SONDERBERICHT 19/2026 **DE**

Erkennung und Bewältigung von Cybersicherheitsvorfällen

Beim Kooperationsrahmen der EU sind Fortschritte zu verzeichnen, doch ist er wegen Verzögerungen bei der Umsetzung und eines begrenzten Informationsaustauschs nur bedingt wirksam

EUROPÄISCHER RECHNUNGSHOF

Inhalt

Ziffer

Anhänge

01 Hauptaussagen

Warum ist dieser Bereich wichtig?

01 Mit der zunehmenden Digitalisierung unserer Wirtschaft und unseres Alltags steigt das Risiko für Cyberangriffe. Cybersicherheit bezeichnet "alle Tätigkeiten, die notwendig sind, um Netz- und Informationssysteme, die Nutzer solcher Systeme und andere von Cyberbedrohungen betroffene Personen zu schützen"[1]. Cybersicherheit erfordert einen ganzheitlichen Ansatz zur Verhütung, Erkennung und Bewältigung von Cyberbedrohungen sowie zur anschließenden Wiederherstellung.

02 Die Cybersicherheitslandschaft der EU umfasst zahlreiche öffentliche und private Akteure, die auf regionaler, nationaler und EU-Ebene im zivilen Bereich tätig sind. Cybersicherheit ist auch ein zentraler Bestandteil der nationalen Sicherheit und Verteidigung.

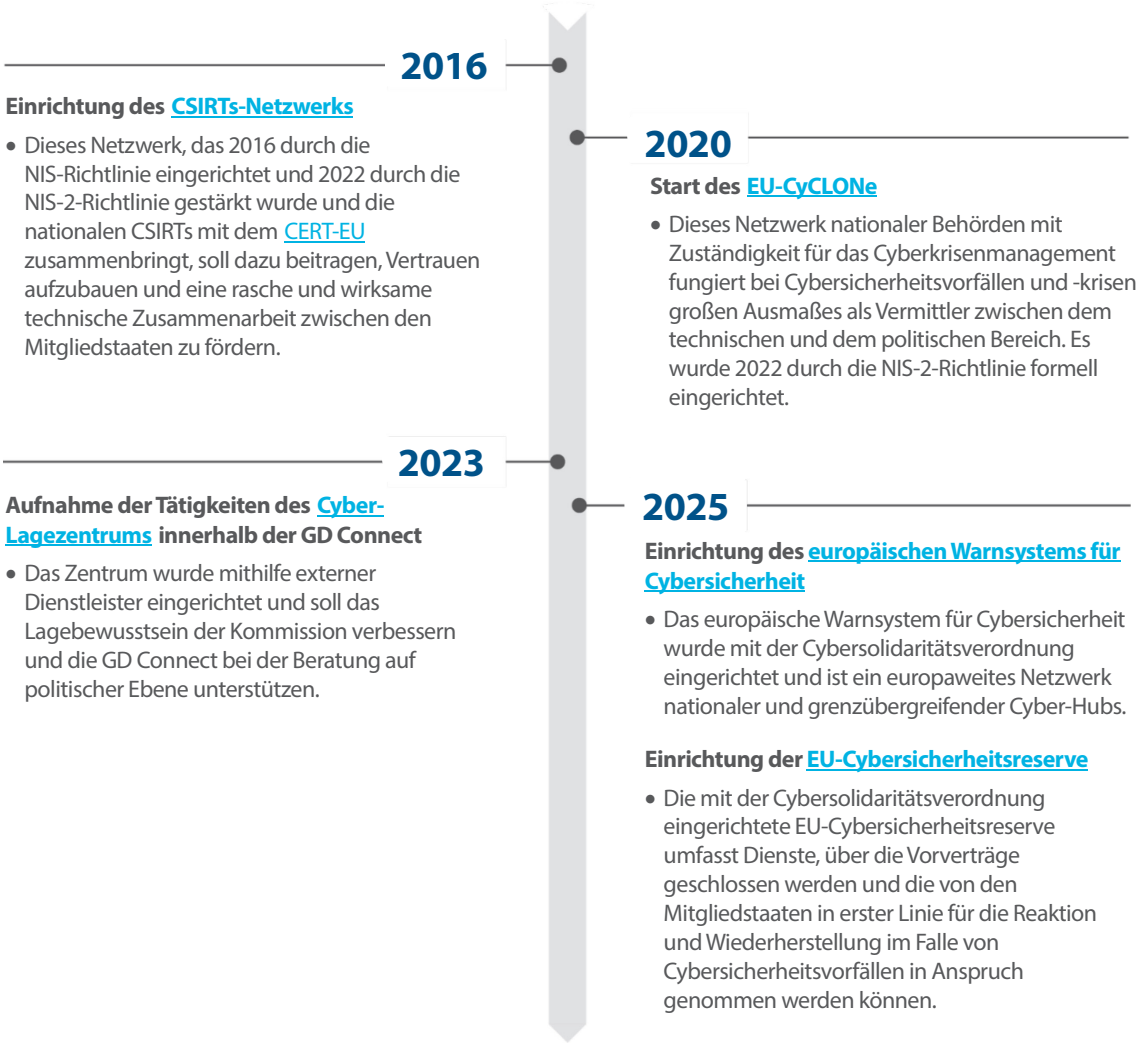
03 Die Mitgliedstaaten tragen die Hauptverantwortung für die Verhütung von, Vorsorge für und Bewältigung von Cybersicherheitsvorfällen und -krisen, die sie betreffen. Da diese Sicherheitsvorfälle das reibungslose Funktionieren des Binnenmarkts beeinträchtigen können, kommt der EU im Falle von erheblichen Sicherheitsvorfällen oder -krisen ebenfalls eine wichtige Rolle zu. In den letzten Jahren hat die EU ihren sich wandelnden Regelungsrahmen für die Cybersicherheit gestärkt[2] und verschiedene Netzwerke und Mechanismen eingerichtet (siehe ***Abbildung 1*** und ***Anhang II***).

---

[1] Verordnung (EU) 2019/881 (Rechtsakt zur Cybersicherheit).

[2] Zum Beispiel hat die Kommission im November 2025 die Digital-Omnibus-Verordnung und im Januar 2026 einen überarbeiteten EU-Rechtsakt zur Cybersicherheit vorgeschlagen.

Abbildung 1 | EU-Cybersicherheitsnetzwerke und -mechanismen 2016–2025



CSIRTs: Computer-Notfallteams
GD Connect: Generaldirektion Kommunikationsnetze, Inhalte und Technologien
EU-CyCLONe: Netzwerk der Verbindungsorganisationen für Cyberkrisen
NIS-Richtlinie: Richtlinie (EU) 2016/1148 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union
NIS-2-Richtlinie: Richtlinie (EU) 2022/2555 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union

Quelle: Europäischer Rechnungshof.

04 Innerhalb des derzeitigen mehrjährigen Finanzrahmens 2021–2027 ist das Programm "Digitales Europa" (DIGITAL) die wichtigste Finanzierungsquelle für die Cybersicherheit. Es verfügt über ein Gesamtbudget von 8,1 Milliarden Euro, wovon 1,4 Milliarden Euro für die Stärkung der Cybersicherheit vorgesehen sind.

05 Ziel der Prüfung des Rechnungshofs war es, zu bewerten, ob die Maßnahmen der EU die Erkennung von erheblichen Cybersicherheitsvorfällen und Cybersicherheitsvorfällen großen Ausmaßes sowie die Reaktion darauf wirksam erleichtern. Der Rechnungshof bewertete, ob dies zutrifft auf

- Netzwerke und Mechanismen auf EU-Ebene (d. h. das Netzwerk von Computer-Notfallteams (CSIRTs-Netzwerk), das Netzwerk der Verbindungsorganisationen für Cyberkrisen (EU-CyCLONe), das europäische Warnsystem für Cybersicherheit, das Cyber-Lagezentrum und die EU-Cybersicherheitsreserve);
- Maßnahmen, die im Rahmen von DIGITAL finanziert wurden.

06 Der Rechnungshof geht davon aus, dass seine Feststellungen zur Stärkung der Cyberresilienz der EU beitragen werden, indem sie zu einer Verbesserung der Wirksamkeit und Effizienz der EU-Netzwerke und -Mechanismen sowie der Auswahl und Überwachung EU-finanzierter Maßnahmen führen.

07 Die Prüfung deckt den Zeitraum von 2022 bis 2025 ab. Sie stützt sich auf eine Aktenprüfung und Analyse einschlägiger Dokumente, Prüfbesuche in drei Mitgliedstaaten (Irland, Griechenland und Italien) sowie schriftliche Fragebögen und Befragungen einschlägiger Interessenträger. Weitere Hintergrundinformationen und Einzelheiten zu Umfang und Ansatz der Prüfung sind ***Anhang I*** zu entnehmen.

Feststellungen und Empfehlungen des Rechnungshofs

08 Insgesamt ergab die Prüfung des Rechnungshofs, dass die Maßnahmen der EU die Erkennung von erheblichen Cybersicherheitsvorfällen und Cybersicherheitsvorfällen großen Ausmaßes sowie die Reaktion darauf nur teilweise erleichtern. Zwar wurde schrittweise ein Kooperationsrahmen geschaffen, doch die vollständige Ausgestaltung ist noch nicht abgeschlossen. Aufgrund des begrenzten Informationsaustauschs und angesichts von Schwachstellen bei der Berichterstattung und erheblichen Verzögerungen bei der Umsetzung kann das Potenzial der EU-Netzwerke und -Mechanismen nicht voll ausgeschöpft werden. Mit den von DIGITAL finanzierten Projekten werden relevante Ziele verfolgt, doch sind mehrere Projekte mit operativen Herausforderungen und Verzögerungen konfrontiert, und der allgemeine Rahmen für die Leistungsüberwachung weist Schwachstellen auf.

09 Der derzeitige Rahmen der EU-Netzwerke und -Mechanismen zur Erleichterung der Erkennung und Bewältigung erheblicher Cybersicherheitsvorfälle wurde schrittweise aufgebaut. Im Jahr 2025 nahm der Rat den Cyber-Konzeptentwurf an, in dem der EU-Rahmen für das Cyberkrisenmanagement festgelegt wird. Der Rechnungshof stellte fest, dass die Aufgaben und Zuständigkeiten in Bezug auf das Cyberkrisenmanagement der EU im Cyber-Konzeptentwurf weitgehend definiert sind. Ungeachtet dessen müssen die Verfahrensregelungen für die Zusammenarbeit zwischen dem (2016 eingerichteten) CSIRTs-Netzwerk und dem (2023 offiziell eingerichteten) EU-CyCLONe noch formell festgelegt werden (siehe Ziffern ***24***–***30***).

10 Der Rechnungshof stellte fest, dass der Informationsaustausch über diese Netzwerke begrenzt ist. Dies ist hauptsächlich zurückzuführen auf Verzögerungen bei der Umsetzung der Richtlinie über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union (NIS-2-Richtlinie), auf Schwierigkeiten bei der Feststellung, ob ein Sicherheitsvorfall grenzübergreifende Auswirkungen hat, sowie auf Rechtsvorschriften über die nationale Sicherheit, die den Informationsaustausch verhindern. Der Mehrwert der Netzwerke ist erheblich geringer, wenn die Mitgliedstaaten nicht bereit sind, zeitnahe und verwertbare Informationen auszutauschen (siehe Ziffern ***31***–***44***).

Empfehlung 1

Informationsaustausch zwischen den Mitgliedstaaten stärken

Um die Erkennung von Cybersicherheitsvorfällen und die Reaktion darauf zu verbessern, sollte die Kommission mit Unterstützung der Agentur der Europäischen Union für Cybersicherheit (ENISA)

a) der Kooperationsgruppe für Netz- und Informationssicherheit vorschlagen, eine detaillierte Analyse der nationalen Sicherheitsbeschränkungen durchzuführen, die den Informationsaustausch einschränken und sich auf die Cyberresilienz der EU auswirken, sowie rechtliche und technische Lösungen zu ermitteln, um den Informationsaustausch unter Achtung der im Bereich der nationalen Sicherheit geltenden Grenzen zu verbessern;

b) unbeschadet der Beschlüsse der beiden gesetzgebenden Organe in Zusammenarbeit mit den Mitgliedstaaten sicherstellen, dass die in der Digital-Omnibus-Verordnung vorgeschlagene zentrale Anlaufstelle zur Meldung von Vorfällen potenzielle grenzübergreifende Sicherheitsvorfälle erkennen kann;

c) Lösungen erarbeiten, die die Meldung von Sicherheitsvorfällen an die ENISA in Echtzeit ermöglichen.

Zieldatum für die Umsetzung: für die Buchstaben a) und b) bis 2027, für den Buchstaben c) bis 2028.

11 Im Jahr 2022 richtete die Kommission ihr Cyber-Lagezentrum ein, um ihr Lagebewusstsein zu verbessern, was sie bei der Erfüllung ihrer institutionellen Aufgaben im Bereich des Krisenmanagements unterstützen sollte. Der Betrieb des Zentrums wird zu einem Großteil von externen Dienstleistern unterstützt, mit denen ein Vertrag abgeschlossen wurde. Der Rechnungshof stellte fest, dass sich die von den externen Dienstleistern erbrachte Arbeit im Bereich der Lageerfassung und der Bedrohungsüberwachung teilweise mit den bestehenden Kapazitäten der Agentur der Europäischen Union für Cybersicherheit (ENISA) überschneidet. Er ist der Auffassung, dass bei der Einrichtung des Cyber-Lagezentrums das Rationalisierungspotenzial, dass die Nutzung bereits verfügbarer Informationen der Kommission und der ENISA geboten hätte, nicht zur Genüge ausgeschöpft wurde. Darüber hinaus stellt das Fehlen eines umfassenden, detaillierten Plans für die Zukunft nach Ablauf des Vertrags ein Risiko für den Betrieb des Cyber-Lagezentrums nach 2026 dar (siehe Ziffern *45*–*51*).

Empfehlung 2

Die EU-Kapazitäten zur Lageerfassung im Bereich der Cybersicherheit rationalisieren und die Verbreitung von Informationen optimieren

Um die Effizienz zu erhöhen, sollte die Kommission in Zusammenarbeit mit der ENISA bewerten, inwiefern Informationen zur Lageerfassung gemeinsam beschafft und analysiert werden können. Sie sollte diese Informationen und die damit verbundenen Berichte über Cyberbedrohungen außerdem allen einschlägigen Dienststellen und Agenturen der EU zur Verfügung stellen.

Zieldatum für die Umsetzung: 2027

12 Mit der Cybersolidaritätsverordnung von 2024 wurde die EU-Cybersicherheitsreserve eingerichtet, mit der die Mitgliedstaaten bei der Reaktion auf schwerwiegende Cybersicherheitsvorfälle und bei der anschließenden Wiederherstellung unterstützt werden sollen. Die Reserve umfasst ausgewählte Dienstleister für die einzelnen Mitgliedstaaten, die rund um die Uhr auf Vorfälle reagieren können. Zwar trägt dieser Ansatz dazu bei, den spezifischen Anforderungen der Mitgliedstaaten gerecht zu werden und Vertrauen aufzubauen, die verfügbaren Mittel werden jedoch zu gleichen Teilen auf die Mitgliedstaaten aufgeteilt, ohne die spezifischen Bedürfnisse der einzelnen Mitgliedstaaten zu berücksichtigen (siehe Ziffern ***52***–***57***).

13 Der Rechnungshof ist der Auffassung, dass der Rückgriff auf Anbieter, mit denen ein Vorvertrag geschlossen wurde, einen raschen Einsatz von Diensten zur Bewältigung von Sicherheitsvorfällen ("Sicherheitsvorfall-Notdienste") ermöglicht. Die EU-Cybersicherheitsreserve dient zwar in erster Linie der Unterstützung der Reaktion auf Sicherheitsvorfälle und der anschließenden Wiederherstellung, jedoch kann sie, wenn sie nicht für Reaktionsmaßnahmen genutzt wird, auch zur Stärkung der Abwehrbereitschaft eingesetzt werden. Dieser flexible Ansatz kann verhindern, dass im Voraus bezahlte Dienste ungenutzt bleiben. Es besteht jedoch die Gefahr, dass die Reserve entgegen ihrer Zweckbestimmung in erster Linie für die Abwehrbereitschaft und nicht für die Reaktion auf Sicherheitsvorfälle eingesetzt wird (siehe Ziffern ***58***–***61***).

14 Das europäische Warnsystem für Cybersicherheit ist ein Netzwerk nationaler und grenzübergreifender Cyber-Hubs, das darauf abzielt, die Erkennung und Analyse von Cyberbedrohungen sowie die Reaktion darauf zu verbessern. Der Rechnungshof stellte fest, dass die beiden Hubs (ATHENA und ENSOC) zum Zeitpunkt der Prüfung aufgrund beträchtlicher Verzögerungen bei der Beschaffung von Instrumenten und Diensten noch nicht betriebsbereit waren und dass das europäische Warnsystem für Cybersicherheit noch nicht funktionierte (siehe Ziffern ***62***–***70***).

15 Eines der Hauptziele des europäischen Warnsystems für Cybersicherheit besteht darin, einen sinnvollen Informationsaustausch zwischen Gruppen von Mitgliedstaaten zu fördern. Dadurch könnten zwar einige der Probleme im Zusammenhang mit dem Informationsaustausch gelöst werden, es ist jedoch sehr schwierig, Cyber-Hubs in die bereits komplexe Cybersicherheitslandschaft zu integrieren. Der Rechnungshof stellte fest, dass die Kooperationsvereinbarungen, gemeinsame Taxonomie und Interoperabilitätsstandards, die für eine vollständige Funktionsfähigkeit des europäischen Warnsystems für Cybersicherheit erforderlich wären, noch nicht vorhanden waren (siehe Ziffern ***71***–***74***).

Empfehlung 3

Das europäische Warnsystem für Cybersicherheit in die Cybersicherheitslandschaft der EU integrieren

Die Kommission sollte gemeinsam mit der ENISA und den Mitgliedstaaten sicherstellen, dass Kooperationsvereinbarungen und Interoperabilitätsstandards bestehen, um den Informationsaustausch zwischen den grenzübergreifenden Hubs, die Teil des europäischen Warnsystems für Cybersicherheit sind, dem CSIRTs-Netzwerk und dem EU-CyCLONe zu erleichtern.

Zieldatum für die Umsetzung: 2028

16 Im Jahr 2018 schlug die Kommission die Einrichtung des Europäischen Kompetenzzentrums für Cybersicherheit (ECCC) vor, mit dem ab 2021 die Cybersicherheitskomponente von DIGITAL verwaltet werden sollte. In der ECCC-Verordnung wurde die Einrichtung einer Kompetenzgemeinschaft für Cybersicherheit gefordert, die sich aus Vertretern von Industrie, Wissenschafts- und Forschungseinrichtungen zusammensetzt. Ausgewählte Mitglieder der Kompetenzgemeinschaft für Cybersicherheit sollten dann eine strategische Beratungsgruppe bilden (siehe Ziffern ***75***–***76***).

17 Der Rechnungshof stellte fest, dass es zu Verzögerungen kam, was die Erreichung finanzieller Autonomie durch das ECCC sowie die Einrichtung der Kompetenzgemeinschaft für Cybersicherheit und der strategischen Beratungsgruppe betrifft. Dadurch konnten die Kompetenzgemeinschaft für Cybersicherheit und die strategische Beratungsgruppe nicht zur Gestaltung der DIGITAL-Arbeitsprogramme beitragen. Der Rechnungshof betrachtet dies als verpasste Gelegenheit (siehe Ziffern ***77***–***81***).

18 Der Rechnungshof stellte fest, dass mit allen von ihm untersuchten Projekten relevante Ziele verfolgt wurden, die dazu beitragen, die DIGITAL-Cybersicherheitsziele zu erreichen. Der Rechnungshof ermittelte jedoch Fälle, in denen die Qualität oder die erzielten Ergebnisse nicht zufriedenstellend waren. Dies war hauptsächlich auf Verzögerungen bei der Umsetzung zurückzuführen (siehe Ziffern ***82***–***87***).

19 Gemäß der DIGITAL-Verordnung ist vorgesehen, dass die Finanzierung der Cybersicherheit aus Sicherheitsgründen auf Rechtsträger beschränkt werden kann, die ihren Sitz innerhalb der Mitgliedstaaten haben und von Mitgliedstaaten oder Staatsangehörigen der Mitgliedstaaten kontrolliert werden. Der zentrale Validierungsdienst der Europäischen Exekutivagentur für die Forschung führt im Auftrag des ECCC eine entsprechende Bewertung der Eigentums- und Kontrollverhältnisse durch (siehe Ziffern ***88***–***91***).

