European Commission

Studie zur Evaluierung der Agentur der Europäischen Union für Netz- und Informationssicherheit (ENISA)

ZUSAMMENFASSUNG

Eine Studie für die Europäische Kommission
Generaldirektion Kommunikationsnetze, Inhalte und Technologien erstellt von:

RAMBØLL

carsa

Digitaler Binnen markt

Diese Studie wurde für die Europäische Kommission durch-geführt von

Karin Attström, Vanessa Ludden, Franziska Lessmann
Ramboll

Pär Weström, Johannes Conrads
Carsa
Carretera de Asúa, 6
48930 Getxo
Vizcaya – Spain
http://www.carsa.es

Unter Mitarbeit von: Helena Farrand Carrapico, Aston University; Andrej Savin, Copenhagen Business School; Cristina de la Maza, RedBorder

Interne Identifikation

Vertragsnummer: 30-CE-0815229/00-33

SMART 2016/0077

ERGÄNZENDER SCHUTZVERMERK

der Europäischen Kommission, Generaldirektion Kommunikationsnetze, Inhalte und Technologien:

Die Informationen und Ansichten in dieser Veröffentlichung sind die der Autoren und spiegeln nicht notwendigerweise die offizielle Meinung der Kommission wider. Die Kommission garantiert nicht die Genauigkeit der in der Studie enthaltenen Daten. Weder die Kommission noch irgendeine Person, die im Namen der Kommission handelt, kann für die Nutzung der hierin enthaltenen Informationen verantwortlich gemacht werden.

ISBN 978-92-79-72112-0

doi:10.2759/561125

ABRISS

Die Agentur der Europäischen Union für Netz- und Informationssicherheit (ENISA) wurde im Jahr 2004 gegründet. Die Agentur bietet Beratung, Empfehlungen sowie Datenanalysen und unterstützt die Sensibilisierung und Zusammenarbeit der Einrichtungen und Mitgliedstaaten der EU im Bereich der Cybersicherheit. Die ENISA nutzt ihre Sachkenntnis, um die Zusammenarbeit zwischen den Mitgliedstaaten sowie Akteuren des öffentlichen und privaten Sektors zu verbessern und den Kapazitätsausbau zu unterstützten.

Die vorliegende Studie umfasst eine Evaluierung der ENISA über den Zeitraum 2013-2016. Bewertet wurden die Leistung, die Führungs- sowie die Organisationsstruktur der Agentur und ihre Positionierung gegenüber anderen Einrichtungen auf EU- und nationaler Ebene. Ferner wurden die Stärken, Schwächen, Chancen und Risiken (SWOT) der ENISA im Hinblick auf die neuen Gegebenheiten im Bereich der Cybersicherheit und des digitalen Datenschutzes bewertet. Die Studie enthält überdies Optionen zur Änderung des Mandats der Agentur, damit auf neue, sich abzeichnende Erfordernisse besser reagiert werden kann. Gleichzeitig wurden die finanziellen Auswirkungen dieser Optionen bewertet.

Die Ergebnisse der Evaluierungsstudie machen deutlich, dass die ENISA eine Reihe bedeutender Erfolge bei der Erhöhung der Netz- und Informationssicherheit (NIS) in der EU verzeichnen kann. Allerdings beeinträchtigen die EU-weit fragmentierte Vorgehensweise in Bezug auf die Cybersicherheit sowie interne Probleme der Agentur, darunter begrenzte finanzielle Mittel, die ENISA in ihrer Fähigkeit, im Zuge technologischer Entwicklungen und wachsender Bedrohungen der Cybersicherheit den steigenden Anforderungen der Interessenträger gerecht zu werden.

ZUSAMMENFASSUNG

Dies ist die Zusammenfassung der „Studie zur Evaluierung der Agentur der Europäischen Union für Netz- und Informationssicherheit (ENISA)".

