EUROPÄISCHE
KOMMISSION

Brüssel, den 4.10.2017
COM(2017) 476 final

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

MITTEILUNG DER KOMMISSION AN DAS EUROPÄISCHE 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

Einleitung

Bei der am 6. Juli 2016 angenommenen Richtlinie (EU) 2016/1148 über die Sicherheit von Netz- und Informationssystemen in der Union[1] (im Folgenden die „NIS-Richtlinie“ oder die „Richtlinie“) handelt es sich um die ersten horizontalen Rechtsvorschriften zur Bewältigung von Herausforderungen der Cybersicherheit. Für die Abwehrfähigkeit gegenüber Cyberangriffen und die Zusammenarbeit in Europa stellt sie einen entscheidenden Wendepunkt dar.

Mit der Richtlinie werden drei Hauptziele verfolgt:

- Stärkung der Kapazitäten der Mitgliedstaaten im Bereich der Cybersicherheit;
- Ausbau der Zusammenarbeit auf EU-Ebene und
- Förderung einer Kultur des Risikomanagements und der Meldung von Sicherheitsvorfällen bei zentralen Wirtschaftsakteuren, insbesondere bei Betreibern wesentlicher Dienste für die Aufrechterhaltung gesellschaftlicher oder wirtschaftlicher Tätigkeiten und bei Anbietern digitaler Dienste.

Die NIS-Richtlinie ist ein Eckstein der Antwort der EU auf die zunehmenden Cyberbedrohungen und -herausforderungen, die mit der Digitalisierung unseres wirtschaftlichen und gesellschaftlichen Lebens einhergehen, und ihre Umsetzung ist somit ein wesentlicher Teil des am 13. September 2017 vorgelegten Cybersicherheitspakets. Solange die NIS-Richtlinie noch nicht in allen Mitgliedstaaten vollständig umgesetzt ist, geht dies zu Lasten der Wirksamkeit der Antwort der Europäischen Union. Auch in der Mitteilung der Kommission „Stärkung der Abwehrfähigkeit Europas im Bereich der Cybersicherheit“[2] aus dem Jahr 2016 wurde dies als entscheidendes Problem identifiziert.

Angesichts der Neuartigkeit der NIS-Richtlinie und der Dringlichkeit, mit der die sich rasch wandelnden Cyberbedrohungen angegangen werden müssen, verdienen die Herausforderungen, mit denen alle Akteure bei der fristgerechten und erfolgreichen Umsetzung der Richtlinie konfrontiert sind, besondere Aufmerksamkeit. So hat die Kommission mit Blick auf die Frist für die Umsetzung bis zum 9. Mai 2018 bzw. bis zum 9. November 2018 für die Ermittlung der Betreiber wesentlicher Dienste den Umsetzungsprozess in den Mitgliedstaaten sowie deren Arbeiten in der Kooperationsgruppe fortlaufend unterstützt.

Die vorliegende Mitteilung und ihr Anhang basieren auf den Vorarbeiten und der Analyse der Kommission im Zusammenhang mit der bisherigen Umsetzung der NIS-Richtlinie, auf den Beiträgen der Europäischen Agentur für Netz- und Informationssicherheit (ENISA) und auf den Erörterungen mit den Mitgliedstaaten in der Umsetzungsphase der Richtlinie, vor allem

[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.

[2] COM(2016) 410 final.

im Rahmen der Kooperationsgruppe[3]. Diese Mitteilung ergänzt die bisherigen Bemühungen insbesondere durch

- die intensiven Arbeiten der Kooperationsgruppe, die sich auf einen Arbeitsplan geeinigt hat, der sich in erster Linie auf die Umsetzung der NIS-Richtlinie und insbesondere auf die Frage der Ermittlung von Betreibern wesentlicher Dienste und ihrer Verpflichtungen hinsichtlich der Sicherheitsanforderungen und Meldungen von Sicherheitsvorfällen konzentriert. Wenngleich die Richtlinie bei der Umsetzung der Bestimmungen in Bezug auf die Betreiber wesentlicher Dienste einen Ermessensspielraum gewährt, erkannten die Mitgliedstaaten, wie wichtig ein diesbezüglich harmonisierter Ansatz[4] ist.
- den Aufbau und schnellen Betrieb des Netzwerks der Computer-Notfallteams der Mitgliedstaaten (CSIRT) im Einklang mit Artikel 12 Absatz 1 der Richtlinie. Seitdem hat dieses Netzwerk begonnen, die Grundlagen für eine strukturierte operative Zusammenarbeit auf europäischer Ebene zu legen.

