Dennis-Kenji Kipker

Die NIS-RL der EU im Vergleich zum deutschen IT-Sicherheitsgesetz

ZD-Aktuell 2016, 05261

Nachdem nun doch einige Jahre seit dem Vorschlag der *Kommission* zur Schaffung einer „Richtlinie über Maßnahmen zur Gewährleistung einer hohen gemeinsamen Netz- und Informationssicherheit in der Union" (NIS-RL) als zentraler Bestandteil der Cyber-Sicherheitsstrategie der EU im Februar 2013 vergangen sind, wurde das europäische Gesetzgebungsverfahren jüngst mit der Annahme des Rechtsetzungsakts durch das *EU-Parlament* am 6.7.2016 abgeschlossen. Deutschland ist dabei für den neuen europäischen Cybersecurity-Raum mit dem IT-Sicherheitsgesetz gut gerüstet.

1. Meilensteine, Vorgeschichte und zentrale Eckpunkte

Das Gesetzgebungsverfahren war von verschiedenen Schwierigkeiten inhaltlicher wie prozeduraler Art geprägt, sodass es nunmehr zu begrüßen ist, dass die RL, wie jüngst angestrebt, zum 8.8.2016 in Kraft treten konnte, nachdem die Veröffentlichung im Amtsblatt der EU am 19.7.2016 stattfand. Im Laufe des Gesetzgebungsverfahrens hat sich auch der Name des Unionsrechtsakts geändert, so lautet die aktuelle Fassung nunmehr „Richtlinie über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der EU" – an der Abkürzung ändert sich dadurch freilich nichts. Die NIS-RL sieht inhaltlich verschiedene Umsetzungsfristen, sog. Meilensteine, vor, von denen an dieser Stelle kurz die wichtigsten genannt werden sollen:

- 9.2.2017: Ablauf der Frist für die Vertretung in der Kooperationsgruppe und im CSIRTs (Computer Security Incident Response Teams)-Netzwerk,
- 9.5.2018: Ablauf der Umsetzungsfrist zur Schaffung der neuen, durch die RL geforderten Rechts- und Verwaltungsvorschriften für die EU-Mitgliedstaaten,
- 10.5.2018: Anwendung der neuen mitgliedstaatlichen Regelungen zur NIS,
- 9.11.2018: Ablauf der Ermittlungsfrist für die Betreiber sog. „wesentlicher Dienste",
- 9.5.2019: Erstellungsfrist für den Kohärenzbericht zur Ermittlung der Betreiber wesentlicher Dienste,
- 9.5.2021: Erster Erfahrungsbericht der *EU-Kommission* zur RL-Umsetzung.

Bei allen durch die RL adressierten Verpflichtungen ist ihre Rechtsnatur zu beachten: Gem. Art. 288 AEUV ist sie hinsichtlich des zu erreichenden Ziels für jeden Mitgliedstaat verbindlich, überlässt den innerstaatlichen Stellen jedoch die Wahl der Form und der Mittel. Dies bedeutet, dass sich die NIS-RL inhaltlich primär zunächst einmal an die staatlichen Organe der EU-Mitgliedstaaten richtet, die ein nationales Gesetz zur Umsetzung der NIS-RL schaffen müssen. In Deutschland werden deshalb vermutlich einige der bisher durch das IT-Sicherheitsgesetz als Artikelgesetz im Einzelnen novellierten Gesetze erneut überarbeitet werden müssen. Bei der Umsetzung der mitgliedstaatlichen Verpflichtungen zur NIS-RL ist der Grundsatz der Mindestharmonisierung zu beachten: Hieraus folgt, dass Deutschland gesetzlich auch ein höheres IT-Sicherheitsniveau schaffen kann, als durch die NIS-RL vorgegeben wird.