20 Im Falle der finanziellen Unterstützung Dritter liegt die Verantwortung für die Bewertung der Eigentums- und Kontrollverhältnisse bei den Projektbegünstigten, die diese auf der Grundlage ihres eigenen Ansatzes und ihrer eigenen Methodik vornehmen. Der Rechnungshof stellte fest, dass das ECCC weder die Methodik validiert noch Kontrollen durchführt, um sicherzustellen, dass ausgewählte Dritte ihren Sitz in der EU haben und von Mitgliedstaaten oder EU-Bürgern kontrolliert werden. Nach Auffassung des Rechnungshofs besteht ein erhebliches Risiko, dass die Begünstigten nicht in der Lage sind, diese Kontrollen ordnungsgemäß durchzuführen. Dieses Risiko wurde nicht angemessen gemindert und könnte zur Exposition sensibler Infrastrukturen, operativer Daten und sicherheitskritischer Technologien führen (siehe Ziffern ***92***–***96***).

Empfehlung 4

Eine solide Bewertung der Eigentums- und Kontrollverhältnisse von Rechtsträgern, die EU-Mittel im Rahmen des Programms "Digitales Europa" erhalten, gewährleisten

Das Europäische Kompetenzzentrum für Cybersicherheit sollte

a) hinreichende Sicherheit dafür erlangen, dass Begünstigte, die für die finanzielle Unterstützung Dritter verantwortlich sind, über die erforderlichen administrativen und technischen Kapazitäten verfügen, um auf der Grundlage der Methodik, die diesen Begünstigten bereitgestellt wird, angemessene Bewertungen der Eigentums- und Kontrollverhältnisse durchzuführen;

b) stichprobenartig prüfen, ob nur förderfähige Rechtsträger EU-Mittel erhalten haben.

Zieldatum für die Umsetzung: für den Buchstaben a) bis 2026, für den Buchstaben b) bis 2027.

21 Begünstigte, die EU-finanzierte Projekte verwalten, müssen dem ECCC über ihre Fortschritte und Ergebnisse Bericht erstatten. Dies erfolgt auf der Grundlage von Etappenzielen und zu erbringenden Leistungen, die für die Projektüberwachung von entscheidender Bedeutung sind und angemessen definiert werden sollten. Der Rechnungshof stellte fest, dass bei fast keinem der Projekte in seiner Stichprobe die Anweisungen zur Festlegung von Etappenzielen und zu erbringenden Leistungen befolgt wurden und dass viele von ihnen für die Verfolgung der Fortschritte nicht nützlich waren (siehe Ziffern ***97***–***99***).

22 Der Rechnungshof stellte fest, dass viele der von den Begünstigten verwendeten Leistungsindikatoren nicht relevant oder messbar sind und keine Ziel- oder Ausgangswerte aufweisen. Darüber hinaus war die Berichterstattung über diese Indikatoren unzureichend und kann daher nicht als Grundlage für die Bewertung der Projektleistung dienen (siehe Ziffern ***100***–***102***).

23 Um die Ergebnisse von DIGITAL als Ganzes zu überwachen, müssen für alle Projekte spezifische Programmindikatoren gemeldet werden, die wiederum in die jährlichen Berichte über die Programmleistung der Kommission einfließen. Das ECCC ist für die Erhebung und Überprüfung der Daten zu diesen Indikatoren zuständig. Der Rechnungshof stellte mehrere Probleme bei der Datenerhebung und der Gesamtqualität der Daten fest. Er fand keine Belege dafür, dass die Richtigkeit der gemeldeten Daten vom ECCC überprüft wurde. Auf der Grundlage seiner Stichprobenkontrollen ist der Rechnungshof der Auffassung, dass die gemeldeten Daten die erzielten Ergebnisse nicht genau widerspiegeln (siehe Ziffern ***103***–***106***).

Empfehlung 5

Den Leistungsüberwachungsrahmen der Cybersicherheitskomponente des Programms "Digitales Europa" stärken

Um eine angemessene Überwachung von Fortschritt und Leistung zu ermöglichen, sollte das Europäische Kompetenzzentrum für Cybersicherheit

a) vor der Unterzeichnung der Finanzhilfevereinbarung sicherstellen, dass für alle Projekte Etappenziele, zu erbringende Leistungen und Leistungsindikatoren festgelegt wurden, die den Anweisungen im Antragsformular entsprechen;

b) ein robustes System zur Erhebung, Rückverfolgbarkeit, Überprüfung und Aggregation der Daten für die Leistungsindikatoren der Cybersicherheitskomponente des Programms "Digitales Europa" konzipieren und einführen, um sicherzustellen, dass die Indikatoren die erzielten Ergebnisse genau widerspiegeln.

Zieldatum für die Umsetzung: 2027

02

Die Bemerkungen des Rechnungshofs näher betrachtet

Die Cybersicherheitsnetzwerke und -mechanismen der EU tragen zwar dazu bei, die Zusammenarbeit und Reaktion zu unterstützen, doch aufgrund des begrenzten Informationsaustauschs und einer unvollständigen Umsetzung ist die Wirksamkeit vermindert

EU-Netzwerke ermöglichen die Zusammenarbeit der Mitgliedstaaten, doch ihr Mehrwert ist aufgrund des begrenzten Informationsaustauschs eingeschränkt

24 Der derzeitige EU-Rahmen für Netzwerke und Mechanismen, welche die Erkennung und Bewältigung erheblicher Cybersicherheitsvorfälle erleichtern sollen, wurde schrittweise eingerichtet. Zunächst wurde hierfür die Richtlinie über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union[3] (NIS-Richtlinie) verabschiedet, die im August 2016 in Kraft trat. Die aktuelle Cybersicherheitslandschaft der EU wird in ***Anhang II*** veranschaulicht.

[3] Richtlinie (EU) 2016/1148.

EU-Netzwerke ermöglichen die Zusammenarbeit der Mitgliedstaaten auf technischer und operativer Ebene

25 Mit der NIS-Richtlinie wurde das CSIRTs-Netzwerk eingerichtet, in dem das CERT-EU (der Cybersicherheitsdienst für die Organe, Einrichtungen und sonstigen Stellen der Union) und die von den Mitgliedstaaten benannten CSIRTs zusammenkommen. Ziel dieses Netzwerks ist es, Vertrauen zwischen den nationalen CSIRTs aufzubauen und eine rasche und wirksame operative Zusammenarbeit zwischen den Mitgliedstaaten zu fördern.

26 Das EU-CyCLONe wurde 2020 als informelles Kooperationsnetzwerk für die nationalen Behörden eingerichtet, die für das Cyberkrisenmanagement zuständig sind. Es dient als Brücke zwischen der technischen Ebene, auf der das CSIRTs-Netzwerk tätig ist, und der politischen Ebene des Rates der Europäischen Union und seiner Integrierten Regelung für die politische Reaktion auf Krisen. Mit dem Inkrafttreten der NIS-2-Richtlinie im Jahr 2023 wurde die Rolle des EU-CyCLONe formell festgelegt und ihm ein klares Mandat erteilt.

27 Der Rechnungshof bewertete, ob die Aufgaben und Zuständigkeiten dieser Netzwerke auf EU-Ebene klar definiert sind und ob sie eine Zusammenarbeit zwischen den Mitgliedstaaten ermöglichen.

28 Die ENISA fungiert als Sekretariat des CSIRTs-Netzwerks und des EU-CyCLONe und stellt ihnen die Ressourcen, das Fachwissen, die Infrastruktur und die IT-Instrumente zur Verfügung, die für die Zusammenarbeit und sichere Kommunikation zum Informationsaustausch erforderlich sind. In ihrer Zufriedenheitsumfrage[4] unter Interessenträgern von Anfang 2025 erzielte die ENISA gute Ergebnisse für ihre Leistung als Sekretariat dieser Netzwerke. Diese positiven Rückmeldungen wurden auch bei den Prüfbesuchen des Rechnungshofs bestätigt, bei denen die nationalen Cybersicherheitsbehörden ihre Wertschätzung zum Ausdruck brachten.

[4] Konsolidierter jährlicher Tätigkeitsbericht 2024 der ENISA, S. 33 und 36.

29 Im Jahr 2025 nahm der Rat den Cyber-Konzeptentwurf an, in dem die Aufgaben und Zuständigkeiten der wichtigsten Akteure (einschließlich des CSIRTs-Netzwerks und des EU-CyCLONe) und die Mechanismen festgelegt sind, die bei Cybersicherheitsvorfällen großen Ausmaßes oder Cyberkrisen zum Tragen kommen. Der Rechnungshof stellte fest, dass der Cyber-Konzeptentwurf die Aufgaben und Zuständigkeiten in Bezug auf das Cyberkrisenmanagement der EU weitgehend klarstellt und den Veränderungen, denen die Cybersicherheitslandschaft seit dem ersten Konzeptentwurf im Jahr 2017 unterworfen war, Rechnung trägt. In dem Konzeptentwurf werden drei Ebenen der Zusammenarbeit definiert: die technische, die operative und die politische Ebene. Zudem werden die seit 2017 eingerichteten neuen Netzwerke und Strukturen – wie das EU-CyCLONe, die EU-Teams für die rasche Reaktion auf hybride Bedrohungen und das europäische Warnsystem für Cybersicherheit – im Einzelnen beschrieben, und es wird dargelegt, wie das Cyberkrisenmanagement in den umfassenderen Krisenreaktionsrahmen der EU integriert werden sollte.

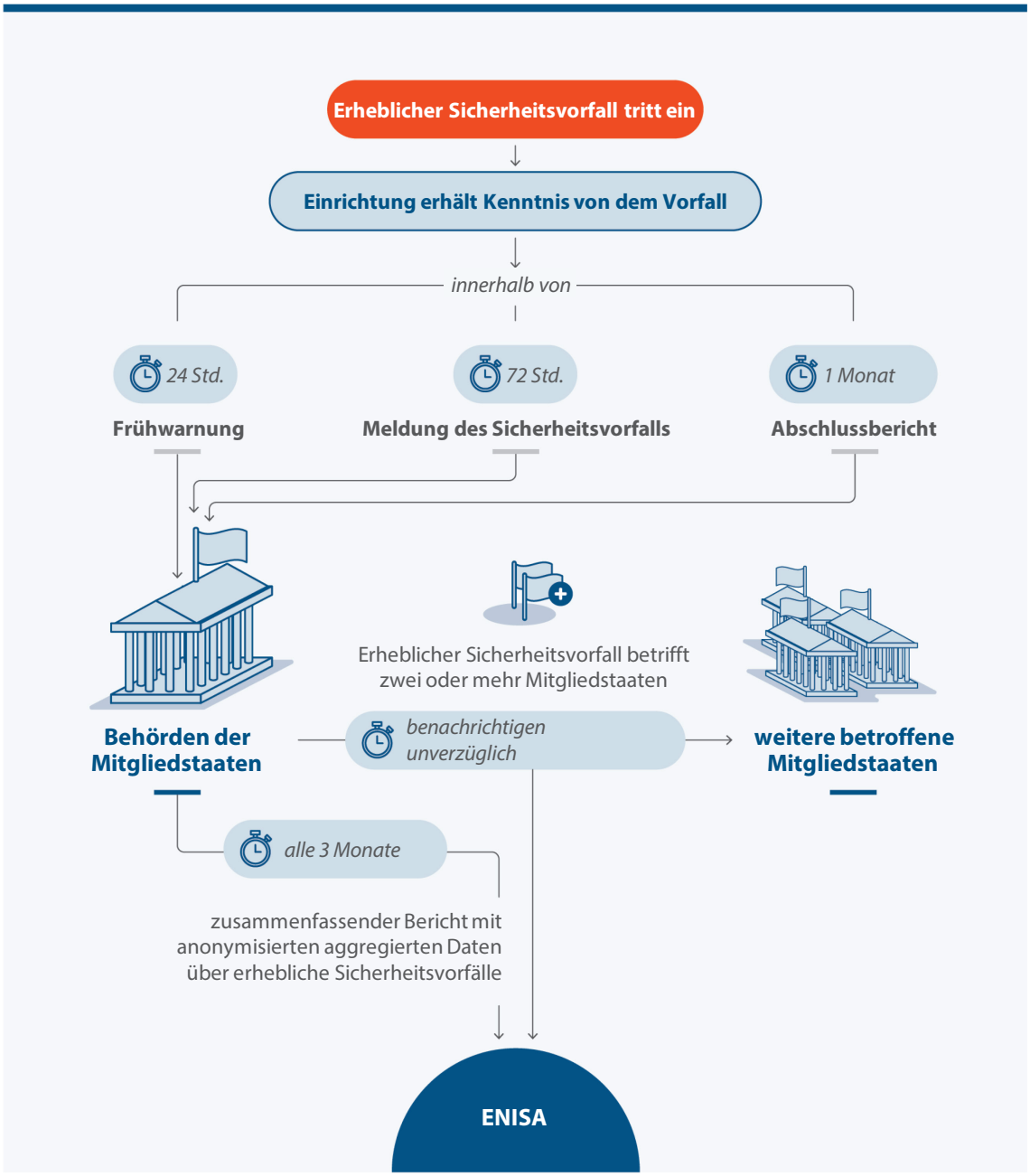
30 Trotz der offiziellen Einrichtung des CSIRTs-Netzwerks im Jahr 2016 und des EU-CyCLONe im Jahr 2023 müssen die Verfahrensregelungen für die Zusammenarbeit der beiden Netzwerke jedoch noch formell festgelegt werden. Ferner wurden bisher noch keine Kriterien vereinbart, nach denen das EU-CyCLONe von dem CSIRTs-Netzwerk darüber informiert werden soll, dass ein beobachteter Cybersicherheitsvorfall einen potenziellen oder andauernden Cybersicherheitsvorfall großen Ausmaßes darstellt. Die beiden Netzwerke müssen sich auch auf eine gemeinsame Taxonomie der Schweregrade von Sicherheitsvorfällen und der Schlüsselbegriffe – wie "Bedrohung", "Bedrohungsakteur", "Vorfall" oder "Auswirkungen" – einigen. Das ist erforderlich, um einen automatisierten Informationsaustausch zu ermöglichen. Derzeit gibt es Interpretationsspielraum hinsichtlich der Frage, wann ein Sicherheitsvorfall als erheblich oder von großem Ausmaß einzustufen ist. Die Sicherheitsbehörden von allen drei Mitgliedstaaten, die der Rechnungshof besuchte, erwähnten, dass eine gemeinsame Taxonomie fehle.

Begrenzter Informationsaustausch und begrenzte Berichterstattung verringern den Mehrwert dieser Netzwerke erheblich

31 Das Eintreten und die Ausbreitung von Cybersicherheitsvorfällen und Cyberangriffen wird durch geografische Grenzen nicht verhindert. Der Informationsaustausch zwischen den Mitgliedstaaten, z. B. über die Taktiken und Techniken, die von den Bedrohungsakteuren eingesetzt werden, und über digitale Anzeichen für die Verletzung eines Netz- oder Informationssystems ("Kompromittierungsindikatoren"), kann erheblich zur Erhöhung der Cybersicherheit beitragen.

32 Der Rechnungshof stellte fest, dass der Informationsaustausch begrenzt war, was den Mehrwert dieser Netzwerke erheblich verringert. Die vom Rechnungshof festgestellten Einschränkungen betreffen hauptsächlich Verzögerungen bei der Umsetzung der NIS-2-Richtlinie, Probleme bei der Feststellung, ob ein Sicherheitsvorfall grenzübergreifende Auswirkungen hat, Rechtsvorschriften über die nationale Sicherheit, die den Informationsaustausch einschränken, und mangelndes Vertrauen. Mit der NIS-2-Richtlinie werden mehrere Berichtspflichten für Einrichtungen, die in den Anwendungsbereich der Richtlinie fallen, und für Behörden der Mitgliedstaaten eingeführt (siehe ***Abbildung 2***).

Abbildung 2 | Zeitrahmen für die Meldung von Sicherheitsvorfällen gemäß der Richtlinie über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der EU (NIS-2-Richtlinie)



Quelle: Europäischer Rechnungshof auf der Grundlage von Daten der ENISA.

33 Die Mitgliedstaaten hatten bis Oktober 2024 Zeit für die Umsetzung der NIS-2-Richtlinie in nationales Recht, aber nur zwei Mitgliedstaaten hielten die Frist ein. Verzögerungen bei der Umsetzung haben erhebliche Auswirkungen auf den Informationsaustausch, da die unter die NIS-2-Richtlinie fallenden Einrichtungen in der Zwischenzeit rechtlich nicht dazu verpflichtet sind, Sicherheitsvorfälle zu melden. Nach Schätzungen der Kommission[5] fielen 15 500 Einrichtungen unter die NIS-Richtlinie, während mehr als 110 000 Einrichtungen in den Anwendungsbereich der NIS-2-Richtlinie fallen. So war beispielsweise die öffentliche Verwaltung – laut dem ENISA-Bericht zur Bedrohungslage 2025 der am stärksten betroffene Sektor in der EU – gemäß der NIS-Richtlinie nicht verpflichtet, Sicherheitsvorfälle zu melden.

34 Dadurch, dass Daten über Sicherheitsvorfälle alle drei Monate an die ENISA gemeldet werden (d. h. lange nach einem Sicherheitsvorfall) ist ihr Mehrwert begrenzt. Diese Daten dienen hauptsächlich statistischen Zwecken und der Meldung historischer Trends, nicht aber der Verbesserung der Erkennung und Reaktion. Die ENISA stellt den Mitgliedstaaten ein Online-Tool für die Übermittlung ihrer Berichte zur Verfügung. Die Vorlage für Meldungen enthält einen Mindestdatensatz, der bereitgestellt werden muss, z. B. die Art des Vorfalls und der betroffene Sektor. Darüber hinaus empfiehlt die ENISA den Mitgliedstaaten, zusätzliche Informationen bereitzustellen, um eine eingehendere Analyse der Daten zu ermöglichen, z. B. durch die Herstellung einer Verbindung zwischen Sicherheitsvorfällen und bestimmten Schwachstellen. Allerdings stellen nicht alle Mitgliedstaaten diese Informationen bereit, wodurch die Qualität und der Mehrwert der erhobenen Daten erheblich verringert werden.

35 Die ENISA stellte in ihrem Bericht über den Stand der Cybersicherheit in der Union 2024 fest, dass Sicherheitsvorfälle vermutlich unzureichend gemeldet werden, da die Anzahl der gemeldeten Vorfälle gering zu sein scheint. In den Jahren 2018 bis 2021 meldeten die Mitgliedstaaten der ENISA jährlich zwischen 100 und 500 Vorfälle. Die Anzahl der Vorfälle nahm schrittweise zu und stieg 2024 auf 1 276[6].

---

[5] Europäische Kommission, Folgenabschätzung aus dem Jahr 2020.

[6] CIRAS-Daten für 2024.

36 In ihrem Bericht zur Bedrohungslage 2025, der den Zeitraum von Juni 2024 bis Juni 2025 abdeckt, wies die ENISA auf rund 4 800 Cybersicherheitsvorfälle hin[7], die sie durch Informationsgewinnung aus frei zugänglichen Quellen wie z. B. Nachrichtenartikeln ermittelt hatte. Diese Sicherheitsvorfälle wären gemäß der NIS-2-Richtlinie nicht alle meldepflichtig gewesen, die ENISA deckt jedoch bei der Datenerhebung ein breiteres Spektrum von Sicherheitsvorfällen ab. Umgekehrt werden viele erhebliche Vorfälle nicht in frei zugänglichen Quellen gemeldet. Da die von den Mitgliedstaaten gemeldeten Daten anonymisiert sind, kann die ENISA die von ihr ermittelten Sicherheitsvorfälle nicht mit den von den Mitgliedstaaten gemeldeten Sicherheitsvorfällen in Verbindung bringen. Es ist daher nicht möglich, genau zu bestimmen, inwieweit zu wenige Vorfälle gemeldet werden. Nach Auffassung des Rechnungshofs deutet die Differenz zwischen der Anzahl der von den Mitgliedstaaten gemeldeten Vorfälle und der im Bericht zur Bedrohungslage gemeldeten Vorfälle jedoch darauf hin, dass nicht alle erheblichen Vorfälle gemeldet werden.

37 Auch die Anzahl der Meldungen zu erheblichen grenzübergreifenden Sicherheitsvorfällen, die an andere betroffene Mitgliedstaaten und die ENISA übermittelt werden, weist auf unzureichende Meldungen hin. Eine ähnliche Meldepflicht bestand im Rahmen der NIS-Richtlinie, wurde jedoch als unwirksam erachtet, da die Kommission im Jahr 2020 zu dem Schluss kam[8], dass trotz dieser Pflicht nur selten Meldungen übermittelt wurden. Sie führte die nicht erfolgten Meldungen darauf zurück, dass es keine klaren Modalitäten für den Informationsaustausch und keine gemeinsamen Ziele gebe, die Anreize für den Austausch schaffen würden.