Sowohl für die politischen als auch für die operativen Ebenen, die durch diese beiden Strukturen vertreten werden, ist es von wesentlicher Bedeutung, dass sich alle Mitgliedstaaten umfassend dafür einsetzen, das Ziel eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union zu erreichen.

Diese Mitteilung und ihr Anhang sollen diese Bemühungen unterstützen, indem die für die Umsetzung der Richtlinie relevanten bewährten Verfahren der Mitgliedstaaten zusammengetragen und miteinander verglichen werden und Leitlinien für die Umsetzung der Richtlinie sowie ausführlichere Erläuterungen bestimmter Vorschriften an die Hand gegeben werden. Übergeordnetes Ziel ist es, den Mitgliedstaaten dabei zu helfen, die NIS-Richtlinie unionsweit wirksam und einheitlich umzusetzen.

Eine weitere Ergänzung dieser Mitteilung bildet die anstehende Durchführungsverordnung der Kommission zur weiteren Spezifizierung von Elementen und Parametern bezüglich der von den Anbietern digitaler Dienste nach Artikel 16 Absatz 8 der NIS-Richtlinie zu erfüllenden Anforderungen an die Sicherheit und die Meldung von Sicherheitsvorfällen. Die Durchführungsverordnung[5] soll die Umsetzung der Richtlinie bezüglich der Pflichten von Betreibern digitaler Dienste erleichtern.

---

[3] Ein Mechanismus für die strategische Zusammenarbeit zwischen den Mitgliedstaaten im Rahmen der NIS-Richtlinie, Artikel 11.

[4] Die Kooperationsgruppe arbeitet derzeit an Leitfäden für unter anderem die Kriterien für die Ermittlung der Kritikalität eines Betreibers gemäß Artikel 5 Absatz 2 der Richtlinie, die Umstände, unter denen die Betreiber wesentlicher Dienste Sicherheitsvorfälle gemäß Artikel 14 Absatz 7 der Richtlinie melden müssen, und die Sicherheitsanforderungen für Betreiber wesentlicher Dienste im Einklang mit Artikel 14 Absätze 1 und 2.

[5] Der Entwurf der Durchführungsverordnung kann eingesehen werden unter: https://ec.europa.eu/info/law/better-regulation/have-your-say_en.

Die Mitteilung enthält die wichtigsten Schlussfolgerungen aus der Analyse der Fragen, die mit Blick auf die Umsetzung in nationales Recht als wichtige Bezugspunkte und mögliche Ansätze gelten. Der wichtigste Schwerpunkt liegt hier auf Vorschriften, die die Kapazitäten und Pflichten der Mitgliedstaaten in Bezug auf in den Anwendungsbereich der Richtlinie fallende Einrichtungen betreffen. Der Anhang enthält eine genauere Prüfung der Bereiche, in denen praktische Umsetzungsleitlinien nach Ansicht der Kommission den größten Nutzen bieten, indem bestimmte Vorschriften der Richtlinie erläutert und ausgelegt und die bisherigen bewährten Verfahren und Erfahrungen mit der Richtlinie dargelegt werden.

Auf dem Weg zu einer wirksamen Umsetzung der NIS-Richtlinie

Das Ziel der NIS-Richtlinie besteht darin, ein hohes gemeinsames Sicherheitsniveau von Netz- und Informationssystemen in der EU zu erreichen. Hierbei geht es um die Erhöhung der Sicherheit des Internets und der privaten Netz- und Informationssysteme, die für das Funktionieren unserer Gesellschaft und Wirtschaft unverzichtbar sind. Das erste wichtige Element in diesem Zusammenhang ist die Abwehrbereitschaft der Mitgliedstaaten, die nach Maßgabe der Richtlinie durch nationale Cybersicherheitsstrategien sowie die Arbeiten der Computer-Notfallteams (CSIRT) und der zuständigen nationalen Behörden sichergestellt werden sollte.