Hinter der NIS-RL stehen verschiedene aktuelle rechtspolitische Erwägungen: So wird die zunehmende Bedeutung der Netz- und Informationssicherheit als zentraler Faktor für ein funktionierendes Gemeinwesen und die europäische Wirtschaft betont, zugleich aber auch eingeräumt, dass Tragweite, Häufigkeit und Auswirkungen von Sicherheitsvorfällen zunehmen. Zudem setzt eine EU-weit koordinierte Cyber-Sicherheitsstrategie hinsichtlich aller Mitgliedstaaten ein Mindestniveau an IT-Sicherheit voraus. Argumentiert wird, dass die bestehenden mitgliedstaatlichen Fähigkeiten in ihrer Gesamtheit nicht ausreichend sind, um ein hohes Niveau von NIS in der EU zu gewährleisten. Deshalb wurde die NIS-RL als umfassender Ansatz konzipiert, um „gemeinsame Mindestanforderungen für Kapazitätsaufbau und -planung, Informationsaustausch, Zusammenarbeit sowie gemeinsame Sicherheitsanforderungen für Betreiber wesentlicher Dienste und Anbieter digitaler Dienste" zu bestimmen, wie es in den Erwägungsgründen lautet.

2. Gegenstand und Anwendungsbereich, Art. 1, 2 und 3

Die NIS-RL richtet sich wie bereits festgestellt nicht unmittelbar an private Stellen bzw. an Betreiber, sondern an die EU-Mitgliedstaaten, die daraus resultierend verschiedene gesetzliche Umsetzungspflichten zur Erhöhung der nationalen IT-Sicherheit treffen. Dies sind im Überblick:

- Festlegung einer nationalen Strategie für NIS,
- Einrichtung einer Kooperationsgruppe zur strategischen Zusammenarbeit und für den interstaatlichen Informationsaustausch zur IT-Sicherheit,
- Einrichtung eines CSIRTs-Netzwerks (Computer Security Incident Response Teams Network) zur Förderung der operativen interstaatlichen Zusammenarbeit im Bereich der IT-Security,
- Festlegung von Sicherheitsanforderungen und Meldepflichten für die Betreiber wesentlicher Dienste und für Anbieter digitaler Dienste,
- Benennung von nationalen IT-Sicherheitsbehörden, zentralen Anlaufstellen sowie von CSIRTs.

Vom Anwendungsbereich der RL werden verschiedene Ausnahmen getroffen für:

- Betreiber öffentlicher Kommunikationsnetze (RL 2002/21/EG),
- Betreiber öffentlich zugänglicher elektronischer Kommunikationsdienste (RL 2002/21/EG),
- Vertrauensdiensteanbieter (VO Nr. 910/2014),
- Verarbeitung personenbezogener Daten gemäß EU-Datenschutzrecht.

Daneben wird als lex specialis-Regel die allgemeine Festlegung getroffen, dass sektorspezifische Anforderungen des EU-Rechts vorrangig sind. Der Anwendungsbereich in Bezug auf Kleinstunternehmen wird hingegen nicht inhaltlich durch die RL selbst, sondern durch die Schwellenwerte zur Ermittlung der Betreiber wesentlicher Dienste beschränkt (Art. 5 Abs. 2, Art. 6).

3. Begriffsbestimmungen, Art. 4

Die NIS-RL enthält ein umfangreiches Verzeichnis zur Definition der verwendeten Begriffe. Hiernach fallen unter „Netz- und Informationssysteme" elektronische Kommunikationsnetze (Kabel; Funk; optische, elektromagnetische Einrichtungen; Satellitennetze; Internet; Stromleitungen, soweit sie zur Signalübertragung genutzt werden; Hörfunk; Fernsehen), Vorrichtungen, die programmgesteuert und automatisiert Daten verarbeiten, sowie digitale Daten, die in den vorgenannten Einrichtungen verarbeitet werden. Die „Betreiber wesentlicher Dienste" umfassen begrifflich sowohl öffentliche wie auch private Einrichtungen. Unter diesem Gesichtspunkt scheint der Anwendungsbereich der NIS-RL gegenüber dem IT-Sicherheitsgesetz zunächst deutlich erweitert zu sein, jedoch wird im Anhang II der RL, auf den ebenfalls verwiesen wird, die Kategorie „Staat und Verwaltung" nicht benannt. Ein „Digitaler Dienst" ist jede in der Regel gegen Entgelt elektronisch im Fernabsatz und auf individuellen Abruf eines Empfängers erbrachte Dienstleistung. Unter einem „Sicherheitsvorfall" sind alle Ereignisse zu verstehen, die tatsächlich nachteilige Auswirkungen auf die Sicherheit von Netz- und Informationssystemen haben. In Art. 4 der NIS-RL finden sich zudem weitere technische Definitionen für IXP, DNS, TLD, Online-Marktplatz und -Suchmaschine sowie für Cloud Computing-Dienste. Die Begriffsbestimmungen erfahren weitere Konkretisierungen durch die Anhänge I bis III der NIS-RL.

