Dennis-Kenji Kipker

Umsetzungsgesetz zur NIS-RL mit nur geringen Anpassungen gegenüber der bisherigen Rechtslage beschlossen

MMR-Aktuell 2017, 389121

Am 27.4.2017 hat der *Deutsche Bundestag* gegen die Stimmen der Opposition das Gesetz zur Umsetzung der RL 2016/1148 „über Maßnahmen zur Gewährleistung einer hohen gemeinsamen Netz- und Informationssicherheit in der Union" (kurz: NIS-RL) beschlossen. Die europäische Richtlinie zur IT-Sicherheit, die als zentraler Bestandteil der Cyber-Sicherheitsstrategie der EU zum 8.8.2016 in Kraft getreten ist, schreibt für die Mitgliedstaaten bis spätestens 9.5.2018 die Umsetzung der in ihr enthaltenen Vorgaben in nationale Rechts- und Verwaltungsvorschriften vor.

In Deutschland wird diese Umsetzung durch das jüngst vom *Bundestag* verabschiedete Gesetz erfolgen. Hierdurch erfahren einige der Rechtsvorschriften, die durch das IT-Sicherheitsgesetz (IT-SiG) im Juli 2015 novelliert oder neu geschaffen wurden, eine Anpassung. Der erste Referentenentwurf eines „Gesetzes zur Umsetzung der Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6.7.2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union" wurde am 7.12.2016 durch das *BMI* vorgelegt. Der darauf basierende Gesetzentwurf der *Bundesregierung* v. 20.2.2017 (BT-Drs. 18/11242), ergänzt um die Stellungnahme des *Bundesrats* mit Gegenäußerung der *Bundesregierung* (BT-Drs. 18/11620), die Beschlussempfehlung des *Innenausschusses* (BT-Drs. 18/11808) sowie der durch den *Bundesrat* abgedruckte Gesetzesbeschluss des *Bundestags* (BR-Drs. 335/17), bilden die wesentlichen Grundlagen des Gesetzgebungsverfahrens. Auf der Beschlussempfehlung und dem Bericht des *Innenausschusses* basierend, sowie inklusive der Maßgaben nach BR-Drs. 335/17, i.Ü. unverändert, hat der *Deutsche Bundestag* den Gesetzentwurf angenommen.

Gegenüber dem ursprünglichen Referentenentwurf für ein Umsetzungsgesetz zur EU NIS-RL haben sich inhaltlich nur geringfügige Änderungen ergeben. Wesentliche Anpassungen werden an dieser Stelle zusammengefasst dargestellt:

