Dennis-Kenji Kipker

# Neuer Verordnungsentwurf für ein einheitliches europäisches IT-Sicherheitsnetzwerk

MMR-Aktuell 2017, 395945

Auf der Grundlage der NIS-RL von 2016 hat das *EU-Parlament* nun einen weiteren und erheblichen Schritt in Richtung einheitlicher und flächendeckender Cybersicherheit in der Europäischen Union getan. Mit dem Entwurf einer Verordnung über die „EU-Cybersicherheitsagentur" (*ENISA*) und zur Aufhebung der VO (EU) Nr. 526/2013 sowie über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik (Rechtsakt zur Cybersicherheit) soll die *ENISA* zukünftig mit weitreichenderen Befugnissen ausgestattet, reformiert und ein europaweites Zertifizierungssystem für Cybersicherheit in der Informations- und Kommunikationstechnik etabliert werden.

Ziel des Entwurfs ist es einerseits, einen gemeinsamen Rahmen für Cyber-Sicherheitszertifizierungen zu schaffen, um das Vertrauen in den digitalen Binnenmarkt und dessen Sicherheit zu stärken, und andererseits, der *ENISA* wichtige Kompetenzen als leitende EU-Cyber-Securitybehörde zu übertragen, um entsprechenden Risiken vorzubeugen und Angriffe EU-weit koordiniert abwehren zu können. Laut dem Verordnungsentwurf sind sichere Informationstechnik sowie Kommunikationsnetze, Produkte und Dienstleistungen ein wichtiger Bestandteil der fortschreitenden Digitalisierung und damit auch maßgeblich für ein stetiges und staatenübergreifendes, gesamteuropäisches Wirtschaftswachstum. Deshalb sieht das EU-Gesetz verschiedene Maßnahmen vor, um der steigenden Bedrohungslage im digitalen Raum gerecht zu werden. Insbesondere sollen spezielle Befugnisse geschaffen werden, mit denen die Europäische Union auf internationale Cyber-Sicherheitsangriffe reagieren kann.

## I. Hintergrund, rechtspolitische Erwägungen und Definition der ENISA als europäische IT-Schlüsselbehörde

Im Rahmen der VO (EU) Nr. 526/2013 wurde die bisherige Arbeit der *ENISA* bewertet und zudem einer Mitteilung der *Kommission* von 2016 entsprechend überprüft. Hierbei stellte sich heraus, dass für die bisher herangezogenen Methoden zur Realisierung europäischer Cybersicherheit ein deutlicher Optimierungsbedarf besteht. Zugleich wurde festgestellt, dass die *ENISA* als Einrichtung der Europäischen Union ihrer leitenden Funktion in der IT-Sicherheit zukünftig nur dann gerecht werden kann, wenn ihr Mandat eine den Anforderungen moderner Cyber-Sicherheitsrisiken entsprechende Anpassung erfährt. Dementsprechend soll ein inhaltlicher und kompetenzbezogener Ausbau der Behörde stattfinden, der über die bisherigen Arbeitsbereiche der Bereitstellung von IT-bezogenem Fachwissen, dem Aufbau von Kapazitäten und der Beratungsfunktion in der politischen Gestaltung des digitalen Binnenmarkts hinausgeht. Zugleich soll der Behörde durch die Umstrukturierung ermöglicht werden, die ihr im Rahmen der NIS-RL zugeteilten Aufgaben, wie z.B. die Stellung des Sekretariats des CSIRTs-Netzwerks, zu übernehmen und den Mitgliedstaaten und der *EU-Kommission* für fachliche Fragen beratend zur Seite zu stehen. Insbesondere die Funktion der politischen Beratung erfährt einen weitergehenden Ausbau. Zwar haben basierend auf der Evaluation auch die technischen Kompetenzen einen erheblichen Stellenwert für die Verbesserung der Netz- und Informationssicherheit, ein wichtiger Erfolgsfaktor zur Optimierung der transnationalen Cybersicherheit liegt aber immer noch in der Schaffung von Möglichkeiten zur Zusammenarbeit und Kooperation zwischen den Mitgliedstaaten und den jeweiligen Fachkreisen. Hierzu wird in Zukunft das Mandat der *ENISA* in der Form einer Erweiterung der Beratungsfunktion sowie der politischen Teilhabe an IT-sicherheitsrelevanten Entscheidungen in der EU eine deutliche Stärkung erfahren, insbesondere auch vor dem Hintergrund einer Begleitung der rechtlichen Entwicklungen in diesem Bereich. Zur Unterstützung der gesetzlichen Anforderungen aus der NIS-RL wird die *ENISA* zudem mit einem ständigen Mandat als EU-Cyber-Sicherheitsagentur betraut werden; ferner werden die Kapazitäten der Behörde ausgebaut und in diesem Zusammenhang neue, klar definierte Befugnisse geschaffen.

