Der IT-Security-Navigator

Ein Lösungsmodell praxisnaher Gesetzeskonkretisierung für KMUs im Bereich von KRITIS

Dennis-Kenji Kipker[1] · Sven Müller[2]

[1]Institut für Informations-, Gesundheits- und Medizinrecht (IGMR)
Universität Bremen
kipker@uni-bremen.de

[2]Deutsche Kommission Elektrotechnik,
Elektronik Informationstechnik (DKE) im VDE
sven.mueller@vde.com

Zusammenfassung

Die aktuellen Vorgaben zeitgemäßer IT-Sicherheit werden vorwiegend aus technischen Normen und Standards sowie aus gesetzlichen Regelungen abgeleitet, die von technischen und juristischen Experten entworfen werden und durch entsprechende Beratungsunternehmen sowie Inhouse-Consulting-Maßnahmen für das einzelne Unternehmen konkretisiert werden können. Was jedoch, wenn ein Unternehmen weder über eigenen technischen noch juristischen Sachverstand verfügt, gleichwohl aber verpflichtet ist, angemessene IT-Security umzusetzen, sei es aufgrund neuer gesetzlicher Verpflichtungen wie beispielsweise aus dem IT-Sicherheitsgesetz und der NIS-RL der EU oder aber, um mögliche Haftungsrisiken zu vermeiden, sollten kritische Systeme ausfallen und Dritte geschädigt werden? Im Regelfall sind gerade solche KMUs, die nicht unmittelbar auf fachspezifischen Sachverstand zurückgreifen können, auf sich allein gestellt, wenn es um die Realisierung der neuen Anforderungen an die IT-Sicherheit im Unternehmen geht. Abhilfe schaffen soll hier der IT-Security Navigator, der in interdisziplinärer Zusammenarbeit zwischen dem Institut für Informations-, Gesundheits- und Medizinrecht (IGMR) an der Universität Bremen und VDE/DKE in Frankfurt am Main nicht nur die für die Realisierung effektiver IT-Security relevanten Rechtsvorschriften ermittelt und in aufbereiteter Form zur Verfügung stellt, sondern die technikrelevanten Gesetze gleichsam praxisnah durch die Vorgaben der technischen Normung und Standardisierung auslegt.

1 Herausforderungen für KRITIS und Industrie 4.0

IT-Sicherheit ist mittlerweile in aller Munde, und spätestens seit den weltweiten Vorfällen um „WannaCry“ im Mai 2017, bei denen bislang unbekannte Angreifer eine Sicherheitslücke im Microsoft-Betriebssystem Windows ausnutzten, um die auf den betroffenen Computern gespeicherten Daten zu verschlüsseln und die Nutzer zur Zahlung eines

P. Schartner · N. Pohlmann (Hrsg.) · D•A•CH Security 2018 · syssec (2018) 131-141.

Lösegelds aufzufordern,[1] ist das Thema auch beim Verbraucher und damit in der breiten Öffentlichkeit angelangt. Politisch jedoch wurde die Thematik der Schaffung flächendeckender IT-Sicherheit in Deutschland bereits mit der ersten Cyber-Sicherheitsstrategie der Bundesregierung im Jahre 2011 aufgegriffen und Ende 2016 mit der Überarbeitung des Positionspapiers aktualisiert;[2] die Europäische Union definierte ihre erste Strategie für sichere IT-Systeme im Jahre 2013[3] und stellte ihre neue Strategie im Herbst 2017 vor. Auf diesen politischen Vorgaben basierend erfolgten mehrere gesetzgeberische Maßnahmen, vornehmlich die IT-Sicherheit der Kritischen Infrastrukturen betreffend: das IT-Sicherheitsgesetz (IT-SiG) aus dem Jahre 2015[4] sowie die Netz- und Informationssicherheitsrichtlinie der EU (NIS-RL) von 2016[5], die im Jahr 2017 über ein Umsetzungsgesetz Eingang in das deutsche Recht fand. Darüber hinaus befindet sich die neue EU Cybersecurity-Verordnung zur Zeit inmitten des Gesetzgebungsverfahrens, das voraussichtlich noch im Jahr 2018 abgeschlossen sein wird und erstmals den Rechtsrahmen einer EU-weiten Cyber-Sicherheitszertifizierung definiert. Längst sind nicht nur die Kritischen Infrastrukturen das Ziel von Cyberangriffen; mit der zunehmenden und allgegenwärtigen Vernetzung von informationstechnischen Systemen sind zunehmend auch digitale Dienste sowie Industrieanlagen einer erhöhten Gefährdungslage ausgesetzt. Für die digitalen Dienste, worunter Online-Marktplätze, Online-Suchmaschinen und Cloud-Computing-Dienste fallen, sieht die NIS-RL in den Artikeln 16 bis 18 deshalb eine mitgliedstaatliche Realisierung von IT-Sicherheitsvorgaben vor, die im Wesentlichen mit denjenigen für Kritische Infrastrukturen vergleichbar sind, indem auch hier technische und organisatorische Maßnahmen und Vorkehrungen (TOM bzw. TOV) zu treffen sind und eine Meldepflicht für solche Sicherheitsvorfälle besteht, die erhebliche Auswirkungen auf die Bereitstellung des digitalen Dienstes haben.[6] Enorme volkswirtschaftliche Schäden über den alleinigen, durch die EU NIS-RL unter anderem bezweckten Schutz des europäischen digitalen Binnenmarktes hinaus können jedoch ebenso aus dem Ausfall von Industrie- und Produktionsanlagen resultieren, die durch Industrie 4.0-Systeme angesteuert werden. Denn auch hier steht die Verzahnung von Technologien im Mittelpunkt, indem die Produktion mit Informations- und Kommunikationssystemen (IuK) vernetzt wird, um im Rahmen so genannter „Smart Factories“ eine effizientere sowie flexiblere und damit letztlich effizientere Steuerung von Indust-

