EUROPÄISCHE
KOMMISSION

Straßburg, den 20.1.2026
SWD(2026) 12 final

ARBEITSUNTERLAGE DER KOMMISSIONSDIENSTSTELLEN

BERICHT ÜBER DIE FOLGENABSCHÄTZUNG (ZUSAMMENFASSUNG)

Begleitunterlage zum

Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die Agentur der Europäischen Union für Cybersicherheit (ENISA), den europäischen Rahmen für die Cybersicherheitszertifizierung und die Sicherheit der IKT-Lieferketten sowie zur Aufhebung der Verordnung (EU) 2019/881 (Cybersicherheitsverordnung 2)

und

Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates zur Änderung der Richtlinie (EU) 2022/2555 im Hinblick auf Vereinfachungsmaßnahmen und die Angleichung an den [Vorschlag für die Cybersicherheitsverordnung 2]

{COM(2026) 11 final} - {SEC(2026) 11 final} - {SWD(2026) 11 final}

Zusammenfassung der Folgenabschätzung

Ziel

Das vorrangige Ziel dieser Folgenabschätzung ist die Bewertung der Angemessenheit der derzeitigen Vorschriften zur Bewältigung sich wandelnder Cybersicherheitsbedrohungen in der EU. Darin wird eine Reihe integrierter politischer Optionen vorgeschlagen, die die Stärkung der Agentur der Europäischen Union für Cybersicherheit (ENISA), die Reform des europäischen Rahmens für die Cybersicherheitszertifizierung (ECCF) und die Vereinfachung der Einhaltung von Vorschriften des bestehenden Rechtsrahmens für Cybersicherheit zum Ziel haben. Durch diese Folgenabschätzung wird unterstrichen, wie wichtig es ist, die Cyber-Governance anzupassen, um sie mit dem technologischen Fortschritt und den Marktanforderungen in Einklang zu bringen und gleichzeitig die Wettbewerbsfähigkeit sicherzustellen und die Umweltauswirkungen zu berücksichtigen.

Problembeschreibung

Trotz laufender Bemühungen ist die Cybersicherheitslandschaft der EU angesichts zunehmend komplexer Bedrohungen weiterhin erheblichen Herausforderungen ausgesetzt. Ein effizientes Cybersicherheitsmanagement wird durch die unzureichende Koordinierung zwischen den Mitgliedstaaten und anderen Akteuren auf EU-Ebene, die stagnierende Umsetzung politischer Instrumente und regulatorische Hürden und Komplexitäten behindert. Durch diese Probleme erhöhen sich die Kosten für Unternehmen und Behörden, steigt das Risiko für Cybervorfälle und bleibt das Schutzniveau für die Bürgerinnen und Bürger uneinheitlich.

Rechtfertigung für das Handeln der EU

Cybersicherheitsbedrohungen gehen über nationale Grenzen hinaus; daher ist ein einheitlicher Ansatz für eine entschlossene Reaktion von entscheidender Bedeutung. Eine Intervention auf EU-Ebene gewährleistet einen einheitlichen Schutz, verbessert die Wettbewerbsfähigkeit, indem gleiche Wettbewerbsbedingungen geschaffen werden, und erleichtert den freien Verkehr digitaler Dienste und Produkte im Binnenmarkt. Die Harmonisierung auf EU-Ebene verringert auch den Verwaltungsaufwand durch eine vereinfachte Einhaltung von Vorschriften und gestraffte Verfahren.

Politische Optionen und bevorzugte Option

In diesem Bericht werden vier Interventionsbereiche analysiert, jeder davon mit einer Reihe politischer Optionen, die im Hinblick auf die zu erreichenden spezifischen Ziele betrachtet werden: 1) das Mandat der ENISA (auch Teil des derzeitigen Rechtsakts zur Cybersicherheit), 2) den ECCF (auch Teil des derzeitigen Rechtsakts zur Cybersicherheit) und 3) gezielte Änderungen der NIS-2-Richtlinie mit dem Ziel der Vereinfachung, wobei dieser Punkt auch mit dem Mandat der ENISA und dem ECCF verknüpft ist. Die einzelnen Bündel an Optionen stellen einen jeweils eigenen Interventionsbereich dar, sind aber gleichzeitig miteinander verknüpft und füreinander relevant.

