CYBERSICHERHEIT – TEIL 1: ENISA-REFORM

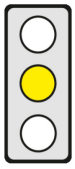
Centrum für Europäische Politik

cep**Analyse** Nr. 06/2018

KERNPUNKTE

Ziel der Verordnung: Die Cybersicherheit soll erhöht und dafür die EU-Cybersicherheitsagentur ENISA gestärkt werden.

Betroffene: ENISA, Mitgliedstaaten, Unternehmen.



Pro: Die Verbesserung der Cybersicherheit ist geboten und muss angesichts der grenzüberschreitenden Dimension auf EU-Ebene erfolgen. Die Entfristung des Mandats der ENISA sowie die Aufstockung ihrer Mittel und ihres Personals sind daher sachgerecht.

Contra: (1) Eine Verlagerung von operativen Aufgaben auf die ENISA kann dazu führen, dass Anstrengungen auf nationaler Ebene unterbleiben („Trittbrettfahrerverhalten").

(2) Klarzustellen ist, ob die Mitgliedstaaten Untersuchungen durch die ENISA ablehnen dürfen, welche Handlungen die ENISA vornehmen und inwieweit sie sensible Informationen nutzen darf.

Die wichtigsten Passagen im Text sind durch einen Seitenstrich gekennzeichnet.

INHALT

Titel

Vorschlag COM(2017) 477 vom 4. Oktober 2017 für eine **Verordnung** des Europäischen Parlaments und des Rates **über die „EU-Cybersicherheitsagentur" (ENISA)** und zur Aufhebung der Verordnung (EU) Nr. 526/2013 sowie über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik

Kurzdarstellung

- **Hintergrund und Ziele**
  - Laut Kommission führt die zunehmende Digitalisierung und Vernetzung vieler gesellschaftlicher Bereiche zu einem Anstieg von Cybersicherheitsrisiken und -angriffen (Erwägungsgrund 2 und 3).
  - Die Kommission will deshalb insbesondere (Erwägungsgrund 5)
    - die Zusammenarbeit zwischen Mitgliedstaaten und EU-Organen, -Einrichtungen und -Stellen verbessern,
    - die Fähigkeiten der Mitgliedstaaten und Unternehmen bei der Abwehr von Cyberangriffen stärken, und
    - das Vertrauen in den digitalen Binnenmarkt durch mehr Transparenz über das Niveau der Sicherheit von Informations- und Kommunikationstechnik (IKT) stärken.
  - Dies soll im Wesentlichen erreicht werden durch (Begründung S. 4 und 7, Erwägungsgrund 11)
    - die Reform der in Griechenland ansässigen EU-Cybersicherheitsagentur „ENISA" (diese cep**Analyse**) und
    - die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik (s. cep**Analyse**).
  - Die vorgeschlagene Verordnung ersetzt die geltende ENISA-Verordnung [(EG) Nr. 526/2013]
  - Die ENISA wurde 2004 gegründet. Als Kompetenzzentrum zur Verbesserung der Netz- und Informationssicherheit unterstützt sie auch die Mitgliedstaaten. (Begründung S. 4, Art. 35)
  - Die ENISA-Reform umfasst neben kleineren organisatorischen Anpassungen
    - die Entfristung ihres befristeten Mandats und die Erhöhung ihrer Finanzausstattung,
    - die Übertragung von zusätzlichen Funktionen und Aufgaben an die ENISA.

- **Entfristung des Mandats, Budget und Personal der ENISA**
  - Das Mandat der ENISA ist bis 2020 befristet. Es wird nun entfristet. (Begründung S. 4, Art. 57 Abs. 4)
  - Das Budget der ENISA soll von bisher 11 Mio. Euro auf 23 Mio. Euro im Jahr 2022 steigen (S. 102).
  - Das Personal der ENISA soll von derzeit 84 auf 125 Mitarbeiter im Jahr 2022 steigen (S. 98).