- **Definitionen:** § 2 Abs. 12 BSIG soll in Zukunft eine Definition des Anbieters digitaler Dienste enthalten, nach der hierunter eine juristische Person zu verstehen ist, die einen digitalen Dienst anbietet.
- **Aufgabenfestlegungen:** Das *Bundesamt für Sicherheit in der Informationstechnik (BSI)* wird nach § 3 Abs. 1 Nr. 13 lit. b BSIG in Zukunft nicht nur die Verfassungsschutzbehörden, sondern ebenso den *MAD* bei der Auswertung und Bewertung von Informationen, die bei der Beobachtung terroristischer Bestrebungen oder nachrichtendienstlicher Tätigkeiten anfallen, unterstützen.
- **Datenübermittlungsbefugnisse:** Die Übermittlungsbefugnis für personenbezogene Daten im IT-Sicherheitsbereich wird ausgedehnt. Eine entsprechende Übermittlung kann nicht nur an das *Bundesamt für Verfassungsschutz (BfV)*, sondern auch an den *MAD* erfolgen, wenn sich sicherheitsgefährdende oder geheimdienstliche Tätigkeiten gegen Personen, Dienststellen oder Einrichtungen im Geschäftsbereich des *BMVg* richten (§ 5 Abs. 5 Satz 2 Nr. 2 BSIG). Neu eingebracht ist in § 5 Abs. 5 Satz 2 Nr. 3 BSIG ferner eine Datenübermittlungsbefugnis des *BSI* an den *BND*, wenn dies zur Unterrichtung über Tatsachen, die einen internationalen kriminellen, terroristischen oder staatlichen Angriff mittels Schadprogrammen oder vergleichbaren schädlich wirkenden informationstechnischen Mitteln auf die Vertraulichkeit, Integrität oder Verfügbarkeit von IT-Systemen in Fällen von erheblicher Bedeutung mit Bezug zur Bundesrepublik Deutschland erkennen lassen. Eine ähnlich gelagerte Datenübermittlungsbefugnis des *BSI* an den *BND* findet sich in § 5 Abs. 6 Satz 1 Nr. 4 BSIG.
- **Einsatz der Mobile Incident Response Teams (MIRT) des BSI:** § 5a BSIG sieht den Einsatz von MIRTs des *BSI* vor, soweit die Sicherheit oder Funktionsfähigkeit informationstechnischer Systeme einer Stelle des Bundes oder eines Betreibers einer Kritischen Infrastruktur in herausgehobenen Fällen beeinträchtigt ist. In Absatz 1 wird nunmehr nochmals besonders betont, dass die von *BSI-MIRT* ergriffenen Maßnahmen ausschließlich der Schadensbegrenzung und der Sicherstellung des Notbetriebs vor Ort dienen. In Absatz 7 wird bestimmt, dass das *BSI-MIRT* auch außerhalb von Stellen des Bunds und den Betreibern der Kritischen Infrastrukturen tätig werden kann, jedoch nur dann, wenn ein herausgehobener Fall i.S.v. § 5a Abs. 2 BSIG vorliegt.
- **Meldepflicht der Betreiber von Kritischen Infrastrukturen:** Die Vorgaben zu den Meldepflichten der Betreiber von Kritischen Infrastrukturen gem. § 8b BSIG werden konkretisiert. Nach Satz 1 Nr. 1 und Nr. 2 ist eine Meldung an das *BSI* dann zu erstatten, wenn es um eine Beeinträchtigung der „Funktionsfähigkeit der betriebenen Kritischen Infrastruktur" geht. Die vorhergehende Formulierung stellte demgegenüber lediglich auf die „Beeinträchtigung" ab, ohne diese weitergehend zu konkretisieren.
- **Besondere Anforderungen an Anbieter digitaler Dienste:** § 8c BSIG sieht für die Anbieter von digitalen Diensten in Umsetzung der EU NIS-RL vor, dass diese geeignete und verhältnismäßige technische und organisatorische Maßnahmen zu treffen haben, um die Risiken für ihre Netz- und Informationssysteme zu bewältigen. Ein neuer Absatz 2 konkretisiert diese Anforderung, wobei in Satz 2 Nr. 2 der allgemeine Begriff der „Bewältigung" von Sicherheitsvorfällen nunmehr durch die „Erkennung, Analyse und Eindämmung" ersetzt wird. In Absatz 4, innerhalb dessen der Verdacht auf Nichterfüllung der gesetzlich festgeschriebenen IT-Sicherheitsanforderungen für die Betreiber der digitalen Dienste geregelt wird, wird die Schwelle für ein Tätigwerden des *BSI* angepasst: Wo vorher „Nachweise" notwendig gewesen sind, ist es nun das Vorliegen von „Anhaltspunkten", welche das *BSI* zum Einschreiten berechtigen.
- **Auskunftsverlangen:** Die Schwelle für Auskunftsverlangen wird durch den neuen § 8e BSIG, vormals § 8d BSIG, verändert: Wo nach der geltenden Regelung die Auskunft zu Informationen und Meldungen nach den §§ 8a, 8b BSIG u.a. dann verweigert werden kann, wenn eine Beeinträchtigung von wesentlichen Sicherheitsinteressen zu erwarten ist, kann dies nunmehr schon dann geschehen, wenn eine Beeinträchtigung jedweder Sicherheitsinteressen auch nur eintreten kann. Damit wird das Verweigerungsrecht des *BSI* in erheblichem Maße ausge-

dehnt. Eine ähnliche Einschränkung findet sich nunmehr für den Zugang zu Akten: Dieser soll u.a. nur dann gewährt werden, wenn schutzwürdige Interessen des betroffenen Betreibers Kritischer Infrastrukturen oder des Anbieters digitaler Dienste dem nicht entgegenstehen und durch den Zugang zu den Akten keine Beeinträchtigung von Sicherheitsinteressen eintreten kann. Das Erfordernis einer „Verfahrensbeteiligung" hingegen wurde gestrichen.

■ **Ermächtigung zum Erlass von Rechtsverordnungen:** § 10 BSIG wird ein neuer Absatz 4 angehängt. Dieser bestimmt, dass wenn die Durchführungsrechtsakte der *EU-Kommission* gem. Art. 16 Abs. 8 und 9 NIS-RL keine abschließenden Bestimmungen über die von Anbietern digitaler Dienste zu treffenden TOM (technisch-organisatorische Maßnahmen) sowie über die Parameter zur Meldepflicht enthalten, diese vom *BMI* durch Rechtsverordnung, die nicht der Zustimmung des *Bundesrats* bedarf, getroffen werden können.