Ähnlich dem *Bundesamt für Sicherheit in der Informationstechnik (BSI)* auf nationaler Ebene nimmt die *ENISA* zukünftig nicht nur eine politische Schlüsselrolle ein, sondern dient gleichsam als Informationsdrehkreuz der europäischen IT-Sicherheit. Die mitgliedstaatliche Zusammenarbeit beim Krisenmanagement wird u.a. durch die Erweiterung der Cyber-Sicherheitsübungen (CyberEurope) eine Ausweitung erfahren. Eine neue Aufgabe stellt zudem die Zertifizierung der Cybersicherheit von IKT-Produkten und -Diensten dar. Diese soll durch unabhängige, akkreditierte Zertifizierungsstellen erfolgen, die anhand noch zu bestimmender Vorgaben und Kriterien entsprechende Bescheinigungen ausstellen. Hierdurch sollen nicht nur die Sicherheit und das Vertrauen in den digitalen Binnenmarkt gestärkt werden, sondern es wird ebenso eine weitere Harmonisierung des gemeinsamen Markts angestrebt. Laut dem Verordnungsentwurf macht die derzeit in Europa vorzufindende, stark fragmentierte Zertifizierungslandschaft das Bedürfnis nach einem gemeinsamen und vereinheitlichten Rahmen in der IT-Sicherheit mehr als deutlich, um nachhaltig Marktzugangshürden für europäische Unternehmen in den Mitgliedstaaten abzubauen und Verwaltungskosten sowie Investitionsrisiken zu senken. Bei der Zertifizierung wird die *ENISA* als Marktbeobachtungsstelle fungieren und soll so auch neue Normen in der Cybersicherheit mitentwickeln. Eine weitere Zuständigkeit der Behörde liegt zukünftig in der Koordination und Zusammenführung der nationalen Stellen zur IT-Sicherheit, worunter insbesondere auch die nationalen Zertifizierungsstellen zu fassen sein werden.

## II. Bestimmungen des Verordnungsentwurfs im Einzelnen

### 1. Ziele und Aufgaben der ENISA (Art. 3-11)

Art. 3 umgrenzt zunächst den Wirkungsbereich der Agentur, indem festgelegt wird, dass die Zuständigkeiten der Mitgliedstaaten im Bereich der Cybersicherheit sowie für Tätigkeiten in Bezug auf die öffentliche Sicherheit, die Verteidigung, die nationale Sicherheit und das staatliche Handeln im Bereich des Strafrechts von den im Folgenden genannten Zielen und Aufgaben der europäischen Netz- und Informationssicherheitsbehörde unberührt bleiben.

Sodann benennt Art. 4 die zentralen Anforderungen an die neu geordnete *ENISA*:

Die Agentur soll künftig die Rolle des europäischen Kompetenzzentrums in Fragen der Cybersicherheit einnehmen. Neben der Unterstützung der EU-Einrichtungen und der Mitgliedstaaten bei der Entwicklung und Umsetzung ihrer Cyber-Sicherheitsstrategien wird die Agentur hierzu die interinstitutionelle sowie die interstaatliche Zusammenarbeit fördern, wobei explizit auch Interessenträger des privaten Sektors einzubeziehen sind. Darüber hinaus ist die *ENISA* ausgehend vom Verordnungsentwurf nunmehr auch explizit für den Ausbau der IT-Sicherheitskapazitäten auf europäischer Ebene verantwortlich. Im Falle von grenzüberschreitenden Sicherheitsvorfällen soll die Behörde auf diese Weise die von den Mitgliedstaaten getroffenen Maßnahmen ergänzen können. Schließlich wird die Agentur auch zum Aufbau und zur Pflege des neuen EU-Zertifizierungsrahmens für die Cybersicherheit beitragen, um das Vertrauen in die Verwendung von IKT-Produkten und -Diensten im gemeinsamen Binnenmarkt weiter zu verbessern.