- **Wesentliche Änderungen an der Organisation der ENISA**
  - Die ENISA kann künftig in einzelnen Mitgliedstaaten Außenstellen einrichten, wenn die Kommission, der Verwaltungsrat und der betroffene Mitgliedstaat dem zustimmen (Art. 12 lit. c, Art. 19, Art. 33).
  - Der Exekutivrat, der den Verwaltungsrat unterstützt, kann für diesen künftig in dringenden Fällen vorläufige Beschlüsse fassen, „vor allem" in Verwaltungs- und Haushaltsangelegenheiten (Art. 12 lit. b, Art. 18).

- **Operative Zusammenarbeit auf EU-Ebene**
  - Die ENISA „unterstützt" bisher die Kooperationsgruppe und das Netzwerk der nationalen Computer-Notfallteams (CSIRTs) bei der Organisation von EU-weiten Cybersicherheitsübungen und berät die Mitgliedstaaten auf deren Antrag bei nationalen Übungen. Künftig „organisiert" sie „jährlich" EU-weite Übungen zur Vorbereitung von gemeinsamen Reaktionen auf „massive, grenzüberschreitende Cybersicherheitsvorfälle" und unterstützt die Mitgliedstaaten auf deren Antrag bei der Organisation dieser Übungen. (Art. 7 Abs. 6)

Autoren: Philipp Eckhardt und Dr. Anja Hoffmann | eckhardt@cep.eu
cep | Kaiser-Joseph-Straße 266 | 79098 Freiburg | Telefon 0761 38693-107 | www.cep.eu

- Die ENISA führt künftig das Sekretariat des Netzwerks der nationalen CSIRTs (Art. 7 Abs. 3 i.V.m. Art. 12 Abs. 2 der NIS-Richtlinie). Sie unterstützt die Mitgliedstaaten innerhalb des Netzes dabei, ihre Fähigkeiten zur „Verhütung, Erkennung und Bewältigung von Sicherheitsvorfällen“ zu verbessern, analysiert Anfälligkeiten, „Artefakte“ und Sicherheitsvorfälle und stellt, falls gewünscht, „technische Hilfe“ bei Vorfällen mit „beträchtlichen oder erheblichen Auswirkungen“ bereit (Art. 7 Abs. 4).
- Die ENISA unterstützt oder unternimmt künftig Ex-post-Untersuchungen von gemeldeten Sicherheitsvorfällen mit „beträchtlichen oder erheblichen Auswirkungen“, wenn mindestens (Art. 7 Abs. 5)
  - zwei betroffene Mitgliedstaaten dies beantragen oder
  - zwei Mitgliedstaaten betroffen sind und die Kommission sie, im Einvernehmen mit allen betroffenen Mitgliedstaaten, dazu auffordert.
- Die ENISA erstellt künftig regelmäßig einen „technischen Lagebericht“ zur Cybersicherheit in der EU und unterstützt die Entwicklung gemeinsamer Schritte zur Reaktion auf „massive, grenzüberschreitende Cybersicherheitsvorfälle oder Cyberkrisen“ (Art. 7 Abs. 7 und 8).

- **Entwicklung und Umsetzung der EU-Politik und des EU-Rechts**
  - Die ENISA trägt wie bisher zur Entwicklung und Umsetzung der EU-Politik und des EU-Rechts zur Cybersicherheit bei durch Beratung, Vorbereitungsarbeiten und Analysen (Art. 5). Künftig tut sie dies auch durch
    - Stellungnahmen, Leitlinien und Austausch bewährter Verfahren zum Risikomanagement und zur Meldung von Sicherheitsvorfällen im Rahmen der Richtlinie zur Netz- und Informationssicherheit [NIS-Richtlinie (EU) 2016/1148, s. cep**Analyse**] (Art. 5 Abs. 2),
    - sektorspezifische Strategien und Rechtsetzungsinitiativen (Art. 5 Abs. 1),
    - das Einbringen von Sachkenntnis in die Arbeit der Kooperationsgruppe, die neben der ENISA aus Vertretern der Mitgliedstaaten und der Kommission besteht (Art. 5 Abs. 3 i.V.m. Art. 11 der NIS-Richtlinie),
    - Beratung, technische Leitlinien und Austausch bewährter Verfahren im Bereich der elektronischen Identität und Vertrauensdienste und zur Förderung eines „höheren Sicherheitsniveaus in der elektronischen Kommunikation“ (Art. 5 Abs. 4 Ziff. 1 und 2), und
    - Jahresberichte zum Stand der Umsetzung des EU-Rechts zu Sicherheitsvorfällen und Integritätsverlusten, die von „Betreibern wesentlicher Dienste“ – u.a. Energieversorger–, von Vertrauensdienstanbietern sowie von TK-Netzbetreibern und -Diensteanbietern gemeldet werden [Art. 5 Abs. 5 i.V.m. Art. 10 Abs. 3 der NIS-Richtlinie, s. cep**Analyse**, Art. 19 Abs. 3 der eIDAS-Verordnung (EU) Nr. 910/2014, s. cep**Analyse**, und Art. 40 des Kodex für elektronische Kommunikation (COM(2016) 590)].

