DENNIS-KENJI KIPKER

Der BMI-Referentenentwurf zur Umsetzung der NIS-RL

Was dürfen Betreiber von Kritischen Infrastrukturen und Anbieter von digitalen Diensten erwarten?

Cybersecurity-Rechtsrahmen

Im Dezember 2016 wurde vom Bundesministerium des Innern der Referentenentwurf für das Umsetzungsgesetz zur EU-Richtlinie 2016/1148 (NIS-RL) zur Anhörung an die Verbände herausgegeben. Der folgende Beitrag befasst sich, basierend auf dieser Entwurfsfassung, mit den wesentlichen, hieraus resultierenden nationalen Gesetzesänderungen und vergleicht diese mit dem Richtlinientext sowie den Vorgaben, die durch das IT-Sicherheitsgesetz von 2015 getroffen wurden; ebenso werden die veranschlagten finanziellen Auswirkungen für die Betreiber wiedergegeben. Ein abschließender Ausblick zeigt den weiteren Weg auf, den Deutschland als Kooperationspartner im europäischen Cyber-Sicherheitsrahmen in den kommenden Jahren beschreiten wird.

Lesedauer: 18 Minuten

I. Der aktuelle nationale und europäische Cybersecurity-Rechtsrahmen

Nachdem zum 8.8.2016 die RL 2016/1148 „über Maßnahmen zur Gewährleistung einer hohen gemeinsamen Netz- und Informationssicherheit in der Union" (kurz: NIS-RL) der EU als zentraler Bestandteil der europäischen Cyber-Sicherheitsstrategie in Kraft getreten ist,[1] begannen für die Mitgliedstaaten verschiedene Umsetzungsfristen zu laufen, die mit dem neuen Rechtsakt zur Schaffung eines höheren IT-Sicherheitsniveaus für die Betreiber von wesentlichen und Anbieter von digitalen Diensten verbunden sind. Zentraler Termin für die EU-Mitgliedstaaten ist dabei der 9.5.2018. Spätestens zu diesem Zeitpunkt müssen die neuen, durch die NIS-RL geforderten Rechts- und Verwaltungsvorschriften umgesetzt sein. Diese Verpflichtung ist auf die Rechtsnatur der RL zurückzuführen: Gem. Art. 288 AEUV ist sie im Hinblick auf das in ihr vorgeschriebene, zu erreichende Ziel verbindlich, überlässt den innerstaatlichen Stellen jedoch die Wahl von Form und Mitteln in Bezug auf ebenjene Zielerreichung. Daraus folgt die rechtliche Konsequenz, dass sich die NIS-RL zunächst an die Organe der EU-Mitgliedstaaten richtet, die den europäischen Rechtsakt mittels eines nationalen Umsetzungsgesetzes in eigenstaatliches Recht transferieren müssen. Für Deutschland geschieht 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". Durch dieses Gesetz erfahren einige der Rechtsvorschriften, die bereits durch das IT-Sicherheitsgesetz (IT-SiG) als Artikelgesetz im Juli 2015[2] neu geschaffen oder novelliert wurden, eine (erneute) Anpassung. Überraschend dabei ist die Kürze der Zeit, innerhalb derer der Entwurf des nationalen Umsetzungsgesetzes für die NIS-RL von Seiten des *BMI* vorgelegt wurde. Deutlich wird hierdurch nicht nur, dass das Thema Cybersecurity durch die verschiedenen und teils prominenten Ereignisse in 2016[3] einen erheblichen rechtspolitischen Auftrieb erhalten hat, sondern auch, dass dem Gesetzgeber daran gelegen ist, für die zahlreichen durch die neuen Regelungen betroffenen Betreiber und Diensteanbieter so früh wie möglich Rechtssicherheit zu schaffen. Parallel dazu werden die Vorgaben zum Anwendungsbereich der europäischen und nationalen IT-Sicherheitsregelungen durch die BSI-Kritisverordnung (BSI-KritisV) konkretisiert. Der erste „Korb" dieser Verordnung, der die Sektoren Energie, Wasser, Ernährung sowie Informationstechnik und Telekommunikation (IKT) abbildet, wurde am 22.4.2016 ausgefertigt[4], die Konkretisierungen für den zweiten Korb mit den Sektoren Transport, Verkehr, Gesundheit sowie Finanz- und Versicherungsdienstleistungen werden aller Voraussicht nach zum 1. Quartal 2017 fertiggestellt sein[5]. Auch damit liegt Deutschland gut im Zeitplan, denn die NIS-RL schreibt in Art. 5. Abs. 1 vor, dass die Mitgliedstaaten die Ermittlung der Betreiber von sog. „wesentlichen Diensten" erst bis zum 9.11.2018 abgeschlossen haben müssen.