Zusätzlich zu den bisherigen, überwiegend beratenden und unterstützenden Tätigkeiten in Angelegenheiten der Netz- und Informationssicherheit – etwa bei der Entwicklung von Unionspolitik und Unionsrecht, beim Aufbau der Fähigkeiten zum Umgang mit Cyber-Sicherheitsvorfällen, bei der Zusammenarbeit der verschiedenen Stellen, in der Forschung und in der internationalen Zusammenarbeit – ist vorgesehen, die *ENISA* mit einigen weiteren neuen Aufgaben zu betrauen: Dazu gehören u.a. die Entwicklung sektorspezifischer Strategien und Rechtsetzungsinitiativen (Art. 5 Abs. 1), die Unterstützung des CERT-EU (Art. 6 Abs. 1 lit. b) und die Kooperation mit den Mitgliedstaaten beim Aufbau und bei der Weiterentwicklung von CSIRTs (Art. 6 Abs. 1 lit. c, f). Der *ENISA* obliegt zudem die Organisation jährlicher und groß angelegter (ggf. auch sektorspezifischer) IT-Sicherheitsübungen auf EU-Ebene, die der Vorbereitung auf massive grenzüberschreitende Cyberangriffe dienen (Art. 5 Abs. 1 lit. g, Art. 7 Abs. 6), ferner die Unterstützung bei der Einrichtung sektorbezogener Informationsaustausch- und -analysezentren (sog. ISACs, Art. 6 Abs. 2), die Durchführung von ex post-Untersuchungen nach IT-Sicherheitsvorfällen mit mindestens zwei betroffenen Mitgliedstaaten (Art. 7 Abs. 5) oder auch die Erstellung von technischen Lageberichten (Art. 7 Abs. 7) und verschiedenen Analysen, z.B. zu den Auswirkungen technischer Innovationen (Art. 9 lit. a).

### 2. Organisationsstruktur und internationale Zusammenarbeit (Art. 12-25, Art. 39)

Die Organisationsstruktur der Agentur bleibt gegenüber der bisherigen Regelung unverändert bestehen. Auch künftig setzt sich die *ENISA* auf der Leitungsebene aus einem Verwaltungsrat, dem je ein Vertreter jedes Mitgliedstaats und zwei von der *EU-Kommission* ernannte Vertreter angehören, einem den Verwaltungsrat unterstützenden Exekutivrat, dem Exekutivdirektor sowie der Ständigen Gruppe der Interessenträger zusammen (Art. 12 ff.). Die Möglichkeit der Zusammenarbeit mit Drittländern und internationalen Organisationen wird gegenüber der bestehenden VO (Nr. 526/2013) erweitert: Art. 39 sieht neben der Möglichkeit einer Beteiligung von Drittländern an der Agentur nunmehr vor, dass die *ENISA* (rechtlich unverbindliche) Arbeitsvereinbarungen mit den zuständigen Behörden von Drittstaaten oder mit internationalen Organisationen treffen kann, soweit dies zur Verwirklichung der in der Verordnung genannten Ziele erforderlich ist. Daneben kommt dem Verwaltungsrat die Aufgabe zu, im Hinblick auf die Tätigkeitsfelder der *ENISA* eine Strategie für die Beziehungen zu Drittländern oder zu internationalen Organisationen zu verabschieden. Vor allem hierdurch wird deutlich, dass grenzüberschreitende IT-Sicherheitsvorfälle auf Grund ihres globalen Charakters auch in politischer Hinsicht internationaler Lösungsansätze bedürfen.

### 3. Europäische Systeme für die Cyber-Sicherheitszertifizierung (Art. 43-54)

Gänzlich neu sind die in der Verordnung vorgeschlagenen Regelungen zur Entwicklung europäischer Systeme für die Cyber-Sicherheitszertifizierung durch die *ENISA*. Diese Systeme dienen gem. Art. 43 „der Bescheinigung, dass die nach einem solchen System zertifizierten IKT-Produkte und -Dienste auf einer bestimmten Vertrauenswürdigkeitsstufe den festgelegten Anforderungen an ihre Fähigkeit genügen, Handlungen zu widerstehen, die darauf abzielen, die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit von gespeicherten, übermittelten oder verarbeiteten Daten, Funktionen oder Diensten zu beeinträchtigen, die von diesen Produkten, Prozessen, Diensten und Systemen angeboten oder über diese zugänglich gemacht werden."