38 Die Pflicht zur Unterrichtung anderer Mitgliedstaaten ist von entscheidender Bedeutung, um eine Ausbreitung von Sicherheitsvorfällen zu verhindern. Fehlende Meldungen wirken sich negativ auf die Cybersicherheit der EU aus. Im Jahr 2025 wurden nur 14 erhebliche grenzübergreifende Vorfälle von sieben Mitgliedstaaten gemeldet. Die Mitgliedstaaten meldeten im Jahr 2024 zwei Sicherheitsvorfälle, im Jahr 2023 keine und im Jahr 2022 drei mit möglichen grenzübergreifenden Auswirkungen. Dies zeigt, dass nur sehr wenige erhebliche grenzübergreifende Vorfälle gemeldet werden und die Meldungen das tatsächliche Ausmaß solcher Angriffe nicht widerspiegeln. Zur besseren Einordnung: In ihrem Bericht zur Bedrohungslage für das Jahr 2024 ermittelte die ENISA 322 Vorfälle, die sich speziell gegen zwei oder mehr Mitgliedstaaten richteten. Der Cybersicherheitsvorfall bei *Collins Aerospace* (siehe ***Kasten 1***) ist ein Beispiel dafür, dass Mitgliedstaaten einen Vorfall nicht melden, obwohl er erhebliche grenzübergreifende Auswirkungen hat.

---

[7] Bericht der ENISA zur Bedrohungslage für das Jahr 2025.

[8] Europäische Kommission, Folgenabschätzung aus dem Jahr 2020.

Kasten 1

Ein Cybersicherheitsvorfall, der den Flughafenbetrieb störte

Im September 2025 erlitt Collins Aerospace, ein wichtiger Technologieanbieter für die Luftfahrtindustrie, einen schwerwiegenden Ransomware-Angriff auf seine Software zur Passagierabfertigung. Der Angriff zwang mehrere große europäische Flughäfen, wieder manuell zu arbeiten, was zu zahlreichen Verspätungen und Flugausfällen führte. Am stärksten betroffen waren die Flughäfen London-Heathrow, Brüssel, Berlin-Brandenburg und Dublin.

Gemäß der NIS-2-Richtlinie gilt ein Sicherheitsvorfall als "erheblich", wenn er u. a. schwerwiegende Betriebsstörungen der Dienste oder finanzielle Verluste für die betreffende Einrichtung verursacht. Dieser Vorfall wurde jedoch von keinem Mitgliedstaat wie ein erheblicher grenzübergreifender Sicherheitsvorfall oder wie ein grenzübergreifender Sicherheitsvorfall großen Ausmaßes behandelt. Daher unterrichtete keiner der betroffenen Mitgliedstaaten die ENISA oder andere Mitgliedstaaten förmlich über den Vorfall. Das CSIRTs-Netzwerk wiederum informierte das EU-CyCLONe nicht, sodass dieses nicht zu einem koordinierten Management des Cybersicherheitsvorfalls beitragen konnte.

Quelle: Analyse des Rechnungshofs auf der Grundlage von Befragungen von Vertretern der ENISA.

39 Ein weiterer Grund für die begrenzte Meldung grenzübergreifender Sicherheitsvorfälle besteht darin, dass es Sache der einzelnen Behörden der Mitgliedstaaten ist, festzustellen, ob ein gemeldeter Sicherheitsvorfall grenzübergreifende Auswirkungen hat und welche Mitgliedstaaten betroffen sind. Auf der Grundlage der verfügbaren Informationen ist der meldenden Einrichtung oder der mitgliedstaatlichen Behörde bei einigen Angriffen möglicherweise nicht bewusst, dass diese grenzübergreifenden Charakter haben. Derzeit gibt es keine EU-weite Plattform, der in Echtzeit Meldungen zu Sicherheitsvorfällen aus allen Mitgliedstaaten übermittelt werden und die Informationen über Sektoren oder Kompromittierungsindikatoren miteinander in Verbindung bringen könnte, um grenzübergreifende Sicherheitsvorfälle aufzudecken. Daher besteht ein erhebliches Risiko, dass einige grenzübergreifende Sicherheitsvorfälle möglicherweise nicht als solche identifiziert und gemeldet werden.

40 Seit 2016 wurde kein Cybersicherheitsvorfall von einem Mitgliedstaat als "von großem Ausmaß" eingestuft. Grundsätzlich fällt jeder Vorfall, der beträchtliche Auswirkungen auf mindestens zwei Mitgliedstaaten hat, unter diese Definition. Allerdings wurden selbst Cybersicherheitsvorfälle, die zu globalen Ausfällen und erheblichen Schäden geführt haben (siehe ***Abbildung 3***), nicht als Sicherheitsvorfälle großen Ausmaßes eingestuft. Infolgedessen fand das Eskalationsverfahren des EU-CyCLONe nie vollständig Anwendung auf einen Cybersicherheitsvorfall großen Ausmaßes.

Abbildung 3 | Beispiele für schwerwiegende Cybersicherheitsvorfälle

WannaCry

2017

Weltweiter Ransomware-Angriff

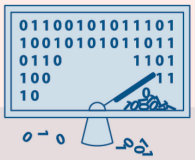
Betraf mehr als 200 000 Computer in über 150 Ländern und führte zur Lahmlegung von Betreibern kritischer Infrastruktur, zur Verschlüsselung von Daten auf infizierten Geräten und zu Forderungen von Lösegeld für die Entschlüsselung der Daten

NotPetya

2017

Zerstörerische Schadsoftware, als Ransomware getarnt

So konzipiert, dass Daten dauerhaft gelöscht wurden, und in erster Linie gegen die Ukraine gerichtet. Breitete sich rasch weltweit aus, legte multinationale Unternehmen lahm und verursachte globale Schäden.



IT-Ausfall im Zusammenhang mit *CrowdStrike*

Juli 2024

Weltweiter massiver IT-Ausfall

Durch eine fehlerhafte Softwareaktualisierung des Cybersicherheitsunternehmens CrowdStrike verursacht, die zum Absturz von Millionen von Computern führte

Quelle: Europäischer Rechnungshof auf der Grundlage von Informationen von Cloudflare, ENISA, Europol, Wired, IBM, CrowdStrike.

41 Zusätzlich zu der Meldepflicht für Einrichtungen und Mitgliedstaaten wurde das CSIRTs-Netzwerk geschaffen, um den Informationsaustausch zu erleichtern. Vertrauen zwischen den Mitgliedstaaten steht im Mittelpunkt des CSIRTs-Netzwerks, in dem Informationen auf freiwilliger Basis ausgetauscht werden. Der Mehrwert des Netzwerks ist erheblich geringer, wenn die Mitgliedstaaten nicht bereit sind, zeitnahe und verwertbare Informationen auszutauschen.

42 Der Informationsaustausch auf EU-Ebene wird durch die Rechtsvorschriften der einzelnen Mitgliedstaaten im Bereich der nationalen Sicherheit eingeschränkt. Ist ein Mitgliedstaat der Auffassung, dass Informationen zu Cyberangriffen auf kritische Einrichtungen als Verschlusssache einzustufen sind oder dass die Meldung eines bestimmten Sicherheitsvorfalls seiner nationalen Sicherheit schaden würde, so ist er nicht verpflichtet, diese Informationen weiterzugeben. Während der Besuche des Rechnungshofs in den Mitgliedstaaten erklärten Vertreter des CSIRTs-Netzwerks und des EU-CyCLONe, dass ein Austausch nur innerhalb der im Bereich der nationalen Sicherheit bestehenden gesetzlichen Grenzen erfolgen kann. Eine Analyse der nationalen Rechtsrahmen der Mitgliedstaaten und ihrer Auswirkungen auf den Informationsaustausch wurde auf EU-Ebene nicht durchgeführt.

43 Im Jahr 2016 bestand das CSIRTs-Netzwerk aus 28 nationalen CSIRTs mit je zwei Vertretern pro Mitgliedstaat. Der mangelnde Informationsaustausch ist ein anhaltendes Problem, und in der von der Kommission durchgeführten Evaluierung der NIS-Richtlinie wurde angemerkt, dass die Mitgliedstaaten Informationen nicht systematisch untereinander austauschen, was sich insbesondere auf die Wirksamkeit der Cybersicherheitsmaßnahmen und die gemeinsame Lageerfassung auf EU-Ebene auswirkt. Im Einklang mit der NIS-2-Richtlinie haben viele Mitgliedstaaten zusätzlich zu ihren nationalen CSIRTs ebenfalls sektorbezogene CSIRTs benannt, sodass das Netzwerk erheblich ausgeweitet wurde. Zum Zeitpunkt der Prüfung umfasste es 42 CSIRTs und mehr als 700 Einzelteilnehmer. Vertrauen aufzubauen wird dadurch zusätzlich erschwert, da es herausfordernd ist, enge Verbindungen zwischen allen Mitgliedern aufrechtzuerhalten.

44 Das CSIRTs-Netzwerk ist sich des Problems des Informationsaustauschs bewusst und erwägt verschiedene Maßnahmen, um das Vertrauen innerhalb des wachsenden Netzwerks zu stärken. Die Schaffung kleinerer Gruppen von Mitgliedstaaten, die grenzübergreifende Hubs bilden (siehe Ziffern ***62***–***74***), ist ein alternativer Ansatz zu einem EU-weiten Netzwerk, der dazu beitragen kann, diese Herausforderung zu bewältigen.

Die für das Cyber-Lagezentrum in Auftrag gegebenen Dienstleistungen überschneiden sich teilweise mit bestehenden Kapazitäten, und die künftige Funktionsweise des Zentrums ist unklar

45 Gemäß der NIS-2-Richtlinie wird die Kommission in Fällen, in denen ein potenzieller oder andauernder Cybersicherheitsvorfall großen Ausmaßes erhebliche Auswirkungen hat oder wahrscheinlich haben wird, Mitglied des EU-CyCLONe[9]. Aufgrund dieser neuen Rolle und der Entwicklung der Bedrohungslage richtete die Kommission im Jahr 2022 eine Taskforce zur Cyber-Koordinierung innerhalb der GD Connect ein. Diese Taskforce umfasst ein Cyber-Lagezentrum, das der Kommission dabei helfen soll, ihr Lagebewusstsein zu verbessern, um sie bei der Erfüllung ihrer institutionellen Aufgaben im Bereich des Krisenmanagements zu unterstützen. Außerdem soll es der GD Connect dabei helfen, Beratung auf politischer Ebene zu leisten.

46 Bei der Organisation des Cyber-Lagezentrums wird die Kommission weitgehend von externen Dienstleistern unterstützt, die im Dezember 2022 einen Auftrag im Wert von fast 18 Millionen Euro über einen Zeitraum von vier Jahren erhalten haben. Der Rechnungshof bewertete die Einrichtung des Zentrums, seine Outputs und die Pläne der Kommission für seine künftige Funktionsweise.

---

[9] Artikel 16 Absatz 2 der NIS-2-Richtlinie.

47 Als Teil der erbrachten Dienste haben die Auftragnehmer ein Dashboard eingerichtet, das sich auf kommerzielle Erkenntnisse über Cyberbedrohungen stützt und mit dem Informationen über Bedrohungen dargestellt und ausgetauscht werden können. Darüber hinaus werden verschiedene Berichte über Cyberbedrohungen erstellt, darunter tägliche und wöchentliche Berichte sowie thematische Berichte zu Ländern oder Wirtschaftszweigen. Das physische Cyber-Lagezentrum wurde in einem der Gebäude der Kommission eingerichtet. Es besteht aus einem Raum, der mit Arbeitsplätzen ausgestattet ist, die mit dem von den Auftragnehmern betriebenen Dashboard per Fernzugriff verbunden sind. Zum Zeitpunkt der Prüfung war eine kleine Anzahl von Kommissionsbediensteten im Cyber-Lagezentrum tätig, die von vielen Analysten der Auftragnehmer sowie von Sachverständigen der ENISA unterstützt wurden.

48 Der Rechnungshof stellte fest, dass sich die von den externen Dienstleistern für das Cyber-Lagezentrum geleistete Arbeit teilweise mit den bestehenden Kapazitäten der ENISA überschneidet. Die ENISA verfügt über ständige Kapazitäten für die Lageerfassung und die Überwachung von Cyberbedrohungen. Sie veröffentlicht regelmäßig Berichte über Cyberbedrohungen, darunter Kurzberichte zu bestimmten Vorfällen und wöchentliche Berichte mit einem Überblick über die Bedrohungen. Die Berichte beruhen auf frei zugänglichen Informationen und ähneln den von den Auftragnehmern erstellten Berichten. Darüber hinaus erstellt die ENISA Kurzinformationen auf hoher Ebene für politische Entscheidungsträger in Krisenzeiten oder trägt zur Erstellung solcher Kurzinformationen bei, die ebenfalls mit den vom Cyber-Lagezentrum verfassten Berichten vergleichbar sind.

49 Des Weiteren beruhen die Daten, die der Erstellung dieser Berichte des Cyber-Lagezentrums zugrunde liegen, auf kommerziellen Erkenntnissen über Cyberbedrohungen und ähneln den Daten, die von anderen Kommissionsdienststellen wie der Generaldirektion Digitale Dienste und dem CERT-EU verwendet werden. Der Rechnungshof ist der Auffassung, dass bei der Einrichtung des Cyber-Lagezentrums das Rationalisierungspotenzial, dass die Nutzung bereits verfügbarer Informationen der Kommission und der ENISA geboten hätte, nicht zur Genüge ausgeschöpft wurde.

50 Der Vertrag läuft im Dezember 2026 aus. Danach werden die Auftragnehmer keine Dienste mehr für das Cyber-Lagezentrum erbringen. Diese Dienste umfassen die Bereitstellung der im Dashboard verfügbaren Daten sowie die Erstellung von Berichten über Cyberbedrohungen und machen einen Großteil der Dienste des Zentrums aus. Das Dashboard wird der Kommission übergeben werden, verliert jedoch seinen Mehrwert, wenn es nicht kontinuierlich mit Erkenntnissen über Cyberbedrohungen aktualisiert wird.

51 Zum Zeitpunkt der Prüfung hatte die Kommission keine Pläne für eine Unterstützung des Betriebs des Cyber-Lagezentrums durch externe Dienstleister nach Ablauf des Vertrags. Nach Auffassung des Rechnungshofs stellt das Fehlen eines umfassenden und detaillierten Plans, der die Zeit nach Ablauf des Vertrags abdeckt, ein Risiko für den Betrieb des Cyber-Lagezentrums nach 2026 dar.

Die EU-Cybersicherheitsreserve ermöglicht den raschen Einsatz von Sicherheitsvorfall-Notdiensten

52 Im Jahr 2022 stellte die Kommission unmittelbar nach der militärischen Aggression Russlands gegen die Ukraine und in Anerkennung der Tatsache, dass groß angelegte Cyberangriffe zugenommen haben, der ENISA außerordentliche Mittel in Höhe von 15 Millionen Euro für die Durchführung der Aktion zur Förderung der Cybersicherheit zur Verfügung. Dieses Pilotprojekt wurde 2023 auf den Weg gebracht. Im Jahr 2023 stellte die Kommission zusätzliche Mittel (etwa 20 Millionen Euro) bereit, um das Programm bis Ende 2026 zu verlängern.

53 Die Kommission hat auch die im Dezember 2024 angenommene Cybersolidaritätsverordnung vorgeschlagen, um Vorbereitungen für Cybersicherheitsvorfälle großen Ausmaßes zu treffen. Mit dem Rechtsakt wurde eine EU-Cybersicherheitsreserve eingerichtet, die Sicherheitsvorfall-Notdienste vertrauenswürdiger Anbieter umfasst. Die Reserve wurde im Jahr 2025 schrittweise in Betrieb genommen und für den Zeitraum 2025–2027 mit einem Budget von 36 Millionen Euro ausgestattet.

54 Der Rechnungshof bewertete die Organisation des Aktionsprogramms zur Förderung der Cybersicherheit, da es die Grundlage für die EU-Cybersicherheitsreserve bildet. Er prüfte auch, ob die seit 2022 gewonnenen Erkenntnisse in die Gestaltung der EU-Cybersicherheitsreserve eingeflossen sind.

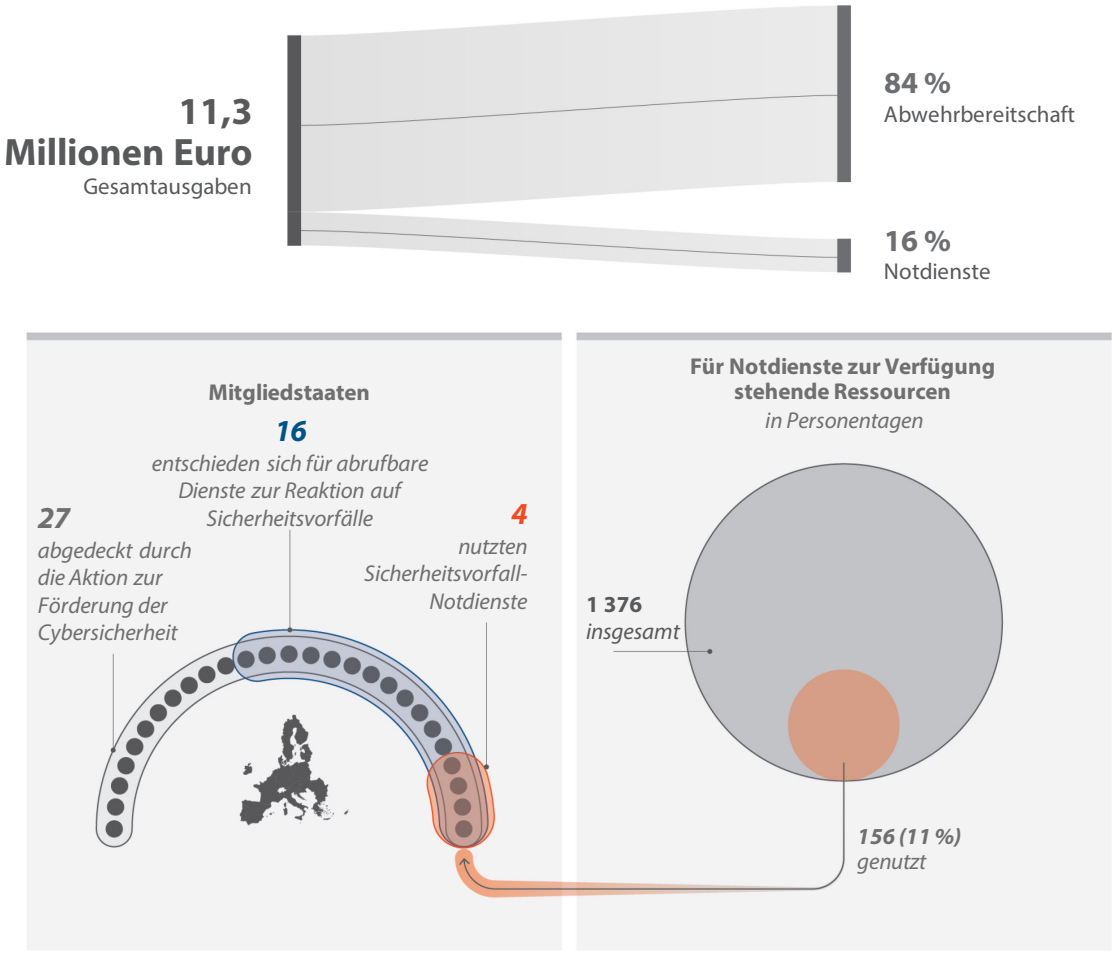
55 Die ENISA konzipierte die Aktion zur Förderung der Cybersicherheit als Mechanismus zur Bereitstellung von Diensten, mit denen die Abwehrbereitschaft und die Reaktion der Mitgliedstaaten in Bezug auf Cybersicherheitsvorfälle oder -krisen großen Ausmaßes unterstützt werden sollen. Für alle Dienste schließt die ENISA Vorverträge ab. Das bedeutet, dass die Dienstleister ihre Arbeit aufnehmen können, sobald die Mitgliedstaaten sie darum bitten. Dies trägt auch dem Umstand Rechnung, dass die ENISA so organisiert ist, dass rund um die Uhr ein Mitarbeiter in Rufbereitschaft zur Verfügung steht, der die Anfragen der Mitgliedstaaten bearbeitet.

56 Die ENISA hat sich dafür entschieden, die verfügbaren Mittel gleichmäßig auf die Mitgliedstaaten aufzuteilen. In der Praxis leitete die Agentur ein offenes Ausschreibungsverfahren ein, das in 27 Lose unterteilt war, eines pro Mitgliedstaat, um bis zu drei private Sicherheitsanbieter auszuwählen, die bis Ende 2026 Dienstleistungen erbringen sollen. Darüber hinaus wählte die ENISA einige Anbieter im Rahmen eines gesamteuropäischen Loses aus, um Dienste für dafür infrage kommende Nicht-EU-Länder sowie für Organe, Einrichtungen und Agenturen der EU zu erbringen oder die Reaktion auf grenzübergreifende Sicherheitsvorfälle zu unterstützen.

