Dennis-Kenji Kipker / Mattea Stelter

Trotz Brexit: Britische Regierung plant langfristige Umsetzung der EU NIS-Richtlinie

MMR-Aktuell 2017, 394832

Die Umsetzung der Richtlinie über Maßnahmen zur Gewährleistung einer hohen gemeinsamen Netz- und Informationssicherheit in der Union (NIS-Richtlinie) ist derzeit Gegenstand des parlamentarischen Prozesses im Vereinigten Königreich. Im Rahmen einer Anhörung der Öffentlichkeit sind von der *britischen Regierung* nun detaillierte Regulierungsvorschläge veröffentlicht worden. Gerade vor dem Hintergrund des bevorstehenden „Brexit" lohnt sich ein Blick auf die konkreten Umsetzungspläne.

I. Hintergrund

Nachdem die NIS-Richtlinie im August 2016 in Kraft getreten ist, bleibt den Mitgliedstaaten noch bis zum 9.5.2018 Zeit, um die Richtlinie in nationales Recht umzusetzen. Auch die *britische Regierung* muss ungeachtet des „Brexit"-Referendums und der laufenden Verhandlungen über den Austritt aus der Europäischen Union zunächst weiterhin EU-Recht umsetzen und anwenden: Noch bis zum Ende der zweijährigen Austrittsverhandlungen im März 2019 bleibt das Vereinigte Königreich ein reguläres Mitglied der EU, sodass die sich aus der Mitgliedschaft ergebenden Rechte und Verpflichtungen bestehen bleiben. Für den Zeitpunkt des Austritts sieht das jüngst vom *britischen Unterhaus* in zweiter Lesung angenommene EU-Austrittsgesetz (EU Withdrawal Bill) vor, dass die mehr als 12.000 EU-Vorschriften vorerst in nationales Recht übertragen werden, die *Regierung* Gesetzesänderungen in der Folge aber auch ohne Beteiligung des *Parlaments* vornehmen kann. In den im August 2017 veröffentlichten Vorschlägen zur Umsetzung der NIS-Richtlinie bekräftigt die *britische Regierung* allerdings, das EU-Recht auch nach dem „Brexit" anwenden zu wollen.

So weist die *Regierung* darauf hin, dass sie die grundlegenden Ziele der NIS-Richtlinie ausdrücklich unterstütze, denn diese stünden mit den Zielvorgaben der nationalen Cyber-Sicherheitsstrategie in Einklang.

Die Umsetzung der Richtlinie soll im gesamten Vereinigten Königreich Geltung haben. I.S.v. Art. 1 Abs. 7 der Richtlinie sollen der Banken- und Finanzmarktsektor von bestimmten Aspekten ausgenommen sein, für die zum Zeitpunkt des Inkrafttretens der Umsetzungsregelungen bereits Bestimmungen existieren, die den Anforderungen der Richtlinie mindestens gleichwertig sind. Die in diesen Sektoren tätigen Unternehmen sowie die Finanzmarktinfrastruktur bleiben damit weiterhin den Vorschriften und Standards der *Bank of England* und der *britischen Finanzaufsichtsbehörde (Financial Conduct Authority)* unterworfen. Die Gesamtkosten für die Umsetzung der NIS-Richtlinie im Vereinigten Königreich wurden im Rahmen einer Folgenabschätzung auf GB£ 51 Mio. geschätzt.

II. Britische Cyber-Sicherheitsstrategie

Die Regulierungsvorschläge knüpfen an eine im November 2016 veröffentlichte nationale Cyber-Sicherheitsstrategie an, die unter den Stichworten „Defend", „Deter" und „Develop" drei wesentliche Zielvorgaben bestimmt, die bis 2021 erfüllt sein sollen. Auf diese Weise will das Vereinigte Königreich künftig auf IT-Sicherheitsvorfälle effektiv reagieren können.

