Centrum für Europäische Politik
FREIBURG | BERLIN

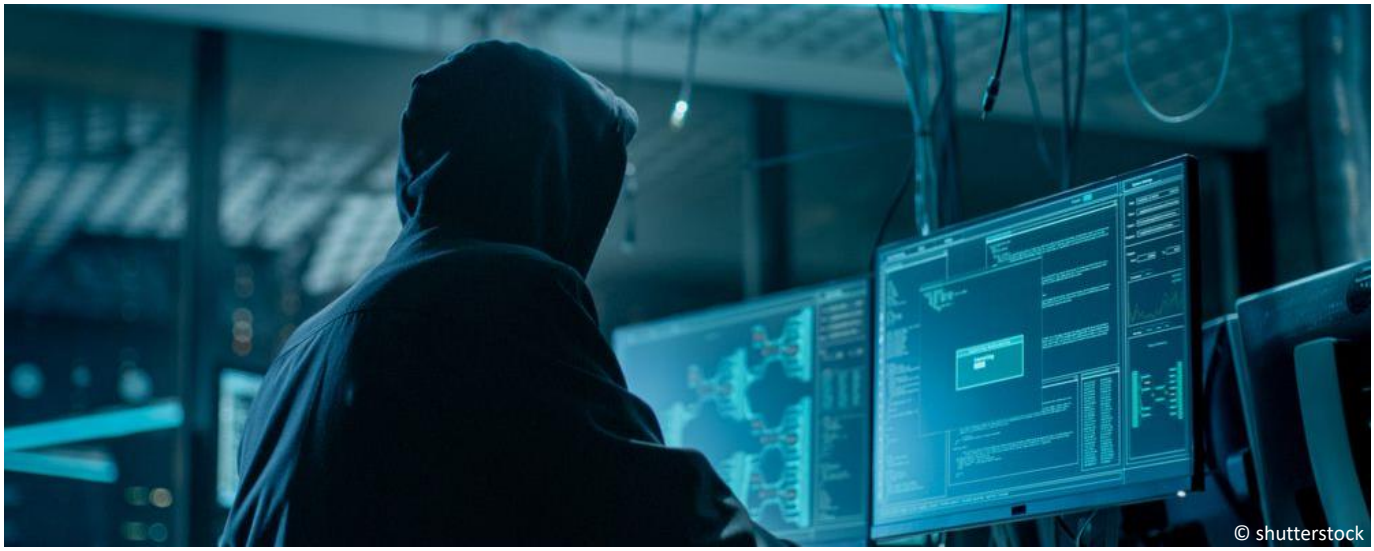
cepAdhoc

Nr. 9 | 2022 13. September 2022

NIS 2-Richtlinie: Neue EU-Vorgaben zur Cybersicherheit

Cyber-Risiken und -Attacken bedrohen zunehmend die europäische Sicherheit

Philipp Eckhardt



Die voranschreitende Digitalisierung und zunehmende geopolitische Bedrohungen erhöhen das Risiko von Cyber-Unfällen und -Attacken deutlich. Cybersicherheit ist zu einer der wichtigsten Säulen der hoheitlichen Sicherheit geworden. Am 13. Mai 2022 einigten sich das Europäische Parlament und der Rat auf neue Cybersicherheitsvorschriften. Künftig sollen ca. 160.000 Unternehmen und Behörden einheitlichen EU-Vorgaben zum Management von Cyberrisken und zur Meldung von Cybersicherheitsvorfällen und -bedrohungen unterliegen. Der cepAdhoc zeigt auf, was auf die Firmen und staatlichen Stellen zukommt und bewertet die Neuregelungen.

- Der klarer gefasste Geltungsbereich der NIS 2-Richtlinie schafft mehr Rechtssicherheit und beugt Wettbewerbsverzerrungen vor. Es ist jedoch fraglich, ob die Aufsichtsbehörden in der Praxis mit der Aufsicht über ca. 160.000 Einrichtungen nicht überfordert sind. Eine stärkere Priorisierung wäre daher angezeigt gewesen.
- Dass Risiken in oft grenzüberschreitenden Lieferketten verstärkt berücksichtigt werden müssen, ist richtig und erhöht das Cybersicherheitsniveau in der EU. Die Verantwortung sollte jedoch nicht allein auf den Schultern der Einrichtungen liegen. Cybersicherheit ist einerseits ein öffentliches Gut und andererseits ein hoheitliches Interesse.
- Die Meldepflichten sind sachgerecht, da von Cybervorfällen betroffene Einrichtungen oft u.a. aufgrund von mit solchen Meldungen einhergehenden Reputationsschäden wenig Anreiz haben, dies freiwillig zu tun. Die Meldungen haben häufig einen hohen externen Nutzen, da sie anderen dabei helfen, Sicherheitslücken zu erkennen und zu schließen.
- Die Stärkung des Risikomanagements von sowie verschärfte Meldepflichten für Unternehmen und Einrichtungen des privaten und öffentlichen Sektors können nur ein Baustein der erforderlichen Regulierung sein. Es ist daher richtig, dass die Kommission mit dem anstehenden „Cyber Resilience Act“ die Cyberresilienz der vernetzten europäischen Volkswirtshaften ein weiteres zentrales Element hinzufügen will.

Inhaltsverzeichnis

1 Hintergrund ... 3
2 NIS 2-Richtlinie: Verschärfte EU-Vorschriften zur Stärkung der Cybersicherheit ... 4
2.1 Anpassungen beim Anwendungsbereich ... 4
2.1.1 Wesentliche Einrichtungen ... 4
2.1.2 Wichtige Einrichtungen ... 6
2.1.3 Ausnahmen für kleine Einrichtungen ... 6
2.1.4 Einrichtungen, die unabhängig von ihrer Größe immer erfasst sind ... 7
2.1.5 Ausgenommene Einrichtungen ... 7
2.1.6 Sektorspezifische Regelungen ... 7
2.2 Management von Cyberrisiken ... 8
2.2.1 Maßnahmen zur Beherrschung von Cyberrisiken: ... 8
2.2.2 Fokus Lieferkette ... 8
2.2.3 Cybersicherheitszertifizierung ... 9
2.2.4 Verantwortlichkeit der Leitungsorgane ... 9
2.3 Meldung von Cybervorfällen und -bedrohungen ... 9
2.3.1 Welche Cybervorfälle und -bedrohungen gemeldet werden müssen? ... 9
2.3.2 Wann Cybervorfälle gemeldet werden müssen ... 10
2.3.3 An wen Cybervorfälle gemeldet werden müssen ... 10
2.3.4 Reaktion der Aufsichtsbehörden ... 11
2.4 Aufsicht, Durchsetzung und Sanktionen ... 11
2.5 Umsetzung der NIS 2-Richtlinie ... 11
3 Bewertung ... 12

