EUROPÄISCHE
KOMMISSION

Brüssel, den 4.10.2017
COM(2017) 476 final

ANNEX 1

NOTE
This language version reflects the corrections done to the original EN version transmitted under COM(2017) 476 final of 13.9.2017 and retransmitted (with corrections) under COM(2017) 476 final/2 of 4.10.2017

ANHANG

der

MITTEILUNG DER KOMMISSION AN DAS EUROÄISCHE PARLAMENT UND DEN RAT

Bestmögliche Netz- und Informationssicherheit - hin zu einer wirksamen Umsetzung der Richtlinie (EU) 2016/1148 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union

DE

INHALTSVERZEICHNIS

ANLAGE

1. Einführung

Dieser Anhang soll zu einer wirksamen Anwendung, Umsetzung und Durchsetzung der Richtlinie (EU) 2016/1148 über die Sicherheit von Netz- und Informationssystemen in der Union[1] (im Folgenden die „NIS-Richtlinie“ oder die „Richtlinie“) beitragen und den Mitgliedstaaten helfen, für eine wirksame Anwendung der EU-Rechtsvorschriften zu sorgen. Insbesondere werden drei Ziele verfolgt: a) mehr Klarheit für die nationalen Behörden hinsichtlich der Verpflichtungen, die sich für sie aus der Richtlinie ergeben, b) Gewährleistung der wirksamen Durchsetzung der Verpflichtungen gemäß der Richtlinie, die für Einrichtungen gelten, die Anforderungen in Bezug auf die Sicherheit und die Meldung von Sicherheitsvorfällen erfüllen müssen, und c) Beitrag zur Rechtssicherheit für alle relevanten Akteure.

Zu diesem Zweck enthält dieser Anhang Leitlinien zu folgenden Aspekten, die von entscheidender Bedeutung für das Erreichen des Ziels der NIS-Richtlinie sind, d. h. zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der EU, die für das Funktionieren unserer Gesellschaften und Volkswirtschaften unverzichtbar sind, darunter:

- die Verpflichtung der Mitgliedstaaten zur Festlegung einer nationalen Strategie für die Sicherheit von Netz- und Informationssystemen (Abschnitt 2);
- die Einrichtung von zuständigen nationalen Behörden, zentralen Anlaufstellen und Computer-Notfallteams (Computer Security Incident Response Teams, CSIRTs) (Abschnitt 3);
- die Anforderungen in Bezug auf die Sicherheit und die Meldung von Sicherheitsvorfällen, die für Betreiber wesentlicher Dienste und die Anbieter digitaler Dienste gelten (Abschnitt 4) und
- das Verhältnis zwischen der NIS-Richtlinie und anderen Rechtsvorschriften (Abschnitt 5).

Zur Vorbereitung dieser Leitlinien hat die Kommission während der Ausarbeitung der Richtlinie Beiträge und Analysen gesammelt, u. a. Beiträge der Europäischen Agentur für Netz- und Informationssicherheit („ENISA“) und der Kooperationsgruppe. Außerdem flossen Erfahrungen aus bestimmten Mitgliedstaaten ein. Wo angebracht, hat sich die Kommission auf die für die Auslegung des EU-Rechts relevanten Grundsätze gestützt, d. h. auf den Wortlaut, den Kontext und die Ziele der NIS-Richtlinie. Da die Richtlinie bisher nicht umgesetzt worden ist, liegen zum jetzigen Zeitpunkt weder Urteile des Gerichtshofs der

[1] 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. Die Richtlinie trat am 8. August 2016 in Kraft.

Europäischen Union (EuGH) noch der nationalen Gerichte vor. Aus diesem Grund ist es nicht möglich, sich an der Rechtsprechung zu orientieren.

Die Zusammenstellung dieser Informationen in einem einzigen Dokument kann den Mitgliedstaaten einen guten Überblick über die Richtlinie liefern und es ihnen ermöglichen, diese Informationen bei der Ausarbeitung ihrer nationalen Rechtsvorschriften zu berücksichtigen. Gleichzeitig hebt die Kommission hervor, dass dieser Anhang nicht bindend ist und mit ihm keine neuen Vorschriften geschaffen werden sollen. Die Zuständigkeit für die Auslegung des EU-Rechts liegt letztendlich beim EuGH.

2. Nationale Strategie für die Sicherheit von Netz- und Informationssystemen

Gemäß Artikel 7 der NIS-Richtlinie sind die Mitgliedstaaten verpflichtet, eine nationale Strategie für die Sicherheit ihrer Netz- und Informationssysteme festzulegen, die einer nationalen Cybersicherheitsstrategie (*National Cyber Security Strategy*, NCSS) gleichzusetzen ist. Eine nationale Strategie dient zur Festlegung der strategischen Ziele sowie angemessener politischer und rechtlicher Maßnahmen in Bezug auf die Cybersicherheit. Der Begriff der nationalen Cybersicherheitsstrategie ist sowohl weltweit als auch in Europa weit verbreitet, insbesondere im Zusammenhang mit der Beteiligung der ENISA an der Ausarbeitung der nationalen Strategien der Mitgliedstaaten, aus der vor kurzem ein aktualisierter Leitfaden für bewährte Verfahren im Bereich der NCSS[2] hervorging.

In diesem Abschnitt legt die Kommission dar, wie die NIS-Richtlinie die Abwehrbereitschaft der Mitgliedstaaten erhöht, indem sie ihnen auferlegt, solide nationale Strategien für die Sicherheit ihrer Netz- und Informationssystemen festzulegen (Artikel 7). Dieser Abschnitt befasst sich mit den folgenden Aspekten: a) Anwendungsbereich der Strategie und b) Inhalt sowie Verfahren zur Festlegung.

Wie im Folgenden näher beschrieben, ist die ordnungsgemäße Umsetzung des Artikels 7 der NIS-Richtlinie von entscheidender Bedeutung für die Verwirklichung der Ziele der Richtlinie und sie erfordert hierzu eine angemessene finanzielle und personelle Ausstattung.

2.1. Anwendungsbereich der nationalen Strategie

Nach dem Wortlaut von Artikel 7 gilt die Verpflichtung zur Festlegung einer NCSS ausschließlich für die in Anhang II genannten Sektoren (z. B. Energie, Verkehr, Bankwesen, Finanzmarktinfrastrukturen, Gesundheitswesen, Trinkwasserlieferung und -versorgung sowie digitale Infrastruktur) und die in Anhang III genannten Dienste (Online-Marktplatz, Online-Suchmaschinen und Cloud-Computing-Dienst).

In Artikel 3 der Richtlinie ist ausdrücklich der Grundsatz der Mindestharmonisierung festgelegt, dem zufolge die Mitgliedstaaten Bestimmungen erlassen oder aufrechterhalten können, mit denen ein höheres Sicherheitsniveau von Netz- und Informationssystemen

[2] ENISA, *National Cyber-Security Strategy Good Practice* 2016. Abrufbar unter https://www.enisa.europa.eu/publications/ncss-good-practice-guide.

erreicht werden soll. Die Anwendung dieses Grundsatzes auf die Verpflichtung zur Festlegung einer NCSS ermöglicht es den Mitgliedstaaten, weitere Sektoren als die in Anhang II und Anhang III der Richtlinie genannten einzubeziehen.

Nach Auffassung der Kommission und angesichts des Ziels der NIS-Richtlinie, d. h. der Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union[3], wäre es ratsam, eine nationale Strategie zu entwickeln, die alle relevanten Dimensionen der Gesellschaft und der Wirtschaft umfasst und nicht nur die in den Anhängen II und III der NIS-Richtlinie genannten Sektoren bzw. digitalen Dienste. Dies steht in Einklang mit auf internationaler Ebene bewährten Verfahren (siehe die im Folgenden genannten ITU-Leitlinien und Analyse der OECD) und der NIS-Richtlinie.

Wie nachstehend näher erläutert, gilt dies insbesondere für öffentliche Verwaltungen, die für andere Sektoren und Dienste als die in den Anhängen II und III der Richtlinie aufgeführten zuständig sind. Öffentliche Verwaltungen verarbeiten möglicherweise sensible Informationen, die die Abdeckung durch eine NCSS und Managementpläne zur Verhinderung der Informationsweitergabe sowie zur Gewährleistung eines angemessenen Schutzes dieser Informationen erforderlich machen.

2.2. Inhalt und Verfahren zur Festlegung der nationalen Strategien

Gemäß Artikel 7 der NIS-Richtlinie muss eine NCSS mindestens folgende Aspekte behandeln:

i) die Ziele und Prioritäten der nationalen Strategie für die Sicherheit von Netz- und Informationssystemen;
ii) einen Steuerungsrahmen zur Erreichung der Ziele und Prioritäten der nationalen Strategie;
iii) die Bestimmung von Maßnahmen zur Abwehrbereitschaft, Reaktion und Wiederherstellung, einschließlich der Zusammenarbeit zwischen dem öffentlichen und dem privaten Sektor;
iv) die Aufstellung der einschlägigen Ausbildungs-, Aufklärungs- und Schulungsprogramme;
v) eine Angabe der Forschungs- und Entwicklungspläne;
vi) einen Risikobewertungsplan zur Bestimmung von Risiken sowie
vii) eine Liste der Akteure, die an der Umsetzung der Strategie beteiligt sind.

Weder Artikel 7 noch der entsprechende Erwägungsgrund 29 enthalten Anforderungen für die Festlegung einer NCSS oder liefern nähere Informationen zum Inhalt der NCSS. Im Hinblick auf das Verfahren sowie zusätzliche Elemente im Zusammenhang mit dem Inhalt der NCSS ist die Kommission der Auffassung, dass das nachstehend erläuterte Vorgehen eine angemessene Möglichkeit zur Festlegung einer NCSS darstellt. Dies beruht auf der Analyse der Erfahrungen von Mitgliedstaaten und von Drittstaaten bei der Entwicklung ihrer eigenen

[3] Siehe Artikel 1 Absatz 1.

Strategien. Eine weitere Informationsquelle ist das NCSS-Schulungsinstrument der ENISA, das in Form von herunterladbaren Videos auf der ENISA-Website zur Verfügung steht.[4]

2.3. Verfahren und zu behandelnde Fragen

Das Verfahren zur Ausarbeitung und anschließenden Festlegung einer nationalen Strategie ist komplex und vielschichtig; es erfordert eine fortgesetzte Zusammenarbeit mit Experten in Sachen Cybersicherheit, Zivilgesellschaft und nationale politische Prozesse, wenn die Strategie wirksam und erfolgreich sein soll. Unerlässliche Bedingungen sind die höhere administrative Unterstützung mindestens auf Ebene des Staatssekretärs oder einer gleichwertigen Position im federführenden Ministerium sowie die politische Unterstützung. Zur erfolgreichen Festlegung einer NCSS kann ein fünfstufiges Verfahren (siehe Abbildung 1) in Betracht gezogen werden:

Schritt 1 – **Festlegung von Leitprinzipien und strategischen Zielen der Strategie**

Zunächst sollten die zuständigen nationalen Behörden einige zentrale Elemente der NCSS festlegen: welche Ergebnisse – nach dem Wortlaut der Richtlinie (Artikel 7 Absatz 1 Buchstabe a) die *„Ziele und Prioritäten"* – werden angestrebt, wie ergänzen diese Ergebnisse die nationalen sozial- und wirtschaftspolitischen Maßnahmen und stehen sie mit den Rechten und Pflichten eines Mitgliedstaats der Europäischen Union im Einklang? Die Ziele sollten spezifisch, messbar, erreichbar, realistisch und zeitgebunden (SMART: *specific, measurable, achievable, realistic and time-bound*) sein. Hier ein anschauliches Beispiel: *„Wir werden dafür sorgen, dass diese [zeitgebundene] Strategie auf strengen und umfassenden Parametern beruht, anhand derer wir die Fortschritte hin zu den zu erzielenden Ergebnissen messen."*[5]

Die genannten Elemente umfassen auch eine politische Bewertung dazu, ob Mittel in nennenswertem Umfang für die Umsetzung der Strategie zur Verfügung gestellt werden können. Des Weiteren beinhalten sie eine Beschreibung des geplanten Anwendungsbereichs der Strategie und der verschiedenen Kategorien von Interessenträgern aus dem öffentlichen und dem privaten Sektor, die in die Ausarbeitung der verschiedenen Ziele und Maßnahmen einbezogen werden sollten.

Dieser erste Schritt könnte durch gezielte Workshops mit leitenden Ministerialbeamten und Politikern erreicht werden, die von Fachleuten im Bereich der Cybersicherheit mit professionellen Kommunikationsfähigkeiten moderiert werden, die die Auswirkungen von nicht vorhandener oder unzureichender Cybersicherheit auf die moderne digitale Wirtschaft und Gesellschaft aufzeigen können.

Schritt 2 – **Entwicklung des Inhalts der Strategie**

Die Strategie sollte unterstützende Maßnahmen, zeitgebundene Aktionen und wichtige Leistungsindikatoren zur anschließenden Bewertung, Verfeinerung und Verbesserung nach

[4] https://www.enisa.europa.eu/topics/national-cyber-security-strategies/national-cyber-security-strategies-training-tool

[5] Auszug aus der nationalen Cybersicherheitsstrategie des Vereinigten Königreichs, 2016–2021, S. 67.

Ablauf eines bestimmten Umsetzungszeitraums enthalten. Diese Maßnahmen sollten zu den als Leitprinzipien festgelegten Zielen, Prioritäten und Ergebnissen beitragen. Die Notwendigkeit von unterstützenden Maßnahmen ist in Artikel 7 Absatz 1 Buchstabe c der NIS-Richtlinie dargelegt.

Es wird empfohlen, einen Lenkungsausschuss unter dem Vorsitz des Ministeriums einzusetzen, um die Ausarbeitung zu steuern und die Mitwirkung zu erleichtern. Dies könnte durch eine Reihe von Redaktionsgruppen aus zuständigen Beamten und Fachleuten zu wesentlichen allgemeinen Themen, z. B. Risikobewertung, Notfallplanung, Management von Sicherheitsvorfällen, Kompetenzentwicklung, Sensibilisierung, Forschung und industrielle Entwicklung usw., erreicht werden. Ferner würde jeder einzelne Sektor (z. B. Energie, Verkehr usw.) gesondert aufgefordert, die Auswirkungen seiner Einbeziehung zu bewerten (u. a. auf die Ressourcen) und die benannten Betreiber wesentlicher Dienste und wichtigsten Anbieter digitaler Dienste in die Festlegung der Prioritäten und der Vorlage von Vorschlägen im Rahmen des Ausarbeitungsverfahrens einzubinden. Die Beteiligung der Interessenträger aus den Sektoren ist auch im Hinblick auf die Notwendigkeit, für eine einheitliche Umsetzung der Richtlinie in den verschiedenen Sektoren zu sorgen und gleichzeitig ihre Besonderheiten zu berücksichtigen, von grundlegender Bedeutung.

Schritt 3 – **Entwicklung eines Steuerungsrahmens**

Um effizient und wirksam zu sein, sollte sich der Steuerungsrahmen auf die wichtigsten Interessenträger, die im Ausarbeitungsverfahren festgelegten Prioritäten sowie die Beschränkungen und den Rahmen der nationalen administrativen und politischen Strukturen stützen. Eine direkte Berichterstattung an die politische Ebene mit Entscheidungs- und Ressourcenzuweisungsbefugnis aufseiten des Steuerungsrahmens wäre ebenso wünschenswert wie die Mitwirkung von Experten in Sachen Cybersicherheit sowie von Interessenträgern aus der Industrie. Artikel 7 Absatz 1 Buchstabe b der NIS-Richtlinie enthält einen Verweis auf den Steuerungsrahmen und setzt ausdrücklich die *„Aufgaben und Zuständigkeiten der staatlichen Stellen und der anderen einschlägigen Akteure“* voraus.

Schritt 4 – **Zusammenstellung und Überprüfung des Strategieentwurfs**

In dieser Phase sollte der Strategieentwurf zusammengestellt und unter Nutzung einer Analyse der Stärken, Schwächen, Chancen und Risiken (SWOT-Analyse) geprüft werden, wodurch bestimmt werden könnte, ob eine Überarbeitung des Inhalts erforderlich wäre. Im Anschluss an die interne Überprüfung sollten die Interessenträger konsultiert werden. Außerdem wäre es wichtig, eine öffentliche Konsultation durchzuführen, um der Öffentlichkeit die Bedeutung der vorgeschlagenen Strategie zu vermitteln, Beiträge aus allen möglichen Quellen zu sammeln und finanzielle Unterstützung, die danach zur Umsetzung der Strategie benötigt wird, zu erlangen.

Schritt 5 – **Förmliche Festlegung**

Dieser letzte Schritt umfasst die förmliche Festlegung auf politischer Ebene mit einer Mittelausstattung, die die Bedeutung spiegelt, die der betreffende Mitgliedstaat der Cybersicherheit beimisst. Zur Erreichung der Ziele der NIS-Richtlinie und durch die Verpflichtung zur Mitteilung der Strategie an die Kommission gemäß Artikel 7 Absatz 3 hält die Kommission die Mitgliedstaaten dazu an, Informationen über die Mittelausstattung vorzulegen. Verpflichtungen in Bezug auf die Mittelausstattung und ausreichende personelle Ressourcen sind für eine wirksame Umsetzung der Strategie und der Richtlinie mit am wichtigsten. Da es sich bei der Cybersicherheit nach wie vor um einen relativ neuen und rasch wachsenden Bereich der Politik handelt, sind in den meisten Fällen neue Investitionen erforderlich, auch wenn die Gesamtsituation der öffentlichen Finanzen Kürzungen und Einsparungen verlangt.

