Rat der
Europäischen Union

Brüssel, den 21. Januar 2026
(OR. en)

5565/26

CYBER 24
JAI 84
DATAPROTECT 21
TELECOM 26
MI 56
IND 47
CADREFIN 25
FIN 99
BUDGET 2

ÜBERMITTLUNGSVERMERK

Absender:	Frau Martine DEPREZ, Direktorin, im Auftrag der Generalsekretärin der Europäischen Kommission
Eingangsdatum:	20. Januar 2026
Empfänger:	Frau Thérèse BLANCHET, Generalsekretärin des Rates der Europäischen Union
Nr. Komm.dok.:	COM(2026) 9 final
Betr.:	BERICHT DER KOMMISSION AN DAS EUROPÄISCHE PARLAMENT UND DEN RAT über die Bewertung der Agentur der Europäischen Union für Cybersicherheit (ENISA) und den europäischen Rahmen für die Cybersicherheitszertifizierung

Die Delegationen erhalten als Anlage das Dokument COM(2026) 9 final.

Anl.: COM(2026) 9 final

EUROPÄISCHE
KOMMISSION

Brüssel, den 20.1.2026
COM(2026) 9 final

BERICHT DER KOMMISSION AN DAS EUROPÄISCHE PARLAMENT UND DEN RAT

über die Bewertung der Agentur der Europäischen Union für Cybersicherheit (ENISA) und den europäischen Rahmen für die Cybersicherheitszertifizierung

{SWD(2026) 2 final}

1. EINFÜHRUNG

1.1 Informationen zur ENISA

Die 2004 gegründete Agentur der Europäischen Union für Cybersicherheit (ENISA) hatte ursprünglich zum Ziel, ein hohes Maß an Netz- und Informationssicherheit in der EU zu gewährleisten und eine Sicherheitskultur zum Nutzen ihrer Interessenträger zu schaffen. Im Laufe der Jahre haben sich das Mandat und die Aufgaben der Agentur erheblich weiterentwickelt, um mit dem raschen Wandel der digitalen Sicherheitslandschaft in Europa Schritt zu halten. Als Reaktion auf die immer komplexeren Herausforderungen im Bereich der Cybersicherheit wurde das Mandat der ENISA mit dem Rechtsakt zur Cybersicherheit 2019 erweitert, und sie erhielt einen dauerhaften Status im institutionellen Gefüge der EU. Durch diese Ausweitung des Mandats wurde die unterstützende Rolle der ENISA bei der Verwaltung und Koordinierung der Cybersicherheitsmaßnahmen in der gesamten EU weiter gestärkt, wobei der Schwerpunkt auf mehreren Schlüsselbereichen lag:

- Unterstützung der Entwicklung und Umsetzung der EU-Politik und des EU-Rechts im Bereich der Cybersicherheit
- Ausbau der Fähigkeit der EU zur Prävention, Erkennung und Abwehr von Cybersicherheitsvorfällen, insbesondere durch operative und technische Unterstützung der Mitgliedstaaten und der EU-Organe
- Förderung des Aufbaus von Cybersicherheitskapazitäten und der Zusammenarbeit innerhalb der EU
- Sensibilisierung für Cybersicherheitsrisiken und Förderung bewährter Verfahren in der breiten Öffentlichkeit, in Organisationen und Unternehmen
- Beitrag zur Einrichtung und Umsetzung des europäischen Rahmens für die Cybersicherheitszertifizierung mit dem Ziel, die Marktfragmentierung zu verringern und die Cybersicherheit von IKT-Produkten, -Diensten und -Prozessen in der gesamten EU zu stärken und
- Unterstützung der Zusammenarbeit mit internationalen Partnern im Einklang mit der Außenpolitik der EU

Die Tätigkeiten der ENISA umfassen nun die Formulierung von Empfehlungen zur grundlegenden Sicherheit, die Ausarbeitung von Berichten zur Bedrohungslage, von Leitlinien für die Normung und von Studien über bewährte Verfahren in verschiedenen Bereichen. Die Agentur organisiert Workshops, Übungen und Schulungsprogramme, um das Fachwissen von Cybersicherheitsfachleuten und politischen Entscheidungsträgern zu erweitern. Darüber hinaus spielt die ENISA eine Schlüsselrolle bei der Beantwortung von Anfragen der Kommission und der Mitgliedstaaten, bei der Unterstützung von Zertifizierungsaufgaben und bei der maßgeschneiderten Beratung zur Entwicklung und Umsetzung von Cybersicherheitsstrategien.

Zur erwarteten Wirkung der Tätigkeit der ENISA gehören die Verbesserung der Netz- und Informationssicherheit in der EU, die Stärkung des Vertrauens in den digitalen Binnenmarkt und die Förderung der Zusammenarbeit im Bereich der Cybersicherheit zwischen den wichtigsten Interessenträgern in Europa. Während Europa seinen digitalen Wandel fortsetzt, gewährleisten die Anpassungsstrategien der ENISA die Sicherheit und Resilienz der digitalen Landschaft der Region, wobei Herausforderungen wie Cybersicherheitsbedrohungen, geopolitische Spannungen und eine fragmentierte Politik der Mitgliedstaaten angegangen werden.

1.2 Über den europäischen Rahmen für die Cybersicherheitszertifizierung (ECCF)

Der europäische Rahmen für die Cybersicherheitszertifizierung (European Cybersecurity Certification Framework, ECCF) wurde durch den Rechtsakt zur Cybersicherheit mit dem vorrangigen Ziel eingerichtet, die Cybersicherheitslandschaft in der gesamten Europäischen Union zu verbessern. Mit dem ECCF soll ein einheitlicher und horizontaler Ansatz für die Cybersicherheitszertifizierung in allen Mitgliedstaaten geschaffen werden, um so die Fragmentierung für IKT-Produkte, -Dienste und -Prozesse im Binnenmarkt zu verringern. Damit stärkt der ECCF das Marktvertrauen, fördert das Wachstum des EU-Cybersicherheitsmarkts und gewährleistet eine robuste Resilienz und solide Kapazitäten im Bereich der Cybersicherheit. Der Rahmen deckt sechs grundlegende Bedürfnisse ab:

- Förderung des EU-weiten Marktvertrauens
- Verbesserung der Cybersicherheitsmaßnahmen und der Resilienz
- Festlegung hoher Standards für die Resilienz von Marktangeboten
- Verbesserung der Zusammenarbeit zwischen den Interessenträgern im Bereich der Cybersicherheit
- Verringerung des Zertifizierungsaufwands und
- Sensibilisierung der europäischen Öffentlichkeit und Unternehmen in Bezug auf Cybersicherheit

Darüber hinaus zielt der ECCF darauf ab, die Vertrauenswürdigkeit der Cybersicherheit transparenter zu machen und Sicherheit durch Technikgestaltung und Voreinstellungen zu fördern, was die Minderung von Schwachstellen und die Einhaltung spezifischer Sicherheitsanforderungen beinhaltet.

