EUROPÄISCHE
KOMMISSION

Brüssel, den 13.9.2017
SWD(2017) 501 final

ARBEITSUNTERLAGE DER KOMMISSIONSDIENSTSTELLEN

ZUSAMMENFASSUNG DER FOLGENABSCHÄTZUNG

Begleitunterlage zum

Vorschlag für eine VERORDNUNG DES EUROPÄISCHEN PARLAMENTS UND DES RATES

über die „EU-Cybersicherheitsagentur“ (ENISA) und zur Aufhebung der Verordnung (EU) Nr. 526/2013 sowie über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik („Rechtsakt zur Cybersicherheit“)

{COM(2017) 477 final}
{SWD(2017) 500 final}
{SWD(2017) 502 final}

A. HANDLUNGSBEDARF

Problemstellung und -ursache

Digitale Technologien und das Internet bilden das Rückgrat von Wirtschaft und Gesellschaft in der EU. Das Kerngeschäft kritischer Wirtschaftssektoren, etwa des Verkehrs-, Energie-, Gesundheits- oder Finanzsektors, hängt immer mehr von Netz- und Informationssystemen ab. Das „Internet der Dinge“ verbindet Gegenstände und Menschen über Kommunikationsnetze miteinander. Diese neue Realität bringt nie zuvor da gewesene Möglichkeiten, aber auch Anfälligkeiten hervor. Cybersicherheitsvorfälle kommen massenhaft vor. Ihre Komplexität und Häufigkeit dürften noch weiter zunehmen, und die Bereiche, in denen sie sich auswirken – vom Zugang zu wesentlichen Dienstleistungen bis hin zu demokratischen Prozessen –, dürften sich noch ausweiten.

In diesem Zusammenhang wurden die folgenden, miteinander verbundenen Probleme ausgemacht:

- Unterschiedliche, nebeneinander bestehende Konzepte und Ansätze im Bereich der Cybersicherheit in den Mitgliedstaaten.
- Verstreute Ressourcen und uneinheitliche Ansätze der Organe, Einrichtungen und sonstigen Stellen der EU im Bereich der Cybersicherheit.
- Unzureichendes Problembewusstsein von Bürgern und Unternehmen hinsichtlich der Cyberbedrohungen und unzureichende Informationen über die Sicherheitsmerkmale der von ihnen gekauften IKT-Produkte und -Dienstleistungen in Verbindung mit dem vermehrten Aufkommen einer Vielzahl von nationalen und sektoralen Zertifizierungssystemen.

Diese Probleme haben Auswirkungen auf die Abwehrfähigkeit gegenüber Cyberangriffen in der EU insgesamt und auf das effektive Funktionieren des Binnenmarkts.

Was soll erreicht werden?

Mit dieser Initiative werden die folgenden politischen Einzelziele verfolgt:

1. Ausbau der Kapazitäten und der Abwehrbereitschaft der Mitgliedstaaten und Unternehmen, insbesondere in Bezug auf kritische Infrastrukturen,
2. Verbesserung der Zusammenarbeit und der Koordinierung zwischen den Mitgliedstaaten und den Organen, Einrichtungen und sonstigen Stellen der EU,
3. Ausbau der Kapazitäten auf EU-Ebene, um die Maßnahmen der Mitgliedstaaten zu ergänzen, insbesondere im Fall von grenzüberschreitenden Cyberkrisen,
4. Stärkere Sensibilisierung der Bürger und Unternehmen für Fragen der Cybersicherheit,
5. Verbesserung der allgemeinen Transparenz bei den Angaben zur Vertrauenswürdigkeit der bescheinigten Cybersicherheit von IKT-Produkten und -Diensten, um das Vertrauen in den digitalen Binnenmarkt und in digitale Innovationen zu stärken,
6. Vermeidung eines Nebeneinanders unterschiedlicher Zertifizierungssysteme in der EU sowie der damit verbundene Anforderungen und Bewertungskriterien in den einzelnen

Mitgliedstaaten und Sektoren.

Worin besteht der Mehrwert des Tätigwerdens auf EU-Ebene?

Angesichts der globalen Dimension von Wirtschaft und Gesellschaft haben die Probleme ein Ausmaß, das deutlich über die Hoheitsgebiete der einzelnen Mitgliedstaaten hinausgeht. Daher ist ein Tätigwerden auf Unionsebene notwendig. Im aktuellen Kontext und mit Blick auf künftige Szenarios können Einzelmaßnahmen von Mitgliedstaaten und ein fragmentierter Ansatz hinsichtlich der Cybersicherheit, insbesondere hinsichtlich ihrer grenzübergreifenden Dimension, die kollektive Cyber-Abwehrfähigkeit der Union nicht verbessern.

B. LÖSUNGEN

Worin bestehen die Optionen zur Verwirklichung der Ziele? Wird eine dieser Optionen bevorzugt?

In dieser Folgenabschätzung werden bestimmte Politikoptionen für die Überprüfung der Agentur der Europäischen Union für Netz- und Informationssicherheit (ENISA) und der IKT-Sicherheitszertifizierung untersucht.

Überprüfung der ENISA

Option 0 - **Basisszenario** - Bei dieser Option geht es um die Aufrechterhaltung des Status quo. Das Mandat der ENISA würde verlängert werden, und die Ziele und Aufgaben der Agentur würden unter Berücksichtigung der Aufgaben, die der ENISA durch spätere EU-Rechtsvorschriften (z. B. NIS-Richtlinie) zugewiesen wurden, weitgehend unverändert bleiben.