Hinweise zum Verfahren für nationale Strategien und zu ihrem Inhalt geben verschiedene öffentliche und wissenschaftliche Quellen, z. B. ENISA[6], die ITU[7], die OECD[8], das globale Forum für Cyber-Fachwissen (Global Forum on Cyber Expertise, GFCE) und die Universität Oxford[9].

2.4. Konkrete von den Mitgliedstaaten vor der Umsetzungsfrist zu ergreifende Maßnahmen

Vor der Annahme der Richtlinie hatten fast alle Mitgliedstaaten[10] bereits als NCSS bezeichnete Dokumente veröffentlicht. In Abschnitt 6 dieses Anhangs sind die aktuellen Strategien der einzelnen Mitgliedstaaten aufgeführt.[11] Sie umfassen in der Regel strategische Grundsätze, Leitlinien, Ziele und in manchen Fällen spezifische Maßnahmen zur Begrenzung der Risiken im Zusammenhang mit der Cybersicherheit.

Da einige dieser Strategien vor der Verabschiedung der NIS-Richtlinie festgelegt wurden, enthalten sie möglicherweise nicht unbedingt alle Elemente gemäß Artikel 7. Um eine ordnungsgemäße Umsetzung zu gewährleisten, müssen die Mitgliedstaaten eine

---

[6] ENISA, *National Cyber-Security Strategy Good Practice* (Leitfaden für bewährte Verfahren im Bereich der NCSS, 2016). Abrufbar unter https://www.enisa.europa.eu/publications/ncss-good-practice-guide.

[7] ITU, *National Cybersecurity Strategy Guide* (Leitfaden für nationale Cybersicherheitsstrategien, 2011). Abrufbar unter: http://www.itu.int/ITU-D/cyb/cybersecurity/docs/ITUNationalCybersecurityStrategyGuide.pdf Außerdem plant die ITU im Jahr 2017 ein Instrument für nationale Cybersicherheitsstrategien *(National Cyber Security Strategy Toolkit)* herauszugeben (siehe Präsentation: http://www.itu.int/en/ITU-D/Cybersecurity/Documents/National%20Strategy%20Toolkit%20introduction.pdf)

[8] OECD, *Cybersecurity Policy Making at a Turning Point: Analysing a New Generation of National Cybersecurity Strategies* (Politikgestaltung im Bereich Cybersicherheit am Scheideweg: Analyse einer neuen Generation nationaler Cybersicherheitsstrategien, 2012). Abrufbar unter: http://www.oecd.org/sti/ieconomy/cybersecurity%20policy%20making.pdf

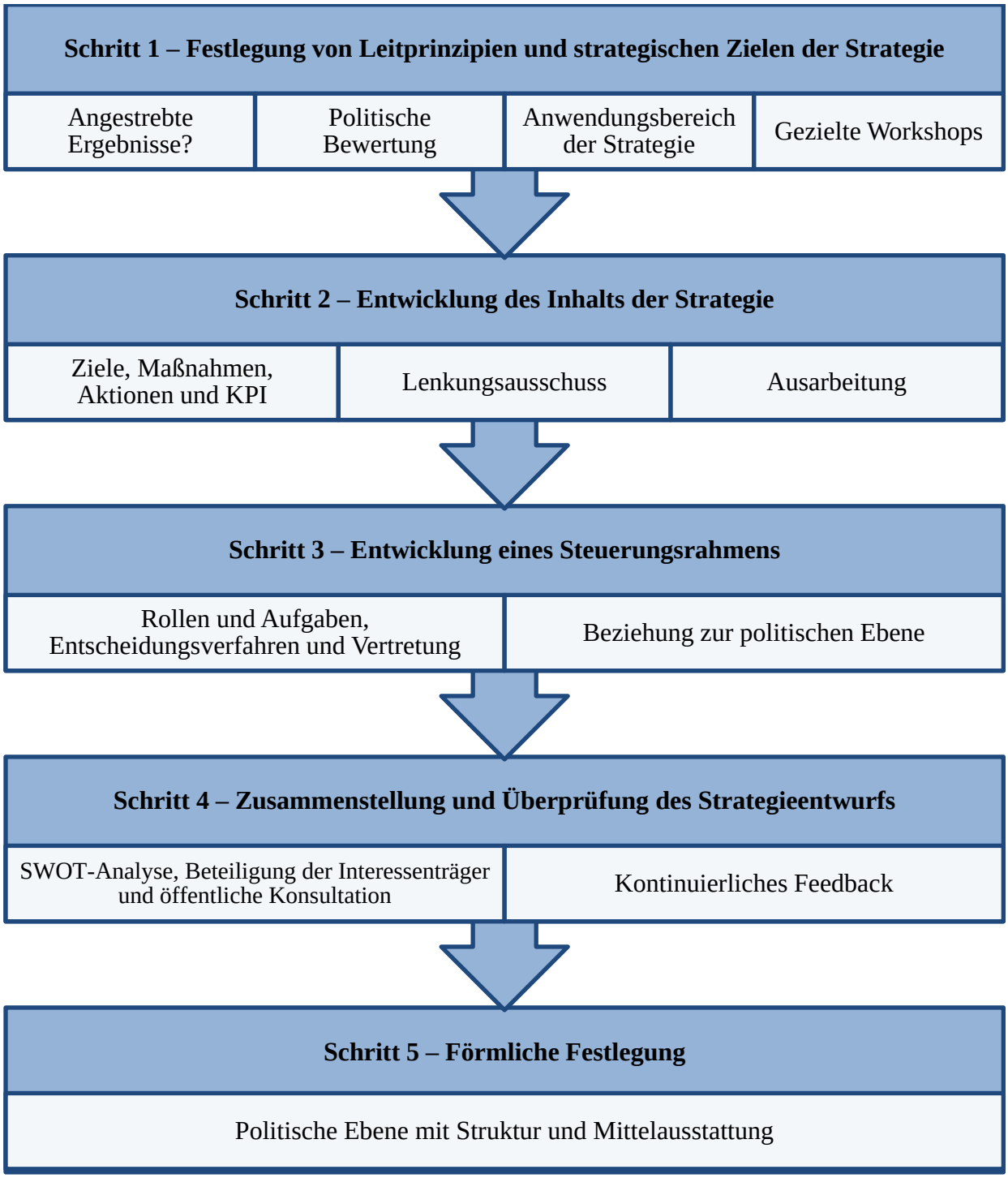
[9] Globale Cyber Security Capacity Centre und Universität Oxford, *Cybersecurity Capacity Maturity Model for Nations (CMM) - Revised Edition* (Reifegradmodell der Cybersicherheit für Staaten – überarbeitete Ausgabe, 2016). Abrufbar unter: https://www.thegfce.com/binaries/gfce/documents/publications/2017/02/13/cybersecurity-cmm-for-nations/CMM+revised+edition.pdf

[10] Abgesehen von Griechenland, wo eine nationale Cybersicherheitsstrategie seit 2014 in Vorbereitung ist (siehe https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/strategies/national-cyber-security-strategy-greece/view).

[11] Diese Informationen beruhen auf dem von der ENISA bereitgestellten Überblick über die NCSS (https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map).

Lückenanalyse erstellen, indem sie die Inhalte ihrer NCSS anhand der sieben Anforderungen in Artikel 7 für den Anwendungsbereich der in Anhang II bzw. Anhang III der Richtlinie aufgeführten Sektoren bzw. Dienste aufgliedern. Festgestellte Lücken können dann im Rahmen einer Überarbeitung ihrer bestehenden NCSS gefüllt werden oder es kann eine vollständige Überprüfung der Grundsätze ihrer nationalen NIS-Strategie von Grund auf beschlossen werden. Die vorangehenden Leitlinien für das Verfahren zur Festlegung der NCSS sind ebenfalls für die Überarbeitung und Aktualisierung bestehender NCSS relevant.

Abbildung 1: Fünfstufiges Verfahren zur Festlegung der NCSS



3. NIS-Richtlinie: zuständige nationale Behörden, zentrale Anlaufstellen und Computer-Notfallteams (CSIRTs)

Gemäß Artikel 8 Absatz 1 benennt jeder Mitgliedstaat eine oder mehrere zuständige nationale Behörden, die mindestens die in Anhang II der Richtlinie genannten Sektoren und die in Anhang III der Richtlinie genannten Dienste abdecken und die Anwendung der Richtlinie

überwachen. Die Mitgliedstaaten können diese Funktion einer oder mehreren bereits bestehenden Behörden zuweisen.

In diesem Abschnitt geht es vor allem darum, wie die NIS-Richtlinie die Abwehrbereitschaft der Mitgliedstaaten erhöht, indem sie wirksame zuständige nationale Behörden und Computer-Notfallteams (CSIRTs) vorschreibt. Genauer gesagt beschäftigt sich der Abschnitt mit der Verpflichtung zur Benennung zuständiger nationaler Behörden, einschließlich der Rolle als zentraler Anlaufstelle. Drei Themen werden behandelt: a) mögliche nationale Steuerungsstrukturen (z. B. zentrale bzw. dezentrale Modelle usw.) und sonstige Anforderungen, b) die Rolle als zentrale Anlaufstelle und c) CSIRTs.

3.1. Art der Behörden

Gemäß Artikel 8 der NIS-Richtlinie muss jeder Mitgliedstaat für die Sicherheit von Netz- und Informationssystemen zuständige nationale Behörden benennen. Dabei wird ausdrücklich darauf hingewiesen, dass *„eine oder mehrere ... zuständige nationale Behörden“* benannt werden können. In Erwägungsgrund 30 der Richtlinie wird diese politische Entscheidung erläutert: *„Angesichts der unterschiedlichen nationalen Verwaltungsstrukturen und zur Beibehaltung bereits bestehender sektorbezogener Vereinbarungen oder von Aufsichts- oder Regulierungsstellen der Union sowie zur Vermeidung von Doppelarbeit sollten die Mitgliedstaaten befugt sein, mehr als eine nationale Behörde zu benennen, die für die Erfüllung der Aufgaben im Zusammenhang mit der Sicherheit von Netz- und Informationssystemen von Betreibern wesentlicher Dienste und Anbietern digitaler Dienste gemäß dieser Richtlinie verantwortlich sind.“*

Dementsprechend steht es den Mitgliedstaaten frei, eine zentrale Behörde, die alle in den Anwendungsbereich der Richtlinie fallenden Sektoren und Dienste abdeckt, oder mehrere Behörden, z. B. je nach der Art des Sektors, zu benennen.

Bei der Entscheidung über das Vorgehen können sich die Mitgliedstaaten auf die Erfahrungen mit den nationalen Ansätzen im Rahmen der bestehenden Rechtsvorschriften über den Schutz kritischer Informationsinfrastrukturen (Critical Information Infrastructure Protection, CIIP) stützen. Wie in Tabelle 1 beschrieben, haben die Mitgliedstaaten im Fall des CIIP bei der Zuweisung der Zuständigkeiten auf nationaler Ebene entweder einen zentralen oder einen dezentralen Ansatz gewählt. Nationale Beispiele sind hier nur zur Veranschaulichung aufgeführt und um die Mitgliedstaaten auf bestehende Organisationsrahmen aufmerksam zu machen. Die Kommission deutet also nicht an, dass das in den jeweiligen Mitgliedstaaten beim CIIP eingesetzte Modell unbedingt für die Umsetzung der NIS-Richtlinie verwendet werden sollte.

Die Mitgliedstaaten können ebenso verschiedene hybride Gestaltungsmöglichkeiten mit Elementen sowohl zentraler als auch dezentraler Ansätze wählen. Die Auswahl kann in Übereinstimmung mit den nationalen Steuerungsregelungen für die verschiedenen in den Anwendungsbereich der Richtlinie fallenden Sektoren und Dienste getroffen oder durch die betreffenden Behörden und die relevanten Interessenträger, d. h. die Betreiber wesentlicher Dienste und Anbieter digitaler Dienste, neu bestimmt werden. Vorhandenes Fachwissen im

Bereich Cybersicherheit, Erwägungen zur Mittelausstattung, das Verhältnis zwischen den Interessenträgern und nationalen Interessen (z. B. wirtschaftliche Entwicklung, öffentliche Sicherheit usw.) können ebenfalls wichtige Faktoren für die Entscheidungen der Mitgliedstaaten sein.

3.2 Öffentlichkeitsarbeit und weitere relevante Aspekte

Gemäß Artikel 8 Absatz 7 müssen die Mitgliedstaaten der Kommission die Benennung der zuständigen nationalen Behörde und deren Aufgaben mitteilen. Dies muss bis zur Umsetzungsfrist geschehen.

Gemäß den Artikeln 15 und 17 der NIS-Richtlinie müssen die Mitgliedstaaten sicherstellen, dass die zuständigen Behörden über bestimmte Befugnisse und die Mittel zur Durchführung der in entsprechenden Artikeln beschriebenen Aufgaben verfügen.

Ferner muss die Benennung bestimmter Einrichtungen als zuständige nationale Behörden öffentlich gemacht werden. In der Richtlinie wird nicht festgelegt, wie diese Veröffentlichung erfolgen muss. Da durch diese Anforderung eine größere Sensibilisierung für die NIS aufseiten der betroffenen Akteure und der Öffentlichkeit erzielt werden soll, ist die Kommission – auch angesichts der Erfahrungen in anderen Sektoren (Telekommunikation, Bankwesen, Arzneimittel) – der Auffassung, dass dies beispielsweise mithilfe eines gut beworbenen Portals erreicht werden könnte.

Gemäß Artikel 8 Absatz 5 der NIS-Richtlinie müssen solche Behörden mit „angemessenen Ressourcen“ ausgestattet sein, damit sie die ihnen mit der Richtlinie übertragenen Aufgaben wahrnehmen können.

Tabelle 1: Nationale Ansätze für den Schutz kritischer Informationsinfrastrukturen (CIIP)

Im Jahr 2016 veröffentlichte die ENISA eine Studie[12] über die unterschiedlichen Ansätze der Mitgliedstaaten zum Schutz ihrer kritischen Informationsinfrastrukturen. Darin werden zwei Profile in Bezug auf die CIIP-Verwaltung in den Mitgliedstaaten beschrieben, die im Zusammenhang mit der Umsetzung der NIS-Richtlinie genutzt werden können.

Profil 1: Dezentraler Ansatz – mit mehreren für die in Anhang II bzw. Anhang III der Richtlinie genannten spezifischen Sektoren bzw. Dienste zuständigen Behörden

Der dezentrale Ansatz zeichnet sich durch folgende Merkmale aus:

(i) Subsidiaritätsprinzip
(ii) Enge Zusammenarbeit zwischen öffentlichen Stellen
(iii)Sektorspezifische Rechtsvorschriften

Subsidiaritätsprinzip

Anstatt eine einzige Stelle einzurichten oder zu benennen, der die Gesamtzuständigkeit übertragen wird, wird beim dezentralen Ansatz das Subsidiaritätsprinzip verfolgt. Das bedeutet, dass die Zuständigkeit für die Umsetzung in Händen einer sektorspezifischen Behörde liegt, die den lokalen Sektor am besten versteht und bereits eine Beziehung mit den Interessenträgern aufgebaut hat. Nach diesem Prinzip werden Entscheidungen durch diejenigen getroffen, die mit den Betroffenen am engsten verbunden sind.

Enge Zusammenarbeit zwischen öffentlichen Stellen

Wegen der Vielfalt der am CIIP beteiligten öffentlichen Stellen haben viele Mitgliedstaaten Kooperationsregelungen entwickelt, um die Arbeit und die Bemühungen der verschiedenen Behörden zu koordinieren. Diese Kooperationsregelungen können die Form informeller Netze oder stärker institutionalisierter Foren oder Regelungen annehmen. Dennoch dienen diese Kooperationsregelungen allein dem Informationsaustausch und der Koordinierung zwischen den verschiedenen öffentlichen Stellen, verfügen aber über keinerlei Weisungsbefugnis.

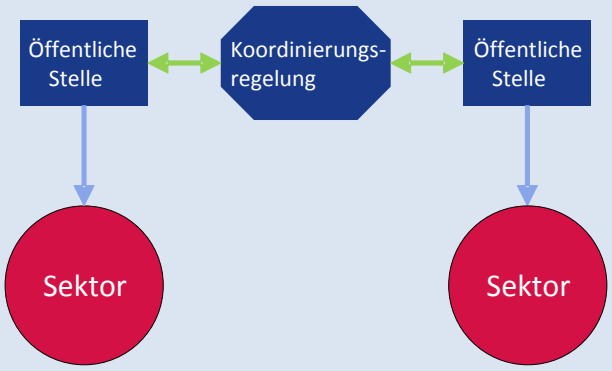
Sektorspezifische Rechtsvorschriften

Die Mitgliedstaaten, die in den kritischen Sektoren einen dezentralen Ansatz verfolgen, verzichten häufig auf CIIP-Gesetzgebung. Stattdessen bleibt die Annahme von Gesetzen und Verordnungen sektorspezifisch und kann daher von einem Sektor zum nächsten stark variieren. Dieser Ansatz hätte den Vorteil einer Angleichung der mit der NIS verbundenen Maßnahmen an bestehende sektorspezifische Vorschriften, um eine bessere Akzeptanz durch den Sektor sowie eine wirksamere Durchsetzung durch die betreffende Behörde zu erzielen.

[12] ENISA, *Stocktaking, Analysis and Recommendations on the protection of CIIs* (Bestandsaufnahme, Analyse und Empfehlungen zum Schutz kritischer Informationsinfrastrukturen, 2016). Abrufbar unter: https://www.enisa.europa.eu/publications/stocktaking-analysis-and-recommendations-on-the-protection-of-ciis

Bei einem rein dezentralen Ansatz besteht die erhebliche Gefahr, dass die Richtlinie über mehrere Sektoren und Dienste hinweg uneinheitlich angewendet wird. In diesem Fall sieht die Richtlinie eine zentrale Anlaufstelle vor, die in grenzüberschreitenden Angelegenheiten die Schnittstelle bildet. Der betreffende Mitgliedstaat könnte diese Stelle außerdem mit der internen Koordination und Zusammenarbeit zwischen verschiedenen zuständigen nationalen Behörden gemäß Artikel 10 der Richtlinie beauftragen.