Um diese Ziele zu erreichen, stützt sich der ECCF auf mehrere zentrale Säulen, wobei die Entwicklung europäischer Systeme für die Cybersicherheitszertifizierung im Mittelpunkt der Maßnahmen steht. Der Schwerpunkt des Rahmens liegt auf einer umfassenden Vertrauenswürdigkeit der Cybersicherheit und auf der EU-weiten Resilienz durch diese Systeme. Der Rahmen fördert den Gemeinschaftsaufbau, um wichtige Beiträge der Interessenträger zu einzuholen und die Zusammenarbeit mit und zwischen den Mitgliedstaaten zu erleichtern. Im Rechtsakt zur Cybersicherheit sind zudem eine öffentliche Konsultation aller infrage kommenden Interessenträger im Wege eines förmlichen, offenen, transparenten und inklusiven Konsultationsprozesses sowie die Bildung von Ad-hoc-Beratungsgremien vorgeschrieben, um im Rahmen der Entwicklung von Zertifizierungssystemen unterschiedliche Perspektiven und Fachkenntnisse einzuholen. Die ENISA spielt eine entscheidende Rolle bei der Koordinierung dieser Maßnahmen, indem sie die Interessenträger systematisch konsultiert, um die Berücksichtigung aller legislativen Elemente sicherzustellen, bevor die endgültigen möglichen Systeme der Europäischen Kommission zur Annahme vorgelegt werden.

Die Cybersicherheitslage, die zur Einrichtung des ECCF führte, ist durch eine sich rasch verändernde Bedrohungslandschaft mit einer steigenden Anzahl von Cyberangriffen gekennzeichnet, bei denen Schwachstellen und unzureichende Sicherheitsvorkehrungen ausgenutzt werden, verbunden mit einer zunehmenden Fragmentierung der Zertifizierung in der EU. Dieses Umfeld unterstreicht die Notwendigkeit, mithilfe des ECCF die Integrität, Vertraulichkeit und Verfügbarkeit von Daten während des gesamten Lebenszyklus von IKT-Produkten, -Diensten und -Prozessen zu gewährleisten. Nach Abschluss seiner Kerntätigkeiten soll der ECCF mehrere Ergebnisse hervorbringen, darunter systembezogene Dokumente, Veröffentlichungen, Veranstaltungen und strukturelle Verbesserungen zur Unterstützung der Umsetzung. Diese Maßnahmen zielen darauf ab, eine stärkere Nutzung von Cybersicherheitszertifizierungen zu fördern, Verfahren zu straffen, das Vertrauen in den Binnenmarkt zu stärken und die Kapazitäten im öffentlichen und privaten Sektor auszubauen.

Durch die Beiträge des ECCF dürfte die Cyberresilienz und Wettbewerbsfähigkeit der EU künftig zunehmen, indem sichere und nahtlose digitale Interaktionen in der EU gewährleistet und gleichzeitig

neue Herausforderungen im Bereich der Cybersicherheit angegangen werden. Mittel- bis langfristig werden erhebliche Auswirkungen erwartet, wobei günstige Ergebnisse von dynamischen internen und externen Faktoren abhängen, einschließlich geopolitischer Verschiebungen, sich wandelnder Sicherheitslandschaften und neuer Marktbedürfnisse.

1.3 Zweck des Berichts

Dieser Bericht dient der Bewertung der Wirkung und der Wirksamkeit der Tätigkeit der ENISA und des ECCF, wobei die Weiterentwicklung des technologischen und regulatorischen Umfelds berücksichtigt wird. Gemäß Artikel 67 der Verordnung (EU) 2019/881, dem Rechtsakt zur Cybersicherheit, werden im Rahmen dieser Bewertung nicht nur das Mandat und die Tätigkeiten der ENISA überprüft, sondern es wird auch die Rolle des ECCF bei der Förderung eines sicheren Cyberumfelds in der gesamten EU im Zeitraum bis zum 28. Juni 2024 bewertet. Die dargelegten Ergebnisse wurden dem vorbereitenden Bewertungsbericht, der im Dezember 2024 fertiggestellt wurde, entnommen.

Die Analyse bezieht sich auf den Zeitraum von 2017 bis 2023, wobei vor allem die folgenden Ziele verfolgt werden. In erster Linie sollen die Leistung, die Governance und die Arbeitsweise der ENISA und des ECCF überprüft werden. Hierfür ist insbesondere zu ermitteln, inwieweit sie ihre Ziele erreicht und zu einer höheren Cybersicherheit und einem besser funktionierenden Binnenmarkt in der EU beigetragen haben. Die Bewertung konzentriert sich auf fünf Hauptkriterien – Wirksamkeit, Effizienz, Relevanz, Kohärenz und EU-Mehrwert – und bietet somit einen Rahmen, um sowohl die Erfolge der beiden Einrichtungen zu erfassen als auch festzustellen, in welchen Bereichen Verbesserungsbedarf besteht.

Durch die Untersuchung dieser Elemente bietet der Bericht Erkenntnisse dazu, wie sich das Mandat der ENISA anpassen ließe und welche Strategien zur Stärkung der Wirkung des ECCF ergriffen werden könnten. Letztlich sollen diese Bewertungen eine fundierte Entscheidungsfindung erleichtern, um die Abwehrfähigkeit der EU im Bereich der Cybersicherheit zu verbessern. Der Bericht besteht aus folgenden Abschnitten: eine Einführung zur ENISA und zum ECCF, eine Analyse der Bewertungsergebnisse und eine Zusammenfassung der Schlussfolgerungen und Empfehlungen.

Mit der Verordnung (EU) 2024/2847 (Cyberresilienz-Verordnung) werden horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen (Hardware und Software, einschließlich ihrer Komponenten, wenn sie getrennt in Verkehr gebracht werden) eingeführt. Ihr Inverkehrbringen auf dem Unionsmarkt wird von der Einhaltung einer Reihe grundlegender Cybersicherheitsanforderungen abhängig gemacht, die dem Ansatz des neuen Rechtsrahmens der Union entsprechen. Die Cyberresilienz-Verordnung trat am 10. Dezember 2024 in Kraft und wird ab dem 11. Dezember 2027 in vollem Umfang gelten. Dem Vorschlag der Kommission lag eine umfassende Folgenabschätzung bei, in der die Gründe für die Einführung dieser Vorschriften analysiert wurden. Vor diesem Hintergrund und angesichts der Tatsache, dass sich die Cyberresilienz-Verordnung noch in der Übergangsphase befindet, wurde es nicht für notwendig erachtet, in diesem Bericht das dritte in Artikel 67 Absatz 3 des Rechtsakts zur Cybersicherheit genannte Element weiter zu prüfen: „Bei der Bewertung wird beurteilt, ob wesentliche Anforderungen an die Cybersicherheit für den Zugang zum Binnenmarkt erforderlich sind, damit keine IKT-Produkte, -Dienste und -Prozesse und verwalteten Sicherheitsdienste auf den Binnenmarkt gelangen, die den grundlegenden Anforderungen an die Cybersicherheit nicht entsprechen.“

Da die Ergebnisse dieses Berichts die politischen Ziele der Überarbeitung des Rechtsakts zur Cybersicherheit untermauern, ist dieser Bericht dem Rechtsakt beigefügt. Deshalb ist es wichtig, den Bericht als Teil dieses Pakets vorzulegen.

2. WICHTIGSTE ERGEBNISSE DER BEWERTUNG

2.1 ENISA

In diesem Abschnitt werden die wichtigsten Ergebnisse der Bewertung der Tätigkeit der ENISA dargelegt, wobei der Schwerpunkt auf der Wirksamkeit, Effizienz, Relevanz und Kohärenz der Tätigkeit der Agentur und auf ihrem Mehrwert für die Cybersicherheitslandschaft der EU liegt. Darüber hinaus werden die interne Governance und die internen Verfahren der Agentur genauer untersucht, um sowohl ihre Funktionsweise als auch verbesserungswürdige Bereiche zu beleuchten.