57 Dieser Ansatz ermöglichte es der ENISA, spezifische nationale Anforderungen, einschließlich Anforderungen bezüglich der Sprache, nationaler Sicherheitsüberprüfungen oder einer etablierten Präsenz in den Mitgliedstaaten, zu berücksichtigen. Da die Anbieter jedoch nicht so ausgewählt wurden, dass sie Dienstleistungen in der gesamten EU erbringen können, besteht ein großer Nachteil dieses Ansatzes darin, dass die Mittel, die für die Erbringung solcher Dienstleistungen in einem bestimmten Mitgliedstaat gebunden sind, nicht zur Unterstützung eines anderen Mitgliedstaats verwendet werden können, wenn ein Mitgliedstaat die Dienste, über die Vorverträge geschlossen wurden, nicht in Anspruch nimmt.

58 Bei der Aktion zur Förderung der Cybersicherheit konnten die Mitgliedstaaten zwischen Diensten im Bereich der Abwehrbereitschaft und Diensten im Bereich der Reaktion und einer Kombination aus beidem wählen. Die Mitgliedstaaten entschieden sich in erster Linie dafür, die verfügbaren Mittel zur Verbesserung ihrer Abwehrbereitschaft zu nutzen (84 % der Ausgaben im Jahr 2023). Mitgliedstaaten, die sich für abrufbare Dienste im Bereich der Reaktion auf Sicherheitsvorfälle entschieden haben (d. h. vorab eine Vereinbarung mit einem Anbieter geschlossen haben, die sicherstellt, dass der Mitgliedstaat die Dienstleistungen des Anbieters bei Bedarf in Anspruch nehmen kann, um eine rasche Reaktion auf Cybersicherheitsvorfälle zu gewährleisten), nahmen diese Kapazitäten nur wenig in Anspruch (siehe ***Abbildung 4***). In den drei besuchten Mitgliedstaaten äußerten sich die Behörden positiv darüber, wie die ENISA die Aktion zur Förderung der Cybersicherheit verwaltete.

Abbildung 4 | Aktion der ENISA zur Förderung der Cybersicherheit bis 2023



Quelle: Europäischer Rechnungshof auf der Grundlage von Daten der ENISA.

59 Für den Zeitraum 2024–2026 beantragten nur neun Mitgliedstaaten die abrufbare Dienste im Bereich der Reaktion auf Sicherheitsvorfälle. In Gesprächen, die der Rechnungshof mit der ENISA und Behörden in drei Mitgliedstaaten führte, wurde bestätigt, dass Maßnahmen in Bezug auf die Abwehrbereitschaft stark bevorzugt werden.

60 Die EU-Cybersicherheitsreserve dient zwar in erster Linie der Unterstützung der Reaktion auf schwerwiegende Sicherheitsvorfälle und der anschließenden Wiederherstellung, jedoch können vorab zugesagte Dienste aus der EU-Cybersicherheitsreserve, die nicht für die Reaktion auf Sicherheitsvorfälle in Anspruch genommen werden, in Dienste in Bezug auf die Abwehrbereitschaft umgewandelt werden. Dieser flexible Ansatz kann verhindern, dass im Voraus bezahlte Dienste ungenutzt bleiben.

61 Nach Auffassung des Rechnungshofs beruht das für die EU-Cybersicherheitsreserve gewählte Modell auf den Erkenntnissen aus dem Aktionsprogramm zur Förderung der Cybersicherheit. Die Daten, die in Bezug auf die Nutzung des Aktionsprogramms zur Förderung der Cybersicherheit vorliegen, deuten jedoch auf das Risiko hin, dass die EU-Cybersicherheitsreserve – entgegen dem in der Cybersolidaritätsverordnung festgelegten Zweck – in erster Linie für die Abwehrbereitschaft und nicht für die Reaktion genutzt werden könnte.

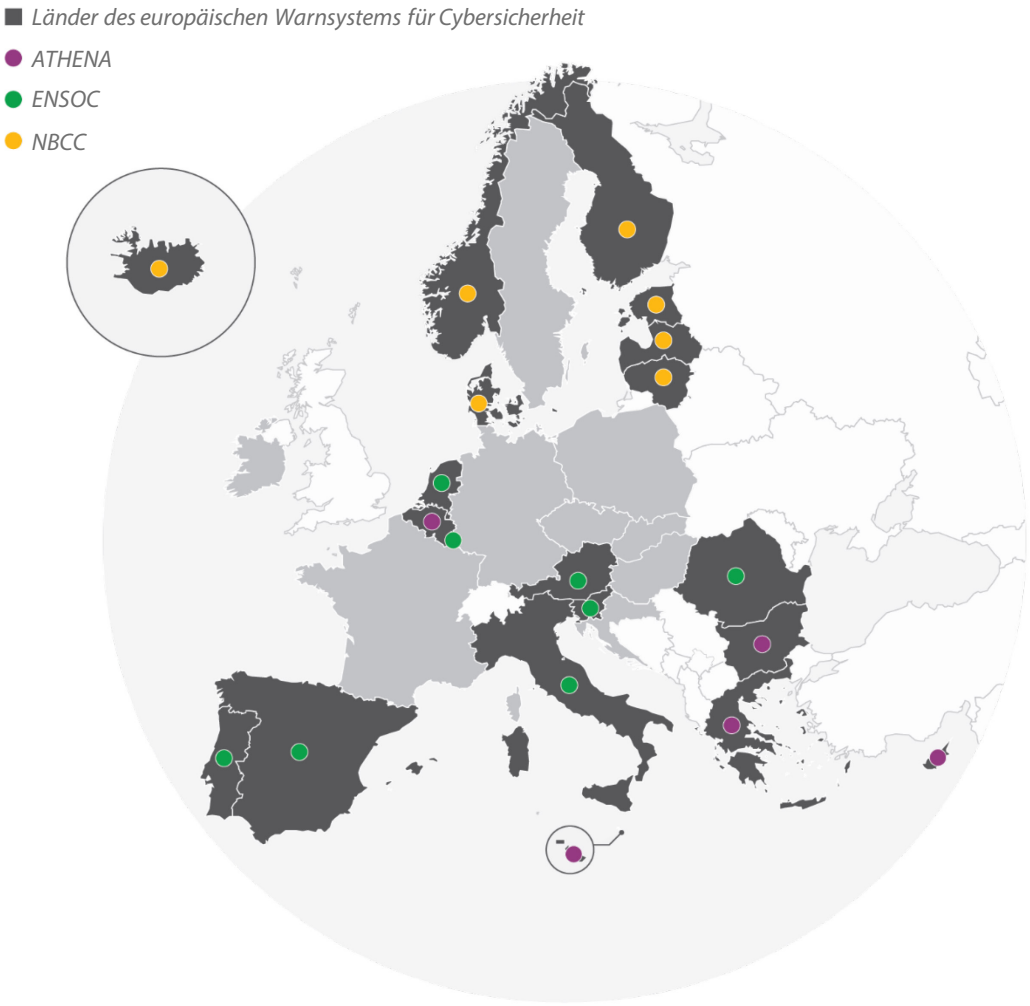
Das europäische Warnsystem für Cybersicherheit zielt darauf ab, die Kapazitäten zur Erkennung von Bedrohungen zu verbessern, ist aber nicht einsatzbereit

62 Eines der Hauptziele des europäischen Warnsystems für Cybersicherheit besteht darin, einen sinnvollen Informationsaustausch zu fördern, um die Erkennung und Analyse von Cyberbedrohungen sowie die Reaktion darauf zu verbessern. Die Teilnahme am Warnsystem ist freiwillig. Mitgliedstaaten, die sich für die Teilnahme an einem grenzübergreifenden Cyber-Hub entscheiden, verpflichten sich jedoch, relevante Informationen mit den anderen Mitgliedern zu teilen. Indem die Mitgliedstaaten in einem vertrauenswürdigen und sicheren Umfeld in Gruppen zusammenarbeiten, könnten sie einige der in den Ziffern ***31***–***44*** genannten Probleme des Informationsaustauschs vermeiden.

63 Zum Zeitpunkt der Prüfung hatten sich 13 Mitgliedstaaten für die Teilnahme am europäischen Warnsystem für Cybersicherheit entschieden und zwei grenzübergreifende Hubs eingerichtet: ATHENA und ENSOC. Einem dritten grenzübergreifenden Cyber-Hub, dem NBCC, wurden im Jahr 2026 Mittel zur Einrichtung zugewiesen, wodurch sich die Mitgliederzahl des Netzwerks auf insgesamt 20 Länder (18 Mitgliedstaaten sowie Island und Norwegen[10]) erhöhte (siehe ***Abbildung 5***).

[10] Assoziierte Nicht-EU-Länder in Einklang mit Artikel 10 Absatz 1 Buchstabe a der Verordnung (EU) 2021/694.

Abbildung 5 | Länder im europäischen Warnsystem für Cybersicherheit



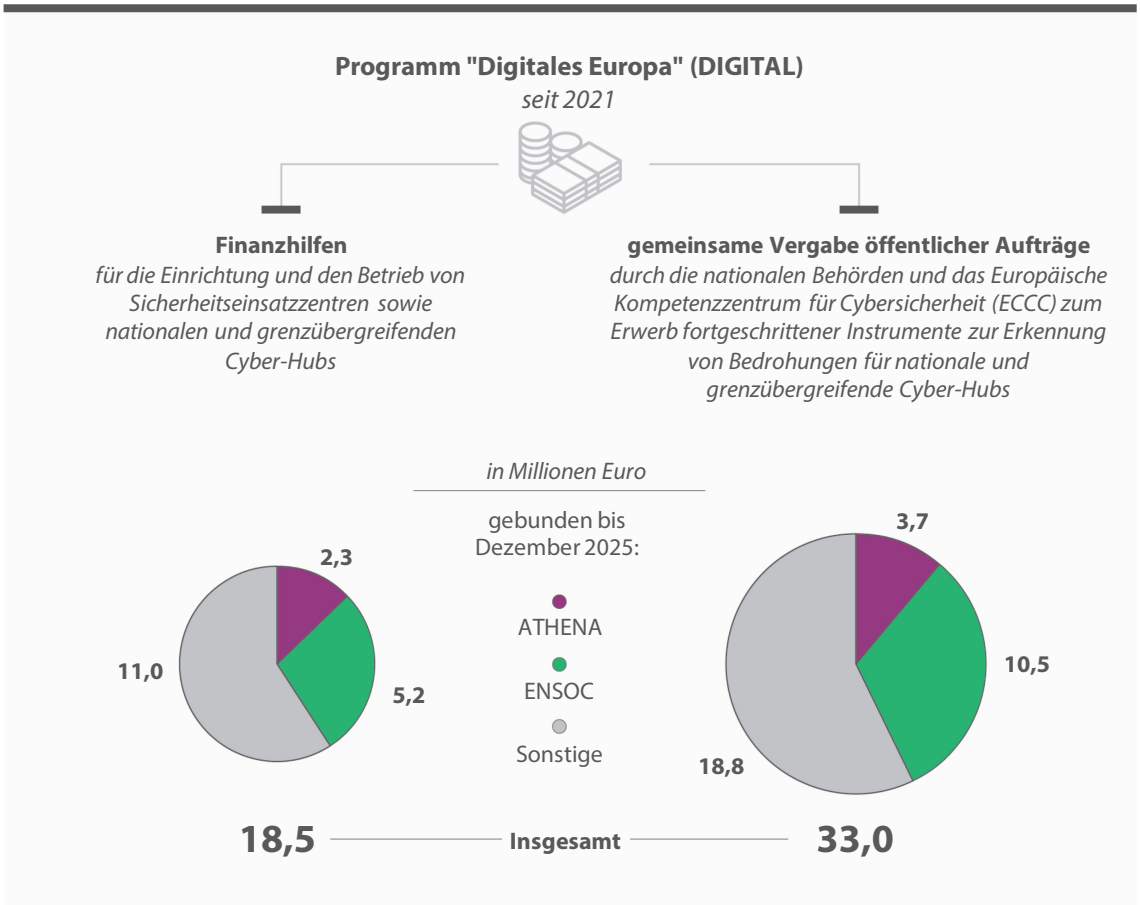
Quelle: Europäischer Rechnungshof.

64 Der Rechnungshof bewertete den Aufbau der ersten beiden grenzübergreifenden Cyber-Hubs und ihre Fortschritte bei der Verwirklichung der Ziele des europäischen Warnsystems für Cybersicherheit. Er untersuchte auch, wie sich die Einrichtung der grenzübergreifenden Cyber-Hubs in die breitere Cybersicherheitslandschaft einfügt und wie das Zusammenspiel mit den bestehenden Netzwerken und Strukturen funktioniert.

Aufgrund beträchtlicher Verzögerungen bei der Auftragsvergabe wurden bislang keine konkreten Ergebnisse erzielt

65 Seit 2021 stehen im Rahmen von DIGITAL Mittel für die Einrichtung nationaler und grenzübergreifender Cyber-Hubs zur Verfügung. Die Bereitstellung der Mittel erfolgt im Rahmen eines komplexen Verfahrens über zwei parallele Kanäle: die traditionellen Finanzhilfen zur Unterstützung der Einrichtung und des Betriebs der Cyber-Hubs sowie die gemeinsame Vergabe öffentlicher Aufträge für fortschrittliche Instrumente zur Erkennung von Bedrohungen (***Abbildung 6***). Nach einer Aufforderung zur Einreichung von Vorschlägen im November 2022 nahmen ATHENA und ENSOC ihre Arbeit im Januar 2024 auf.

Abbildung 6 | Finanzierung von Cyber-Hubs durch das Programm "Digitales Europa"



Quelle: Europäischer Rechnungshof auf der Grundlage von Daten des ECCC.

66 Die zweiphasigen nichtoffenen Vergabeverfahren[11] wurden von den Mitgliedern von ATHENA und ENSOC sowie der GD Connect (erste Phase) und dem neu eingerichteten ECCC (zweite Phase) organisiert. Der zweiphasige Ansatz zielt darauf ab, die Verbreitung sensibler Informationen zu begrenzen, indem die detaillierten technischen Spezifikationen nur den in der ersten Phase ausgewählten Bewerbern zur Verfügung gestellt werden.

67 Die erste Phase wurde im Mai 2024 für ENSOC und im Juli 2024 für ATHENA eingeleitet. Interessierte Unternehmen hatten einen Monat Zeit, um sich zu bewerben.
Die erfolgreichen Bewerber wurden jedoch erst im April 2025, d. h. fast ein Jahr nach Einleitung des Verfahrens, benachrichtigt.

68 Darüber hinaus konnte zu diesem Zeitpunkt weder das Vergabeverfahren für ENSOC noch das für ATHENA zur zweiten Phase übergehen, da es den Hub-Mitgliedern und dem ECCC nicht möglich war, den Unternehmen aus der engeren Wahl die für die Abgabe eines Angebots erforderlichen technischen Spezifikationen zur Verfügung zu stellen, weil sie noch an deren Fertigstellung arbeiteten.

69 Die zweite Phase der Vergabeverfahren begann für einige ENSOC-Lose erst im August 2025 und war für ATHENA für Anfang 2026 geplant. Zum Zeitpunkt der Prüfung, d. h. 18 Monate nach Einleitung des Vergabeverfahrens, war für keines der Lose ein Vertrag unterzeichnet worden. Der Rechnungshof ist der Auffassung, dass die unzureichende Vorbereitung und die Komplexität der Vergabeverfahren deren fristgerechten Abschluss verhindert haben.

70 Daher stellte der Rechnungshof fest, dass die grenzübergreifenden Cyber-Hubs nicht auf gutem Weg sind, um ihre Ziele zu erreichen. Ohne die Instrumente zur Erkennung von Bedrohungen und zum Informationsaustausch lagen ihre Tätigkeiten still, und das europäische Warnsystem für Cybersicherheit funktioniert noch nicht. Dadurch verzögert sich die wirksame Entwicklung fortgeschrittener Fähigkeiten zur Erkennung und Verhütung von Cyberbedrohungen und -sicherheitsvorfällen. Es wurden Änderungen zur Verlängerung der Laufzeit der Finanzhilfevereinbarung unterzeichnet, um den bisherigen Verzögerungen bei den Vergabeverfahren Rechnung zu tragen (15 Monate für ATHENA und 18 Monate für ENSOC).

[11] ENSOC-Ausschreibung und ATHENA-Ausschreibung.

Grenzübergreifende Cyber-Hubs schaffen zusätzliche Kommunikationskanäle, die die Komplexität weiter erhöhen

71 Eine der Hauptaufgaben der grenzübergreifenden Cyber-Hubs besteht darin, einschlägige Informationen auszutauschen, um die Erkennung von Bedrohungen und die Reaktion darauf zu verbessern. Dazu gehören Informationen über Cyberbedrohungen, Schwachstellen, Kompromittierungsindikatoren und Bedrohungsakteure. Die Aufgaben der grenzübergreifenden Cyber-Hubs decken sich teilweise mit denen der nationalen CSIRTs und des CSIRTs-Netzwerks, insbesondere bezüglich des Informationsaustauschs über Cyberbedrohungen und Schwachstellen. Die Rollen der grenzübergreifenden Cyber-Hubs und der CSIRTs sind nicht klar voneinander abgegrenzt. Gemäß dem Cyber-Konzeptentwurf aus dem Jahr 2025 (siehe Ziffer ***29***) sollen grenzübergreifende Cyber-Hubs sowohl auf technischer Ebene (wie die nationalen CSIRTs und das CSIRTs-Netzwerk) als auch auf operativer Ebene (wie das EU-CyCLONe) tätig werden.

72 Nach der Cybersolidaritätsverordnung müssen grenzübergreifende Cyber-Hubs Kooperationsvereinbarungen miteinander unterzeichnen, um den Informationsaustausch zu erleichtern. Die ENISA hätte, wie in der Cybersolidaritätsverordnung vorgeschrieben, bis Februar 2026 Leitlinien für die Interoperabilität zwischen grenzübergreifenden Cyber-Hubs herausgeben sollen. In der Zwischenzeit gewährte das ECCC im Dezember 2025 einem Konsortium (einschließlich bestimmter Mitglieder von ENSOC und ATHENA) eine Finanzhilfe zur Festlegung eines technischen Rahmens für die Interoperabilität zwischen grenzübergreifenden Cyber-Hubs. Die Leitlinien und der Rahmen werden jedoch erst fertiggestellt werden, wenn die grenzübergreifenden Cyber-Hubs in Betrieb sind.
Wie der Rechnungshof in seiner Stellungnahme von 2023 zum Vorschlag für die Cybersolidaritätsverordnung[12] dargelegt hat, besteht das Risiko, dass ohne eine rasche Einigung Systeme entwickelt werden, die nicht miteinander vereinbar sind, was zu höheren Kosten führt.

[12] Stellungnahme 02/2023 zu dem Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über Maßnahmen zur Stärkung der Solidarität und der Kapazitäten in der Union für die Erkennung, Vorsorge und Bewältigung von Cybersicherheitsbedrohungen und -vorfällen, Ziffer 26.

73 Grenzübergreifende Cyber-Hubs sind auch verpflichtet, relevante Informationen über Cybersicherheitsvorfälle großen Ausmaßes unverzüglich an das EU-CyCLONe und das CSIRTs-Netzwerk weiterzugeben. Auf Ebene der Mitgliedstaaten werden durch die Einrichtung nationaler Cyber-Hubs und die Beteiligung an grenzübergreifenden Cyber-Hubs zusätzliche Kommunikationsebenen geschaffen. Die Abstimmung mit Nicht-EU-Mitgliedstaaten[13], die keine Mitglieder des CSIRTs-Netzwerks oder des EU-CyCLONe sind, erhöht ebenfalls die Komplexität.

74 Klare Kooperationsvereinbarungen sind erforderlich, um sich auf eine gemeinsame Taxonomie und den Ablauf des Informationsaustauschs zu einigen und die Interoperabilität zu gewährleisten. Die aus dem CSIRTs-Netzwerk gewonnenen Erkenntnisse zeigen, dass dies eine große Herausforderung darstellt. Der Rechnungshof stellte fest, dass zum Zeitpunkt der Prüfung keine Verfahrensregelungen für die Zusammenarbeit und den Informationsaustausch vereinbart worden waren. Er ist der Auffassung, dass die Einrichtung nationaler und grenzübergreifender Cyber-Hubs einem wirksameren Informationsaustausch förderlich sein könnte. Die Integration der grenzübergreifenden Hubs in die bereits komplexe Cybersicherheitslandschaft wird jedoch anspruchsvoll sein und zusätzliche Kommunikationskanäle und Kooperationsvereinbarungen erfordern.

[13] Island und Norwegen.