Abbildung 2 – Dezentraler Ansatz



Beispiele für den dezentralen Ansatz

Schweden ist ein gutes Beispiel für einen Mitgliedstaat, der einen dezentralen Ansatz zum Schutz kritischer Informationsinfrastrukturen verfolgt. Schweden nimmt eine „Systemperspektive“ ein, d. h., dass verschiedenen Behörden und Gemeinden für die Hauptaufgaben des CIIP zuständig sind, darunter die Bestimmung unerlässlicher Dienste und kritischer Infrastrukturen, die Koordinierung und Unterstützung der Betreiber, Regulierungsaufgaben sowie Maßnahmen zur Notfallvorsorge. Bei diesen Stellen handelt es sich um das schwedische Amt für Zivilschutz (MSB), die schwedische Agentur für Post und Telekommunikation (PTS) und mehrere schwedische Verteidigungs-, Militär- und Strafverfolgungsbehörden.

Zur Koordinierung der Maßnahmen der verschiedenen Stellen und öffentlichen Einrichtungen hat die schwedische Regierung ein Kooperationsnetz aus Behörden mit „besonderen gesellschaftlichen Zuständigkeiten in Sachen Informationssicherheit“ entwickelt. Diese Kooperationsgruppe für Informationssicherheit (SAMFI) besteht aus Vertretern der verschiedenen Behörden und kommt mehrmals im Jahr zusammen, um Fragen der nationalen Informationssicherheit zu erörtern. Die Themenbereiche der SAMFI liegen vor allem in politisch-strategischen Bereichen und erstrecken sich z. B. auf technische Fragen und Normung, nationale und internationale Entwicklungen im Bereich der Informationssicherheit, das Management und die Vermeidung von IT-Sicherheitsvorfällen. (Schwedisches Amt für Zivilschutz (MSB), 2015).

Schweden hat keine zentralen Rechtsvorschriften zum CIIP erlassen, die für die Betreiber kritischer Informationsinfrastrukturen über alle Sektoren hinweg gelten. Stattdessen sind die jeweiligen Behörden für den Erlass von Rechtsvorschriften mit Verpflichtungen für Unternehmen in bestimmten Sektoren zuständig. Das MSB ist beispielsweise befugt, Verordnungen für die staatlichen Behörden im Bereich der Informationssicherheit zu erlassen. Das PTS wiederum kann Betreiber verpflichten, bestimmte technische und organisatorische Sicherheitsmaßnahmen auf Grundlage des Sekundärrechts umzusetzen.

Ein weiteres Beispiel für einen Mitgliedstaat, der diese Merkmale aufweist, ist Irland. Irland verfolgt eine „Subsidiaritätsdoktrin", nach der jedes Ministerium für die Bestimmung der kritischen Informationsinfrastrukturen und für die Risikobewertung in seinem Bereich verantwortlich ist. Darüber hinaus wurden keine besonderen Regelungen für den Schutz kritischer Informationsinfrastrukturen auf nationaler Ebene erlassen. Die Rechtsvorschriften bleiben sektorspezifisch und gelten vor allem für den Energie- und den Telekommunikationssektor (2015). Weitere Beispiele sind Österreich, Zypern und Finnland.

Profil 2: Zentraler Ansatz – mit einer zentralen für alle in Anhang II bzw. Anhang III der Richtlinie genannten Sektoren bzw. Dienste zuständigen Behörde

Der zentrale Ansatz zeichnet sich durch folgende Merkmale aus:

i) Eine zentrale Behörde für alle Sektoren
ii) Umfassende Rechtsvorschriften

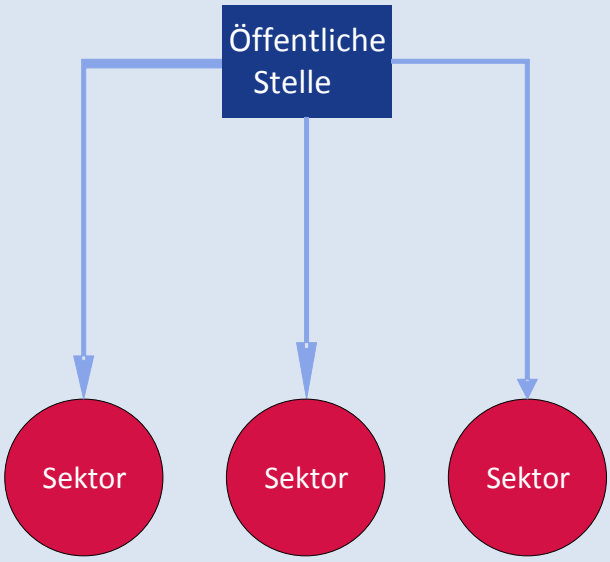
Eine zentrale Behörde für alle Sektoren

Mitgliedstaaten, die einen zentralen Ansatz verfolgen, haben Behörden mit Zuständigkeiten und weitreichenden Kompetenzen in mehreren oder allen kritischen Sektoren eingerichtet oder diese Befugnisse bestehenden Behörden übertragen. Die wichtigsten Behörden für den CIIP vereinen mehrere Aufgaben wie die Notfallplanung, Notfallmaßnahmen, Regulierungsaufgaben und die Unterstützung von privaten Betreibern an einer Stelle. In vielen Fällen ist das nationale oder staatliche CSIRT Teil der CIIP-Hauptbehörde. Angesichts des allgemeinen Mangels an Kompetenzen in der Cybersicherheit verfügt eine zentrale Behörde zumeist über eine höhere Konzentration an Fachwissen im Bereich der Cybersicherheit als mehrere sektorale Behörden.

Umfassende Rechtsvorschriften

Mit umfassenden Rechtsvorschriften werden Verpflichtungen und Anforderungen für alle Betreiber kritischer Informationsinfrastrukturen in allen Sektoren geschaffen. Dies kann durch neue, umfassende Gesetze oder durch eine Ergänzung der bestehenden sektorspezifischen Rechtsvorschriften erzielt werden. Dieser Ansatz würde eine einheitliche Anwendung der NIS-Richtlinie über alle abgedeckten Sektoren und Dienste hinweg erleichtern. Somit würde das Risiko von Lücken bei der Umsetzung vermieden, das sich im Falle von mehreren Behörden mit spezifischen Zuständigkeiten ergeben könnte.

Abbildung 3 – zentraler Ansatz



Beispiele für den zentralen Ansatz

Frankreich ist ein gutes Beispiel für einen Mitgliedstaat mit einem zentralen Ansatz. Frankreichs nationale Agentur für die Sicherheit von Informationssystemen (ANSSI) wurde im Jahr 2011 zur nationalen Behörde für den Schutz der Informationssysteme ernannt. Die ANSSI spielt eine starke Rolle bei der Beaufsichtigung von „Betreibern von entscheidender Bedeutung“. Die Agentur kann den Betreibern die Einhaltung von Sicherheitsmaßnahmen auferlegen und ist befugt, Sicherheitsprüfungen bei ihnen durchzuführen. Darüber hinaus ist sie die zentrale Anlaufstelle für die Betreiber von entscheidender Bedeutung, die verpflichtet sind, der Agentur Sicherheitsvorfälle zu melden.

Bei Sicherheitsvorfällen agiert die ANSSI als Notfallzentrum für den Schutz kritischer Informationsinfrastrukturen und beschließt die Maßnahmen, die die Betreiber zur Bewältigung der Krise ergreifen müssen. Die Maßnahmen der Regierung werden vom Operationszentrum der ANSSI koordiniert. Die Erkennung von Bedrohungen und die Reaktion auf Sicherheitsvorfälle auf operativer Ebene übernimmt CERT-FR, das der ANSSI angehört.

Frankreich hat einen umfassenden Rechtsrahmen für den Schutz kritischer Informationsinfrastrukturen geschaffen. Im Jahr 2006 ordnete der Premierminister die Aufstellung einer Liste von Sektoren mit kritischen Infrastrukturen an. Auf Grundlage dieser Liste, in der zwölf Sektoren von entscheidender Bedeutung benannt wurden, legte die Regierung rund 250 Betreiber von entscheidender Bedeutung fest. Im Jahr 2013 wurde das

Gesetz zur militärischen Planung (LPM)[13] verkündet. Darin werden unterschiedliche Verpflichtungen für Betreiber von entscheidender Bedeutung festgelegt, darunter die Meldung von Sicherheitsvorfällen oder die Umsetzung von Sicherheitsmaßnahmen. Diese Anforderungen sind für alle Betreiber von entscheidender Bedeutung in allen Sektoren verbindlich (französischer Senat 2013).

3.3. NIS-Richtlinie, Artikel 9: Computer-Notfallteams (CSIRTs)

Gemäß Artikel 9 benennt jeder Mitgliedstaat ein oder mehrere CSIRTs, die mit der Bewältigung von Risiken und Vorfällen in den in Anhang II bzw. Anhang III der NIS-Richtlinie aufgeführten Sektoren bzw. Dienste betraut sind. Unter Berücksichtigung der Mindestharmonisierungsanforderung gemäß Artikel 3 der Richtlinie steht es den Mitgliedstaaten frei, die CSIRTs auch in anderen Sektoren, die nicht unter diese Richtlinie fallen, wie der öffentlichen Verwaltung, einzusetzen.

Die Mitgliedstaaten können sich dafür entscheiden, ein CSIRT innerhalb der zuständigen nationalen Behörde einzurichten.[14]

3.4. Aufgaben und Anforderungen

Die Aufgaben der benannten CSIRTs gemäß Anhang I der NIS-Richtlinie umfassen Folgendes:

- Überwachung von Sicherheitsvorfällen auf nationaler Ebene;
- Ausgabe von Frühwarnungen und Alarmmeldungen sowie Bekanntmachung und Verbreitung von Informationen über Risiken und Sicherheitsvorfälle unter den einschlägigen Interessenträgern;
- Reaktion auf Sicherheitsvorfälle;
- dynamische Analyse von Risiken und Sicherheitsvorfällen und Lagebeurteilung sowie
- Beteiligung am nationalen CSIRTs-Netzwerk gemäß Artikel 12.

Weitere besondere Aufgaben in Bezug auf die Meldung von Sicherheitsvorfällen sind in Artikel 14 Absatz 3, Artikel 14 Absatz 5, Artikel 14 Absatz 6, Artikel 16 Absatz 3, Artikel 16 Absatz 6 und Artikel 16 Absatz 7 festgelegt, sofern ein Mitgliedstaat beschließt, dass das CSIRT solche Aufgaben neben den zuständigen nationalen Behörden oder an ihrer Stelle durchführen kann.

[13] *Loi de programmation militaire.*
[14] Siehe Artikel 9 Absatz 1 letzter Satz.

Bei der Umsetzung der Richtlinie haben die Mitgliedstaaten verschiedene Option im Hinblick auf die Rolle der CSIRTs bezüglich der Verpflichtung zur Meldung von Sicherheitsvorfällen. Die Verpflichtung zur direkten Meldung bei den CSIRTs ist möglich und bringt Vorteile für die Verwaltungseffizienz mit sich. Alternativ hierzu können die Mitgliedstaaten beschließen, eine Verpflichtung zur direkten Meldung bei den zuständigen nationalen Behörden einzuführen und den CSIRTs ein Recht auf Zugang zu den gemeldeten Informationen einzuräumen. Letztlich sind die CSIRTs bei der Problemlösung mit ihren Interessenträgern an der Abschreckung, Erkennung, Bewältigung und Minderung der Auswirkungen von Cybervorfällen (einschließlich solcher, die keiner Meldepflicht unterliegen) interessiert. Die Einhaltung der Rechtsvorschriften zu gewährleisten, ist Sache der zuständigen nationalen Behörden.

Gemäß Artikel 9 Absatz 3 der Richtlinie müssen die Mitgliedstaaten auch sicherstellen, dass solche CSIRTs Zugang zu einer sicheren und robusten Kommunikations- und Informationsinfrastruktur haben.

Gemäß Artikel 9 Absatz 4 der Richtlinie müssen die Mitgliedstaaten die Kommission über den Zuständigkeitsbereich der benannten CSIRTs sowie über die wichtigsten Elemente der entsprechenden Verfahren zur Bewältigung von Sicherheitsvorfällen unterrichten.

Anhang I der NIS-Richtlinie enthält die Anforderungen an die von den Mitgliedstaaten benannten CSIRTs. Ein CSIRT sorgt für einen hohen Grad der Verfügbarkeit seiner Kommunikationsdienste. Seine Räumlichkeiten und die unterstützenden Informationssysteme sind an sicheren Standorten eingerichtet und gewährleisten Betriebskontinuität. Ferner sollte das CSIRT die Möglichkeit haben, sich an internationalen Kooperationsnetzen zu beteiligen.

3.5. Unterstützung bei der Entwicklung von CSIRTs

Das Programm für die Netzsicherheit der Infrastrukturen für digitale Dienste (DSI) im Rahmen der Fazilität „Connecting Europe“ (CEF) kann umfangreiche EU-Finanzierungsmittel zur Verfügung stellen, um die CSIRTs der Mitgliedstaaten bei der Verbesserung ihrer Fähigkeiten und der Zusammenarbeit untereinander mithilfe eines Kooperationsmechanismus für den Informationsaustausch zu unterstützen. Der im Rahmen des SMART-Projekts 2015/1089 in der Entwicklung befindliche Kooperationsmechanismus zielt darauf ab, eine zügige und wirksame operative Zusammenarbeit zwischen den CSIRTs der Mitgliedstaaten auf freiwilliger Basis zu fördern, und zwar vor allem zur Unterstützung der dem CSIRT-Netzwerk gemäß Artikel 12 der Richtlinie übertragenen Aufgaben.

Einzelheiten der Aufforderungen zur Einreichung von Vorschlägen für den Aufbau der Kapazitäten der CSIRTs der Mitgliedstaaten sind über die Website der Exekutivagentur für Innovation und Netze (INEA) der Europäischen Kommission[15] abrufbar.

Das DSI-Leitungsgremium im Rahmen der CEF bietet eine informelle Struktur für die Lenkung und Unterstützung der CSIRTs der Mitgliedstaaten auf politischer Ebene, damit deren Kapazitäten aufgebaut und der freiwillige Kooperationsmechanismus umgesetzt wird.

[15] Abrufbar unter: https://ec.europa.eu/inea/en/connecting-europe-facility

Ein neu geschaffenes oder zur Erfüllung der Aufgaben gemäß Anhang I der NIS-Richtlinie eingerichtetes CSIRT kann sich auf die Beratung und Sachkenntnis der ENISA stützen, um seine Leistung zu verbessern und seine Arbeit effizienter zu verrichten.[16] In diesem Zusammenhang sei darauf hingewiesen, dass sich die CSIRTs der Mitgliedstaaten auf aktuelle Arbeiten der ENISA stützen könnte. Wie insbesondere in Abschnitt 7 dieses Anhangs aufgeführt, hat die Agentur eine Reihe von Dokumenten und Studien über bewährte Verfahren sowie technische Empfehlungen, einschließlich Reifegradbewertungen von CSIRTs, für verschiedene CSIRT-Fähigkeiten und -Dienste veröffentlicht. Darüber hinaus haben CSIRTs-Netzwerke sowohl auf globaler (FIRST[17]) als auch auf europäischer (Trusted Introducer, TI[18]) Ebene Leitlinien und bewährte Verfahren verbreitet.

3.6. Rolle der zentralen Anlaufstelle

Gemäß Artikel 8 Absatz 3 der NIS-Richtlinie benennt jeder Mitgliedstaat eine zentrale Anlaufstelle, die die grenzüberschreitenden Zusammenarbeit mit den entsprechenden Behörden in anderen Mitgliedsaaten sowie mit der Kooperationsgruppe und dem CSIRTs-Netzwerk[19], die beide mit der Richtlinie geschaffen wurden, gewährleistet. In Erwägungsgrund 31 und Artikel 8 Absatz 4 werden die Gründe für diese Anforderung erläutert, nämlich die Erleichterung der grenzüberschreitenden Zusammenarbeit und Kommunikation. Dies ist insbesondere erforderlich, da die Mitgliedstaaten beschließen können, die Zuständigkeiten mehr als einer nationalen Behörde zu übertragen. Daher würde eine zentrale Anlaufstelle die Ermittlung der entsprechenden Behörden der einzelnen Mitgliedstaaten sowie ihre Zusammenarbeit erleichtern.