[1] Zur Funktionsweise von „WannaCry“, den technischen Auswirkungen sowie dem aus dem Cyberangriff resultierenden Handlungsbedarf siehe unter https://community.beck.de/2017/05/19/wannacry-weltweit-groesste-cyberattacke-zeigt-handlungsbedarf-fuer-kritis-betreiber-bei-der-umsetzung.

[2] Bundesministerium des Innern, Cyber-Sicherheitsstrategie für Deutschland 2016, https://www.bmi.bund.de/ cybersicherheitsstrategie/BMI_CyberSicherheitsStrategie.pdf.

[3] European Commission, Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, JOIN(2013) 1 final, http://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf.

[4] BT-Drs. 18/4096 und BT-Drs. 18/5121.

[5] 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.

[6] Kipker, ZD-Aktuell 2016, 05261; Kipker, MMR 2017, 143 (143 f.); Kipker, MMR-Aktuell 2017, 389121.

rieanlagen zu ermöglichen. Eine erhöhte Vernetzung von Computersystemen führt letztlich jedoch ebenso zu stärkeren Abhängigkeiten der Produktions- und Logistikprozesse von funktionierenden Informations- und Kommunikationsstrukturen. Dass auch von staatlicher Seite aus nicht nur die zunehmende wirtschaftliche Relevanz von Industrie 4.0, sondern auch die damit einhergehenden technischen Risiken erkannt wurden, wird bei einem Blick unter anderem in die diesbezügliche Forschungsstrategie des Bundesministeriums für Bildung und Forschung (BMBF) für die nächsten Jahre deutlich: So stellte das BMBF fest, dass die im deutschen Mittelstand am häufigsten geäußerte Befürchtung ist, dass bei Anwendungsprozessen der Industrie 4.0 die Datensicherheit nicht gewahrt sei, dass Geschäftsgeheimnisse verloren gehen oder Unternehmensinterna gegenüber konkurrierenden Unternehmen offenbart werden könnten.[7] Um einer solchen Entwicklung vorzubeugen, fördert das Ministerium spezielle Forschungsprojekte mit dem Fokus auf der Reduzierung von IT-Sicherheitsrisiken in Umgebungen der Industrie 4.0. Darüber hinaus bildet die IT-Sicherheit für Industrie 4.0 einen Schwerpunkt im neuen IT-Sicherheitsforschungsprogramm der Bundesregierung.

2 Herausforderungen für Recht und Technik

Interdisziplinär betrachtet können die Ergebnisse einer Regelsetzung sowohl Gesetze als auch technische Vorgaben wie zum Beispiel Normen und Spezifikationen sein. Vorrangigstes Ziel einer guten Regelsetzung – sowohl im juristischen wie auch im technischen Bereich – ist stets die Verständlichkeit für den Anwender als Adressaten einer Vorschrift. Dies muss für Rechtsvorschriften insbesondere für solche Arbeitsbereiche gelten, in denen nicht nur ausgebildete Juristen mit rechtlichen Regelwerken in Berührung kommen. Hier ist die Vorgabe der Schaffung eines hohen Maßes an Anwenderverständlichkeit umso wichtiger, wenn die Rechtsvorschriften Verpflichtungen bestimmen, die bei Nichteinhaltung haftungs- und bußgeldbewehrt sein können.

2.1 Die Problematik der „unbestimmten Rechtsbegriffe“

Insbesondere für den Bereich der Cybersicherheit stellen sich die vorgenannten Probleme der Verständlichkeit und Haftungsrelevanz in einem besonderen Maße – und dies nicht erst seit dem Inkrafttreten des IT-Sicherheitsgesetzes, wo erstmals gezielt neue technische und organisatorische Anforderungen sowie Meldepflichten für die Betreiber von Kritischen Infrastrukturen bestimmt wurden.[8] Ganz im Gegenteil, die Vorschriften des IT-Sicherheitsgesetzes dürften im Vergleich mit anderen Gesetzen hinsichtlich ihrer Transparenz und Verständlichkeit deutlich besser abschneiden, da sie bereits einen gesetzgeberisch intendierten Technikbezug aufweisen. Anders sieht dies jedoch für solche Gesetze aus, die teils schon seit Jahren existieren und bei denen deshalb der Bezug zu

[7] Hierzu und zur Forschungsagenda des BMBF zu Industrie 4.0: https://www.bmbf.de/de/zukunftsprojekt-industrie-4-0-848.html.