Dazu sollen zum einen Netzwerke, Daten und Systeme geschützt und widerstandsfähig sein. Bürger, Unternehmen und der öffentliche Sektor sollen über die Kenntnisse und Fähigkeiten verfügen, sich selbst gegen Cyberbedrohungen zu verteidigen. Darüber hinaus soll der Staat über die Mittel verfügen, gegen Angriffe im Cyberspace offensiv vorzugehen, und Täter sollen strafrechtlich verfolgt werden. Schließlich wird das Ziel einer innovativen, wachsenden Cyber-Sicherheitsindustrie, gestützt durch eine weltweit führende wissenschaftliche Forschung, aufgestellt. Künftige Bedrohungen und Herausforderungen sollen mit Hilfe modernster Analysen und Fachkompetenzen bewältigt werden. Hinsichtlich der Abwehr von Cyberbedrohungen (Defend) bestimmt die Cyber-Sicherheitsstrategie zudem, dass die *britische Regierung* mit ihren internationalen Partnern zusammenarbeiten werde, um innerhalb Europas einen angemessenen Rechtsrahmen zu gewährleisten, der Anreize für erhöhte IT-Sicherheit schafft, aber unnötige Belastungen für Unternehmen vermeidet.

III. Identifikation der Betreiber wesentlicher Dienste

In Bezug auf die Betreiber wesentlicher Dienste, die gem. Art. 5 der Richtlinie von den Mitgliedstaaten bis zum 9.11.2018 ermittelt werden müssen, schlägt die *britische Regierung* als Kriterien zur Identifikation u.a. die folgenden Schwellenwerte vor, die grundsätzlich in allen Landesteilen gelten sollen: Im Sektor Trinkwasserversorgung werden als Betreiber wesentlicher Dienste diejenigen Betriebe angesehen, die mindestens 350.000 Menschen versorgen. Im Sektor Energie ist etwa der Schwellenwert für die Bereiche Stromübertragung, Stromverteilung und Endversorgung auf mehr als 250.000 Verbraucher festgelegt, wobei hier für Nordirland abweichende Schwellenwerte vorgeschlagen werden. Im Gesundheitswesen sollen alle Einrichtungen des staatlichen Gesundheitssystems National Health Service als Betreiber wesentlicher Dienste gelten (genannt werden die als Trusts bzw. Boards bezeichneten Organisationen des NHS in England, Wales,

Schottland und Nordirland; der Gesundheitsdienst ist in den Landesteilen jeweils unabhängig organisiert). Im Transportwesen werden u.a. Flughäfen und Flugverkehrsdienstleister an Flughäfen mit jährlich mehr als 10 Mio. Passagieren als Betreiber wesentlicher Dienste vorgeschlagen. Die Grenze von 10 Mio. Passagieren soll (neben speziellen Schwellenwerten für die Frachtschifffahrt) ebenso in der Schifffahrt zur Anwendung kommen, etwa bei Hafenbehörden und Schiffsverkehrsdiensten. Im Schienenverkehr werden u.a. alle im Bereich des nationalen Schienennetzes tätigen Betreiber umfasst (etwa Betreiber von Zügen, Schienennetzen, Bahnhöfen).

Der *Regierung* zufolge sind die Schwellenwerte dabei so angesetzt, dass nur die wichtigsten Betreiber jedes Sektors erfasst werden. Die auf diese Weise ermittelten Betreiber sollen von der jeweiligen zuständigen Behörde benachrichtigt werden.

Zudem schlägt die *britische Regierung* eine behördliche Befugnis vor, die es ermöglicht, bestimmte Betreiber auch unabhängig vom Erreichen der Schwellenwerte zu Betreibern wesentlicher Dienste ernennen zu können. So können laut *Regierung* auch bestimmte kleinere Betreiber, die diese Schwellenwerte zwar nicht erreichen, aber dennoch als Betreiber wesentlicher Dienste angesehen werden müssen, erfasst werden, ohne dass der Anwendungsbereich der Richtlinie zu sehr ausgeweitet wird. Diese Befugnis soll jedoch nur genutzt werden können, wenn die Ernennung aus Gründen der nationalen Sicherheit, wegen einer potenziellen Gefahr für die öffentliche Sicherheit oder der Möglichkeit erheblich nachteiliger sozialer oder ökonomischer Auswirkungen, ausgelöst durch einen Störfall, erfolgt. Zudem soll die Befugnis nur in Bezug auf diejenigen Betreiber genutzt werden können, die unter einen der Sektoren im Sinne der Richtlinie fallen.

