EUROPÄISCHE
KOMMISSION

Brüssel, den 15.9.2022
SWD(2022) 283 final

ARBEITSUNTERLAGE DER KOMMISSIONSDIENSTSTELLEN

BERICHT ÜBER DIE FOLGENABSCHÄTZUNG (ZUSAMMENFASSUNG)

zum Cyberresilienzgesetz

Begleitunterlage zum

Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates

über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen und zur Änderung der Verordnung (EU) 2019/1020

{COM(2022) 454 final} - {SEC(2022) 321 final} - {SWD(2022) 282 final}

Zusammenfassung (höchstens zwei Seiten)

Folgenabschätzung zum Cyberresilienzgesetz

A. Handlungsbedarf

Worin besteht das Problem und warum muss ihm auf EU-Ebene begegnet werden?

Hardware- und Softwareprodukte sind häufig Ziel erfolgreicher Cyberangriffe, die bis 2021 weltweit Cyberkriminalitätskosten von jährlich insgesamt 5,5 Billionen EUR verursacht haben. Diese Produkte leiden unter zwei großen Problemen, die für ihre Nutzer und die Gesellschaft zu zusätzlichen Kosten führen: 1) ein niedriges Cybersicherheitsniveau, das sich an weitverbreiteten Schwachstellen und der unzureichenden und uneinheitlichen Bereitstellung von Sicherheitsaktualisierungen ablesen lässt, sowie 2) Informationen, die für die Nutzer nur bedingt verständlich und zugänglich sind, sodass diese kaum in der Lage sind, Produkte mit angemessenen Cybersicherheitsmerkmalen auszuwählen oder sicher zu verwenden.

Die Cybersicherheit von Produkten mit digitalen Elementen hat eine ausgeprägte grenzübergreifende Dimension, da die in einem Land hergestellten Produkte häufig im gesamten Binnenmarkt verwendet werden. Zudem breiten sich Vorfälle, die ursprünglich nur eine einzige Stelle oder einen einzigen Mitgliedstaat betreffen, oft innerhalb von Minuten auf den gesamten Binnenmarkt aus.

Zwar bestehen für bestimmte Produkte mit digitalen Elementen bereits Binnenmarktvorschriften, doch die Cybersicherheit der meisten Hardware- und Softwareprodukte wird noch von keiner EU-Vorschrift erfasst. Insbesondere erstreckt sich der derzeitige EU-Rechtsrahmen nicht auf die Cybersicherheit nicht eingebetteter Software, obwohl Cyberangriffe zunehmend auf Schwachstellen in diesen Produkten abzielen und erhebliche gesellschaftliche und wirtschaftliche Kosten verursachen. Jüngste Beispiele sind die Spähsoftware Pegasus, die sich Schwachstellen in Mobilfunkgeräten zunutze machte, oder der Ransomware-Wurm WannaCry, der unter Ausnutzung einer Windows-Schwachstelle weltweit Computer befiel.

Was soll erreicht werden?

Für ein reibungsloses Funktionieren des Binnenmarkts wurden zwei Hauptziele festgelegt: 1) Schaffung der Voraussetzungen für die Entwicklung sicherer Produkte mit digitalen Elementen, damit Hardware- und Softwareprodukte mit weniger Schwachstellen in Verkehr gebracht werden und Hersteller die Sicherheit über den gesamten Lebenszyklus eines Produkts hinweg ernst nehmen; und 2) Schaffung der Voraussetzungen, die es Nutzern ermöglichen, bei der Auswahl und Verwendung von Produkten mit digitalen Elementen die Cybersicherheit zu berücksichtigen. Hierfür wurden vier Einzelziele festgelegt: i) Gewährleistung, dass Hersteller von Produkten mit digitalen Elementen bereits in der Konzeptions- und Entwicklungsphase und über den gesamten Lebenszyklus des Produkts für eine größere Sicherheit sorgen; ii) Gewährleistung eines kohärenten Cybersicherheitsrahmens, der den Hardware- und Software-Herstellern die Einhaltung der Vorschriften erleichtert; iii) Erhöhung der Transparenz der Sicherheitseigenschaften von Produkten mit digitalen Elementen und iv) Schaffung der Voraussetzungen, damit Unternehmen und Verbraucher Produkte mit digitalen Elementen sicher verwenden können.

Worin besteht der Mehrwert des Tätigwerdens auf EU-Ebene (Subsidiarität)?