II. Die zentralen Neuregelungs- und Änderungsvorschläge

1. Schutz von Anbietern „digitaler Dienste"

Ein zentrales Anliegen der EU bei Schaffung der NIS-RL stellte der Schutz vor allem auch des digitalen europäischen Binnenmarkts dar. Da immer mehr Dienstleistungen auf nicht-körperlichem Wege erbracht werden, sind zahlreiche Wirtschaftszweige von der Funktionsfähigkeit der sog. „digitalen Dienste" abhängig,[6] die deshalb auch mit besonderen Anforderungen von der NIS-RL und damit auch im nationalen Umsetzungsgesetz belegt werden. Basierend auf Art. 4 Nr. 5 und 6 sowie Nr. 17-19 werden die digitalen Dienste zunächst in die Begriffsbestimmungen in § 2 Abs. 9 BSIG aufgenommen. Im Wesentlichen können demgemäß unter digitalen Diensten solche Dienste der Informationsgesellschaft verstanden werden, die von einer juristischen Person angeboten werden und die es Verbrauchern ermöglichen, Online-Kaufverträge oder Online-Dienstleistungsverträge mit Unternehmen auf Online-Marktplätzen abzuschließen. Daneben unterfallen dem Begriff der digitalen Dienste aber auch Online-Suchmaschinen. Dies sind ausgehend von der in das BSIG aus der NIS-RL übernommenen Definition solche Dienste, die es Nutzern ermöglichen, unterschiedliche Abfragen durchzuführen, und als Ergebnisse Links anzeigen, die im Zusammenhang mit dem angeforderten Inhalt stehen. Auch Cloud Computing-Dienste werden als digitale Dienste in Zu-

1 Dazu *Kipker*, ZD-Aktuell 2016, 05363.
2 BT-Drs. 18/4096 und 18/5121.
3 So z.B. der Angriff organisierter Cyberkrimineller auf den Industriekonzern Thyssenkrupp, der erfolgreich abgewehrt werden konnte; s. dazu heise-online v. 8.12.2016, „Massiver Hacker-Angriff auf Thyssenkrupp", abrufbar unter: https://www.heise.de/newsticker/meldung/Massiver-Hacker-Angriff-auf-Thyssenkrupp-3565857.html.
4 Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-Kritisverordnung – BSI-KritisV), abrufbar unter: https://www.gesetze-im-internet.de/bundesrecht/bsi-kritisv/gesamt.pdf.
5 intrapol.org, abrufbar unter: http://intrapol.org/2016/02/05/der-referentenentwurf-des-bmi-zur-bsi-kritisverordnung-bsi-kritisv-v. 13.1.2016/.
6 So Erwägungsgrund Nr. 3 der RL 2016/1148/EU.

kunft vom BSIG erfasst sein. Technisch greift die Definition dabei weit, indem bestimmt wird, dass für das Cloud Computing lediglich der Zugang zu einem skalierbaren und elastischen Pool gemeinsam genutzter Rechenressourcen ermöglicht werden muss.

Besondere Anforderungen an die Anbieter der zuvor definierten digitalen Dienste werden durch den neu eingefügten § 8c BSIG-E bestimmt. Hierdurch werden die Vorgaben der Art. 16 und 17 der NIS-RL umgesetzt. Von den Sicherheitsanforderungen des neuen § 8c BSIG-E erfasst werden solche Anbieter von digitalen Diensten, die ihre Leistungen im Inland bereitstellen oder, soweit sie einen digitalen Dienst ausschließlich in einem oder mehreren anderen Mitgliedstaaten der EU zur Nutzung bereitstellen, wenn sie ihren Hauptsitz im Inland haben oder dort IT-Systeme betreiben, die sie für ihre Diensteerbringung in der EU nutzen. Im Einzelnen sind die Vorgaben, die an die Anbieter von digitalen Diensten gestellt werden, mit denjenigen für Kritische Infrastrukturen vergleichbar: So sind gem. § 8c Abs. 1 BSIG-E ebenfalls geeignete und verhältnismäßige technische und organisatorische Maßnahmen (TOM) zu treffen, um eine maximale Verfügbarkeit zu gewährleisten. Berücksichtigt werden muss hierbei der Stand der Technik, der als Begriff bereits aus dem IT-SiG bekannt ist.[7] Die notwendigen Maßnahmen werden durch Durchführungsrechtsakte der *EU-Kommission* näher bestimmt. In § 8c Abs. 2 BSIG-E wird zudem auch für die Anbieter von digitalen Diensten eine gesetzliche Meldepflicht bestimmt. Hiernach ist jeder Sicherheitsvorfall, der erhebliche Auswirkungen auf die Bereitstellung eines digitalen Dienstes hat, unverzüglich dem *BSI* mitzuteilen. Auch hier erfolgt eine nähere Konkretisierung der an das Meldeverfahren zu stellenden Anforderungen durch die *EU-Kommission*. Die dabei zu berücksichtigenden Parameter entsprechen im Wesentlichen ebenso wieder den Vorgaben, die das IT-SiG für KRITIS-Betreiber anlegt. So kommt es auf die Zahl der betroffenen Nutzer, die Vorfallsdauer, die geografische Ausbreitung, das Ausmaß der Unterbrechung und deren Auswirkungen auf wirtschaftliche und gesamtgesellschaftliche Zusammenhänge an. Falls es Hinweise darauf gibt, dass ein Diensteanbieter die gesetzlichen Vorgaben für IT-Sicherheit nicht befolgt, werden dem *BSI* verschiedene Informationszugangs-, Prüf- und Weisungsrechte eingeräumt. Gem. § 14 Abs. 1 Nr. 5-7 BSIG-E sind die neu geschaffenen Verpflichtungen für die Anbieter digitaler Dienste bei Nichteinhaltung grundsätzlich bußgeldbewehrt, wodurch Art. 21 der NIS-RL umgesetzt wird. Ebenso werden die von den Betreibern von Energieversorgungsnetzen und Energieanlagen i.S.d. § 11 EnWG als Spezialregelung schon bisher zu treffenden und mit den allgemeinen §§ 8a, 8b BSIG vergleichbaren Vorgaben zu TOV und Meldepflichten auch in Umsetzung des Art. 21 der NIS-RL in Zukunft bußgeldbewehrt sein. Dies wird durch die Änderung von § 95 EnWG erzielt. Im Hinblick auf die materiellen Verpflichtungen zur IT-Sicherheit ändert sich für die Betreiber dadurch jedoch nichts.