- **Aufbau von Fähigkeiten und Kompetenzen gegen Cybersicherheitsvorfälle**
  - Die ENISA unterstützt EU-Einrichtungen und Mitgliedstaaten wie bisher bei der „Verhütung, Erkennung und Analyse“ von Cybersicherheitsvorfällen und bei der „Stärkung ihrer Kapazitäten“, d.h. ihrer Fähigkeit zur Bewältigung der Vorfälle. Die Mitgliedstaaten müssen diese Unterstützung bisher beantragen. Künftig kann die ENISA ihnen gegenüber von sich aus tätig werden. (Begründung S. 8, Art. 6 Abs. 1 lit. a und b)
  - Die ENISA unterstützt künftig die Mitgliedstaaten auf deren Antrag beim Aufbau nationaler Computer-Notfallteams (CSIRTs), die Sicherheitsvorfälle auf nationaler Ebene überwachen, Frühwarnungen herausgeben und auf sie reagieren. Ferner unterstützt sie die Mitgliedstaaten auf deren Antrag hin bei der Entwicklung nationaler Strategien für die Sicherheit von Netz- und Informationssystemen und fördert deren EU-weite Verbreitung. (Art. 6 Abs. 1 lit. c und d i.V.m. Art. 7 Abs. 2 und Art. 9 Abs. 5 der NIS-Richtlinie)
  - Für „Betreiber wesentlicher Dienste“ gelten besondere Anforderungen an die Sicherheit ihrer Netz- und Informationssysteme; insbesondere müssen sie Sicherheitsvorfälle an ihre zuständige Behörde oder ihr CSIRT melden (Art. 14 der NIS-Richtlinie). Die Mitgliedstaaten legen jeweils die „Betreiber wesentlicher Dienste“ in ihrem Hoheitsgebiet fest (Art. 8 der NIS-Richtlinie). Die ENISA unterstützt die Mitgliedstaaten künftig im Rahmen der Kooperationsgruppe durch den Austausch bewährter Verfahren bei der Ermittlung der „Betreiber wesentlicher Dienste“ (Art. 6 Abs. 1 lit. i i.V.m. Art. 11 Abs. 3 lit. l der NIS-Richtlinie).
  - Die ENISA fördert künftig den Aufbau von sektorspezifischen Informationsaustausch- und -analysezentren (ISACs), insbesondere für Sektoren mit Betreibern wesentlicher Dienste (Art. 6 Abs. 2).

Subsidiaritätsbegründung der Kommission

Weil die grenzübergreifenden Abhängigkeiten zwischen Netz- und Informationssystemen groß sind, können einzelne Akteure die Cybersicherheitsbedrohungen nicht alleine bewältigen. Daher sind EU-Maßnahmen notwendig.

Politischer Kontext

2016 wurde die Richtlinie zur Netz-und Informationssicherheit [RL (EU) 2016/1148, s. cep**Analyse**] verabschiedet. Zudem legte die Kommission eine Mitteilung zur Stärkung der Abwehrfähigkeit Europas bei der Cybersicherheit vor [COM(2016) 410], in der sie die Überprüfung der ENISA-Verordnung ankündigte.

