagement, S. 376.
14 *Mangiapane/Büchler*, Modernes IT-Management, S. 14.
15 Vgl. BSI, IT-Grundschutz-Kataloge, S. 108.

Tabelle 2 | Übersicht der Ergebnisse des IT-Sicherheitsaudits

Zielwert	Erreicht	Abschnitt
3	0,67	Allgemeine Informationen (Referenz zu ISO 27002: A.4)
3	1	Informationssicherheitsrichtlinien (Referenz zu ISO 27002: A.5)
3	1,67	Organisation der Informationssicherheit (Referenz zu ISO 27002: A.6)
3,5	0,5	Personalsicherheit (Referenz zu ISO 27002: A.7)
2,67	1,33	Verwaltung der Werte (Referenz zu ISO 27002: A.8)
3,2	1,8	Zugangssteuerung (Referenz zu ISO 27002: A.9)
2	0	Kryptographie (Referenz zu ISO 27002: A.10)
2,67	1,67	Physische und umgebungsbezogene Sicherheit (Referenz zu ISO 27002: A.11)
3,14	1	Betriebssicherheit (Referenz zu ISO 27002: A.12)
3	1	Kommunikationssicherheit (Referenz zu ISO 27002: A.13)
3	1	Anschaffung, Entwicklung und Instandhalten von Systemen (Referenz zu ISO 27002: A.14)
3	1	Lieferantenbeziehungen (Referenz zu ISO 27002: A.15)
4	0,5	Handhabung von Informationssicherheitsvorfällen (Referenz zu ISO 27002: A.16)
3	1	IT-Sicherheitsaspekte beim Business Continuity Management (BCM, Referenz zu ISO 27002: A.17)
3,33	1,33	Compliance (Referenz zu ISO 27002: A.18)

von Interesse, sondern ebenso aus Gesichtspunkten der zivilrechtlichen Haftung, sollte es durch den Betriebsausfall zu Vermögensschäden kommen. Die Norm ISO 27001 stellt deshalb umfangreiche Anforderungen an eine umfassende Dokumentation der Geschäftsprozesse eines Unternehmens. Für eine solche Dokumentation muss die Unternehmensführung ausreichende Ressourcen bereitstellen und nachhaltig die Umsetzung vorantreiben. Daher sollten alle Unternehmenswerte umfassend inventarisiert und alle relevanten Geschäftsprozesse durch ein Betriebshandbuch festgestellt werden. Des Weiteren sind die Durchführung einer Risikoanalyse zur Identifizierung von Schwachstellen sowie die Einstufung von Informationen hinsichtlich ihres Schutzbedarfs notwendig. Außerdem sollten Richtlinien zum Umgang mit mobilen und ungenutzten Geräten und Datenträgern sowie zur Datenvernichtung aufgestellt oder – soweit vorhanden – auf Zweckmäßigkeit hin geprüft und gegebenenfalls verschärft werden. Zudem ist die Einführung einer sogenannten „Clean-Desk-Policy" zu empfehlen. In diesem Zuge sollten einheitliche Besucherregeln festgesetzt werden, die auch den organisatorischen Umgang mit Fremdpersonal und externen Partnern adressieren. Ergänzend sollte die Dokumentation einer Vertretungsregelung angestrebt werden

In Anbetracht der für die Zivilgesellschaft hochrangigen Funktion als Betreiber einer Kritischen Infrastruktur sollten vorab schriftliche Handlungsanweisungen für Notsituationen/Ausnahmefälle fixiert und hierbei klare personelle Rollen zugewiesen werden. Insbesondere sollten Maßnahmen gegen Naturkatastrophen, vorsätzliche Angriffe und Unfälle dokumentiert werden. Die entsprechende Dokumentation sollte jedem Mitarbeiter zur Verfügung stehen. Ebenso müssen Prozesse protokolliert werden. Die Steuerungssysteme sind in das Patch-Management der Gesamt-IT zu integrieren.

Um einen Notbetrieb und schnelle Reaktionsfähigkeit zu gewährleisten, sind alle relevanten Ansprechpartner innerhalb des Unternehmens und für unter Umständen zuständige Behörden aktuell aufzulisten. Die Umsetzung von Maßnahmen sollte geprobt werden.

Falls der Aufbau eines ISMS geplant ist, sollte der Entwicklungsfortschritt ebenso dokumentiert werden. Auch hier zeigt sich folglich wieder, dass IT-Sicherheit als ein fortwährender Prozess zu begreifen ist. Interne Audits oder, soweit das hierfür notwendige Know-how nicht zur Verfügung steht, Audits durch externe Prüfstellen, werden empfohlen. Soweit ein Datenschutzbeauftragter (gesetzlich) bestellt ist, kann auch dieser schon wertvolle Informationen und Handlungsanweisungen zur Verfügung stellen.