Optionen zur Beseitigung der Diskrepanz zwischen dem politischen Rahmen der EU für die Cybersicherheit und den Bedürfnissen der Interessenträger in einer zunehmend feindseligen Umgebung

Option A.1: *Präzisierung des Mandats der ENISA und Festlegung von Prioritäten* – Mit dieser Option würde ein klarer, stabiler Rahmen für die Aufgaben der ENISA sichergestellt, indem die in anderen Rechtsvorschriften enthaltenen Aufgaben in diesen Rechtsakt aufgenommen würden.

Option A.2: *Reform des Mandats der ENISA* – Mit dieser Option würde der Rechtsakt zur Cybersicherheit aufgehoben und ersetzt und dadurch das Mandat der Agentur neu gefasst.

Option A.3: *Reform des Mandats der ENISA mit besonderem Augenmerk auf operative Unterstützung* – Diese Option würde auf Option A.2 aufbauen. Darüber hinaus würde die ENISA Fähigkeiten entwickeln, um Einrichtungen gemäß der NIS-2-Richtlinie auf Ersuchen eines Mitgliedstaats bei der Reaktion auf Cybersicherheitsvorfälle und der Wiederherstellung danach unmittelbar zu unterstützen.

Optionen für den europäischen Zertifizierungsrahmen für die Cybersicherheit

Option B.1: *Klarstellung des Umfangs, der Elemente und Ziele des ECCF und Einführung eines Mechanismus für die Systempflege* – Mit dieser Option wird ein neuer, von der ENISA umzusetzender Mechanismus für die Pflege der Systeme nach ihrer Annahme geschaffen.

Option B.2: *Reform des ECCF durch Überarbeitung der Verfahren und Ausweitung des Umfangs, um die Einhaltung von Vorschriften zu erleichtern* – Mit dieser Option würde der Rechtsakt zur Cybersicherheit aufgehoben und durch eine neue Verordnung ersetzt. Zusätzlich zu Option B.1 würden das Verfahren im Zusammenhang mit der Inauftraggabe, Entwicklung und Annahme von Systemen überarbeitet, um die Rechenschaftspflicht und Effizienz zu verbessern.

Option B.3: *Reform des ECCF gemäß Option B.2 plus Einführung einer obligatorischen Zertifizierung für Cyberabwehr* – Diese Option würde auf Option B.2 aufbauen, aber auch darauf abzielen, die Wirkung des Rahmens weiter zu stärken, indem eine obligatorische Zertifizierung für wesentliche Einrichtungen unter der NIS-2-Richtlinie eingeführt würde, bei der spezifische Risikoszenarien berücksichtigt würden, anstatt sich ausschließlich auf die freiwillige Zertifizierung von Einrichtungen zu verlassen.

Optionen zur Vereinfachung

Option C.1: *Verfolgung eines Soft-Law-Ansatzes und der Anwendung nichtlegislativer Instrumente, einschließlich der Nutzung bestehender Befugnisübertragungen (Erlass von Durchführungsrechtsakten gemäß Artikel 21 Absatz 5 und Artikel 23 Absatz 11 der NIS-2-Richtlinie)* – Diese Option beinhaltet den Erlass von Durchführungsrechtsakten auf der Grundlage bestehender Befugnisübertragungen im Rahmen der NIS-2-Richtlinie, um für mehr Harmonisierung bei den Risikomanagementmaßnahmen im Bereich der Cybersicherheit, bei den Schwellenwerten für die Meldung von Sicherheitsvorfällen und der Informationen,

Formate und Verfahren für Meldungen sowie der Annahme einer Reihe von Leitlinien zur Verbesserung der Rechtssicherheit und der harmonisierten Umsetzung zu sorgen.