Stand der Gesetzgebung

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

Politische Einflussmöglichkeiten

Generaldirektionen:	GD Kommunikationsnetze, Inhalte und Technologien (federführend)
Ausschüsse des Europäischen Parlaments:	Industrie, Technologie und Energie (federführend), Berichterstatterin: Angelika Niebler (EVP-Fraktion, Deutschland)
Bundesministerien:	Bundesministerium für Inneres (federführend)
Ausschüsse des Deutschen Bundestags:	Innenausschuss (federführend)
Entscheidungsmodus im Rat:	Qualifizierte Mehrheit (Annahme durch 55% der Mitgliedstaaten, die 65% der EU-Bevölkerung ausmachen)

Formalien

Kompetenznorm:	Art. 114 AEUV (Binnenmarkt)
Art der Gesetzgebungszuständigkeit:	Geteilte Zuständigkeit (Art. 4 Abs. 2 AEUV)
Verfahrensart:	Art. 294 AEUV (ordentliches Gesetzgebungsverfahren)

BEWERTUNG

Ökonomische Folgenabschätzung

Der wirtschaftliche Schaden durch Cyberkriminalität in der EU hat sich nach Angaben der Kommission zwischen 2013 und 2017 verfünffacht und könnte sich bis 2019 vervierfachen (Mitteilung JOIN(2017) 450, S. 2]. Cybersicherheitsvorfälle treffen häufig nicht nur einzelne Mitgliedstaaten. Auch verfügen etliche EU-Staaten über kein der Bedrohung angemessenes Sicherheitsniveau und gefährden damit im einheitlichen Markt auch die übrigen Länder.

Die Verbesserung der Cybersicherheit ist angesichts dieser Entwicklung **geboten und muss angesichts der grenzüberschreitenden Dimension auf EU-Ebene erfolgen. Die Entfristung des Mandats der ENISA sowie die Aufstockung ihrer Mittel und ihres Personals sind daher sachgerecht.** Fungiert die ENISA als zentrale Stelle, über die die Mitgliedstaaten sich zu Cyberbedrohungen und -sicherheitsvorfällen austauschen, Tätigkeiten koordinieren und bewährte Praktiken bekanntgeben können, reduziert dies Kosten und hebt Synergien.

Eine darüberhinausgehende **Verlagerung von operativen Aufgaben auf die ENISA kann** jedoch **dazu führen, dass Anstrengungen auf nationaler Ebene** zur Stärkung der Cybersicherheit **unterbleiben („Trittbrettfahrerverhalten").** Diese Gefahr droht in denjenigen Mitgliedstaaten, die nur über schwache Strukturen zur Abwehr von Cybergefahren verfügen. Dies gilt es zu vermeiden. Neben Unternehmen und Bürgern sollten auch die Mitgliedstaaten für cybersichere IT-Infrastrukturen sorgen. Denn häufig besteht auf nationaler Ebene aufgrund der Nähe zu von Sicherheitsvorfällen betroffenen Unternehmen und Bürgern ein Wissensvorsprung, den die ENISA nur mit hohem Ressourcenaufwand – sie müsste letztlich in jedem Mitgliedstaat eine Außenstelle einrichten – aufholen könnte. Damit sind Effizienzgewinne durch eine Übertragung von operativen Aufgaben an die ENISA unwahrscheinlich.

Die ENISA sollte daher in erster Linie koordinierend tätig sein. Folglich sind auch einige der neuen Aufgaben der ENISA – etwa die Bereitstellung „technischer Hilfe", die sonstige operative Unterstützung bei Sicherheitsvorfällen und deren Ex-post-Untersuchung – in der vorgesehenen Form nicht zielführend. Sie sorgen entweder für unnötige Doppelstrukturen oder aber es unterbleiben in der Konsequenz Maßnahmen auf nationaler Ebene zur Stärkung der Cybersicherheit. Sollten der ENISA diese operativen Funktionen dennoch angedient werden, ist es notwendig, dass Mitgliedstaaten, die auf die Hilfe der ENISA zurückgreifen wollen, diese Unterstützung auch vergüten müssen.