Wirksamkeit

Im vorbereitenden Bewertungsbericht wird hervorgehoben, dass die ENISA ihr Mandat erfüllt hat, da sie fast alle geplanten Ergebnisse erzielt hat. Es sei jedoch darauf hingewiesen, dass die Wirksamkeitsanalyse in Ermangelung ausreichender Indikatoren hauptsächlich auf Interviews und Befragungen unter den Interessenträgern beruht. Die Agentur hat insbesondere in schwierigen Zeiten wie der COVID-19-Pandemie und dem Angriffskrieg Russlands gegen die Ukraine Flexibilität bewiesen und wurde von Interessenträgern positiv bewertet. Während der COVID-19-Pandemie unterstützte die ENISA die Kommission und die Mitgliedstaaten bei der kurzfristigen Festlegung von Sicherheitsanforderungen für die COVID-19-Anwendung. Außerdem spielte sie eine Rolle bei der Zusammenarbeit mit der Ukraine, durch die sichergestellt werden sollte, dass Angriffe auf kritische Infrastrukturen und Sektoren wie Energie nicht zu Ausstrahlungseffekten führen. Die Wirksamkeit der Tätigkeit der ENISA ergibt sich aus einer robusten Governance-Struktur und einem matrixbasierten Organisationsmodell, das die Erfüllung der Aufgaben und die Zusammenarbeit erleichtert. Die ENISA hat viele ihrer Ziele erreicht. Die Beiträge der ENISA zur Stärkung der Abwehrfähigkeit der EU im Bereich der Cybersicherheit wurden von den Interessenträgern allgemein anerkannt und geschätzt. Die Agentur förderte die Zusammenarbeit und den Informationsaustausch zwischen den Mitgliedstaaten und anderen Interessenträgern, um die Cybersicherheitsziele der EU zu unterstützen. Die Bemühungen der Agentur, um die technische Zusammenarbeit zu erleichtern, gemeinsame Cybersicherheitsstandards zu fördern und Initiativen zum Kapazitätsaufbau zu unterstützen, wurden besonders geschätzt. Ferner geht aus dem Bewertungsbericht hervor, dass die Prioritätensetzung bei den Aufgaben der ENISA verbessert werden könnte. Durch eine Neubewertung ihres operativen Schwerpunkts kann die ENISA bestehende Rahmen und Rückmeldungen der Interessenträger nutzen, um ihre Aufgaben noch besser zu erfüllen. Dieser Ansatz ist besonders wichtig, um neue Prioritäten anzugehen, ohne bestehende Verpflichtungen zu beeinträchtigen. Zu den Stärken der ENISA zählt ihr anhaltendes Engagement für die Einbeziehung und Konsultation der Interessenträger, doch bei den operativen Kapazitäten verfügt die Agentur über unzureichende Ressourcen. Um eine zeitnahe Bearbeitung neuer Anfragen zu ermöglichen und die Fähigkeit der ENISA, auf Herausforderungen im Bereich der Cybersicherheit zu reagieren, in gewissem Maße zu verbessern, könnte es hilfreich sein, Aufgaben und Ressourcen dynamischer umzuverteilen. Das Ziel der Agentur, ihren Ruf in Cybersicherheitskreisen zu pflegen und zu stärken, könnte weiter verwirklicht werden, indem sichergestellt wird, dass die Aufgaben nicht nur auf die strategischen Ziele, sondern auch auf die operativen Kapazitäten abgestimmt sind. Diese Prioritätensetzung sollte durch gemeinsame Anstrengungen der ENISA, der Mitgliedstaaten und der politischen Entscheidungsträger der EU erleichtert werden, um die Abstimmung auf die strategischen Ziele und auf die operativen Kapazitäten zu gewährleisten.

Effizienz

Im Bewertungszeitraum von 2017 bis 2023 hat sich die ENISA mit ihrer bestehenden Governance-Struktur als effizient erwiesen. Der matrixbasierte Organisationsrahmen half der ENISA dabei, Aufgaben zu priorisieren, die Ressourcenabstimmung zu optimieren und die Zusammenarbeit zwischen verschiedenen Stellen zu fördern. Dieser Ansatz trug in Verbindung mit einer ausgewogenen Mischung aus Betriebs- und Verwaltungspersonal dazu bei, die Erfüllung ihrer Aufgaben zu erleichtern. Es besteht jedoch ein eindeutiges Potenzial für die ENISA, ihre Effizienz durch eine bessere Prioritätensetzung, eine klare Ausrichtung und eine strategischere Ressourcenzuteilung zu steigern. Die Effizienz der Agentur wurde gelegentlich durch externe Faktoren und den Bedarf an einer strafferen internen Governance beeinträchtigt. Intern hat die ENISA innovative Lösungen entwickelt, wie z. B. ein matrixbasiertes Organisationsmodell, um Betriebs- und Verwaltungsfunktionen wirksamer zu koordinieren.

Trotzdem wurden in der Bewertung mehrere Schlüsselbereiche hervorgehoben, in denen die ENISA noch mehr Effizienz erzielen kann. Aus Befragungen von Beschäftigten der ENISA, Umfragen unter Interessenträgern und internen Unterlagen ging hervor, dass die Agentur Schwierigkeiten hatte, mit den steigenden Anforderungen Schritt zu halten und spezialisierte Stellen zu besetzen, was durch den weltweiten Mangel an IT-Fachkräften noch verschärft wurde. Dies hat zu Verzögerungen, zu einer Neugewichtung der Aufgaben und zu Phasen mit hoher Stress- und Arbeitsbelastung geführt. Gleichwohl könnten diese Herausforderungen durch bestimmte Anpassungen abgemildert werden. Die jüngsten strategischen Entscheidungen zur Umverteilung von Personalressourcen zeigen, dass sich Schwerpunktverlagerungen in gewissem Maße bewältigen lassen. Obwohl 2022 eine beträchtliche Erhöhung der Haushaltsmittel um 15 Mio. EUR vorgenommen wurde, um dem Aktionsprogramm zur Förderung der Cybersicherheit gerecht zu werden, wurde das Personal nicht in einem vergleichbaren Maße aufgestockt. Tatsächlich zeigt eine Neuzuweisung von rund 10,5 VZÄ im Jahr 2022, um das Aktionsprogramm zur Förderung der Cybersicherheit zu unterstützen, dass die derzeitigen Ressourcen erforderlichenfalls optimiert werden können. Allerdings wurden die zur Umsetzung des Aktionsprogramms benötigten VZÄ in diesem Fall teilweise durch Auftragsvergabe und teilweise durch Vertragsverwaltungspersonal beschafft, wie im vorbereitenden Bewertungsbericht hervorgehoben wurde. Die 10,5 VZÄ wurden aus dem bestehenden Arbeitsprogramm der Agentur umverteilt, davon 4 VZÄ aus Tätigkeit 4 („Ermöglichung der operativen Zusammenarbeit“), 4 VZÄ aus Tätigkeit 5 („Gemeinsame Reaktion auf Ebene der Union und der Mitgliedstaaten“) und 2,5 VZÄ aus anderen Tätigkeiten. Folglich hat die ENISA im Jahr 2023 Schritte unternommen, um bestimmte Tätigkeiten hintenanzustellen und/oder zurückzufahren, und ihr Personal auf operative Aufgaben verlagert, die sich insbesondere aus konkreten Aufgaben in den Rechtsvorschriften ergeben. Dies wirkte sich negativ auf andere Aufgaben aus, die weniger klar aus dem ENISA-Mandat hervorgingen, z. B. in Bezug auf Kompetenzen und Sensibilisierung.