§ 15 BSIG-E bestimmt abschließend, dass die die Anbieter digitaler Dienste betreffenden Vorschriften ab dem 10.5.2018 anwendbar sind (vgl. für die europäische Umsetzungsfrist Art. 25 der NIS-RL).

2. IT-Notfall-Unterstützungsleistungen des BSI in herausgehobenen Fällen

Eine weitere zentrale Änderung betrifft den neuen § 5a BSIG-E (Wiederherstellung der Sicherheit oder Funktionsfähigkeit informationstechnischer Systeme in herausgehobenen Fällen). Zurückzuführen ist diese Neuregelung auf Kapitel II i.V.m. Anhang I der NIS-RL. Hier wird die Vorgabe aufgestellt, dass die Mitgliedstaaten über angemessene technische und organisatorische Fähigkeiten zur Prävention, Erkennung, Reaktion und Abschwächung von Sicherheitsvorfällen und Risiken bei Netz- und Informationssystemen verfügen müssen und wirksame und kompatible Fähigkeiten zur Bewältigung von IT-Sicherheitsvorfällen und Risiken gewährleisten. Mit § 5a BSIG-E soll zur Erreichung dieser Ziele eine geeignete Grundlage aufgestellt werden, wobei die Maßnahmenkoordination im Nationalen Cyber-Abwehrzentrum stattfindet. Abs. 1 ermöglicht dem *BSI*, bei einer Beeinträchtigung der Sicherheit oder Funktionsfähigkeit eines IT-Systems einer Stelle des Bundes oder eines Betreibers von KRITIS auf Ersuchen der betroffenen Stellen durch ein Mobile Incident Response Team (MIRT) und ggf. unter Zuhilfenahme der Unterstützung Dritter, die gem. Abs. 5 eine IT-Sicherheitskooperation mit dem *BSI* eingegangen sind, diejenigen Maßnahmen zu treffen, die zur Systemwiederherstellung erforderlich sind, soweit es sich um einen herausgehobenen Fall handelt. Ebenso kann der Hersteller betroffener IT-Komponenten einbezogen werden (Abs. 6). Ein herausgehobener Fall liegt dann vor, wenn der Angriff von besonderer technischer Qualität ist oder die zügige Wiederherstellung der Sicherheit oder Funktionsfähigkeit des betroffenen IT-Systems ein besonderes öffentliches Interesse genießt. Das Kriterium der besonderen technischen Qualität ist dann zu bejahen, wenn ein Verdacht auf Advanced Persistent Threats (APTs) besteht, als ein weiteres Beispiel werden in der Entwurfsbegründung auch Distributed Denial of Service-Angriffe (DDoS) genannt. Das öffentliche Interesse kann z.B. dann bejaht werden, wenn Kritischen Infrastrukturen ein Ausfall droht, die Öffentlichkeit gefährdende Anlagen angegriffen werden oder die Kompromittierung von staatlichen IT-Systemen erfolgt.[8] Die Tätigkeit des *BSI* erfolgt dabei unvergütet, dient jedoch allein der schnellen Wiederherstellung der betroffenen IT-Systeme, d.h. es erfolgt keine dauerhafte Unterstützung von Seiten der Behörde. Hierdurch soll vermieden werden, dass Betreiber davon Abstand nehmen, kostenpflichtige IT-Services Dritter in Anspruch zu nehmen und sich stattdessen auf die regelmäßige, unvergütete Hilfestellung durch das *BSI* verlassen.[9] Da es sich um eine „Kann-Vorschrift" handelt, besteht auch keine gesetzliche Verpflichtung des *Bundesamts*, in jedem Falle tätig zu werden. Der Ausnahmecharakter der Vorschrift des § 5a BSIG-E wird am Beispiel der sog. „Verschlüsselungstrojaner" nochmals deutlich, die im Februar 2016 die öffentliche Aufmerksamkeit erregten, indem sie die Datenbestände eines Krankenhauses in Nordrhein-Westfalen unbrauchbar machten.[10] Hierzu wird festgestellt, dass das *BSI* im Regelfall nur dann tätig wird, wenn neuartige Angriffsvektoren eingesetzt werden. Für den Fall der Verschlüsselungstrojaner wäre nunmehr somit ein Eingriff durch das *BSI-MIRT* regelmäßig ausgeschlossen, da dieses Angriffsmittel in der Öffentlichkeit bereits hinreichende Bekanntheit erlangt hat. § 5a Abs. 7 BSIG-E legt abschließend fest, dass das *BSI-MIRT* auch in bestimmungsgemäß unkritischen Fällen tätig werden kann, soweit ein vergleichbares öffentliches Interesse an der Vorfallsbehebung besteht. Das ist z.B. dann der Fall, wenn der Betroffene der staatlichen Geheimschutzbetreuung unterfällt oder aber solche Anlagen oder Systeme von einem Angriff betroffen sind, deren Ausfall ähnlich weitreichende Auswirkungen hätte wie eine Beeinträchtigung von Kritischen Infrastrukturen.[11]