Im Rahmen der Folgenabschätzung wurden seitens der *Regierung* bereits Schätzungen bzgl. der Zahl der von der Umsetzung der Richtlinienbestimmungen betroffenen Einrichtungen und Unternehmen veröffentlicht. So könnten im Sektor Trinkwasserversorgung 19 Unternehmen bzw. staatliche Versorger unter die Bestimmungen für Betreiber wesentlicher Dienste fallen. Im Sektor Digitale Infrastruktur ist von sechs, im Sektor Energie von 51 und im Transportwesen von 79 Betreibern wesentlicher Dienste die Rede. Im Gesundheitssektor wären alle 243 NHS-Trusts betroffen.

IV. Nationaler Rahmen

In Art. 7-10 schreibt die NIS-Richtlinie einen umfassenden nationalen Ordnungsrahmen zur IT-Sicherheit vor, der die Festlegung einer nationalen Strategie zur Netz- und Informationssicherheit, die Benennung einer oder mehrerer national zuständigen Behörden, die Benennung einer zentralen Anlaufstelle sowie die Einrichtung von CSIRTs umfasst. In diesem Zusammenhang schlägt die *britische Regierung* als nationale Strategie i.S.v. Art. 7 der Richtlinie die vorhandene Cyber-Sicherheitsstrategie vom November 2016 vor. In dieser Strategie seien die Anforderungen der Richtlinie größtenteils bereits thematisiert, für darüber hinausgehende, spezielle Anforderungen der Richtlinie soll die Strategie ergänzt werden.

Bzgl. der Ernennung zuständiger Behörden gem. Art. 8 der Richtlinie spricht sich die *Regierung* für sektorspezifische Behörden aus. In den Regulierungsvorschlägen wird hierzu umfassend erläutert, dass der Ansatz, dezentral nicht nur eine, sondern mehrere zuständige Behörden zu ernennen, den Vorteil habe, dass durch sektorspezifische Expertise die individuellen Herausforderungen einzelner Sektoren besser gemeistert werden könnten.

Die ernannten Behörden sollen durch das 2016 als Teil des Geheimdienstes *GCHQ* gegründete *National Cyber Security Centre (NCSC)* Unterstützung erhalten, die Verantwortlichkeit solle letztlich jedoch allein bei der jeweiligen zuständigen Behörde liegen.

Innerhalb Großbritanniens sollen die Zuständigkeiten für einige Sektoren in den drei Landesteilen einheitlich geregelt werden. Die zuständigen Behörden in Nordirland sind derzeit noch Gegenstand der Diskussion, daher wurden für Nordirland noch keine konkreten Vorschläge veröffentlicht. Im Sektor Energie wird für England, Schottland und Wales das *Ministerium für Wirtschaft, Energie und Industriestrategie (BEIS)* als zuständige Behörde vorgeschlagen, wobei noch geprüft wird, ob für den Bereich Elektrizität und Gas (Downstream) bestimmte Aufgaben an die Aufsichtsbehörde *Ofgem (Office of Gas and Electricity Markets)* übertragen werden können. Für die übrigen Teilsektoren wird ebenfalls die Einbeziehung entsprechender Einrichtungen in Erwägung gezogen. Im Sektor Digitale Infrastruktur soll in allen Landesteilen Großbritanniens die Aufsichtsbehörde *Ofcom (Office of Communications)* zuständige Behörde sein. Im Transportwesen soll in Großbritannien überwiegend (mit abweichenden Zuständigkeiten für Schottland und Wales im Teilsektor Straßenverkehr) das *Ministerium für Transport (DfT)* zuständig sein, im Bereich Luftfahrt sollen dabei bestimmte Aufgaben der Zivilluftfahrtbehörde *CAA (Civil Aviation Authority)* zukommen. Für die Anbieter digitaler Dienste soll die Zuständigkeit ausschließlich bei der britischen Datenschutzbehörde *ICO (Information Commissioner's Office)* liegen, die keinem Ministerium untersteht, jedoch vom *Ministerium für Digitales, Kultur, Medien und Sport* gefördert wird. In den Sektoren Trinkwasserversorgung und Gesundheit wird zwischen England, Wales und Schottland differenziert: So sind für England das *Ministerium für Umwelt, Ernährung und Angelegenheiten des ländlichen Raums (Defra)* bzw. das *Gesundheitsministerium (DH)* als zuständige Behörden vorgesehen, wobei im Bereich Gesundheit einige Aufgaben an *NHS Digital* übertragen werden sollen. Für Wales nehmen diese Rolle wohl die *Kabinettsminister für Umwelt und Angelegenheiten des ländlichen Raums* (*Cabinet Secretary for Environment and Rural Affairs*) sowie für *Gesundheit, Wohlbefinden und Sport* (*Cabinet Secretary for Health, Well-being and Sport*) wahr. Bzgl. der Zuständigkeiten in Schottland finden zurzeit noch Beratungen mit der *schottischen Regierung* statt.