Andere operative Aufgaben der ENISA – etwa gemeinsame Cybersicherheitsübungen bieten einen echten Mehrwert. Denn der dabei stattfindende Austausch über effektive Strategien zur Reaktion auf Sicherheitsvorfälle kann Synergie- und Lerneffekte erzeugen, die bei rein nationalen Übungen nicht in gleichem Maße entstehen können.

Fraglich ist, ob die zusätzlichen Mittel und das zusätzliche Personal der ENISA –-12 Mio. Euro, 41 Mitarbeiter – für ihre neuen Aufgaben ausreichen. Schon mit der 2016 in Kraft getretenen NIS-Richtlinie hat die ENISA viele zusätzliche nichtoperative Aufgaben bekommen, etwa beim Austausch bewährter Verfahren zum Risikomanagement und bei der Meldung von Sicherheitsvorfällen, beim Aufbau nationaler Computer-Notfallteams (CSIRTs) und bei der Entwicklung nationaler Strategien für die Sicherheit von Netz- und Informationssystemen. Es sollten daher die Erfahrungen mit der NIS-Richtlinie abgewartet werden, bevor der Mittel- und Personalbedarf der ENISA für die Aufgaben im Bereich der Cybersicherheit fixiert wird und die ENISA operative Aufgaben übertragen bekommt.

Juristische Bewertung

Kompetenz

Der Europäische Gerichtshof hat schon 2006 entschieden, dass die Schaffung der ENISA sowie die Übertragung der in der ENISA-Verordnung [(EG) Nr. 460/2004] vorgesehenen Aufgaben auf die ENISA durch die Binnenmarktkompetenz (Art. 114 AEUV) gedeckt sind. Der Unionsgesetzgeber hat bei komplexen technischen Materien ein weites Ermessen und darf als „Angleichungsmaßnahme" auch Befugnisse an eine Unionsagentur übertragen, soweit diese Aufgaben im engen Zusammenhang mit den Zielen eines Harmonisierungspakets stehen und zu dessen Umsetzung, Anwendung oder einheitlicher Durchführung beitragen können (Rs. C-217/04, Rn. 44 ff; Rs C-270/12, Rn. 103). Dies ist auch bei der Erweiterung des Aufgabenbereichs der ENISA der Fall, durch die das ordnungsgemäße Funktionieren des Binnenmarkts gewährleistet werden soll (Art. 1). Die neuen Aufgaben der ENISA stehen im engen Zusammenhang mit den Zielen der NIS-Richtlinie und des EU-Telekommunikationsrechts, zu denen auch die Sicherstellung der – für das Funktionieren des Binnenmarkts notwendigen – Integrität und Verfügbarkeit von Netz-und Informationssystemen gehört. Die Tätigkeit der ENISA soll und kann (Art. 5 Nr. 2) die einheitliche Umsetzung, Anwendung und Durchführung dieser Rechtsakte erleichtern. Die Verordnung wird daher zu Recht auf Art. 114 AEUV gestützt.

Subsidiarität

Unproblematisch. Die Mitgliedstaaten können die kollektive Cybersicherheit der EU durch rein dezentrale Aktionen nicht ausreichend gewährleisten. Die Koordinierung und Unterstützung durch die ENISA ist zur Gewährleistung der wirksamen und einheitlichen Durchsetzung des EU-Rechts erforderlich. Auch die operativen Befugnisse der ENISA, bei schwerwiegenden Sicherheitsvorfällen auf Ersuchen technische Hilfe bereitzustellen und/oder Ex-post-Untersuchungen zu unterstützen oder selbst vorzunehmen, haben gegenüber rein nationalem Handeln vor allem dann einen Mehrwert, wenn die Mitgliedstaaten – bzw. ihre nationalen CSIRTs – hierzu im Einzelfall nicht ausreichend in der Lage sind.