Bei der Haushaltsführung besteht ebenfalls Verbesserungspotenzial. Aufgrund von Verzögerungen bei Maßnahmen wie dem Aktionsprogramm zur Förderung der Cybersicherheit verzeichnete die Agentur zwischen 2019 und 2022 einen Abwärtstrend beim Ausgleich genehmigter und gebundener Mittel. Durch die Umkehrung dieses Trends und durch gezielte Maßnahmen für das Management der Verwaltungsausgaben, einschließlich der Vermeidung von Verzögerungen bei der Auftragsvergabe, könnte die interne Effizienz weiter verbessert werden.

Relevanz

Die Relevanz der Tätigkeit der ENISA im Bereich der Cybersicherheit wird durch ihre Fähigkeit unterstrichen, auf veränderte Bedürfnisse der Interessenträger zu reagieren und sich flexibel an die sich

wandelnde Landschaft anzupassen. Die Agentur hat beständig unter Beweis gestellt, dass sie in der Lage ist, ihre Tätigkeitsbereiche zu überprüfen und neu auszurichten, um auf neue Entwicklungen einzugehen und so ihre Position als wesentliche Komponente des Cybersicherheitsrahmens der EU zu bekräftigen. Während die Interessenträger mit den Maßnahmen der ENISA im Allgemeinen zufrieden sind, gibt es auch Bereiche, in denen ihre Relevanz ausbaufähig ist. Trotz ihrer Reaktionsfähigkeit könnte die ENISA die Unterstützung und Sichtbarkeit gegenüber verschiedenen Sektoren und Interessenträgern verbessern, insbesondere bei KMU, die häufig Schwierigkeiten haben, die Cybersicherheitsanforderungen zu erfüllen. Durch eine Verlagerung hin zur Bereitstellung direkterer Instrumente und Ressourcen, die auf bestimmte Sektoren zugeschnitten sind, aber auch Erkenntnisse und Instrumente zur Bewältigung neuer Bedrohungen bieten, kann die Agentur ihre Wirkung erhöhen. Der Ansatz der Agentur für die Einbeziehung der Interessenträger war wirksam; mithilfe von Foren, Ausschüssen und Arbeitsgruppen wurden nationale Sachverständige aktiv in Aktionen und Veröffentlichungen eingebunden. Die komplexe dezentrale Struktur in einigen Mitgliedstaaten brachte jedoch Herausforderungen mit sich, die durch eine bessere Organisation und eine klarere Koordinierung mit den nationalen Behörden abgemildert werden könnten. Die laufenden Initiativen der Agentur, einschließlich der Entwicklung von Cybersicherheitsleitlinien und Programmen zum Kapazitätsaufbau, spiegeln ihr Engagement für die Förderung der Zusammenarbeit und die Stärkung der kollektiven Cybersicherheitslage der EU wider. Durch die Förderung einer engeren Zusammenarbeit zwischen den Wirtschaftszweigen und die Verbesserung des Informationszugangs könnten einige der von der Industrie wahrgenommenen Einschränkungen beseitigt werden. Das erhebliche Verbesserungspotenzial der ENISA liegt in der Überprüfung von Prioritäten, der Straffung von Verfahren, dem Erwerb neuer geeigneter Ressourcen und der effizienten Maximierung vorhandener Ressourcen, um ihre grundlegende Rolle im europäischen Cybersicherheitsökosystem zu stärken. Durch eine strategische Abstimmung auf die europäische Cybersicherheitsstrategie könnte die ENISA mit überarbeiteten Prioritäten den Weg für wirkungsvollere Beiträge ebnen. Damit die Agentur in der Lage ist, bessere politische und technische Unterstützung zu leisten, könnte die Bereitstellung von mehr Ressourcen, eine selektivere Auswahl ihrer Verpflichtungen und eine Verfeinerung ihrer operativen Schwerpunkte erforderlich sein. Zusammenfassend lässt sich sagen, dass trotz einer klaren Relevanz der Tätigkeit der ENISA noch Verbesserungsbedarf besteht. Durch die Neugewichtung der Tätigkeiten, die Bereitstellung von mehr Ressourcen und die Optimierung der vorhandenen Ressourcen kann die ENISA sowohl ihre Effizienz als auch ihre allgemeine Wirkung steigern und sich stärker an den dynamischen Anforderungen der europäischen Cybersicherheitslandschaft ausrichten.

Kohärenz

In der Bewertung der Kohärenz der Tätigkeit der ENISA werden sowohl Stärken als auch verbesserungswürdige Bereiche hervorgehoben. Das Engagement der ENISA für die Förderung der Kooperation im Bereich der Cybersicherheit auf EU-Ebene kommt klar zum Ausdruck, insbesondere in ihrer Vermittlerrolle und der direkten Zusammenarbeit mit Interessenträgern. Durch diesen dualen Ansatz konnte die ENISA einen wesentlichen Beitrag zum Cyberbereich leisten, der im Einklang mit den jüngsten Rechtsrahmen steht. Obwohl die ENISA als Vermittlerin und Koordinatorin eine positive Rolle spielt, sind in mehreren Bereichen Verbesserungen erforderlich, um die Kohärenz zu steigern. Bei der Bewertung wurde festgestellt, dass die Synergien zwischen den Zuständigkeiten und Maßnahmen der ENISA und denen anderer EU-Einrichtungen, darunter das Europäische Kompetenzzentrum für Cybersicherheit (ECCC) sowie die nationalen Cybersicherheitsbehörden, verbessert werden müssen. Obwohl diese Rollen oft komplementär sind, gibt es Möglichkeiten, die Abläufe weiter zu straffen und die organisatorische Effizienz zu verbessern. Durch formalisierte Kooperationsvereinbarungen mit

anderen Einrichtungen, wie der EMSA und der Gemeinsamen Forschungsstelle (JRC), könnte die ENISA Synergien besser nutzen und einen einheitlichen Ansatz für Cybersicherheitsinitiativen gewährleisten. Die interne Kommunikation und das Ressourcenmanagement innerhalb der ENISA sollten ebenfalls optimiert werden. Die Interaktion der Agentur mit privaten Interessenträgern und internationalen Partnern muss vorhersehbarer und transparenter sein, um das Vertrauen aufrechtzuerhalten und gemeinsame Anstrengungen zu fördern. Im Einklang mit der Cyberresilienz-Verordnung und der NIS-2-Richtlinie könnte eine klare Abgrenzung der Aufgaben der ENISA bei der Unterstützung der Politikumsetzung für mehr Effizienz sorgen und die Kohärenz zwischen den Regulierungsmaßnahmen gewährleisten. Durch diese Klarheit wäre die ENISA auch besser in der Lage, auf sektorale regulatorische Anforderungen zu reagieren. Zusammenfassend lässt sich sagen, dass die ENISA zwar eine solide Grundlage für die Förderung der Kohärenz der Cybersicherheit in der EU geschaffen hat, jedoch noch Spielraum für eine Neugewichtung ihrer Tätigkeiten besteht. Dieser Ansatz wird dazu beitragen, dass sie ihr Mandat effizient erfüllen und sich an die Weiterentwicklung der Cybersicherheitslandschaft anpassen kann. Durch die Beseitigung der derzeitigen Ineffizienzen und die Verbesserung der behördenübergreifenden Koordinierung kann die ENISA weiterhin eine entscheidende Rolle im Cybersicherheitsrahmen der EU einnehmen.