[8] Ausführlich Hornung, NJW 2015, 3334 (3336 f.); Roos, MMR 2015, 636 (638 ff.).

IT-Sicherheit und im weitesten Sinne Datenschutz nicht explizit benannt wird, von denen als Bestandteil einer guten Corporate Governance und IT-Compliance aber allgemein anerkannt ist, dass sie auch einen eindeutigen Technikbezug aufweisen.

2.1.1 Der „Stand der Technik“ im Sinne des IT-SiG

Durch das IT-Sicherheitsgesetz wurde mit dem § 8a BSIG als wesentliche Verpflichtung für den Betreiber einer Kritischen Infrastruktur festgelegt, dass er angemessene technische und organisatorische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit der von ihm genutzten informationstechnischen Systeme zu treffen hat, um die Funktionsfähigkeit der Kritischen Infrastruktur aufrechtzuerhalten. Bei der Umsetzung dieser Anforderung soll der „Stand der Technik“ eingehalten werden. Was genau aber hierunter zu verstehen ist, wird durch das Gesetz nicht unmittelbar selbst bestimmt. In der Gesetzesbegründung heißt es dazu im Wesentlichen nur, dass der „Stand der Technik“ der Entwicklungsstand fortschrittlicher Verfahren, Einrichtungen oder Betriebsweisen ist, der die praktische Eignung einer Maßnahme zum Schutz der Funktionsfähigkeit von informationstechnischen Systemen gesichert erscheinen lässt. Zur näheren Bestimmung wird auf internationale, europäische und nationale Normen und Standards verwiesen.[9]

Bei solchen bewusst offen formulierten gesetzlichen Angaben handelt es sich um so genannte „unbestimmte Rechtsbegriffe“[10], synonym wird auch der Begriff der „Generalklausel“[11] genannt. Unbestimmte Rechtsbegriffe kommen grundsätzlich immer dann zur Anwendung, wenn es unpraktikabel scheint oder unmöglich ist, einen Lebenssachverhalt vollumfänglich durch eine gesetzliche Vorschrift zu regeln. Gerade auch, weil die Schaffung effektiver IT-Sicherheit ein enges Zusammenspiel von Recht und Technik erfordert, besteht hier in einem besonderen Maße das Bedürfnis, den unbestimmten Rechtsbegriff als Schnittstelle zwischen den verschiedenen Fachdisziplinen zu verwenden. Ein weiterer Grund für die Nutzung der unbestimmten Rechtsbegriffe liegt in der damit verbundenen Technikoffenheit und der hieraus folgenden Anpassungsfähigkeit des Rechts an die zukünftige und nicht selten rasche Entwicklung im Bereich der Informationssysteme. Denn im Zweifelsfall lässt sich das allgemeine Verständnis einer Rechtsvorschrift flexibler und schneller anpassen als die Schaffung eines neuen Gesetzes möglich ist, sollten sich die technologischen Rahmenbedingungen wieder einmal geändert haben.

Obgleich der „Stand der Technik“ der am meisten verwandte unbestimmte Rechtsbegriff ist, kann er dennoch nicht allein und losgelöst betrachtet werden, will man seine inhaltliche Aussage bestimmen. Das Handbuch der Rechtsförmlichkeit des BMJV stellt im Zusammenhang mit dem Stand der Technik auf zwei weitere Generalklauseln ab:

---

[9] BT-Drs. 18/4096, S. 26.

[10] Vgl. Michaelis, DuD 2016, 458 (458).

[11] So Bundesministerium der Justiz und für Verbraucherschutz (BMJV), Handbuch der Rechtsförmlichkeit, Rn. 252 ff.

auf die „allgemein anerkannten Regeln der Technik“ sowie auf den „Stand von Wissenschaft und Technik“. Erstere werden für Fälle mit vergleichsweise geringem Gefährdungspotenzial oder für Fälle verwendet, die auf Grund gesicherter Erfahrungen technisch beherrschbar sind. Demgemäß sind allgemein anerkannte Regeln der Technik schriftlich fixierte oder mündlich überlieferte technische Festlegungen für Verfahren, Einrichtungen und Betriebsweisen, die nach herrschender Auffassung der beteiligten Kreise (Fachleute, Anwender, Verbraucher und öffentliche Hand) geeignet sind, das gesetzlich vorgegebene Ziel zu erreichen und die sich in der Praxis allgemein bewährt haben oder deren Bewährung nach herrschender Auffassung in überschaubarer Zeit bevorsteht.[12] Der „Stand von Wissenschaft und Technik“ beschreibt demgegenüber das höchste Anforderungsniveau und wird deshalb in Fällen mit einem sehr hohen Gefährdungspotenzial verwendet. Stand von Wissenschaft und Technik ist der Entwicklungsstand fortschrittlichster Verfahren, Einrichtungen und Betriebsweisen, die nach Auffassung führender Fachleute aus Wissenschaft und Technik auf der Grundlage neuester wissenschaftlich vertretbarer Erkenntnisse im Hinblick auf das gesetzlich vorgesehene Ziel für erforderlich gehalten werden und das Erreichen des Ziels gesichert erscheinen lassen.[13] Gemessen an den „allgemein anerkannten Regeln der Technik“ sowie am „Stand von Wissenschaft und Technik“ stellt der „Stand der Technik“ folglich das Mittelmaß dar: Hierbei handelt es sich im Hinblick auf die IT-Sicherheit um solche Vorkehrungen, die zwar noch nicht unbedingt bei jedem Fachmann oder Anwender angelangt sein müssen, aber zugleich auch nicht so neu sind, dass sie die Grenze des wissenschaftlich bzw. technisch Realisierbaren bedeuten.