Der ausgeprägte grenzüberschreitende Charakter der Cybersicherheit und die steigende Anzahl von Vorfällen, die sich über Grenzen, Sektoren und Produkte hinweg auswirken, machen deutlich, dass die Ziele von den Mitgliedstaaten allein nicht wirksam erreicht werden können. Angesichts des globalen Charakters der Märkte für Produkte mit digitalen Elementen sehen sich die Mitgliedstaaten mit denselben

Risiken bei denselben Produkten mit digitalen Elementen in ihrem Hoheitsgebiet konfrontiert. Der sich abzeichnende Flickenteppich potenziell abweichender einzelstaatlicher Vorschriften kann auch dazu führen, dass die Herausbildung eines offenen und wettbewerbsfähigen Binnenmarkts für Produkte mit digitalen Elementen gefährdet wird. Daher ist ein gemeinsames Vorgehen auf EU-Ebene erforderlich, um mit Blick auf die in der EU in Verkehr gebrachten Produkte mit digitalen Elementen das Vertrauen der Nutzer zu stärken und die Attraktivität dieser Produkte zu erhöhen. Auch kommt es dem Binnenmarkt zugute, wenn für die Hersteller der Produkte mit digitalen Elementen Rechtssicherheit und gleiche Wettbewerbsbedingungen gewährleistet sind.

B. Lösungen

Worin bestehen die Optionen zur Verwirklichung der Ziele? Wird eine dieser Optionen bevorzugt? Falls nicht, warum nicht?

Untersucht wurden vier Politikoptionen und entsprechende Unteroptionen, die über den Status quo hinausgehen: 1) Nicht zwingendes Recht und freiwillige Maßnahmen; 2) produktspezifische Ad-hoc-Regulierung der Cybersicherheit materieller Produkte mit digitalen Elementen und entsprechender eingebetteter Software; 3) gemischter Ansatz mit verbindlichen horizontalen Vorschriften für die Cybersicherheit materieller Produkte mit digitalen Elementen und entsprechender eingebetteter Software und einem abgestuften Ansatz für nicht eingebettete Software mit zwei Unteroptionen für die Konformitätsbewertung; und 4) eine horizontale Regulierung mit Cybersicherheitsanforderungen für ein breites Spektrum von Produkten mit digitalen Elementen, darunter auch solche mit nicht eingebetteter Software, mit Unteroptionen für den Anwendungsbereich und die Konformitätsbewertung.

Die Folgenabschätzung ergab die Option 4 als **bevorzugte Option**, da sie sich auf alle Produkte mit digitalen Elementen erstreckt und eine verbindliche Bewertung kritischer Produkte durch Dritte vorsieht, bei der die Wirksamkeit anhand konkreter Ziele, Kosteneffizienz, Kosten-Nutzen-Verhältnis und Kohärenz bewertet wird.

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

Zur Bewertung der Wirksamkeit der Maßnahmen ergab die öffentliche Konsultation, dass die Option 4 als die wirksamste Maßnahme gesehen wird (4,08 auf einer Skala von 1 bis 5). Es beteiligten sich u. a. Verbraucherorganisationen (5,00), sich als „Nutzer“ bezeichnende Teilnehmer (4,22), notifizierte Stellen (4,17), Marktüberwachungsbehörden (5,00) und Hersteller von Produkten mit digitalen Elementen (3,85), darunter kleine und mittlere Unternehmen (4,05).

C. Auswirkungen der bevorzugten Option

Worin bestehen die Vorteile der bevorzugten Option bzw. der wesentlichen Optionen?

Die bevorzugte Option würde den verschiedenen Beteiligten erhebliche Vorteile bringen: Für Unternehmen würden keine unterschiedlichen Sicherheitsvorschriften für Produkte mit digitalen Elementen gelten und die Kosten der Einhaltung der entsprechenden Cybersicherheitsvorschriften wären geringer. Die Anzahl der Cybervorfälle wäre rückläufig und damit auch die hierbei entstehenden Kosten und der Image-Schaden. Für die gesamte EU wird davon ausgegangen, dass sich mit der Initiative die Kosten infolge von Vorfällen, bei denen Unternehmen geschädigt werden, um etwa 180 bis 290 Mrd. EUR pro Jahr senken lassen. Zudem dürfte die Initiative zu Umsatzsteigerungen aufgrund einer steigenden Nachfrage nach Produkten mit digitalen Elementen führen. Außerdem dürften die Unternehmen weltweit einen Imagegewinn verzeichnen und damit ihren Absatz auch außerhalb der EU

steigern können. Für Endnutzer dürfte die bevorzugte Option die Transparenz der Sicherheitseigenschaften erhöhen und die Verwendung der Produkte mit digitalen Elementen vereinfachen. Verbraucher und Bürger würden auch von einem besseren Schutz ihrer Grundrechte, wie Schutz der Privatsphäre und Datenschutz, profitieren.

Welche Kosten entstehen bei Umsetzung der bevorzugten Option bzw. der wichtigsten Optionen?