EU-Mehrwert

Die ENISA hat wesentlich zur Förderung des Cybersicherheitsökosystems der EU beigetragen, doch es besteht noch Verbesserungspotenzial, um diese Wirkung zu verstärken. Als zentrale Stelle hat die ENISA die unverzichtbare EU-weite Zusammenarbeit erleichtert, die nationalen Bemühungen, insbesondere in Mitgliedstaaten mit weniger entwickelten Cybersicherheitsinfrastrukturen, ergänzt und die Cybersicherheitspraktiken und -strategien aufeinander abgestimmt. Als dezentrale EU-Agentur mit besonderem Mandat konnte die ENISA das Fachwissen im Bereich der Cybersicherheit konsolidieren und wirksam mit den Mitgliedstaaten zusammenzuarbeiten, sodass sie entscheidend zur Gestaltung der Cybersicherheitslandschaft Europas beiträgt. In diesem Zusammenhang muss die ENISA den Fokus auf die Mitgliedstaaten legen, da sie Einblicke in neu auftretende Bedrohungen liefert und Instrumente und Strategien zu deren Bekämpfung empfiehlt. Die Agentur könnte die internationale Zusammenarbeit im Einklang mit den Prioritäten der Union weiter verstärken, auch mit Partnern in Drittländern, internationalen Organisationen und Cybersicherheitsagenturen, um dem globalen Charakter von Cyberbedrohungen besser Rechnung zu tragen. Darüber hinaus spielt die ENISA eine kritische Rolle bei der Förderung der Cybersicherheitszertifizierung und der Unterstützung von Normungstätigkeiten, um die Marktfragmentierung zu verringern und robuste Cybersicherheitspraktiken in der gesamten EU voranzutreiben. Trotz der Tatsache, dass es keine vergleichbaren Einrichtungen mit dem Fachwissen und der organisatorischen Flexibilität der ENISA gibt, kritisierten Interessenträger des Privatsektors ihren derzeitigen Hauptschwerpunkt auf den nationalen Behörden. Rückmeldungen großer Industrieakteure deuten darauf hin, dass mehr getan werden könnte, um Erkenntnisse auf die spezifischen Herausforderungen des Privatsektors abzustimmen. Obwohl der Hauptschwerpunkt auf den nationalen Behörden von entscheidender Bedeutung ist, könnten diese Bedenken ausgeräumt werden, indem die Einbeziehung der Interessenträger und die Zusammenarbeit mit der Industrie strategisch verbessert werden. Darüber hinaus könnte das Mandat der ENISA von einer strategischen Neubewertung ihrer Prioritäten profitieren, damit sie sich reibungslos an die sich wandelnden Herausforderungen im Bereich der Cybersicherheit anpassen kann. Dies würde es der ENISA ermöglichen, weiterhin wertvolle Beiträge zur EU zu leisten und gleichzeitig den wachsenden Bedürfnissen ihrer verschiedenen Interessenträger wirksam gerecht zu werden.

Wichtige Ergebnisse und Herausforderungen

Aufgrund ihres guten Rufs, ihrer hochwertigen Veröffentlichungen und ihrer wichtigen Rolle bei der Förderung der Zusammenarbeit zwischen den Mitgliedstaaten und anderen Cybersicherheitseinrichtungen ist die ENISA in den Cybersicherheitskreisen der EU weithin anerkannt. Die Arbeit der ENISA, die zur Harmonisierung der Cybersicherheitsanforderungen beiträgt, ist für die Schaffung eines einheitlichen Schutzniveaus in allen Mitgliedstaaten von wesentlicher Bedeutung und trägt unmittelbar zum Kapazitätsaufbau bei, insbesondere für kleinere Mitgliedstaaten. Diese Harmonisierung gewährleistet nicht nur ein sicheres digitales Umfeld in der gesamten EU, sondern erhöht auch die Abwehrbereitschaft im Bereich der Cybersicherheit für alle Interessenträger.

Die Bewertung ergab jedoch, dass die ENISA vor mehreren Herausforderungen steht. Auf sich wandelnde Cybersicherheitsbedrohungen reagiert die ENISA nur begrenzt flexibel, was zu potenziellen Verzögerungen bei ihren Tätigkeiten führen kann. Um die Herausforderungen im Zusammenhang mit Ressourcenknappheit abzumildern, betonten die konsultierten Interessenträger[2] unter anderem die Notwendigkeit verbesserter Einstellungsverfahren und Strategien zur Bewältigung der Arbeitsbelastung. Durch eine Ausweitung des Mandats der ENISA zur Stärkung ihrer operativen Rolle könnten diese Bedenken ausgeräumt und die ENISA in die Lage versetzt werden, technologische Fortschritte zu nutzen und die Cybersicherheitsrahmen zu verbessern. Mithilfe einer solchen Umstrukturierung könnte die ENISA dynamische Bedrohungen proaktiv angehen und ihre Wirkung durch gemeinsame Schulungsinitiativen und Beiträge zu politischen Entscheidungsprozessen ausbauen.

Schließlich werden die Konsultation der Interessenträger und die Managementsysteme der ENISA als wirksam erachtet, um die Bedürfnisse und Erwartungen der Interessenträger zu verwalten. Nichtsdestotrotz ist eine stärkere und transparentere Beziehung zu den Mitgliedstaaten erforderlich, um die Zusammenarbeit und den Informationsaustausch zu verbessern. Zu den künftigen Prioritäten gehört eine Aktualisierung der internen Rahmen, um die wachsenden Zuständigkeiten und die vielfältigen Herausforderungen besser zu bewältigen und sicherzustellen, dass die ENISA ihre Aufgaben mit dem bestehenden Personal voll und ganz erfüllen kann.

2.2 ECCF

In diesem Abschnitt werden die wichtigsten Ergebnisse der Bewertung in Bezug auf den ECCF dargelegt, wobei der Schwerpunkt auf seiner Wirksamkeit, Effizienz, Relevanz, Kohärenz und seinem Mehrwert für die Cybersicherheitslandschaft der EU liegt. Darüber hinaus werden die wichtigsten ermittelten Stärken und Schwächen des Rahmens auf der Grundlage einer SWOT-Analyse zusammengefasst.

Wirksamkeit

Der ECCF war als Säule für eine höhere Vertrauenswürdigkeit der Cybersicherheit im gesamten EU-Binnenmarkt vorgesehen, um die Zertifizierung von IKT-Produkten, -Diensten und -Prozessen zu harmonisieren. Er wurde eingerichtet, um anhaltende Probleme wie Marktfragmentierung und den Bedarf an mehr Transparenz und einem größeren Vertrauen der Öffentlichkeit in digitale Lösungen anzugehen. Durch das strukturierte Governance-Modell des ECCF, an dem Einrichtungen wie die ENISA, die Europäische Gruppe für die Cybersicherheitszertifizierung (ECCG) und das Netz der nationalen Behörden für die Cybersicherheitszertifizierung beteiligt sind, wurde die Grundlage für eine verstärkte Koordinierung zwischen den Interessenträgern, einschließlich der Mitgliedstaaten und privater Einrichtungen, geschaffen. Die praktische Umsetzung dieser Ziele war jedoch mit zahlreichen