Tabellenverzeichnis

Tabelle 1: Öffentliche und private wesentliche Einrichtungen ... 4
Tabelle 2: Öffentliche und private wichtige Einrichtungen ... 6

1 Hintergrund

Laut dem Bundeskriminalamt (BKA) ist im Jahr 2021 die Anzahl der Cybercrime-Delikte um 12% im Vergleich zum Vorjahr gestiegen und nach Zahlen des Bitkom-Verband haben sich die durch Cybercrime verursachten Schäden im Vergleich zum Jahr 2019 auf einen Höchstwert von 223,5 Mrd. Euro mehr als verdoppelt.[1,2] Und auch vor dem Hintergrund der russischen Invasion in der Ukraine wachsen die Befürchtungen vor zunehmenden Cyberattacken, insbesondere auf kritische Infrastrukturen wie etwa Energieversorger, Wasserwerke und Krankenhäuser.[3,4]

Auf EU-Ebene ist seit 2016 die Richtlinie zur Netz- und Informationssicherheit ["NIS 1-Richtlinie", (EU) 2016/1148] in Kraft. Sie verpflichtet die Mitgliedstaaten insbesondere dazu, nationale Cybersicherheitsstrategien aufzustellen und etabliert verschiedene Gremien, um die Zusammenarbeit zwischen den Mitgliedstaaten im Bereich der Cybersicherheit zu stärken. Ferner legt sie fest, dass die Mitgliedstaaten verbindliche Regeln für das Cybersicherheitsrisikomanagement und Meldepflichten für Cybersicherheitsvorfälle etablieren müssen.

Mitte Dezember 2020 legte die EU-Kommission einen Vorschlag zur Überarbeitung der Richtlinie [COM(2020) 823] vor, da sie einige Mängel am bestehenden Rechtsrahmen feststellte. Sie monierte insbesondere, dass der Geltungsbereich der Richtlinie "zu begrenzt" sei und damit eine Vielzahl von Unternehmen sowie staatliche Stellen keinen EU-weiten Mindestvorgaben zur Cybersicherheit unterliegen würden. Ferner biete der Anwendungsbereich "keine hinreichende Klarheit", sodass der Spielraum für Mitgliedstaaten bei der Festlegung, wer die Vorgaben der Richtlinie erfüllen muss, zu groß sei. Zudem bemängelte die Kommission die übermäßigen Freiheitsgrade der Mitgliedstaaten bei der Umsetzung von Anforderungen an das Management von Cybersicherheitsrisiken und auch die Pflichten zur Meldung von Cybervorfällen seien zu unpräzise. Und nicht zuletzt kritisierte die Kommission die Unwirksamkeit der Aufsichts- und Durchsetzungsvorschriften der Richtlinie.[5]

Am 13. Mai 2022 einigten sich Unterhändler des Europäischen Parlaments (EP) und des Rates auf eine Neufassung der NIS 1-Richtlinie.[6] Der Kompromiss, den das EP und der Rat nun noch formal bestätigen müssen, hat es in sich. Künftig werden ca. 160.000 Unternehmen und öffentliche Einrichtungen von einheitlichen EU-Mindestvorgaben zur Sicherstellung eines hohen Cybersicherheitsniveaus in der EU betroffen sein.[7,8] Dieser cep**Adhoc** zeigt auf, was auf die betroffenen Unternehmen bzw. auf die

---

1 Bundeskriminalamt (BKA), Cybercrime, Bundeslagebild 2021.

2 Bitkom Research 2021, Angriffsziel deutsche Wirtschaft: mehr als 220 Milliarden Euro Schaden pro Jahr, Presseinformation, 5. August 2021.

3 Der Rat wies bspw. jüngst darauf hin, dass „böswillige Handlungen im Cyberraum […] von staatlichen als auch von nichtstaatlichen Akteuren […] zugenommen haben […] und […] dass mit der Rückkehr zur Machtpolitik einige Länder zunehmend versuchen, die regelbasierte internationale Ordnung im Cyberraum in Frage zu stellen“. Er warnt davor, dass „ groß angelegte, systemgefährdende Cyberangriffe, […] zugenommen haben, unsere wirtschaftliche Sicherheit untergraben und unsere demokratischen Institutionen und Prozesse beeinträchtigen könnten“ [Rat der Europäischen Union, Schlussfolgerungen des Rates zur Entwicklung der Cyberabwehr der Europäischen Union, 23. Mai 2022].

4 Die deutsche Bundesregierung beschloss im Rahmen der Verhandlungen zur Etablierung eines Sondervermögens für die Bundeswehr auch Maßnahmen zur Stärkung der Cybersicherheit, die durch den Bundeshaushalt finanziert werden sollen. Sie will zeitnah eine „Strategie zur Stärkung der Sicherheit im Cyber- und Informationsraum“ vorlegen.

5 EU-Kommission, COM(2020) 823, Vorschlag für eine Richtlinie über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union und zur Aufhebung der Richtlinie (EU) 2016/1148, S. 5 und 6.

6 Rat der EU, Stärkung der EU-weiten Cybersicherheit und Resilienz – vorläufige Einigung zwischen Rat und Europäischem Parlament, Pressemitteilung, 13. Mai 2022.

7 Ausschuss für Industrie, Forschung und Energie (ITRE), Cybersecurity: deal with Council to strengthen EU-wide resilience, Pressemitteilung, 13.05.2022.

8 Richtlinie über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union und zur Aufhebung der Richtlinie (EU) 2016/1148 (NIS 2-Richtlinie).