In Fällen, in denen die nationale zentrale Anlaufstelle weder ein CSIRT noch Mitglied der Kooperationsgruppe ist, wird die vermittelnde Rolle der zentralen Anlaufstelle voraussichtlich den Austausch mit den Sekretariaten der Kooperationsgruppe und des CSIRTs-Netzwerkes erfordern. Darüber hinaus müssen die Mitgliedstaaten sicherstellen, dass die zentralen Anlaufstellen über die von Betreibern wesentlicher Dienste und Anbietern digitaler Dienste übermittelten Meldungen unterrichtet sind.[20]

Sofern ein Mitgliedstaat einen zentralen Ansatz verfolgt, d. h. nur eine zuständige Behörde benennt, ist in Artikel 8 Absatz 3 der Richtlinie festgelegt, dass dieser Behörde auch die Rolle der zentralen Anlaufstelle zukommt. Entscheidet sich ein Mitgliedstaat für einen dezentralen Ansatz, könnte er eine der verschiedenen zuständigen Behörden als zentrale Anlaufstelle wählen. Unabhängig vom gewählten institutionellen Modell müssen die Mitgliedstaaten, wenn zuständige Behörde, CSIRT und zentrale Anlaufstelle getrennte Einrichtungen sein

[16] Siehe Artikel 9 Absatz 5 der NIS-Richtlinie.
[17] Forum of Incident Response and Security Teams (https://www.first.org/)
[18] https://www.trusted-introducer.org/
[19] Netzwerk der nationalen CSIRTs für eine operative Zusammenarbeit zwischen den Mitgliedstaaten gemäß Artikel 12.
[20] Siehe Artikel 10 Absatz 3.

sollen, dafür sorgen, dass diese bei der Erfüllung der in der Richtlinie festgelegten Pflichten zusammenarbeiten.[21]

Die zentrale Anlaufstelle legt der Kooperationsgruppe bis zum 9. August 2018 und danach jährlich einen zusammenfassenden Bericht über die eingegangenen Meldungen, einschließlich der Zahl der Meldungen, der Art der gemeldeten Sicherheitsvorfälle sowie die von den Behörden ergriffenen Maßnahmen, wie etwa die Unterrichtung anderer betroffener Mitgliedstaaten über den Vorfall oder die Übermittlung einschlägiger Informationen an die meldenden Unternehmen zur Bewältigung des Vorfalls, vor.[22] Auf Ersuchen der zuständigen Behörde oder des CSIRT leitet die zentrale Anlaufstelle die Meldungen von Betreibern wesentlicher Dienste an die zentralen Anlaufstellen der anderen von den Vorfällen betroffenen Mitgliedstaaten weiter.[23]

Die Mitgliedstaaten unterrichten die Kommission bis zum Ende der Umsetzungsfrist über die Benennung der zentralen Anlaufstelle sowie deren Aufgaben. Die Benennung der zentralen Anlaufstelle ist in der gleichen Weise wie bei den zuständigen nationalen Behörden öffentlich zu machen. Die Kommission veröffentlicht eine Liste der benannten zentralen Anlaufstellen.

3.7. Sanktionen

Artikel 21 gibt den Mitgliedstaaten einen Ermessensspielraum im Hinblick auf die Art der anwendbaren Sanktionen, sofern sie wirksam, angemessen und abschreckend sind. Mit anderen Worten steht den Mitgliedstaaten die Entscheidung über den in ihren nationalen Rechtsvorschriften festgelegten Höchstbetrag für Sanktionen frei. Der festgelegte Betrag oder Prozentsatz sollte es den nationalen Behörden jedoch gestatten, in jedem konkreten Fall wirksame, angemessene und abschreckende Sanktionen unter Berücksichtigung verschiedener Faktoren wie beispielsweise der Schwere oder Häufigkeit des Verstoßes zu verhängen.

4. Einrichtungen mit Auflagen in Bezug auf Sicherheitsanforderungen und die Meldung von Sicherheitsvorfällen

Die in Artikel 4 Nummer 4 und Artikel 4 Nummer 5 genannten Einrichtungen, die als Betreiber wesentlicher Dienste (*operators of essential services*, OES) bzw. Anbieter digitaler Dienste (*digital service providers*, DSP) eine wichtige Rolle für Gesellschaft und Wirtschaft spielen, sind verpflichtet, angemessene Sicherheitsvorkehrungen zu treffen und Sicherheitsvorfälle den zuständigen nationalen Behörden zu melden. Anlass hierfür ist die Überlegung, dass Sicherheitsvorfälle in solchen Diensten unter Umständen eine erhebliche Bedrohung für den Betrieb solcher Dienste darstellen und zu größeren Störungen des Wirtschaftslebens sowie der Gesellschaft insgesamt führen können, was potenziell das Vertrauen der Nutzer untergraben und der Wirtschaft der Union erheblichen Schaden zufügen kann[24].

[21] Siehe Artikel 10 Absatz 1.
[22] Ebenda.
[23] Siehe Artikel 14 Absatz 5.
[24] Siehe Erwägungsgrund 2.

Dieser Abschnitt bietet einen Überblick über die in den Anwendungsbereich der Anhänge II und III der NIS-Richtlinie fallenden Einrichtungen und führt ihre Verpflichtungen auf. Die Ermittlung der Betreiber wesentlicher Dienste wird angesichts der Bedeutung dieses Prozesses für die harmonisierte Umsetzung der NIS-Richtlinie in der gesamten EU umfassend abgedeckt. Ferner enthält der Abschnitt ausführliche Erläuterungen zur Definition digitaler Infrastrukturen und zum Begriff Anbieter digitaler Dienste. Außerdem wird die mögliche Einbeziehung weiterer Sektoren geprüft und die konkrete Vorgehensweise in Bezug auf Anbieter digitaler Dienste erörtert.

4.1. Betreiber wesentlicher Dienste (OES)

Die NIS-Richtlinie legt nicht ausdrücklich fest, welche Einrichtungen genau als OES im Anwendungsbereich der Richtlinie gelten. Vielmehr enthält sie Kriterien, die die Mitgliedstaaten bei dem Ermittlungsverfahren anwenden müssen, von dem letztlich abhängt, welche einzelnen Unternehmen, die zu der Art der in Anhang II aufgeführten Einrichtungen gehören, als Betreiber wesentlicher Dienste anzusehen sind und daher den Verpflichtungen gemäß der Richtlinie unterliegen.

4.1.1. Art der in Anhang II der NIS-Richtlinie aufgeführten Einrichtungen

Gemäß Artikel 4 Nummer 4 bezeichnet der Ausdruck „Betreiber wesentlicher Dienste“ öffentliche oder private Einrichtungen einer in Anhang II der Richtlinie genannten Art, die den Anforderungen des Artikels 5 Absatz 2 entspricht. In Anhang II sind die Sektoren, Teilsektoren und Arten von Einrichtungen aufgeführt, für die jeder Mitgliedstaat das Ermittlungsverfahren gemäß Artikel 5 Absatz 2 durchführen muss[25]. Dazu gehören u. a. die Sektoren Energie, Verkehr, Bankwesen, Finanzmarktinfrastrukturen, Gesundheitswesen, Wasserversorgung und digitale Infrastrukturen.

Für die meisten der Einrichtungen der „traditionellen Sektoren“ enthalten die EU-Rechtsvorschriften gut ausgearbeitete Begriffsbestimmungen, auf die in Anhang II Bezug genommen wird. Auf den in Anhang II Nummer 7 genannten Sektor für digitale Infrastruktur, der beispielsweise Internet-Knoten, Domänennamensysteme (DNS) und Register für Domänen oberster Stufe (*TLD name registries*) umfasst, trifft dies nicht zu. Zur Klarstellung dieser Begriffe folgen daher detaillierte Erläuterungen dieser Ausdrücke.

1) Internet-Knoten (IXP)

Der Begriff „Internet-Knoten“ (*Internet Exchange Point*, IXP) wird in Artikel 4 Nummer 13 definiert und in Erwägungsgrund 18 näher erläutert. Er beschreibt eine Netzeinrichtung, die die Zusammenschaltung von mehr als zwei unabhängigen technisch autonomen Systemen ermöglicht, in erster Linie zur Erleichterung des Austauschs von Internet-Datenverkehr. Internet-Knoten kann auch einen physischen Ort bezeichnen, an dem eine Reihe von Netzen

[25] Siehe Abschnitt 4.1.6 für weitere Einzelheiten zum Ermittlungsverfahren.

mithilfe einer Schaltzentrale Internet-Datenverkehr untereinander austauschen. Der Hauptzweck eines IXP besteht darin, die direkte Zusammenschaltung von Netzen über den Knoten zu ermöglichen anstatt über ein oder mehrere Drittnetze. Der IXP-Anbieter ist in der Regel nicht für das Routing des Internetverkehrs verantwortlich. Dies übernehmen die Netzbetreiber. Die direkte Zusammenschaltung hat zahlreiche Vorteile; Kosten, Latenz und Bandbreite sind jedoch die Hauptgründe. Datenverkehr, der durch einen Knoten fließt, wird in der Regel von keiner Partei in Rechnung gestellt, Datenverkehr zu einem vorgelagerten Internetdienstanbieter (ISP) jedoch schon. Durch die direkte Zusammenschaltung – oftmals in derselben Stadt wie beide Netze befindlich – wird vermieden, dass die Daten über große Entfernungen von einem Netz zum anderen übertragen werden müssen, sodass sich die Latenz verringert.

Es sei darauf hingewiesen, dass sich die Begriffsbestimmung eines „IXP“ nicht auf physische Knotenpunkte erstreckt, an denen nur zwei physische Netze zusammengeschaltet sind (d. h. zwischen Netzbetreibern wie Base und Proximus). Daher müssen die Mitgliedstaaten bei der Umsetzung der Richtlinie zwischen Betreibern, die den Austausch aggregierten Internetverkehrs zwischen mehreren Netzbetreibern erleichtern, und jenen, die ein einziges Netz betreiben und die ihre Netze auf Grundlage einer Zusammenschaltungsvereinbarung physisch zusammenschalten, unterscheiden. Im letzteren Fall fallen die Netzbetreiber nicht unter die Begriffsbestimmung gemäß Artikel 4 Nummer 13. Eine Klarstellung dieser Frage findet sich in Erwägungsgrund 18, wonach die IXP keinen Netzzugang ermöglicht und weder als Transit-Anbieter noch als Carrier fungiert. Bei der letzten Anbieterkategorie handelt es sich um Unternehmen, die öffentliche Kommunikationsnetze und/oder -dienste bereitstellen, für die die Sicherheitsanforderungen und Meldepflichten gemäß den Artikeln 13a und 13b der Richtlinie 2002/21/EG gelten und die aus diesem Grund aus dem Anwendungsbereich der NIS-Richtlinie ausgeschlossen sind[26].

2) Domain-Namen-System (DNS)

Der Begriff „Domain-Namen-System (DNS)“ bezeichnet gemäß Artikel 4 Nummer 14 *„ein hierarchisch unterteiltes Bezeichnungssystem in einem Netz zur Beantwortung von Anfragen zu Domain-Namen“*. Genauer gesagt handelt es sich beim DNS um ein hierarchisch unterteiltes Bezeichnungssystem für Computer, Dienste oder jede andere Ressource, die an das Internet angeschlossen ist und es ermöglicht, Domain-Namen in IP-Adressen (Internet-Protokoll) aufzulösen. Die Hauptaufgabe des Systems besteht darin, die zugewiesenen Domain-Namen in IP-Adressen umzuwandeln. Zu diesem Zweck verfügt das DNS über eine Datenbank und arbeitet mit Name-Servern und Resolvern, um diese Art von „Umwandlung“ von Domainnamen in IP-Adressen zu ermöglichen. Zwar ist die Auflösung von Domänennamen nicht die einzige Aufgabe des DNS, sie gehört aber zu den Kernaufgaben des Systems. Bei der Legaldefinition in Artikel 4 Nummer 14 liegt der Schwerpunkt auf der wesentlichen Rolle des Systems aus Sicht der Nutzer ohne weitere technische Einzelheiten,

[26] Siehe Abschnitt 5.2 für weitere Informationen über das Verhältnis zwischen der NIS-Richtlinie und der Richtlinie 2002/21/EG.

wie z. B. der Betrieb des Domänennamensraums, von Name-Servern, Resolvern usw. In Artikel 4 Nummer 15 wird schließlich bestimmt, wer als DNS-Diensteanbieter anzusehen ist.

3) Top-Level-Domain-Name-Registry (TLD-Name-Registry)

Gemäß Artikel 4 Nummer 16 bezeichnet der Begriff „Top-Level-Domain-Name-Registry" eine Einrichtung, die die Registrierung von Internet-Domain-Namen innerhalb einer spezifischen Top-Level-Domain (TLD) verwaltet und betreibt. Eine solche Verwaltung von Domänennamen beinhaltet die Auflösung von TLD-Namen in IP-Adressen.

Die IANA (Internet Assigned Numbers Authority) ist für die weltweite Koordinierung der DNS-Rootzone, IP-Adressierung und anderen IP-Ressourcen zuständig. Insbesondere übernimmt die IANA die Vergabe allgemeiner Domänennamen oberster Stufe (generic Top Level Domains, gTLD) (z. B. „.com") und der Länderdomänen oberster Stufe (country code Top Level Domains, ccTLD) (z. B. „.be") an Betreiber (Register) und die Pflege technischer und administrativer Elemente. Die IANA betreibt ein weltweites Register zugewiesener TLD und spielt eine Rolle bei der Veröffentlichung dieser Liste an Internetnutzer auf der ganzen Welt sowie bei der Einführung neuer TLD.

Eine wichtige Aufgabe der Register besteht in der Zuweisung von Domainnamen zweiter Stufe an die so genannten Registranten in der jeweiligen TLD. Diese Registranten können sich auch dafür entscheiden, selbst Domainnamen dritter Stufe zuzuweisen. Die ccTLD werden entsprechend der Norm ISO 3166-1 zur Abbildung eines Landes oder Hoheitsgebiets festgelegt. Die gTLD sind in der Regel nicht auf ein geografisches Gebiet oder Land festgelegt.

Der Betrieb der TLD-Name-Registry kann auch die Bereitstellung von DNS umfassen. Gemäß den Delegationsregeln der IANA muss die zur Verwaltung der ccTLD benannte Stelle in dem entsprechenden Land u. a. die Betreuung der Domänennamen und den Betrieb des DNS übernehmen[27]. Derartige Umstände müssen die Mitgliedstaaten bei der Durchführung des Verfahrens zur Ermittlung der Betreiber wesentlicher Dienste gemäß Artikel 5 Absatz 2 berücksichtigen.

4.1.2. Ermittlung der Betreiber wesentlicher Dienste

Im Einklang mit den Anforderungen des Artikels 5 der Richtlinie muss jeder Mitgliedstaat für alle in Anhang II genannten Arten von Einrichtungen, die im Hoheitsgebiet dieses Mitgliedstaats niedergelassen sind, ein Ermittlungsverfahren durchführen. Als Ergebnis dieser Bewertung werden alle Einrichtungen, die die Kriterien nach Artikel 5 Absatz 2 erfüllen, als OES identifiziert und unterliegen somit den Sicherheitsanforderungen und Meldepflichten gemäß Artikel 14.

Die Mitgliedstaaten haben noch bis zum 9. November 2018 Zeit zur Ermittlung der Betreiber in jedem Sektor und Teilsektor. Zur Unterstützung der Mitgliedstaaten während dieses

[27] Informationen abrufbar unter: https://www.icann.org/resources/pages/delegation-2012-02-25-en

Prozesses arbeitet die Kooperationsgruppe derzeit an einen Leitfaden mit einschlägigen Informationen über die erforderlichen Schritte und bewährte Verfahren bei der Ermittlung von OES.

Gemäß Artikel 24 Absatz 2 muss die Kooperationsgruppe außerdem das Verfahren, den Inhalt und die Art der nationalen Maßnahmen, die die Ermittlung der Betreiber wesentlicher Dienste in einem bestimmten Sektor gestatten, erörtern. Die Mitgliedstaaten können die Kooperationsgruppe vor dem 9. November 2018 um die Erörterung ihrer geplanten nationalen Maßnahmen zur Ermittlung der Betreiber wesentlicher Dienste ersuchen.

4.1.3. Einbeziehung zusätzlicher Sektoren

Unter Berücksichtigung der Mindestharmonisierungsanforderung gemäß Artikel 3 können die Mitgliedstaaten Rechtsvorschriften erlassen oder beibehalten, um für ein höheres Sicherheitsniveau von Netz- und Informationssystemen zu sorgen. In diesem Hinblick steht es den Mitgliedstaaten grundsätzlich frei, die Sicherheitsanforderungen und Meldepflichten gemäß Artikel 14 auf Einrichtungen aus andere Sektoren und Teilsektoren als den in Anhang II der NIS-Richtlinie aufgeführten auszuweiten. Mehrere Mitgliedstaaten haben bereits beschlossen oder erwägen derzeit, einige der folgenden Sektoren einzubeziehen:

i) Öffentliche Verwaltungen

Öffentliche Verwaltungen können u. U. wesentliche Dienste entsprechend Anhang II der Richtlinie erbringen und die Kriterien des Artikels 5 Absatz 2 erfüllen. In diesem Fall würden die einschlägigen Sicherheitsanforderungen und Meldepflichten für die derartige Dienste erbringenden öffentlichen Verwaltungen gelten. Wenn öffentliche Verwaltungen hingegen Dienste erbringen, die nicht in den genannten Anwendungsbereich fallen, gelten die einschlägigen Verpflichtungen nicht für diese Dienste.