Als zentrale Anlaufstelle i.S.v. Art. 8 der Richtlinie schlägt die *Regierung* das *NCSC* vor. Auch bei der Benennung der Computer Security Incident Response Teams (CSIRTs) gem. Art. 9 der Richtlinie fällt die Wahl auf das *NCSC*. Diese Rolle ist für die Behörde nicht neu, schon das bestehende Computer-Notfallteam *CERT UK* ist seit 2016 in das *NCSC* integriert. Um bereits existierende Meldesysteme einbeziehen zu können, soll das *NCSC* die Möglichkeit haben, Aufgaben an bestehende CERTs (etwa bei *NHS Digital*) zu übertragen.

V. Sicherheitsanforderungen und Meldepflichten für Betreiber wesentlicher Dienste

Gem. Art. 14 der Richtlinie müssen die Mitgliedstaaten sicherstellen, dass die Betreiber wesentlicher Dienste geeignete und verhältnismäßige technische und organisatorische Maßnahmen ergreifen, um Bedrohungen der IT-Sicherheit entgegenzuwirken. Dies möchte die *britische Regierung* mit Hilfe von sog. „high level security principles" gewährleisten, die durch umfangreiche Orientierungshilfen (guidance) komplettiert werden sollen.

Die Sicherheitsgrundsätze beschreiben die von den Betreibern zwingend zu erzielenden Sicherheitserfolge; sie wurden durch das *NCSC* in Zusammenarbeit mit Ministerien und zuständigen Behörden bestimmt und anlässlich der Anhörung der Öffentlichkeit bereits veröffentlicht. Die weiteren Orientierungshilfen, allgemeingültiger wie auch sektorspezifischer Natur, sollen im Laufe der Zeit durch das *NCSC* und die zuständigen Behörden bekanntgemacht und fortwährend aktualisiert werden. Dazu sieht die *Regierung* den folgenden Zeitrahmen vor: Die sektorübergreifenden Orientierungshilfen werden im Januar 2018 veröffentlicht, anschließend sollen im Frühjahr 2018 die zuständigen Behörden signalisieren, wie diese Orientierungshilfen von den Betreibern auszulegen sind. Schließlich ist für November 2018 geplant, dass die zuständigen Behörden in Abstimmung mit den Betreibern und dem *NCSC* weitere, auf den jeweiligen Sektor zugeschnittene Orientierungshilfen vorlegen. Insgesamt wird diesbezüglich eine gemeinschaftliche, proaktive Herangehensweise von Behörden und Betreibern beabsichtigt.