Mit EU-finanzierten Projekten im Rahmen von DIGITAL soll die Cybersicherheit gestärkt werden, bei der Umsetzung und Berichterstattung bestehen jedoch Herausforderungen

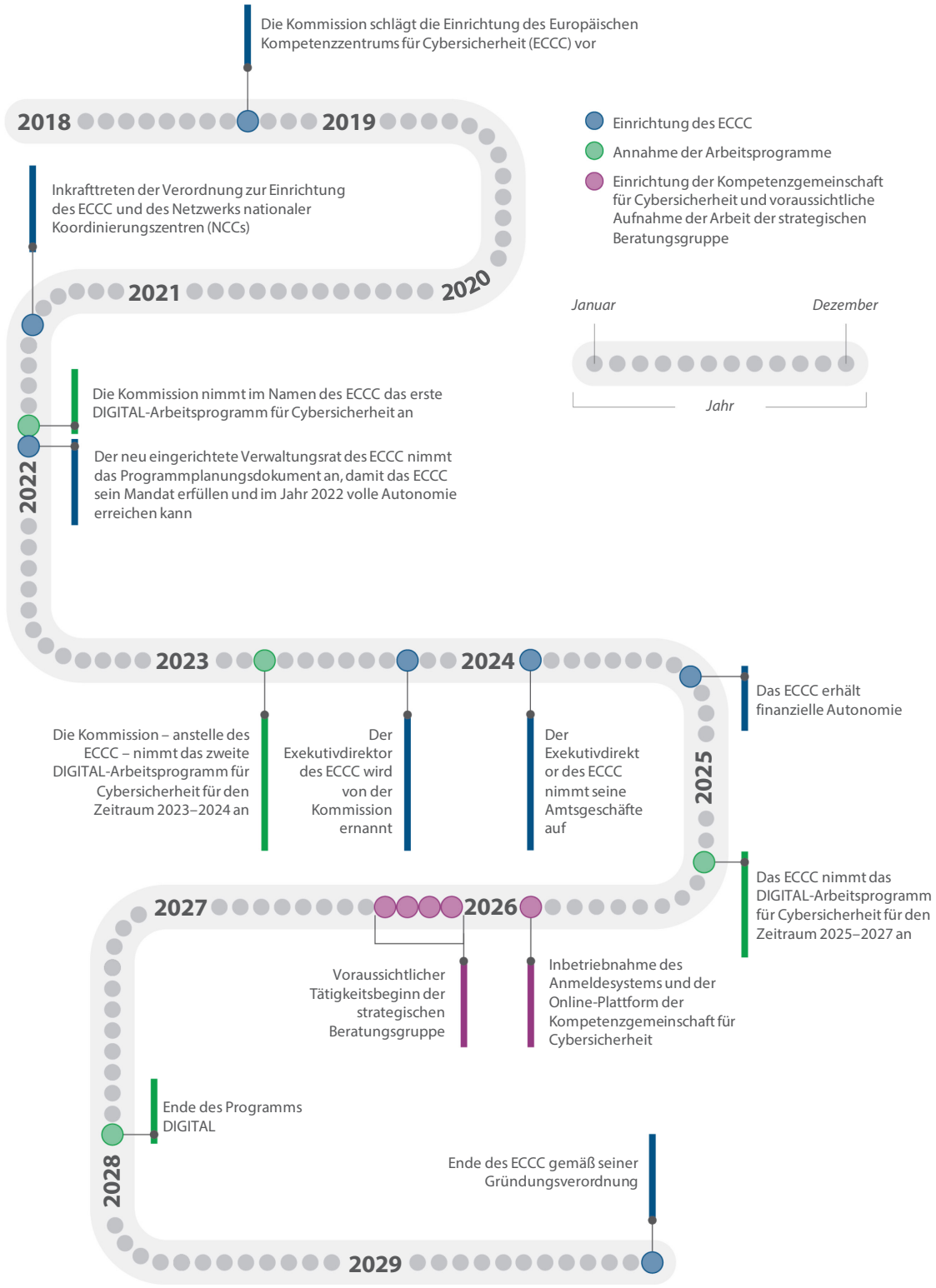
Verzögerungen bei der Einrichtung hinderten die Kompetenzgemeinschaft für Cybersicherheit daran, DIGITAL entsprechend ihren Bedürfnissen zu gestalten

75 Zur Verwaltung der Cybersicherheitskomponente von DIGITAL schlug die Kommission 2018 die Einrichtung des Europäischen Kompetenzzentrums für Cybersicherheit (ECCC) vor. In der ECCC-Verordnung war vorgesehen, dass das ECCC durch ein Netzwerk von 29 nationalen Koordinierungszentren (NCCs) unterstützt wird, eines für jeden Mitgliedstaat sowie Island und Norwegen. Darüber hinaus wurde die Schaffung einer Kompetenzgemeinschaft für Cybersicherheit (im Folgenden "Gemeinschaft") gefordert, die sich aus Vertretern der Industrie, Wissenschaft und Forschung sowie anderen einschlägigen Organisationen der Zivilgesellschaft zusammensetzt.

76 Bis zu 20 Mitglieder der Gemeinschaft sollten in die strategische Beratungsgruppe berufen werden, die eine von drei Komponenten der Struktur des ECCC darstellt. Eine der Hauptaufgaben der strategischen Beratungsgruppe besteht darin, öffentliche Konsultationen zu organisieren, deren Ergebnisse in die Agenda des ECCC und die Arbeitsprogramme von DIGITAL einfließen.

77 Der Rechnungshof bewertete, ob DIGITAL und die dazugehörigen Arbeitsprogramme auf der Grundlage einer fundierten Bedarfsanalyse angenommen wurden, und er untersuchte, wie das ECCC, das Netzwerk der nationalen Koordinierungszentren, die Gemeinschaft und die strategische Beratungsgruppe zu den Arbeitsprogrammen beitragen konnten. In der Praxis wurden das ECCC, das Netzwerk der nationalen Koordinierungszentren, die Gemeinschaft und die strategische Beratungsgruppe schrittweise über mehrere Jahre hinweg aufgebaut (siehe ***Abbildung 7***).

Abbildung 7 | Zeitplan für die Einrichtung des Europäischen Kompetenzzentrums für Cybersicherheit, des Netzwerks nationaler Koordinierungszentren, der Gemeinschaft und der strategischen Beratungsgruppe



Quelle: Europäischer Rechnungshof.

78 Da das ECCC erst im September 2024 voll funktionsfähig war, nahm die Kommission im Namen des ECCC die Arbeitsprogramme für die Zeiträume 2021–2022 und 2023–2024 an. In die beiden von der Kommission angenommenen Arbeitsprogramme flossen keine Beiträge der Gemeinschaft ein.

79 In der Zwischenzeit begannen die Mitgliedstaaten mit der Einrichtung ihrer nationalen Koordinierungszentren, die auf nationaler Ebene als Kontaktstellen für die Gemeinschaft fungieren. Einrichtung und Betrieb dieser Zentren wurden von DIGITAL kofinanziert, wobei zum Zeitpunkt der Prüfung EU-Mittel in Höhe von über 90 Millionen Euro gewährt worden waren, darunter rund 44 Millionen Euro, die in Form von finanzieller Unterstützung an Dritte weitergeleitet werden. Bis 2027 wurden weitere 38 Millionen Euro für die Unterstützung der nationalen Koordinierungszentren veranschlagt.

80 Der Rechnungshof stellte fest, dass im Dezember 2025, d. h. vier Jahre nach der Einrichtung des ECCC und des Netzwerks der nationalen Koordinierungszentren, die Gemeinschaft noch nicht eingerichtet und die Mitglieder der strategischen Beratungsgruppe noch nicht ernannt worden waren. Das ECCC nahm am 14. März 2025 das jüngste DIGITAL-Arbeitsprogramm für Cybersicherheit für den Zeitraum 2025–2027 an. Zwar hat das ECCC sein Arbeitsprogramm nach umfassenden Konsultationen mit den Mitgliedstaaten und dem Netzwerk der nationalen Koordinierungszentren ausgearbeitet und angenommen, doch kamen dem Programm keine Beiträge und Ratschläge der Gemeinschaft oder der strategischen Beratungsgruppe zugute. Dies steht im Widerspruch zu den Bestimmungen der Gründungsverordnung, und der Rechnungshof sieht dies als verpasste Chance an.

81 DIGITAL läuft im Jahr 2027 aus, und das ECCC wird voraussichtlich 2029 aufgelöst, wenn sein Mandat nicht verlängert wird. Daher ist die Unterstützung vonseiten des Netzwerks der nationalen Koordinierungszentren, der Gemeinschaft und der strategischen Beratungsgruppe, sobald diese eingerichtet sind, möglicherweise nur für einen kurzen Zeitraum relevant.

Mit EU-finanzierten Projekten werden relevante Ziele verfolgt, doch viele von ihnen sind mit operativen Problemen konfrontiert

82 Der Rechnungshof wählte eine Stichprobe von elf Projekten aus, die für die Erkennung von Cybersicherheitsvorfällen und die Reaktion darauf relevant sind und im Zeitraum 2022–2025 im Rahmen von DIGITAL finanziert wurden (siehe ***Abbildung 5*** in ***Anhang I*** und ***Anhang III***). Der Rechnungshof bewertete, ob

- die Ziele der Projekte mit den erwarteten Wirkungen, die in den Aufforderungen zur Einreichung von Vorschlägen aufgeführt waren, sowie mit denen von DIGITAL insgesamt im Einklang standen;
- die geplanten Outputs und Ergebnisse der Projekte bisher erreicht wurden;
- die Outputs der Projekte fristgerecht erbracht wurden.

Das Ergebnis dieser Bewertung ist ***Anhang IV*** zu entnehmen.

Einige Projekte zeigen erste Ergebnisse, aber viele sind mit operativen Herausforderungen und Verzögerungen konfrontiert

83 Der Rechnungshof stellte fest, dass alle Projekte Ziele verfolgen, die zur Verwirklichung der Cybersicherheitsziele von DIGITAL[14] beitragen, und dass die meisten Ziele der Aufforderungen zur Einreichung von Vorschlägen[15] berücksichtigt werden.

84 Von den elf Projekten in der Stichprobe des Rechnungshofs befanden sich zwei Projekte in einer frühen Phase der Durchführung, sodass der Rechnungshof keine Schlussfolgerungen zu ihrer Leistung ziehen konnte. Von den übrigen Projekten bewertete der Rechnungshof vier als zufriedenstellend in Bezug auf die Erreichung der geplanten Outputs und Ergebnisse. Der Rechnungshof war der Auffassung, dass zwei Projekte einige Schwachstellen aufwiesen, und bewertete drei Projekte als nicht zufriedenstellend (siehe ***Anhang IV***).

---

[14] Artikel 6 der Verordnung (EU) 2021/694 zur Aufstellung des Programms "Digitales Europa".

[15] Aufforderungen zur Einreichung von Vorschlägen: Aufbau von Kapazitäten in den Sicherheitseinsatzzentren; Aufbau des Netzwerks nationaler Koordinierungszentren mit den Mitgliedstaaten; Steigerung der Abwehrbereitschaft und gegenseitige Unterstützung sowie neuartige Anwendungen von KI und anderen grundlegenden Technologien für Sicherheitseinsatzzentren.

85 DIGITAL zielt ausdrücklich darauf ab, das Cybersicherheitsniveau kleiner und mittlerer Unternehmen (KMU) zu erhöhen. In dieser Hinsicht bieten mehrere Projekte konkrete Lösungen für KMU (siehe ***Kasten 2***).

Kasten 2

Beispiele für Projekte, die greifbare Ergebnisse für KMU bringen

Ziel des Projekts GR-SME-SOC (Projekt 6 in ***Anhang III***) ist es, KMU in Griechenland Cybersicherheitsinstrumente und -dienste zur Verfügung zu stellen, indem ein auf ihre Bedürfnisse zugeschnittenes Sicherheitseinsatzzentrum (SOC) eingerichtet wird. Das Projekt begann im Januar 2024 und wird von einem Konsortium aus fünf griechischen Organisationen durchgeführt. Geplant ist, 120 KMU ein Jahr lang kostenlos Cybersicherheitsdienste anzubieten. Danach werden die Dienste kommerziell verfügbar sein. Das Projekt bietet KMU fortschrittliche Dienste wie Echtzeitüberwachung, KI-gestützte Erkennung von Bedrohungen und flexible Reaktion auf Sicherheitsvorfälle an.

Mit dem Projekt NCC-IE (Projekt 3 in ***Anhang III***) stellte der Projektkoordinator rund 1,8 Millionen Euro an Finanzhilfen für mehr als 50 irische KMU zur Verbesserung ihrer Cybersicherheit bereit. Die Förderregelung kam Unternehmen mit rund 2−200 Beschäftigten zugute, u. a. Familienunternehmen, Start-up-Unternehmen und globalen Exporteuren in verschiedenen Sektoren. Die Finanzhilfen waren ausschließlich für Unternehmen bestimmt, die zuvor einer von der Regierungsbehörde *Enterprise Ireland* durchgeführten Überprüfung der Cybersicherheit unterzogen worden waren. Sie deckten jeweils 80 % der Kosten (bis zu 60 000 Euro) für die Umsetzung der Empfehlungen aus der Überprüfung ab.

Quelle: Europäischer Rechnungshof.

86 Bei vielen Projekten in der Stichprobe des Rechnungshofs gibt es Probleme mit der Einhaltung von Fristen oder operative Herausforderungen (siehe ***Anhang IV***). Der Rechnungshof stellte fest, dass es bei vier Projekten zu beträchtlichen Verzögerungen gekommen ist. Dazu gehören ENSOC und ATHENA (siehe Ziffern ***65***–***70***). Weitere Beispiele sind ***Kasten 3*** zu entnehmen.

Kasten 3

Beispiele für Projekte mit operativen Herausforderungen und Verzögerungen

In Irland ist die *Local Government Management Authority* der einzige Begünstigte der Finanzhilfe für das Projekt ILG-SOC (Projekt 8 in ***Anhang III***). Ziel des Projekts ist die Einrichtung eines zentralen Sicherheitseinsatzzentrums für 31 lokale Behörden zur Nutzung fortschrittlicher Instrumente bei der Erkennung von Bedrohungen und der Reaktion darauf. Das Projekt begann im Oktober 2023 und hat eine Laufzeit von drei Jahren. Infolge der Ergebnisse der Halbzeitüberprüfung wurden alle zu erbringenden Leistungen abgelehnt. Das Projekt umfasst mehrere Vergabeverfahren, die gescheitert sind oder sich verzögert haben. Die Laufzeit des Projekts soll verlängert werden (ohne zusätzliche Finanzierung), was dem Projekt genügend Zeit für einen erfolgreichen Abschluss verschaffen könnte.

In Griechenland zielt das Projekt EL-SOC (Projekt 5 in ***Anhang III***) darauf ab, ein konsolidiertes Sicherheitseinsatzzentrum auf nationaler Ebene einzurichten, in dem Informationen aus sektorspezifischen Sicherheitseinsatzzentren zusammengeführt werden sollen. Dadurch soll ein umfassender Überblick über die Cybersicherheitslage in Echtzeit geboten werden. Das Projekt läuft von Januar 2024 bis Dezember 2026. Die geplante Beschaffung von Hardware und Dienstleistungen verzögerte sich aufgrund von Problemen bei der Fertigstellung und Veröffentlichung der technischen Spezifikationen für die Ausschreibung. Als Gründe für die Verzögerung führte der Projektkoordinator u. a. Probleme in Bezug auf die Bewilligung nationaler Kofinanzierungsmittel und die begrenzte Verfügbarkeit von Personal im Bereich der Auftragsvergabe an.

Quelle: Europäischer Rechnungshof.

87 Bei zwei weiteren Projekten in der Stichprobe des Rechnungshofs kam es zu geringfügigen Verzögerungen. Drei Projekte haben ihre Outputs bislang fristgerecht erbracht. Schließlich befinden sich zwei Projekte in einer frühen Phase der Durchführung, sodass der Rechnungshof keine Schlussfolgerungen dazu ziehen kann.

Sicherheitsbeschränkungen haben zu operativen Herausforderungen geführt, und es bestehen erhebliche Risiken, wenn die Kontrollen von den Begünstigten durchgeführt werden

88 Die DIGITAL-Verordnung sieht vor, dass die Finanzierung der Cybersicherheit aus Sicherheitsgründen auf Rechtsträger beschränkt werden kann, die ihren Sitz in der EU haben und von Mitgliedstaaten oder EU-Bürgern kontrolliert werden. Diese Beschränkung zielt darauf ab, das Risiko des Eindringens oder der Einflussnahme durch Nicht-EU-Länder zu mindern und zu verhindern, dass sensible Sicherheitsinformationen an Behörden aus Drittstaaten weitergegeben werden.

89 Die Verpflichtung, im Eigentum und unter der Kontrolle von Mitgliedstaaten oder EU-Bürgern zu stehen, gilt nicht nur für Begünstigte von Finanzhilfen, sondern auch für deren Unterauftragnehmer und alle Empfänger finanzieller Unterstützung für Dritte. Mit Ausnahme der letztgenannten Kategorie (siehe Ziffern ***92***–***96***) nimmt der zentrale Validierungsdienst der Europäischen Exekutivagentur für die Forschung die diesbezügliche Bewertung vor. Die endgültige Entscheidung über die Berechtigung zur Teilnahme an beschränkten Aufforderungen zur Einreichung von Vorschlägen liegt jedoch nach wie vor bei der Bewilligungsbehörde, d. h. der GD Connect oder dem ECCC.

90 Während der Prüfungsarbeit des Rechnungshofs wiesen die Begünstigten wiederholt auf die praktischen Herausforderungen hin, die sich aus den Bewertungen der Eigentums- und Kontrollverhältnisse ergeben. Die Bewertung, ob ein Rechtsträger im Eigentum und unter der Kontrolle von Mitgliedstaaten oder EU-Bürgern steht, kann ein komplexer und langwieriger Prozess sein. Er erfordert eine Analyse der gesamten Eigentumsstruktur und Kontrollkette der einzelnen Organisationen, einschließlich aller Eigentümerschichten bis hin zu den eigentlichen Eigentümern. Der zentrale Validierungsdienst verlangt, dass jede Einrichtung umfassende Belege über ihre Eigentumsstruktur sowie bestimmte Rechte, die Unternehmensführung und -kontrolle und alle kommerziellen, finanziellen oder sonstigen Verbindungen, aus denen sich eine Kontrolle über die betreffende Einrichtung ergibt, vorlegt.

91 Bei drei EU-finanzierten Projekten in der Stichprobe des Rechnungshofs wurde mindestens ein Begünstigter, der Teil eines Konsortiums war, später ausgeschlossen, da davon ausgegangen wurde, dass er im Eigentum oder unter der Kontrolle von Drittländern oder deren Staatsangehörigen steht. Der Ausschluss von Konsortiumsmitgliedern zeigt, dass das Konzept, dass Rechtsträger im Eigentum und unter der Kontrolle von Mitgliedstaaten oder EU-Bürgern stehen müssen, nicht von allen Teilnehmern des Programms DIGITAL vollständig verstanden wird. Den Daten des zentralen Validierungsdienstes zufolge bestanden im Zeitraum 2022–2025 insgesamt 7 % aller Antragsteller von DIGITAL-Finanzhilfen im Bereich Cybersicherheit oder ihre Unterauftragnehmer die Bewertung nicht. Die Einreichung von Anträgen nicht förderfähiger Teilnehmer im Rahmen einer Aufforderung zur Einreichung von Vorschlägen führt zu Verzögerungen (siehe ***Kasten 4***).

Kasten 4

Beispiel für einen Fall, in dem Begünstigte nach nicht bestandenen Sicherheitsprüfungen ausgeschlossen wurden

Zwei der Konsortiumsmitglieder des Projekts NG-SOC (Projekt 7 in ***Anhang III***) scheiterten an der Bewertung der Eigentums- und Kontrollverhältnisse. Das Ergebnis wurde etwa einen Monat vor Ablauf der Frist für die Unterzeichnung der Finanzhilfevereinbarung bekannt gegeben. Der Projektkoordinator musste sich bereit erklären, die Arbeit zu übernehmen, die zuvor den beiden ausgeschlossenen Mitgliedern übertragen worden war, da keine Zeit blieb, um einen neuen Partner zu finden. Eines der ausgeschlossenen Mitglieder war in einem bestimmten Wirtschaftszweig tätig, in dem die entwickelte Lösung erprobt werden sollte. Daher konnte ein erheblicher Teil des Projekts, bei dem es um die Erprobung der Lösungen in der Praxis ging, nicht wie geplant durchgeführt werden. Dieser Situation wurde später dadurch Abhilfe geschaffen, dass die Finanzhilfevereinbarung geändert wurde, um neue Mitglieder aufzunehmen.

Quelle: Europäischer Rechnungshof.

92 Bei zwei der vom Rechnungshof überprüften Projekte (NCC-IE und CYberSynchrony) wird finanzielle Unterstützung für Dritte bereitgestellt. Dieser Finanzierungsmechanismus ermöglicht es den Begünstigten der Finanzhilfen, einen Teil der Mittel im Rahmen von offenen Aufforderungen zur Einreichung von Vorschlägen an andere Einrichtungen zu vergeben. Finanzielle Unterstützung für Dritte kann den Zugang zu EU-Mitteln erleichtern. In diesem Fall tragen die Begünstigten die alleinige Verantwortung für die Bewertung der Eigentums- und Kontrollverhältnisse, und der zentrale Validierungsdienst ist nicht beteiligt.