■ **Berichtspflichten:** Die Regelungen zu den Berichtspflichten in § 13 BSIG sind gegenüber dem ursprünglichen Referentenentwurf vom Dezember 2016 im Wesentlichen unverändert geblieben. Absatz 3 bestimmt nunmehr noch zusätzlich, dass die an die *EU-Kommission* übermittelten Informationen zu den Betreibern Kritischer Infrastrukturen ebenso an verschiedene Bundesbehörden weiterzuleiten sind.

■ **Meldepflicht für die Betreiber von Energieversorgungsnetzen und Energieanlagen:** § 11 Abs. 1c EnWG, der die Meldepflicht von Betreibern aus dem Energiesektor regelt, wird neu gefasst. In der derzeit geltenden Fassung des Gesetzes besteht eine Meldepflicht im Falle von erheblichen Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit der IT-Systeme, Komponenten und Prozesse, die zu einem Ausfall oder einer Beeinträchtigung der Funktionsfähigkeit des Energieversorgungsnetzes oder der betreffenden Energieanlage führen können oder bereits geführt haben. Nach der Neufassung besteht eine Meldepflicht für Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit der IT-Systeme, Komponenten oder Prozesse, die tatsächlich zu einem Ausfall oder einer erheblichen Beeinträchtigung der Funktionsfähigkeit des Energieversorgungsnetzes oder der betreffenden Energieanlage geführt haben, oder aber bei erheblichen Störungen des IT-Systems, seiner Komponenten oder Prozesse, die lediglich zu einem Ausfall oder einer erheblichen Beeinträchtigung der Funktionsfähigkeit führen können. Das schon bestehende Erheblichkeitskriterium wird somit – den Vorgaben der EU NIS-RL folgend – im Wesentlichen nicht mehr auf den Grad des IT-Vorfalls, sondern auf den Grad der Beeinträchtigung der Funktionsfähigkeit der Kritischen Infrastruktur bezogen. Die Zahl der meldepflichtigen Ereignisse dürfte sich für die Betreiber hierdurch reduzieren, denn in jedem Falle muss sich der IT-Vorfall, unabhängig von seiner Schwere, in erheblicher Weise auf den Netz- oder auf den Anlagenbetrieb auswirken. Eine weitere Neuerung betrifft den Inhalt der Meldepflicht: Dem auch auf der Richtlinie basierenden europäischen Kooperationsrahmen in Sachen Cybersicherheit folgend, muss die Meldung nunmehr auch Angaben zu möglichen grenzüberschreitenden Auswirkungen des IT-Vorfalls enthalten. Erwähnenswert ist zudem noch eine redaktionelle Änderung: In § 11 Abs. 1c Satz 6 EnWG wurde bisher auf die nicht-existenten §§ 11a bis 11c EnWG verwiesen. Nunmehr wird klargestellt, dass es sich dabei um die Absätze 1a bis 1c des § 11 EnWG handelt.

■ **Änderungen im TKG – Ausweitung und Konkretisierung der Datenerhebung zu Zwecken der IT-Sicherheit durch die Diensteanbieter, Erweiterung der Mitteilungspflichten, weitere Maßnahmen bei von Nutzern ausgehenden Störungen:** Ausgehend von § 100 Abs. 1 TKG, der bei Verabschiedung des IT-SiG vielfach als „kleine Vorratsdatenspeicherung" kritisiert wurde, darf der Diensteanbieter Bestands- und Verkehrsdaten von Teilnehmern und Nutzern zu Zwecken der IT-Sicherheit erheben und verwenden. Nunmehr ist auch eine Verarbeitung der Steuerdaten des informationstechnischen Protokolls zur Datenübertragung zulässig. Klargestellt wird dabei, dass die Kommunikationsinhalte selbst nicht Bestandteil der Steuerdaten des Protokolls sind. Flankierend werden durch § 100 Abs. 1 TKG nunmehr auch Datenschutzregelungen getroffen, so für die Löschung, die Zweckbindung, zum betrieblichen Datenschutzbeauftragten und der *BfDI* und zu möglichen Berichtspflichten an den Betroffenen. Die in § 109 TKG geregelten Mitteilungspflichten der TK-Diensteanbieter an die *BNetzA* werden ausgedehnt, so ist nunmehr bei allen im Gesetz genannten Arten von Beeinträchtigungen zugleich auch das *BSI* zu informieren, wohingegen dies zuvor nur bei Sicherheitsverletzungen mit einem Bezug zur Informationstechnik notwendig gewesen ist. Ergänzende Regelungen werden zudem auch in 109a TKG getroffen, soweit es um Störungen geht, die von den Datenverarbeitungssystemen der Nutzer ausgehen: So darf der Diensteanbieter Teile des Datenverkehrs in Bezug auf das störende System umleiten, die Nutzung des TK-Diensts einschränken, umleiten oder unterbinden und den Datenverkehr zu Störungsquellen einschränken. Die Bußgeldvorschriften in § 149 TKG werden an die neuen datenschutzrechtlichen Vorgaben in § 100 Abs. 1 TKG angepasst.

