NETZ- UND INFORMATIONSSICHERHEIT

Centrum für Europäische Politik
FREIBURG | BERLIN

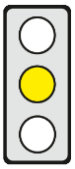
cepAnalyse Nr. 13/2021

KERNPUNKTE

Hintergrund: Die Kommission hat mehrere Schwachstellen in der geltenden NIS-Richtlinie ausgemacht. Diese will sie beheben.

Ziel der Richtlinie: Die EU-Kommission will das Niveau der Cybersicherheit in der EU verbessern.

Betroffene: Wesentliche und wichtige private und öffentliche Einrichtungen, EU- und nationale Cybersicherheitsbehörden und -gremien.



Pro: (1) Cybersicherheitsanforderungen für Unternehmen, welche für das Funktionieren einer Gesellschaft zentral sind, sind angemessen, da die wirtschaftlichen Anreize für Investitionen in die Cybersicherheit unzureichend sind und die Kosten für die Gesellschaft bei Cybervorfällen, die wesentliche und wichtige Unternehmen betreffen, besonders hoch.

(2) Die neuen Meldeverfahren erhöhen die Rechtsklarheit und die zentralen Meldestellen reduzieren den Verwaltungsaufwand für die meldepflichtigen Einrichtungen.

Contra: (1) Die neuen Pflichten wesentlicher und wichtiger Unternehmen, Risiken der Lieferkette zu berücksichtigen, sollten sich auf Risiken beschränken, die Lieferanten von IKT-Produkten und -Dienstleistungen betreffen, die als sicherheitsrelevant für die Geschäftstätigkeit der Unternehmen gelten.

(2) Die Pflicht, Vorfälle binnen 24 Stunden zu melden, könnte sich als zu anspruchsvoll erweisen.

Die wichtigsten Textstellen sind durch einen Randstrich gekennzeichnet.

INHALT

Titel

Vorschlag COM(2020) 823 vom 16. Dezember 2020 für eine **Richtlinie über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union** und zur Aufhebung der Richtlinie (EU) 2016/1148

Kurzdarstellung

- **Hintergrund und Ziele**
  - Die Richtlinie zur Netz- und Informationssicherheit ["NIS 1.0", (EU) 2016/1148, s. cep**Analyse**] sieht vor, dass
    - die Mitgliedstaaten nationale Cybersicherheitsstrategien aufstellen und Cybersicherheitsbehörden benennen müssen,
    - verschiedene Foren zur Verbesserung der Zusammenarbeit im Bereich der Cybersicherheit zwischen den Mitgliedsstaaten eingerichtet werden müssen,
    - die Mitgliedstaaten verbindliche Regeln für das Cybersicherheitsrisikomanagement festlegen müssen, und
    - die Mitgliedstaaten Meldepflichten für Cybersicherheitsvorfälle etablieren müssen.
  - Laut Kommission hat sich die Cyberresilienz der EU seit Inkrafttreten der Richtlinie deutlich verbessert. Allerdings hat sie auch einige Schwachstellen identifiziert: [Erwägungsgrund 2, S. 5 und 6]
    - Der Anwendungsbereich der Richtlinie ist "zu begrenzt" und "bietet keine hinreichende Klarheit";
    - Der Ermessensspielraum der Mitgliedstaaten bei der Umsetzung von Anforderungen an das Cyberssicherheitsrisikomanagement und der Pflichten zur Meldung von Vorfällen ist zu groß;
    - Die Aufsichts- und Durchsetzungsvorschriften sind "nicht wirksam".
  - Der Richtlinienvorschlag "NIS 2.0" adressiert diese Schwachstellen und hebt die bestehende NIS-Richtlinie auf.
- **Geltungsbereich**
  - Die Richtlinie gilt für alle öffentlichen und privaten Einrichtungen mit mehr als 50 Beschäftigten oder einem Jahresumsatz oder einer Jahresbilanz von mindestens 10 Mio. €, sofern sie eingestuft sind als (vollständige Liste s. cep**Dokument**) [Art. 2 Abs. 1]
    - "wesentliche" Einrichtungen, z. B. Strom- und Wasserversorger, Ölproduzenten, Banken; oder
    - "wichtige" Einrichtungen, z. B. Hersteller von Medizinprodukten, Lebensmittelproduzenten oder Betreiber von Online-Marktplätzen.
  - Unabhängig von ihrer Größe gilt die Richtlinie für "wesentliche" oder "wichtige" öffentliche und private Einrichtungen, die [Art. 2 Abs. 2]
    - Anbieter öffentlicher elektronischer Kommunikationsnetze und -dienste, von Vertrauensdiensten oder von Top-Level-Domain (TLD)-Namensregistern und -systemen sind,
    - öffentliche Verwaltungen der Zentralregierungen, der sozioökonomischen Großregionen und Basisregionen, die u. a. Rechtspersönlichkeit besitzen, zur Erfüllung von im allgemeinen Interesse liegenden Zwecken