Ziele

Die ENISA ist die für Netz- und Informationssicherheit zuständige Agentur der EU. Sie wurde im Jahr 2004 durch die Verordnung (EG) Nr. 460/2004 gegründet. Das Mandat der ENISA wurde seither einmal überprüft und mehrere Male verlängert. Die jüngsten Änderungen wurden im Rahmen der Verordnung (EU) Nr. 526/2013 (im Folgenden „die Verordnung") umgesetzt. Gemäß Artikel 32 Absatz 1 der Verordnung ist die Kommission verpflichtet, „eine Bewertung insbesondere der Wirkung, Wirksamkeit und Effizienz der Agentur und ihrer Arbeitsmethoden [vorzulegen]. Die Bewertung betrifft auch die eventuell erforderliche Änderung des Mandats der Agentur und die finanziellen Auswirkungen einer solchen Änderung."

Die vorliegende Studie umfasst eine Bewertung der ENISA über den Zeitraum 2013-2016. Bewertet wurden die Leistung, die Führungs- sowie die Organisationsstruktur der Agentur und ihre Positionierung gegenüber anderen Einrichtungen auf EU- und nationaler Ebene. Ferner wurden die Stärken, Schwächen, Chancen und Risiken (SWOT) der ENISA im Hinblick auf die neuen Gegebenheiten im Bereich der Cybersicherheit und des digitalen Datenschutzes bewertet. Die Studie enthält Optionen zur Änderung des Mandats der Agentur, damit auf die neuen Erfordernisse besser reagiert werden kann. Gleichzeitig wurden die finanziellen Auswirkungen dieser Optionen bewertet.

Methodischer Ansatz

Ziel der Evaluierungsstudie ist es, die Relevanz, Wirksamkeit, Effizienz, Kohärenz und Komplementarität sowie den EU-Mehrwert der ENISA zu bewerten. Sie bietet Antworten auf 46 Bewertungsfragen auf der Grundlage des Fahrplans der Europäischen Kommission für die Bewertung der ENISA[1]. Die Schlussfolgerungen der Bewertung wurden auf der Grundlage der Sammlung primärer und sekundärer Daten sowie von Analysen gezogen, die in die Antworten auf die Bewertungsfragen eingeflossen sind. Für die Bewertung wurden Daten in großem Umfang gesammelt. Hierfür wurden unter anderem verschiedene Gruppen von Interessenträgern konsultiert (darunter Mitarbeiter und Führungskräfte der ENISA, der Verwaltungsrat der ENISA, nationale Computer-Notfallteams (Computer Emergency Response Teams – CERTs) und Reaktionsteams für Computersicherheitsverletzungen (Computer Security Incident Response Teams – CSIRTs), EU-Institutionen sowie private Interessenträger). Die primären Daten wurden mithilfe von ausführlichen Interviews, zwei Onlineumfragen, einer offenen öffentlichen Konsultation und einem Workshop gesammelt. Die Bewertung wird durch eine Bewertungsmatrix untermauert, in der die Bewertungsfragen mit den zur Beantwortung verwendeten Datenquellen, Indikatoren und Analysestrategien verknüpft wurden und somit verdeutlicht wird, wie die Schlussfolgerungen gezogen wurden.

Die Bewertung wurde zwischen November 2016 und Juli 2017 von Ramboll Management Consulting und CARSA unter Beteiligung drei externer Experten durchgeführt. Letztere befassten sich mit den politischen, rechtlichen und technischen Aspekten der Cybersicherheit.

Erkenntnisse und Schlussfolgerungen

In der folgenden Tabelle ist die Bewertung der Leistung, Führungs- und Organisationsstruktur sowie Positionierung der Agentur anhand der Evaluierungskriterien für den Zeitraum 2013-2016 zusammengefasst. Weiter unten werden die wesentlichen Erkenntnisse, die zu dieser Bewertung geführt haben, vorgestellt.