Die bevorzugte Option führt zu zusätzlichen Befolgungs- und Durchsetzungskosten für Unternehmen, notifizierte Stellen und Behörden, worunter auch Notifizierungs-, Akkreditierung- und Marktüberwachungsbehörden fallen. Für Softwareentwickler und Hardwarehersteller werden sich die direkten Befolgungskosten erhöhen, die aufgrund neuer Cybersicherheitsanforderungen, Konformitätsbewertungen sowie Dokumentations- und Meldepflichten entstehen und sich insgesamt auf rund 29 Mrd. EUR bei einem geschätzten Marktwert der Produkte mit digitalen Elementen von bis 1,485 Billionen EUR Umsatz belaufen werden. Auf Seiten der Endnutzer können sich für gewerbliche Nutzer, Verbraucher und Bürger höhere Preise für Produkte mit digitalen Elementen ergeben. Dies sollte jedoch vor dem Hintergrund der vorstehend beschriebenen erheblichen Vorteile gesehen werden. Für notifizierte Stellen dürften die Zusatzkosten durch den steigenden Umsatz ausgeglichen werden.

Worin bestehen die Auswirkungen auf KMU und die Wettbewerbsfähigkeit?

KMU werden von den neuen Anforderungen sowohl als Hersteller als auch als Endnutzer betroffen sein. Die Befolgungskosten dürften bei den KMU grundsätzlich stärker ins Gewicht fallen als bei großen Unternehmen, die in der Regel Größenvorteile erzielen und sich der Cybersicherheitsproblematik stärker bewusst sind. KMU dürften von der Initiative jedoch stark profitieren, da die in Produkten mit digitalen Elementen eingebettete Software den KMU als Nutzern zu beträchtlichen Einsparungen verhelfen kann. Als Hersteller könnten KMU von einem größeren Vertrauen der Endnutzer und von Neukunden profitieren. Ein reibungsloser Zugang zum Binnenmarkt und eine geringere Marktfragmentierung können gerade für KMU, die weniger gut für den Umgang mit unterschiedlichen Rechtsvorschriften gerüstet sind, von besonderem Vorteil sein. KMU unterstrichen zwar die Notwendigkeit eines die Verhältnismäßigkeit wahrenden Ansatzes und von Unterstützungsmaßnahmen, doch favorisierten sie im Allgemeinen gleiche Wettbewerbsvoraussetzungen für alle Unternehmen und waren nicht der Auffassung, dass sie in einem Szenario horizontaler verbindlicher Vorschriften gegenüber großen Unternehmen im Nachteil wären.

Wird es spürbare Auswirkungen auf nationale Haushalte und Behörden geben?

Die Initiative wird sich auf nationale Behörden, wie nationale Notifizierungs-, Akkreditierungs- und Marktüberwachungsbehörden auswirken, die für die Überwachung und Durchsetzung der vorgeschlagenen Maßnahmen zuständig sind. Diesen Behörden entstehen zusätzliche Kosten durch Anpassungen (z. B. Ausbildung und Personal) sowie für die Durchsetzung der neuen Vorschriften. Die den Akkreditierungsstellen entstehenden Kosten werden jedoch dadurch ausgeglichen, dass sie überwiegend von Konformitätsbewertungsstellen, die Akkreditierungsdienste in Anspruch nehmen, getragen werden.

Gibt es andere nennenswerte Auswirkungen?

Andere nennenswerte negative Auswirkungen sind nicht zu erwarten. Die bevorzugte Politikoption dürfte dazu führen, dass die Anzahl und Schwere der Vorfälle abnimmt, auch die Verletzungen des Schutzes personenbezogener Daten, und die Cyberkriminalität zurückgeht, was sich positiv auf die Gesellschaft auswirkt. Die Nachfrage nach professionellem Personal mit Cybersicherheitskenntnissen dürfte steigen und damit die Informationsasymmetrie bei der Cybersicherheit zurückgehen.

Verhältnismäßigkeit?
Die bevorzugte Option geht nicht über das für die zufriedenstellende Verwirklichung der spezifischen Ziele erforderliche Maß hinaus. Mit der Maßnahme würde sichergestellt, dass Produkte mit digitalen Elementen über ihren gesamten Lebenszyklus hinweg so sicher sind, wie dies im Verhältnis zu den von ihnen ausgehenden Risiken erforderlich ist.
D. Folgemaßnahmen
Wann wird die Maßnahme überprüft?
Bis zum [36 Monate nach dem Datum der Anwendung dieser Initiative] und danach alle vier Jahre legt die Kommission dem Europäischen Parlament und dem Rat einen Bericht über die Bewertung und Überprüfung dieser Initiative vor.