Ulrike Lechner | Sebastian Dännart | Andreas Rieb | Steffi Rudel

CASE|KRITIS

Fallstudien zur IT-Sicherheit in Kritischen Infrastrukturen

λογος

Bibliografische Information der Deutschen Nationalbibliothek

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

Lektorat: Dr. Heiner Lohmann, www.lektorat-lohmann.de

Coverdesign: Artes Advertising, www.artes.de

© Coverbild: iStockphoto

ISBN 978-3-8325-4727-1

Logos Verlag Berlin GmbH
Comeniushof, Gubener Str. 47,
10243 Berlin
Tel.: +49 (0)30 42 85 10 90
Fax: +49 (0)30 42 85 10 92
INTERNET: http://www.logos-verlag.de

Inhaltsverzeichnis

1.3 Gesetzliche Anforderungen an die IT-Sicherheit in Deutschland und Europa

Dennis-Kenji Kipker, Universität Bremen
Benedikt Buchner, Universität Bremen

Während sich früher die Verpflichtung zur Realisierung angemessener IT-Sicherheitsmaßnahmen vorwiegend aus allgemeinen gesetzlichen Rahmenvorschriften ergab und zur Einhaltung nicht näher bestimmter Sorgfaltspflichten, die keinen unmittelbaren IT-Sicherheitsbezug aufwiesen, gehörte, hat insbesondere seit dem Jahr 2015 eine umfassende rechtliche Regulierung speziell der IT-Sicherheit stattgefunden, die in politischer Hinsicht auf den deutschen und europäischen Cybersicherheitsstrategien basiert. Seither ist es erstmals möglich, insbesondere auch für den Schutz von Einrichtungen, denen für das Funktionieren des Gemeinwesens eine besonders hohe Bedeutung zukommt – den sogenannten Kritischen Infrastrukturen – einen einheitlichen Rechtsrahmen vorzuhalten.

Auf nationaler und europäischer Ebene sind in diesem Zusammenhang im Wesentlichen bisher vier Rechtsakte zu benennen, die unter Gesichtspunkten der Cybersicherheit eine besondere Aufmerksamkeit verdienen: das deutsche IT-Sicherheitsgesetz (IT-SiG) aus 2015; die Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-KritisV) aus 2016 und 2017; die EU-Richtlinie 2016/1148 „über Maßnahmen zur Gewährleistung einer hohen gemeinsamen Netz- und Informationssicherheit in der Union" (EU NIS-RL) aus 2016, die im Jahr 2017 durch ein Umsetzungsgesetz in das deutsche Recht implementiert wurde, sowie der Entwurf einer Verordnung über die „EU-Cybersicherheitsagentur" (ENISA) sowie über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik („Rechtsakt zur Cybersicherheit").

Das deutsche IT-SiG war der erste Rechtsakt, der einen Fokus auf die IT-Sicherheit speziell der Kritischen Infrastrukturen legte. Basierend auf der Cybersicherheitsstrategie der Bundesregierung aus dem Jahr 2011 trat das Gesetz am 25. Juli 2015 in Kraft und zielt auf eine „signifikante Verbesserung der Sicherheit informationstechnischer Systeme in Deutschland" ab. Zu solchen IT-Systemen gehören aber nicht nur große Unternehmensnetzwerke, sondern auch der vernetzte Anwender-PC, sodass unter anderem auch der Verbraucher in die Betrachtung ganzheitlicher Cybersecurity einbezogen wird. Zur allgemeinen Verbesserung der Cybersecurity wird das Bundesamt für Sicherheit in der Informationstechnik (BSI) als zentrale deutsche Informationssicherheitsbehörde gestärkt und erfährt einen laufenden Ausbau. In praktischer Hinsicht ist anzumerken, dass die Verpflichtungen aus dem IT-SiG keine unmittelbare Wirkkraft gegenüber Unternehmen und Bürger entfalten: Da es sich bei dem IT-SiG um ein Artikelgesetz handelt, werden durch dieses lediglich verschiedene und bereits bestehende einzelgesetzliche Vorschriften modifiziert und ergänzt, zum Beispiel das Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSIG), das Telekommunikationsgesetz (TKG) und das Telemediengesetz (TMG). Dies hat zur Folge, dass trotz der Regelungen des IT-SiG weiterhin auf die bestehenden Einzelgesetze zur IT-Sicherheit Bezug genommen wird. Die umfangreichsten Anpassungen durch das IT-SiG hat das BSIG erfahren. So werden neuerdings in § 2 Abs. 10 BSIG Kritische Infrastrukturen definiert als Einrichtungen, Anlagen oder Teile davon, die den Sektoren Energie, Informationstechnik und Telekommunikation (IuK), Transport und Verkehr, Gesundheit, Wasser, Ernährung sowie Finanz- und Versicherungswesen angehören und von hoher Bedeutung für das Funktionieren des Gemeinwesens sind, weil durch ihren Ausfall oder durch ihre Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit eintreten würden. Die Betreiber der in diesem Sinne bestimmten Infrastrukturen trifft eine Reihe von Pflichten zur Verbesserung der IT-Sicherheit. Zentral sind hier die Änderungen, die durch die §§ 8a und 8b BSIG vorgegeben werden: Zuvorderst besteht die Anforderung, angemessene organisatorische und technische Vorkehrungen (TOV) zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit der informationstechnischen Systeme, Komponenten oder Prozesse zu treffen, die für die Funktionsfähigkeit der betriebenen Kritischen Infrastruktur maßgeblich sind. Dabei soll der Stand der Technik eingehalten werden. Dieser unbestimmte Rechtsbegriff ist vor allem durch die technische Normung und Standardisierung auszufüllen (Kipker, 2016c)[1]. § 8b BSIG regelt über die in § 8a BSIG normierten TOV hinausgehend den Umgang mit IT-Sicherheitsinformationen. Dazu hat das BSI einen Ausbau als zentrale Meldestelle für Betreiber unter anderem von Kritischen Infrastrukturen in Angelegenheiten der Sicherheit in der Informationstechnik erfahren. So hat die Behörde auch die Aufgabe, die für die Abwehr von Gefahren für die IT-Sicherheit relevanten Informationen zu sammeln und auszuwerten und die Betreiber sowie die (Aufsichts-)Behörden über kritische Vorgänge zu informieren. Damit korrespondierend trifft die Betreiber die Verpflichtung, eine Kontaktstelle einzurichten, um für die Unterrichtungen des BSI jederzeit erreichbar zu sein.