[1] Europäische Kommission (2016): Evaluation Roadmap – Evaluation of the European Union Agency for Network and Information Security (ENISA) (Fahrplan für die Bewertung der Agentur der Europäischen Union für Netz- und Informationssicherheit (ENISA))

Tabelle 1: Bewertung der ENISA anhand der Evaluierungskriterien

Bewertungskriterium	Gesamtbewertung
Relevanz	Zum großen Teil erfüllt
Wirksamkeit	Teilweise erfüllt
Effizienz	Zum großen Teil erfüllt
Kohärenz	Teilweise erfüllt
EU-Mehrwert	Teilweise erfüllt

Relevanz: Im Kontext technologischer Entwicklungen und wachsender Bedrohungen besteht ein dringender Bedarf an mehr Netz- und Informationssicherheit (NIS) in der EU. Die unlängst dem Rechtsrahmen hinzugefügten Elemente wie die NIS-Richtlinie[2] unterstreichen dies. Die Mitgliedstaaten und Einrichtungen der EU sind abhängig von Sachkenntnis zur Entwicklung der NIS, in den Mitgliedstaaten müssen Kapazitäten für das Verständnis von und die Reaktion auf Bedrohungen ausgebaut werden, und die Interessenträger müssen über thematische Bereiche und Institutionen hinweg zusammenarbeiten. Vor diesem Hintergrund erwiesen sich die im Mandat der ENISA festgelegten Ziele über den Bewertungszeitraum als relevant, und sie sind auch jetzt noch von großer Relevanz.

Zwar sind die Ziele der Agentur im Mandat breit gefasst, sodass der Verwaltungsrat der ENISA die Möglichkeit hat, Prioritäten aufgrund jüngster Entwicklungen festzulegen und so auf sich ändernde Erfordernisse und wachsende Bedrohungen zu reagieren, dennoch entsprechen die Aktivitäten der ENISA nicht uneingeschränkt den Anforderungen all ihrer Interessenträger:

- Das Arbeitsprogramm der ENISA wird von den Interessen der Mitgliedstaaten dominiert, jedoch ist es notwendig, eine längerfristige Perspektive und die Aktivitäten anderer Interessenträger im Bereich der Cybersicherheit (etwa anderer EU-Agenturen oder des privaten Sektors) zu berücksichtigen, um fortdauernde Relevanz der Agentur sicherzustellen.
- Die Interessenträger der ENISA haben unterschiedliche Bedürfnisse, weshalb es schwierig ist, sie alle zu erfüllen. Einige Mitgliedstaaten (wie Deutschland, Frankreich oder Schweden) besitzen erhebliche Kapazitäten und Mittel im Bereich der Cybersicherheit und greifen nur für bestimmte Dienstleistungen auf die ENISA zurück. Andere Mitgliedstaaten (aus Ost- und Südeuropa) wiederum haben weniger Erfahrung und stützen sich in größerem Umfang auf die Sachkenntnis und Kapazitäten der ENISA. Die Kommission hat eigene Anforderungen und Erwartungen an die Dienste, welche die ENISA den verschiedenen Generaldirektionen erbringen kann. Darüber hinaus stellen Interessenträger aus der Industrie, zu denen zahlreiche kleine und mittlere Unternehmen (KMU) zählen, wichtige Akteure in der NIS dar. Ihnen könnten die Tätigkeiten der ENISA ebenfalls zugutekommen.

Wirksamkeit: Im Allgemeinen erfüllt die ENISA ihre Aufgaben und erreicht ihre festgelegten Ziele. Die ENISA hat durch die vier in nachstehender Tabelle aufgeführten Aufgaben zu höherer NIS in Europa beigetragen, wenngleich bei jeder dieser Aufgaben noch Verbesserungspotenzial besteht.

Gemeinschaftsbildung		**Ausbau von Kapazitäten**	
Erfolge	Bereiche mit Verbesserungspotenzial	Erfolge	Bereiche mit Verbesserungspotenzial
✓ Wichtiger Beitrag zu besserer Zusammenarbeit zwischen Mitgliedstaaten und einschlägigen NIS-	- Zusammenarbeit zwischen ENISA und der Kommission, anderen EU-Agenturen sowie dem Privatsektor könnte verstärkt	✓ Beitrag zu verbesserten Kapazitäten in den Mitgliedstaaten, insbesondere in Mitgliedstaaten mit	- Kapazitätsausbau mit dem Privatsektor könnte verstärkt werden