4. Schutz wesentlicher Dienste, Art. 5, 6, 14, 15

Eine der zentralen Zielsetzungen der NIS-RL liegt im Schutz von Betreibern sog. „wesentlicher Dienste". Obwohl hier ein anderer Begriff verwendet wird, entsprechen diese Dienste in ihrem Sinn den Kritischen Infrastrukturen des IT-Sicherheitsgesetzes. Bis zum 9.11.2018 trifft die Mitgliedstaaten die Pflicht, die Betreiber solcher wesentlicher Dienste mit einer Niederlassung in ihrem Hoheitsgebiet zu ermitteln. Die einschlägigen Sektoren und Teilsektoren der wesentlichen Dienste werden im Anhang II bezeichnet – verglichen mit dem IT-Sicherheitsgesetz sozusagen als „Qualitätskriterium" einer bestimmten Branche. Die Unterschiede zum IT-Sicherheitsgesetz sind hier augenfällig eher gering und werden sich vermutlich in der Feinabstimmung im Laufe der Umsetzungsphase in nationales Recht weiter konkretisieren. Wesentliche Dienste i.S.d. NIS-RL sind in den folgenden Bereichen zu verorten:

- Energie (Elektrizität, Erdöl, Erdgas),
- Verkehr (Luftverkehr, Schienenverkehr, Schifffahrt, Straßenverkehr),
- Bankwesen (Kreditinstitute),
- Finanzmarktinfrastrukturen (Börsen),
- Gesundheitswesen (medizinische Versorgungseinrichtungen, Krankenhäuser, Privatkliniken),
- Trinkwasserlieferung und -versorgung,
- digitale Infrastruktur (IXPs, DNS-Diensteanbieter, TLS-Name Registries).

Im IT-Sicherheitsgesetz bzw. in § 2 Abs. 10 BSIG werden die Kritischen Infrastrukturen über die NIS-RL hinaus noch um die Bereiche Ernährung und Versicherungswesen ergänzt.

Indem die Festlegung der Sektoren wesentlicher Dienste im Sinne des Qualitätskriteriums zunächst die generelle Kritikalität einer bestimmten Branche bestimmt, erfolgt die weitergehende Zuordnung eines so ermittelten Dienstes als „wesentlich" durch drei Kriterien, welche, verglichen mit dem IT-Sicherheitsgesetz, die Quantität der Leistung widerspiegeln:

- Der Dienst ist unerlässlich zur Aufrechterhaltung kritischer gesellschaftlicher/wirtschaftlicher Tätigkeiten.
- Die Bereitstellung des Dienstes ist abhängig von Netz- und Informationssystemen.
- Ein möglicher Sicherheitsvorfall bewirkt eine erhebliche Störung, u.a. gemessen an der Nutzerzahl, „Dominoeffekten", dem Marktanteil des Dienstes und alternativen Ausweichlösungen.

Ausgehend von den vorgenannten Kriterien erstellen die Mitgliedstaaten eine Liste wesentlicher Dienste; in Deutschland kommt diese Konkretisierungsaufgabe der Kritis-Verordnung des BSI (BSI-KritisV) zu. Die so ermittelte Liste von Betreibern ist mind. alle zwei Jahre zu überprüfen, um einen EU-weit vereinheitlichten Bewertungsmaßstab zur Ermittlung Kritischer Infrastrukturen zu erhalten.