Diese sprachliche Definition der technisch umzusetzenden Anforderungen dürfte dem Juristen im Regelfall ausreichen – für den mit der Realisierung der IT-Sicherheit beauftragten Techniker stellt sie jedoch bestenfalls einen groben und damit unzureichenden Anhaltspunkt für seine Arbeit dar. Zwar werden auch Auslegungshilfen für den Stand der Technik entwickelt: So hat beispielsweise speziell für die Vorgaben des IT-Sicherheitsgesetzes der Bundesverband IT-Sicherheit e.V. (TeleTrusT) eine vornehmlich technische Handreichung zur Konkretisierung des Standes der Technik entwickelt, die 2018 umfassend überarbeitet wurde.[14] Generell lässt sich feststellen, dass zumindest für die Betreiber von Kritischen Infrastrukturen der „Stand der Technik“ durch ein Information Security Management System (ISMS) nach ISO/IEC 27001 bzw. gemäß BSI-Grundschutz ausgefüllt werden kann, indem laufend neue Bedrohungslagen erfasst sowie aktuelle und wirksame Gegenmaßnahmen implementiert werden. Schlüsselbegriffe

[12] Bundesministerium der Justiz und für Verbraucherschutz (BMJV), Handbuch der Rechtsförmlichkeit, Rn. 255. Siehe auch BVerfG, Beschl. v. 08.08.1978, Az. 2 BvL 8/77 (Kalkar I).

[13] Bundesministerium der Justiz und für Verbraucherschutz (BMJV), Handbuch der Rechtsförmlichkeit, Rn. 257. Siehe auch BVerfG, Beschl. v. 08.08.1978, Az. 2 BvL 8/77 (Kalkar I).

[14] TeleTrusT e.V., Handreichung zum „Stand der Technik“ im Sinne des IT-Sicherheitsgesetzes ITSiG https:// www. teletrust. de/ fileadmin/ docs/ fachgruppen/ ag-stand-der-technik/TeleTrusT-Handreichung_Stand_ der_ Technik_-_Ausgabe_2018.pdf.

in diesem Zusammenhang sind das „Business Continuity Management“ (BCM) und der „Plan-Do-Check-Act“-Zyklus (PDCA).[15]

Obwohl die Verwendung von unbestimmten Rechtsbegriffen unter rechtsstaatlichen Gesichtspunkten grundsätzlich zulässig und sogar erwünscht ist, kann sie in der Anwendungspraxis zu erheblichen Schwierigkeiten und damit zu Rechtsunsicherheit führen. Nicht nur, dass unbestimmte Rechtsbegriffe auch gesetzliche Pflichten regeln können, die bei Verstoß zu einem Schadensersatzanspruch führen oder bußgeldbewehrt sind – wie zum Beispiel im Falle der durch das BSIG nach § 8a zu treffenden technischen und organisatorischen Vorkehrungen. Auch die zur Konkretisierung erforderliche – und damit zur Verwendung der entsprechenden Gesetze zwingend notwendige – Auslegung der unbestimmten Rechtsbegriffe kann vor allem unter zwei Gesichtspunkten Probleme bereiten: Erstens dann, wenn durch sie auf Sachverhalte Bezug genommen wird, die deutlich außerhalb des Rechts als wissenschaftlicher Disziplin liegen. Zweitens in dem Falle, wenn die Konkretisierung der unbestimmten Rechtsbegriffe nicht oder noch nicht in abschließender Weise erfolgt ist. Das ist primär bei neu geschaffenen Gesetzen der Fall, die sich vorwiegend auch im IT-Recht finden. Hier existiert für nicht wenige der gesetzlich festgeschriebenen unbestimmten Rechtsbegriffe keinerlei Handreichung oder ein Organisationsmodell, um die abstrakten Vorschriften praxisgerecht aufbereitet zu konkretisieren. Vielmehr werden die Rechtsbegriffe oftmals für den Einzelfall durch Behörden und insbesondere durch die Rechtsprechung der Gerichte ausgefüllt, was eine gewisse Zeit in Anspruch nimmt. Dies hat zur Folge, dass selbst wenn ein technischer Anwender sämtliche für ihn einschlägigen Vorschriften zur Umsetzung der IT-Sicherheit kennt, er dennoch vor dem Problem steht, diese gesetzeskonform umzusetzen – und dies auch in denjenigen Fällen, in denen noch keine Konkretisierung von staatlicher oder privater Seite aus stattgefunden hat.

