EUROPÄISCHE
KOMMISSION

Brüssel, den 16.12.2020
SWD(2020) 344 final

ARBEITSUNTERLAGE DER KOMMISSIONSDIENSTSTELLEN

BERICHT ÜBER DIE FOLGENABSCHÄTZUNG (ZUSAMMENFASSUNG)

Begleitunterlage zum

Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates

über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union und zur Aufhebung der Richtlinie (EU) 2016/1148

{COM(2020) 823 final} - {SEC(2020) 430 final} - {SWD(2020) 345 final}

Zusammenfassung

Folgenabschätzung zur *Überprüfung der Richtlinie (EU) 2016/1148 vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union (im Folgenden „NIS-Richtlinie“).*

A. Handlungsbedarf

Worin besteht das Problem und warum sind Maßnahmen auf EU-Ebene erforderlich?

Trotz der großen Errungenschaften der NIS-Richtlinie, die in vielen Mitgliedstaaten ein erhebliches Umdenken in Bezug auf das institutionelle und regulatorische Cybersicherheitskonzept bewirkt hat, haben sich inzwischen auch ihre Grenzen gezeigt. Mit dem zunehmenden digitalen Wandel der Gesellschaft, der durch die COVID-19-Krise noch an Tempo gewonnen hat, haben auch die Bedrohungen für die Cybersicherheit zugenommen. Dies bringt neue Herausforderungen mit sich, die entsprechende innovative Antworten erfordern. Die Zahl der Cyberangriffe steigt weiter, wobei die Angriffe von verschiedensten Seiten innerhalb und außerhalb der EU ausgehen und immer komplexer werden.

Auf der Grundlage der Bewertung der Funktionsweise der NIS-Richtlinie wurden in der Folgenabschätzung folgende Probleme ermittelt: niedriges Cyberresilienzniveau bei in der EU tätigen Unternehmen; unterschiedlich starke Resilienz der Mitgliedstaaten und Sektoren, schwach ausgeprägte gemeinsame Lageerfassung und mangelnde gemeinsame Krisenreaktion. Als Ergebnis einiger dieser Probleme und Faktoren fallen beispielsweise in einem Mitgliedstaat bestimmte große Krankenhäuser nicht unter die NIS-Richtlinie und müssen folglich die entsprechenden Sicherheitsmaßnahmen nicht ergreifen, während die NIS-Sicherheitsanforderungen in einem anderen Mitgliedstaat für nahezu alle Krankenhäuser gelten.

Was soll erreicht werden?

Mit der Überprüfung der NIS-Richtlinie werden drei allgemeine Ziele verfolgt:

1. **Stärkung der Cyberresilienz eines alle relevanten Sektoren umfassenden Spektrums von Unternehmen, die in der Europäischen Union tätig sind**, durch Einführung von Vorschriften, mit denen sichergestellt wird, dass alle öffentlichen und privaten Einrichtungen im gesamten Binnenmarkt, die wichtige Funktionen für die Wirtschaft und die Gesellschaft als Ganzes erfüllen, verpflichtet sind, angemessene Cybersicherheitsmaßnahmen zu ergreifen.
2. **Förderung einer gleich starken Resilienz bei den bereits unter die Richtlinie fallenden Sektoren im Binnenmarkt**, durch weitere Angleichung 1) des De-facto-Anwendungsbereichs, 2) der Sicherheitsanforderungen und Meldepflichten bei Sicherheitsvorfällen, 3) der Bestimmungen für die nationale Aufsicht und Durchsetzung sowie 4) der Kapazitäten der zuständigen Behörden in den Mitgliedstaaten.
3. **Verbesserung der gemeinsamen Lageerfassung und der kollektiven Vorsorge und Reaktionsfähigkeit**, durch Maßnahmen zur Stärkung des Vertrauens zwischen den zuständigen Behörden, durch einen verstärkten Informationsaustausch und durch die Festlegung von Regeln und Verfahren im Falle weitreichender Sicherheitsvorfälle oder Krisen.

Worin besteht der Mehrwert von Maßnahmen auf EU-Ebene (Subsidiarität)?