93 Im Jahr 2021 veröffentlichte die Kommission allgemeine öffentliche Leitlinien für Antragsteller im Rahmen beschränkter Aufforderungen zur Einreichung von Vorschlägen. Diese Leitlinien wurden 2026 aktualisiert. Obwohl bereits seit 2021 im Rahmen der Aufforderungen zur Einreichung von Vorschlägen für DIGITAL die Möglichkeit besteht, finanzielle Unterstützung für Dritte zu vergeben, haben weder die Kommission noch das ECCC den Begünstigten eine detaillierte Methodik für die Durchführung der Bewertung der Eigentums- und Kontrollverhältnisse von Dritten, denen sie finanzielle Unterstützung gewähren, zur Verfügung gestellt. Im Juli 2025 gab das ECCC unverbindliche Leitlinien heraus, die dem Netzwerk der nationalen Koordinierungszentren einen strukturierten Ansatz für die Bewertung der Eigentums- und Kontrollverhältnisse an die Hand geben. Der Leitfaden enthält allgemeine Grundsätze und mögliche Maßnahmen. In den Leitlinien ist jedoch nicht festgelegt, wie die Kontrollen durchzuführen sind, sodass die Verantwortung für die Ausarbeitung eines eigenen Ansatzes bei den Begünstigten liegt.

94 Der Rechnungshof stellte fest, dass das ECCC weder die von den Begünstigten angewandte Methodik validiert noch stichprobenartige Kontrollen durchführt, um sicherzustellen, dass die Methodik solide genug ist und die ausgewählten Empfänger finanzieller Unterstützung tatsächlich im Eigentum und unter der Kontrolle von Mitgliedstaaten oder EU-Bürgern stehen.

95 In seinem Jahresbericht 2024 stellte der Rechnungshof fest, dass die Begünstigten, die von der Kommission mit der Verwaltung der finanziellen Unterstützung für Dritte (im Forschungsbereich) betraut wurden, nicht verpflichtet waren, die Wirksamkeit ihrer Kontrollen nachzuweisen, um die Ordnungsmäßigkeit der EU-Ausgaben sicherzustellen. Ebenso wenig untersuchte das ECCC die administrativen und technischen Kapazitäten der Begünstigten, um festzustellen, ob sie in der Lage waren, die Bewertung der Eigentums- und Kontrollverhältnisse ordnungsgemäß durchzuführen. Wie in Ziffer *90* dargelegt, kann diese Bewertung komplex sein und wird auf EU-Ebene von einem speziellen Dienst mit Fachwissen durchgeführt.

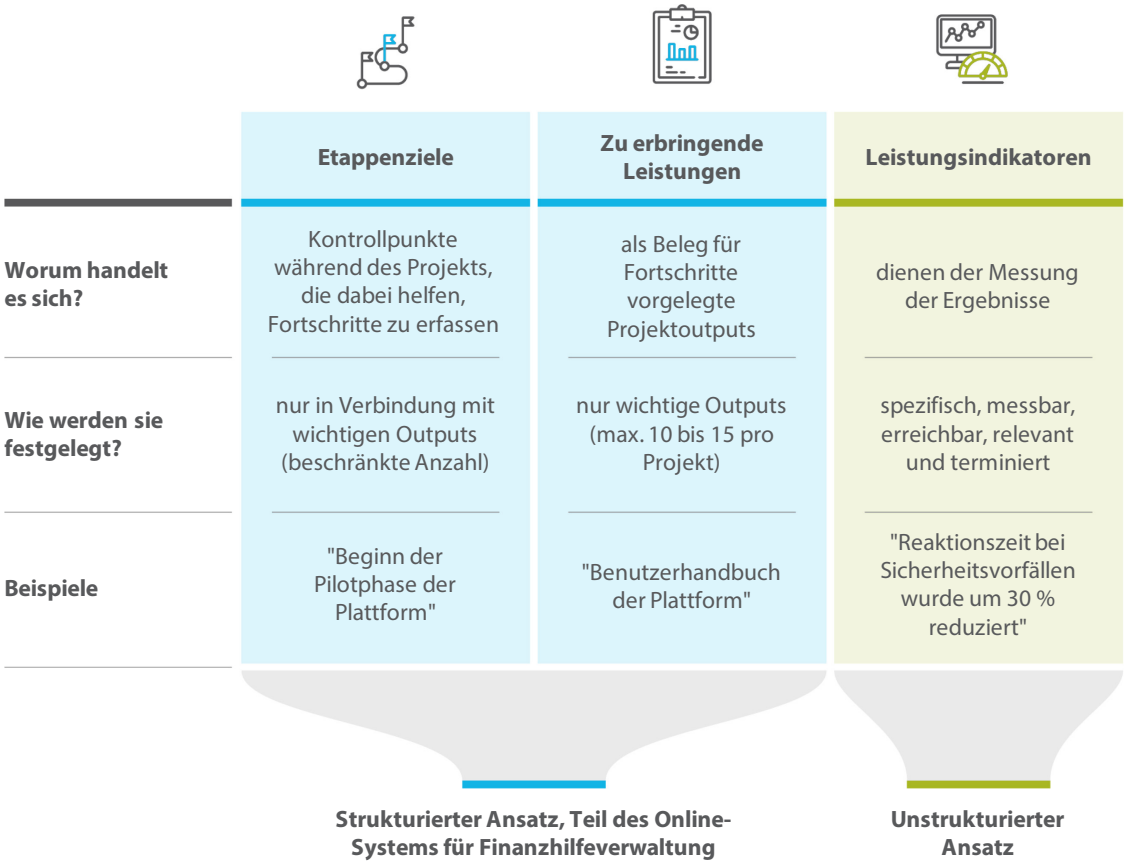
96 In diesem Zusammenhang besteht nach Auffassung des Rechnungshofs ein erhebliches Risiko, dass die Begünstigten, die für die Bewertung der Eigentums- und Kontrollverhältnisse zuständig sind, nicht in der Lage sind, diese ordnungsgemäß durchzuführen. In Anbetracht der Art der finanzierten Tätigkeiten könnte dieser Mangel sensible Infrastrukturen, operative Daten und sicherheitskritische Technologien gefährden.

Die Leistungsrahmen der meisten EU-finanzierten Projekte sind unzureichend, und die Leistungsdaten von DIGITAL im Bereich der Cybersicherheit sind nicht korrekt

Die Leistungsrahmen der meisten EU-finanzierten Projekte sind unzureichend

97 Begünstigte, die EU-finanzierte Projekte verwalten, müssen dem ECCC auf der Grundlage von Etappenzielen, zu erbringenden Leistungen und Indikatoren über ihre Fortschritte und Ergebnisse Bericht erstatten (siehe ***Abbildung 8***). Der Rechnungshof bewertete, ob die für die einzelnen Projekte festgelegten Etappenziele und zu erbringenden Leistungen eine angemessene Projektüberwachung ermöglichen. Darüber hinaus bewertete der Rechnungshof, ob die Leistungsindikatoren relevant und messbar sind und einen Ausgangs- und Zielwert haben.

Abbildung 8 | Etappenziele, zu erbringende Leistungen und Leistungsindikatoren bei DIGITAL-Projekten



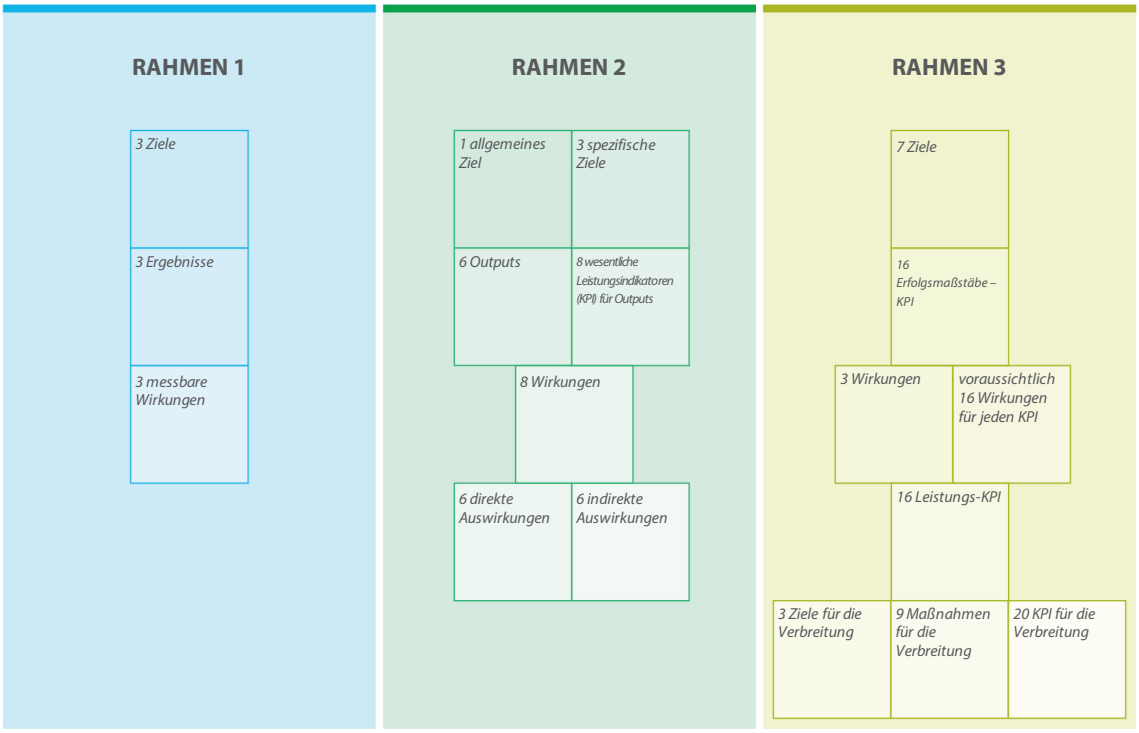
Quelle: Europäischer Rechnungshof auf der Grundlage des Formulars zur Beantragung von Finanzhilfen.

98 In ihrem Projektvorschlag müssen die Begünstigten auf der Grundlage eines strukturierten Ansatzes, der in den Anweisungen für die Antragsteller festgelegt ist, eine Reihe von Etappenzielen und zu erbringenden Leistungen definieren. Alle Etappenziele und zu erbringenden Leistungen sind im Online-System für die Finanzhilfeverwaltung aufgeführt, um deren Nachverfolgung zu erleichtern. Das ECCC überprüft in der Regel jedes Projekt zweimal: einmal nach der Hälfte der Projektlaufzeit und einmal nach Abschluss des Projekts. Bei diesen Überprüfungen untersuchen externe Sachverständige, ob die Etappenziele und zu erbringenden Leistungen erreicht wurden. Anschließend werden sie vom ECCC validiert. Etappenziele und zu erbringende Leistungen sind daher für die Projektüberwachung von entscheidender Bedeutung und sollten ordnungsgemäß festgelegt werden.

99 Der Rechnungshof stellte fest, dass bei fast keinem der Projekte in seiner Stichprobe die Anweisungen in Bezug auf die Anzahl der Etappenziele und zu erbringenden Leistungen befolgt wurden: Die Anzahl der Etappenziele pro Projekt liegt zwischen 8 und 39, und die Anzahl der zu erbringenden Leistungen zwischen 8 und 45. Viele der Etappenziele und zu erbringenden Leistungen wurden nicht gemäß den Anweisungen festgelegt und sind daher nicht geeignet, um Fortschritte zu kontrollieren (z. B. "Sitzung zur Einleitung der Ausarbeitung der Aufforderung zur Einreichung von Forschungsvorschlägen" oder "formelles Protokoll der Projektsitzung"). Bei drei Projekten hatte der Evaluierungsausschuss diese Probleme vor der Unterzeichnung der Finanzhilfevereinbarung ermittelt. In zwei Fällen schlugen die Begünstigten nur geringfügige Änderungen vor (z. B. in Bezug auf die Fristen), ohne das eigentliche Problem anzugehen, im dritten Fall wurden keine Änderungen vorgenommen. Bei sechs weiteren Projekten in der Stichprobe zeigt die Analyse des Rechnungshofs, dass die Etappenziele oder zu erbringenden Leistungen nicht den Anweisungen entsprechen und nicht immer angemessen sind. Der Rechnungshof ist der Auffassung, dass es schwierig ist, Fortschritte zu verfolgen, wenn die zu erbringenden Leistungen oder Etappenziele unzureichend definiert sind oder zu viele davon festgelegt wurden.

100 Im Gegensatz zu den Etappenzielen und zu erbringenden Leistungen werden die Leistungsindikatoren nicht auf der Grundlage eines strukturierten Ansatzes festgelegt und auch nicht in einer Tabelle im Finanzhilfeverwaltungssystem zusammengefasst. Stattdessen sind sie in verschiedenen Abschnitten des Vorschlags enthalten. Dieser Ansatz hat dazu geführt, dass die Begünstigten eine Vielzahl von Leistungsrahmen vorschlugen. Während einige nur Projektziele festlegten, die mit Leistungsindikatoren verknüpft waren, arbeiteten andere deutlich komplexere Leistungsrahmen aus. Einige Beispiele sind ***Abbildung 9*** zu entnehmen.

Abbildung 9 | Beispiel für die Vielzahl an Leistungsrahmen, die für die Projekte konzipiert wurden



Quelle: Europäischer Rechnungshof.

101 Die Analyse des Rechnungshofs ergab, dass viele der bei den Projekten verwendeten Leistungsindikatoren nicht relevant oder messbar sind und dass Ziel- oder Ausgangswerte fehlen (siehe ***Kasten 5***). Darüber hinaus wurden bei sieben Projekten 20 oder mehr Indikatoren festgelegt, bei einem Projekt waren es 52. Das Ergebnis dieser Bewertung ist ***Anhang IV*** zu entnehmen.

Kasten 5

Beispiele für unzureichende Leistungsindikatoren

Nicht messbar:

- "Der Kompromittierungsindikator und andere erbrachte Dienste stärken die Cybersicherheitskapazitäten von KMU"
- "Bereitstellung von Instrumenten und Methoden für die Reaktion auf Sicherheitsvorfälle, die eine Integration in die Kommunikationskanäle des EU-CyCLONe ermöglichen"

Ausgangs- oder Zielwert fehlt:

- "≥ 20 % Verbesserung der Fähigkeiten des Personals im Bereich der Abwehrbereitschaft"
- "≥ 20 % Verringerung des Aufwands, der zur Anpassung an die und Einhaltung der einschlägigen Cybersicherheitsinitiativen der EU erforderlich ist"

Nicht leistungsbezogen:

- "Abschlussbericht über das Projekt am Ende der Förderphase"
- "Anzahl der Personen, die an allen Schulungen teilnehmen werden"

Quelle: Europäischer Rechnungshof auf der Grundlage der Projektunterlagen.

102 Insgesamt ist der Rechnungshof der Auffassung, dass die vielen verschiedenen Leistungsrahmen sowie die mangelhafte Ausarbeitung und übermäßige Anzahl der Indikatoren die Leistungsüberwachung erheblich erschweren. Daher ist es nicht möglich, die Projektleistung ordnungsgemäß zu bewerten. Dies wird zusätzlich dadurch erschwert, dass in dem Berichtsmuster kein spezieller Abschnitt für die Leistungsindikatoren der Projekte vorgesehen ist und die meisten Projekte in der Stichprobe des Rechnungshofs daher keinen Bericht darüber erstatteten.

Die Leistungsdaten für die Cybersicherheitskomponente von DIGITAL sind nicht korrekt

103 Zur Überwachung der Resultate von DIGITAL enthält die Verordnung Programmindikatoren, über die für alle Projekte Bericht erstattet werden muss (siehe ***Kasten 6***).

Kasten 6

Indikatoren des Programms DIGITAL im Bereich der Cybersicherheit

1.a Anzahl der gemeinsam beschafften Cybersicherheitsinfrastrukturen oder -werkzeuge oder beider, auch im Rahmen des europäischen Warnsystems für Cybersicherheit

1.b Anzahl der eingesetzten Cybersicherheitsinfrastrukturen oder -werkzeuge oder beider

2. Anzahl der Nutzer und Nutzergemeinschaften, die Zugang zu europäischen Cybersicherheitseinrichtungen erhalten

3. Anzahl der Maßnahmen zur Unterstützung der Abwehrbereitschaft und der Reaktion auf Cybersicherheitsvorfälle im Rahmen des Cybernotfallmechanismus

Quelle: Anhang II der Verordnung (EU) 2021/694 zur Aufstellung des Programms "Digitales Europa"; Überwachungs- und Evaluierungsrahmen für das Programm "Digitales Europa" (SWD(2024) 37).

104 Der Rechnungshof bewertete, ob für die Projekte in seiner Stichprobe über diese Indikatoren Bericht erstattet wurde, und untersuchte, wie das ECCC diese Daten erhebt und überprüft.

105 Für alle Projekte muss vor der Halbzeit- und Abschlussüberprüfung im Finanzhilfeverwaltungssystem über die Indikatoren des Programms DIGITAL Bericht erstattet werden. Der Rechnungshof stellte fest, dass diese Indikatoren nur für drei von sieben Projekten gemeldet wurden, die zum Zeitpunkt der Prüfung die Hälfte ihres Zeitplans erreicht hatten und für die daher eine solche Meldung hätte erfolgen müssen. Für zwei dieser drei Projekte wurden keine korrekten Informationen übermittelt: Bei einem Projekt wurde über den falschen Indikator berichtet, bei dem anderen Projekt wurden Zielwerte statt der erzielten Ergebnisse angegeben.

106 Die Kommission meldet diese Indikatoren jedes Jahr in ihren Berichten über die Programmleistung. Dies ermöglicht es den Interessenträgern, zu beurteilen, ob das Programm seine Ziele erreicht. Laut den Berichten über die Programmleistung für das Jahr 2024 entwickeln sich die Indikatoren des Programms DIGITAL für die Cybersicherheit wie geplant. Das ECCC erklärte dem Rechnungshof, dass es diese Indikatoren anhand der Ergebnisse einer Reihe von Umfragen, die den Projektbegünstigten übermittelt wurden, und nicht auf der Grundlage des Finanzhilfeverwaltungssystems zusammengetragen hat. Der Rechnungshof überprüfte die vom ECCC bereitgestellten aufgeschlüsselten Daten und stellte zahlreiche Probleme bei der Datenerhebung und der Gesamtqualität der Daten fest. Er stellte fest, dass die erhobenen Daten nicht mit den im Bericht über die Programmleistung angegebenen Werten übereinstimmen. Somit ist unklar, wie die gemeldeten Werte berechnet wurden. Der Rechnungshof fand keine Belege dafür, dass die Richtigkeit der gemeldeten Daten vom ECCC überprüft wurde. Auf der Grundlage seiner Prüfung der Projekte der Stichprobe ist der Rechnungshof der Auffassung, dass die gemeldeten Daten die erzielten Ergebnisse nicht angemessen widerspiegeln, da die meisten Werte fehlen oder fehlerhaft sind.

Dieser Bericht wurde von Kammer III unter Vorsitz von Herrn George-Marius Hyzler, Mitglied des Rechnungshofs, in ihrer Sitzung vom 16. Juni 2026 in Luxemburg angenommen.