Betreiber wesentlicher Dienste haben spezielle Sicherheitsanforderungen zu treffen. Hierzu legt die NIS-RL fest, dass geeignete und verhältnismäßige technische und organisatorische Maßnahmen (sog. TOM) zu besorgen sind, die den Stand der Technik unter Einbeziehung von Normen sowie technischen Leitlinien der *ENISA* (Art. 19) berücksichtigen. Der Begriff der „Berücksichtigung" ist zwar insoweit schwächer als die Vorgabe aus dem IT-Sicherheitsgesetz, wo im ver-

gleichbaren § 8a BSIG der Stand der Technik „eingehalten werden soll", jedoch greift hier die Vorgabe der Mindestharmonisierung, sodass der nationale Gesetzgeber an dieser Stelle auch höhere Anforderungen bestimmen kann. Ziel der angeordneten Schutzmaßnahmen ist die Förderung der maximalen Dienstverfügbarkeit.
Neben der Einrichtung der TOM wird ferner die Schaffung einer inhaltlichen Meldepflicht der Betreiber für Sicherheitsvorfälle mit einer erheblichen Auswirkung auf die Dienstverfügbarkeit vorgeschrieben. Auch hier geht das IT-Sicherheitsgesetz weiter als die NIS-RL, denn nach deutschem Recht ist bereits die potenzielle Dienstbeeinträchtigung zur Auslösung der Meldepflicht ausreichend. Die NIS-RL definiert verschiedene Kriterien zur Meldepflichtauslösung:

- Betroffene Nutzerzahl,
- Dauer des Sicherheitsvorfalls,
- dessen geographische Ausbreitung,
- daneben sieht das Regelwerk die Möglichkeit zur Festlegung EU-weiter Kriterien für eine Meldepflichtauslösung vor.

Die jeweilige Meldung wird inhaltlich in den transnationalen, EU-weiten Informationsaustausch einbezogen. Die national zuständige Behörde, hierzulande das *Bundesamt für Sicherheit in der Informationstechnik (BSI),* kann ferner Hinweise an den Meldenden zur Bewältigung des Sicherheitsvorfalls geben. Daneben besteht in Einzelfällen die Möglichkeit zur behördlichen Unterrichtung der Öffentlichkeit.
Interessant für das Segment der wesentlichen Dienste dürfte zudem die Vorschrift des Art. 15 Abs. 1 der NIS-RL sein: Hiernach haben die Mitgliedstaaten sicherzustellen, dass die Behörden bewerten können, ob die Betreiber ihren Pflichten zu den TOM sowie zur Meldung tatsächlich nachkommen. In der Praxis stellt sich bei einer von der *Bundesregierung* ermittelten Zahl von in etwa 2.000 betroffenen Betreibern die Frage, wie dies effektiv realisiert werden soll und ob stichprobenartige Kontrollen hierzu ausreichend sind. Abschließend wird für die wesentlichen Dienste bestimmt, dass mitgliedstaatlich ebenso zu gewährleisten ist, dass geeignete behördliche Ressourcen zur Überprüfung der vorgegebenen Sicherheitsanforderungen bereitstehen, zudem ist den zuständigen Behörden von den Mitgliedstaaten eine Weisungsbefugnis gegenüber den Betreibern bei festgestellten Sicherheitsmängeln einzuräumen.