Die Betreiber sind bereits ab dem Zeitpunkt des Inkrafttretens der Umsetzungsregelungen am 10.5.2018 verpflichtet, die Sicherheitsgrundsätze einzuhalten. Aufgabe der zuständigen Behörden ist es, zu prüfen, ob die Betreiber hinreichende Maßnahmen getroffen haben, anderenfalls können die Behörden den Betreibern verbindliche Anweisungen erteilen.

In Bezug auf die Meldepflichten von Betreibern legen die vorgeschlagenen Umsetzungsregelungen fest, wie ein meldepflichtiger Sicherheitsvorfall definiert ist, welche Schwellenwerte gelten, um zu bestimmen, ob ein Vorfall mit erheblichen Auswirkungen vorliegt, und in welchem Zeitfenster ein Vorfall gemeldet werden muss. So handelt es sich laut Definition der *Regierung* dann um einen Sicherheitsvorfall mit Auswirkungen auf die Verfügbarkeit, wenn es zu einem Ausfall, einer Einschränkung oder einer Beeinträchtigung des Dienstes kommt. Betreiber sollen darüber hinaus ermutigt werden, freiwillige Meldungen abzugeben, z.B. wenn Malware gefunden wurde, die potenziell geeignet ist, eine Störung des Dienstes hervorzurufen. Hinsichtlich einer Definition, wann ein Vorfall mit erheblichen Auswirkungen vorliegt, werden in den Anhörungsdokumenten seitens der *Regierung* noch keine Angaben zu konkreten Schwellenwerten gemacht. Hierzu heißt es, diese Schwellenwerte seien von Sektor zu Sektor verschieden und würden nach Ende der Anhörung durch die zuständigen Behörden in Abstimmung mit Betreibern und dem *NSCS* bestimmt werden. Die *Regierung* schlägt ferner vor, dass die Meldungen ohne schuldhafte Verzögerung und so schnell wie möglich erfolgen müssten, das maximale Zeitfenster betrage 72 Stunden nach Kenntnis des Vorfalls.

Um die Belastungen für Betreiber gering zu halten, sollen die sich aus der Richtlinie ergebenden Anforderungen mit den in vielen Sektoren bereits seit Jahren bestehenden Vereinbarungen zur Meldung von Sicherheitsvorfällen abgestimmt werden. Zudem sollen zwecks geringeren bürokratischen Aufwands alle Meldungen an das *NCSC* (in Funktion des CSIRT) erfolgen, das die Meldungen anschließend an die jeweils zuständige Behörde weitergeben muss.

VI. Anbieter digitaler Dienste

Der Ansatz der *Regierung*, IT-Sicherheitsanforderungen an Betreiber in Form von „principles and guidance" festzulegen, soll in gleicher Weise auch für die Anbieter digitaler Dienste gem. Art. 16 der Richtlinie Anwendung finden. Diesbezüglich gibt die *britische Regierung* an, dass die noch ausstehende Rahmensetzung durch die *EU-Kommission* abzuwarten sei. Die daher noch festzulegenden Sicherheitsgrundsätze für Anbieter digitaler Dienste sollen sich maßgeblich an den Vorgaben der *Kommission* sowie den Bestimmungen der DS-GVO orientieren. Die Orientierungshilfen wiederum sollen eng an die Leitlinien der *European Network and Information Security Agency (ENISA)* angelehnt sein, denn schließlich, so heißt es, werde die Erfüllung europäischer Leitlinien künftig Bedingung für den Zugang zum europäischen Binnenmarkt sein. In puncto Meldepflichten beabsichtigt die *Regierung* ebenfalls, den für die Betreiber wesentlicher Dienste vorgeschlagenen Ansatz zu übernehmen. Auch hier sollen die Meldepflichten in Einklang mit denen der DS-GVO stehen, um zusätzliche Belastungen der Unternehmen zu vermeiden. Zu den digitalen Diensten gehören gem. der NIS-Richtlinie Online-Suchmaschinen, Online-Marktplätze und Cloud Computing-Dienste. Unternehmen mit weniger als 50 Mitarbeitern und einem Jahresumsatz/einer Jahresbilanz von höchstens GB£ 10 Mio. sind vom Anwendungsbereich der Richtlinie ausgenommen. Im Rahmen der Folgenabschätzung geht die *britische Regierung* davon aus, dass es gegenwärtig keine im Vereinigten Königreich ansässigen Online-Suchmaschinenanbieter gibt, die unter die genannten Schwellenwerte fallen. Dagegen wurden zwei Anbieter von Online-Marktplätzen ausfindig gemacht, die betroffenen Cloud Computing-Dienste werden mit 169 beziffert.