1 Ein Tool zur Bestimmung des „Standes der Technik" für einzelne Sektoren und Branchen im Umfeld von Industrie 4.0 und KRITIS stellt der „IT-Security NAVIGATOR" dar (ITSKRITIS 2017).

Diese Kontaktstelle dient aber nicht nur der Informationsentgegennahme, sondern ebenso der Durchführung von eigenständigen Meldungen an das BSI, zu denen die neuen gesetzlichen Vorgaben verpflichten. Demgemäß haben die Betreiber unverzüglich Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse, die zu einem Ausfall oder zu einer erheblichen Beeinträchtigung der Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastruktur geführt haben, oder erhebliche Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse, die zu einem Ausfall oder zu einer erheblichen Beeinträchtigung der Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastruktur führen können, zu melden. Die Meldung kann grundsätzlich pseudonym[2], also ohne direkte Namensnennung des Betreibers, erfolgen, es sei denn, dass die Störung tatsächlich zu einem Ausfall oder einer Beeinträchtigung der Funktionsfähigkeit der Kritischen Infrastruktur geführt hat. Die Meldung an das BSI muss unter anderem Angaben zur Störung, zu den Auswirkungen und zu den technischen Rahmenbedingungen sowie zur vermuteten oder tatsächlichen Ursache enthalten, soweit diese Informationen dem Betreiber in der konkreten Situation zur Verfügung stehen.

Das IT-SiG umschreibt zwar die wesentlichen rechtlichen Anforderungen, die für die Betreiber der Kritischen Infrastrukturen gelten, legt jedoch nicht fest, welche Betreiber und Anlagen im Einzelnen unter die gesetzlichen Vorgaben fallen. Hier beschränkt sich das Gesetz in § 2 Abs. 10 BSIG auf die bloße Benennung von einzelnen Sektoren. Nach Inkrafttreten des IT-SiG gab es deshalb einen erheblichen Raum für Spekulationen, welche Unternehmen tatsächlich von den neuen Vorgaben betroffen sein würden. Klärung hat hier die BSI-KritisV gebracht, die vom Bundesministerium des Innern (BMI) nach Maßgabe des § 10 Abs. 1 S. 1 BSIG erlassen wurde. Basierend auf den sogenannten Sektorstudien des BSI, welche die Bereiche Energie, Ernährung und Wasser, Gesundheit, Finanz- und Versicherungswesen, Informationstechnik und Telekommunikation, Transport und Verkehr, Logistik sowie Medien und Kultur abdecken, wurde anhand der Berechnung von sogenannten Schwellenwerten ermittelt, welche Anlagenkategorien im Einzelnen als Kritische Infrastrukturen im Sinne des IT-SiG anzusehen sind (Kipker, 2016a). Zunächst wird dabei im Rahmen eines dreistufigen Verfahrens ermittelt, welche der im jeweiligen Sektor erbrachten Dienstleistungen aufgrund ihrer Bedeutung generell als kritisch anzusehen sind. In einem zweiten Schritt werden diejenigen Kategorien von Anlagen identifiziert, die für die Erbringung der zuvor ermittelten kritischen Dienstleistung erforderlich sind. Im dritten und zugleich letzten Schritt wird ermittelt, welche konkreten Anlagen oder Teile davon einen aus gesamtgesellschaftlicher Sicht bedeutenden Versorgungsgrad aufweisen; dies sowohl unter Qualitäts- wie auch unter Quantitätsgesichtspunkten. Bewusst hat der Gesetzgeber für die Bestimmung der konkreten Kritischen Infrastrukturen das Rechtsinstrument der Verordnung gewählt, da diese als untergesetzlicher, ministerieller Rechtsakt in der Lage ist, schneller auf eine Änderung der technischen Rahmenbedingungen zu reagieren, als dies durch ein formelles Parlamentsgesetz möglich ist. Die