---

7 S. zur technischen Konkretisierung dieses unbestimmten Rechtsbegriffs bzw. der Generalklausel *Kipker*, DuD 2016, 610 und *Kipker/Pfeil*, DuD 2016, 810 ff.

8 Referentenentwurf des *BMI* für ein Gesetz zur Umsetzung der NIS-RL (im Folgenden: RefE), abrufbar unter: http://www.bmi.bund.de/SharedDocs/Downloads/DE/Gesetzestexte/Entwuerfe/entwurf-umsetzung-nis-richtlinie.pdf?__blob=publicationFile, S. 33.

9 RefE (o. Fußn. 8), S. 32.

10 Heise Online v. 12.2.2016, „Ransomware-Virus legt Krankenhaus lahm", abrufbar unter: https://www.heise.de/newsticker/meldung/Ransomware-Virus-legt-Krankenhaus-lahm-3100418.html.

11 RefE (o. Fußn. 8), S. 36 f.

3. Konfliktfeld IT-Sicherheit und Datenschutz

Der Konflikt zwischen IT-Sicherheit und Datenschutz, der sich zuletzt im Juli 2015 mit der Schaffung des § 100 TKG (sog. „kleine Vorratsdatenspeicherung“[12]) für das IT-SiG entzündete, indem TK-Diensteanbieter Bestands- und Verkehrsdaten von Nutzern zu Zwecken der IT-Sicherheit verarbeiten können, aktualisiert sich nunmehr für das *BSI* mit dem § 5a Abs. 3 BSIG-E. Demgemäß darf die Behörde bei MIRT-Maßnahmen auch personenbezogene oder dem Fernmeldegeheimnis unterliegende Daten erheben und verarbeiten, soweit dies für die IT-Sicherheit erforderlich und angemessen ist. Die Übermittlung von Daten an Strafverfolgungs- und Verfassungsschutzbehörden oder an den *BND* ist bereits gem. § 5 Abs. 5 und 6 BSIG in der geltenden Fassung zulässig. Soweit ein Angriff auf kritische IT-Systeme vorliegt, soll im Regelfall zugleich ein Anfangsverdacht zur Begehung von Straftaten oder eine Gefahr für die öffentliche Sicherheit bestehen.[13] Ansonsten gilt ausgehend von § 5a Abs. 4 BSIG-E für Datenbestände der Einwilligungsgrundsatz, d.h. die anfallenden Informationen dürfen nur mit dem Einverständnis des Betroffenen übermittelt werden, es sei denn, die Daten lassen keinen Rückschluss auf diesen zu. Insoweit besteht infolge der neuen Regelung nunmehr durchaus eine explizite Vergleichbarkeit im Umgang mit Unternehmens- und personenbezogenen Daten.

4. Anpassung der TOV für die Betreiber von Kritischen Infrastrukturen

Die NIS-RL stellt höhere Anforderungen an die Dokumentation und Überprüfung der IT-Sicherheitsmaßnahmen, die von den Betreibern der Kritischen Infrastrukturen ergriffen werden müssen, als dies bisher durch das IT-SiG der Fall gewesen ist. So wird in Art. 15 der RL explizit festgeschrieben, dass die zuständige Behörde die Umsetzung der TOV, die für die Funktionsfähigkeit von KRITIS maßgeblich sind, überprüfen und verlangen können muss, dass die zur Kontrolle der IT-Sicherheit notwendigen Informationen vom Betreiber zur Verfügung gestellt werden. Schon im Vorfeld der nationalen Umsetzung der NIS-RL war in Fachkreisen streitig, wie diese doch recht strenge Anforderung bei einer Zahl von ca. 2.000 betroffenen KRITIS-Betreibern effektiv realisiert werden kann. Im BSIG sollen die Anforderungen der NIS-RL neben einer erweiterten Dokumentationspflicht vornehmlich durch das Einfügen eines neuen § 8a Abs. 4 umgesetzt werden. Diese Vorschrift erlaubt es dem *Bundesamt* sowie sog. „qualifizierten Stellen“ i.S.d. § 9 Abs. 3 BSIG (vom *BSI* anerkannte sachverständige Stellen, z.B. Penetrationstester oder Grundschutz-Auditoren[14]), die Geschäfts- und Betriebsräume während der üblichen Betriebszeiten zu betreten und sich die für die IT-Sicherheit relevanten Aufzeichnungen, Schriftstücke und sonstigen Unterlagen in geeigneter Weise vorlegen zu lassen. Der Betreiber hat dabei Auskünfte zu erteilen und die für die Arbeit des *BSI* erforderliche Unterstützung zu gewährleisten. Hierdurch soll das *BSI* in die Lage versetzt werden, unabhängig von der Meldung von IT-Sicherheitsmängeln durch die Betreiber zu überprüfen, ob diese ihrer gesetzlichen Pflicht zu TOV gem. § 8a Abs. 1 BSIG nachkommen. Zudem stelle laut der Entwurfsbegründung die unmittelbare Einsichtnahme vor Ort zugleich eine geringere Belastung für die Betreiber dar.[15] Das *BSI* kommt seinem Betretensrecht primär in denjenigen Fällen nach, in denen die Prüfung der gem. § 8a Abs. 3 Satz 1 BSIG von den Betreibern alle zwei Jahre vorzulegenden IT-Sicherheitsnachweise in Einzelfällen nicht ausreichend ist. Falls bei der Vor-Ort-Einsichtnahme zusätzliche Kosten entstehen sollten, sind diese vom jeweiligen Betreiber zu tragen.