Nicht wenige Unternehmen verlassen sich, soweit es um die IT-Sicherheit geht, auf den Sachverstand externer Anbieter. Auch hier gilt aber, dass IT-Sicherheit kein selbstständiger Vorgang ist, der mit der Beauftragung eines Unternehmens beginnt und zugleich auch endet. So sollten auch im Umgang mit externen Partnern regelmäßige Qualitätsprüfungen der erbrachten Leistungen erfolgen, in denen der Fortschritt von Projekten und die Einhaltung von Anforderungen an die Organisation des Partners kontrolliert werden.

Speziell zur Gewährleistung der Schutzziele Datenauthentizität und Datenintegrität empfiehlt es sich, elektronische Signaturen und Verschlüsselungstechnologien bei E-Mail-Versand und -empfang einzurichten. (Back Up)-Daten sollten ebenso verschlüsselt werden, um eine verlässliche Dokumentation zu gewährleisten.

„Awareness" ist ein Begriff, der, soweit es um die IT-Sicherheit geht, schon fast als Modewort gelten kann, jedoch kaum aktiv gelebt wird. Nicht selten wird sich damit begnügt, ein Handbuch zu erwerben, abzustellen und auf die intrinsische Motivation der Einsichtnahme zu hoffen. Da IT-Sicherheit aber als fortlaufender Prozess zu begreifen ist, sollte dies auch für die Awareness gelten, die somit nur durch regelmäßige Coachings und Mitarbeiterschulungen erreicht werden kann.

Soweit es die Datensicherheit betrifft, ist es höchst empfehlenswert, redundante technische Systeme wie auch organisatorische Strukturen zu errichten. Wenn eine Meldepflicht nach § 8b BSIG oder den entsprechenden spezialgesetzlichen Vorschriften bestehen sollte, müssen relevante IT-Sicherheitsvorfälle standardisiert dokumentiert und behandelt werden, um Vergleichbarkeit zu gewährleisten und Angriffsmuster erkennen zu können. Hierzu bietet es sich an, verschiedene Eskalationsstufen zu identifizieren.

Last but not least umfasst IT-Sicherheit auch bauliche Schutzmaßnahmen. Hierzu gehören der Brandschutz des Serverraums sowie der Archivräume. Hinreichend eng gefasste Zutritts- und Zugangsregelungen zur zentralen Anlagensteuerung der Kritischen Infrastruktur sind ebenso zu implementieren. Eine Zugangsmöglichkeit ohne vorherige Authentifizierung darf nicht bestehen. Weiterhin wird empfohlen, Anlagengebäude besser gegen Einbruch zu sichern. Statusinformationen der Anlagen können über reine Monitoring-Stationen sichtbar gemacht werden.

4 Fazit und Ausblick

Die beispielhafte Untersuchung der IT-Sicherheit eines Betreibers Kritischer Infrastrukturen hat gezeigt, dass auch über ein Jahr nach Inkrafttreten des IT-SiG noch nicht von einem einheitlich hohen IT-Sicherheitsstandard ausgegangen werden kann. So wäre für den untersuchten Fall keine Zertifizierung nach ISO 27001 möglich gewesen.

Die als Problemstellung im ersten Abschnitt aufgeworfene Frage hingegen, ob ein Mindeststandard der IT-Sicherheit auf dem Stand der Technik gemäß den Anforderungen des IT-SiG durch etablierte Methoden eines ISMS umgesetzt werden kann, ist im Wesentlichen zu bejahen. Denn das ISMS als flexibles Rahmenwerk trägt entscheidend dazu bei, dass IT-Sicherheit von Beginn an als dauerhafter Prozess begriffen wird, welcher sich an der der technischen Entwicklung folgenden Ausfüllung des unbestimmten Rechtsbegriffs „Stand der Technik" orientiert. Was als Maßnahme früher noch dem hochinnovativen „Stand von Wissenschaft und Technik" entsprach, entwickelt sich mit der zunehmend Verbreitung und Anerkennung zum „Stand der Technik" weiter, um schließlich als „allgemein anerkannte Regel der Technik" nicht mehr den Vorgaben des IT-SiG zu genügen.[16] Insoweit kann das Rahmenwerk der ISO 2700X auch als Hilfestellung begriffen werden, als Betreiber stets diejenigen Maßnahmen zu ergreifen, die gerade den Stand der Technik wiedergeben. Insoweit kommt es bei der Beurteilung des „Standes der Technik" in der praktischen Umsetzung auch nicht unbedingt darauf an, welche IT-Sicherheitsmaßnahmen gerade aktuell sind, sondern dass regelmäßig überprüft wird, dass die getroffenen Vorkehrungen noch den zum jeweiligen Zeitpunkt einschlägigen Maßnahmen entsprechen – von dieser Bürde kann der Betreiber einer Kritischen Infrastruktur folglich auch nicht entbunden werden. Die Kontrolle des Reifegrades der getroffenen Prozesse durch (externe) Auditoren wird hier jetzt und in Zukunft eine bedeutende Rolle spielen. Für den Regelfall wird davon auszugehen sein, dass wenn ein ISMS einen Zielreifegrad von mindestens 3 („Gesteuert") erfüllt, dies eine entsprechende Prozesskontrolle impliziert, durch die festgestellt werden kann, ob das Schutzziel erreicht ist oder neue Maßnahmen getroffen werden müssen. Dadurch ist die Überprüfung der Einhaltung des Standes der Technik sichergestellt. Die in diesem Beitrag gegebenen Handlungsempfehlungen geben in aller Kürze diejenigen technischen Vorgaben wieder, die unter Zugrundelegung des ISMS aktuell mit den Anforderungen des Standes der Technik konform sind und für den untersuchten Versorger das Minimum für den ersten Schritt des Aufbaus eines ISMS darstellen.