5. Schutz der Anbieter digitaler Dienste, Art. 16, 17, 18

Einen weiteren inhaltlichen Schwerpunkt der NIS-RL stellt der Schutz von Anbietern digitaler Dienste dar. Ein digitaler Dienst ist eine Dienstleistung der Informationsgesellschaft. Hierunter ist jede in der Regel gegen Entgelt elektronisch im Fernabsatz und auf individuellen Abruf eines Empfängers erbrachte Dienstleistung zu verstehen. Konkretisiert werden die digitalen Dienstleistungen durch den Anhang III der RL als Online-Marktplatz, Online-Suchmaschine und Cloud Computing-Dienst. Im Vergleich zum IT-Sicherheitsgesetz werden die Vorgaben für „digitale Dienste" durch § 13 Abs. 7 TMG bestimmt. Hiernach ist bei geschäftsmäßig angebotenen Telemedien durch den Diensteanbieter unter Berücksichtigung des Stands der Technik sicherzustellen, dass kein unerlaubter Zugriff auf technische Einrichtungen möglich sowie eine Absicherung gegen Datenschutzverletzungen und äußere Angriffe vorhanden ist. Von der NIS-RL hingegen wird vorgeschrieben, dass geeignete, verhältnismäßige TOM von den Diensteanbietern zu treffen sind, um unter Berücksichtigung des Stands der Technik Risiken für die Netz- und Informationssicherheit zu bewältigen. Gem. Art. 4 Nr. 9 sind unter Risiken alle mit vernünftigem Aufwand feststellbaren Umstände oder Ereignisse zu verstehen, die potenziell nachteilige Auswirkungen auf die Sicherheit von NIS haben. Bei der Bestimmung der TOM erfolgt eine Einbeziehung von Normen und technischen Leitlinien der *ENISA* (Art. 19). Soweit in diesem Falle eine Gegenüberstellung von nationalem und europäischem IT-Sicherheitsrecht erfolgt, lassen sich auf den ersten Blick nur wenige Unterschiede der verschiedenen Vorgaben ausmachen: Während das Schutzziel durch die NIS-RL zunächst weiter gefasst zu sein scheint, erfolgt aber wiederum eine Eingrenzung des Anwendungsbereichs mit der Beschränkung auf den Anhang III, das TMG hingegen betrifft sämtliche Telemedien.
Auch für digitale Diensteanbieter sieht die NIS-RL Meldepflichten bei Sicherheitsvorfällen vor, die erhebliche Auswirkungen auf die Bereitstellung des Dienstes haben. Zur Beurteilung der Erheblichkeit werden ähnliche Bemessungskriterien wie schon für die wesentlichen Dienste herangezogen. Ebenso besteht eine Meldepflicht, soweit wesentliche Dienste mit digitalen Diensten verknüpft sind und wenn der Sicherheitsvorfall beim digitalen Dienst eine Verfügbarkeitseinschränkung des wesentlichen Diensts zur Folge hat. Bei einem im öffentlichen Interesse liegenden Vorfall ist die behördliche Benachrichtigung der Öffentlichkeit möglich. Ausnahmen von der Meldepflicht gelten für solche Anbieter, die nicht über den Zugang zu den für die Vorfallsbewertung relevanten Informationen verfügen sowie für Kleinstunternehmen i.S.d. EU-Rechts mit weniger als zehn Mitarbeitern und einer Jahresbilanz, die nicht größer als € 2 Mio. ist. Falls sich Hinweise auf die Nichteinhaltung von Meldepflicht und TOM ergeben sollten, besteht laut NIS-RL die Möglichkeit zu einer nachträglichen behördlichen Überprüfung. Eine besondere Regelung findet sich noch in Art. 18: Demgemäß müssen Anbieter digitaler Dienste ohne Sitz in der EU einen Vertreter in der EU benennen. Die gerichtliche Zuständigkeit bemisst sich nach dem Niederlassungsort dieses Vertreters.

6. Meldung für unkritische Strukturen, Art. 20

Wo für die Betreiber wesentlicher und digitaler Dienste eine Meldepflicht gilt, wandelt sich diese für unkritische Strukturen in eine fakultative Meldeoption um. Diese Meldemöglichkeit ist ebenso beschränkt auf Sicherheitsvorfälle, die erhebliche Auswirkungen auf die Dienstverfügbarkeit haben. Das behördliche Bearbeitungsverfahren für diese freiwilligen Meldungen folgt methodisch demjenigen für die Betreiber wesentlicher Dienste, jedoch wird bestimmt, dass eine Bearbeitung nur dann stattfindet, soweit diese keinen unverhältnismäßigen Aufwand erfordert. Denknotwendigerweise besitzen die freiwilligen Meldungen auch eine geringere Priorisierung in ihrer Verarbeitung als die obligatorischen Meldungen. Ausdrücklich wird festgestellt, dass aus der freiwilligen Option keine Verpflichtungen für die einmeldende Stelle resultieren.