Umfang der nationalen Strategien

Es ist wichtig, dass die Mitgliedstaaten bei der Umsetzung der NIS-Richtlinie von der Gelegenheit Gebrauch machen, ihre nationale Cybersicherheitsstrategie unter den Gesichtspunkten Schwachstellen, bewährte Vorgehensweisen und neue Herausforderungen, die Gegenstand des Anhangs sind, zu prüfen.

Während sich die Richtlinie auf Unternehmen und Dienste von entscheidender Bedeutung konzentriert, ist es angesichts der zunehmenden Abhängigkeit von der Informations- und Kommunikationstechnik notwendig, die Cybersicherheit in Wirtschaft und Gesellschaft ganzheitlich und konsequent anzugehen. Daher würde die Annahme umfassender nationaler Strategien, die über die Mindestanforderungen der NIS-Richtlinie (d. h. über die in Anhang II bzw. Anhang III der Richtlinie aufgelisteten Sektoren und Dienste) hinausgehen, das Sicherheitsniveau von Netz- und Informationssystemen insgesamt erhöhen.

Da es sich bei der Cybersicherheit noch um einen verhältnismäßig neuen und rasch wachsenden Politikbereich handelt, bedarf es meist neuer Investitionen, auch wenn die Gesamtsituation der öffentlichen Finanzen Kürzungen und Einsparungen verlangt. Für die Verwirklichung der Ziele der Richtlinie kommt es daher darauf an, ehrgeizige Beschlüsse zu fassen, um die für die wirksame Umsetzung der nationalen Strategien unerlässliche finanzielle und personelle Ausstattung, auch der nationalen Behörden und der CSIRT, sicherzustellen.

Wirksamkeit der Um- und Durchsetzung

Die Notwendigkeit, zuständige nationale Behörden bzw. zentrale Anlaufstellen zu benennen, wird in Artikel 8 der Richtlinie behandelt und ist ein wesentliches Element für die wirksame

Umsetzung der NIS-Richtlinie und die grenzübergreifende Zusammenarbeit. In diesem Zusammenhang haben sich in den Mitgliedstaaten sowohl eher zentrale als auch dezentrale Ansätze entwickelt. Entscheidet sich ein Mitgliedstaat für einen eher dezentralen Ansatz bei der Benennung der zuständigen nationalen Behörden, gilt es, solide Kooperationsvereinbarungen zwischen zahlreichen Behörden und der zentralen Anlaufstelle zu treffen (*siehe Tabelle 1, Abschnitt 3.2 des Anhangs*). Dies verbessert die Wirksamkeit der Umsetzung und erleichtert die Durchsetzung.

Frühere Erfahrungen beim Schutz kritischer Informationsinfrastrukturen (CIIP) können dabei helfen, ein optimales Regelungsmodell für die Mitgliedstaaten zu entwerfen, das sowohl eine wirksame sektorale Umsetzung der NIS-Richtlinie als auch einen kohärenten horizontalen Ansatz (*siehe Abschnitt 3.1. des Anhangs*) gewährleistet.