5. Anpassung der Meldepflicht und neuer Fokus auf die Funktionsfähigkeit der Kritischen Infrastruktur

Ebenfalls eine Anpassung durch die NIS-RL erhält § 8b BSIG (Zentrale Stelle für die Sicherheit in der Informationstechnik Kritischer Infrastrukturen). Diese Vorschrift wird in zweierlei Weise überarbeitet: Zum einen finden sich hier erste Vorgaben zur Errichtung des transnationalen europäischen Cybersecurity-Rahmens, indem das *BSI* die von den Betreibern erhaltenen Meldungen nicht nur auswertet, sondern ggf. auch die zuständigen Behörden in einem anderen Mitgliedstaat über IT-Security-Incidents informiert (vgl. § 8b Abs. 2 Nr. 4 lit. d BSIG-E, ausgenommen sind Genehmigungsinhaber gem. §§ 6, 7 und 9 AtG). Zum anderen werden die meldepflichtauslösenden Fälle sowie die Meldeinhalte an Art. 14 Abs. 3 der NIS-RL angepasst. Hierzu wird das zur Beurteilung der Meldeschwelle herangezogene Erheblichkeitskriterium nicht mehr auf den Grad des IT-Vorfalls, sondern auf den Grad der Beeinträchtigung der Funktionsfähigkeit einer Kritischen Infrastruktur bezogen. Dies führt nunmehr dazu, dass eine Meldepflicht sowohl dann besteht, wenn „einfache“ Störungen der IT zu einem Ausfall oder zu einer erheblichen Beeinträchtigung der Funktionsfähigkeit geführt haben, als auch für den Fall, dass „erhebliche“ Störungen der IT zu einem Ausfall oder einer erheblichen Beeinträchtigung lediglich führen können. Inhaltlich wird die Meldung ebenfalls an den neuen europäischen Rahmen zur Informationssicherheit angepasst, der bisherige Bezugspunkt „Branche des Betreibers“ wird aufgehoben und anstelle dessen i.S.d. BSI-KritisV auf die „erbrachte kritische Dienstleistung sowie die Auswirkungen der Störung auf diese“ abgestellt, s. § 8b Abs. 4 BSIG-E.

6. Anpassungen im KRITIS-Anwendungsbereich

Einige interessante Anpassungen des BSIG finden sich auch im Hinblick auf den Anwendungsbereich der gesetzlichen Regelungen zum Schutz von KRITIS. Durch das Umsetzungsgesetz zur NIS-RL wird die bisherige Regelung, dass die in § 8c Abs. 3 Nr. 1-4 BSIG genannten Betreiber (öffentliche TK-Netze, öffentlich zugängliche TK-Dienste, Energieversorgungsnetze, Energieanlagen, Telematikinfrastruktur, Genehmigungsinhaber gem. AtG) keine Kontaktstelle einrichten müssen, mit dem Ziel eines verbesserten Informationsaustauschs verschärft, indem für diese nunmehr lediglich die Verpflichtung aus § 8b Abs. 4 BSIG (Meldepflicht) ausgenommen wird, wohingegen zuvor § 8b Abs. 3-5 BSIG (Einrichtung der Kontaktstelle, Meldepflicht und gemeinsame übergeordnete Ansprechstelle) für nicht anwendbar erklärt wurden. Begründet wird diese Erweiterung mit der Notwendigkeit, den Betreibern Informationen und Warnungen zukommen zu lassen.[16] Für die meisten der vorgenannten Betreiber von KRITIS dürfte sich durch diese Novellierung einer allgemeinen BSIG-Vorschrift aber allein schon deshalb nicht viel ändern, weil sie bereits jetzt spezialgesetzlich in das Meldesystem eingebunden sind, was automatisch den Betrieb einer Ansprechstelle erfordert.