Eine unionsweite Cyberresilienz kann nicht erreicht werden, solange sie in nationalen oder regionalen Silos uneinheitlich angegangen wird. Mit der NIS-Richtlinie sollte dieser Mangel behoben werden, indem ein Rahmen für die Sicherheit der Netz- und Informationssysteme auf der Ebene der Mitgliedstaaten und

auf Unionsebene geschaffen wurde. Aber bei der Umsetzung in nationales Recht und der Anwendung der Richtlinie wurden inhärente Mängel und Grenzen einiger Bestimmungen oder Ansätze deutlich, wie etwa die unklare Abgrenzung des Anwendungsbereichs der NIS-Richtlinie. Hinzu kommt, dass die europäische Wirtschaft seit Beginn der COVID-19-Krise stärker von Netz- und Informationssystemen abhängig ist als je zuvor und Sektoren und Dienste immer enger miteinander verflochten sind. Die erste Überprüfung der NIS-Richtlinie bietet daher die Gelegenheit für weitere Maßnahmen der EU. Ein Tätigwerden der EU über die geltenden Maßnahmen der NIS-Richtlinie hinaus ist hauptsächlich durch folgende Faktoren gerechtfertigt: i) den grenzüberschreitenden Charakter des Problems; ii) das Potenzial der EU-Maßnahmen zur Verbesserung und Förderung wirksamer nationaler Strategien; iii) den Beitrag konzertierter und kooperativer NIS-Politikmaßnahmen zum wirksamen Schutz des Datenschutzes und der Privatsphäre.

B. Lösungen

Welche Optionen bestehen zum Erreichen der Ziele? Gibt es eine bevorzugte Option? Wenn nein, warum nicht?

In der Folgenabschätzung wurden vier politische Optionen analysiert: 0) Beibehaltung des Status quo; 1) nichtlegislative Maßnahmen zur Angleichung der Umsetzung; 2) begrenzte Änderungen der NIS-Richtlinie zur weiteren Harmonisierung; 3) systemische und strukturelle Änderungen der NIS-Richtlinie. Option 1 wurde in einem frühen Stadium verworfen, da sie nicht wesentlich vom Status quo abweicht. In der Folgenabschätzung wird der Schluss gezogen, dass **Option 3** (d. h. **systemischen und strukturellen Änderungen des NIS-Rahmens**) der **Vorzug** zu geben ist, da sie eine grundlegendere Verlagerung des Ansatzes auf ein breiteres Segment der Volkswirtschaften in der gesamten Union vorsehen würde, jedoch mit einer gezielteren Aufsicht, die auf verhältnismäßig große und wichtige Unternehmen abzielt, und gleichzeitig den Anwendungsbereich eindeutig festlegt. Außerdem würden die sicherheitsrelevanten Verpflichtungen für Unternehmen vereinheitlicht und weiter harmonisiert. Zudem würden ein wirksamerer Rahmen für operative Aspekte, eine klare Grundlage für die gemeinsame Verantwortung und Rechenschaftspflicht der einschlägigen Akteure sowie Anreize für den Informationsaustausch geschaffen.

Welchen Standpunkt vertreten die verschiedenen Interessenträger? Wer unterstützt welche Option?

Die Mehrheit der zuständigen Behörden und Unternehmen hat sich für eine Überarbeitung der NIS-Richtlinie ausgesprochen. Während mehrerer Konsultationen wiesen sie darauf hin, dass eine überarbeitete NIS-Richtlinie zusätzliche (Teil-) Sektoren abdecken und weitere Sicherheitsmaßnahmen und Meldepflichten angleichen oder vereinheitlichen sollte. Die Interessenträger bekundeten auch Unterstützung für neue Konzepte oder politikbezogene Maßnahmen, die nur Teil der bevorzugten Option sind (z. B. Strategien für die Sicherheit der Lieferkette, Institutionalisierung eines funktionierenden EU-Krisenmanagementrahmens).

C. Auswirkungen der bevorzugten Option

Worin bestehen die Vorteile der bevorzugten Option (bzw. der wichtigsten Optionen)?

Die bevorzugte Option hätte erhebliche Vorteile: Schätzungen auf der Grundlage einer wirtschaftlichen Modellierung, die durch eine unterstützende Studie für die NIS-Überprüfung entwickelt wurde, deuten darauf hin, dass mit der bevorzugten Option die durch Cybersicherheitsvorfälle verursachten Kosten um 11,3 Mrd. EUR gesenkt werden könnten.

Der sektorale Anwendungsbereich würde im Rahmen des NIS-Rahmens erheblich erweitert, aber neben den oben genannten Vorteilen wäre die Belastung, die sich aus den NIS-Anforderungen ergeben könnte,

insbesondere aus aufsichtsrechtlicher Sicht, sowohl für die neu abzudeckenden Einrichtungen als auch für die zuständigen Behörden ausgewogen. Dies liegt daran, dass mit dem neuen NIS-Rahmen ein zweischichtiger Ansatz eingeführt würde, mit Schwerpunkt auf großen und wesentlichen Einrichtungen und einer Differenzierung der Aufsichtsregelung, die nur eine Ex-post-Aufsicht (d. h. reaktive und keine allgemeine Verpflichtung zur systematischen Dokumentation der Einhaltung der Vorschriften) für eine große Zahl dieser Einrichtungen vorsieht, insbesondere derer, die als „wichtig", aber nicht „wesentlich" angesehen werden.