[2] Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union

Interessenträgern, insbesondere zwischen CERTs/CSIRTs	werden	eingeschränkten Möglichkeiten und Ressourcen im Bereich Cybersicherheit ✓ Wichtige Aktivitäten umfassen das Projekt „Cyber Europe" sowie Schulungen für CERT/CSIRT	
Bereitstellung von Sachkenntnis		**Unterstützung der Entwicklung und Umsetzung politischer Strategien**	
Erfolge	Bereiche mit Verbesserungspotenzial	Erfolge	Bereiche mit Verbesserungspotenzial
✓ Wichtiger Beitrag durch Unterstützung von CERTs/CSIRTs	- ENISA ist es nicht gelungen, sich als anerkanntes Fachzentrum oder Bezugspunkt für andere Interessenträger, wie EU-Institutionen oder den Privatsektor, zu etablieren - Hohe Abhängigkeit von externer Sachkenntnis und begrenzte Verfügbarkeit interner Ressourcen	✓ ENISA hat die Mitgliedstaaten und die Kommission bei der Entwicklung und Umsetzung politischer Strategien unterstützt	- ENISA wird von der Kommission nicht konsequent in NIS-bezogene Aktivitäten eingebunden

Der Beitrag der ENISA zur NIS in Europa wird durch mehrere zentrale Faktoren begrenzt, darunter:

- Das umfassende Mandat, gemäß dem ein breites Aufgabenspektrum abzudecken ist, wodurch wenig Spielraum für eigeninitiatives Arbeiten und Tätigkeiten, die nicht auf Anfrage erfolgen, besteht
- Die Schwierigkeiten der Agentur, Cybersicherheitsexperten als Mitarbeiter zu gewinnen und zu halten, die auf verschiedene Gründe zurückzuführen sind, einschließlich schwacher Verfahren im Bereich der Humanressourcen während des Prüfungszeitraums
- Die begrenzte Sichtbarkeit der ENISA – die Agentur ist EU-weit nicht ausreichend bekannt und war im Gegensatz zu anderen EU-Agenturen nicht in der Lage, eine eigene Marke zu etablieren

Effizienz: Verglichen mit anderen EU-Agenturen verfügt die ENISA mit über den geringsten Etat und die geringsten Mitarbeiterzahlen. Um die verschiedenen Aufgaben entsprechend ihrem Mandat zu erfüllen, muss die ENISA bei der Ausführung ihres Haushaltsplans überaus effizient sein und sorgfältig abwägen, für welche Bereiche Ressourcen und Arbeitsstunden aufgewendet werden können. Die Agentur erarbeitet jedes Jahr eine große Zahl von Veröffentlichungen und führt zahlreiche weitere Aktivitäten durch. Trotz ihres geringen Haushalts ist es der Agentur gelungen, zum Erreichen spezifischer Ziele und Wirkungen beizutragen, was von großer Effizienz bei der Verwendung der Haushaltsmittel zeugt.

Im Hinblick auf die Effizienz steht die ENISA vor zwei wesentlichen Herausforderungen:

- Einer Reihe von administrativen Anforderungen vonseiten der Kommission, die zwar für alle EU-Agenturen gleich sind, für kleinere Agenturen jedoch stärker ins Gewicht fallen
- Der Aufteilung der Arbeitsorte auf Athen und Heraklion, was zusätzliche Koordinierungsanstrengungen erfordert und zusätzliche Kosten mit sich bringt.

Kohärenz: Die Aktivitäten der ENISA stehen im Allgemeinen mit den Strategien und Tätigkeiten ihrer Interessenträger im Einklang, allerdings muss die Vorgehensweise im Bereich der Cybersicherheit auf EU-Ebene besser koordiniert werden. Das Potenzial für Zusammenarbeit zwischen ENISA und Europäischer Kommission sowie anderen EU-Einrichtungen wird nicht vollständig genutzt. Beispielsweise sollte die Aufteilung der Zuständigkeiten zwischen der ENISA und CERT-EU besser geklärt werden.

Die Aktivitäten der ENISA stehen weitgehend im Einklang mit den Arbeiten, die auf nationaler Ebene im Bereich der Cybersicherheit durchgeführt werden. Besonders groß ist die Kohärenz zwischen den CERTs/CSIRTs und der ENISA. Einige Überschneidungen wurden zwischen den Aktivitäten der ENISA und denen der Mitgliedstaaten mit hoher Sachkenntnis im Bereich Cybersicherheit festgestellt, doch den Mitgliedstaaten mit geringeren Kapazitäten und Ressourcen auf dem Gebiet der Cybersicherheit kommen die Tätigkeiten der ENISA noch immer zugute.