Öffentliche Verwaltungen sind für die ordnungsgemäße Erbringung öffentlicher Dienste durch staatliche Stellen, regionale und lokale Behörden, Agenturen und mit ihnen verbundene Unternehmen verantwortlich. Zu diesen Diensten gehören häufig die Erfassung und Verwaltung personenbezogener und dienstlicher Daten über Individuen und Organisationen, die gemeinsam genutzt und mehreren öffentlichen Stellen zur Verfügung gestellt werden können. Ganz allgemein haben die Gesellschaft und die Wirtschaft als Ganzes großes Interesse an einem hohen Sicherheitsniveau der Netz- und Informationssysteme der öffentlichen Verwaltungen. Nach Auffassung der Kommission täten die Mitgliedstaaten daher gut daran, die Einbeziehung der öffentlichen Verwaltung in den Anwendungsbereich der nationalen Rechtsvorschriften zur Umsetzung der Richtlinie über die Bereitstellung wesentlicher Dienste gemäß Artikel 5 Absatz 2 sowie Anhang II hinaus zu erwägen.

ii) Postsektor

Zum Postsektor gehört die Erbringung von Postdiensten, wie Sammlung, Sortierung, Transport und Zustellung von Postsendungen.

iii) Lebensmittelbranche

Die Lebensmittelbranche umfasst die Herstellung landwirtschaftlicher Erzeugnisse und anderer Nahrungsmittel und könnte wesentlich Dienste erbringen, darunter die Gewährleistung der Ernährungssicherheit und die Sicherung der Lebensmittelqualität und -sicherheit.

iv) Chemische Industrie und Atomindustrie

Die chemische Industrie und die Atomindustrie befassen sich insbesondere mit der Lagerung, Herstellung und Verarbeitung von chemischen und petrochemischen Erzeugnissen bzw. von Kernmaterial.

v) Umweltsektor

Umweltmaßnahmen erstrecken sich auf die Bereitstellung von Gütern und Erbringung von Diensten, die zum Schutz der Umwelt und zur Bewirtschaftung der Ressourcen erforderlich sind. Diese Maßnahmen sollen also Umweltverschmutzungen vermeiden, verringern und beseitigen sowie die verfügbaren natürlichen Ressourcen erhalten. Zu den wesentlichen Diensten in diesem Sektor könnten die Überwachung und Kontrolle von Verschmutzung (z. B. von Luft und Wasser) und von meteorologischen Phänomenen zählen.

vi) Katastrophenschutz

Ziel des Katastrophenschutzes ist die Prävention, Vorsorge und Abwehr von Naturkatastrophen und vom Menschen verursachten Katastrophen. Die zu diesem Zweck erbrachten wesentlichen Dienste können die Aktivierung von Notrufnummern und die Umsetzung der Maßnahmen umfassen, die der Information über Notsituationen, ihrer Eingrenzung sowie der Reaktion darauf dienen.

4.1.4. Gerichtliche Zuständigkeit

Gemäß Artikel 5 Absatz 1 muss jeder Mitgliedstaat OES mit Niederlassung in seinem Hoheitsgebiet ermitteln. Die Art der Niederlassung wird in der Bestimmung ist nicht näher festgelegt. Allerdings wird in Erwägungsgrund 21 klargestellt, dass eine solche Niederlassung die effektive und tatsächliche Ausübung einer Tätigkeit durch eine feste Einrichtung voraussetzt. Die Rechtsform solcher Einrichtungen sollte jedoch nicht ausschlaggebend sein. Dies bedeutet, dass die Gerichte eines Mitgliedstaats u. U. nicht nur dann zuständig sind, wenn ein Betreiber wesentlicher Dienste seinen Hauptsitz in dem jeweiligen Hoheitsgebiet hat, sondern auch dann, wenn der Betreiber dort eine Zweigniederlassung oder eine andere Art der Niederlassung unterhält.

Somit können mehrere Mitgliedstaaten zugleich für dieselbe Einrichtung gerichtlich zuständig sein.

4.1.5. Der Kommission zu übermittelnde Informationen

Für die Zwecke der Überprüfung, die die Kommission gemäß Artikel 23 Absatz 1 der NIS-Richtlinie durchzuführen hat, müssen die Mitgliedstaaten der Kommission bis zum 9. November 2018 und danach alle zwei Jahre die folgenden Informationen übermitteln:

- die nationalen Maßnahmen zur Ermittlung der OES;
- die Liste der wesentlichen Dienste;

- die Zahl der für jeden der in Anhang II genannten Sektoren ermittelten OES und ihre Bedeutung für den jeweiligen Sektor und

- soweit vorhanden, Schwellenwerte zur Bestimmung des einschlägigen Versorgungsgrads unter Bezugnahme auf die Zahl der Nutzer, die den jeweiligen Dienst gemäß Artikel 6 Absatz 1 Buchstabe a in Anspruch nehmen oder unter Bezugnahme auf die Bedeutung der Einrichtung gemäß Artikel 6 Absatz 1 Buchstabe f.

Die in Artikel 23 Absatz 1 vorgesehene Überprüfung, die der umfassenden Überarbeitung der Richtlinie vorgeschaltet ist, spiegelt die Bedeutung wider, die die beiden gesetzgebenden Organe der ordnungsgemäßen Umsetzung der Richtlinie in Bezug auf die Ermittlung der Betreiber wesentlicher Dienste beimessen, um eine Marktfragmentierung zu vermeiden.

Zur bestmöglichen Durchführung dieses Prozesses legt die Kommission den Mitgliedstaaten nahe, dieses Thema zu erörtern sowie sich in der Kooperationsgruppe über einschlägige Erfahrungen auszutauschen. Ferner regt die Kommission an, dass die Mitgliedstaaten der Kommission neben allen Informationen, die sie ihr gemäß der Richtlinie übermitteln müssen, auch die Liste der ermittelten Betreiber wesentlicher Dienste (die letztendlich ausgewählt wurden) zur Verfügung zu stellen – erforderlichenfalls vertraulich. Die Verfügbarkeit solcher Listen würde die Bewertung der Kohärenz der Ermittlungsverfahren durch die Kommission erleichtern und verbessern. Außerdem ließen sich so die Ansätze der Mitgliedstaaten vergleichen, was zu einer besseren Umsetzung der Ziele der Richtlinie führen würde.

4.1.6. Durchführung des Ermittlungsverfahrens

Wie Abbildung 4 zeigt, sollte eine nationale Behörde bei der Durchführung des Ermittlungsverfahrens zu einer bestimmten Einrichtung sechs zentrale Fragen stellen. Jede Frage im folgenden Abschnitt entspricht einem Schritt, der gemäß Artikel 5 in Verbindung mit Artikel 6 und unter Berücksichtigung der Anwendbarkeit von Artikel 1 Absatz 7 durchzuführen ist.

Schritt 1 – **Gehört die Einrichtung zu einem Sektor/Teilsektor und einer Art von Einrichtung gemäß Anhang II der Richtlinie?**

Eine nationale Behörde sollte prüfen, ob eine im Hoheitsgebiet ihres Mitgliedstaats niedergelassene Einrichtung zu den in Anhang II der Richtlinie aufgeführt Sektoren und Teilsektoren gehört. Anhang II deckt verschiedene Wirtschaftssektoren ab, die als wesentlich für das ordnungsgemäße Funktionieren des Binnenmarkts erachtet werden. Insbesondere werden in Anhang II die folgenden Sektoren und Teilsektoren genannt:

- Energie: Elektrizität, Erdöl und Erdgas
- Verkehr: Luftverkehr, Schienenverkehr, Schifffahrt und Straßenverkehr
- Bankwesen: Kreditinstitute
- Finanzmarktinfrastrukturen: Handelsplätze, zentrale Gegenparteien
- Gesundheitswesen: Gesundheitsdienstleister (einschließlich Krankenhäuser und Privatkliniken)
- Wasserversorgung: Trinkwasserlieferung und -versorgung

- Digitale Infrastruktur: Internet-Knoten (IXP), DNS-Diensteanbieter, TLD-Name-Registries[28]

Schritt 2 – **Ist eine *Lex specialis* anwendbar?**

Als Nächstes muss die nationale Behörde prüfen, ob die *Lex-specialis*-Bestimmung gemäß Artikel 1 Absatz 7 Anwendung findet. Erlegt ein EU-Rechtsakt der Union den Betreibern wesentlicher Dienste oder den Anbietern digitaler Dienste Sicherheitsanforderungen und/oder Meldepflichten auf, die in ihrer Wirkung den in der NIS-Richtlinie enthaltenen Pflichten mindestens gleichwertig sind, besagt die Bestimmung insbesondere, dass die Verpflichtungen nach Maßgabe des besonderen Rechtsakts gelten. Des Weiteren wird in Erwägungsgrund 9 klargestellt, dass die Mitgliedstaaten bei Erfüllung der Anforderungen gemäß Artikel 1 Absatz 7 die Bestimmungen des betreffenden sektorspezifischen EU-Rechtsakts anwenden sollten. Die einschlägigen Bestimmungen der NIS-Richtlinie finden hingegen keine Anwendung. In diesem Fall sollte die zuständige Behörde das Ermittlungsverfahren gemäß Artikel 5 Absatz 2 nicht fortsetzen[29].

Schritt 3 – **Erbringt der Betreiber einen „wesentlichen Dienst" im Sinne der Richtlinie?**

Gemäß Artikel 5 Absatz 2 Buchstabe a stellt eine dem Ermittlungsverfahren zu unterziehende Einrichtung einen Dienst bereit, der für die Aufrechterhaltung kritischer gesellschaftlicher und/oder wirtschaftlicher Tätigkeiten unerlässlich ist. Bei der Durchführung dieser Bewertung sollten die Mitgliedstaaten berücksichtigen, dass eine Einrichtung sowohl wesentliche als auch nicht wesentliche Dienste erbringen kann. Dies bedeutet, dass die Sicherheitsanforderungen und Meldepflichten gemäß der NIS-Richtlinie für einen bestimmten Betreiber nur für die von ihm erbrachte Bereitstellung wesentlicher Dienste gelten.

Im Einklang mit Artikel 5 Absatz 3 sollte jeder Mitgliedstaat eine Liste aller von OES in seinem Hoheitsgebiet erbrachten wesentlichen Dienste erstellen. Diese Liste muss der Kommission bis zum 9. November 2018 und danach alle zwei Jahre übermittelt werden[30].

Schritt 4 – **Ist der Dienst von Netz- und Informationssystemen abhängig?**

Ferner sollte geklärt werden, ob dieser Dienst das zweite Kriterium gemäß Artikel 5 Absatz 2 Buchstabe b erfüllt und insbesondere ob die Bereitstellung des wesentlichen Dienstes von Netz- und Informationssystemen im Sinne von Artikel 4 Nummer 1 abhängig ist.

Schritt 5 – **Würde ein Sicherheitsvorfall eine erhebliche Störung bewirken?**

Gemäß Artikel 5 Absatz 2 Buchstabe c muss die nationalen Behörde bewerten, ob ein Sicherheitsvorfall eine erhebliche Störung bei der Bereitstellung dieses Dienstes bewirken

[28]Diese Einrichtungen werden in Abschnitt 4.1.1 näher erläutert.

[29] Weitere Einzelheiten über die Anwendbarkeit der *Lex specialis* finden sich in Abschnitt 5.1.
[30] Siehe Artikel 5 Absatz 7 Buchstabe b.

würde. In diesem Zusammenhang werden in Artikel 6 Absatz 1 mehrere sektorübergreifende Faktoren festgelegt, die bei der Bewertung zu berücksichtigen sind. Darüber hinaus ist in Artikel 6 Absatz 2 geregelt, dass die Bewertung gegebenenfalls auch sektorspezifischen Faktoren Rechnung tragen sollte.

Folgende **sektorübergreifende Faktoren** sind in Artikel 6 Absatz 1 aufgeführt:

- Zahl der Nutzer, die den von der jeweiligen Einrichtung angebotenen Dienst in Anspruch nehmen;
- Abhängigkeit anderer in Anhang II genannter Sektoren von dem von dieser Einrichtung angebotenen Dienst;
- mögliche Auswirkungen von Sicherheitsvorfällen – hinsichtlich Ausmaß und Dauer – auf wirtschaftliche und gesellschaftliche Tätigkeiten oder die öffentliche Sicherheit;
- Marktanteil dieser Einrichtung;
- geografische Ausbreitung des Gebiets, das von einem Sicherheitsvorfall betroffen sein könnte;
- Bedeutung der Einrichtung für die Aufrechterhaltung des Dienstes in ausreichendem Umfang, unter Berücksichtigung der Verfügbarkeit von alternativen Mitteln für die Bereitstellung des jeweiligen Dienstes.

Im Hinblick auf die **sektorspezifischen Faktoren** enthält Erwägungsgrund 28 einige Beispiele (siehe Tabelle 4), die eine nützliche Orientierungshilfe für die nationalen Behörden bieten könnten.

Tabelle 4: Beispiele für sektorspezifische Faktoren, die bei der Bestimmung erheblicher Störungen im Falle eines Sicherheitsvorfalls zu berücksichtigen sind.

Sektor	Beispiele für sektorspezifische Faktoren
Energieversorger	Menge oder Anteil der landesweit produzierten Energie
Öllieferanten	Menge des geförderten Öls pro Tag
Luftverkehr (einschließlich Flughäfen und Luftfahrtunternehmen) **Schienenverkehr** **Seehäfen**	Anteil des landesweiten Verkehrsvolumens, Anzahl der Passagiere oder der Frachtdienste pro Jahr
Bank- oder Finanzmarktinfrastrukturen	Systemrelevanz aufgrund der Bilanzsumme; Anteil dieser Bilanzsumme am BIP
Gesundheitsbereich	Anzahl der vom Anbieter jährlich versorgten Patienten
Wassergewinnung, -aufbereitung und -versorgung	Wassermenge, Anzahl und Arten der belieferten Verbraucher (einschließlich beispielsweise Krankenhäuser, öffentlicher Dienstleister oder Einzelpersonen), Vorhandensein alternativer Wasserquellen zur Versorgung desselben geografischen Gebiets

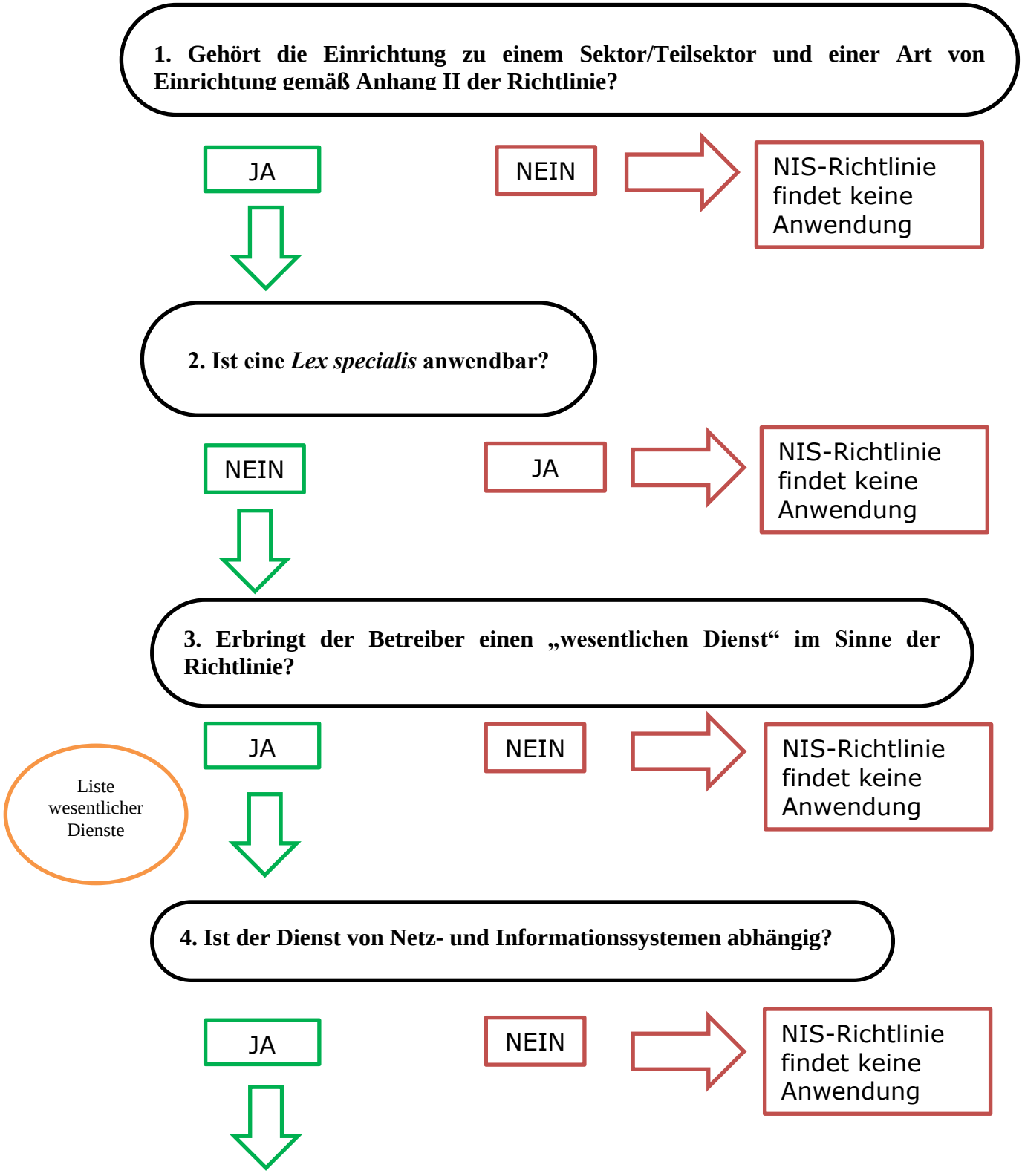
Es sei darauf hingewiesen, dass die Mitgliedstaaten bei der Bewertung gemäß Artikel 5 Absatz 2 keine Kriterien zu den in dieser Bestimmung aufgeführt hinzufügen sollten, da dies die Zahl der ermittelten OES einschränken und die Mindestharmonisierung der OES gemäß Artikel 3 der Richtlinie gefährden könnte.

Schritt 6 – **Erbringt der betreffende Betreiber wesentliche Dienste in anderen Mitgliedstaaten?**

Schritt 6 bezieht sich auf Fälle, in denen ein Betreiber seinen wesentlichen Dienst in zwei oder mehr Mitgliedstaaten erbringt. Die Mitgliedstaaten sind gemäß Artikel 5 Absatz 4 gehalten, vor Abschluss des Ermittlungsverfahrens Konsultationen mit den anderen betreffenden Mitgliedstaaten aufzunehmen[31].

[31] Weitere Informationen über die Konsultation finden Sie in Abschnitt 4.1.7.