Für den Rechnungshof

Tony Murphy
Präsident

Anhänge

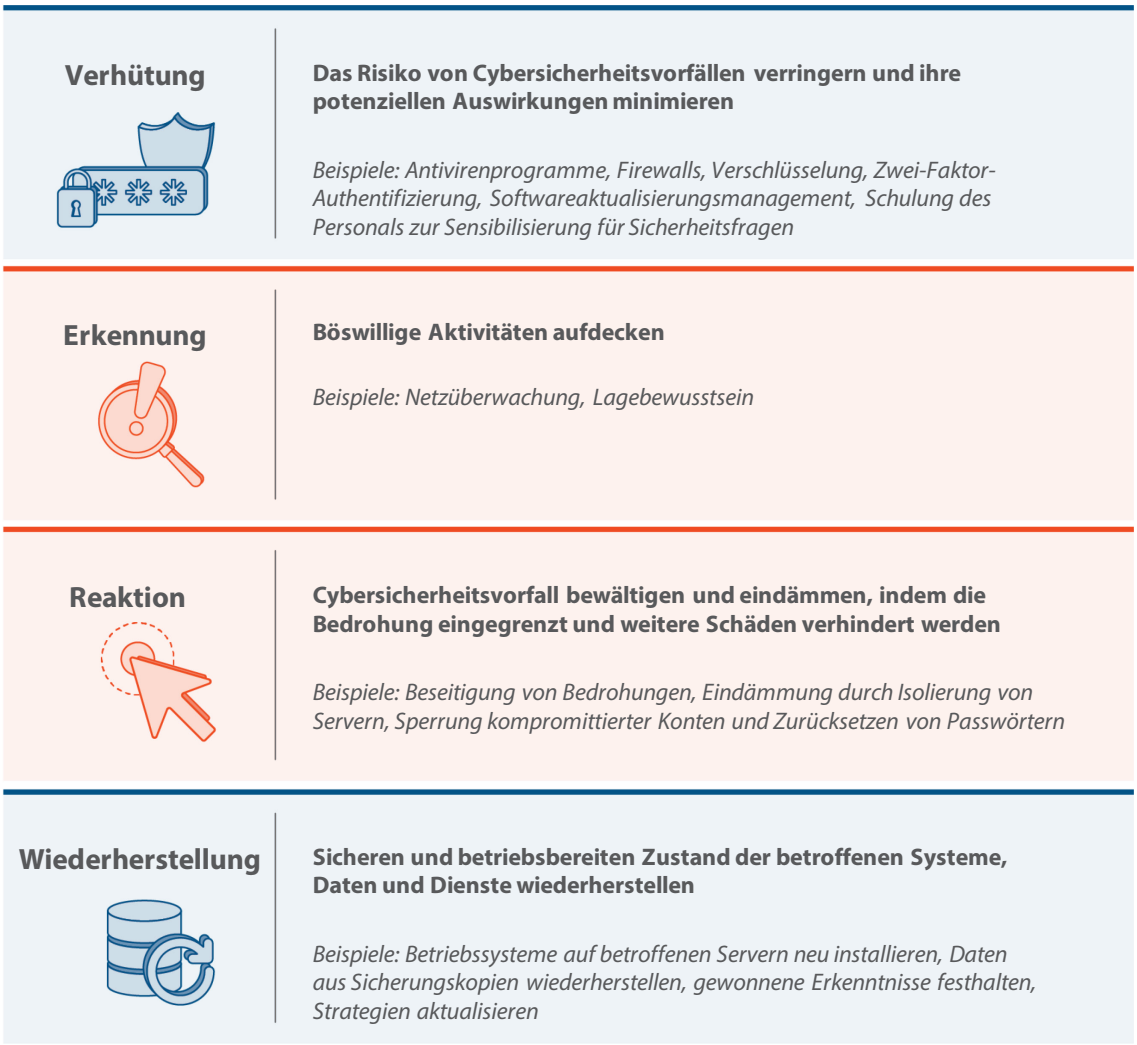
Anhang I – Über die Prüfung

01 Cybersicherheit bezeichnet "alle Tätigkeiten, die notwendig sind, um Netz- und Informationssysteme, die Nutzer solcher Systeme und andere von Cyberbedrohungen betroffene Personen zu schützen"[1]. Cyberbedrohung bezeichnet "einen möglichen Umstand, ein mögliches Ereignis oder eine mögliche Handlung, der/das/die Netz- und Informationssysteme, die Nutzer dieser Systeme und andere Personen schädigen, stören oder anderweitig beeinträchtigen könnte"[2]. Cybersicherheit erfordert einen ganzheitlichen Ansatz, bestehend aus einer Reihe miteinander verbundener Tätigkeiten zur Verhütung, Erkennung und Bewältigung von Cyberbedrohungen sowie zur anschließenden Wiederherstellung (siehe ***Abbildung 1***).

[1] Verordnung (EU) 2019/881 (Rechtsakt zur Cybersicherheit).

[2] Artikel 2 des Rechtsakts zur Cybersicherheit.

Abbildung 1 | Beispiele für Cybersicherheitsmaßnahmen

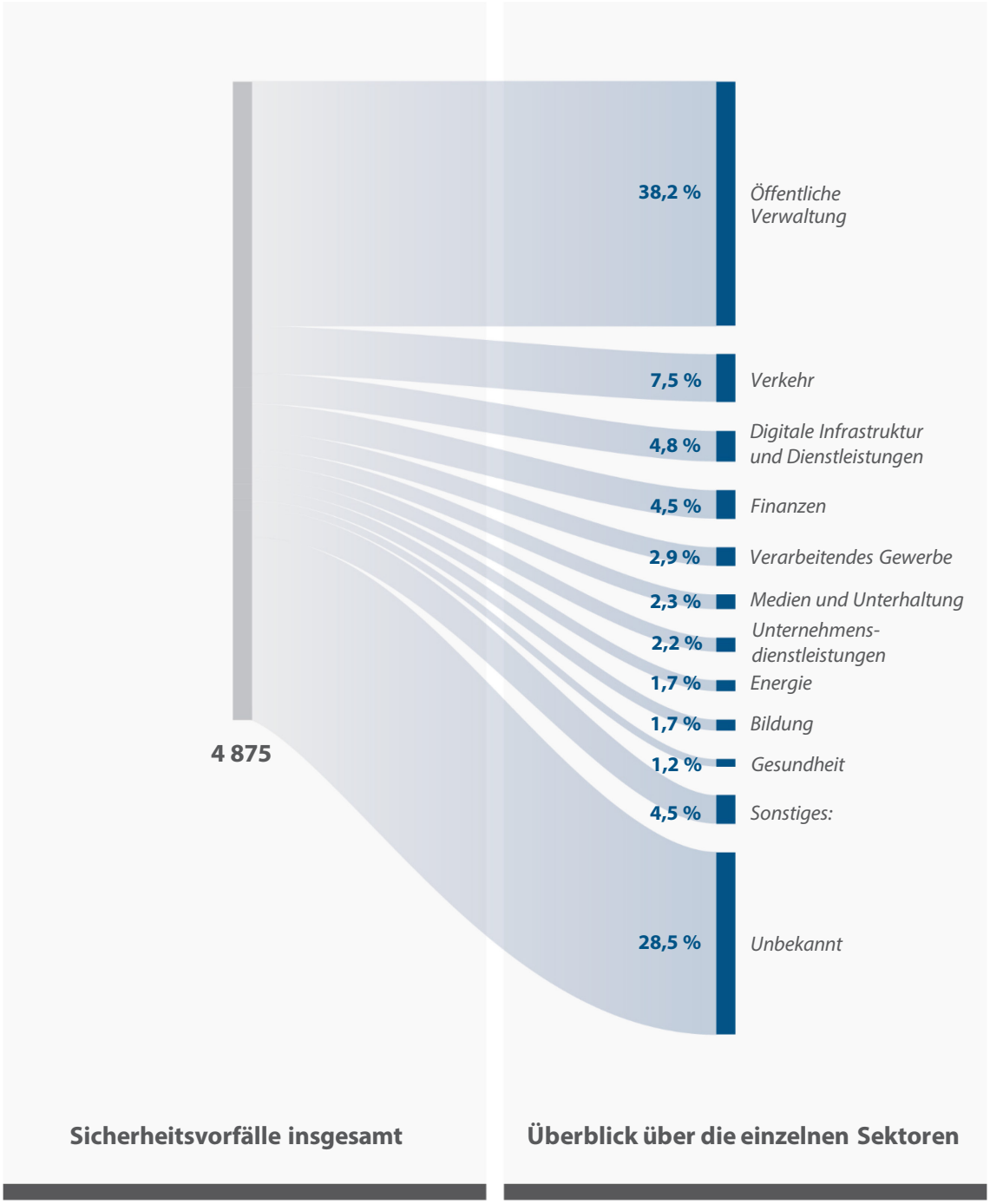


Quelle: Europäischer Rechnungshof auf der Grundlage von Erwägungsgrund 78 der Richtlinie (EU) 2022/2555 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau (NIS-2-Richtlinie).

02 Die Agentur der Europäischen Union für Cybersicherheit (ENISA) hält die Bedrohungslage im Bereich der Cybersicherheit für ernst und weist gleichzeitig darauf hin, dass die Cyberbedrohungslandschaft erheblich komplexer geworden ist und sich dieser Trend fortsetzt[3]. Diese Bedrohungen führen vor Augen, welche große Bedeutung der Cybersicherheit in zunehmend digitalen Volkswirtschaften und Gesellschaften zukommt. In ihrem Bericht zur Bedrohungslage für das Jahr 2025 stufte die ENISA Ransomware als die kritischste Bedrohung in der EU ein. ***Abbildung 2*** zeigt die betroffenen Sektoren.

[3] Bericht der ENISA über den Stand der Cybersicherheit in der Union 2024.

Abbildung 2 | Von Cyberangriffen betroffene Sektoren



Quelle: Europäischer Rechnungshof auf der Grundlage von Daten der ENISA.

Erhebliche Cybersicherheitsvorfälle und Cybersicherheitsvorfälle großen Ausmaßes

03 Cybersicherheitsvorfälle, einschließlich Cyberbedrohungen und unbeabsichtigter Ereignisse (siehe ***Abbildung 3*** und Ziffer ***40***), können "die Erbringung öffentlicher Dienstleistungen [und] die Ausübung wirtschaftlicher Tätigkeiten beeinträchtigen, erhebliche finanzielle Verluste verursachen, das Vertrauen der Nutzer untergraben und der Wirtschaft und den demokratischen Systemen der Union schweren Schaden zufügen und könnten sogar gesundheitliche oder lebensbedrohliche Folgen haben"[4]. Ein Cybersicherheitsvorfall gilt als[5]

- **erheblich**, wenn er schwerwiegende Betriebsstörungen der Dienste oder finanzielle Verluste für die betreffende Einrichtung verursacht hat oder verursachen kann oder wenn er andere natürliche oder juristische Personen durch erhebliche materielle oder immaterielle Schäden beeinträchtigt hat oder beeinträchtigen kann;

- von **großem Ausmaß**, wenn er eine Störung verursacht, deren Ausmaß die Reaktionsfähigkeit eines Mitgliedstaats übersteigt, oder beträchtliche Auswirkungen auf mindestens zwei Mitgliedstaaten hat.

04 Ein Cybersicherheitsvorfall großen Ausmaßes könnte sich verschärfen und zu einer **EU-weiten Cyberkrise entwickeln, die das reibungslose Funktionieren des Binnenmarkts verhindert oder ein ernsthaftes, die öffentliche Sicherheit betreffendes Risiko für** Einrichtungen und Bürger in mehreren Mitgliedstaaten oder in der gesamten Union darstellt[6].

---

[4] Erwägungsgrund 2 der Verordnung (EU) 2025/38 (Cybersolidaritätsverordnung).

[5] Artikel 6 und 23 der NIS-2-Richtlinie, näher ausgeführt in der Durchführungsverordnung (EU) 2024/2690 der Kommission für eine Reihe von Anbietern im Bereich der digitalen Infrastruktur.

[6] Erwägungsgrund 69 der NIS-2-Richtlinie.

Der politische Rahmen der EU

05 Das Cyberökosystem der EU ist komplex und vielschichtig und betrifft eine ganze Reihe interner Politikbereiche wie Justiz und Inneres, den digitalen Binnenmarkt und die Forschung[7]. In den Außenbeziehungen ist die Cybersicherheit ein Thema in der Diplomatie und zunehmend Teil der neu entstehenden Verteidigungspolitik der EU[8].

06 In den letzten Jahren hat die EU ihren Rechtsrahmen für die Cybersicherheit verstärkt. In ***Abbildung 3*** sind die wichtigsten Rechtsvorschriften und politischen Instrumente auf EU-Ebene aufgeführt. Im Einklang mit seinem Prüfungsumfang (siehe Ziffern ***13***–***14***) legte der Rechnungshof seinen Schwerpunkt auf Instrumente für die Erkennung von erheblichen Cybersicherheitsvorfällen und Cybersicherheitsvorfällen großen Ausmaßes und die Reaktion darauf.

---

[7] Themenpapier des Rechnungshofs zu den Herausforderungen für eine wirksame Cybersicherheitspolitik der EU, S. 13.

[8] Beispiele hierfür sind die Schlussfolgerungen des Rates zur Entwicklung der Cyberabwehr der Europäischen Union (2022), der Rahmen für eine koordinierte Reaktion der EU auf hybride Kampagnen (2022), die EU-Cyberabwehrpolitik (2023) und das überarbeitete Instrumentarium für die Cyberdiplomatie (2023).

Abbildung 3 | Relevante Rechtsvorschriften und politische Instrumente der EU

Quelle: Europäischer Rechnungshof.

Aufgaben und Zuständigkeiten

07 Die Cybersicherheitslandschaft der EU umfasst zahlreiche private und öffentliche Akteure auf regionaler, nationaler und EU-Ebene im zivilen Bereich, einschließlich Strafverfolgungsbehörden. Cybersicherheit ist ferner ein Schlüsselelement der nationalen Sicherheit und Verteidigung[9]. Die aktuelle Cybersicherheitslandschaft der EU wird in ***Anhang II*** veranschaulicht.

08 Die Mitgliedstaaten tragen die Hauptverantwortung für die Verhütung von, Vorsorge für und Bewältigung von Cybersicherheitsvorfällen und -krisen, die sie betreffen. Gemäß Artikel 4 Absatz 2 des Vertrags über die Europäische Union fällt die nationale Sicherheit weiterhin in die alleinige Verantwortung der einzelnen Mitgliedstaaten. Da Cybersicherheitsvorfälle kritische Informationsinfrastrukturen, von denen das reibungslose Funktionieren des Binnenmarkts abhängt, stören und schädigen könnten, kommt der EU im Falle von erheblichen Vorfällen oder Krisen ebenfalls eine wichtige Rolle zu[10]. Die wichtigsten Einrichtungen auf EU-Ebene sind in ***Abbildung 4*** dargestellt.

[9] Stellungnahme 02/2023 zur vorgeschlagenen Cybersolidaritätsverordnung.

[10] EU-Konzeptentwurf für das Cyberkrisenmanagement.

Abbildung 4 | Einrichtungen auf EU-Ebene mit einer Schlüsselrolle im Bereich der Cybersicherheit

Generaldirektion Kommunikationsnetze, Inhalte und Technologien (GD Connect)

zuständig für die Entwicklung und Umsetzung der EU-Cybersicherheitspolitik, einschließlich der Ausarbeitung einschlägiger Rechtsvorschriften und des Aufbaus der Cybersicherheitskapazitäten der EU

Agentur der Europäischen Union für Cybersicherheit (ENISA)

verfügt über ein umfassendes Mandat, ihr Hauptziel besteht jedoch darin, ein hohes gemeinsames Cybersicherheitsniveau in der gesamten EU zu erreichen

Europäisches Kompetenzzentrum für Cybersicherheit (ECCC)

wurde 2021 gegründet und ist für die Umsetzung der Cybersicherheitskomponente von DIGITAL und der einschlägigen Projekte im Rahmen von Horizont Europa zuständig

Rat der Europäischen Union

kann die Integrierte Regelung für die politische Reaktion auf Krisen aktivieren, um die politische Reaktion auf schwerwiegende Krisen auf EU-Ebene zu koordinieren

Quelle: Europäischer Rechnungshof.

EU-Finanzierung

09 Im Rahmen des derzeitigen mehrjährigen Finanzrahmens 2021–2027 ist das Programm "Digitales Europa" (DIGITAL) die wichtigste Finanzierungsquelle für die Cybersicherheit. Es wurde 2021 ins Leben gerufen und ist das erste EU-Programm, das speziell darauf abzielt, den digitalen Wandel in der EU voranzutreiben. Es verfügt über ein Gesamtbudget von 8,1 Milliarden Euro[11].

10 Unter dem Programm DIGITAL werden Cybersicherheitsmaßnahmen im Rahmen des spezifischen Ziels 3 – "Cybersicherheit und Vertrauen" finanziert. Konkret stehen 1,4 Milliarden Euro zur Verfügung, um

- die Koordinierung der Cybersicherheit zwischen den Instrumenten und der Dateninfrastruktur der Mitgliedstaaten zu stärken;
- eine breite Einführung der Cybersicherheitslösungen in allen Bereichen der Wirtschaft zu gewährleisten.

11 Der Großteil der im Rahmen von DIGITAL für Cybersicherheit verfügbaren Mittel wird über Aufforderungen zur Einreichung von Vorschlägen bereitgestellt, wobei zwischen November 2021 und Dezember 2025 zwölf Aufforderungen veröffentlicht wurden. Für diese Aufforderungen stehen EU-Mittel in Höhe von 825 Millionen Euro zur Verfügung. In den Jahren 2026 und 2027 sind neue Aufforderungen zur Einreichung von Vorschlägen geplant, durch die weitere 212 Millionen Euro an Finanzhilfen gewährt werden sollen.

12 Ein weiteres bedeutendes EU-Programm zur Förderung der Cybersicherheit ist Horizont Europa. Cybersicherheitsprojekte werden hauptsächlich im Rahmen des Clusters 3 – "Zivile Sicherheit für die Gesellschaft" – finanziert und stecken in der Regel noch in den Kinderschuhen, da der Schwerpunkt von Horizont Europa auf Forschung und Innovation liegt. Außerdem werden durch die Aufbau- und Resilienzfazilität Mittel für Cybersicherheitsmaßnahmen bereitgestellt.

[11] Programm "Digitales Europa".

Prüfungsumfang und Prüfungsansatz

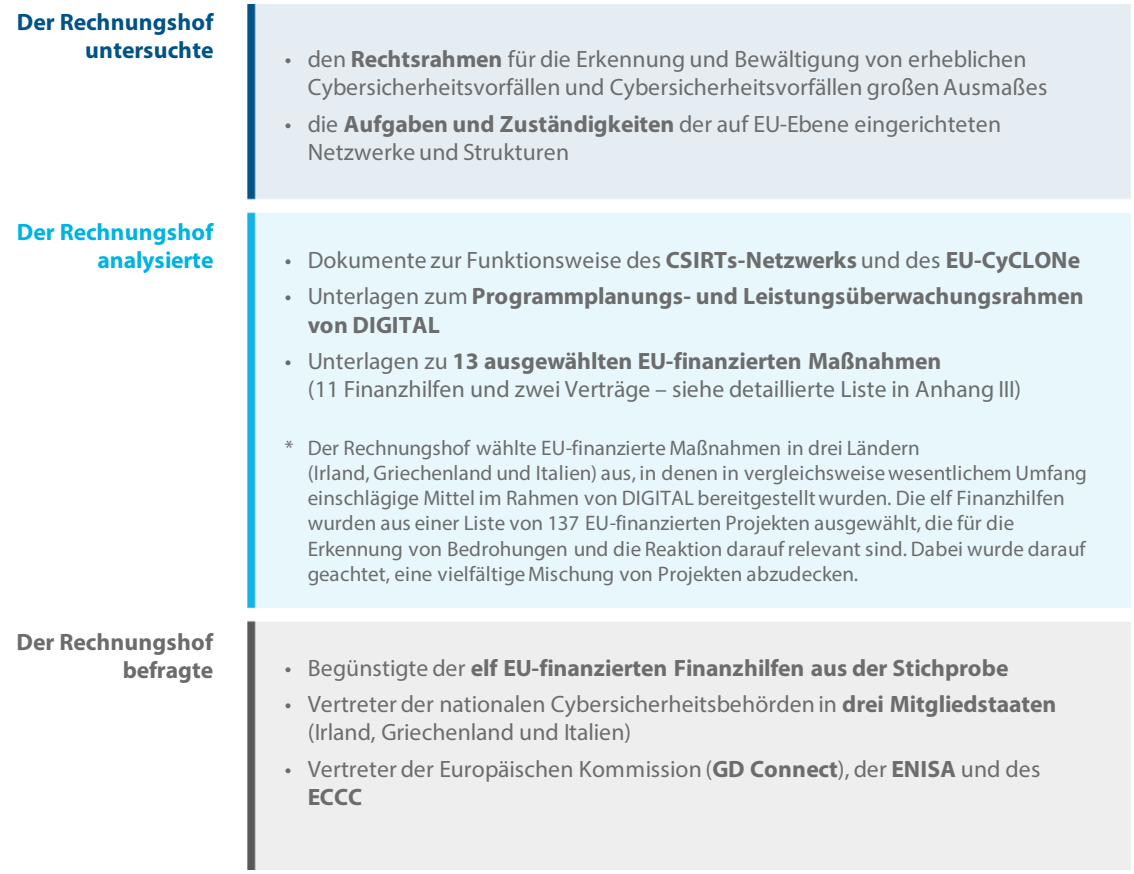
13 Die Zunahme von Cyberbedrohungen und ihre potenziellen Auswirkungen haben deutlich gemacht, dass die kollektive Cyberresilienz gestärkt werden muss. Ziel der Prüfung des Rechnungshofs war es, zu bewerten, ob die Maßnahmen der EU die Erkennung von erheblichen Cybersicherheitsvorfällen und Cybersicherheitsvorfällen großen Ausmaßes sowie die Reaktion darauf wirksam erleichtern. Insbesondere bewertete der Rechnungshof, ob dies zutrifft auf

- Netzwerke und Mechanismen auf EU-Ebene (und zwar das CSIRTs-Netzwerk, das EU-CyCLONe, das europäische Warnsystem für Cybersicherheit, das Cyber-Lagezentrum und die EU-Cybersicherheitsreserve);
- Maßnahmen, die im Rahmen von DIGITAL finanziert wurden.

Der Rechnungshof untersuchte weder die EU-weite Zusammenarbeit auf dem Gebiet der Strafverfolgung noch die auf EU-Ebene durch diplomatische Maßnahmen oder Verteidigungsmaßnahmen ergriffenen Tätigkeiten zur Cyberabschreckung.

14 Die Prüfung deckt den Zeitraum von 2022 bis 2025 ab. Sie stützt sich auf eine Aktenprüfung und Analyse einschlägiger Dokumente, Prüfbesuche in drei Mitgliedstaaten (Irland, Griechenland und Italien) sowie schriftliche Fragebögen und Befragungen einschlägiger Interessenträger. ***Abbildung 5*** zeigt, wie der Rechnungshof Belege einholte, um seine Bemerkungen zu untermauern.