EU-Mehrwert: Der Mehrwert der ENISA liegt vorrangig in ihrer Fähigkeit zur Verbesserung der Zusammenarbeit, insbesondere zwischen den Mitgliedstaaten, aber auch mit einschlägigen Akteursgruppen im NIS-Bereich. Auf EU-Ebene gibt es keinen zweiten Akteur, der die Zusammenarbeit einer ähnlich großen Vielfalt an Interessenträgern im Bereich der NIS fördert. Der Mehrwert der ENISA unterscheidet sich in den einzelnen Mitgliedstaaten – je nach ihren Kapazitäten und Ressourcen im Bereich der Cybersicherheit. Die Aktivitäten der Agentur hinsichtlich der Bereitstellung von Sachkenntnis und des Ausbaus von Kapazitäten stellen für Mitgliedstaaten mit geringen nationalen Ressourcen auf dem Gebiet der Cybersicherheit einen wichtigen Mehrwert dar. Für Mitgliedstaaten mit umfangreicheren Kapazitäten in diesem Bereich ist dies weniger der Fall.

Folglich hätte eine Einstellung der Tätigkeiten der ENISA unterschiedliche Auswirkungen auf die Mitgliedstaaten. Während die Mitgliedstaaten mit umfangreichen Kapazitäten im Bereich der Cybersicherheit in der Lage wären, die von der ENISA erbrachten Dienste zumindest teilweise zu ersetzen, wäre dies für Mitgliedstaaten mit weniger Ressourcen nicht möglich. Letztere sind in Bezug auf Kapazitätsausbau, Zugang zu Fachwissen und Unterstützung bei der Politikumsetzung und Gesetzgebung in höherem Maße von den Diensten der ENISA abhängig. Cybersicherheit macht an Grenzen nicht halt, daher ist es notwendig, Kapazitäten auszubauen, um Schwachstellen zu vermeiden, die sich auf die Cybersicherheit in der gesamten EU auswirken können. Es müssen EU-weite Antworten gefunden werden. Ohne eine dezentrale EU-Agentur für Cybersicherheit wird es nicht möglich sein, in allen Mitgliedstaaten das gleiche Maß an Gemeinschaftsbildung und Zusammenarbeit zu gewährleisten; die Situation würde sich fragmentierter gestalten, falls eine von der ENISA hinterlassene Lücke durch bilaterale oder regionale Zusammenarbeit geschlossen würde. Daher bedarf es einer Koordinierung auf EU-Ebene.
Eine mögliche Einstellung der Tätigkeiten der ENISA wäre eine verlorene Gelegenheit für alle Mitgliedstaaten. Die meisten Interessenträger vertraten die Ansicht, dass die ENISA künftig eine bedeutendere Rolle im Bereich der EU-Cybersicherheit übernehmen könnte, wodurch eine gemeinsame Reaktionsfähigkeit sichergestellt wäre. Dieses Potenzial der Agentur zur Nutzung künftiger Chancen wäre im Falle einer Einstellung der Tätigkeiten verloren.

SWOT-Analyse: Auf der Grundlage einer Analyse des Kontextes – nämlich der Entwicklung der Bereiche Cybersicherheit und digitaler Datenschutz seit der letzten Überarbeitung des Mandats der ENISA im Jahr 2013 – bietet die Studie eine Bewertung der wesentlichen Stärken und Schwächen der ENISA sowie der Chancen und Risiken angesichts der neuen Gegebenheiten in den Bereichen Cybersicherheit und digitaler Datenschutz. Diese Elemente sind in der nachstehenden Abbildung dargestellt.