Option C.2: *Gezieltes Tätigwerden – weitere Vereinfachung der Einhaltung des einschlägigen Rechtsrahmens der Union für die Cybersicherheit* – Diese Option beinhaltet ein begrenztes Tätigwerden durch Änderungen des Rechtsakts zur Cybersicherheit und der NIS-2-Richtlinie mit dem Ziel, bestimmte Aspekte des Cybersicherheitsrahmens zu vereinfachen, einschließlich Anpassungen des Umfangs, einer größtmöglichen Harmonisierung bei Durchführungsrechtsakten, des Nachweises der Rechtsbefolgung durch Zertifizierung und der Annahme einer Reihe von Leitlinien, wie unter Option C1 vorgesehen.

Option C.3: *Harmonisierung der in den Unionsvorschriften enthaltenen Maßnahmen im Bereich der Cybersicherheit* – Diese Option würde auf Option C.2 aufbauen und alle Risikomanagementmaßnahmen im Bereich der Cybersicherheit oder Befugnisübertragungen im Zusammenhang mit solchen Maßnahmen in sektoralen Rechtsvorschriften entfernen. Stattdessen würde das Ökosystem der NIS-2-Richtlinie geändert, um gestraffte Anforderungen für alle Arten von Einrichtungen festzulegen und so für mehr Harmonisierung zu sorgen.

Optionen für die Sicherheit der IKT-Lieferketten

Option D.1: Verfolgung eines *Soft-Law-Ansatzes zur Reaktion auf Cybersicherheitsrisiken in den IKT-Lieferketten* – Bei dieser Option würden auf EU-Ebene keine Regulierungsmaßnahmen ergriffen. Stattdessen würde die Kommission die Zahl der koordinierten Risikobewertungen und der freiwilligen Instrumentarien erhöhen.

Option D.2: *Ad-hoc-Regulierungsmaßnahmen zur Kodifizierung des 5G-Instrumentariums* – Mit dieser Option würden die Maßnahmen zum 5G-Instrumentarium kodifiziert. Dadurch würden die Mitgliedstaaten verpflichtet, dafür zu sorgen, dass in wichtigen Assets des Netzes keine Komponenten von Hochrisikoanbietern verwendet werden.

Option D.3: *Umfassender horizontaler Rahmen, um den Cybersicherheitsrisiken in den IKT-Lieferketten zu begegnen* – Mit dieser Option würde ein horizontaler, technologie- und branchenneutraler Regelungsrahmen geschaffen, um nicht technischen Cybersicherheitsrisiken in den IKT-Lieferketten zu begegnen.

Nach eingehender Analyse umfasst das bevorzugte Maßnahmenpaket: Option A.2 – Reform des Mandats der ENISA, Option B.2 – Reform des ECCF durch Überarbeitung der Verfahren und Ausweitung des Umfangs, um die Einhaltung von Vorschriften zu erleichtern, Option C.2 – gezieltes Tätigwerden – weitere Vereinfachung der Einhaltung des einschlägigen Rechtsrahmens der Union für die Cybersicherheit und Option D.3 – umfassender horizontaler Rahmen, um den Cybersicherheitsrisiken in den IKT-Lieferketten zu begegnen.

Diese Kombination bietet eine ausgewogene Antwort auf die ermittelten politischen Herausforderungen und verbessert die Wirksamkeit, Effizienz und Kohärenz in der gesamten EU erheblich.