Insgesamt würde die bevorzugte Option zu effizienten Kompromissen und Synergien führen und nach Analyse der Optionen über das größte Potenzial verfügen, unionsweit ein höheres und einheitliches Cyberresilienzniveau wesentlicher Einrichtungen zu gewährleisten, das letztlich zu Kosteneinsparungen sowohl für Unternehmen und als auch für die Gesellschaft führen würde.

Welche Kosten sind mit der bevorzugten Option (bzw. den wichtigsten Optionen) verbunden?

Die bevorzugte Option würde zu gewissen Einhaltungs- und Durchsetzungskosten für die zuständigen Behörden der Mitgliedstaaten führen (Schätzungen zufolge bedeutet dies eine Aufstockung der Ressourcen um insgesamt 20-30 %). Der neue Rahmen würde jedoch auch erhebliche Vorteile bringen, indem er einen besseren Überblick über wichtige Unternehmen und eine bessere Interaktion mit ihnen, eine verstärkte grenzübergreifende Zusammenarbeit auf operativer Ebene sowie Amtshilfe und Peer-Review-Mechanismen bietet. Dadurch würden die Cybersicherheitskapazitäten in den Mitgliedstaaten insgesamt erhöht.

Für die Unternehmen, die in den Anwendungsbereich des NIS-Rahmens fallen würden, wird geschätzt, dass sie in den ersten Jahren nach der Einführung des neuen NIS-Rahmens ihre derzeitigen Ausgaben für die IKT-Sicherheit um maximal 22 % erhöhen müssten (für Unternehmen, die bereits in den Anwendungsbereich der aktuellen NIS-Richtlinie fallen, wären dies 12 %). Dieser durchschnittliche Anstieg der Ausgaben für die IKT-Sicherheit würde jedoch zu einem entsprechenden Nutzen solcher Investitionen führen, insbesondere dadurch, dass die Kosten von Cybersicherheitsvorfällen erheblich reduziert würden (schätzungsweise um 11,3 Mrd. EUR über einen Zeitraum von zehn Jahren).

Worin bestehen die Auswirkungen für KMU und die Wettbewerbsfähigkeit?

Klein- und Kleinstunternehmen würden im Rahmen der bevorzugten Option vom Anwendungsbereich des NIS-Rahmens ausgenommen. Für mittlere Unternehmen ist davon auszugehen, dass die Ausgaben für IKT-Sicherheit in den ersten Jahren nach Einführung des neuen NIS-Rahmens steigen werden. Gleichzeitig würde eine Anhebung der Sicherheitsanforderungen für diese Unternehmen auch Anreize zur Stärkung ihrer Cybersicherheitskapazitäten schaffen und dazu beitragen, ihr IKT-Risikomanagement zu verbessern.

Wird es erhebliche Auswirkungen auf nationale Haushalte und Behörden geben?

Es wird folgende Auswirkungen auf nationale Haushalte und Behörden geben: Kurz- und mittelfristig ist mit einem Anstieg der benötigten Ressourcen um schätzungsweise 20-30 % zu rechnen.

Wird es andere erhebliche Auswirkungen geben?

Es sind keine weiteren signifikanten negativen Auswirkungen zu erwarten. Es wird erwartet, dass der Vorschlag zu robusteren Cybersicherheitskapazitäten führt und folglich die Anzahl und den Schweregrad von Sicherheitsvorfällen, einschließlich Verstößen gegen den Datenschutz, stärker eindämmen wird. Er dürfte sich auch positiv auf die Gewährleistung gleicher Wettbewerbsbedingungen in allen Mitgliedstaaten auswirken, und zwar für alle Einrichtungen, die in den Anwendungsbereich der NIS fallen, und die

Informationsasymmetrien im Bereich der Cybersicherheit verringern.
Verhältnismäßigkeit
Die bevorzugte Option geht nicht über das für die zufriedenstellende Verwirklichung der spezifischen Ziele erforderliche Maß hinaus. Die Angleichung und Vereinheitlichung der Sicherheitsmaßnahmen und Meldepflichten, wie sie im Vorschlag vorgesehen sind, entsprechen den Forderungen der Mitgliedstaaten und Unternehmen nach einer Verbesserung des geltenden Rahmens.
D. Folgemaßnahmen
Wann wird die Strategie überprüft?
Die erste Überprüfung würde 54 Monate nach Inkrafttreten des Rechtsinstruments stattfinden. Die Kommission würde dem Europäischen Parlament und dem Rat einen Bericht über die Überprüfung vorlegen. Die Überprüfung würde mit Unterstützung der ENISA und der Kooperationsgruppe vorbereitet werden.