Tabelle 2: Stärken, Schwächen, Chancen und Risiken (SWOT) der ENISA

Stärken	Schwächen
- Neutral, Mittlerfunktion, frei von politischer Voreingenommenheit oder kommerziellen Interessen - Anerkannte Unterstützung der Mitgliedstaaten bei Kapazitätsausbau und Fähigkeitsentwicklung zur Stärkung der Widerstandsfähigkeit gegenüber Cyber-Bedrohungen - Anerkannte Zusammenarbeit und Gemeinschaftsbildung mit einem breiten Spektrum an Akteuren, einschl. Mitgliedstaaten, Industrie, EU-Einrichtungen usw. - Horizontale Sachkenntnis, allgemeine Übersicht über die Cybersicherheitsstrategien der Mitgliedstaaten	- Geringe Sichtbarkeit aus verschiedenen Gründen: mangelnde Sachkenntnis, schwache Kommunikation/schwaches Marketing und begrenztes Durchsetzungsvermögen innerhalb der cybersicherheitspolitischen Landschaft der EU - Fehlen einer langfristigen, strategischen Vision - Schwierigkeiten bei der Personalrekrutierung - Verringerte Effizienz aufgrund der Aufteilung der Arbeitsorte - Distanz zu EU-Entscheidungsträgern in Brüssel - Zu geringe finanzielle und personelle Ressourcen, um etwas zu bewirken
Chancen	**Risiken**
- Wachsender Bedarf an Synergien zwischen Betreibern von Informations- und Kommunikationstechnologie (IKT) zur Gewährleistung abgestimmter und kollaborativer Maßnahmen im Bereich der NIS-Politik - NIS-Richtlinie birgt Potenzial zur Stärkung der Rolle der ENISA in der EU-Cybersicherheitspolitik - Anerkannter Bedarf und Nachfrage vonseiten der Interessenträger nach Stärkung der Sensibilisierung für Cybersicherheit - Unterstützung in der Gemeinschaft für IKT-Standardisierung und -Zertifizierung wird stärker	- Fragmentierung der Politik auf EU-Ebene und unterschiedliche politische Prioritäten in EU-Mitgliedstaaten schränken Handlungsspielraum von ENISA ein - Sich rasch entwickelnde und komplexe Bedrohungslage in vielerlei Bereichen schafft neue Schwachpunkte, z. B. Internet der Dinge - Mangel an (technischen) Nachwuchskräften im Bereich Cybersicherheit verschärft Schwierigkeiten der ENISA bei Personalrekrutierung

Zusammenfassend wurde festgestellt, dass bei folgenden **zentralen Problemen** Handlungsbedarf besteht, um die Relevanz, Wirksamkeit, Effizienz, Kohärenz und den Mehrwert der ENISA künftig zu verbessern und sie letztendlich dabei zu unterstützen, zu mehr NIS in der EU beizutragen:

- *Schwacher institutioneller und rechtlicher Rahmen für die Cybersicherheit in der EU* – Die Cybersicherheit wird in erster Linie als ein nationaler Kompetenzbereich gesehen, wobei sie in Wirklichkeit nicht an Grenzen Halt macht
- *Fragmentierung der Cybersicherheitspolitik auf EU-Ebene* – Die Fragmentierung der Cybersicherheitspolitik ist darauf zurückzuführen, dass auf EU-Ebene eine gewisse Anzahl an Akteuren im Bereich der Cybersicherheit tätig ist und unzureichende Koordinierung zwischen ihnen herrscht Ein wichtiger Faktor ist hier die Aufteilung der Zuständigkeiten zwischen der ENISA und dem CERT-EU.
- *Einschränkungen der ENISA aufgrund ihrer Größe* – Die ENISA hat Schwierigkeiten, im weiten Feld der NIS etwas zu bewirken, da ihr nur begrenzt personelle und finanzielle Ressourcen zur Erfüllung ihres umfassenden Mandats zur Verfügung stehen.
- *Begrenzte Sichtbarkeit* – Der ENISA ist es nicht gelungen, einen starken Markennamen zu entwickeln, und sie wird auf europäischer Ebene nicht als Bezugspunkt für die Cybersicherheit wahrgenommen.
- *ENISA wird nicht als proaktive, visionäre Agentur wahrgenommen* – Aufgrund ihres breiten Mandats muss die ENISA die Anforderungen von möglichst vielen Interessenträgern erfüllen, jedoch verliert sie dadurch an Fokus. Die ENISA ist nicht in der Lage, ihr eigenes Wissen zu nutzen, um Arbeitsprioritäten festzulegen, da das Arbeitsprogramm von den Mitgliedstaaten dominiert wird.
- *Mandat ist nicht auf Anforderungen im Bereich Cybersicherheit abgestimmt* – Bedrohungen der Cybersicherheit sind zu einem permanenten Problem in der EU geworden, und der ENISA wurden langfristige Zuständigkeiten (z. B. im Rahmen der NIS-Richtlinie) übertragen, die ein permanentes Mandat erfordern.
- *ENISA erfüllt nicht ausreichend die Anforderungen all ihrer Interessenträger* – Im Rahmen der derzeitigen Führungsstruktur finden die Bedürfnisse des Privatsektors nicht ausreichend Gehör und werden somit in den Arbeitsprogrammen der Agentur nicht angemessen berücksichtigt.
- *ENISA sollte ihre Aktivitäten ausweiten, um besser den Anforderungen der Interessenträger gerecht zu werden* – Vonseiten einiger (wenn auch nicht aller) Interessenträger wird gefordert,