Im Hinblick auf die Bestimmung branchenspezifischer Sicherheitsstandards gem. § 8a Abs. 2 BSIG kann festgestellt werden, dass für die allermeisten Sektoren Kritischer Infrastrukturen vergleichbare physische Strukturen zum Einsatz kommen, sodass folglich auch die Beurteilung potenzieller Bedrohungslagen und damit auch die zu ergreifenden technischen und organisatorischen Gegenmaßnahmen deutliche Parallelen aufweisen. In Bezug auf die Vollständigkeit der Maßnahmen zur Umsetzung der IT-Sicherheit ergibt sich daraus die Frage, ob es Anlagen(teile) gibt, die nicht durch ein ISMS nach ISO 27001 mit eingeschlossen werden können. Um diese Einzelheiten auf der Grundlage von ISO 27001 zu ergänzen, bedürfte es branchenspezifischer Sicherheitsstandards, die zusätzliche, über die Norm hinausgehende Anforderungen regeln. Teils werden spezielle Assets aber auch schon durch die ISO-Standards selbst adressiert, so zum Beispiel für den Gesundheitssektor durch die ISO 27799 (Health informatics – Information security management in health using ISO/IEC 27002).

Zur Beantwortung der weiteren Frage, welche zusätzlichen Anforderungen durch die Verpflichtung kritischer Infrastrukturbetreiber, sicherheitskritische Vorfälle zu melden, entstehen und wie diesen entsprochen werden kann, ist festzustellen, dass nach wie vor nicht abschließend und im Einzelnen geklärt ist, wann genau die Meldepflicht auslöst und welche Informationen zur Erfüllung von § 8b Abs. 4 BSI-Gesetz tatsächlich genügen. Insbesondere hier zeigt sich, dass der Umsetzungsprozess der Vorgaben aus dem IT-SiG zurzeit noch fortdauert. Für viele Betreiber ist diese Erkenntnis unbefriedigend, dennoch stellt sich die Frage, welche technisch-organisatorischen Maßnahmen zur Realisierung der Meldepflicht bereits jetzt getroffen werden können.[17] Auch hier bietet das ISMS mit seinem konzeptionalisierten Vorgehen zur Verbesserung der IT-Sicherheit entscheidende Hilfestellungen an: So sieht dieses von sich aus bereits umfangreiche Dokumentationsvorgaben zur Protokollierung von Zugangs-, Zutritts-, Zugriffs- und weiterer Regeln vor. Auch IT-Security-Incidents sind als Bestandteil des fortlaufenden Prozesses zu dokumentieren. Die Einrichtung des ISMS trägt somit nicht nur den Verpflichtungen aus § 8a BSIG, sondern ebenso denjenigen aus § 8b BSIG Rechnung.

Im Ergebnis kann festgestellt werden, dass mit einem gut aufgebauten ISMS den Vorgaben des IT-SiG tatsächlich entsprochen werden kann. Wichtig bei der Umsetzung ist, dass zwischen verschiedenen domänenspezifischen Infrastrukturen innerhalb einer Organisation nicht unterschieden wird, sondern alle Anlagen und Systeme gleichwertig behandelt werden. Die Implementierung des Informationssicherheitsmanagements nach ISO 2700X ist deshalb für Betreiber Kritischer Infrastrukturen empfehlenswert, obgleich dies vor allem für KMUs mit einer erheblichen Arbeitsbelastung verbunden sein kann. Nichtsdestotrotz stellt das ISMS auch im Vorgriff auf die am 8. August 2016 in Kraft getretene europäische NIS-RL[18] ein geeignetes Mittel zur Umsetzung effektiver Informationssicherheit im Unternehmen dar.

Der Autoren besonderer Dank gilt Lena Specker, Mitarbeiterin des BMBF-Förderschwerpunkts ITS|KRITIS, für ihre hilfreiche Unterstützung zur Vorbereitung dieser Publikation.

16 Siehe zur näheren Erläuterung dieser Trias gesetzgeberisch anerkannter Begriffe des Technikrechts BMJV, Handbuch der Rechtsförmlichkeit, Rn. 252 ff.

17 Teils wird zur Konkretisierung der Meldepflicht auf Anlage 1 zur Allgemeinen Verwaltungsvorschrift über das Meldeverfahren gem. § 4 Abs. 6 BSIG verwiesen, welche eine Auflistung erheblicher Sicherheitsvorfälle enthält, die als Orientierungswert herangezogen werden können.

18 Siehe hierzu und im Vergleich zum IT-SiG detailliert *Kipker*, ZD-Aktuell 2016, 05261.