Abbildung 4: Ermittlungsverfahren in 6 Schritten



5. Würde ein Sicherheitsvorfall eine erhebliche Störung bewirken?

Sektorübergreifende Faktoren (Artikel 6 Absatz 1)

- **Zahl der Nutzer**, die den Dienst in Anspruch nehmen
- **Abhängigkeit** anderer wesentlicher Sektoren von dem Dienst
- Mögliche Auswirkungen von Sicherheitsvorfällen auf **wirtschaftliche und gesellschaftliche Tätigkeiten** oder **die öffentliche Sicherheit**

Sektorspezifische Faktoren (Beispiele aus Erwägungsgrund 28)

- **Energie**: Menge oder Anteil der landesweit produzierten Energie
- **Verkehr**: Anteil des landesweiten Verkehrsvolumens und Anzahl der Dienste pro Jahr
- **Gesundheitswesen**: Anzahl der vom

JA

NEIN → NIS-Richtlinie findet keine Anwendung

6. Erbringt der betreffende Betreiber wesentliche Dienste in anderen Mitgliedstaaten?

JA

NEIN → NIS-Richtlinie findet keine Anwendung

Verpflichtende Konsultation der

Annahme nationaler Maßnahmen (z. B. Liste der Betreiber wesentlicher Dienste, politische und rechtliche Maßnahmen).

4.1.7. Grenzübergreifendes Konsultationsverfahren

Stellt ein Betreiber wesentliche Dienste in zwei oder mehr Mitgliedstaaten bereit, so nehmen diese Mitgliedstaaten gemäß Artikel 5 Absatz 4 vor Abschluss des Ermittlungsverfahrens Konsultationen miteinander auf. Diese Konsultation soll dabei helfen, die kritische Rolle des Betreibers im Hinblick auf grenzüberschreitende Auswirkungen zu beurteilen.

Mit der Konsultation wird angestrebt, dass die beteiligten nationalen Behörden Argumente und Standpunkte austauschen und idealerweise zum gleichen Ergebnis in Bezug auf die Ermittlung des betreffenden Betreibers kommen. Die NIS-Richtlinie hindert die Mitgliedstaaten jedoch nicht daran, unterschiedlich über die Einstufung einer bestimmten Einrichtung als OES zu entscheiden. In Erwägungsgrund 24 wird die Möglichkeit erwähnt, dass die Mitgliedstaaten in der Angelegenheit die Unterstützung der Kooperationsgruppe anfordern.

Nach Auffassung der Kommission sollten sich die Mitgliedstaaten um einen Konsens in diesen Fragen bemühen, um zu vermeiden, dass dieselbe Einrichtung in verschiedenen Mitgliedstaaten eine unterschiedliche Rechtsstellung innehat. Abweichungen sollten wirklich die Ausnahme bleiben, z. B. wenn ein OES in einem Mitgliedstaat in einem anderen Mitgliedstaat nur in geringfügigem und unbedeutendem Maße tätig ist.

4.2. Sicherheitsanforderungen

Gemäß Artikel 14 Absatz 1 stellen die Mitgliedstaaten sicher, dass OES unter Berücksichtigung des Stands der Technik geeignete und verhältnismäßige technische und organisatorische Maßnahmen ergreifen, um die Risiken für die Sicherheit der Netz- und Informationssysteme, die sie für die Bereitstellung ihrer Dienste nutzen, zu bewältigen. Im Einklang mit Artikel 14 Absatz 2 beugen geeignete Maßnahmen den Auswirkungen von Sicherheitsvorfällen vor bzw. halten diese so gering wie möglich.

Eine spezielle Arbeitsgruppe innerhalb der Kooperationsgruppe befasst sich derzeit mit der Ausarbeitung nicht verbindlicher Leitlinien für die Sicherheitsmaßnahmen der OES[32]. Die Gruppe will die Leitlinien im 4. Quartal 2017 fertigstellen. Die Kommission regt die Mitgliedstaaten an, den von der Kooperationsgruppe entwickelten Leitlinien genau zu folgen, sodass sich die nationalen Bestimmungen über die Sicherheitsanforderungen soweit wie möglich daran ausrichten. Die Harmonisierung solcher Anforderungen würde sowohl ihre Einhaltung durch die OES, die oftmals in mehreren Mitgliedstaaten wesentliche Dienste bereitstellen, als auch die Beaufsichtigung durch die zuständigen nationalen Behörden und die CSIRTs deutlich vereinfachen.

[32] Für die Zwecke dieser Arbeitsgruppe wurden Listen internationaler Standards, bewährter Verfahren und Risikobewertungs-/Risikomanagementmethoden aller unter die NIS-Richtlinie fallender Sektoren ausgegeben und als Vorgaben für die vorgeschlagenen Sicherheitsbereiche und -maßnahmen verwendet.

4.3 Meldepflichten

Gemäß Artikel 14 Absatz 3 stellen die Mitgliedstaaten sicher, dass OES „*Sicherheitsvorfälle, die erhebliche Auswirkungen auf die Verfügbarkeit der ... wesentlichen Dienste haben, ... melden*". Folglich sollten die OES keine kleineren, sondern nur schwerwiegende Vorfälle melden, die sich auf die Verfügbarkeit der wesentlichen Dienste auswirken. Der Ausdruck „Sicherheitsvorfall" bezeichnet gemäß Artikel 4 Nummer 7 „*alle Ereignisse, die tatsächlich nachteilige Auswirkungen auf die Sicherheit von Netz- und Informationssystemen haben*". Ferner bezeichnet „Sicherheit von Netz- und Informationssystemen" gemäß Artikel 4 Nummer 2 „*die Fähigkeit von Netz- und Informationssystemen, auf einem bestimmten Vertrauensniveau alle Angriffe abzuwehren, die die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit gespeicherter oder übermittelter oder verarbeiteter Daten oder entsprechender Dienste, die über diese Netz- und Informationssysteme angeboten werden bzw. zugänglich sind, beeinträchtigen*". Folglich könnte jeder Vorfall mit nachteiligen Auswirkungen sowohl auf die Verfügbarkeit als auch die Authentizität, Integrität oder Vertraulichkeit von Daten oder entsprechenden Diensten potenziell meldepflichtig sein. Die Verfügbarkeit der Dienste im Sinne von Artikel 14 Absatz 3 kann also nicht nur in den Fällen, in denen die physische Verfügbarkeit betroffen ist, gestört sein, sondern auch bei jedem sonstigen Sicherheitsvorfall zum Nachteil der ordnungsgemäßen Erbringung der Dienstleistung[33].

Eine spezielle Arbeitsgruppe innerhalb der Kooperationsgruppe befasst sich derzeit mit der Ausarbeitung nicht verbindlicher Meldeleitlinien für Umstände, unter denen die Betreiber wesentlicher Dienste Sicherheitsvorfälle gemäß Artikel 14 Absatz 7 melden müssen sowie die Muster und Verfahren für nationale Meldungen. Die Leitlinien sollen im 4. Quartal 2017 vorliegen.

Unterschiedliche nationale Meldepflichten können zu rechtlicher Unsicherheit, komplizierteren und umständlicheren Verfahren und erheblichen Verwaltungskosten für grenzübergreifend tätige Betreiber führen. Die Kommission begrüßt daher die Arbeit der Kooperationsgruppe. Wie im Falle der Sicherheitsanforderungen regt die Kommission die Mitgliedstaaten an, den von der Kooperationsgruppe entwickelten Leitlinien genau zu folgen, sodass sich die nationalen Bestimmungen über die Meldung von Sicherheitsvorfällen soweit wie möglich daran ausrichten.

4.4. NIS-Richtlinie, Anhang III: Anbieter digitaler Dienste

Digital Service Provider (DSP) bilden die zweite Kategorie von Einrichtungen im Anwendungsbereich der NIS-Richtlinie. Diese Einrichtungen gelten als wichtige Wirtschaftsakteure, da sie von vielen Unternehmen für die Bereitstellung ihrer eigenen Dienste genutzt werden und eine Störung des digitalen Dienstes Auswirkungen auf wesentliche wirtschaftliche und gesellschaftliche Tätigkeiten haben könnte.

[33] Dasselbe gilt für DSP.

4.4.1. Kategorien von DSP

In Artikel 4 Nummer 5, wo der Begriff „digitaler Dienst“ bestimmt wird, wird auf die Legaldefinition gemäß Artikel 1 Nummer 1 Buchstabe b der Richtlinie (EU) 2015/1535 verwiesen, deren Anwendungsbereich auf Dienste einer in Anhang III genannten Art beschränkt wird. Insbesondere handelt es sich bei diesen Diensten im Sinne des Artikels 1 Nummer 1 Buchstabe b der Richtlinie (EU) 2015/1535 um „*jede in der Regel gegen Entgelt elektronisch im Fernabsatz und auf individuellen Abruf eines Empfängers erbrachte Dienstleistung*“. In Anhang III der NIS-Richtlinie werden drei Arten von Diensten genannt: Online-Marktplätze, Online-Suchmaschinen und Cloud-Computing-Dienste. Im Gegensatz zu den Betreibern wesentlicher Dienste müssen die Mitgliedstaaten die Anbieter digitaler Dienste, die den einschlägigen Verpflichtungen unterliegen, nicht ermitteln. Daher gelten die einschlägigen Vorschriften der Richtlinie, also die Sicherheitsanforderungen und Meldepflichten gemäß Artikel 16, für alle Anbieter digitaler Dienste in ihrem Anwendungsbereich.

Die folgenden Abschnitte enthalten weitere Ausführungen zu den drei Arten digitaler Dienste im Anwendungsbereich der Richtlinie.

1. Anbieter von Online-Marktplätzen

Online-Marktplätze ermöglichen es einer großen Zahl und Vielfalt von Unternehmen, ihren Handelstätigkeiten mit den Verbrauchern nachzugehen und Geschäftsbeziehungen zwischen Unternehmen zu pflegen. Sie bieten Unternehmen die grundlegende Infrastruktur für den Handel im Internet und über Grenzen hinweg. Sie spielen in der Wirtschaft eine wichtige Rolle, indem sie insbesondere KMU Zugang zum breiteren digitalen Binnenmarkt der EU verschaffen. Auch die Bereitstellung ausgelagerter Rechendienste, die die wirtschaftlichen Tätigkeiten des Kunden, einschließlich der Verarbeitung von Transaktionen sowie der Zusammenstellung von Informationen über Käufer, Zulieferer und Produkte, unterstützen, kann zu den Tätigkeiten des Anbieters eines Online-Marktplatzes gehören, ebenso wie die Erleichterung der Suche nach geeigneten Produkten, die Bereitstellung von Produkten, Transaktionswissen und die Zusammenführung von Käufern und Verkäufern.

Der Begriff „Online-Marktplatz“ wird in Artikel 4 Nummer 17 bestimmt und in Erwägungsgrund 15 näher erläutert. Demnach ermöglicht es ein Online-Marktplatz Verbrauchern und Unternehmern, Online-Kaufverträge oder Online-Dienstleistungsverträge mit Unternehmern abzuschließen, und ist der endgültige Bestimmungsort für den Abschluss dieser Verträge. So kann ein Anbieter wie beispielsweise *eBay* als Online-Marktplatz angesehen werden, da er anderen die Einrichtung von Online-Shops auf seiner Plattform erlaubt, um Verbrauchern und Unternehmen diese Produkte und Dienste Online anzubieten. Auch Online-Application-Stores zum Vertrieb von Anwendungen und Softwareprogrammen sind als Online-Marktplatz einzuordnen, denn sie ermöglichen es App-Entwicklern, Verbrauchern oder anderen Unternehmen ihre Dienste zum Kauf anzubieten oder diese zu vertreiben. Im Gegensatz dazu fallen Vermittler von Diensten Dritter wie beispielsweise *Skyscanner* und Preisvergleichsdienste, die die Nutzer auf die Website des Händlers umleitet,

wo der eigentliche Vertrag für die Dienstleistung oder das Produkt abgeschlossen wird, nicht unter die Begriffsbestimmung gemäß Artikel 4 Nummer 17.

2. Anbieter von Internet-Suchmaschinen

Der Ausdruck „Online-Suchmaschine“ wird in Artikel 4 Nummer 18 definiert und in Erwägungsgrund 16 näher erläutert. Es handelt es sich um einen digitalen Dienst, der es Nutzern ermöglicht, Suchen grundsätzlich auf allen Websites oder auf Websites in einer bestimmten Sprache anhand einer Abfrage zu einem beliebigen Thema vorzunehmen. Auf die Suche innerhalb einer Website oder auf Preisvergleichswebsites beschränkte Suchfunktionen sind nicht erfasst. So kann beispielsweise eine Suchmaschine wie diejenige auf der EUR-Lex-Website[34] nicht als Suchmaschine im Sinne der Richtlinie betrachtet werden, da sich ihre Suchfunktion auf den Inhalt dieser konkreten Website beschränkt.

3. Anbieter von Cloud-Computing-Diensten

Gemäß Artikel 4 Nummer 19 bezeichnet der Ausdruck „Cloud Computing“ „*einen digitalen Dienst, der den Zugang zu einem skalierbaren und elastischen Pool gemeinsam nutzbarer Rechenressourcen ermöglicht*“; Erwägungsgrund 17 enthält weitere Erläuterungen zu den Begriffen „Rechenressourcen“, „skalierbar“ und „elastischer Pool“.

Zusammenfassend lässt sich „Cloud Computing“ als spezielle Art von Rechendienst beschreiben, der gemeinsame Ressourcen zur Datenverarbeitung auf Abruf nutzt. „Gemeinsame Ressourcen“ bezieht sich dabei auf jede Art von Hardware- oder Softwarekomponenten (z. B. Netze, Server oder sonstige Infrastruktur, Speicher, Anwendungen und Dienste), die den Nutzern auf Abruf zur Datenverarbeitung zur Verfügung gestellt werden. Der Begriff „gemeinsam nutzbar“ bezeichnet Rechenressourcen derselben physischen Infrastruktur, die zahlreiche Nutzer zur Datenverarbeitung verwenden. Die Rechenressourcen lassen sich als gemeinsam nutzbar definieren, wenn der vom Anbieter genutzte Ressourcen-Pool jederzeit je nach den Anforderungen der Nutzer ausgeweitet oder verkleinert werden kann. D. h., Datenzentren oder einzelne Komponenten in einem Datenzentrum könnten hinzugefügt oder entfernt werden, wenn die Datenverarbeitungs- oder Speicherkapazität insgesamt eine Aktualisierung erfordern. Der Begriff „elastischer Pool“ beschreibt somit eine Reaktion auf verändertes Arbeitsaufkommen durch das automatische Bereitstellen oder Entfernen von Ressourcen, sodass die verfügbaren Ressourcen jederzeit so genau wie möglich dem aktuellen Bedarf entsprechen[35].

Derzeit gibt es drei Haupttypen von Cloud-Computing-Diensten im Angebot der Anbieter:

- In der Cloud bereitgestellte Infrastruktur (Infrastructure as a Service, IaaS): Dies ist eine Kategorie von Cloud-Computing-Diensten, bei der dem Kunden die Cloud-Kapazitäten in Form einer Infrastruktur zur Verfügung gestellt werden. Sie umfasst die virtuelle

[34] Abrufbar unter: http://eur-lex.europa.eu/homepage.html

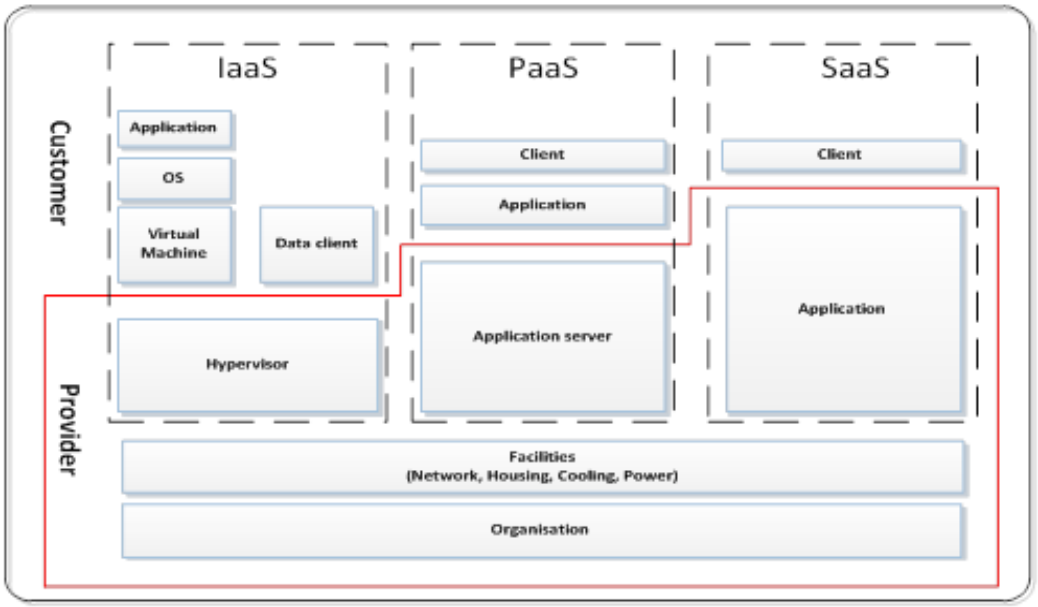
[35] Nikolas Roman Herbst, Samuel Kounev, Ralf Reussner, „Elasticity in Cloud Computing: Was It Is, and What It Is Not“ (Elastizität im Cloud-Computing: was ist das?) (Karlsruher Institut für Technologie), abrufbar unter: https://sdqweb.ipd.kit.edu/publications/pdfs/HeKoRe2013-ICAC-Elasticity.pdf. Siehe auch COM(2012) 529, S. 2–5.

Bereitstellung von Rechenressourcen in Form von Hardware-, Netzwerk- und Speicherdiensten. Die IaaS liefert Server, Speicherplatz, Netze und Betriebssysteme. Sie fungiert als Unternehmensinfrastruktur, in der das Unternehmen seine Daten speichern und die für den täglichen Betrieb erforderlichen Anwendungen ausführen kann.