Verhältnismäßigkeit gegenüber den Mitgliedstaaten

Unklar ist, wie weit die neuen operativen **Befugnisse der ENISA zur Durchführung von** Analysen und Ex-post-**Untersuchungen von Sicherheitsvorfällen** (zusammengefasst: Untersuchungen) **reichen. Präzisiert werden muss**, **welche Handlungen die ENISA** dabei im Einzelnen **vornehmen darf und** ob sie auch in Mitgliedstaaten tätig werden darf, die eine Untersuchung ablehnen. Es muss geklärt werden, **ob die Mitgliedstaaten Untersuchungen durch die ENISA ablehnen** oder bestimmte sensible Bereiche hiervon ausnehmen **dürfen**, und wenn ja, unter welchen Voraussetzungen – z.B. wenn aus ihrer Sicht überwiegende nationale (Sicherheits-)Interessen entgegenstehen oder nur dann, wenn die Untersuchung sich auf Bereiche erstreckt, die ihre – enger zu fassende – „nationale Sicherheit", d.h. den Bestand oder die Funktionsfähigkeit ihres Staates berühren. Da die nationale Sicherheit in die alleinige Verantwortung der Mitgliedstaaten fällt (Art. 4 Abs. 2 S. 2 EUV), ist ein klarstellender Ablehnungsvorbehalt mindestens für diese Fälle nötig.

Zudem dürfen die Mitgliedstaaten die Erteilung von Auskünften, deren Preisgabe „wesentliche Sicherheitsinteressen" entgegenstehen, gegenüber der ENISA verweigern (Art. 346 Abs. 1 lit. a AEUV). **Inwieweit die ENISA** aber – ggf. auch gegen den Willen eines Mitgliedstaats – sicherheitsrelevante oder andere **sensible Informationen selbst erheben und nutzen darf und wie sie diese Informationen schützen muss, sollte** daher **ebenfalls klargestellt werden**.

Sonstige Vereinbarkeit mit EU-Recht

Die Befugnisse der ENISA, Analysen bzw. Ex-post-Untersuchungen von Sicherheitsvorfällen vorzunehmen, könnten in die unternehmerische Freiheit (Art. der EU-Grundrechtecharta (Art. 16 GRCh) und/oder das Eigentumsrecht der betroffenen Unternehmen (Art. 17 GRCh) eingreifen. Es muss klar geregelt werden, welche Handlungen diese Befugnisse umfassen, insbesondere, ob und unter welchen Voraussetzungen die ENISA – ggf. auch gegen den Willen der betroffenen Unternehmen – eigene Untersuchungen vornehmen darf und wie dabei vertrauliche und wirtschaftlich sensible Informationen angemessen geschützt werden können. Ohne Konkretisierung sind die Befugnisse unverhältnismäßig.

Auswirkungen auf das deutsche Recht

Da es sich um eine nicht umsetzungsbedürftige Verordnung handelt, die im Wesentlichen Ausstattung und Befugnisse der ENISA betrifft, sind wesentliche Änderungen im deutschen Recht nicht vorzunehmen.

Zusammenfassung der Bewertung

Die Verbesserung der Cybersicherheit ist geboten und muss angesichts der grenzüberschreitenden Dimension auf EU-Ebene erfolgen. Die Entfristung des Mandats der ENISA als EU-Cybersicherheitsagentur sowie die Aufstockung ihrer Mittel und ihres Personals sind daher sachgerecht. Eine Verlagerung von operativen Aufgaben auf die ENISA kann dazu führen, dass Anstrengungen auf nationaler Ebene unterbleiben („Trittbrettfahrerverhalten"). Unklar ist, wie weit die Befugnisse der ENISA zur Durchführung von Untersuchungen bestimmter Sicherheitsvorfälle reichen. Präzisiert werden muss, welche Handlungen die ENISA vornehmen darf und ob die Mitgliedstaaten Untersuchungen durch die ENISA ablehnen dürfen. Inwieweit die ENISA sensible Informationen selbst erheben und nutzen darf und wie sie diese Informationen schützen muss, sollte ebenfalls klargestellt werden.