Da mit dem neuen § 8c BSIG auch neue rechtliche Anforderungen für die Anbieter der digitalen Dienste getroffen werden, ist es ebenso notwendig, speziell für diese Dienste spezifische Ausnahmeregelungen vorzusehen. Hierzu wird ein neuer Abs. 4 geschaffen. Demgemäß gelten die Regelungen zu den TOM und zu den Meldepflichten im Hinblick auf digitale Dienste nicht für Kleinstunternehmen und kleine Unternehmen i.S.d. Empfehlung 2003/361/EC der *EU-Kommission*. Hier wird somit ein Gleichlauf mit der schon bestehenden Ausnahmeregelung für Kritische Infrastrukturen in § 8c Abs. 1 BSIG (neu: § 8d Abs. 1 BSIG-E) hergestellt. Die Meldepflicht gem. § 8c Abs. 2 BSIG-E

12 Dazu *Eckhardt*, ZD 2014, 599, 603 f.
13 RefE (o. Fußn. 8), S. 35.
14 RefE (o. Fußn. 8), S. 40.
15 RefE (o. Fußn. 8), S. 39.
16 RefE (o. Fußn. 8), S. 43.

gilt ferner nicht für Anbieter, die ihren Hauptsitz in einem anderen Mitgliedstaat der EU haben oder, soweit sie nicht in einem Mitgliedstaat der EU niedergelassen sind, einen Vertreter in einem anderen Mitgliedstaat der EU benannt haben, in dem die digitalen Dienste ebenfalls angeboten werden.

7. Erweiterung der Verordnungsermächtigungen des BMI

§ 10 Abs. 1 BSIG enthält bereits jetzt die Verordnungsermächtigung des *BMI* für den Erlass der BSI-KritisV, die die allgemeinen Vorgaben zur Bestimmung der Kritischen Infrastrukturen gem. § 2 Abs. 10 BSIG weiter konkretisiert.[17] Darüber hinaus ist nunmehr vorgesehen, die Verordnungsermächtigungen des *BMI* um zwei weitere Absätze zu ergänzen: Mittels der Einfügung eines neuen Abs. 4 besteht die Möglichkeit des *BMI*, soweit die Durchführungsrechtsakte der *EU-Kommission* zur NIS-RL im Hinblick auf die Festlegung der TOV und Meldepflichten nicht abschließend bestimmt sein sollten, für diesen Bereich durch Rechtsverordnung eine eigenständige Regelung zu schaffen. Darüber hinaus kann das *BMI* gem. § 10 Abs. 5 BSIG-E ebenso durch Rechtsverordnung nähere Vorgaben zur Feststellung der Erheblichkeit von Beeinträchtigungen der Funktionsfähigkeit Kritischer Infrastrukturen treffen, die eine Meldepflicht gem. § 8b Abs. 4 BSIG-E auslösen können.

8. Gesetzliche Implementierung der europäischen Cybersecurity-Kooperation

Ein zentrales Anliegen der NIS-RL ist es, einen einheitlichen europäischen Cybersecurity-Raum zu schaffen, darüber hinaus auch die (politischen) Grundlagen für internationale Kooperationen im Bereich der IT-Sicherheit zu legen.[18] Zu diesem Zweck enthält die RL zahlreiche Vorgaben, die sich speziell an die mit der IT-Sicherheit befassten Behörden in den jeweiligen Mitgliedstaaten richten. Um die nationale Anbindung an den neuen europäischen Rahmen zu gewährleisten, wird durch das Umsetzungsgesetz u.a. der § 13 BSIG (Berichtspflichten) angepasst, indem die Absätze 3-5 angefügt werden. Bestimmt wird hier, dass das *BSI* bis zum 9.11.2018 verschiedene Informationen an die *EU-Kommission* übermitteln muss:

- die nationalen Maßnahmen zur Ermittlung der Betreiber von Kritischen Infrastrukturen;
- eine Aufstellung der KRITIS-Sektoren, der als kritisch anzusehenden Dienstleistungen und ihres als bedeutend anzusehenden Versorgungsgrads (sog. Schwellenwerte);
- eine zahlenmäßige Aufstellung der ermittelten KRITIS-Betreiber.

Soweit ein KRITIS-Betreiber in einem anderen EU-Mitgliedstaat seine Dienstleistungen bereitstellt, nimmt das *BSI* mit der jeweils zuständigen mitgliedstaatlichen Behörde Konsultationen auf (Abs. 4). § 13 Abs. 5 BSIG-E legt fest, dass das *BSI* die Meldungen für KRITIS sowie für digitale Dienste gem. §§ 8b, 8c BSIG-E bis zum 9.8.2018 und danach jährlich als zusammenfassenden Bericht an die *EU-Kooperationsgruppe* nach Art. 11 der NIS-RL übermittelt. Die *EU-Kooperationsgruppe* wird zur Verbesserung der strategischen Zusammenarbeit sowie des transnationalen Informationsaustauschs einberufen und setzt sich aus Vertretern der Mitgliedstaaten, der *Kommission* und der *ENISA* zusammen.