Autoren: Philipp Eckhardt und Dr. Martina Anzini | eckhardt@cep.eu
cep | Kaiser-Joseph-Straße 266 | 79098 Freiburg | Deutschland | Telefon + 49 761 38693-107 | www.cep.eu

gegründet wurden und Verwaltungs- oder Regulierungsentscheidungen treffen können, die den freien Personen-, Waren-, Dienstleistungs- und Kapitalverkehr betreffen,
- der einzige Erbringer eines Dienstes in einem Mitgliedstaat sind,
- Anbieter von Diensten sind,
  - deren Störung die öffentliche Sicherheit, Ordnung, oder Gesundheit, oder die grenzüberschreitende Systemstabilität gefährden könnte, oder
  - die auf regionaler oder nationaler Ebene besonders kritisch sind, oder
  - die von den Mitgliedstaaten gemäß der vorgeschlagenen Richtlinie über die Resilienz kritischer Einrichtungen [COM(2020) 829] als "kritisch", d. h. als wesentlich für die Aufrechterhaltung essenzieller gesellschaftlicher oder wirtschaftlicher Tätigkeiten, eingestuft werden.

– Die Vorschriften der Richtlinie an das Risikomanagement und die Meldung gelten nicht, sofern andere EU-Vorschriften strengere Anforderungen vorsehen [Art. 2 Abs. 6)]. Dies gilt etwa für Unternehmen des Finanzsektors, die der vorgeschlagenen Verordnung zur digitalen Betriebsstabilität [COM(2020) 595, s.cep**Analyse**] unterliegen [Erwägungsgrund 13].

► **Cybersicherheitsrisikomanagement durch wesentliche und wichtige Unternehmen**

– Wesentliche und wichtige Unternehmen müssen " geeignete und verhältnismäßige technische und organisatorische Maßnahmen“ ergreifen, um die Risiken für die Sicherheit der Netz- und Informationssysteme (NIS), die sie für die Erbringung ihrer Dienste nutzen, zu beherrschen. Dies muss mindestens die Risikoanalyse, Sicherheitskonzepte für Informationssysteme, die Bewältigung von Zwischenfällen, die Aufrechterhaltung des Betriebs, die Sicherheit von Lieferketten und die Nutzung von Verschlüsselung umfassen. [Art. 18 Abs. 1 und 2]
– Wesentliche und wichtige Unternehmen müssen bezüglich der Sicherheit ihrer Lieferketten die spezifischen Schwachstellen jedes Lieferanten, sowie die Qualität der Produkte und Cybersicherheitspraktiken der Lieferanten berücksichtigen [Art. 18 Abs. 3].
– Die Leitungsorgane der wesentlichen und wichtigen Unternehmen müssen die Maßnahmen zum Risikomanagement billigen und deren Umsetzung überwachen. Sie sind für jede Nichteinhaltung der Richtlinie rechenschaftspflichtig und müssen regelmäßige Schulungen zu Cybersicherheitsrisiken und deren Auswirkungen auf das Unternehmen durchführen. [Art. 17]
– Die Kommission kann Durchführungsrechtsakte zur Festlegung der "technischen und methodischen Spezifikationen" für die Risikomanagementmaßnahmen sowie delegierte Rechtsakte zur Erweiterung der Liste der Maßnahmen erlassen [Art. 18 Abs. 5 und 6].
– Die Kommission kann – über delegierte Rechtsakte – beschließen, dass bestimmte Kategorien wesentlicher Einrichtungen ein Cybersicherheitszertifikat für IKT-Produkte, -Dienstleistungen oder -Prozesse im Rahmen spezifischer europäischer Systeme für die Cybersicherheitszertifizierung erhalten müssen (s. auch cep**Analyse**). Die Mitgliedsstaaten können ferner einzelne wesentliche und wichtige Einrichtungen dazu verpflichten. [Art. 21]