öffentlichen Verwaltungen zukommt und gibt eine kurze Einschätzung der getroffenen Änderungen ab. Dabei fokussieren wir uns auf die Anpassungen der NIS 2-Richtlinie hinsichtlich des Anwendungsbereichs, zum Management von Cyberrisiken, zu den überarbeiteten Meldepflichten sowie zu den Vorschriften zur Aufsicht, zur Rechtsdurchsetzung und zu Sanktionen.

2 NIS 2-Richtlinie: Verschärfte EU-Vorschriften zur Stärkung der Cybersicherheit

2.1 Anpassungen beim Anwendungsbereich

Der Anwendungsbereich der Richtlinie soll nach den Vorstellungen des EP und des Rates deutlich erweitert werden. Nach der NIS 2-Richtlinie müssen künftig eine Vielzahl weiterer Unternehmen aus bestimmten Sektoren und erstmals Einrichtungen aus dem öffentlichen Sektor EU-weit einheitliche Cybersicherheitsvorgaben erfüllen.

2.1.1 Wesentliche Einrichtungen

Wie bisher gilt die Richtlinie für eine Reihe von Einrichtungen, die als „wesentlich“ eingestuft werden[9], da sie von kritischer Bedeutung für die Funktionsfähigkeit einer Gesellschaft sind. Dazu zählen u.a. Elektrizitätsversorger, Eisenbahnunternehmen und Banken. Künftig wird die Liste „wesentlicher“ Einrichtungen jedoch noch deutlich erweitert. So fallen künftig u.a. auch Einrichtungen im Bereich Wasserstofferzeugung, -speicherung und -fernleitung, Hersteller von pharmazeutischen Erzeugnissen, Abwasserentsorgungsunternehmen und auch bestimmte Einrichtungen der öffentlichen Verwaltung unter diese Kategorie (s. Tabelle 1).[10]

Tabelle 1: Öffentliche und private wesentliche Einrichtungen

Die in rot und fett markierten Einrichtungen kommen durch die NIS 2-Richtlinie neu hinzu.		
Sektor	**Teilsektor**	**Art der Einrichtung**
Energie	Elektrizität	• Elektrizitätsversorger • Verteilernetzbetreiber • Übertragungsnetzbetreiber • **Erzeuger von Elektrizität** • **Nominierte Strommarktbetreiber (NEMO)** • **Elektrizitätsmarktteilnehmer (Aggregierungs-, Laststeuerungs- oder Energiespeicherungsdienste)** • **Ladeinfrastrukturbetreiber**
	Fernwärme und -kälte	**Fernwärme oder Fernkälte zur Förderung der Nutzung von Energie aus erneuerbaren Quellen**
	Erdöl	• Betreiber von Erdöl-Fernleitungen • Betreiber von Anlagen zur Produktion, Raffination und Aufbereitung von Erdöl • Betreiber von Erdöllagern und -leitungen • **zentrale Erdölbevorratungsstellen**
	Erdgas	• Erdgasversorgungsunternehmen • Erdgasverteilernetzbetreiber • Erdgasfernleitungsnetzbetreiber • Betreiber von Erdgasspeicheranlagen • LNG-Anlagenbetreiber • Erdgasunternehmen • Betreiber von Anlagen zur Raffination und Aufbereitung von Erdgas
	Wasserstoff	**Betreiber im Bereich Wasserstofferzeugung, -speicherung und -fernleitung**

[9] Sie wurden bisher als „Betreiber wesentlicher Dienste“ bezeichnet.
[10] Art. 2 i.V.m. Anhang I, NIS 2-Richtlinie.

Verkehr	Luftverkehr	• Luftfahrtunternehmen, die für gewerbliche Zwecke genutzt werden • Flughafenleitungsorgane • Flughäfen • Betreiber von Verkehrsmanagement- und Verkehrssteuerungssystemen
	Schienenverkehr	• Infrastrukturbetreiber • Eisenbahnunternehmen
	Schifffahrt	• Passagier- und Frachtbeförderungsunternehmen in der Binnen-, See- und Küstenschifffahrt • Leitungsorgane von Häfen • Betreiber von Schiffsverkehrsdiensten
	Straßenverkehr	• Straßenverkehrsbehörden, die für Verkehrsmanagement und -steuerung zuständig sind, ausgenommen solchen, für die dies nur ein unwesentlicher Teil ihrer Tätigkeit darstellt • Betreiber intelligenter Transportsysteme
Bankenwesen und Finanzmarktinfrastrukturen		• Banken • Betreiber von Handelsplätzen • Zentrale Gegenparteien (CCPs)
Gesundheitswesen		• Gesundheitsdienstleister • EU-Referenzlaboratorien zu schwerwiegenden grenzüberschreitenden Gesundheitsgefahren • **Einrichtungen, die Forschungs- und Entwicklungstätigkeiten in Bezug auf Arzneimitteln ausüben** • **Hersteller von pharmazeutischen Erzeugnissen** • **Hersteller von Medizinprodukten, die während einer Notlage im Bereich der öffentlichen Gesundheit als kritisch gelten**
Trinkwasser		Lieferanten von und Unternehmen der Versorgung mit Trinkwasser, ausgenommen solchen, für die dies nur ein unwesentlicher Teil ihrer Tätigkeit darstellt
Abwasser		**Unternehmen, die Abwasser sammeln, entsorgen oder behandeln, ausgenommen solchen, für die dies nur ein unwesentlicher Teil ihrer Tätigkeit darstellt**
Digitale Infrastruktur		• Betreiber von Internet-Knoten • DNS-Diensteanbieter, ausgenommen Betreiber von Root-Name-Servern • TLD-Namensregister • Anbieter von Cloud Computing-Diensten[1] • **Anbieter von Rechenzentrumsdiensten** • **Anbieter von Content-Delivery-Netzworks** • **Anbieter von Vertrauensdiensten[2]** • **Anbieter öffentlicher elektronischer Kommunikationsnetze und -dienste[3]** • **Managed service provider (MSP) und Managed Security service provider (MSSP)**
Öffentliche Verwaltung		• **Einrichtungen der öffentlichen Verwaltung von Zentralregierungen, ausgenommen Justiz, Parlamente und Zentralbanken** • **Einrichtungen der öffentlichen Verwaltung auf regionaler Ebene[11]**
Weltraum		**Betreiber von Bodeninfrastrukturen zur Unterstützung weltraumgestützter Dienste**

[1] Sie werden bisher in der NIS-Richtlinie 1 als „Anbieter digitaler Dienste“ bezeichnet.
[2] Sie sind bislang durch die Verordnung über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt [(EU) Nr. 910/2014] abgedeckt.
[3] Sie sind bislang durch die Richtlinie über den europäischen Kodex für die elektronische Kommunikation [(EU) 2018/1972] abgedeckt.