2.1.2 Auslegungsoffene unbestimmte Rechtsbegriffe

Noch weitergehende Probleme stellen sich für den nicht-versierten Rechtsanwender für den Fall der unbestimmten Rechtsbegriffe ohne einen eindeutigen Bezug zu IT-Sicherheit – bei denen jedoch im Wege der Auslegung gemeinhin vertreten wird, dass sie letztlich auch dem Bereich der Cybersecurity zuzuordnen sind. Als allgemeingültigstes Beispiel einer solchen Vorschrift können die §§ 91 Abs. 2, 93 Abs. 1 AktG herangezogen werden. Davon ausgehend hat der Vorstand geeignete Maßnahmen zu treffen, damit „den Fortbestand der Gesellschaft gefährdende Entwicklungen“ frühzeitig erkannt werden. Daneben haben die Vorstandsmitglieder bei ihrer Geschäftsführung „die Sorgfalt eines ordentlichen und gewissenhaften Geschäftsleiters“ anzuwenden. Bei diesen beiden interpretationsbedürftigen Formulierungen ergibt sich der Bezug zur IT-Security nicht einmal aus dem Gesetzeswortlaut. Anerkannt ist dennoch, dass unter die

[15] Darüber hinaus ist es bei der Umsetzung eines ISMS möglich, die verschiedenen IT- und Organisationsprozesse innerhalb eines Reifegradmodells abzubilden. Ausgehend von „SPICE“ kann bei einem Zielreifegrad von mindestens 3 („Gesteuert“) angenommen werden, dass eine entsprechende Prozesskontrolle implementiert wurde, die zur Einhaltung des Standes der Technik notwendig ist. Siehe Kipker/Pfeil, DuD 2016, 810 (814).

vorgenannten Beobachtungs- und Sorgfaltspflichten des Gesellschaftsrechts auch Maßnahmen der IT-Sicherheit zu fassen sind.[16] Dies gilt aber nicht nur für große, am Kapitalmarkt beteiligte Aktiengesellschaften, sondern auch für die zahllosen kleinen und mittelständischen Unternehmen (KMU), die in der Rechtsform der GmbH agieren. Hier ist allgemeine Auffassung, dass die Geschäftsführer der Sache nach die gleichen Sorgfaltspflichten wie der Vorstand einer Aktiengesellschaft treffen. Dies lässt sich aus § 43 Abs. 1 GmbHG ableiten – auch hier ergibt sich der Bezug zur IT-Sicherheit aber nicht aus der Vorschrift selbst und ist für den Rechtslaien deshalb auch nicht ohne weiteres erkennbar.[17] Über diese beiden gesellschaftsrechtlichen Beispiele hinaus existiert eine unübersichtliche Vielzahl weiterer Gesetze aus allen möglichen Arbeitsbereichen im Europa-, Bundes- und Landesrecht wie auch in untergesetzlichen Rechtsvorschriften, die zum Teil weitere zwingende IT-Compliance-Vorgaben enthalten, ohne dass dies explizit im Gesetz festgeschrieben wird.

2.2 Domänenübergreifende Normung in der IT-Sicherheit

Im Bereich der Cybersicherheit steht jedoch nicht nur die Rechtsetzung vor neuen Herausforderungen, sondern ebenso die technische Normung. Hier gilt es zum einen nicht nur, abstrakt Technik und Technologien zu betrachten, sondern auch zugehörige Prozesse und den Faktor Mensch. Hinzu kommt, dass die meisten technischen Regeln eine sehr domänenspezifische Sichtweise wiedergeben, die der zunehmenden Vernetzung und Digitalisierung nicht gerecht wird. Als Beispiel seien hier die beiden Bereiche Informationssicherheit und Funktionale Sicherheit genannt. Als Informationssicherheit bezeichnet man Eigenschaften von informationsverarbeitenden und -lagernden (technischen oder nicht-technischen) Systemen, welche die Schutzziele Vertraulichkeit, Verfügbarkeit und Integrität sicherstellen. Sie dient dem Schutz vor Gefahren bzw. Bedrohungen, der Vermeidung von wirtschaftlichen Schäden und der Minimierung von Risiken. Funktionale Sicherheit bezeichnet den Teil der (physischen) Sicherheit eines Systems, der von der korrekten Funktion des sicherheitsbezogenen Systems und anderer risikomindernder Maßnahmen abhängt. Am Beispiel der Automatisierungstechnik lässt sich aufzeigen, dass sich insbesondere vor dem Hintergrund zunehmender Vernetzung die Informationssicherheit wie auch die funktionale Sicherheit gegenseitig beeinflussen. Beide Themenbereiche wurden bisher getrennt bearbeitet und in unterschiedlichen Normungsgremien behandelt: So fordert die IEC 61508[18] „Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme“ die Berücksichtigung boshafter und nicht autorisierter Handlungen während der Gefährdungs- und Risikoanalyse und verweist dabei hauptsächlich auf die IEC 62443 „IT-

[16] Vgl. Conrad, in: Auer-Reinsdorff, Handbuch IT- und Datenschutzrecht, § 33, Rn. 36.