► **Meldung von Cybervorfällen und -bedrohungen an Behörden und Dienstnutzer**

– Wesentliche und wichtige Einrichtungen müssen den zuständigen nationalen Behörden oder den nationalen Reaktionsteams für IT-Sicherheitsvorfälle (CSIRTs) unverzüglich melden alle signifikanten [Art. 20]
  - Cybervorfälle, d. h. solche Vorfälle, die zu erheblichen Betriebsstörungen oder finanziellen Verlusten für das Unternehmen oder zu erheblichen materiellen oder immateriellen Verlusten für andere natürliche oder juristische Personen führen können, und
  - Cyberbedrohungen, die potenziell zu einem signifikanten Cybervorfall hätten führen können.
– Signifikante Cybervorfälle müssen in der Regel binnen 24 Stunden gemeldet werden, wobei anzugeben ist, ob ein Vorfall "vermutlich auf rechtswidrige oder böswillige Handlungen zurückzuführen ist“ [Art. 20 Abs. 4].
– Auf Ersuchen einer zuständigen Behörde oder des CSIRT muss ein Zwischenbericht mit Statusaktualisierungen vorgelegt werden [Art. 20 Abs. 4].
– Binnen eines Monats nach einem Vorfall muss ein Abschlussbericht vorgelegt werden, in dem der Schweregrad und die Auswirkungen des Vorfalls, die Art der Bedrohung, die Ursache und die getroffenen Abhilfemaßnahmen beschrieben werden müssen [Art. 20 Abs. 4].
– Wesentliche und wichtige Einrichtungen müssen ihre Dienstnutzer ggfs. unverzüglich benachrichtigen über [Art. 20 Abs. 1 und 2]
  - Cybervorfälle, die die Erbringung ihrer Dienste beeinträchtigen könnten, und
  - signifikante Cyberbedrohungen und Maßnahmen, die sie als Reaktion auf diese ergreifen könnten.
– Die zuständige Behörde oder das CSIRT müssen binnen 24 Stunden eine erste Rückmeldung abgeben und auf Ersuchen des Unternehmens Hilfe zur Durchführung von Abhilfemaßnahmen bereitstellen [Art. 20 Abs. 5].
– Die zuständige Behörde oder das CSIRT kann die Öffentlichkeit über den Vorfall informieren oder dies von der betroffenen Einrichtung verlangen, sofern die Sensibilisierung der Öffentlichkeit den Vorfall verhindern kann, zu dessen Bewältigung beiträgt oder im öffentlichen Interesse liegt [Art. 20 Abs. 7].
– Die Mitgliedstaaten sollten eine nationale zentrale Anlaufstelle für alle Meldungen einrichten, die z. B. auch Meldungen von Verstößen gegen die Datenschutzgrundverordnung [GDPR, (EU) 2016/679] und die ePrivacy-Richtlinie [2002/58/EG] abdecken soll [Erwägungsgrund 56].