Mit dem jüngst vom *Bundestag* beschlossenen Umsetzungsgesetz zur EU NIS-RL wird deutlich, dass dem Thema Cybersicherheit in Deutschland auf politischer Ebene eine erhebliche Bedeutung zugemessen wird. Dies zeigt sich nicht nur anhand der Geschwindigkeit, mit der die europarechtlichen Vorgaben in nationales Recht gefasst wurden; die entsprechende Frist von Seiten der EU läuft erst am 9.5.2018 aus. Inhaltlich stellt das Umsetzungsgesetz eine konsequente Fortsetzung des IT-SiG von 2015 dar, was sich vor allem auch daran zeigt, dass der deutsche Gesetzgeber infolge der im Bereich der Cybersicherheit geleisteten Vorarbeit keine erheblichen und strukturellen Anpassungen mehr treffen muss; vielfach bleibt es auch bei rein redaktionellen Änderungen ohne materielle Auswirkungen und bei marginalen inhaltlichen Anpassungen. Dies kommt im Sinne der Rechtssicherheit vor allem auch den zurzeit mit der Umsetzung der Anforderungen befassten Unternehmen zugute. Die neuen Aufgabenfestlegungen und Datenübermittlungsbefugnisse des *BSI* verdeutlichen zudem, dass die Cybersecurity immer mehr auch verteidigungspolitische und nachrichtendienstliche Relevanz besitzt. Um das Vertrauen der Betreiber in die gesetzlich geschaffenen Strukturen aber nicht zu unterminieren, muss trotz erweiterter Datenverarbeitungsbefugnis-

se zu Zwecken der IT-Sicherheit auch ihren Interessen an Vertraulichkeit und Geheimhaltung Rechnung getragen werden – auch diesen will das Umsetzungsgesetz in einem angemessenen Rahmen Genüge tun. Ebenso wird versucht, möglichen Datenschutzbedenken, die mit einer erweiterten Datennutzung zu Zwecken der IT-Sicherheit verbunden sind, entgegenzutreten.

Die EU NIS-RL schreibt den Mitgliedstaaten vor, bis zum 9.11.2018 die Kritischen Infrastrukturen zu ermitteln, die von den gesetzlichen Cybersecurity-Verpflichtungen betroffen sind. Für Deutschland geschieht dies durch die Rechtsverordnung nach § 10 Abs. 1 BSIG, die sog. BSI-KritisV. Der erste Korb, welcher die Sektoren Energie, Wasser, Ernährung sowie Informations- und Kommunikationstechnik abdeckt, wurde am 22.4.2016 ausgefertigt, die Veröffentlichung des zweiten Korbs mit den Sektoren Transport, Verkehr, Gesundheit sowie Finanz- und Versicherungsdienstleistungen ist nach mehrmaligen Verzögerungen für Ende Mai/Anfang Juni 2017 angesetzt. Zur vereinheitlichten Bestimmung konkreter Betreiber von Kritischen Infrastrukturen nimmt die NIS-RL auf verschiedene weitere europäische Rechtsakte Bezug, sodass sich auch hier noch inhaltliche Anpassungen ergeben könnten. Da die von der NIS-RL im Rahmen der Mindestharmonisierung zwingend vorausgesetzten Sektoren aber bereits durch das IT-SiG abgebildet werden, dürften eventuelle, vereinzelte Änderungen bei der Bestimmung von Betreibern vornehmlich nur die branchenspezifischen Schwellenwerte (oder deren Aktualisierung) betreffen. Mit der Veröffentlichung des zweiten Korbs der BSI-KritisV wird das gesetzgeberische Tätigwerden in den Bereichen der nationalen und europäischen Cybersecurity-Regulierung daher zumindest vorerst abgeschlossen sein.

■ Vgl. auch *Kipker*, MMR 2017, 143; *Kipker*, ZD-Aktuell 2016, 05363 und MMR-Aktuell 2017, 389108.

Dr. Dennis-Kenji Kipker
ist Wissenschaftlicher Geschäftsführer 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“ (ITS | kritis) als bestandteil der Hightech-Strategie der Bundesregierung.