- In der Cloud bereitgestellte Plattform (Platform as a Service, PaaS): Dies ist eine Kategorie von Cloud-Computing-Diensten, bei der dem Kunden die Cloud-Kapazitäten in Form einer Plattform zur Verfügung gestellt werden. Sie umfasst Online-Rechenplattformen, die es Unternehmen gestatten, bestehende Anwendungen auszuführen oder neue zu entwickeln und zu erproben.

- In der Cloud bereitgestellter Dienst (Service as a Service, SaaS): Dies ist eine Kategorie von Cloud-Computing-Diensten, bei der dem Kunden die Cloud-Kapazitäten in Form einer Anwendung oder Software über das Internet zur Verfügung gestellt werden. Bei dieser Art von Cloud-Diensten entfällt für den Endnutzer die Notwendigkeit, die Software zu kaufen, zu installieren und zu verwalten; sie bringt den Vorteil mit sich, dass die Software mit einer Internetverbindung von überall zugänglich ist.

Abbildung 5: Modelle und Komponenten von Cloud-Computing-Diensten



Die ENISA hat umfassende Leitlinien zu spezifischen Themen im Bereich des Cloud Computing[36] sowie einen Leitfaden über die Grundlagen des Cloud Computing[37] bereitgestellt.

[36] Abrufbar unter: https://www.enisa.europa.eu/topics/cloud-and-big-data/cloud-security
[37] ENISA, *Cloud Security Guide for SMEs* (Leitfaden über die Sicherheit im Cloud Computing für KMU, 2015). Abrufbar unter: https://www.enisa.europa.eu/publications/cloud-security-guide-for-smes

4.4.2. Sicherheitsanforderungen

Gemäß Artikel 16 Absatz 1 stellen die Mitgliedstaaten sicher, dass die DSP geeignete und verhältnismäßige technische und organisatorische Maßnahmen ergreifen, um die Risiken für die Sicherheit der Netz- und Informationssysteme, die die Unternehmen für die Bereitstellung ihrer Dienste nutzen, zu bewältigen. Diese Sicherheitsmaßnahmen sollten den Stand der Technik berücksichtigen und den folgenden fünf Elementen Rechnung tragen: i) Sicherheit der Systeme und Anlagen, ii) Bewältigung von Sicherheitsvorfällen, iii) Business continuity management, iv) Überwachung, Überprüfung und Erprobung, v) Einhaltung der internationalen Normen.

In diesem Zusammenhang wird der Kommission die Befugnis übertragen, gemäß Artikel 16 Absatz 8 Durchführungsrechtsakte zu erlassen, um diese Elemente genauer zu bestimmen und ein hohes Maß an Harmonisierung für diese Diensteanbieter zu gewährleisten. Die Kommission wird den Durchführungsrechtsakt voraussichtlich im Herbst 2017 annehmen. Außerdem müssen die Mitgliedstaaten sicherstellen, dass die Anbieter digitaler Dienste Maßnahmen treffen, um den Auswirkungen von Sicherheitsvorfällen vorzubeugen beziehungsweise diese so gering wie möglich zu halten, damit die Verfügbarkeit dieser Dienste gewährleistet wird.

4.4.3. Meldepflichten

DSP sollten verpflichtet werden, schwerwiegende Sicherheitsvorfälle den zuständigen Behörden oder den CSIRTs zu melden. Gemäß Artikel 16 Absatz 3 der NIS-Richtlinie setzt die Meldepflicht für Anbieter digitaler Dienste bei einem Sicherheitsvorfall ein, der erhebliche Auswirkungen auf die Bereitstellung des Dienstes hat. Zur Feststellung der Auswirkungen sind in Artikel 16 Absatz 4 fünf Parameter aufgeführt, die die Anbieter digitaler Dienste zu berücksichtigen haben. In diesem Zusammenhang wird der Kommission die Befugnis übertragen, gemäß Artikel 16 Absatz 8 Durchführungsrechtsakte zu erlassen, um diese Parameter im Einzelnen zu präzisieren. Die weitere Ausführung dieser Parameter erfolgt im Rahmen des Durchführungsrechtsakts, der der genaueren Bestimmung der unter Nummer 4.4.2 genannten Sicherheitselemente dienen soll und den die Kommission im Herbst anzunehmen beabsichtigt.

4.4.4. Risikobasierter Regulierungsansatz

Artikel 17 sieht vor, dass die DSP der Ex-post-Überwachung durch die zuständigen nationalen Behörden unterliegen. Die Mitgliedstaaten müssen dafür sorgen, dass die zuständigen Behörden tätig werden, wenn ihnen Nachweise dafür vorlegt werden, dass ein DSP die Anforderungen gemäß Artikel 16 der Richtlinie nicht erfüllt.

Ferner wird der Kommission gemäß Artikel 16 Absätze 8 und 9 die Befugnis übertragen, Durchführungsrechtsakte in Bezug auf die Meldepflichten und die Sicherheitsanforderungen zu erlassen, sodass das Maß an Harmonisierung für DSP verbessert wird. Des Weiteren ist es den Mitgliedstaaten gemäß Artikel 16 Absatz 10 nicht gestattet, den DSP neben den Anforderungen der Richtlinie weitere Sicherheits- oder Meldepflichten aufzuerlegen, außer in den Fällen, in denen diese Maßnahmen zum Schutz ihrer grundlegenden staatlichen

Funktionen, insbesondere Maßnahmen zum Schutz der nationalen Sicherheit, und zur Ermöglichung der Ermittlung, Aufklärung und Verfolgung von Straftaten erforderlich sind.

Angesichts des grenzüberschreitenden Charakters der DSP entspricht die Richtlinie nicht dem Modell mehrerer paralleler Zuständigkeiten, sondern verfolgt einen Ansatz auf Grundlage des Kriteriums der Hauptniederlassung des Unternehmens in der EU[38]. Dieser Ansatz ermöglicht es, dass ein einziges Regelwerk für die DSP gilt und eine Behörde für ihre Überwachung zuständig ist. Dies ist besonders wichtig, da viele DSP ihre Dienste in mehreren Mitgliedstaaten gleichzeitig anbieten. Dieses Vorgehen minimiert die Befolgungskosten für DSP und gewährleistet das ordnungsgemäße Funktionieren des digitalen Binnenmarktes.

4.4.5. Gerichtliche Zuständigkeit

Wie bereits dargelegt, unterliegt der DSP gemäß Artikel 18 Absatz 1 der NIS-Richtlinie der gerichtlichen Zuständigkeit des Mitgliedstaats, in dem das Unternehmen seinen Hauptsitz hat. Sollte ein bestimmter DSP Dienste innerhalb der EU bereitstellen, jedoch nicht in der EU niedergelassen sein, muss der DSP gemäß Artikel 18 Absatz 2 einen Vertreter in der Union benennen. In diesem Fall unterliegt das Unternehmen der gerichtlichen Zuständigkeit des Mitgliedstaats, in dem der Vertreter niedergelassen ist. Erbringt ein DSP Dienste in einem Mitgliedstaat, hat aber keinen Vertreter in der EU benannt, kann der Mitgliedstaat im Grunde Maßnahmen gegen den DSP ergreifen, da der Anbieter gegen seine Verpflichtungen gemäß der Richtlinie verstößt.

4.4.6. Ausnahme kleinerer Anbieter digitaler Dienste vom Anwendungsbereich der Sicherheitsanforderungen und Meldepflichten

Gemäß Artikel 16 Absatz 11 sind Anbieter digitaler Dienste, bei denen es sich um Kleinstunternehmen und kleine Unternehmen im Sinne der Empfehlung 2003/361/EG der Kommission39 handelt, vom Anwendungsbereich der Sicherheitsanforderungen und Meldepflichten nach Artikel 16 ausgenommen. Dies bedeutet, dass jene Unternehmen, die weniger als 50 Mitarbeiter beschäftigen und deren Jahresumsatz 50 Mio. EUR und/oder Jahresbilanzsumme 10 Mio. EUR nicht überschreiten, diese Anforderungen nicht erfüllen müssen. Bei der Bestimmung der Größe der Einrichtung ist es nicht von Bedeutung, ob das betreffende Unternehmen ausschließlich digitale Dienste im Sinne der NIS-Richtlinie oder auch andere Dienste erbringt.

5. Verhältnis zwischen der NIS-Richtlinie und anderen Rechtsvorschriften

In diesem Abschnitt liegt der Schwerpunkt auf der *Lex-specialis*-Bestimmung gemäß Artikel 1 Absatz 7 der NIS-Richtlinie und es werden drei bisher von der Kommission geprüfte Beispiele für die *Lex specialis* erörtert. Außerdem werden die für Telekommunikations- und Vertrauensdiensteanbieter geltenden Sicherheitsanforderungen und Meldepflichten erläutert.

[38] Siehe insbesondere Artikel 18 dieser Richtlinie.
[39] ABl. L 24 vom 20.5.2003, S. 36.

5.1. NIS-Richtlinie, Artikel 1 Absatz 7: Die *Lex-specialis*-Bestimmung

Gemäß Artikel 1 Absatz 7 der NIS-Richtlinie finden die Bestimmungen über die Sicherheitsanforderungen und/oder die Meldepflichten für die Anbieter digitaler Dienste oder die Betreiber wesentlicher Dienste gemäß der Richtlinie keine Anwendung, sofern sektorspezifische Rechtsvorschriften für Sicherheitsanforderungen und/oder Meldepflichten gelten, die in ihrer Wirkung den in der NIS-Richtlinie enthaltenen Pflichten mindestens gleichwertig sind. Die Mitgliedstaaten müssen Artikel 1 Absatz 7 bei der allgemeinen Umsetzung der Richtlinie Rechnung tragen und der Kommission Informationen über die Anwendung der *Lex-specialis*-Bestimmung übermitteln.

Methode

Bei der Bewertung der Gleichwertigkeit sektorspezifischer EU-Rechtsvorschriften mit den einschlägigen Bestimmungen der NIS-Richtlinie sollte der Frage, ob die Sicherheitsanforderungen in den sektorspezifischen Rechtsvorschriften Maßnahmen zur Gewährleistung der Sicherheit von Netz- und Informationssystemen gemäß Artikel 4 Nummer 2 der Richtlinie umfassen, besondere Bedeutung beigemessen werden.

Im Hinblick auf die Meldepflichten ist in Artikel 14 Absatz 3 und Artikel 16 Absatz 3 der NIS-Richtlinie vorgesehen, dass Betreiber wesentlicher Dienste und Anbieter digitaler Dienste der zuständigen Behörde oder dem CSIRT Sicherheitsvorfälle, die erhebliche Auswirkungen auf die Bereitstellung ihrer Dienste haben, unverzüglich melden. Hier muss insbesondere darauf geachtet werden, dass die Meldungen der Betreiber wesentlicher Dienste bzw. Anbieter digitaler Dienste Informationen enthalten müssen, die es der zuständigen Behörde oder dem CSIRT ermöglichen, zu bestimmen, ob der Sicherheitsvorfall grenzübergreifende Auswirkungen hat.

Derzeit gibt es keine sektorspezifischen Rechtsvorschriften für die Kategorie der Anbieter digitaler Dienste, die mit den Vorgaben des Artikels 16 der NIS-Richtlinie vergleichbare Sicherheitsanforderungen und Meldepflichten vorsehen, die im Rahmen der Anwendung von Artikel 1 Absatz 7 der NIS-Richtlinie in Erwägung gezogen werden könnten[40].

Im Hinblick auf die Betreiber wesentlicher Dienste unterliegen derzeit der Finanzsektor sowie insbesondere die in Anhang II Nummern 4 und 5 genannten Sektoren Bankwesen und Finanzmarktinfrastrukturen Sicherheitsanforderungen und/oder Meldepflichten, die sich aus sektorspezifischen EU-Rechtsvorschriften ergeben. Dies ist auf die Tatsache zurückzuführen, dass die Sicherheit und Solidität der IT-, Netz- und Informationssysteme von Finanzinstituten ein wesentlicher Bestandteil der Eigenmittelanforderungen für das operationelle Risiko sind, die Finanzinstituten mit den EU-Rechtsvorschriften auferlegt wurden.

Beispiele

i) Zweite Zahlungsdiensterichtlinie

[40] Dies gilt unbeschadet der Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde gemäß Artikel 33 der Datenschutz-Grundverordnung.

In Bezug auf den Bankensektor, insbesondere was die Bereitstellung von Zahlungsdiensten durch Kreditinstitute im Sinne von Artikel 4 Nummer 1 der Verordnung (EU) Nr. 575/2013 betrifft, enthält die so genannte zweite Zahlungsdiensterichtlinie[41] (Payment Services Directive 2, PSD2) in den Artikeln 95 und 96 Sicherheitsanforderungen und Meldepflichten.

Genauer gesagt müssen Zahlungsdienstleister gemäß Artikel 95 Absatz 1 angemessene Risikominderungsmaßnahmen und Kontrollmechanismen zur Beherrschung der operationellen und der sicherheitsrelevanten Risiken im Zusammenhang mit den von ihnen erbrachten Zahlungsdiensten ergreifen. Diese Maßnahmen umfassen die Festlegung und Anwendung wirksamer Verfahren für das Management von Vorfällen – auch zur Aufdeckung und Klassifizierung schwerer Betriebs- und Sicherheitsvorfälle. Die Art dieser Sicherheitsmaßnahmen wird in den Erwägungsgründen 95 und 96 der PSD2 weiter präzisiert. Aus diesen Bestimmungen geht hervor, dass die vorgeschriebenen Maßnahmen auf die Beherrschung der Risiken im Zusammenhang mit den zur Bereitstellung von Zahlungsdiensten verwendeten Netz- und Informationssystemen ausgerichtet sind. Diese Sicherheitsanforderungen können daher als in ihrer Wirkung den entsprechenden Vorgaben von Artikel 14 Absätze 1 und 2 der NIS-Richtlinie mindestens gleichwertig betrachtet werden.

In Bezug auf die Meldepflichten ist in Artikel 96 Absatz 1 der PSD2 vorgesehen, dass die Zahlungsdienstleister im Falle eines schwerwiegenden Sicherheitsvorfalls unverzüglich die zuständige Behörde unterrichten. Ferner ist die zuständige Behörde gemäß Artikel 96 Absatz 2 der PSD2 – vergleichbar mit Artikel 14 Absatz 5 der NIS-Richtlinie – verpflichtet, die zuständigen Behörden anderer Mitgliedstaaten über den Vorfall zu unterrichten, sofern dieser für sie relevant ist. Diese Verpflichtung bedeutet gleichzeitig, dass die Meldung des Sicherheitsvorfalls Informationen umfassen muss, die es der zuständigen Behörde gestatten, die grenzüberschreitenden Auswirkungen eines Vorfalls zu beurteilen. Gemäß Artikel 96 Absatz 3 Buchstabe a der PSD2 ist die EBA in Zusammenarbeit mit der EZB in diesem Zusammenhang ermächtigt, Leitlinien über den genauen Inhalt und das Format der Meldung herauszugeben.

Daraus folgt gemäß Artikel 1 Absatz 7 der NIS-Richtlinie, dass für die Bereitstellung von Zahlungsdiensten durch Kreditinstitute die Sicherheitsanforderungen und Meldepflichten gemäß den Artikel 95 und 96 der PSD2 anstelle der entsprechenden Vorschriften des Artikels 14 der NIS-Richtlinie gelten sollten.

ii) Verordnung (EU) Nr. 648/2012 des Europäischen Parlaments und des Rates vom 4. Juli 2012 über OTC-Derivate, zentrale Gegenparteien und Transaktionsregister

Die Verordnung (EU) Nr. 648/2012 in Verbindung mit der Delegierten Verordnung (EU) Nr. 153/2013 enthält Vorschriften im Hinblick auf Finanzmarktinfrastrukturen für Sicherheitsanforderungen an zentrale Gegenparteien (central counterparties, CCP), die als *Lex*

[41] Richtlinie (EU) 2015/2366 (ABl. L 337 vom 23.12.2015, S. 35).

specialis angesehen werden können. Insbesondere sind in den Rechtsakten technische und organisatorische Maßnahmen im Hinblick auf die Sicherheit der Netz- und Informationssysteme vorgesehen, die im Detail sogar über die Anforderungen von Artikel 14 Absätze 1 und 2 der NIS-Richtlinie hinausgehen, sodass davon ausgegangen werden kann, dass die Vorgaben von Artikel 1 Absatz 7 der NIS-Richtlinie in Bezug die Sicherheitsanforderungen erfüllt sind.

Im Einzelnen muss eine Einrichtung gemäß Artikel 26 Absatz 1 der Verordnung (EU) Nr. 648/2012 „*über solide Regelungen zur Unternehmensführung verfügen, wozu eine klare Organisationsstruktur mit genau abgegrenzten, transparenten und kohärenten Verantwortungsbereichen, wirksamen Ermittlungs-, Steuerungs-, Überwachungs- und Berichterstattungsverfahren für die Risiken, denen sie ausgesetzt ist oder ausgesetzt sein könnte, sowie angemessene interne Kontrollmechanismen einschließlich solider Verwaltungs- und Rechnungslegungsverfahren zählen*". Gemäß Artikel 26 Absatz 3 muss die Organisationsstruktur mithilfe angemessener und verhältnismäßiger Systeme, Ressourcen und Verfahren die Verfügbarkeit und das ordnungsgemäße Funktionieren der Dienstleistungen und Tätigkeiten sicherstellen.