- **Aufsicht, Durchsetzung und Sanktionen**
  - Den zuständigen nationalen Behörden muss ein Mindestumfang an Aufsichtsbefugnissen eingeräumt werden, u. a. für Vor-Ort-Prüfungen, Sicherheitsprüfungen. Wesentliche Einrichtungen unterliegen einer ex-ante- und ex-post-Aufsicht, wichtige Einrichtungen nur einer ex-post-Aufsicht. [Art. 29 Abs. 2 und 30 Abs. 2]
  - Den Behörden muss zudem ein Mindestumfang an Durchsetzungsbefugnissen eingeräumt werden, u. a. für die Erteilung von Verwarnungen und Anweisungen. Diese können sich sowohl an wesentliche als auch an wichtige Einrichtungen richten. [Art. 29 Abs. 4 und Art. 30 Abs. 4]
  - Kommen die Unternehmen den Durchsetzungsmaßnahmen nicht nach, können die Behörden Sanktionen verhängen. Sanktionen können gegen die Einrichtungen und gegen die für die Geschäftsführung verantwortlichen Personen verhängt werden. [Art. 29 Abs. 5]

Wesentliche Änderungen des Status quo

- Die NIS 2.0 deckt eine Reihe von Einrichtungen und Sektoren ab, die von der NIS 1.0 nicht erfasst wurden, z. B. Betreiber im Bereich Wasserstofferzeugung, Abwasserunternehmen und Kraftwagenhersteller (s. cep**Dokument**).
- Die NIS 1.0 unterscheidet zwischen Betreibern wesentlicher Dienste und Anbietern digitaler Dienste und die Mitgliedstaaten haben einen weiten Ermessensspielraum bei der Definition dieser Einrichtungen. Die NIS 2.0 unterscheidet zwischen wesentlichen und wichtigen Einrichtungen und legt ein einheitliches Kriterium in Form eine Schwellenwertes für die Größe der Einrichtungen fest.
- In der NIS 1.0 ist der Umfang der vorgeschriebenen Maßnahmen zum Cybersicherheitsrisikmanagement vage. Die Mitgliedstaaten haben einen großen Ermessensspielraum. Die NIS 2.0 liefert mehr Details und legt einen stärkeren Fokus auf Risiken in der Lieferkette.
- In der NIS 1.0 ist der Umfang der Meldepflichten vage. Die NIS 2.0 sieht klarere Regeln vor, welche, wann und wie Cybervorfälle gemeldet werden müssen. Sie führt eine Meldepflicht für Cyberbedrohungen ein.

Subsidiaritätsbegründung der Kommission

Das Eingreifen der EU ist wegen des grenzüberschreitenden Charakters NIS-bezogener Bedrohungen gerechtfertigt.

Politischer Kontext

NIS 2.0 ergänzt die vorgeschlagene Richtlinie zur Resilienz kritischer Einrichtungen [COM(2020) 829].

Stand der Gesetzgebung

16.12.2020	Annahme durch Kommission
Offen	Annahme durch Europäisches Parlament und Rat, Veröffentlichung im Amtsblatt, Inkrafttreten

Politische Einflussmöglichkeiten

Generaldirektionen:	DG Kommunikationsnetze, Inhalte und Technologien
Ausschüsse des Europäischen Parlaments:	ITRE (federführend), Berichterstatterin: Angelika Niebler (EVP, DE)
Bundesministerien:	Inneres, Bau und Heimat
Ausschüsse des Deutschen Bundestages:	Inneres und Heimat (federführend)
Entscheidungsmodus im Rat:	Qualifizierte Mehrheit (Zustimmung von 55% der Mitgliedstaaten, die 65% der EU-Bevölkerung ausmachen)

Formalien

Kompetenznorm:	Art. 114 AEUV (Binnenmarkt)
Art der Gesetzgebungskompetenz:	Geteilte Zuständigkeit (Art. 4 (2) AEUV)
Verfahren:	Art. 294 AEUV (ordentliches Gesetzgebungsverfahren)