ein kohärentes IKT-Zertifizierungs- und -Standardisierungssystem in der EU einzurichten. Mitgliedstaaten mit weniger Ressourcen und Sachkenntnis benötigen zusätzliche Unterstützung, damit sie Informationen über Bedrohungen der Cybersicherheit erhalten und diese Bedrohungen bewerten und so auf Angriffe entsprechend reagieren können.

Trotz dieser Probleme birgt die ENISA ein erhebliches Potenzial, sofern sie mit einem hinreichenden Mandat und ausreichend finanziellen und personellen Ressourcen ausgestattet wird, damit sie zu mehr NIS in der EU beitragen kann. Es besteht ein eindeutiger Bedarf an Zusammenarbeit und Koordinierung zwischen verschiedenen Interessenträgern, und die ENISA ist als dezentrale EU-Agentur imstande, für ein koordiniertes Vorgehen im Hinblick auf Cyberbedrohungen in der EU zu sorgen.

Optionen für die Zukunft der Agentur

Ausgehend von den genannten zentralen Problemen, die sich aus den Erkenntnissen und Schlussfolgerungen der Studie ableiten ließen, wurden vier Optionen für eine Überarbeitung des derzeitigen Mandats der ENISA entwickelt. Sie sind in nachstehender **Error! Reference source not found.** aufgeführt; zusätzlich wird für jede der Optionen angegeben, welche Elemente geändert werden könnten.

Tabelle 3: Optionen für die Zukunft der ENISA

Option	Zu änderndes Element
Option 0: Ausgangslage, Beibehaltung des Status quo Diese Option umfasst eine Erweiterung des derzeitigen Mandats hinsichtlich des Geltungsbereichs und der Ziele, wobei jedoch die Bestimmungen der NIS-Richtlinie, der eIDAS-Verordnung[3] und der Rahmenrichtlinie für Telekommunikation[4] berücksichtigt werden müssten.	**Überarbeitung des Mandats der ENISA, um ihre neuen Aufgaben gemäß jüngst erlassenen/anstehenden Rechtsvorschriften spezifischer zu machen** • Einbindung in die Kooperationsgruppe, wie in der NIS-Richtlinie gefordert • Sekretariat für das CSIRT-Netzwerk • Kodex für die elektronische Kommunikation, Erwägung 92 (Rahmenrichtlinie für Telekommunikation) • eIDAS
Option 1: Ablauf des Mandats der ENISA (Einstellung der Tätigkeiten der ENISA) Diese Option würde die Schließung der ENISA umfassen, wobei keine andere Institution auf EU-Ebene geschaffen, sondern auf bestehende Institutionen/Organisationen zurückgegriffen würde, um Verpflichtungen zu erfüllen, die sich beispielsweise im Rahmen der NIS-Richtlinie oder aufgrund bilateraler oder regionaler Verbindungen auf Ebene der Mitgliedstaaten ergeben.	Entfällt
Option 2: Stärkung der ENISA (Beibehaltung der ENISA mit Änderungen am Mandat) Bei dieser Option würden erhebliche Änderungen am Mandat der ENISA vorgenommen, um die in dieser Studie ermittelten zentralen Probleme anzugehen; dabei würde auf ihrer derzeitigen Rolle aufgebaut und sichergestellt, dass das neue Mandat besser auf die sich ändernden Gegebenheiten im Bereich der	**Stärkung der operativen Rolle der ENISA:** • Regelmäßige Bereitstellung von Informationen über Bedrohungen und Ad-hoc-Warnungen • Unterstützung des Plans für Reaktionen auf Vorfälle großen Ausmaßes im Bereich der Cybersicherheit auf EU-Ebene • Notfallreaktion im Bereich der Cybersicherheit **Stärkung der Rolle der ENISA bei der Entwicklung und Umsetzung politischer**