2 In Abgrenzung zur anonymen Meldung, die gesetzlich jedoch nicht vorgesehen ist, ermöglicht die pseudonyme Meldung für die Behörde aber immer noch die Zuordnung des individuellen Betreibers.

BSI-KritisV zur Konkretisierung des Anwendungsbereiches der aus dem IT-SiG folgenden Regelungen erschien in zwei sogenannten Körben, wovon der zweite mit den Sektoren Gesundheit, Finanz- und Versicherungswesen sowie Transport und Verkehr erst am 30. Juni 2017 seine Rechtskraft entfaltet hat, wohingegen der Entwurf des ersten Korbes schon zu Beginn 2016 veröffentlicht wurde (Kipker, 2017b).

Die Europäische Union verfolgt bei der gesetzlichen Regulierung der IT-Sicherheit einen Ansatz, der über die Kritischen Infrastrukturen des deutschen Rechts hinausgeht und im Besonderen auch auf den Schutz des digitalen europäischen Binnenmarktes abzielt. Im Mittelpunkt steht dabei die EU NIS-RL, die als Wegbereiter zur Umsetzung der europäischen Cybersicherheitsstrategien von 2013 und 2017 gesehen werden kann. Neben neuen Anforderungen an die Betreiber von „wesentlichen Diensten", die maßgeblich den deutschen Kritischen Infrastrukturen entsprechen, zielt die NIS-RL vor allem auch auf digitale Dienste ab und geht damit zumindest in ihrem Anwendungsbereich zunächst über das nationale Recht hinaus (Kipker 2016b). Als europäische Richtlinie, die im Gegensatz zum EU-Rechtsetzungsakt der Verordnung gemäß Art. 288 des Vertrages über die Arbeitsweise der Europäischen Union (AEUV) keine unmittelbare Geltung in den Mitgliedstaaten besitzt, sondern nur hinsichtlich des zu erreichenden Ziels verbindlich ist, den Mitgliedstaaten aber die Wahl der Form und der Mittel zur Zielerreichung offenlässt, muss die NIS-RL durch ein Umsetzungsgesetz in den nationalen Rechtsrahmen überführt werden, um dort grundsätzlich Wirksamkeit zu entfalten. Für Deutschland ist dies durch das „Gesetz zur Umsetzung der Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union" geschehen. Das Umsetzungsgesetz zur EU NIS-RL hat am 27. April 2017 den Deutschen Bundestag passiert, wodurch einige der Rechtsvorschriften, die bereits durch das IT-SiG neu geschaffen oder novelliert worden waren, eine weitere Anpassung erfuhren (Kipker 2017c). Im Mittelpunkt stehen dabei die neuen Anforderungen für digitale Dienste: Nach § 2 Abs. 11 BSIG sind hierunter vor allem solche Dienste der Informationsgesellschaft zu verstehen, die es Verbrauchern oder Unternehmern ermöglichen, Kauf- oder Dienstleistungsverträge auf Online-Marktplätzen abzuschließen, und Dienste, die es Nutzern gestatten, bestimmte Suchanfragen im Internet durchzuführen – Online-Suchmaschinen –, sowie Cloud-Computing-Dienste, die den Zugang zu einem skalierbaren und elastischen Pool von gemeinsam genutzten Rechenressourcen gewährleisten. Kleinstunternehmen und kleine Unternehmen im Sinne der Empfehlung 2003/361/EG der EU-Kommission sind gemäß Art. 16 Abs. 11 EU NIS-RL hiervon aber ausgenommen. Für die betroffenen Anbieter von digitalen Diensten gelten nach den neuen, in das deutsche Recht umgesetzten europarechtlichen Vorgaben mit Kritischen Infrastrukturen vergleichbare Anforderungen. So sind gemäß § 8c BSIG angemessene technische und organisatorische Maßnahmen (TOM) zu treffen, um die Funktionsfähigkeit der digitalen Dienste in der EU sicherzustellen, ebenso besteht nach Realisierung erheblicher IT-Sicherheitsvorfälle eine Meldepflicht an das BSI.