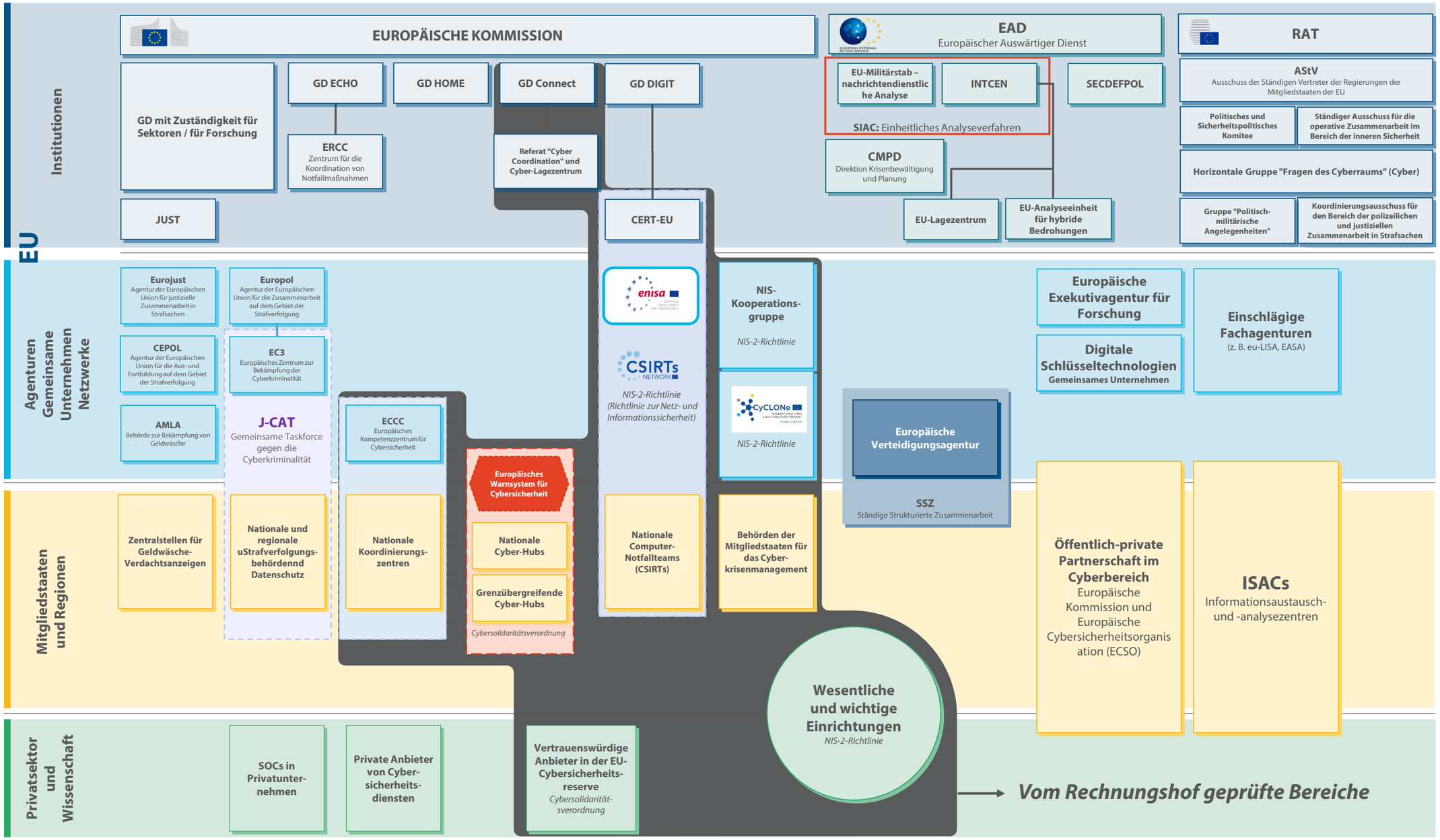
Abbildung 5 | Durchgeführte Prüftätigkeiten



Quelle: Europäischer Rechnungshof.

15 Der Rechnungshof geht davon aus, dass seine Feststellungen dazu beitragen werden, die Wirksamkeit und Effizienz der Erkennung und Reaktion der EU auf erhebliche Cybersicherheitsvorfälle und Cybersicherheitsvorfälle großen Ausmaßes sowie die Art und Weise, wie EU-finanzierte Maßnahmen ausgewählt und überwacht werden, zu verbessern. Die Prüfungsmethodik des Rechnungshofs entspricht den internationalen Prüfungsnormen der Internationalen Organisation der Obersten Rechnungskontrollbehörden (INTOSAI).

Anhang II – Die Cybersicherheitslandschaft der EU



GD Connect: Generaldirektion Kommunikationsnetze, Inhalte und Technologien
GD ECHO: Generaldirektion Europäischer Katastrophenschutz und humanitäre Hilfe
GD HOME: Generaldirektion Migration und Inneres
GD JUST: Generaldirektion Justiz und Verbraucher

GD DIGIT: Generaldirektion Digitale Dienste
EASA: Agentur der Europäischen Union für Flugsicherheit
EU-CyCLONe: Netzwerk der Verbindungsorganisationen für Cyberkrisen

eu-LISA: Agentur der Europäischen Union für das Betriebsmanagement von IT-Großsystemen im Raum der Freiheit, der Sicherheit und des Rechts
INTCEN: Zentrum der Europäischen Union für Informationsgewinnung und Lageerfassung

SECDEFPOL: Direktion Sicherheits- und Verteidigungspolitik
SOC: Sicherheitseinsatzzentrum

Anhang III – Ausgewählte Cybersicherheitsmaßnahmen

Nr.	Bezeichnung	Land/Länder	Projektbeginn	Projektende	Gesamtkosten (in Millionen Euro) und EU-Beitrag (in %)	Link zum Förder- und Ausschreibungsportal der EU
Finanzhilfen für grenzübergreifende Cyber-Hubs, die Teil des europäischen Warnsystems für Cybersicherheit sind						
1	**Einrichtung grenzübergreifender Sicherheitseinsatzzentren (ATHENA)**	Bulgarien, Griechenland, Zypern, Malta	1.1.2024	31.3.2028	4,7 (50 %)	
2	**GRENZÜBERGREIFENDE PLATTFORM ENSOC (ENSOC)**	Spanien, Italien, Luxemburg, Niederlande, Österreich, Portugal, Rumänien	1.1.2024	30.6.2028	10,4 (50 %)	
Finanzhilfen für den Aufbau des Netzwerks nationaler Koordinierungszentren (NCCs) in den Mitgliedstaaten						
3	**Entwicklung und Umsetzung des nationalen Zentrums für die Koordinierung und Entwicklung der Cybersicherheit für Irland (NCC-IE)**	Irland	2.10.2023	1.10.2026	4,2 (47 %)	
4	**Italienisches nationales Koordinierungszentrum (NCC-IT)**	Italien	1.11.2023	31.10.2025	2,0 (50 %)	

Nr.	Bezeichnung	Land/Länder	Projektbeginn	Projektende	Gesamtkosten (in Millionen Euro) und EU-Beitrag (in %)	Link zum Förder- und Ausschreibungsportal der EU
Finanzhilfen für den Aufbau der Kapazitäten von Sicherheitseinsatzzentren (SOCs), die Förderung neuartiger Anwendungen von KI und anderer grundlegender Technologien für SOCs sowie die Bereitstellung von Unterstützung bei der Abwehrbereitschaft und gegenseitiger Unterstützung						
5	**Ausbau der Kapazitäten des konsolidierten Sicherheitseinsatzzentrums Griechenlands (EL-SOC)**	Griechenland, Zypern	1.1.2024	31.12.2026	9,7 (50 %)	
6	**Griechisches Sicherheitseinsatzzentrum für kleine und mittlere Unternehmen (GR-SME-SOC)**	Griechenland	1.1.2024	31.12.2026	12,1 (50 %)	
7	**Sicherheitseinsatzzentren der nächsten Generation (NG-SOC)**	Griechenland, Spanien, Zypern, Luxemburg, Slowenien, Norwegen	1.1.2024	31.12.2026	4,8 (50 %)	
8	**Irisches Sicherheitseinsatzzentrum für lokale Behörden (ILG-SOC)**	Irland	1.10.2023	30.9.2026	8,3 (50 %)	
9	**Ein verflochtenes Ökosystem von Netzwerken für die Koordinierung und Reaktion im Bereich der Cybersicherheit (Cyber-CORE-Netzwerk)**	Irland	1.1.2024	31.12.2026	3,6 (50 %)	
10	**Harmonisierung von Menschen, Prozessen und Technologien für eine robuste Cybersicherheit (CYberSynchrony)**	Belgien, Griechenland, Italien, Zypern, Niederlande	1.6.2024	31.5.2027	7,0 (100 %)	
11	**Fortschrittliche kooperative Sicherheitseinsatzzentren (ACSOC)**	Griechenland, Italien, Rumänien	1.1.2025	31.12.2027	3,0 (50 %)	

Nr.	Bezeichnung	Land/Länder	Projektbeginn	Projektende	Gesamtkosten (in Millionen Euro) und EU-Beitrag (in %)	Link zum Förder- und Ausschreibungsportal der EU
Rahmenvertrag für die Aktion zur Förderung der Cybersicherheit der ENISA						
12	**Unterstützung der ENISA bei der Erbringung von Diensten im Rahmen der Aktion zur Förderung der Cybersicherheit (28 Lose)**	27 Lose für die Mitgliedstaaten ein gesamteuropäisches Los	1.12.2022[1]	31.12.2025	28,3 (100 %)	
Dienstleistungsauftrag für das Cyber-Lagezentrum der GD Connect						
13	**Maßgeschneiderter Dienst zur Unterstützung des Cyber-Lage- und Analysezentrums der Europäischen Kommission**	-	30.12.2022	30.12.2026	18,0 (100 %)	

Quelle: Europäischer Rechnungshof.

[1] Im Dezember 2022 wurden mehrere Verträge unterzeichnet.

Anhang IV – Bewertung von EU-finanzierten Cybersicherheitsprojekten durch den Rechnungshof

Zufriedenstellend *Einige Schwachstellen*
Nicht zufriedenstellend *Schlussfolgerung nicht möglich (zu früh)*

Nr.	Projekt	Mit dem Projekt wird der in der Aufforderung zur Einreichung von Vorschlägen ermittelte Bedarf größtenteils gedeckt	Die geplanten Outputs und Ergebnisse des Projekts wurden bisher erreicht	Die Outputs des Projekts wurden fristgerecht erbracht	Die Leistungsindikatoren des Projekts sind relevant und messbar und haben sowohl einen Ausgangs- als auch einen Zielwert
1	Einrichtung grenzübergreifender SOCs (ATHENA)	Zufriedenstellend	Nicht zufriedenstellend	Nicht zufriedenstellend	Nicht zufriedenstellend
2	GRENZÜBERGREIFENDE PLATTFORM ENSOC (ENSOC)	Zufriedenstellend	Nicht zufriedenstellend	Nicht zufriedenstellend	Nicht zufriedenstellend
3	Entwicklung und Umsetzung des nationalen Zentrums für die Koordinierung und Entwicklung der Cybersicherheit für Irland (NCC-IE)	Zufriedenstellend	Zufriedenstellend	Einige Schwachstellen	Einige Schwachstellen
4	Italienisches nationales Koordinierungszentrum (NCC-IT)	Zufriedenstellend	Zufriedenstellend	Zufriedenstellend	Einige Schwachstellen
5	Ausbau der Kapazitäten des konsolidierten Sicherheitseinsatzzentrums Griechenlands (EL-SOC)	Zufriedenstellend	Einige Schwachstellen	Nicht zufriedenstellend	Nicht zufriedenstellend
6	Griechisches Sicherheitseinsatzzentrum für kleine und mittlere Unternehmen (GR-SME-SOC)	Zufriedenstellend	Zufriedenstellend	Zufriedenstellend	Einige Schwachstellen
7	Sicherheitseinsatzzentren der nächsten Generation (NG-SOC)	Zufriedenstellend	Zufriedenstellend	Zufriedenstellend	Einige Schwachstellen
8	Irisches Sicherheitseinsatzzentrum für lokale Behörden (ILG-SOC)	Zufriedenstellend	Nicht zufriedenstellend	Nicht zufriedenstellend	Nicht zufriedenstellend
9	Ein verflochtenes Ökosystem von Netzwerken für die Koordinierung und Reaktion im Bereich der Cybersicherheit (Cyber-CORE-Netzwerk)	Zufriedenstellend	Einige Schwachstellen	Einige Schwachstellen	Einige Schwachstellen
10	Harmonisierung von Menschen, Prozessen und Technologien für eine robuste Cybersicherheit (CYberSynchrony)	Einige Schwachstellen	Schlussfolgerung nicht möglich (zu früh)	Schlussfolgerung nicht möglich (zu früh)	Einige Schwachstellen
11	Fortschrittliche kooperative Sicherheitseinsatzzentren (ACSOC)	Zufriedenstellend	Schlussfolgerung nicht möglich (zu früh)	Schlussfolgerung nicht möglich (zu früh)	Nicht zufriedenstellend

Abkürzungen

Abkürzung	Definition/Erklärung
CSIRT	*Computer Security Incident Response Team* (Reaktionsteam für Computersicherheitsverletzungen)
DIGITAL	Programm "Digitales Europa"
ECCC	*European Cybersecurity Competence Centre* (Europäisches Kompetenzzentrum für Cybersicherheit)
ENISA	*European Union Agency for Cybersecurity* (Agentur der Europäischen Union für Cybersicherheit)
EU-CyCLONe	*European Cyber Crisis Liaison Organisation Network* (Netzwerk der Verbindungsorganisationen für Cyberkrisen)
GD Connect	Generaldirektion Kommunikationsnetze, Inhalte und Technologien
KMU	kleine und mittlere Unternehmen
NCC	*National coordination centre* (nationales Koordinierungszentrum)
NIS	Netz- und Informationssicherheit
SOC	*Security operations centre* (nationales Sicherheitseinsatzzentrum)

Glossar

Begriff	Definition/Erklärung
Bedrohungsakteure	Einzelpersonen oder Gruppen, die vorsätzlich Schaden anrichten, Dienste stören oder Daten stehlen, indem sie Schwachstellen in IT-Systemen, -Netzwerken und -Geräten ausnutzen.
Cyberbedrohung	potenzielle Nutzung des Cyberraums zur Beeinträchtigung der Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit von Daten oder Informationssystemen.
Cyber-Hub	zentrale Plattform, auf der verschiedene Dienste, Instrumente und IT-Experten zusammengeführt werden, um die Überwachung, Erkennung und Analyse von Cyberbedrohungen zu verbessern, Cybersicherheitsvorfälle zu verhindern und die Gewinnung von Erkenntnissen in Bezug auf Cyberbedrohungen zu unterstützen.
Cybersicherheitsvorfall	Ereignis, das die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit von Daten oder Informationssystemen beeinträchtigt.
Cybersicherheitsvorfall großen Ausmaßes	Sicherheitsvorfall, der entweder zu erheblich ist, als dass ein Mitgliedstaat ihn allein bewältigen könnte, oder beträchtliche Auswirkungen auf mindestens zwei Mitgliedstaaten hat.
Erheblicher Cybersicherheitsvorfall	Cybersicherheitsvorfall, der schwerwiegende Störungen oder finanzielle Verluste für eine Organisation oder beträchtliche Schäden für andere Einrichtungen oder Einzelpersonen verursacht hat oder verursachen kann.
Ransomware	Schadprogramm, das den Opfern den Zugang zu einem Computersystem verwehrt oder Dateien durch Verschlüsselung unlesbar macht, üblicherweise, um von den Opfern ein Lösegeld zu erzwingen, damit der Zugang wiederhergestellt wird.
Sicherheitseinsatzzentrum	Organisationseinheit, die sich für die Verhütung von Cyberbedrohungen und -vorfällen einsetzt und damit zusammenhängende Erkenntnisse erhebt.
Taxonomie	Klassifizierungssystem (im Bereich der Cybersicherheit), das verwendet wird, um Wissen über Schlüsselbegriffe wie Bedrohungen und Sicherheitsvorfälle zu organisieren, zu kategorisieren und zu strukturieren.

Antworten der Kommission

https://www.eca.europa.eu/de/publications/SR-2026-19

Antworten des Europäischen Kompetenzzentrums für Cybersicherheit (ECCC)

https://www.eca.europa.eu/de/publications/SR-2026-19

Antworten der Agentur der Europäischen Union für Cybersicherheit (ENISA)

https://www.eca.europa.eu/de/publications/SR-2026-19

Zeitplan

https://www.eca.europa.eu/de/publications/SR-2026-19

Prüfungsteam

Die Sonderberichte des Rechnungshofs enthalten die Ergebnisse seiner Prüfungen zu Politikbereichen und Programmen der Europäischen Union oder zu Fragen des Finanzmanagements in spezifischen Haushaltsbereichen. Bei der Auswahl und Gestaltung dieser Prüfungsaufgaben ist der Rechnungshof darauf bedacht, maximale Wirkung dadurch zu erzielen, dass er die Risiken für die Wirtschaftlichkeit oder Regelkonformität, die Höhe der betreffenden Einnahmen oder Ausgaben und künftige Entwicklungen sowie das politische und öffentliche Interesse abwägt.

Diese Wirtschaftlichkeitsprüfung wurde von Prüfungskammer III "Externe Politikbereiche, Sicherheit und Justiz" unter Vorsitz von George-Marius Hyzler, Mitglied des Rechnungshofs, durchgeführt. Die Prüfung stand unter der Leitung von George-Marius Hyzler, Mitglied des Rechnungshofs. Herr Hyzler wurde unterstützt von seinem Kabinettchef Romuald Kayibanda, der Attachée Annette Farrugia, dem Leitenden Manager Cyril Messein, dem Aufgabenleiter Frédéric Soblet sowie den Prüfern Jurgen Manjé und Flavia Di Marco. Zoe Amador Martínez leistete sprachliche Unterstützung. Dunja Weibel leistete Unterstützung bei der grafischen Gestaltung.

Von links nach rechts: Frédéric Soblet, Romuald Kayibanda, George-Marius Hyzler, Jurgen Manjé, Cyril Messein.

URHEBERRECHTSHINWEIS

HTML	ISBN 978-92-849-7855-7	ISSN 1977-5644	doi:10.2865/7324077	QJ-01-26-032-DE-Q
PDF	ISBN 978-92-849-7856-4	ISSN 1977-5644	doi:10.2865/8965887	QJ-01-26-032-DE-N

ZITIERHINWEIS

Europäischer Rechnungshof, Sonderbericht 19/2026 "Erkennung und Bewältigung von Cybersicherheitsvorfällen: Beim Kooperationsrahmen der EU sind Fortschritte zu verzeichnen, doch ist er wegen Verzögerungen bei der Umsetzung und eines begrenzten Informationsaustauschs nur bedingt wirksam", Amt für Veröffentlichungen der Europäischen Union, 2026.

In den letzten Jahren hat die EU ihren Regelungsrahmen für die Cybersicherheit gestärkt und verschiedene Netzwerke und Mechanismen eingerichtet, um Cybersicherheitsvorfälle zu bewältigen. Die EU finanziert auch Cybersicherheitsprojekte im Rahmen des Programms "Digitales Europa".

Die Prüfung des Rechnungshofs ergab, dass die Maßnahmen der EU die Erkennung von erheblichen Cybersicherheitsvorfällen und Cybersicherheitsvorfällen großen Ausmaßes sowie die Reaktion darauf nur teilweise erleichtern. Zwar wurde schrittweise ein Kooperationsrahmen geschaffen, doch die vollständige Ausgestaltung ist noch nicht abgeschlossen. Aufgrund des begrenzten Informationsaustauschs und angesichts von Schwachstellen bei der Berichterstattung und erheblichen Verzögerungen bei der Umsetzung kann das Potenzial der EU-Netzwerke und -Mechanismen nicht voll ausgeschöpft werden. Mit den Projekten werden relevante Ziele verfolgt, doch mehrere Projekte sind mit operativen Herausforderungen und Verzögerungen konfrontiert. Ferner weist der allgemeine Rahmen für die Leistungsüberwachung Schwächen auf. Der Rechnungshof legt Empfehlungen zur Behebung dieser Mängel vor.

Sonderbericht des Hofes gemäß Artikel 287 Absatz 4 Unterabsatz 2 AEUV.

EUROPÄISCHER RECHNUNGSHOF

Amt für Veröffentlichungen der Europäischen Union

EUROPÄISCHER RECHNUNGSHOF
12, rue Alcide De Gasperi
1615 Luxembourg
LUXEMBURG

Tel. (+352) 4398-1

Kontaktformular: eca.europa.eu/de/contact
Website: eca.europa.eu
Soziale Netzwerke: @EUauditors