Des Weiteren stellt Artikel 26 Absatz 6 klar, dass eine CCP „*informationstechnische Systeme (betreiben muss), die der Komplexität, der Vielfalt und der Art ihrer Dienstleistungen und Tätigkeiten angemessen sind, so dass hohe Sicherheitsstandards und die Integrität und Vertraulichkeit der Informationen gewahrt sind*". Darüber hinaus schreibt Artikel 34 Absatz 1 die Festlegung, Umsetzung und Befolgung einer angemessenen Strategie zur Fortführung des Geschäftsbetriebs sowie eines Notfallwiederherstellungsplans vor, durch die eine rechtzeitige Wiederherstellung des Geschäftsbetriebs gewährleistet sein sollte.

Diese Verpflichtungen werden in der Delegierten Verordnung (EU) Nr. 153/2013 der Kommission vom 19. Dezember 2012 zur Ergänzung der Verordnung (EU) Nr. 648/2012 des Europäischen Parlaments und des Rates in Bezug auf technische Regulierungsstandards für Anforderungen an zentrale Gegenparteien[42] weiter ausgeführt. Insbesondere erlegt Artikel 4 der CCP die Verpflichtung auf, angemessene Instrumente für das Risikomanagement zu entwickeln, die die Steuerung und Meldung aller einschlägigen Risiken ermöglichen, präzisiert die Art der Maßnahmen (z. B. Unterhaltung solider Informations- und Risikokontrollsysteme, Verfügbarkeit von Ressourcen und Fachkenntnissen sowie Zugang zu allen einschlägigen Informationen für die Risikomanagementfunktion, Verfügbarkeit angemessener Mechanismen der internen Kontrolle wie solide Verwaltungs- und Rechnungslegungsverfahren, um die CCP bei der Überwachung und Bewertung der Angemessenheit und Wirksamkeit ihrer Grundsätze, Verfahren und Systeme des Risikomanagements zu unterstützen).

Darüber hinaus nimmt Artikel 9 ausdrücklich Bezug auf die Sicherheit der informationstechnischen Systeme und sieht konkrete technische und organisatorische Maßnahmen im Zusammenhang mit der Aufrechterhaltung eines robusten Rahmens zur

[42] ABl. L 52 vom 23.2.2013, S. 41.

Steuerung des Informationssicherheitsrisikos vor. Solche Maßnahmen sollten auch Mechanismen und Verfahren umfassen, um die Verfügbarkeit der Dienste sowie den Schutz der Authentizität, Integrität und Vertraulichkeit von Daten zu gewährleisten.

iii) Richtlinie 2014/65/EU des Europäischen Parlaments und des Rates vom 15. Mai 2014 über Märkte für Finanzinstrumente sowie zur Änderung der Richtlinien 2002/92/EG und 2011/61/EU[43]

Im Hinblick auf Handelsplätze müssen Betreiber gemäß Artikel 48 Absatz 1 der Richtlinie 2014/65/EU im Fall von Störungen in ihren Handelssystemen die Kontinuität ihres Geschäftsbetriebs gewährleisten. Diese allgemeine Verpflichtung wurde kürzlich weiter spezifiziert und durch die Delegierte Verordnung (EU) 2017/584 vom 14. Juli 2016 zur Ergänzung der Richtlinie 2014/65/EU des Europäischen Parlaments und des Rates durch technische Regulierungsstandards zur Festlegung der organisatorischen Anforderungen an Handelsplätze[44] ergänzt[45]. Insbesondere sieht Artikel 23 Absatz 1 dieser Verordnung vor, dass Handelsplätze über Verfahren und Vorkehrungen zur Gewährleistung der physischen und elektronischen Sicherheit verfügen müssen, die ihre Systeme vor Missbrauch und unberechtigtem Zugriff schützen und die Integrität der Daten wahren. Diese Maßnahmen sollten die Verhütung oder Minimierung des Risikos von Angriffen auf ihre Informationssysteme ermöglichen.

Ferner sollten die Maßnahmen und Vorkehrungen der Betreiber gemäß Artikel 23 Absatz 2 eine umgehende Erkennung und Steuerung des Risikos im Zusammenhang mit etwaigen unberechtigten Zugriffen, schweren Behinderungen oder Störungen des Betriebs eines Informationssystems und Eingriffen in Daten, die Verfügbarkeit, Integrität oder die Authentizität der Daten beeinträchtigen, zulassen. Darüber hinaus müssen Handelsplätze gemäß Artikel 15 der Verordnung über wirksame Notfallvorkehrungen verfügen, die eine hinreichenden Stabilität des Systems und die Bewältigung von Störungen gewährleisten. Insbesondere sollten diese Maßnahmen dem Betreiber die Wiederaufnahme des Handels innerhalb von zwei Stunden oder einer geringfügig längeren Frist erlauben und gleichzeitig sicherstellen, dass der Datenverlust nahezu null beträgt.

In Artikel 16 heißt es weiter, dass die zum Umgang mit Störungen und ihrer Bewältigung festgelegten Maßnahmen Teil des Plans Notfallplans der Handelsplätze sein und bestimmte Elemente beinhalten sollten, die der Betreiber bei der Annahme des Notfallplans zu berücksichtigen hat (z. B. Einrichtung eines speziellen Sicherheitsteams, die Durchführung einer Folgenabschätzung über die Risiken, die regelmäßig überprüft wird).

In Anbetracht ihres Inhalts dienen diese Sicherheitsmaßnahmen offenbar der Steuerung und Bewältigung der Risiken im Zusammenhang mit der Verfügbarkeit, Authentizität, Integrität und Vertraulichkeit der Daten oder erbrachten Dienste. Daraus lässt sich schließen, dass die

[43] ABl. L 173 vom 12.6.2014, S. 349.
[44] ABl. L 87 vom 31.3.2017, S. 350.
[45] http://ec.europa.eu/finance/securities/docs/isd/mifid/rts/160714-rts-7_de.pdf

genannten sektorspezifischen EU-Rechtsvorschriften Sicherheitsanforderungen enthalten, die in ihrer Wirkung den entsprechenden Vorgaben des Artikels 14 Absätze 1 und 2 der NIS-Richtlinie mindestens gleichwertig sind.

5.2 NIS-Richtlinie, Artikel 1 Absatz 3: Telekommunikationsanbieter und Vertrauensdiensteanbieter

Gemäß Artikel 1 Absatz 3 gelten die in der Richtlinie vorgesehenen Sicherheitsanforderungen und Meldepflichten nicht für Anbieter, die den Anforderungen der Artikel 13a und 13b der Richtlinie 2002/21/EG unterliegen. Artikel 13a und 13b der Richtlinie 2002/21/EG gelten für Unternehmen, die öffentliche Kommunikationsnetze oder öffentlich zugängliche elektronische Kommunikationsdienste bereitstellen. Was also die Bereitstellung öffentlicher Kommunikationsnetze oder öffentlich zugänglicher elektronischer Kommunikationsdienste betrifft, so müssen die Unternehmen den Sicherheitsanforderungen und Meldepflichten gemäß der Richtlinie 2002/21/EG entsprechen.

Stellt dasselbe Unternehmen jedoch auch andere Dienste wie z. B. digitale Dienste (z. B. Cloud-Computing-Dienste oder Online-Marktplätze) gemäß Anhang III der NIS-Richtlinie oder Dienste wie die DNS oder IXP gemäß Anhang II Nummer 7 der NIS-Richtlinie bereit, unterliegt das Unternehmen hinsichtlich der Bereitstellung dieser spezifischen Dienste den Sicherheitsanforderungen und Meldepflichten der NIS-Richtlinie. Es sei darauf hingewiesen, dass die Mitgliedstaaten aufgrund der Tatsache, dass es sich bei den Diensteanbietern gemäß Anhang II Nummer 7 um Betreiber wesentlicher Dienste handelt, ein Ermittlungsverfahren gemäß Artikel 5 Absatz 2 durchführen und ermitteln müssen, welche einzelnen Anbieter von DNS-, IXP- oder TLD-Diensten den Anforderungen der NIS-Richtlinie entsprechen sollten. Dies bedeutet, dass im Anschluss an eine solche Bewertung nur jene Anbieter von DNS, IXP oder TLD, die die Kriterien des Artikels 5 Absatz 2 der NIS-Richtlinie erfüllen, zur Einhaltung der Anforderungen dieser Richtlinie verpflichtet sind.

In Artikel 1 Absatz 3 wird ferner präzisiert, dass die Sicherheitsanforderungen und Meldepflichten der Richtlinie auch für Vertrauensdiensteanbieter, die ähnlichen Anforderungen gemäß Artikel 19 der Verordnung (EU) Nr. 910/2014 unterliegen, nicht gelten.

6. Veröffentliche nationale Cybersicherheitsstrategien

	Mitgliedstaat	Titel der Strategie und verfügbare Links
1	Österreich	*Austrian Cybersecurity Strategy* (Österreichische Strategie für Cyber Sicherheit, 2013) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/AT_NCSS.pdf (EN)
2	Belgien	*Securing Cyberspace* (Sicherung des Cyberspace, 2012) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/ncss-be-fr (FR)
3	Bulgarien	*Киберустойчива България 2020* (Ein gegenüber Cyberattacken standhaftes Bulgarien 2020, 2016) http://www.cyberbg.eu/ (BG)
4	Kroatien	*The national cyber security strategy of the republic of Croatia* (Die nationale Cybersicherheitsstrategie der Republik Kroatien, 2015) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/CRNCSSEN.pdf (EN)
5	Tschechische Republik	*National cyber security strategy of the Czech Republic for the period from 2015 to 2020* (Nationale Cybersicherheitsstrategie der Tschechischen Republik für den Zeitraum 2015–2020, 2015) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/CzechRepublic_Cyber_Security_Strategy.pdf (EN)
6	Zypern	*Cybersecurity Strategy of the Republic of Cyprus* (Cybersicherheitsstrategie der Republik Zypern, 2012) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/CybersecurityStrategyoftheRepublicofCyprusv10_English.pdf (EN)
7	Dänemark	*The Danish Cyber and Information Security Strategy* (Die dänische Cyber- und Informationssicherheitsstrategie, 2015) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/DK_NCSS.pdf (EN)
8	Estland	*Cyber Security Strategy* (Cybersicherheitsstrategie, 2014) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Estonia_Cyber_security_Strategy.pdf (EN)
9	Finnland	*Finland´s Cyber security Strategy* (Finnlands Cybersicherheitsstrategie, 2013) https://www.enisa.europa.eu/topics/national-cyber-security-

		strategies/ncss-map/FinlandsCyberSecurityStrategy.pdf (EN)
10	Frankreich	*French national digital security strategy* (Nationale französische Strategie für digitale Sicherheit, 2015) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/France_Cyber_Security_Strategy.pdf (EN)
11	Irland	*National Cyber Security Strategy 2015-2017* (Nationale Cybersicherheitsstrategie 2015–2017, 2015) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/NCSS_IE.pdf (EN)
12	Italien	*National Strategic Framework for Cyberspace Security* (Nationaler strategischer Rahmen für Sicherheit im Cyberspace, 2013) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/IT_NCSS.pdf (EN)
13	Deutschland	*Cyber-Sicherheitsstrategie für Deutschland* (2016) http://www.bmi.bund.de/SharedDocs/Downloads/DE/Themen/ModerneVerwaltung-OeffentlicherDienst/Informationsgesellschaft/cybersicherheitsstrategie-2016.pdf?__blob=publicationFile (DE)
14	Ungarn	*National Cyber Security Strategy of Hungary* (Nationale Cybersicherheitsstrategie Ungarns, 2013) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/HU_NCSS.pdf (EN)
15	Lettland	*Cyber Security Strategy of Latvia 2014–2018* (Cybersicherheitsstrategie Lettlands 2014–2018, 2014) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/lv-ncss (EN)
16	Litauen	*The programme for the development of electronic information security (cyber-security) for 2011–2019* (Programm für die Entwicklung der Sicherheit elektronischer Informationen (Cybersicherheit) für den Zeitraum 2011–2019, 2011) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Lithuania_Cyber_Security_Strategy.pdf (EN)
17	Luxemburg	*National Cybersecurity Strategy II (Nationale Cybersicherheitsstrategie II, 2015)* https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Luxembourg_Cyber_Security_strategy.pdf (EN)
18	Malta	*National Cyber Security Strategy Green Paper* (Grünbuch zur nationalen Cybersicherheitsstrategie, 2015) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/NCSSGreenPaper.pdf (EN)

19	Niederlande	*National Cyber Security Strategy 2* (Nationale Cybersicherheitsstrategie 2, 2013) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/NCSS2Engelseversie.pdf (EN)
20	Polen	*Cyberspace Protection Policy of the Republic of Poland* (Strategie der Republik Polen zum Schutz des Cyberspace, 2013) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/copy_of_PO_NCSS.pdf (EN)
21	Rumänien	*Strategiei de securitate cibernetică a României* (Die Cybersicherheitsstrategie Rumäniens, 2011) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/StrategiaDeSecuritateCiberneticaARomaniei.pdf (RO)
22	Portugal	*Portuguese National Cyberspace Security Strategy* (Nationale portugiesische Cybersicherheitsstrategie, 2015) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/portuguese-national-cyber-security-strategy/view (EN)
23	Slowakische Republik	*Cyber Security Concept of the Slovak Republic for 2015–2020* (Cybersicherheitskonzept der Slowakischen Republik für den Zeitraum 2015–2020, 2015) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/cyber-security-concept-of-the-slovak-republic-1 (EN)
24	Slowenien	*Cyber Security Strategy establishing a system to ensure a high level of cyber security* (Cybersicherheitsstrategie zum Aufbau eines hohen Cybersicherheitsniveaus, 2016) http://www.uvtp.gov.si/fileadmin/uvtp.gov.si/pageuploads/Cyber_Security_Strategy_Slovenia.pdf (EN)
25	Spanien	*National Cyber Security Strategy* (Nationale Cybersicherheitsstrategie, 2013) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/NCSS_ESen.pdf (EN)
26	Schweden	*A National Cybersecurity Strategy* (Eine nationale Cybersicherheitsstrategie, 2017) http://www.government.se/49edf4/contentassets/b5f956be6c50412188fb4e1d72a5e501/fact-sheet-a-national-cyber-security-strategy.pdf (EN)
27	Vereinigtes Königreich	*National Cyber Security Strategy 2016–2021* (Nationale Cybersicherheitsstrategie 2016–2021, 2016) https://www.enisa.europa.eu/topics/national-cyber-security-

strategies/ncss-map/national_cyber_security_strategy_2016.pdf (EN)

7. Liste der von der ENISA veröffentlichten bewährten Verfahren und Empfehlungen

Zur Reaktion auf Sicherheitsvorfälle

- ✓ Strategies for Incident Response and Cyber Crisis Cooperation (Reaktionsstrategien und Zusammenarbeit im Fall von Cyberkrisen)[46]

Zur Bewältigung von Sicherheitsvorfällen

- ✓ Projekt zur automatisierten Bewältigung von Sicherheitsvorfällen[47]
- ✓ Good Practice Guide for Incident Management (Leitfaden der bewährten Verfahren für den Umgang mit Sicherheitsvorfällen)[48]

Zur Einstufung von Sicherheitsvorfällen und Schemata

- ✓ Überblick über bestehende Schemata[49]
- ✓ Leitfaden für gute Praxis bei der Verwendung von Schemata im Bereich der Verhütung und Aufdeckung von Vorfällen[50]

Zur Ausgereiftheit von CSIRTs

- ✓ Challenges for National CSIRTs in Europe in 2016: Study on CSIRT Maturity (Herausforderungen für nationale CSIRTs in Europa im Jahr 2016: Studie zur Ausgereiftheit von CSIRTs)[51]
- ✓ Study on CSIRT Maturity – Evaluation Process (Studie zur Ausgereiftheit von CSIRTs – Bewertungsverfahren)[52]
- ✓ Leitlinien zur Bewertung der Ausgereiftheit von nationalen und staatlichen CSIRTs[53]

Zu Kapazitätsaufbau und Schulungsmaßnahmen für CSIRTs

- ✓ Leitfaden der bewährten Verfahren für Schulungsmethoden[54]

---

[46] ENISA, *Strategies for Incident Response and Cyber Crisis Cooperation*, 2016. Abrufbar unter:https://www.enisa.europa.eu/publications/strategies-for-incident-response-and-cyber-crisis-cooperation
[47] Weitere Informationen: https://www.enisa.europa.eu/topics/csirt-cert-services/community-projects/incident-handling-automation
[48] ENISA, *Good Practice Guide for Incident Management*, 2010. Abrufbar unter:https://www.enisa.europa.eu/publications/good-practice-guide-for-incident-management
[49] Weitere Informationen: https://www.enisa.europa.eu/topics/csirt-cert-services/community-projects/existing-taxonomies
[50] ENISA, *A good practice guide of using taxonomies in incident prevention and detection* (2017). Abrufbar unter:https://www.enisa.europa.eu/publications/using-taxonomies-in-incident-prevention-detection
[51] ENISA, *Challenges for National CSIRTs in Europe in 2016: Study on CSIRT Maturity*, 2017. Abrufbar unter:https://www.enisa.europa.eu/publications/study-on-csirt-maturity
[52] ENISA, *Study on CSIRT Maturity – Evaluation Process*, 2017. Abrufbar unter:https://www.enisa.europa.eu/publications/study-on-csirt-maturity-evaluation-process
[53] ENISA, CSIRT Capabilities. *How to assess maturity? Guidelines for national and governmental CSIRTs*, 2016. Abrufbar unter: https://www.enisa.europa.eu/publications/csirt-capabilities
[54] ENISA, *Good Practice Guide on Training Methodologies*, 2014. Abrufbar unter:https://www.enisa.europa.eu/publications/good-practice-guide-on-training-methodologies

Weitere Informationen über bestehende CSIRTs in Europa: Überblick über CSIRTs nach Mitgliedstaaten[55]

[55] Weitere Informationen: https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-inventory/certs-by-country-interactive-map