VII. Fazit

Die veröffentlichten Regulierungsansätze zeigen, dass die *britische Regierung* der Sicherheit informationstechnischer Systeme große Bedeutung beimisst. Eine tragende Rolle, etwa als zentrale Anlaufstelle und CSIRT, kommt in den Plänen zur Umsetzung der EU NIS-Richtlinie dem *National Cyber Security Centre* zu. Bemerkenswert ist jedoch, dass die *Regierung* bei der Benennung der zuständigen Behörden indes nicht allein auf das *NCSC* zurückgreift, sondern einen dezentralen Ansatz verfolgt. Dies hat zweifelsohne den Vorteil sektorspezifischer Kenntnisse bei den einzelnen Behörden, dürfte aber einige Herausforderungen mit sich bringen: So muss einerseits das *NCSC* künftig gleich mit einer Vielzahl zuständiger Behörden zusammenarbeiten und die entsprechenden Kommunikationsstrukturen schaffen. Andererseits könnte auch für die jeweils zuständigen Behörden ein hoher Aufwand entstehen, weil sichergestellt werden muss, dass die im Hinblick auf die Cybersicherheit zumeist „fachfremden" Behörden über ausreichend IT-Expertise verfügen.

In der Gesamtbetrachtung ist zu begrüßen, dass das Vereinigte Königreich mit der Umsetzung der NIS-Richtlinie nicht nur seinen Pflichten als Noch-Mitglied der EU nachkommen will, sondern die *Regierung* vielmehr die Ziele der Richtlinie mitträgt und die neuen Regelungen auch nach dem EU-Austritt im März 2019 Bestand haben sollen. Deutlich wird damit zugleich auch die hohe und transnational impulsgebende Qualität der europäischen Vorgaben im Bereich der Cybersicherheit. Schlussendlich ist zu hoffen, dass auch das Vereinigte Königreich weiterhin zu dem mit der NIS-Richtlinie verfolgten Ziel eines hohen Niveaus der IT-Sicherheit in Europa beiträgt und dass die mit den Richtlinienbestimmungen, etwa zur Einrichtung einer Kooperationsgruppe sowie eines CSIRTS-Netzwerks, nunmehr gefestigte europäische Zusammenarbeit in Fragen der IT-Sicherheit angesichts des „Brexit" nicht geschwächt wird.

■ Vgl. auch *Kipker*, MMR-Aktuell 2017, 394677; *Gierschmann*, MMR 2016, 501; *Kipker*, MMR-Aktuell 2017, 389121; *ders.*, MMR 2017, 143; *ders.*, ZD-Aktuell 2016, 05363; MMR-Aktuell 2017, 394324; *Roth*, ZD 2015, 17 und *Rockstroh/Kunkel*, MMR 2017, 77.

Dr. Dennis-Kenji Kipker
ist Wissenschaftlicher Geschäftsführer des Instituts für Informations-, Gesundheits- und Medizinrecht (IGMR) an der Universität Bremen, Projektmanager beim Verband der Elektrotechnik, Elektronik und Informationstechnik (VDE) e.V. in Frankfurt/M., Abteilung CERT@VDE, und Mitglied des Vorstands der Europäischen Akademie für Informationsfreiheit und Datenschutz (EAID) in Berlin.

Mattea Stelter
ist Wissenschaftliche Mitarbeiterin am Institut für Informations-, Gesundheits- und Medizinrecht (IGMR) an der Universität Bremen, Forschungsprojekt „Vernetzte IT-Sicherheit für Kritische Infrastrukturen" (VeSiKi).