Die Anforderungen an ein solches Zertifizierungssystem werden in den Art. 45-47 näher beschrieben: So benennt Art. 45 zunächst die Sicherheitsziele, denen die Systeme Rechnung tragen sollen. Das sind z.B. der Schutz von Daten gegen zufällige oder unbefugte Speicherung, Verarbeitung, Preisgabe und Zerstörung sowie gegen zufälligen oder unbefugten Zugriff, zufälligen Verlust oder zufällige Änderung. Ein weiteres Sicherheitsziel ist die Gewährleistung, dass IKT-Produkte oder -Dienste mit aktueller Software ohne bekannte Schwachstellen bereitgestellt werden. Die Vertrauenswürdigkeit der auf Grundlage eines solchen Systems zertifizierten IKT-Produkte oder -Dienste soll mit den unterschiedlichen Stufen „niedrig" (begrenztes Maß an Vertrauen in die vom Anbieter erklärten Cyber-Sicherheitseigenschaften eines Produkts oder Dienstes), „mittel" (durchschnittliches Maß an Vertrauen in die vom Anbieter erklärten Cyber-Sicherheitseigenschaften eines Produkts oder Dienstes) und „hoch" (ein über dem durchschnittlichen Maß an Vertrauen liegendes Level für die vom Anbieter erklärten Cyber-Sicherheitseigenschaften eines Produkts oder Dienstes) angegeben werden (Art. 46). Art. 47 legt die in einem europäischen System für die Cyber-Sicherheitszertifizierung notwendig enthaltenen Elemente fest. Hierzu gehören u.a. die Art der erfassten IKT-Produkte und -Dienste, eine detaillierte Spezifikation der Sicherheitsanforderungen (etwa unter Bezugnahme auf technische Normen), die Vertrauenswürdigkeitsstufen, die für die Zertifizierung vom Anbieter vorzulegenden Informationen, der Inhalt der ausgestellten Zertifikate, aber etwa auch Vorschriften für die Überwachung der Einhaltung von mit dem Zertifikat verbundenen Anforderungen sowie Vorschriften für die Meldung bislang nicht erkannter Schwachstellen in der Cybersicherheit von Produkten und Diensten.

Die Zertifizierung ist gem. Art. 48 Abs. 2 des Verordnungsentwurfs für die Anbieter freiwillig. Die Zertifikate werden in der Regel von entsprechend akkreditierten

Konformitätsbewertungsstellen ausgestellt, in bestimmten Fällen sollen die Zertifikate jedoch nur durch öffentliche Stellen vergeben werden dürfen (Art. 48 Abs. 3, 4). Die Zertifikate sollen höchstens drei Jahre gültig sein und bei Erfüllung der entsprechenden Voraussetzungen verlängert werden können (Art. 48 Abs. 6). Soweit bestehende nationale Cyber-Sicherheitszertifizierungssysteme hinsichtlich der erfassten Produkte und Dienste unter ein gemäß der Verordnung neu eingeführtes europäisches System fallen, werden diese ausgehend von Art. 49 Abs. 1 unwirksam. Das bedeutet folglich auch, dass Mitgliedstaaten künftig keine neuen nationalen Zertifizierungssysteme mehr einführen dürfen, wenn die entsprechenden Produkte und Dienste unter ein geltendes europäisches System fallen (Art. 49 Abs. 2).

Bei der Ausarbeitung eines Zertifizierungssystems soll die *ENISA* eng mit der hierzu gem. Art. 53 neu einzurichtenden „Europäischen Gruppe für die Cybersicherheitszertifizierung" zusammenarbeiten. Diese Gruppe wird durch die nationalen Aufsichtsbehörden für die Zertifizierung gebildet, die nach Art. 50 von jedem Mitgliedstaat ernannt werden müssen. Neben ihrer Funktion als Mitglied der Gruppe sind die nationalen Aufsichtsbehörden u.a. für die Überwachung und Durchsetzung der Bestimmungen in Titel III der Verordnung (Zertifizierungsrahmen) sowie für die Beaufsichtigung der Tätigkeiten der Konformitätsbewertungsstellen verantwortlich (Art. 50 Abs. 6). Die Aufsichtsbehörden erhalten dabei umfangreiche Befugnisse. Dazu gehört etwa die Möglichkeit, Untersuchungen bei Konformitätsbewertungsstellen und Zertifikatsinhabern durchzuführen, um die Einhaltung der Bestimmungen der Verordnung zu überprüfen, darüber hinaus die Befugnis zur Ergreifung geeigneter Maßnahmen, um sicherzustellen, dass die Konformitätsbewertungsstellen und Zertifikatsinhaber den Anforderungen der Verordnung bzw. des Zertifizierungssystems genügen, und auch die Möglichkeit, Zertifikate zu widerrufen, wenn diese Anforderungen nicht erfüllt werden (Art. 50 Abs. 7). Für jedes nach Art. 44 angenommene Zertifizierungssystem müssen die nationalen Aufsichtsbehörden die für die Erteilung von Zertifikaten akkreditierten Konformitätsbewertungsstellen an die *EU-Kommission* melden (Art. 52 Abs. 1).