Herausforderungen verbunden, was die Wirksamkeit des ECCF beeinträchtigt hat. Ein erheblicher Mangel des derzeitigen ECCF besteht darin, dass sich die Fragmentierung der Zertifizierungssysteme in der EU damit nicht wirksam bekämpfen lässt, was hauptsächlich auf verfahrensbezogene Einschränkungen zurückzuführen ist. Obwohl mit dem Rahmen eine Harmonisierung der Zertifizierungsverfahren angestrebt wurde, besteht diese Fragmentierung fort, was zu Inkohärenz und Ineffizienz bei der Vertrauenswürdigkeit der Cybersicherheit führt. Dies zeigt sich in der erheblichen Verzögerung bei der Umsetzung des ersten Zertifizierungssystems, der Gemeinsamen Kriterien der EU (EUCC), die von der Einleitung bis zur Annahme 57 Monate dauerte. Diese Verzögerung verdeutlicht die Ineffizienz der Verfahren des Rahmens, die hauptsächlich durch die komplexen und vielschichtigen Genehmigungsverfahren verursacht wird. Darüber hinaus haben Unklarheiten bei den Zuständigkeiten und der Rechenschaftspflicht der Interessenträger die Zielerreichung des Rahmens weiter erschwert. Externe Faktoren haben die Ziele des ECCF zusätzlich beeinträchtigt. Durch den Wandel der geopolitischen Landschaft, die durch zunehmende Cyberbedrohungen und politische Spannungen im Zusammenhang mit Datensouveränität und digitaler Kontrolle gekennzeichnet ist, waren Anpassungsmaßnahmen erforderlich, die im ECCF nur schwer zeitnah umgesetzt werden konnten. Dieser externe Druck führte zu Verzögerungen bei der Annahme von Systemen wie beispielsweise dem EUCS (Europäisches Cloud-Zertifizierungssystem), bei dem die Beratungen aufgrund nichttechnischer Debatten wie Datenlokalisierungsauflagen zum Stillstand kamen. Trotz dieser Hindernisse wurden positive Ergebnisse erzielt – insbesondere bei der Sensibilisierung der Mitgliedstaaten für die Bedeutung und die Komplexität der Cybersicherheitszertifizierung. Obwohl die COVID-19-Pandemie zu operativen Verzögerungen führte, verdeutlichte sie auch den Bedarf an einer resilienten digitalen Infrastruktur, wodurch die Cybersicherheit zu einem Brennpunkt der Politik wurde. COVID-19 hatte sowohl negative als auch positive Auswirkungen auf den ECCF. Auf der „negativen“ Seite trug der plötzliche Umstieg auf Online-Beratungen zu Verzögerungen bei der Systementwicklung bei. Auf der „positiven“ Seite hat die COVID-19-Pandemie das Bewusstsein für die Bedeutung resilienter Lieferketten geschärft, die weniger von Drittländern abhängig sind. Darüber hinaus erbrachte die Analyse wichtige Lehren, und es wurde festgestellt, dass die ungleiche Verteilung der Ressourcen auf die verschiedenen Interessenträger, darunter die Mitgliedstaaten, eine einheitliche Entwicklung und Umsetzung von Zertifizierungssystemen behindert. Die Beseitigung dieses Ungleichgewichts ist für die künftige Effizienz und Wirksamkeit von entscheidender Bedeutung, insbesondere durch die Bindung von Fachpersonal in der ENISA und die Förderung eines ständigen Dialogs zwischen allen Beteiligten.

Effizienz

Die Effizienz des ECCF wurde angesichts der längeren Fristen für die Annahme von Systemen für die Cybersicherheitszertifizierung und der vielschichtigen Komplexität, die damit einhergeht, einer Prüfung unterzogen. Trotz der strategischen Absicht, das Zertifizierungsverfahren in der gesamten EU zu straffen, wurde die Effizienz des ECCF insbesondere durch langwierige Diskussionen und Vorbereitungsphasen beeinträchtigt, die zu erheblichen Verzögerungen führten; das erste System wurde erst Anfang 2024 angenommen, d. h. fast fünf Jahre nach der Einführung. Diese langen Fristen wurden durch vielfältige Herausforderungen verursacht, die sowohl politischer als auch technischer Art waren.

Politische Herausforderungen, einschließlich der Politisierung der Diskussionen über Zertifizierungsanforderungen, haben den Fortschritt behindert, weil sie zu einem Umfeld mit mangelnder Transparenz und Kommunikation führten. So wurde beispielsweise das europäische Cloud-Zertifizierungssystem (EUCS) erheblich von Debatten über Anforderungen an die Datensouveränität beeinträchtigt, wodurch politischer Druck von Drittländern und der Industrie außerhalb der EU entstand und der technische Diskurs innerhalb der ECCG in einen politischen Diskurs umschlug.

Technische Komplexitäten trugen ebenfalls zur Ineffizienz bei, insbesondere die schwierige Umsetzung von Systementwürfen in Rechtsakte, da die für die Zertifizierung vorgesehenen Produkte/Dienstleistungen wie 5G und Cloud-Computing weit gefächert und anspruchsvoll sind. Die umfangreichen Anforderungen und das Fehlen etablierter Standards in bestimmten Bereichen haben die Vorbereitungs- und Annahmeprozesse zusätzlich erschwert, weil zahlreiche Interessenträger in vielen Phasen für die Abstimmung mit bestehenden Strategien und Verfahren sorgen müssen. Trotz dieser Ineffizienzen gab es innerhalb des Rahmens auch mehrere positive Elemente. Die Einrichtung spezieller Gruppen und Foren, einschließlich der Europäischen Gruppe für die Cybersicherheitszertifizierung (ECCG), der Ad-hoc-Arbeitsgruppe (AHWG) für spezifische Systeme und der Gruppe der Interessenträger für die Cybersicherheitszertifizierung (SCCG), erleichterte die erforderliche Einbeziehung der Interessenträger. Dennoch besteht nach wie vor erheblicher Verbesserungsbedarf, um die optimale Funktion dieser Strukturen sicherzustellen; so sahen die SCCG-Mitglieder beispielsweise eine mangelnde Einbeziehung der Gruppe in den ECCF. Die interne Governance muss unbedingt verbessert werden, um die aktive Beteiligung und den strategischen Beitrag der Interessenträger zu gewährleisten.

Relevanz

Der ECCF ist eine wichtige Reaktion auf die zunehmende Komplexität und Raffinesse von Cyberbedrohungen in der gesamten EU, denn er soll für die Einführung harmonisierter Systeme für die Cybersicherheitszertifizierung sorgen, die Vertrauen gewährleisten und einen sicheren digitalen Markt fördern. Trotz seiner vielversprechenden Prämisse wird die Relevanz des Rahmens nach wie vor eher als potenziell denn als praktisch angesehen, da Zertifizierungssysteme erst vor Kurzem in die operative Phase übergegangen sind. Diese Verzögerung bei der Erzielung greifbarer Ergebnisse unterstreicht die Diskrepanz bei der Umsetzung und lässt Unsicherheit in Bezug auf den derzeitigen Stellenwert des ECCF in der Cybersicherheitslandschaft aufkommen. Die Bedeutung des ECCF liegt in seiner strategischen Rolle, um die Cybersicherheitsstandards zu erhöhen und die gegenseitige Anerkennung von Zertifizierungen in allen Mitgliedstaaten zu ermöglichen, sodass die Kosten einzelner Unternehmen sinken und das Funktionieren des Binnenmarkts verbessert wird. Es wird eine solide Integration des Rahmens mit anderen EU-Rechtsakten angestrebt, um die Verfahren zu straffen und den grenzüberschreitenden Handel zu erleichtern.