9. Anpassung und Erweiterung der Sonderregelungen für die Telematikinfrastruktur

Bereits das geltende BSIG legt in seiner Vorschrift zum Anwendungsbereich in § 8c allgemein fest, dass für sonstige Betreiber von Kritischen Infrastrukturen, die vergleichbare Anforderungen an TOV wie auch an das Meldeverfahren erfüllen müssen, gesetzliche Spezialregelungen getroffen werden können, die denjenigen des BSIG vorgehen (s. § 8c Abs. 2 Nr. 5 und Abs. 3 Nr. 5 BSIG). Unter diese Sonderregelungen fallen sowohl die *Gesellschaft für Telematik* als Betreiber der Telematikinfrastruktur gem. § 291a Abs. 7 SGB V sowie die Betreiber von Diensten der Telematikinfrastruktur im Hinblick auf die nach § 291b Abs. 1a und 1e SGB V zugelassenen Dienste und Betreiber von Diensten, soweit sie die Telematikinfrastruktur für nach § 291b Abs. 1b SGB V bestätigte Anwendungen nutzen.[19] Diese Betreiber unterliegen bereits nach der geltenden Vorschrift des § 291b SGB V umfassenden Vorgaben, die den von Art. 14 Abs. 1-3 der NIS-RL geforderten Maßnahmen im Hinblick auf TOV und Meldepflichten für KRITIS entsprechen. In Art. 15 der NIS-RL wird darüber hinaus vorgeschrieben, dass die Mitgliedstaaten sicherzustellen haben, dass die zuständigen Behörden über Befugnisse und Mittel verfügen, um bewerten zu können, ob die KRITIS-Betreiber ihren vorgenannten Pflichten gem. Art. 14 der RL tatsächlich nachkommen. Im Hinblick auf diese Regelung stellt sich für die *Gesellschaft für Telematik* das Problem, dass sie einerseits zwar über umfassende Aufsichtsbefugnisse gegenüber den Betreibern von Diensten der Telematikinfrastruktur verfügt, andererseits aber hinsichtlich der Umsetzung der für sie als Betreiber der Telematikinfrastruktur gem. § 291a Abs. 7 SGB V geltenden Anforderungen und Meldepflichten allerdings nur einer eingeschränkten Aufsicht unterliegt. So erfolgt zwar die Einbindung des *BSI* bei der Erstellung von Vorgaben für den sicheren Betrieb der Telematikinfrastruktur sowie für die Zulassung von Komponenten und Diensten (s. § 291b Abs. 1 und 1a SGB V). Die Festlegung von Vorgaben und der Kriterien für das Bestätigungsverfahren für Dienstebetreiber der Telematikinfrastruktur und die Vornahme von Maßnahmen zur Gefahrenabwehr und Überwachung (§ 291b Abs. 6 und 7 SGB V) erfolgen aber lediglich in Abstimmung mit dem *BSI*, wodurch der *Gesellschaft für Telematik* ein Abweichungsrecht eingeräumt wird. Der durch das Umsetzungsgesetz neu zu schaffende § 291b Abs. 8 SGB V-E soll für diese Fälle sicherstellen, dass das *BSI* abweichende Entscheidungen der *Gesellschaft für Telematik* mittels ausreichender Informationen prüfen und im Zweifelsfall Anweisungen zur Abhilfe möglicherweise festgestellter Mängel erteilen kann. Hierdurch wird die europarechtliche Vorgabe aus Art. 15 Abs. 3 der NIS-RL zur Umsetzung gebracht.[20] Durch eine zusätzliche Gesetzesänderung in § 307 SGB V werden die teils neuen Verpflichtungen aus § 291b SGB V als Ordnungswidrigkeit geahndet, womit zugleich Art. 21 der NIS-RL berücksichtigt wird.

III. Bezifferbarer Erfüllungsaufwand für die Wirtschaft

Laut Entwurfsbegründung entsteht für die Betreiber von öffentlichen TK-Netzen, Energieversorgungsnetzen und Energieanlagen, die ausgehend von den Vorgaben des BSIG als Kritische Infrastrukturen eingestuft werden, ein Erfüllungsaufwand für das Betreiben der gesetzlich vorgeschriebenen Kontaktstelle. Der *Gesellschaft für Telematik* entsteht ein Erfüllungsaufwand ebenfalls für das Betreiben einer Kontaktstelle sowie durch die neuen Kooperationsanforderungen mit dem *BSI* nach § 291b Abs. 8 SGB V-E. Es wird erwartet, dass in etwa 300 Betreiber zum Betrieb einer Kontaktstelle verpflichtet werden, hierfür liegt der geschätzte Erfüllungsaufwand bei ca. € 660,– pro Stelle, sodass sich ein Gesamtkostenaufwand von € 200.000,– ergibt.[21]

Für KRITIS allgemein entsteht daneben ein weiterer Erfüllungsaufwand vor allem auch durch die Angabe zusätzlicher Informa-

17 S. zum Referentenentwurf des *BMI* zur BSI-Kritis-VO *Kipker*, MMR-Aktuell 2016, 375759.
18 S. Erwägungsgründe Nr. 4, 5 und 6 der RL 2016/1148/EU.
19 S. BT-Drs. 18/4096, S. 29.
20 RefE (o. Fußn. 8), S. 50 f.
21 RefE (o. Fußn. 8), S. 25.

tionen im Falle eines grenzüberschreitenden Bezugs von Sicherheitsvorfällen mit erheblicher Auswirkung, wodurch die EU-bezogene Kooperationsstrategie der NIS-RL in besonderem Maße zutage tritt. Zahlenmäßig wird nach wie vor davon ausgegangen, dass die Gesamtzahl der betroffenen Anlagen bei 2.000 liegt, wobei das *BSI* nicht mehr als 100 pro Jahr vor Ort überprüfen wird. Bei einem angesetzten Kostenpunkt von € 35.000,– je Vor-Ort-Begleitung ergibt sich damit ein wirtschaftlicher Gesamtaufwand von maximal € 3,5 Mio.[22]