## III. Evaluation und Gesamtkosten

Art. 56 des Entwurfs der Verordnung sieht abschließend vor, dass die *EU-Kommission* spätestens fünf Jahre nach Inkrafttreten sowie anschließend nach jeweils fünf Jahren eine Bewertung der Wirkung, Wirksamkeit und Effizienz der Agentur sowie der Bestimmungen zur Cyber-Sicherheitszertifizierung vornimmt und insbesondere prüft, ob hinsichtlich des der *ENISA* erteilten Mandats Änderungsbedarf besteht. Die Gesamtkosten der Realisierung des europäischen Cyber-Sicherheitszertifizierungsrahmens werden zurzeit auf € 86 Mio. beziffert.

## IV. Fazit

Insgesamt ist festzustellen, dass mit dem vorgelegten Verordnungsentwurf ein weitreichender Rahmen für die Harmonisierung des Cyber-Sicherheitsstandards im europäischen Binnenmarkt geschaffen wird. Dieser wird, was seinen Geltungsbereich anbelangt, umfassend ausgestaltet. Allerdings bleibt abzuwarten, wie der Ausbau und die Reform der *ENISA* tatsächlich zu verbesserten Arbeitsergebnissen bei der Beratung, dem Informationsaustausch und bei einer politischen Mitentwicklung der transnationalen Cyber-Sicherheitsstrategie beitragen werden. Vorrangig wird sich die Behörde zunächst als Kompetenzzentrum mit den neu verordneten Aufgaben bewähren müssen, wobei die Ergebnisse sowie die erreichten Fortschritte spätestens in fünf Jahren mit dem Vorliegen der neuen Beurteilungsstufe von Seiten der *EU-Kommission* einsehbar sein werden. Mit dem vorliegenden Gesetzentwurf ist zumindest aber ein erheblicher Schritt in die Richtung des gemeinsamen Binnenmarkts getan, indem die Europäische Union nun auch bisherige unternehmerische Hemmnisse im Bereich der grenzüberschreitenden Cybersicherheit aktiv aufgreift. Nichtsdestotrotz wird sich das neu vorgeschlagene Zertifizierungssystem in naher Zukunft noch bewähren müssen; auch ist das entsprechende Rahmenwerk mit den sektorspezifischen Normen zur Zertifizierung mit weitergehenden Inhalten auszufüllen und wird in Anbetracht der stetig wachsenden Bedrohungen im Cyberraum laufender Anpassung bedürfen. Zu klären sollte in Bälde ebenso sein, inwieweit die Normung sowie die grundsätzlich einzubeziehende Industrie an den Entwicklungsprozessen der Zertifizierung teilhaben werden.

■ Dieser Beitrag entstand im Rahmen des vom *BMBF* geförderten Forschungsschwerpunkts „IT-Sicherheit Kritischer Infrastrukturen" als Bestandteil der Hightech-Strategie der *Bundesregierung*. Vgl. auch *Kipker*, MMR-Aktuell 2017, 394677; *ders.*, MMR 2017, 143; ZD-Aktuell 2016, 05363; *Kipker*, MMR-Aktuell 2017, 389121 und *ders.*, ZD-Aktuell 2016, 05363.

**Dr. Dennis-Kenji Kipker**
ist Wissenschaftlicher Geschäftsführer des Instituts für Informations-, Gesundheits- und Medizinrecht (IGMR) an der Universität Bremen, Projektmanager beim Verband der Elektrotechnik, Elektronik und Informationstechnik (VDE) e.V. in Frankfurt/M., Abteilung CERT@VDE, und Mitglied des Vorstands der Europäischen Akademie für Informationsfreiheit und Datenschutz (EAID) in Berlin.