[17] Vgl. Grützner/Jakob, Compliance von A-Z, Schlagwort „IT-Sicherheit“.

[18] IEC 61508, Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme, Deutsche Fassung EN 61508 (VDE 0803)

Sicherheit für industrielle Automatisierungssysteme“, während die IEC 62443[19] die funktionale Sicherheit nicht ausreichend fokussiert.

Aufgrund der umfangreichen Verzahnung von technischen Normen und Regeln auf Basis der DIN EN ISO/IEC 27002[20]-Norm mit Verknüpfung zur ISO/IEC TR 27019[21] ist eine Realisierung effektiver IT-Sicherheit für KMUs im Ergebnis mit erheblichen Schwierigkeiten verbunden. Da nicht nur die Management-Prozesse bei einer Zertifizierung überprüft werden, sondern auch die sicherheitstechnischen Anforderungen der IEC/ISO TR 27019, wodurch wiederum ein Verweis auf die technische Normung gegeben ist, wird die ISMS-Zertifizierung zunehmend komplex und damit eine Herausforderung für ein KMU. Zur Hilfestellung hat der VdS die Richtlinie für Informationssicherheit (VdS 3473[22], „Informationssicherheit in kleinen und mittelständischen Unternehmen (KMU), Anforderungen“) herausgegeben. Diese ermöglicht KMUs einen Quick-Audit für Cyber-Security.

Zusätzlich kann sich ein KRITIS-Betreiber nach dem branchenspezifischen Sicherheitsstandard (B3S) überprüfen lassen. Dies ist eine erweiterte Prüfgrundlage auf Basis der DIN EN ISO/IEC 27001. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) möchte damit eine kostspielige Komplettzertifizierung auf Basis der ISO/IEC 27001 vermeiden und nur den branchenspezifischen Teil der Managementprozesse überprüfen lassen.

3 Der IT-Security Navigator als Lösungsmodell

Bei einer Gesamtbetrachtung der Regelsetzung im Bereich der IT-Sicherheit – dies sowohl auf rechtlicher wie auch auf technischer Ebene – wird deutlich, dass eine Diskrepanz zwischen den abstrakten Anforderungen und deren praktischer Umsetzung besteht. Dieses Defizit ist im Wesentlichen nicht auf Unzulänglichkeiten innerhalb des Prozesses der Regelsetzung selbst, sondern vielmehr auf die Interdisziplinarität der Materie und den damit zwangsläufig verbundenen Wissensdefiziten des mit der Umsetzung von IT-Sicherheit befassten Personals zurückzuführen. Besondere Herausforderungen bestehen dabei vor allem im Bereich der kleinen und mittelständischen Unternehmen (KMU), die zumeist weder über eine eigene Rechts- noch über eine technische Fachabteilung verfügen, sondern damit verbundene Dienste und Aufgaben für den Regelfall an externe Leistungserbringer ausgelagert haben. Nicht selten hat dies in der Praxis zur Folge, dass Personengruppen, die sich beruflich bisher gar nicht oder nur am Rande mit Fragen von

[19] IEC 62443, IT-Sicherheit für industrielle Automatisierungssysteme, Deutsche Fassung DIN IEC 62443 (VDE 0802)

[20] DIN EN ISO/IEC 27002:2017-06, Informationstechnik – Sicherheitsverfahren – Leitfaden für Informationsmaßnahmen

[21] DIN ISO/IEC TR 27019 DIN SPEC 27019:2015-03, Informationstechnik - Sicherheitsverfahren - Leitfaden für das Informationssicherheitsmanagement von Steuerungssystemen der Energieversorgung auf Grundlage der ISO/IEC 27002

[22] VdS 3473: 2015-07, Cyber-Security für kleine und mittlere Unternehmen (KMU) - Anforderungen, VdS Schadenverhütung GmbH

Corporate Governance, Compliance und unternehmerischer Cybersicherheit auseinandergesetzt haben, sich in Umsetzung der gesetzlichen Anforderungen in ein neues Berufsbild wie zum Beispiel dasjenige des IT-Sicherheitsbeauftragten von Grund auf neu einarbeiten müssen. Um unter anderem diese Einarbeitung zu erleichtern, aber auch, um die Schaffung flächendeckender IT-Sicherheit in Deutschland zu unterstützen und zu fördern, wird das wissenschaftliche Konzept des IT-Security Navigators als Lösungsmodell für eine praxisnahe Gesetzeskonkretisierung für KMUs in den Bereichen von KRITIS sowie Industrie 4.0 vom Institut für Informations-, Gesundheits- und Medizinrecht (IGMR) und von der Deutschen Kommission Elektrotechnik Elektronik Informationstechnik (DKE) im VDE erarbeitet.