Mehrere Faktoren verstärken die Relevanz des ECCF trotz der Herausforderungen, die mit der Wahrnehmung seiner Aufgaben verbunden sind. Der rasante Anstieg der Cyberbedrohungen führt zu einem deutlich höheren Bedarf an einer gemeinsamen Cybersicherheitsstrategie, die sich rasch an veränderte Szenarien anpassen lässt, wie z. B. die zunehmende Bedeutung von Zertifizierungen in Bereichen mit hohen Sicherheitsanforderungen wie Cloud-Dienste und 5G-Infrastrukturen. Die öffentlichen Aufträge in diesen Sektoren spiegeln die wachsende Nachfrage nach einem einheitlichen und zuverlässigen Zertifizierungsrahmen wider, und diese Nachfrage kann mit dem ECCF erfüllt werden. Darüber hinaus unterstreicht die Verknüpfung des ECCF mit neuen Rechtsakten, insbesondere der Cyberresilienz-Verordnung und der NIS-2-Richtlinie (Netz- und Informationssicherheitsrichtlinie), seinen erwarteten Nutzen für die Bewältigung kritischer Infrastrukturbedürfnisse und die Einhaltung der Rechtsvorschriften in der gesamten EU. Die proaktive Rolle der ENISA und die Einrichtung nationaler Behörden für die Cybersicherheitszertifizierung sind entscheidende Meilensteine für die Stärkung der kooperativen Interaktion und die Förderung der Zertifikatseinführung. Die Unterschiede in der Ressourcenverteilung und im Fachwissen zwischen größeren und kleineren Mitgliedstaaten führen jedoch weiterhin zu Ungleichgewichten hinsichtlich der Beteiligung und Wirksamkeit, was die Entwicklung gemeinsamer Systeme beeinträchtigt.

Kohärenz

Die Kohärenz des ECCF wird auch durch das Fehlen klarer Rechenschaftsmechanismen beeinträchtigt, was die Angleichung seiner Ziele an andere legislative Maßnahmen erschwert hat. Diese mangelnde Abstimmung birgt die Gefahr von Überschneidungen und Ineffizienzen in der Cybersicherheitslandschaft. Die vollständige Kohärenz des ECCF mit anderen EU-Rechtsinstrumenten, einschließlich der NIS-2-Richtlinie und der Cyberresilienz-Verordnung, ist für die Gewährleistung eines einheitlichen Cybersicherheitskonzeptes unverzichtbar. Theoretisch steht der ECCF im Einklang mit diesen gesetzgeberischen Maßnahmen, die darauf abzielen, verschiedene Aspekte der Cybersicherheit in der EU zu regeln. In der Praxis bleibt die Integration jedoch komplex und erfordert eine sorgfältige Überwachung. Mit der bevorstehenden Umsetzung der Gemeinsamen Kriterien der EU (EUCC) wird diese Kohärenz auf eine wichtige Probe gestellt, da ihre erfolgreiche Einführung die Fähigkeit des ECCF unter Beweis stellen wird, zusätzliche legislative Bemühungen zu harmonisieren und wirksam zu nutzen. Die Interessenträger haben betont, dass eine sorgfältige Abstimmung zwischen dem ECCF und neuen Rechtsakten erforderlich ist, um Überschneidungen zu vermeiden, die die Effizienz beeinträchtigen und die beabsichtigten Auswirkungen in allen Sektoren verwässern könnten. Insbesondere gibt es Bedenken hinsichtlich der Schnittstelle zwischen dem ECCF und der Cyberresilienz-Verordnung, da beide Initiativen darauf abzielen, die Cybersicherheitsstandards zu verbessern, aber die Gefahr von Redundanzen besteht, wenn sie nicht in vollständiger Synergie angewandt werden, sodass sich die beiden Rechtsvorschriften gegenseitig unterstützen und ergänzen. Auf sektoraler Ebene muss die Kohärenz ausgeweitet werden, um den kontinuierlichen technologischen Fortschritt zu berücksichtigen und sicherzustellen, dass Cybersicherheitsinitiativen angemessen differenziert werden, um dem Bedarf an kritischer Infrastruktur gerecht zu werden.

EU-Mehrwert

Trotz seines Potenzials hat der ECCF Schwierigkeiten, seinen Mehrwert bei der Förderung eines einheitlichen und wirksamen Cybersicherheitsumfelds in der gesamten EU zu entfalten. Mit dem ECCF sollte die Cybersicherheitslandschaft der EU erheblich verbessert werden, indem ein völlig neues Entwicklungsverfahren und eine beispiellose Governance-Struktur für Zertifizierungsverfahren eingeführt werden. Grundlegend bedeutet der ECCF einen entscheidenden Fortschritt für die Fähigkeit der EU, einen harmonisierten Ansatz für die Zertifizierung von IKT-Produkten, -Diensten und -Prozessen zu schaffen. Der inhärente EU-Mehrwert dieses Rahmens liegt in seinem Potenzial, unterschiedliche nationale Ansätze in Einklang zu bringen und einen Binnenmarkt mit kohärenten, zuverlässigen und anerkannten Cybersicherheitsstandards in allen Mitgliedstaaten zu fördern. Die langwierigen Zeitpläne und die fragmentierte Umsetzung der Systeme haben jedoch verhindert, dass der geplante Wert des ECCF voll ausgeschöpft werden konnte. Insbesondere die Verzögerung bei den umsetzbaren Systemen, die sich in der späten Annahme von Initiativen wie den Gemeinsamen Kriterien der EU (EUCC) zeigte, beeinträchtigte die unmittelbaren Auswirkungen, sodass das theoretische Potenzial des ECCF weitgehend ungenutzt blieb. Die Diskrepanzen bei der systemischen Umsetzung, die durch eine unterschiedliche Bereitschaft und Ressourcenverfügbarkeit in den Mitgliedstaaten noch verstärkt werden, schwächen den umfassenden Einfluss des Rahmens weiter ab. Dennoch wurde mit dem ECCF die Dynamik der EU-weiten Zusammenarbeit gestärkt. Durch die Einrichtung von Gruppen wie der ECCG wurden die Koordinierungsbemühungen institutionalisiert, was eine breitere Einbeziehung auf verschiedenen Governance-Ebenen ermöglicht hat. Diese kooperative Infrastruktur fördert den Informationsaustausch und gemeinsame Strategien und unterstützt so eine einheitliche Cybersicherheitspolitik gegen sich wandelnde Bedrohungen. Damit der ECCF seinen vollen EU-

Mehrwert entfalten kann, ist eine verstärkte und gezielte Beteiligung der Interessenträger von entscheidender Bedeutung. Die Förderung eines inklusiven Umfelds, in dem Industriepartner, nationale Behörden und EU-Einrichtungen aktiv zum Zertifizierungsverfahren beitragen und dieses steuern, wird eine breite Akzeptanz und Wirksamkeit der Cybersicherheitsstandards gewährleisten.

Wichtige Ergebnisse und Herausforderungen

Der ECCF dient als kritisches Instrument zur Verbesserung der Zusammenarbeit zwischen der ENISA, den Mitgliedstaaten und der Industrie auf EU-Ebene, was seine Relevanz im dynamischen Cybersicherheitsumfeld unterstreicht. Seine Flexibilität erleichtert die Systementwicklung durch Ad-hoc-Arbeitsgruppen und steht im Einklang mit EU-Rechtsrahmen wie der NIS-2-Richtlinie. Dieses beträchtliche Potenzial bleibt jedoch weitgehend ungenutzt, da Systeme nur begrenzt tatsächlich umgesetzt werden.

Der ECCF spielt eine entscheidende Rolle, um neue Cybersicherheitsbedrohungen zu bewältigen und die Einhaltung der Vorschriften zu fördern, insbesondere bei der Nutzung neuer Technologien wie der künstlichen Intelligenz. Die Interessenträger bestätigen seine Bedeutung für eine stärkere Zusammenarbeit der Mitgliedstaaten und eine bessere Abwehrbereitschaft im Bereich der Cybersicherheit. Sein Wert für die Förderung des Austauschs im Binnenmarkt, indem nationale Zertifizierungssysteme durch EU-weite ersetzt werden, wird ebenfalls anerkannt.