[11] Ausgenommen sind zudem Einrichtungen der öffentlichen Verwaltung in den Bereichen Verteidigung, nationale Sicherheit, öffentliche Sicherheit oder Strafverfolgung.

2.1.2 Wichtige Einrichtungen

In der NIS 1-Richtlinie gab es noch eine zweite Kategorie erfasster Unternehmen, so genannte „Anbieter digitaler Dienste“. Diese Kategorie soll nun durch die NIS 2-Richtlinie abgeschafft und durch eine Kategorie so genannter „wichtiger Einrichtungen“ ersetzt werden. Diese Kategorie erfasst zwar auch Anbieter digitaler Dienste, z.B. Anbieter von Online-Marktplätzen und -Suchmaschinen, jedoch sollen hierunter künftig u.a. auch Hersteller von Medizinprodukten, Maschinenbauunternehmen, Anbieter von Post- und Kurierdiensten sowie Autohersteller fallen (s. Tabelle 2).[12]

Tabelle 2: Öffentliche und private wichtige Einrichtungen

Die in rot und fett markierten Einrichtungen kommen in der NIS 2-Richtlinie neu hinzu.		
Sektor	**Teilsektor**	**Art der Einrichtung**
Verarbeitendes Gewerbe / Herstellung von Waren	**Medizinprodukte und In-vitro-Diagnostika**	• **Hersteller von Medizinprodukten** • **Hersteller von In-vitro-Diagnostika**
	Datenverarbeitungsgeräte, elektronische und optische Erzeugnisse	**Hersteller von Datenverarbeitungsgeräten, elektronischen und optischen Erzeugnissen**
	Elektrische Ausrüstungen	**Hersteller von elektrischen Ausrüstungen**
	Maschinenbau	**Maschinenbauunternehmen**
	Kraftwagen und Kraftwagenteilen	**Hersteller von Kraftwagen und Kraftwagenteilen**
	Sonstiger Fahrzeugbau	**Schiffbau, Herstellung von Booten, Schienenfahrzeugen, Luft- und Raumfahrzeugen**
Abfallbewirtschaftung		**Abfallentsorgungsunternehmen (als Haupttätigkeit)**
Post- und Kurierdienste		**Anbieter von Post- und Kurierdiensten**
Lebensmittel		**Produktion, Verarbeitung und Vertrieb von Lebensmitteln im Großhandel oder in der industriellen Produktion und Verarbeitung**
Chemische Stoffe		**Produktion, Herstellung von Stoffen und Gemischen sowie Hersteller von Erzeugnissen aus den Stoffen und Gemischen**
Forschung		**Forschungseinrichtungen, deren Forschung kommerziellen Zwecken dient, ausgenommen Bildungseinrichtungen[13]**
Anbieter digitaler Dienste		• Anbieter von Online-Marktplätzen • Anbieter von Online-Suchmaschinen • **Anbieter von Plattformen für Dienste sozialer Netzwerke**

2.1.3 Ausnahmen für kleine Einrichtungen

Die NIS 2-Richtlinie soll grundsätzlich nur für wesentliche und wichtige Einrichtungen gelten, die die Schwellenwerte als mittelgroße Einrichtungen überschreiten. So ist vorgesehen, dass die Einrichtungen zumindest 50 Mitarbeiter haben müssen, einen Jahresumsatz von mindestens 10 Mio. Euro oder eine Jahresbilanz von mindestens 10 Mio. Euro.[14]

[12] Art. 2 i.V.m. Anhang I, NIS 2-Richtlinie.
[13] Die Mitgliedstaaten können jedoch beschließen, die Richtlinie auf Bildungseinrichtungen anzuwenden, insbesondere wenn diese kritische Forschungstätigkeiten durchführen (Art. 2 Abs. 2b).
[14] Art. 2, NIS 2-Richtlinie.

2.1.4 Einrichtungen, die unabhängig von ihrer Größe immer erfasst sind

Einige wesentliche oder wichtige öffentliche und private Einrichtungen sind auch unabhängig von ihrer Größe von der Richtlinie erfasst (keine Schwellenwerte). Das gilt u.a. für[15]

- Betreiber von öffentlichen elektronischen Kommunikationsnetzen und -diensten,
- Einrichtungen, die in einem Mitgliedstaat die einzigen Erbringer eines Dienstes sind, welcher für die Aufrechterhaltung kritischer gesellschaftlicher oder wirtschaftlicher Aktivitäten unerlässlich ist, sowie
- Anbieter von Diensten, deren Störung die öffentliche Sicherheit, Ordnung, oder Gesundheit, oder die grenzüberschreitende Systemstabilität in schwerwiegender Weise gefährden könnte.

Grundsätzlich sind auch Einrichtungen der öffentlichen Verwaltungen der Zentralregierungen unabhängig von ihrer Größe erfasst. Dies gilt ebenso für Einrichtungen der öffentlichen Verwaltungen auf regionaler Ebene, sofern der Ausfall der von ihnen bereitgestellten Dienste schwerwiegende Auswirkungen für gesellschaftliche oder wirtschaftliche Aktivitäten hätte. Die Mitgliedstaaten können ferner beschließen, dass auch öffentliche Verwaltungen auf lokaler Ebene von der NIS 2-Richtlinie erfasst sind (mitgliedstaatliches Wahlrecht).[16]

2.1.5 Ausgenommene Einrichtungen

Nicht erfasst von der Richtlinie sind „öffentliche Verwaltungen“ in den Bereichen Verteidigung, nationale Sicherheit, öffentliche Sicherheit oder Strafverfolgung, sowie Parlamente und Zentralbanken.[17] Ebenfalls ausgenommen sind eine Vielzahl von insbesondere Förderbanken – z. B. die Kreditanstalt für Wiederaufbau –, sofern ein Mitgliedstaat sich dafür entschieden hat, diese auch von den sektorspezifischen Cybersicherheitsvorgaben der Verordnung über die Betriebsstabilität von Finanzunternehmen [Digital Operational Resilience Act (DORA), s. cep**Analyse**][18] auszunehmen.[19]