[3] Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG

[4] Richtlinie 2002/21/EG des Europäischen Parlaments und des Rates vom 7. März 2002 über einen gemeinsamen Rechtsrahmen für elektronische Kommunikationsnetze und -dienste (Rahmenrichtlinie)

Option	Zu änderndes Element
Cybersicherheit abgestimmt ist.	**Strategien:** • Verpflichtende Konsultation der ENISA durch die Kommission in Angelegenheiten der Cybersicherheit • Formelle Einbeziehung der ENISA in die Fazilität „Connecting Europe" • Einrichtung regelmäßiger Treffen zwischen der ENISA und anderen Agenturen/internationalen Organisationen
	Umwandlung des Mandats der ENISA in ein permanentes Mandat
	Stärkung der Führungsstruktur der ENISA: • Stärkung der Rolle der Ständigen Gruppe der Interessenträger (Permanent Stakeholders' Group – PSG) • Größere Flexibilität für die ENISA bei der Festlegung ihrer Arbeitsprioritäten
	Einbeziehung der ENISA in die Standardisierung und Zertifizierung auf EU-Ebene: • Unterstützung des IKT-Sicherheitszertifizierungsrahmens der EU • Unterstützung der IKT-Sicherheitsstandardisierung
	Stärkung der Rolle der ENISA im Hinblick auf Forschung und Innovation: • Teilnahme an der Umsetzung der Programmplanung • ODER Teilnahme an der Programmplanung in beratender Funktion • ODER Erhalt von EU-Forschungs- und -Entwicklungsfinanzierung
	Erhöhung der Sichtbarkeit der ENISA: • Einrichtung eines Verbindungsbüros in Brüssel • Schaffung eines speziellen Kommunikationsteams innerhalb der ENISA
Option 3: Europäische Agentur mit vollen operativen Fähigkeiten (Einrichtung eines Zentrums für Cybersicherheit) Bei dieser Option würde die ENISA in eine neue Einrichtung auf EU-Ebene umgewandelt, welche den gesamten Lebenszyklus im Bereich Cybersicherheit abdecken würde und für die Prävention und Erkennung von und Reaktion auf Cybervorfälle zuständig wäre.	**Schaffung eines EU-Cybersicherheitsschirms:** • Dieser Schirm würde die ENISA und das CERT-EU umfassen
	Schaffung eines virtuellen europäischen CSIRT: • Koordinierung der Vorgänge im CSIRT-Netzwerk • Erstellung von Informations-Feeds zur Echtzeit-Lageerkennung und zur Erfassung dynamischer Bedrohungen • Unterhaltung und Bereitstellung einer eigenen Reaktionskapazität bei Cybersicherheitsvorfällen an den öffentlichen und privaten Sektor
	Alle Elemente im Zusammenhang mit Option 2 könnten im Rahmen von Option 3 erfüllt werden.

Europäische Kommission

Evaluierung der Agentur der Europäischen Union für Netz- und Informationssicherheit (ENISA)

Luxemburg, Amt für Veröffentlichungen der Europäischen Union

2017 – 11 Seiten

ISBN 978-92-79-72112-0
doi:10.2759/561125

KK-02-17-971-DE-N

doi:10.2759/561125 ISBN 978-92-79-72112-0

Error! Reference source not found.