Allerdings wird der ECCF durch erhebliche Schwachstellen behindert. Langwierige Verfahren für die Annahme von Systemen beeinträchtigen seine Wirksamkeit, und diese Herausforderung wird durch technische Komplexität und politischen Druck durch die Lobbyarbeit der Industrie noch verschärft. Diese Verzögerungen untergraben das Vertrauen und verhindern eine rasche Einführung europäischer Systeme für die Cybersicherheitszertifizierung. Obwohl Möglichkeiten bestehen, mit dem ECCF die EU-Rahmen für die Cybersicherheit zu verbessern, stellen Faktoren wie Ressourcenknappheit und geopolitische Spannungen eine Herausforderung dar. Verschiebungen bei den politischen Prioritäten und potenzielle Überschneidungen bei den Rechtsvorschriften könnten die Wirksamkeit des Rahmens beeinträchtigen und zu Marktinkonsistenzen führen. Diese Probleme müssen unbedingt bewältigt werden, um die Weiterentwicklung des ECCF von einem vielversprechenden Konzept zu einem voll funktionsfähigen Mechanismus sicherzustellen und so die Standardisierung und Zertifizierung der Cybersicherheit in der EU voranzutreiben.

3. SCHLUSSFOLGERUNGEN UND EMPFEHLUNGEN

3.1 ENISA

In der Bewertung der ENISA wird ihre maßgebliche Rolle bei der Schaffung einer kohärenten Cybersicherheitslandschaft in der gesamten EU hervorgehoben. Die ENISA hat sich als wirksam erwiesen und wertvolle Ergebnisse erzielt. Da die Anforderungen an die ENISA weiter steigen, ist es wichtig, ihre Tätigkeiten neu zu bewerten und ihren Betrieb zu straffen, um Ressourcen und Prioritäten besser aufeinander abzustimmen. Dabei sollte der Schwerpunkt auf der Unterstützung der Mitgliedstaaten bei der Bewältigung ihrer Cybersicherheitsbedrohungen und der Verbesserung ihrer Cybersicherheitsinfrastrukturen auf nationaler Ebene liegen. Eine Optimierung des Verfahrens zur Erstellung von Berichten, indem Berichte durch visuelle Hilfsmittel und prägnante Zusammenfassungen benutzerfreundlicher und zugänglicher gemacht werden, könnte die Wirksamkeit und Relevanz der Tätigkeit der ENISA vor dem Hintergrund der aktuellen Bedrohungslage erhöhen. Die Stärkung der

Kommunikationskanäle ist unerlässlich, um sicherzustellen, dass die Tätigkeiten und Dienste der ENISA für die Interessenträger, einschließlich der Akteure aus der Industrie, deutlich sichtbar sind. Eine klar definierte Kommunikationsstrategie könnte dazu beitragen, stärkere Verbindungen und eine engere Zusammenarbeit innerhalb bestehender Cybersicherheitsnetze wie den Zentren für Informationsaustausch und Analysen (ISAC) zu fördern.

Die ENISA kann ihre Effizienz durch einen strategischeren Fokus auf der Priorisierung von Aufgaben verbessern und damit ihren Ansatz für die Bewältigung des Arbeitsaufkommens straffen. Um die Relevanz unter den Interessenträgern zu erhöhen, sollte die zentrale Rolle der ENISA bei der Unterstützung der Mitgliedstaaten ausgebaut werden, indem ihre Fähigkeit gestärkt wird, zeitnahe Einblicke in neue Bedrohungen und strategische Abwehrmaßnahmen zu geben. Darüber hinaus hat eine Reihe von Interessenträgern angemerkt, dass die ENISA strukturiertere und transparentere Methoden für die Zusammenarbeit mit privaten Einrichtungen, einschließlich der Unterstützung von KMU, einführen könnte. Die Rolle der ENISA bei der Umsetzung der Politik mit anderen EU-Organen muss präzisiert werden, um sicherzustellen, dass die Zusammenarbeit mit den Mitgliedstaaten bei den Bemühungen, die Kohärenz der einheitlichen Cybersicherheitsstrategie der EU zu stärken, an vorderster Front steht. Dies würde auch eine engere Zusammenarbeit mit anderen EU-Agenturen und die Suche nach Synergien mit anderen Cybersicherheitsstellen umfassen, um gemeinsame Maßnahmen zur Verbesserung der operativen Kohärenz in ganz Europa zu ergreifen.

Insgesamt ist es wichtig, den Status der ENISA als spezialisierte Agentur innerhalb des EU-Rahmens beizubehalten, da sie einen kontinuierlichen Schwerpunkt auf den Prioritäten im Bereich der Cybersicherheit sicherstellt. Diese Empfehlungen sollen helfen, die Fähigkeit der ENISA zur wirksamen Wahrnehmung ihrer Zuständigkeiten zu verbessern und ihre Rolle als führende Einrichtung im Bereich der Cybersicherheit zu bekräftigen.

3.2 ECCF

Aus der Bewertung des ECCF ergeben sich mehrere strategische Empfehlungen. Erstens wurde trotz der zentralen Rolle der ENISA bei der Förderung der Zusammenarbeit und der operativen Kohäsion zwischen den Mitgliedstaaten und anderen Interessenträgern deutlich, dass die Effizienz und Wirksamkeit des ECCF beschränkt waren, was hauptsächlich auf die komplexen Verfahren zur Annahme der Systeme zurückzuführen ist. Diese Probleme unterstreichen, dass die Governance-Strukturen grundlegend überarbeitet werden müssen, um die operative Klarheit und Rechenschaftspflicht auf allen Ebenen zu verbessern.

Aufgrund dieser Ergebnisse werden mehrere Maßnahmen empfohlen, um den Beitrag der ENISA zum ECCF zu optimieren. Es sollten konzertierte Anstrengungen unternommen werden, um eine kohärente und angemessene Verteilung der finanziellen und personellen Ressourcen auf die ENISA und andere Interessenträger innerhalb des ECCF zu gewährleisten. Die Beschäftigungsverhältnisse müssen zwingend stabilisiert werden, um die Fluktuation zu senken und das institutionelle Gedächtnis zu stärken und so eine effiziente Umsetzung und kontinuierliche Pflege von Systemen zu erleichtern. Die Einrichtung strafferer Entscheidungsprozesse innerhalb des ECCF, mit klaren Aufgaben und Zuständigkeiten, wird für mehr Transparenz und Effizienz sorgen, insbesondere beim Ausbau der gemeinsamen Bemühungen zwischen den Mitgliedstaaten, der Kommission und der ENISA. Dies wird die Rechenschaftspflicht fördern und Ineffizienzen verringern. Die Verpflichtung, realistische Zeitpläne für die Entwicklung und Umsetzung von Zertifizierungssystemen festzulegen und einzuhalten, spielt eine

wesentliche Rolle. Dies beinhaltet die Unterstützung detaillierter technischer Analysen und die Stärkung vorbereitender Maßnahmen, um politische Einflüsse wirksam zu antizipieren und abzumildern.

Darüber hinaus sind aktive Investitionen in die Ausbildung und Bindung von Fachpersonal innerhalb der ENISA unverzichtbar, um Kontinuität und Fachwissen bei der Bewältigung komplexer Cybersicherheitsherausforderungen zu gewährleisten. Die langfristige Stabilität der Belegschaft wird für die dauerhafte operative Wirksamkeit des ECCF entscheidend sein. Ferner sollten die Industrie und die Verbraucher durch gezielte Kampagnen und strategische Einbeziehung sensibilisiert werden, wobei der Wert zertifizierter Produkte und Dienste hervorgehoben wird. Es muss unbedingt ein proaktiver Ansatz verfolgt werden, um die Unterstützung der Interessenträger zu gewinnen, damit die Nachfrage nach und das Vertrauen in ECCF-Initiativen steigt.