2.1.6 Sektorspezifische Regelungen

Existieren sektorspezifische EU-Rechtsakte zur Cybersicherheit für Einrichtungen im Anwendungsbereich der NIS 2-Richtlinie – wie etwa die Verordnung über die Betriebsstabilität von Finanzunternehmen – müssen diese Einrichtungen die Vorgaben der NIS 2-Richtlinie zum Management von Cyberrisiken (s. Abschnitt 2.2) und zur Meldung von Cybervorfällen und -bedrohungen (s. Abschnitt 2.3) nicht erfüllen, sofern die sektorspezifischen Vorschriften diesbezüglich mindestens äquivalent zu den Vorgaben der NIS 2-Richtlinie sind.[20]

---

15 Art. 2, NIS 2-Richtlinie.
16 Ebd.
17 Ebd.
18 Die DORA-Verordnung wurde parallel zur NIS 2-Richtlinie verhandelt und ergänzt die Richtlinie um sektorspezifische Regelungen zur Stärkung der Cybersicherheit von Finanzunternehmen. Ein Trilogergebnis zu diesem Rechtsakt wurde am 11. Mai erzielt. Mehr Details hier.
19 Art. 2 Abs. 3d, NIS 2-Richtlinie.
20 Art. 2b, NIS 2-Richtlinie.

2.2 Management von Cyberrisiken

Wie bereits die NIS 1-Richtlinie schreibt auch die NIS 2-Richtlinie den erfassten wesentlichen und wichtigen Einrichtungen die Ergreifung von Maßnahmen vor, um Cybersicherheitsrisiken adäquat zu managen. Dabei wird die NIS 2-Richtlinie nun konkreter und schränkt den Ermessensspielraum der Mitgliedstaaten deutlich ein.

2.2.1 Maßnahmen zur Beherrschung von Cyberrisiken:

Die von der Richtlinie erfassten Einrichtungen müssen „geeignete und verhältnismäßige technische, betriebliche und organisatorische Maßnahmen“ ergreifen, um die Risiken für die Sicherheit der Netz- und Informationssysteme (NIS), die sie für ihre Tätigkeiten oder für die Erbringung ihrer Dienste nutzen, zu beherrschen. Zudem müssen die ergriffenen Maßnahmen die Folgen von Cybervorfällen auf die Empfänger ihrer Dienste und auf andere Dienste eindämmen bzw. verhindern.[21] Die Maßnahmen, die neben der Sicherheit der NIS auch deren physische Umgebung schützen sollen, müssen insbesondere umfassen[22]

- die Risikoanalyse,
- die Erstellung von Sicherheitskonzepten für die Informationssysteme,
- Maßnahmen zur Bewältigung von Cybervorfällen, d.h. ihre Vorbeugung, Erkennung, Analyse, Eindämmung sowie Schritte zur Reaktion auf den Vorfall sowie zur Wiederherstellung nach einem Vorfall,
- Maßnahmen zur Aufrechterhaltung des Betriebs (z.B. Backup-Management und Notfallwiederherstellung) sowie zum Krisenmanagement,
- Schritte zur Gewährleistung der Sicherheit der Lieferketten,
- grundlegende Praktiken der Cyberhygiene und Schulungen zur Cybersicherheit,
- Einsatz von Multi-Faktor-Authentifizierungs- oder kontinuierlichen Authentifizierungslösungen und
- Strategien und Verfahren für den Einsatz von Kryptographie und ggfs. Verschlüsselungstechniken.

Die Verhältnismäßigkeit der Maßnahmen soll sich dabei am Grad der Risikoexposition der Einrichtung, ihrer Größe, der Wahrscheinlichkeit des Auftretens von Cybervorfällen und deren Schweregrad bemessen. Zudem sollen gesellschaftliche und wirtschaftliche Auswirkungen Berücksichtigung finden.[23]

Die Kommission kann technische, methodische und ggfs. sektorspezifische Spezifikationen für die Risikomanagementmaßnahmen im Rahmen von Durchführungsrechtsakten festlegen.[24]

2.2.2 Fokus Lieferkette

Einen Fokus richtet die NIS 2-Richtlinie auf Cybergefahren innerhalb der Lieferkette. So werden die wesentlichen und wichtigen Einrichtungen verpflichtet, Maßnahmen zur Stärkung der Sicherheit ihrer Lieferketten zu treffen. Im Fokus soll dabei das Verhältnis der Einrichtungen mit ihren „direkten“ Lieferanten und Dienstleistern (z.B. Cloud-Diensteanbieter) stehen. So sollen die Einrichtungen die spezifischen Schwachstellen und Cybersicherheitspraktiken jedes „direkten“ Lieferanten bzw. Dienstleisters in den Blick nehmen und insbesondere die Qualität gelieferter Produkte genau prüfen. Zudem müssen

[21] Art. 18 Abs. 1, NIS 2-Richtlinie.
[22] Art. 18 Abs. 2, NIS 2-Richtlinie.
[23] Art. 18 Abs. 1, NIS 2-Richtlinie.
[24] Art. 18 Abs. 5, NIS 2-Richtlinie.

die Einrichtungen im Rahmen ihres Risikomanagements besonders solche IKT-Produkte und -Dienste von ihren Lieferanten und Dienstleistern prüfen, die die EU-Kommission gemeinsam mit einer Kooperationsgruppe[25] und der ENISA[26] als besonders kritisch eingestuft hat.[27]

2.2.3 Cybersicherheitszertifizierung

Die Kommission soll künftig, sofern sie das Cybersicherheitsniveau als unzureichend einstuft, mittels delegierter Rechtsakte festlegen können, dass bestimmte Kategorien von wesentlichen bzw. wichtigen Einrichtungen nur noch IKT-Produkte oder IKT-Dienste einsetzen dürfen, die zertifiziert wurden oder die ein Zertifikat im Rahmen europäischer Cybersicherheitssysteme benötigen. Die Mitgliedsstaaten können ferner einzelne wesentliche und wichtige Einrichtungen dazu verpflichten nur noch bestimmte IKT-Produkte bzw. IKT-Dienste nutzen zu dürfen, die diese entweder selbst entwickeln oder von Dritten beziehen, und die im Rahmen europäischer Cybersicherheits-Zertifizierungssysteme zertifiziert sind. Hiermit sollen die Einrichtungen dann auch die Einhaltung der Maßnahmen zum Cyberrisikomanagement nachweisen können.[28]