Größere nationale CSIRT-Kapazitäten

Ohne eine effektive und angemessene Ressourcenausstattung der nationalen Computer-Notfallteams in der gesamten EU, wie in Artikel 9 der NIS-Richtlinie dargelegt ist, wird die EU weiterhin durch grenzübergreifende Cyberbedrohungen gefährdet sein. Die Mitgliedstaaten könnten es daher in Betracht ziehen, den Aktionsbereich der CSIRT über die im Anwendungsbereich der Richtlinie erfassten Sektoren und Dienste hinaus zu erweitern (*siehe Abschnitt 3.3 des Anhangs*). Die nationalen CSIRT könnten dadurch bei Sicherheitsvorfällen, die in Unternehmen und Organisationen, welche zwar nicht in den Anwendungsbereich der Richtlinie fallen, aber dennoch für die Gesellschaft und die Wirtschaft von Bedeutung sind, auftreten, eine operative Unterstützung bieten. Darüber hinaus könnten die Mitgliedstaaten zusätzliche Finanzierungsmöglichkeiten des Programms für die Netzsicherheit der Infrastrukturen für digitale Dienste im Rahmen der Fazilität „Connecting Europe“ (CEF), das die Kapazitäten der nationalen CSIRT und deren Zusammenarbeit stärken soll, umfassend in Anspruch nehmen (*siehe Abschnitt 3.5 des Anhangs*).

Kohärenz der Verfahren zur Ermittlung von Betreibern wesentlicher Dienste

Die Mitgliedstaaten müssen nach Artikel 5 der NIS-Richtlinie bis zum 9. November 2018 die Einrichtungen ermitteln, die als Betreiber wesentlicher Dienste anzusehen sind. Dabei könnten die Mitgliedstaaten in Betracht ziehen, die in dieser Mitteilung enthaltenen Definitionen und Leitlinien durchgängig anzuwenden, um sicherzustellen, dass ähnliche Einrichtungen mit einer ähnlichen Rolle im Binnenmarkt auch in anderen Mitgliedstaaten konsequent als Betreiber wesentlicher Dienste ermittelt werden. Angesichts der Rolle, die öffentliche Verwaltungen für die Gesellschaft und die Wirtschaft insgesamt spielen, könnten die Mitgliedstaaten außerdem erwägen, den Anwendungsbereich der NIS-Richtlinie auf diese auszudehnen (*siehe Abschnitte 2.1. und 4.1.3.des Anhangs).*

Es wäre sehr nützlich, die nationalen Ansätze für die Ermittlung von Betreibern wesentlicher Dienste unter Berücksichtigung der Leitlinien der Kooperationsgruppe (*siehe Abschnitt 4.1.2. des Anhangs*) so weit wie möglich aufeinander abzustimmen, da dies zu einer einheitlicheren Anwendung der Bestimmungen der Richtlinie führen und das Risiko einer Fragmentierung des Marktes verringern würde. In Fällen, in denen Betreiber wesentlicher Dienste diese wesentlichen Dienste in zwei oder mehr Mitgliedstaaten bereitstellen, ist es von entscheidender Bedeutung, dass sich die Mitgliedstaaten (im Rahmen der Konsultation nach Artikel 5 Absatz 4) auf die einheitliche Ermittlung von Einrichtungen einigen (*siehe Abschnitt 4.1.7. des Anhangs)*, sodass eine unterschiedliche regulatorische Behandlung von ein und derselben Einrichtung im Rahmen der verschiedenen Rechtssysteme der Mitgliedstaaten vermieden werden kann.

Übermittlung von Informationen über die Ermittlung von Betreibern wesentlicher Dienste an die Kommission

Nach Artikel 5 Absatz 7 sind die Mitgliedstaaten gehalten, der Kommission Informationen über die nationalen Maßnahmen zur Ermittlung der Betreiber wesentlicher Dienste zu übermitteln, ebenso wie die Liste der wesentlichen Dienste, die Zahl der ermittelten Betreiber wesentlicher Dienste und die Bedeutung der betreffenden Betreiber für den Sektor. Darüber hinaus müssen die Mitgliedstaaten Schwellenwerte, soweit vorhanden, mitteilen, die bei dem Ermittlungsprozess angewandt wurden, um den einschlägigen Versorgungsgrad oder die Bedeutung des betreffenden Betreibers für die Aufrechterhaltung eines einschlägigen Versorgungsgrads zu bestimmen. Die Mitgliedstaaten könnten außerdem erwägen, die Liste der ermittelten Betreiber wesentlicher Dienste, gegebenenfalls auf vertraulicher Basis, mit der Kommission zu teilen, da dies dazu beitragen würde, die Genauigkeit und die Qualität der Bewertung der Kommission zu verbessern (*siehe Abschnitte 4.1.5 und 4.1.6 des Anhangs*).