7. Nationaler Ordnungsrahmen, Art. 7, 8, 9, 10

Die NIS-RL bestimmt nicht nur Pflichten für Betreiber und Diensteanbieter, sondern legt darüber hinaus einen umfassenden nationalen Ordnungsrahmen der IT-Sicherheit fest. So wird vorgegeben, dass jeder Mitgliedstaat eine nationale Strategie für die Netz- und Informationssicherheit zu bestimmen hat. Deutschland ist hier bereits gut aufgestellt mit dem nationalen Plan zum Schutz der Informationsinfrastrukturen (NPSI) von 2005, der im Jahr 2011 durch die umfangreiche Cyber-Sicherheitsstrategie der *Bundesregierung* abgelöst wurde.

Durch die NIS-RL wird ebenso die Verpflichtung zur Benennung einer für die NIS zuständigen Behörde und zentralen Anlaufstelle festgesetzt, für Deutschland kann das *BSI* diese Rolle ausfüllen, das als Verbindungsstelle zur transnationalen Zusammenarbeit und zur Zusammenarbeit mit Strafverfolgungs- und Datenschutzbehörden fungieren kann. Die nationale NIS-Strategie und die Aufstellung über die national zuständigen Behörden sind der *EU-Kommission* mitzuteilen, welche diese Liste EU-weit publiziert.

Jeder Mitgliedstaat steht zudem in der Pflicht, eigene mitgliedstaatliche CSIRTs (Computer Security Incident Response Team) bzw. CERTs (Computer Emergency Response Team) zu benennen. In Deutschland kann in dieser Rolle der CERT-Bund, welcher beim *BSI* angesiedelt ist, fungieren, welcher bereits die wesentlichen, in diesem Zusammenhang stehenden Anforderungen aus Anhang I der NIS-RL erfüllt. Die *EU-Kommission* ist über die Tätigkeit der nationalen CSIRTs zu unterrichten, ferner sind jährliche Zwischenberichte auf EU-Ebene über nationale IT-Sicherheitsvorfälle einzureichen.

8. Europäischer und internationaler Ordnungsrahmen, Art. 11, 12, 13

Da die NIS-RL den Aufbau einer einheitlichen europäischen Cyber-Sicherheitsstrategie zum Ziel hat, enthält sie denknotwendigerweise auch umfängliche Vorgaben zur Schaffung eines europäischen – und darüber hinaus auch internationalen – Ordnungsrahmens für die Netz- und Informationssicherheit. Hierzu wird eine EU-weite Kooperationsgruppe zur strategischen Zusammenarbeit und zum zwischenstaatlichen Vertrauensaufbau für die NIS eingesetzt. Diese Kooperationsgruppe setzt sich aus Vertretern der Mitgliedstaaten, der *EU-Kommission* und der *ENISA* zusammen. Daneben besteht die Möglichkeit, externe Interessengruppen zu beteiligen. Es ist geplant, die Kooperationsgruppe in internationale Übereinkünfte zur IT-Sicherheit und zum Datenschutz einzubinden. Als wesentliche Aufgaben der EU-weiten Kooperationsgruppe bestimmt die NIS-RL die folgenden:

- Erstellung von Arbeitsprogrammen/strategischen Leitlinien,
- Informationsaustausch zur Verbesserung der EU-weiten Koordination und Zusammenarbeit,
- Informationsaustausch hinsichtlich Awareness, Forschung und Entwicklung, Verfahren zur Ermittlung wesentlicher Dienste, Meldepflichten,
- Bewertung und Verbesserung nationaler NIS-Strategien,
- Förderung der europäischen Normung,
- Sammlung von Informationen zur Koordination von IT-Sicherheitsvorfällen,
- Erstellung regelmäßiger Berichte zur Bewertung der transnationalen Zusammenarbeit.