2.2.4 Verantwortlichkeit der Leitungsorgane

Im Rahmen der NIS 2-Richtlinie soll auch die Verantwortung der Leitungsorgane der wesentlichen und wichtigen Einrichtungen für das Management der Cyberrisiken deutlich steigen. So fällt es künftig explizit in ihren Zuständigkeitsbereich, die Maßnahmen zum Risikomanagement zu billigen und deren Umsetzung zu überwachen. Die Leitungsorgane können für die Nichteinhaltung der Vorgaben der Richtlinie haftbar gemacht werden. Sie werden zudem dazu verpflichtet, regelmäßig an Schulungen zu Cybersicherheitsrisiken und deren Auswirkungen auf die Einrichtung teilzunehmen und sie sollen allen ihren Mitarbeitern ermöglichen, auch an ähnlichen Schulungen teilzunehmen.[29]

2.3 Meldung von Cybervorfällen und -bedrohungen

Wie auch schon die NIS 1-Richtlinie verpflichtet auch die neu gefasste NIS 2-Richtlinie die erfassten Einrichtungen dazu, Cybersicherheitsvorfälle zu melden. Nachdem die Regelungen in der NIS 1-Richtlinie recht vage waren und der Interpretationsspielraum sehr groß war, sieht die NIS 2-Richtlinie nun klarere Regeln vor, was, wann, an wen und wie Vorfälle gemeldet werden müssen.

2.3.1 Welche Cybervorfälle und -bedrohungen gemeldet werden müssen?

Wesentliche und wichtige Einrichtungen müssen alle „signifikanten“ Cybervorfälle melden. Als „signifikant gelten Cybervorfälle dann, wenn sie[30]

- zu erheblichen Betriebsstörungen des Dienstes der Einrichtung führen oder führen können,
- zu erheblichen finanziellen Verlusten für die Einrichtung führen,

[25] Die Kooperationsgruppe ist ein Gremium aus Vertretern der Mitgliedstaaten, der Kommission und der ENISA. Es unterstützt den Informationsaustausch zwischen den Mitgliedstaaten bezüglich der Anwendung der Richtlinie.
[26] Die European Network and Information Security Agency (ENISA) ist eine bereits 2004 etablierte EU-Cybersicherheitsagentur.
[27] Art. 18 Abs. 2 und 3, Art. 19, NIS 2-Richtlinie.
[28] Art. 21, NIS 2-Richtlinie.
[29] Art. 17, NIS 2-Richtlinie.
[30] Art. 20 Abs. 1 und 3, NIS 2-Richtlinie.

- zu erheblichen materiellen oder immateriellen Verlusten für andere natürliche oder juristische Personen führen oder führen können.

Die Einrichtungen müssen zudem ggfs. auch den Nutzern ihrer Dienste, die potenziell von einer „signifikanten Cyberbedrohung“[31] betroffen sein könnten, über (Abhilfe-)Maßnahmen informieren, mit denen sie der Bedrohung begegnen können. Ggfs. informieren sie die Nutzer auch über die Bedrohung selbst.[32]

2.3.2 Wann Cybervorfälle gemeldet werden müssen

24h-Meldung: Die Meldung muss grundsätzlich „unverzüglich“ erfolgen. In jedem Fall ist eine Meldung im Sinne einer „Frühwarnung“ jedoch zumindest binnen 24 Stunden nach Bekanntwerden eines solchen Vorfalls abzugeben. In dieser Erstmeldung muss angegeben werden, ob der Vorfall vermutlich durch eine rechtswidrige oder böswillige Handlung verursacht wurde und inwiefern er grenzüberschreitende Folgen hat.[33]

74h-Meldung: Binnen 72 Stunden nach Bekanntwerden des Cybervorfalls muss eine zweite Meldung abgegeben werden. Diese soll die Erstmeldung aktualisieren und eine erste Analyse des Vorfalls enthalten, insbesondere hinsichtlich dessen Schwere und Auswirkungen und, falls bereits möglich, zu Indikatoren für Gefährdungen.[34]

Zwischenbericht: Eine weitere Meldung hat auf Ersuchen des CSIRT oder der zuständigen Behörde zu erfolgen. Diese hat die Form eines Zwischenberichts und soll Status-Updates enthalten.[35]

Abschlussbericht: Binnen eines Monats nach der 74h-Frist-Meldung muss ferner 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.[36]

Fortschrittsbericht: Ist ein Cybervorfall auch binnen eines Monats nicht behoben, muss statt des Abschlussberichts ein Fortschrittsbericht vorgelegt werden. Der Abschlussbericht muss dann spätestens einen Monat, nachdem es gelungen ist, den Vorfall zu beheben, vorgelegt werden.[37]

2.3.3 An wen Cybervorfälle gemeldet werden müssen

Die Cybervorfälle müssen in erster Linie den nationalen Reaktionsteams für IT-Sicherheitsvorfälle (CSIRTs) gemeldet werden oder ggfs. den zuständigen nationalen Behörden. Geht die Meldung an eine zuständige Behörde, muss diese die Meldung an das CSIRT weiterleiten. Falls angemessen, müssen die Einrichtungen zudem ihre Dienstnutzer informieren.[38] Dabei ist festgelegt, dass eine Notifizierung eines solchen Cybervorfalls nicht dazu führen soll, dass die meldende Einrichtung mit höheren Haftungsrisiken rechnen muss.[39]

---

[31] Eine „signifikante Cyberbedrohung“ ist eine Cyberbedrohung, bei der davon ausgegangen werden kann, dass sie das Potenzial hat, die NIS einer Einrichtung oder ihrer Nutzer durch die Verursachung erheblicher materieller oder immaterieller Verluste schwer zu schädigen [Art. 4 Abs. 1 Ziff. 7a].
[32] Art. 20 Abs. 2, NIS 2-Richtlinie.
[33] Art. 20 Abs. 1 und 4, NIS 2-Richtlinie.
[34] Art. 20 Abs. 4, NIS 2-Richtlinie.
[35] Ebd.
[36] Ebd.
[37] Ebd.
[38] Art. 20 Abs. 1, NIS 2-Richtlinie.
[39] Art. 20 Abs. 1, NIS 2-Richtlinie.