Abgestimmte Ansätze bezüglich der Anforderungen an die Sicherheit und die Meldung von Sicherheitsvorfällen für Betreiber wesentlicher Dienste

Was die Pflichten der Betreiber wesentlicher Dienste im Zusammenhang mit den Sicherheitsanforderungen und der Meldung von Sicherheitsvorfällen (Artikel 14 Absätze 1, 2 und 3) angeht, würde ein abgestimmter Ansatz in Bezug auf die Sicherheitsanforderungen und die Meldung von Sicherheitsvorfällen, der es den Betreibern wesentlicher Dienste erleichtern würde, länderübergreifend ihre Pflichten einzuhalten, einem Binnenmarkt im größtmöglichen Umfang förderlich sein. Als Referenz gilt hier nach wie vor die Arbeit an einem Leitfaden innerhalb der Kooperationsgruppe (*siehe Abschnitte 4.2 und 4.3 des Anhangs*).

Bei einem Cybersicherheitsvorfall großen Ausmaßes, von dem mehrere Mitgliedstaaten betroffen sind, ist es sehr wahrscheinlich, dass eine obligatorische Meldung von einem Betreiber wesentlicher Dienste oder von einem Anbieter digitaler Dienste nach Artikel 14 Absatz 3 bzw. Artikel 16 Absatz 3 ergeht oder eine freiwillige Meldung nach Artikel 20 Absatz 1 von einer anderen Einrichtung, die nicht in den Anwendungsbereich der Richtlinie fällt. Im Einklang mit der Empfehlung der Kommission für eine koordinierte Reaktion auf

Cybersicherheitsvorfälle und -krisen großen Ausmaßes könnten die Mitgliedstaaten eine Abstimmung ihrer nationalen Ansätze prüfen, sodass die sachdienlichen Informationen, die auf diesen Meldungen basieren, so rasch wie möglich an die zuständigen Behörden oder die CSIRT anderer betroffener Mitgliedstaaten weitergeleitet werden können. Akkurate und verwertbare Informationen sind von entscheidender Bedeutung, wenn es darum geht, die Zahl der Infektionen zu verringern oder Sicherheitslücken vor ihrer Ausnutzung zu beheben.

Im Geiste der Partnerschaft und einer optimalen Nutzung der NIS-Richtlinie beabsichtigt die Kommission, die Unterstützung aller von dieser Rechtsvorschrift betroffenen Interessenträger im Rahmen der Fazilität „Connecting Europe“ zu erweitern. Während der Schwerpunkt auf dem Aufbau von Kapazitäten der CSIRT und auf einer Plattform für eine schnelle und wirksame operative Zusammenarbeit zur Stärkung des CSIRT-Netzes lag, wird die Kommission nun prüfen, wie eine Finanzierung im Rahmen der Fazilität „Connecting Europe“ auch den zuständigen nationalen Behörden und Betreibern wesentlicher Dienste und Anbietern digitaler Dienste zugute kommen kann.

Schlussfolgerung

Angesichts des bevorstehenden Fristablaufs für die Umsetzung der NIS-Richtlinie in nationales Recht am 9. Mai 2018 und für die Ermittlung der Betreiber wesentlicher Dienste am 9. November 2018 sollten die Mitgliedstaaten mit geeigneten Maßnahmen sicherstellen, dass die Bestimmungen und die Kooperationsmodelle der NIS-Richtlinie auf EU-Ebene bestmöglich geeignet sind, um ein hohes gemeinsames Sicherheitsniveau von Netz- und Informationssystemen in der EU zu erreichen. Die Kommission ersucht die Mitgliedstaaten, bei diesem Prozess den einschlägigen Informationen, Leitlinien und Empfehlungen in dieser Mitteilung Rechnung zu tragen.

Diese Mitteilung lässt sich mit weiteren Maßnahmen, die sich beispielsweise aus den laufenden Arbeiten der Kooperationsgruppe ergeben, ergänzen.