BEWERTUNG

Ökonomische Folgenabschätzung

Cybersicherheitsanforderungen für Unternehmen, welche für das Funktionieren einer Gesellschaft zentral sind, sind angemessen: Unternehmen haben bereits ein Eigeninteresse daran, ihre Netz- und Informationssysteme (NIS) vor Cybervorfällen und -bedrohungen zu schützen, da ein Nichthandeln mit erheblichen Umsatzverlusten und Reputationsschäden einhergehen kann. Obwohl sie mit erheblichen Kosten verbunden sind und die unternehmerische Freiheit einschränken, sind einheitliche technische und organisatorische EU-Maßnahmen bezüglich NIS dennoch gerechtfertigt, **da die wirtschaftlichen Anreize für Investitionen in die Cybersicherheit unzureichend sind**. Dies liegt zum einen daran, dass Unternehmen oft nicht die vollen Kosten, die durch Cybervorfälle entstehen, selbst tragen müssen **und** einen Teil der Kosten auf Dritte, z. B. ihre Kunden, abwälzen können. Zweitens profitieren Unternehmen von den Investitionen in Cybersicherheit anderer Unternehmen, da diese Investitionen oft nicht nur die NIS-Resilienz des Investierenden,

sondern indirekt auch die Resilienz Dritter erhöhen. Darüber hinaus sind **die Kosten für die Gesellschaft bei Cybervorfällen, die wesentliche und wichtige Unternehmen betreffen, besonders hoch.**

Im Gegensatz zur NIS 1.0 verbessert die Neujustierung des Geltungsbereichs der Richtlinie die Rechtsklarheit, begrenzt Regulierungsarbitrage und damit Wettbewerbsverzerrungen. Allerdings ist der Geltungsbereich zu weit gefasst: Er umfasst viele Unternehmen, die keine Produkte oder Dienstleistungen anbieten, die für das Funktionieren einer Gesellschaft zentral sind, z. B. Kraftwagenhersteller, die daher ausgenommen werden sollten. Außerdem ist fraglich, ob die zuständigen Behörden in der Lage wären, alle Unternehmen, die unter die Richtlinie fallen, angemessen zu beaufsichtigen – z.B. alle Hersteller von Waren, d.h. 31.000 mittlere und große Unternehmen [SWD(2020) 345, Seite 63]. Auch die Größe als alleiniges Kriterium ist ungeeignet, da diese allein nicht zwangsläufig auf ein höheres Cybersicherheitsrisiko hindeutet. Andere Kriterien wie die Anzahl der Kunden sollten auch Berücksichtigung finden.

Die neuen Pflichten wesentlicher und wichtiger Unternehmen, im Rahmen ihres Risikomanagements **Risiken der Lieferkette** in größerem Umfang als nach der NIS 1.0 **zu berücksichtigen**, können das Cybersicherheitsniveau in der EU erhöhen. Sie **sollten sich** jedoch **auf Risiken beschränken, die Lieferanten von IKT-Produkten und -Dienstleistungen betreffen, die als sicherheitsrelevant für die Geschäftstätigkeit der Unternehmen gelten.** Die Last sollte ferner nicht nur auf den wesentlichen und wichtigen Unternehmen am Ende der Lieferketten liegen. Es sollte auch Vorgaben für Lieferanten in der Wertschöpfungsketten geben, um sicherzustellen, dass deren IKT-Produkte und -Dienstleistungen, wenn sie an wesentliche und wichtige Unternehmen geliefert werden, cybersicher sind.

Unternehmen haben angesichts der Meldekosten und des potenziellen Reputationsschadens wenig Anreize, Cybervorfälle und -bedrohungen zu melden. Gleichzeitig helfen Meldungen anderen dabei, Sicherheitslücken zu erkennen und zu schließen. Die Meldung von Cybervorfällen und -bedrohungen bringt daher einen erheblichen externen Nutzen mit sich, so dass es angemessen ist, Unternehmen zur Meldung zu zwingen. **Die neuen Meldeverfahren erhöhen die Rechtsklarheit und die zentralen Meldestellen reduzieren den Verwaltungsaufwand für die meldepflichtigen Einrichtungen. Die** vorgesehene **Pflicht, Vorfälle binnen 24 Stunden zu melden** und dabei aussagekräftige Informationen zu liefern, **könnte sich als zu anspruchsvoll erweisen.** Dies gilt insbesondere für kleinere Unternehmen. Solch rasche Meldungen können bei den Einrichtungen auch wertvolle Ressourcen binden, die besser zur Bewältigung der Cybervorfälle genutzt werden sollten.