2.3.4 Reaktion der Aufsichtsbehörden

Das CSIRT oder die zuständige Behörde müssen unverzüglich und falls möglich binnen 24 Stunden eine erste Rückmeldung abgeben und auf Ersuchen des Unternehmens Hilfe zur Durchführung von Abhilfemaßnahmen bereitstellen. Das CSIRT oder die zuständige Behörde 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.[40]

2.4 Aufsicht, Durchsetzung und Sanktionen

Die NIS 2-Richtlinie sieht vor, dass sowohl die wesentlichen als auch die wichtigen Einrichtungen einer Aufsicht unterliegen sollen. So sollen nationale Aufsichtsbehörden darüber wachen, dass die Einrichtungen den Vorgaben zum Risikomanagement und zur Meldung von Cybervorfällen genüge leisten. Generell soll nationalen Behörden ein Mindestumfang an Aufsichtsbefugnissen eingeräumt werden, u. a. für Vor-Ort-Prüfungen oder auch für regelmäßige und gezielte Sicherheitsprüfungen bei den beaufsichtigten Unternehmen, inklusive Adhoc-Prüfungen im Fall schwerwiegender Cybervorfälle.[41]

Die Aufsicht über wichtige Einrichtungen soll weniger streng ausfallen als bei wesentlichen Einrichtungen. Während für letztere nur eine ex-post-Aufsicht vorgesehen ist, die erst auf Basis von Hinweisen und Informationen zu potenziellen Verstößen gegen die Richtlinie aktiviert wird, soll für wesentliche Einrichtungen eine vollumfängliche – d.h. ex-ante und ex-post – Aufsicht greifen.[42]

Die nationalen Aufsichtsbehörden sollen zudem eine Reihe von Durchsetzungsbefugnissen erhalten. So sollen sie bspw. Verwarnungen an wesentliche und wichtige Einrichtungen erteilen dürfen, sofern sie den Vorgaben der Richtlinie nicht Folge leisten. Auch verbindliche Anweisungen, etwa zu Schritten zur Vorbeugung oder Eindämmung von Cybervorfällen, inklusive Zeitvorgaben für deren Implementierung, sollen sie geben können.[43]

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.[44]

2.5 Umsetzung der NIS 2-Richtlinie

Nachdem sich der Rat und das EP nun im Trilog geeinigt haben, müssen die beiden Gesetzgebungsorgane dem gefundenen Kompromiss nun noch formal zustimmen. Damit ist im Frühherbst zu rechnen. Nach dem Inkrafttreten der Richtlinie haben die Mitgliedstaaten dann 21 Monate Zeit, die erforderlichen Rechts- und Verwaltungsvorschriften in nationalem Recht zu verankern.[45] Mit einer Anwendung der Richtlinie ist daher frühestens 2025 zu rechnen.

---

[40] Art. 20 Abs. 7, NIS 2-Richtlinie.
[41] Art. 29 Abs. 1 und 2 und Art. 30 Abs. 1 und 2, NIS 2-Richtlinie.
[42] Erwägungsgrund 70, Art. 29 und Art. 30, NIS 2-Richtlinie.
[43] Art. 29 Abs. 4 und Art. 30 Abs. 4, NIS 2-Richtlinie.
[44] Art. 29 Abs. 5 und 6, Art. 30 Abs. 5 und 6, NIS 2-Richtlinie.
[45] Art. 38, NIS 2-Richtlinie.

3 Bewertung

Vor dem Hintergrund zunehmender Cyberbedrohungen und -vorfälle haben das EP und der Rat nun beschlossen, mit der NIS 2-Richtlinie eine Vielzahl von Unternehmen sowie Einrichtungen des öffentlichen Sektors dazu zu verpflichten, verstärkt Maßnahmen zum Management von Cybersicherheitsrisiken zu ergreifen und signifikante Cybervorfälle an Aufsichtsbehörden zu melden. Aber sind diese regulatorischen Vorgaben zur Stärkung der europäischen Cyberresilienz wirklich notwendig? Grundsätzlich ließe sich argumentieren, dass Unternehmen bereits ein Eigeninteresse daran haben müssten, ihre Netz- und Informationssysteme (NIS) vor Cybervorfällen und -bedrohungen hinreichend zu schützen. Denn tun sie dies nicht, kann dies im Angriffsfall zu erheblichen Umsatzverlusten und Reputationsschäden führen. Unternehmen müssten daher eigentlich von sich aus gewillt sein, in die Stabilität ihrer Systeme zu investieren. Dies ist jedoch häufig ein Trugschluss. Denn regelmäßig sind die wirtschaftlichen Anreize für Investitionen in Cybersicherheit unzureichend. Denn erstens müssen Unternehmen, die von einem Cybervorfall betroffen sind, oft nicht die vollen Kosten der mangelnden Sicherheit ihrer Netz- und Informationssysteme tragen. Stattdessen können sie regelmäßig einen Teil dieser Kosten auf Dritte, etwa ihre Kunden, abwälzen. Zweitens erhöhen die Anstrengungen des einen Unternehmens in die Stärkung seiner Cyberresilienz oft auch die Resilienz anderer Unternehmen. Unternehmen preisen diese positiven externen Effekte jedoch selten in ihr Entscheidungskalkül mit ein. Einheitliche Vorgaben zum Management von Cyberrisiken sind daher angemessen, auch im Sinne des Charakters der Cybersicherheit als öffentliches Gut und einem grundsätzlichen hoheitlichen Interesse an stabilen und resilienten Volkswirtschaften. Dies gilt umso eher, je relevanter ein Unternehmen für die Grundversorgung bzw. für die Funktionsfähigkeit einer Gesellschaft ist, da deren Beeinträchtigung oder Ausfall mit besonders hohen Kosten für die Gesellschaft verbunden ist. Die anvisierte Abstufung bei der Regulierungstiefe zwischen wesentlichen und wichtigen Unternehmen ist daher sachgerecht, ungeachtet der vielfältigen Verwobenheiten und kritischen Abhängigkeiten, wie sie auch zwischen wesentlichen und wichtigen Unternehmen bestehen.