Auf Basis der EU NIS-RL hat die Europäische Union im Herbst 2017 den Entwurf eines weiteren Rechtsakts im Bereich der Cybersicherheit veröffentlicht, die Verordnung über die „EU-Cybersicherheitsagentur" (ENISA) und zur Aufhebung der Verordnung (EU) Nr. 526/2013

sowie über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik („Rechtsakt zur Cybersicherheit"), die gemeinhin auch als „Cybersecurity-Verordnung" bezeichnet wird. Als Verordnung, die einen Kernbestandteil der neuen europäischen Cybersicherheitsstrategie (Kipker 2017d) darstellt, gilt das neue Gesetz unmittelbar in allen Mitgliedstaaten der Europäischen Union und bedarf deshalb keines nationalen Umsetzungsaktes mehr, wie dies noch für die EU NIS-RL der Fall gewesen ist. Die Anforderungen der Cybersecurity-Verordnung gehen inhaltlich weit über Kritische Infrastrukturen hinaus und zielen auf die Regulierung des gesamteuropäischen, digitalen Binnenmarktes ab. Im Mittelpunkt steht dabei die Schaffung eines europaweit einheitlichen Zertifizierungsrahmens für die IT-Sicherheit von Produkten und Diensten der Informations- und Kommunikationstechnik, sodass das Anbieten grenzüberschreitender digitaler Dienste in Zukunft eine deutliche Erleichterung erfahren wird. Hierbei wird die ENISA als Marktbeobachtungsstelle fungieren und unter anderem auch neue Normen zur Cybersicherheit aktiv mitgestalten (Kipker 2017e).

Im Ergebnis ist festzustellen, dass nicht nur die nationale, sondern auch die EU-weite rechtliche Regulierung von Cybersicherheit zunehmend an Fahrt gewinnt. Während zunächst vor allem die Kritischen Infrastrukturen zentraler Anknüpfungspunkt des gesetzgeberischen Handelns waren, werden die neuen Vorgaben zunehmend branchenübergreifend realisiert und stellen vor allem wirtschaftliche Schutzgüter in den Vordergrund – dies nicht nur im Bereich des produzierenden Gewerbes der Industrie 4.0, sondern auch speziell bezogen auf digitale Dienste, die mittlerweile einen erheblichen Anteil des europäischen Binnenmarktes ausmachen. Doch nicht nur in Deutschland und der EU haben die Gesetzgeber die hohe Bedeutung von funktionierenden IT-Systemen erkannt – so finden sich neue Regulierungsansätze auch in China (Kipker 2017a) und in Japan. Insbesondere in Japan, wo bisher keine speziellen IT-Sicherheitsgesetze existierten, steht die Sicherheit von Produkten des Internet of Things (IoT) im Vordergrund.[3] Darüber hinausgehend übernimmt der britische Gesetzgeber trotz des Austritts aus der EU wesentliche Vorgaben der neuen europäischen IT-Sicherheitsgesetzgebung (Kipker & Stelter, 2017). Mit der EU Datenschutz-Grundverordnung (EU DS-GVO), die vor allem in Art. 32 wesentliche Datensicherheitsanforderungen bestimmt und ab dem 25. Mai 2018 anzuwenden ist, rückt zudem die Verknüpfung von technischer IT-Sicherheit und Datenschutz immer weiter in den Vordergrund. Diese Entwicklung verdeutlicht, dass das Thema der IT-Sicherheit nicht nur zunehmend an Bedeutung gewinnt, sondern zugleich ein domänenübergreifendes und vorwiegend interdisziplinär geprägtes Arbeitsfeld darstellt, das eine rein branchenspezifische Betrachtung von Bedrohungslage und Gegenmaßnahmen obsolet macht.

Der Begriff des „Stands der Technik" beschreibt, welchen Anforderungen Unternehmen zur Erfüllung des IT-SiG genügen müssen. In einem dynamischen Umfeld wie dem der Cybersicherheit spielen bei dieser Festlegung des State of the Art Normen und Standards eine wichtige Rolle – nicht zuletzt auch deswegen, weil Technologieanbieter und Kunden gleichermaßen für ihre Lösungen Nachhaltigkeit und Investitionsschutz anstreben.

3 Ein Katalog zur IoT-Sicherheit wurde im Juli 2016 in Zusammenarbeit mit dem japanischen Ministry of Internal Affairs and Communications und dem Ministry of Economy, Trade and Industry erarbeitet (siehe IoTAC, 2016).