Wo als Bestandteil der nationalen NIS-Strategie einzelne CSIRTs geschaffen werden, verfolgt die NIS-RL auf europäischer Ebene das Ziel, ein CSIRT-Netzwerk zur Förderung der übernationalen, operativen Zusammenarbeit zu errichten, das sich aus Vertretern der nationalen CSIRTs, des CERT-EU und unterstützend auch durch die *ENISA* zusammensetzt. Das CSIRT-Netzwerk erstellt regelmäßige Berichte zu den Ergebnissen der interstaatlichen Zusammenarbeit. Im Wesentlichen hat es folgende Aufgaben:

- Planung der operativen Zusammenarbeit der nationalen CSIRTs,
- Informationsaustausch unter den einzelnen CSIRTs,
- Ausarbeitung koordinierter Reaktionen auf Sicherheitsvorfälle,
- Unterstützung der Mitgliedstaaten bei der Bewältigung grenzüberschreitender Sicherheitsvorfälle,
- Unterrichtung der Kooperationsgruppe,
- Auswertung von Übungen zur Netz- und Informationssicherheit.

9. Sanktionen, Art. 21

Abschließend wird in Art. 21 der RL die mitgliedstaatliche Verpflichtung bestimmt, Sanktionsvorschriften bei einem Verstoß gegen die auf der RL basierenden nationalen Vorgaben zur NIS zu erlassen. Die Maßgabe dabei lautet, dass die Sanktionen „wirksam, angemessen und abschreckend" sein müssen. Für das deutsche Recht ist davon auszugehen, dass diesen Vorgaben entsprechende Regelungen bereits mit dem IT-Sicherheitsgesetz durch § 14 BSIG und § 16 TMG vorgegeben sind.

10. Fazit, Ausblick und Empfehlungen

Obgleich die NIS-RL umfangreich ausgefallen ist, ist nicht zu vermuten, dass sie speziell für die Betreiber Kritischer Infrastrukturen hierzulande erheblichen Handlungsbedarf mit sich bringt: So ist nach derzeitigem Erkenntnisstand wohl nicht zu erwarten, dass es zu einer Änderung oder gar Erweiterung der Sektoren Kritischer Infrastrukturen kommen wird. Ebenso stehen keine erheblichen Änderungen im Bereich der TOM und der Meldepflicht der Betreiber in Aussicht. Befürchtungen in Richtung eines „doppelten Implementierungsaufwands" infolge der parallelen nationalen und europäischen Gesetzgebung sind deshalb unbegründet, es sind lediglich Feinanpassungen zu erwarten. Den Betreibern Kritischer Infrastrukturen ist deshalb zu empfehlen, die Anforderungen des IT-Sicherheitsgesetzes wie ursprünglich geplant umzusetzen. Für den nationalen Gesetzgeber und die Behörden jedoch wird die Umsetzung des erweiterten europäischen Kooperationsrahmens zur Cybersicherheit mit einem größeren Aufwand verbunden sein. Insgesamt jedoch ist Deutschland durch sein bisheriges rechtspolitisches Handeln im Bereich der IT-Sicherheit für den neuen europäischen Cybersecurity-Raum gut gerüstet.

- Vgl. auch *Voigt/Gehrmann*, ZD 2016, 355; ZD-Aktuell 2016, 04945 und *Mehrbrey/Schreibauer*, MMR 2016, 75.

Dennis-Kenji Kipker
ist wissenschaftlicher Assistent am Institut für Informations-, Gesundheits- und Medizinrecht (IGMR) an der Universität Bremen und Mitglied im Vorstand der Europäischen Akademie für Informationsfreiheit und Datenschutz (EAID) in Berlin. Dieser Beitrag entstand im Rahmen des vom *BMBF* geförderten Forschungsschwerpunkts „IT-Sicherheit für Kritische Infrastrukturen" als Bestandteil der Hightech-Strategie der *Bundesregierung*.