Der Geltungsbereich der NIS 2-Richtlinie bietet jedoch auch Raum für Kritik. Zwar wird durch die Überarbeitung der NIS 1-Richtlinie der Anwendungsbereich klarer gefasst, sodass mehr Rechtssicherheit darüber geschaffen wurde, wer von den NIS 2-Vorschriften betroffen ist. Damit werden auch die Möglichkeiten für Regulierungsarbitrage begrenzt und Wettbewerbsverzerrungen vorgebeugt. Allerdings ist der Geltungsbereich der Richtlinie nun zu weit gefasst: Denn es fallen auch viele Unternehmen darunter, die keine Produkte oder Dienstleistungen anbieten, die für die Versorgung und das Funktionieren einer Gesellschaft als absolut zentral gelten können. Dazu zählen etwa die Unternehmen aus dem verarbeitenden Gewerbe, wie etwa Maschinenbauunternehmen. Zudem ist fraglich, ob die Aufsichtsbehörden in der Praxis mit der Aufsicht über ca. 160.000 Unternehmen und öffentliche Stellen nicht überfordert sind und daher eine stärkere Priorisierung angezeigt gewesen wäre. Ferner ist die Größe einer Einrichtung als alleiniges Kriterium für ihre Aufnahme in den Geltungsbereich ungeeignet, da diese allein nicht zwangsläufig auf ein höheres Cybersicherheitsrisiko hindeutet. Andere Kriterien hätten hier ebenfalls eine Rolle spielen sollen, wie etwa die Anzahl der Kunden eines Unternehmens.

Dass wesentliche und wichtige Einrichtungen im Rahmen ihres Risikomanagements nun Risiken der Lieferkette in größerem Umfang als nach der NIS 1-Richtlinie berücksichtigen müssen, kann das Cybersicherheitsniveau in der EU erhöhen. Jedoch sollte die Verantwortung der Sicherstellung der Cybersicherheit nicht allein auf den Schultern der wesentlichen und wichtigen Einrichtungen am Ende der Wertschöpfungskette liegen. Denn eine intensive Prüfung jedes einzelnen Lieferanten innerhalb der Lieferkette wäre nicht nur zeitaufwändig, sondern würde auch nur mir enormen Kosten einhergehen.

Dass nun auf die direkten Lieferanten abgestellt wird, ist daher sachgerecht. Entscheidend ist ferner, dass es auch direkte Vorgaben für die Lieferanten von IKT-Produkten und -Diensten geben sollte, sie also mit in die Verantwortung genommen werden. Dass die Kommission hierfür mit dem „Cyber Resilience Act“ voraussichtlich am 13. September 2022 legislative Schritte plant und Cybersicherheitsanforderungen für digitale Produkte schaffen will, ist daher zu begrüßen.

Die Verpflichtung zur Meldung schwerwiegender Cybervorfällen an Aufsichtsbehörden ist sachgerecht. Denn von solchen Vorfällen betroffene Einrichtungen haben oft aufgrund von hohen Meldekosten sowie wegen der mit solchen Meldungen einhergehenden potenziellen Reputationsschäden wenige Anreize, dies freiwillig zu tun. Die Meldungen haben jedoch häufig einen hohen externen Nutzen, da sie etwa anderen dabei helfen, Sicherheitslücken zu erkennen und zu schließen. Positiv sind auch die Festlegung klarer Fristen und Abläufe zur Meldung von Cybervorfällen. Diese erhöhen einerseits die Rechtsklarheit und reduzieren andererseits den Verwaltungsaufwand für die meldepflichtigen Einrichtungen, da diese nun die Meldung nunmehr an eine zentrale Stelle abgeben können. Die rasche Meldung von Cybervorfällen ist dabei zwingend, um Schäden rasch eindämmen zu können. Die 24h-Frist ist daher zwar ambitioniert, aber letztlich alternativlos. Jedoch darf der Wert dieser Erstmeldung nicht überschätzt werden. Denn es ist fraglich, ob in dieser kurzen Frist hinreichend aussagekräftige Informationen übermittelt werden können. Dies gilt insbesondere für kleinere Unternehmen, die ggfs. nicht auf allzu große Inhouse-Ressourcen zur Analyse von Cybervorfällen zurückgreifen können, zumal solch zeitnahe Meldeanforderungen auch wertvolle Kapazitäten binden können, die für die Bewältigung der Cybervorfälle eingesetzt werden sollten.

Grundsätzlich reichen die strengeren Maßnahmen zum Risikomanagement und die Meldepflichten der NIS 2-Richtlinie natürlich nicht aus, um die Resilienz der europäischen Unternehmenslandschaft hinsichtlich Cyberrisiken sicherzustellen. Sie können nur ein Baustein sein. Sie sind jedoch ein zentraler Eckpfeiler in einem Konzert aus zahlreichen insbesondere nationalen, aber auch europäischen Regulierungsmaßnahmen. Neben den in diesem cep**Adhoc** dargestellten Schritten enthält die NIS 2-Richtlinie bspw. noch zahlreiche Maßnahmen zur Verbesserung der Zusammenarbeit der Mitgliedstaaten oder auch der relevanten Behörden bei Cybervorfällen. Zudem wurde der „Agentur der Europäischen Union für Cybersicherheit (ENISA)“ zahlreiche neue Aufgaben übertragen und bereits ein EU-Regelwerk zur Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik geschaffen [Verordnung (EU) 2019/881, s. cep**Analyse** (zur ENISA) und cep**Analyse** (zur Cybersicherheitszertifizierung)]. Und auch der noch für diese Woche angekündigte „Cyber Resilience Act“ soll einen wesentlichen Beitrag zur Stärkung der Sicherheit der vernetzten europäischen Volkswirtschaften leisten.

Centrum für Europäische Politik
FREIBURG | BERLIN

Autor:

Philipp Eckhardt, Wissenschaftlicher Referent des Fachbereichs Finanzmärkte und Informationstechnologien

eckhardt@cep.eu

Centrum für Europäische Politik FREIBURG | BERLIN
Kaiser-Joseph-Straße 266 | D-79098 Freiburg
Schiffbauerdamm 40 Raum 4315 | D-10117 Berlin
Tel. + 49 761 38693-0