Die beiden Forschungspartner verfolgen dabei vornehmlich eine Arbeitsmethode, welche sich eine möglichst genaue Konkretisierung der in den IT-sicherheitsrelevanten Rechtsvorschriften enthaltenen unbestimmten Rechtsbegriffe zum Ziel gesetzt hat. In interdisziplinärer Zusammenarbeit sind hierzu zunächst sämtliche Rechtsvorschriften sowohl im Europa-, Bundes- und Landesrecht, die für die IT-Sicherheit als auch für den (technischen) Datenschutz eine Relevanz besitzen, für alle Sektoren Kritischer Infrastrukturen wie auch für den Bereich der Industrie 4.0 ermittelt worden. Zur Verbesserung der Anwenderfreundlichkeit hat eine geeignete Aufbereitung der Vorschriften sortiert nach Kategorien und Rechtsetzungsinstanz, daneben aber auch nach Anwenderrelevanz, stattgefunden. Für jede Kategorie von Rechtsvorschriften wurden darüber hinaus einschlägige Publikationen und die Rechtsprechung erfasst. Zur leichteren Anwendbarkeit sind sämtliche Gesetze online verlinkt worden, und relevante Einzelparagraphen werden separat nach Relevanz sortiert aufgeführt, sodass ein schneller und gezielter Abruf möglich ist. Diese so geschaffene, mehrere Hundert Gesetze umfassende Sammlung von Rechtsvorschriften erfährt eine laufende Aktualisierung und ist online frei und kostenlos zur Nutzung verfügbar. Die Online-Maske enthält zudem verschiedene Filter, sodass ein einfacher wie intuitiver Gebrauch möglich ist.

Um den für die Realisierung effektiver IT-Sicherheit verantwortlichen Personengruppen nicht nur einen schnellen und einfachen Überblick über die für sie relevanten Gesetze verschaffen zu können, sondern die Rechtsvorschriften und die in vielen von ihnen enthaltenen unbestimmten Rechtsbegriffe zu konkretisieren, werden in einem zweiten Schritt der wissenschaftlichen Forschung gezielt sämtliche in den Gesetzen mit IT-Bezug enthaltenen unbestimmten Rechtsbegriffe ermittelt und katalogisiert. Darauf basierend erfolgt im Anschluss die Konkretisierung der unbestimmten Rechtsbegriffe mit Technikbezug für sämtliche Sektoren Kritischer Infrastrukturen und für den Bereich Industrie 4.0 in Zusammenarbeit mit verschiedenen Normungsgremien von VDE/DKE.

Parallel zur Sammlung und Aufbereitung rechtlicher Vorgaben wurde von VDE/DKE eine korrespondierende, umfassende Übersicht sämtlicher relevanter technischer Normen und Spezifikationen mit IT-Sicherheits- und Datenschutzbezug erstellt. In einer Symbiose aus Recht und Technik werden im nächsten Projektschritt in enger Zusammenarbeit mit den Normungsgremien die Schnittstellen zwischen den Normen und Spezifikationen und den entsprechenden unbestimmten Rechtsbegriffen ermittelt, das heißt es wird für jede Generalklausel in jeder relevanten Rechtsvorschrift geprüft, welche

technischen Normen und Spezifikationen zur Ausfüllung bzw. zur praxisgerechten Auslegung herangezogen werden können. Nach Abschluss dieses Abgleichs werden nahezu sämtliche IT-sicherheitsrelevanten Rechtsvorschriften und technischen Normen bzw. Spezifikationen im Rahmen des IT-Security Navigators zusammengeführt und dem Anwender öffentlich zugänglich gemacht.

Durch die damit geleistete Forschungsarbeit ist es möglich, nicht nur eine Vielzahl rechtlicher Vorgaben zur IT-Sicherheit vollumfassend und einfach systematisiert darzustellen, sondern mit Hilfe der unmittelbar stattfindenden Konkretisierung durch einschlägige technische Normen und Spezifikationen dem Anwender eine sofortige und zuverlässige Erst-Entscheidungshilfe zur Verfügung zu stellen, um für ihn möglicherweise verpflichtende IT-Security-Maßnahmen auf angemessene Weise zu implementieren. Das neu geschaffene Werkzeug steht im Internet jedem kostenfrei zur Verfügung. Zudem wird es laufend mit neuen Features ausgestattet, wie beispielsweise zusätzlichen Such- und Filteroptionen, der Anzeige weiterer Informationen zu den Normen und Spezifikationen auf Anforderung des Nutzers und einer grafischen Darstellung der Ergebnisse (z. B. zur Aktivität in den Normungsgremien/Domänen als Tortendiagramm und als Heat Map; daneben Statistiken zur Zahl der Referenzierungen in Gesetzen und Standards). Da die Praxistauglichkeit der Plattform im Vordergrund steht, erhält auch der Anwender die Möglichkeit zur Mitwirkung, indem er selbst neue Gesetze sowie Normen und Spezifikationen vorschlagen kann, die nach einer Prüfung in die Datenbank implementiert und dort miteinander vernetzt werden. In Zukunft wird der IT-Security Navigator um die mobile App „Wizard“ ergänzt werden, die zusätzlich zur Suche nach Rechtsvorschriften oder Normen und Standards einen komplett strukturierten Entscheidungsbaum beinhaltet, der dem Anwender konkrete Vorschläge macht, welchen IT-Compliance-Vorgaben er genügen sollte und wie diese für ihn zu realisieren sind.