Wesentliche Auswirkungen

Kosten-Nutzen-Analyse: Die Umsetzung des vorgeschlagenen Regelungsrahmen wird Kosten verursachen, sowohl für die ENISA, die über einen Zeitraum fünf Jahren schätzungsweise bis zu 161,3 Mio. EUR zur Erfüllung ihrer neuen Aufgaben benötigt, als auch für die Behörden in der gesamten EU, die Kosten von bis zu 80 Mio. EUR über einen Zeitraum von fünf Jahren für die Beaufsichtigung tragen müssen (unter Berücksichtigung der relevanten Kosteneinsparungen). Was die Unternehmen betrifft, so könnte die schrittweise Aussonderung bestimmter Hochrisikoausrüstungen über einen Übergangszeitraum von drei Jahren zu jährlichen Kosten von 3,4 bis 4,3 Mrd. EUR für Mobilfunknetzbetreiber führen, während die Investitionen in vertrauenswürdige Anbieter zugleich auf bis zu 2 Mrd. EUR pro Jahr steigen könnten. Darüber hinaus dürften gestraffte und reduzierte Pflichten zur Einhaltung von Vorschriften zu Kosteneinsparungen von bis zu 14,6 Mrd. EUR für Unternehmen führen. Ferner würden sich aus der Verbesserung der allgemeinen Cyberabwehr und der technologischen Souveränität der EU sowie aus der Förderung von Innovation und Wettbewerbsfähigkeit erhebliche Vorteile für die Bürgerinnen und Bürger, die Behörden und die Unternehmen ergeben, die die anfänglich entstehenden Ausgaben langfristig weitgehend ausgleichen dürften.

Wettbewerbsfähigkeit: Durch weniger Marktfragmentierung und eine harmonisierte Regulierung sorgen die bevorzugten Optionen für fairere Wettbewerbsbedingungen in der gesamten EU und bieten den Unternehmen klarere Perspektiven für die Einhaltung von Vorschriften und Innovationen.

Prüfung der Klimaverträglichkeit: In der Folgenabschätzung wurden die möglichen Umweltauswirkungen jeder Option berücksichtigt. Besonderes Augenmerk galt der Energieeffizienz, den Emissionen im Zuge von Reisen und der Konsolidierung von Infrastruktur. Die bevorzugten Optionen A.2, B.2 und C.2 haben begrenzte Umweltauswirkungen und Option D.3 trägt der Umweltneutralität Rechnung, indem der Produktlebenszyklus und die Übergangszeiträumen für den Ersatz wichtiger Assets berücksichtigt werden. Dies steht im Einklang mit dem Engagement der EU für Nachhaltigkeit.

„Standardmäßig digital“: Die Konzentration auf straffere digitale Prozesse zeigt, dass sich die EU für einen Zuerst-digital-Ansatz einsetzt, der einen schnelleren und zuverlässigeren Datenaustausch und eine schnellere und zuverlässigere Entscheidungsfindung gewährleistet. Option D.3 könnte auch große Auswirkungen auf die Digitalisierung haben, da Komponenten ersetzt würden, die von Einrichtungen stammen, die in Drittländern, für die Cybersicherheitsbedenken bestehen, niedergelassen sind oder von Einrichtungen in solchen Drittländern kontrolliert werden.

Vereinfachung und Verringerung des Verwaltungsaufwands: Die bevorzugten Optionen tragen durch die Präzisierung des Anwendungsbereichs und die Einführung von Maßnahmen zur Straffung der Einhaltung der Vorschriften und der Überwachung zur Vereinfachung bei und verringern so den Verwaltungsaufwand. Der One-in-one-out-Grundsatz wird erwogen, da

so sichergestellt wird, dass neue Verpflichtungen durch den Wegfall von Verpflichtungen an anderer Stelle ausgeglichen werden.

Fazit

Diese Folgenabschätzung enthält eine umfassende Strategie zur Verbesserung der Cybersicherheit der EU, zur Beseitigung regulatorischer Ineffizienzen und zur Vorbereitung der digitalen Landschaft auf künftige Herausforderungen. Es wird darin ein kooperativer und kohärenter Ansatz empfohlen, der die politischen Reformen in den bestehenden Rahmen verankert und sie gleichzeitig an die neuen technologischen Gegebenheiten anpasst. Durch diese Maßnahmen will die EU eine resiliente, wettbewerbsfähige und nachhaltige digitale Wirtschaft gewährleisten.