Juristische Bewertung

Kompetenz

Die Richtlinie wird zu Recht auf Art. 114 AEUV gestützt. Dies gilt auch für die Einbeziehung derjenigen öffentlichen Verwaltungen in den Geltungsbereich, die Verwaltungs- oder Regulierungsentscheidungen treffen, die die vier Grundfreiheiten berühren. Maßnahmen, die auf Art. 114 AEUV gestützt werden, müssen nämlich darauf abzielen, die Bedingungen für die Errichtung und das Funktionieren des Binnenmarkts zu verbessern, indem entweder Behinderungen der Grundfreiheiten oder erhebliche Wettbewerbsverzerrungen beseitigt werden [Urteil vom 3.9.2015, C-398/13 P, Inuit Tapiriit Kanatami u. a./Kommission, EU:C:2015:535, Rn. 26]. Einheitliche Vorschriften zur Stärkung der Cybersicherheit öffentlicher Verwaltungen erfüllen die genannten Kriterien, wenn sie nationale Behörden betreffen, auf die juristische und natürliche Personen bei der Ausübung ihrer Rechte auf Personen-, Waren-, Dienstleistungs- oder Kapitalverkehr zurückgreifen. Dies kann bspw. der Fall sein, wenn eine Aufsichtsbehörde einem Unternehmen eine Genehmigung erteilt, seine Dienste im gesamten Binnenmarkt anzubieten. In solchen Fällen ist die Fähigkeit der öffentlichen Verwaltungen, ihre Aufgaben kontinuierlich und sicher zu erfüllen, eine Bedingung, die erfüllt sein muss, damit natürliche oder juristische Personen, die genannten Rechte tatsächlich ausüben können.

Subsidiarität

Unproblematisch, angesichts des grenzüberschreitenden Charakters von NIS-bezogenen Vorfällen und Bedrohungen.

Verhältnismäßigkeit in Bezug auf die Mitgliedsstaaten

Die Mitgliedstaaten behalten die Befugnis, Cybersicherheitsmaßnahmen für Unternehmen zu regeln, die der Richtlinie nicht unterliegen. Auch behalten sie einen gewissen Spielraum bei der Entscheidung über die Angemessenheit und Verhältnismäßigkeit technischer und organisatorischer Risikomanagementmaßnahmen. Da die Richtlinie eine Mindestharmonisierung [Art. 3] vorsieht, können die Mitgliedstaaten Vorgaben treffen, die auf ein höheres Maß an Cybersicherheit hinwirken.

Zusammenfassung der Bewertung

Cybersicherheitsanforderungen für Unternehmen, welche für das Funktionieren einer Gesellschaft zentral sind, sind angemessen, da die wirtschaftlichen Anreize für Investitionen in die Cybersicherheit unzureichend sind und die Kosten für die Gesellschaft bei Cybervorfällen, die wesentliche und wichtige Unternehmen betreffen, besonders hoch. Die neuen Pflichten wesentlicher und wichtiger Unternehmen, Risiken der Lieferkette zu berücksichtigen, sollten sich auf Risiken beschränken, die Lieferanten von IKT-Produkten und -Dienstleistungen betreffen, die als sicherheitsrelevant für die Geschäftstätigkeit der Unternehmen gelten. Die neuen Meldeverfahren erhöhen die Rechtsklarheit und die zentralen Meldestellen reduzieren den Verwaltungsaufwand für die meldepflichtigen Einrichtungen. Die Pflicht, Vorfälle binnen 24 Stunden zu melden, könnte sich als zu anspruchsvoll erweisen.