4 Fazit und Ausblick

Der Mensch steht an der Schnittstelle zur Technik, indem er unmittelbar mit der Umsetzung zeitgemäßer IT-Sicherheits- und auch Datenschutzvorgaben betraut ist. Hierfür ist ein interdisziplinäres Wissen erforderlich, das sowohl die rechtliche wie auch die technische Betrachtung des Schutzes im digitalen Arbeitsraum rund um KRITIS wie auch Industrie 4.0 einbezieht. In der Praxis aber fehlt ein solches Schnittstellenwissen oftmals; insbesondere KMU sind mit der Realisierung effektiver Cybersicherheit deshalb häufig überfordert. Mit der Forschung zum IT-Security Navigator wird aus diesem Grunde das Ziel verfolgt, vor allem das in kleinen wie mittelständischen Unternehmen tätige IT-Personal in seiner täglichen Arbeitspraxis zu entlasten, indem ihm einerseits ein effektives und gleichermaßen effizientes Werkzeug zur Bestimmung möglicher rechtlicher Pflichten im Bereich IT-Sicherheit, andererseits zur Konkretisierung der damit verbundenen technischen Vorgaben, zur Seite gestellt wird. Gerade für den mit der Umsetzung gesetzlicher Bestimmungen konfrontierten Endadressaten, der möglicherweise nicht immer über den unmittelbaren Zugriff auf juristische Ressourcen sowie auf Normen und Spezifikationen verfügt, ist eine solche einfache, schnelle wie auch verlässliche Erstorientierung wichtig, um die rechtlichen und technischen Maßstäbe seiner

Arbeit zeitsparend und kostengünstig definieren zu können. Verschiedene Rückmeldungen aus den entsprechenden Fachkreisen bestätigen dies. Der IT-Security Navigator leistet damit einen bedeutsamen Beitrag zur Verbesserung der flächendeckenden IT-Sicherheit in Deutschland.

Literatur

[1] T. Grützner, A. Jakob: Compliance von A-Z, München 2015.

[2] G.Hornung: Neue Pflichten für Betreiber kritischer Infrastrukturen, NJW 2015, 3334-3340.

[3] P. Roos: Das IT-Sicherheitsgesetz: Wegbereiter oder Tropfen auf den heißen Stein?, MMR 2015, 636-645.

[4] I. Conrad: Compliance, IT-Sicherheit, Ordnungsmäßigkeit der Datenverarbeitung, in: Astrid Auer-Reinsdorff/Isabell Conrad (Hrsg.), Handbuch IT- und Datenschutzrecht, München 2016, § 33.

[5] D.-K. Kipker: Die NIS-RL der EU im Vergleich zum deutschen IT-Sicherheitsgesetz, ZD-Aktuell 2016, 05261.

[6] D.-K. Kipker, D. Pfeil: IT-Sicherheitsgesetz in Theorie und Praxis: Was Betreiber (wirklich) beachten müssen – Eine interdisziplinäre Fallstudie, DuD 2016, 810-814.

[7] P. Michaelis: Der „Stand der Technik“ im Kontext regulatorischer Anforderungen, DuD 2016, 458-462.

[8] D.-K. Kipker: Der BMI-Referentenentwurf zur Umsetzung der NIS-RL: Was dürfen Betreiber von Kritischen Infrastrukturen und Anbieter von digitalen Diensten erwarten?, MMR 2017, 143-147.

[9] D.-K. Kipker: Umsetzungsgesetz zur NIS-RL mit nur geringen Anpassungen gegenüber der bisherigen Rechtslage beschlossen, MMR-Aktuell 2017, 389121.

[10] IEC 61508, Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme, Deutsche Fassung EN 61508 (VDE 0803).

[11] IEC 62443, IT-Sicherheit für industrielle Automatisierungssysteme, Deutsche Fassung DIN IEC 62443 (VDE 0802).

[12] DIN EN ISO/IEC 27002:2017-06, Informationstechnik – Sicherheitsverfahren – Leitfaden für Informationsmaßnahmen.

[13] DIN ISO/IEC TR 27019 DIN SPEC 27019:2015-03, Informationstechnik - Sicherheitsverfahren – Leitfaden für das Informationssicherheitsmanagement von Steuerungssystemen der Energieversorgung auf Grundlage der ISO/IEC 27002.

[14] VdS 3473: 2015-07, Cyber-Security für kleine und mittlere Unternehmen (KMU) – Anforderungen, VdS Schadenverhütung GmbH.