Für die Anbieter von digitalen Diensten werden in erster Linie Erfüllungsaufwände angesetzt für die Durchführung der TOM und der Meldepflichten nach § 8c BSIG-E. Gerechnet wird im Rahmen einer ersten zahlenmäßigen Annäherung mit 1.100 Anbietern mit mehr als 50 Mitarbeitern bzw. einer Bilanzsumme, die € 10 Mio. überschreitet. Im Hinblick auf die Umsetzungskosten der TOM werden keine Vermutungen angestellt, jedoch wird angenommen, dass zahlreiche Betreiber digitaler Dienste schon jetzt entsprechende Maßnahmen eingeführt haben. Für das neue Meldeverfahren wird prognostiziert, dass pro Betreiber und Jahr die Meldung eines schweren Sicherheitsvorfalls erfolgt. Für den bisher im Meldeverfahren ebenso herangezogenen Kostensatz von € 660,– pro Meldung sollen sich für die Meldepflicht digitaler Dienste dadurch Gesamtkosten in Höhe von € 700.000,– ergeben.[23]

IV. Fazit und Ausblick

Nach Inkrafttreten der NIS-RL im August 2016 konnten bereits einige Spekulationen darüber angestellt werden, wie die nationale Umsetzung der europäischen Vorgaben zur IT-Sicherheit erfolgen würde. Nach Veröffentlichung des entsprechenden Referentenentwurfs des *BMI* im Dezember 2016 gab es nur wenig Überraschendes: Die Änderungen im BSIG, im AtG und im EnWG liegen allesamt im erwartbaren Rahmen und die Maßgaben für die betroffenen Betreiber erfahren keine wesentlichen Anpassungen, lediglich die Anforderungen, die durch die Änderungen des SGB V an die *Gesellschaft für Telematik* gestellt werden, wurden durch das IT-SiG von 2015 nur am Rande betrachtet. Die zentralsten Neuerungen im BSIG betreffen sowohl den § 5a wie auch den § 8c: Ersterer regelt die Unterstützungsleistungen des *BSI* zur Wiederherstellung der Sicherheit oder Funktionsfähigkeit von IT-Systemen in herausgehobenen Fällen durch Mobile Incident Response Teams (MIRT), letzterer die neuen Anforderungen an die IT-Security für die Anbieter von digitalen Diensten.

Deutlich wird mit dem Umsetzungsgesetz zur NIS-RL zudem, dass sich die bisherige gesetzgeberische Vorarbeit in Deutschland für den Bereich der IT-Security auszahlt: So konnte nicht nur das IT-SiG Einfluss auf die inhaltliche Ausgestaltung der europäischen NIS-RL nehmen, sondern Deutschland konnte sich ebenso im Bereich der IT-Sicherheit gesetzlich als europäischer Vorreiter etablieren. Für die betroffenen Unternehmen steht deshalb nicht wie teils befürchtet ein „doppelter Implementierungsaufwand" ins Haus, lediglich im Hinblick auf die Konkretisierung des Anwendungsbereichs der Regelungen zu Kritischen Infrastrukturen durch die BSI-KritisV könnten sich infolge des neuen Bezugs zum Europarecht neben einigen sonstigen Feinanpassungen Erweiterungen ergeben. Einen erheblichen Aufwand dürfte die nationale Umsetzung der NIS-RL aber für die beteiligten Behörden bedeuten.[24] Hier steht Europa nicht nur vor der Herausforderung, ein faktisch ungleiches IT-Sicherheitsniveau in den Mitgliedstaaten durch ein Gesetz anzugleichen, sondern ebenso den transnationalen Informationsaustausch und das dazu notwendige Vertrauen in die zwischenstaatliche Zusammenarbeit zu stärken. Hierzu ist es wichtiger denn je, dass sich Gesetzgebung und Verwaltung, Wissenschaft und Anwendungspraxis bestmöglich aufeinander abstimmen.

Fünf Jahre nach seinem Inkrafttreten wird das Umsetzungsgesetz zur NIS-RL einer Evaluierung gemäß dem Arbeitsprogramm der *Bundesregierung* zur besseren Rechtsetzung unterzogen.

Dr. Dennis-Kenji Kipker
ist Wissenschaftlicher Geschäftsführer des Instituts für Informations-, Gesundheits- und Medizinrecht (IGMR) an der Universität Bremen sowie Vorstandsmitglied der Europäischen Adademie für Informationsfreiheit und Datenschutz (EAID) in Berlin.

Dieser Beitrag entstand im Rahmen des vom *BMBF* geförderten Forschungsschwerpunkts „IT-Sicherheit für Kritische Infrastrukturen" (ITS/KRITIS) als Bestandteil der Hightech-Strategie der Bundesregierung.

22 RefE (o. Fußn. 8), S. 23.
23 RefE (o. Fußn. 8), S. 23 f.
24 Für den Erfüllungsaufwand der Verwaltung s. RefE (o. Fußn. 8), S. 25 ff.