Option 1 - **Auslaufen des ENISA-Mandats** (Einstellung der Arbeit der ENISA). Diese Option würde die Einstellung der Arbeit der ENISA am Ende ihres Mandats (Juni 2020) und möglicherweise eine Neuverteilung der Zuständigkeiten/Tätigkeiten auf EU-Ebene und/oder nationaler Ebene zur Folge haben.

Option 2 - **„Reformierte ENISA“**. Diese Option würde auf dem gegenwärtigen Mandat der ENISA aufbauen und selektive Änderungen zum Ziel haben, die die Entwicklung der Cybersicherheitslage berücksichtigen. Die Agentur würde über ein ständiges Mandat auf der Grundlage der folgenden zentralen Bausteine verfügen: Unterstützung der Entwicklung und Umsetzung politischer Maßnahmen der EU, Kapazitätsaufbau, Wissen und Information, marktbezogene Aufgaben, Forschung und Innovation sowie operative Zusammenarbeit und Krisenmanagement.

Option 3 - **vollständig einsatzfähige EU-Cybersicherheitsagentur.** Diese Option sieht eine Reform der ENISA dahingehend vor, dass drei Hauptfunktionen zusammengeführt werden: 1. politische/beratende Funktion, 2. Informations- und Kompetenzzentrum und 3. Computer-Notfallteam (Computer Emergency Response Team, CERT). Bei dieser Option wären die Änderungen des Zuständigkeitsbereichs des Mandats weitgehend dieselben wie bei der Option 2. Im Bereich der Reaktion auf Sicherheitsvorfälle und des Krisenmanagements würden jedoch weitere Aufgaben hinzukommen, sodass die Agentur den gesamten Cybersicherheitszyklus abdecken und sich mit der Prävention, Erkennung und Bewältigung von Cybervorfällen befassen würde.

Zertifizierung

Option 0 – Basisszenario – Status quo. Bei dieser Option würde die Kommission den Status quo beibehalten und keine politischen oder legislativen Maßnahmen ergreifen.

Option 1 – Nichtlegislative (nicht zwingende) Maßnahmen. Bei dieser Option würde die Kommission „weiche" politische Instrumente (z. B. Mitteilungen zu Auslegungsfragen, Unterstützung EU-weiter Initiativen zur Selbstregulierung und Normung) nutzen, um die Transparenz zu verbessern und die Fragmentierung zu verringern.

Option 2 – Ein EU-Rechtsakt zur Ausweitung des SOG-IS-Abkommens auf alle Mitgliedstaaten. Bei dieser Option würde die Kommission einen Rechtsakt zur Ausweitung der Mitgliedschaft auf alle Mitgliedstaaten vorschlagen.

Option 3 – Ein EU-Rahmen für die allgemeine IKT-Sicherheitszertifizierung. Diese Option sieht die Festlegung eines europäischen Rahmens für die IKT-Sicherheitszertifizierung (einschließlich einer aus nationalen Behörden zusammengesetzten Sachverständigengruppe) vor, wobei, soweit möglich, auf bestehenden IKT-Sicherheitszertifizierungssystemen aufgebaut werden soll. Im Kern würde der Rahmen die Einführung von EU-Zertifizierungssystemen ermöglichen, die in allen Mitgliedstaaten akzeptiert werden.

Die bevorzugte Option ist eine Kombination aus der Option 2 für die ENISA und der Option 3 für die Zertifizierung.

Wer sind die Interessenträger? Wer unterstützt welche Option?

Die große Mehrheit der Interessenträger aller Kategorien (Mitgliedstaaten, Industrie, EU-Organe, Forschung), die an den Beratungen teilnahmen, begrüßt offenbar die bevorzugte Option, da sie sich für die Stärkung der ENISA und für die Schaffung eines Rahmens für die europäische IKT-Sicherheitszertifizierung aussprechen.

Insbesondere besteht Konsens über die Notwendigkeit, (mindestens) über eine gut funktionierende EU-Agentur mit einem auf Dauer angelegten Mandat zu verfügen, die mit angemessenen Ressourcen ausgestattet ist und den Auftrag hat, den gegenwärtigen und künftigen Herausforderungen im Bereich der Cybersicherheit zu begegnen. Ferner findet die Schaffung eines freiwilligen, skalierbaren europäischen Rahmens bei den Interessenträgern breite Zustimmung.

Diese Lösung für die Zertifizierung wird industrieseitig von Unternehmen unterstützt, für die bereits Zertifizierungsanforderungen gelten und die von einem EU-weiten Mechanismus, der auf der gegenseitigen Anerkennung der Zertifikate beruht, profitieren würden. Sie findet auch Zustimmung bei KMU, für die die Nachteile am größten wären, ganz gleich, ob sie bereits jetzt unterschiedliche Zertifizierungsverfahren in den Mitgliedstaaten durchlaufen müssen oder diese künftig durchlaufen müssten. Einige Mitgliedstaaten, insbesondere diejenigen mit geringeren Ressourcen, und einige Vertreter der Industrie und der EU-Organe äußerten sich auch zur Option 3 für die ENISA positiv.

C. AUSWIRKUNGEN DER BEVORZUGTEN OPTION

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

Bei der bevorzugten Option würde die EU über eine Agentur verfügen, deren Schwerpunkt darauf liegt, die Mitgliedstaaten, EU-Organe und Unternehmen in Bereichen zu unterstützen, in denen die Unterstützung den größten Mehrwert hätte. Diese Bereiche sind: Unterstützung der Umsetzung der NIS-Richtlinie; Entwicklung und Umsetzung politischer Maßnahmen; Information, Wissen und Sensibilisierung; Forschung; operative Zusammenarbeit und Krisenmanagement sowie der Markt. Die ENISA würde insbesondere die EU-Politik auf dem Gebiet der IKT-Sicherheitszertifizierung unterstützen, indem sie dafür sorgen würde, dass der europäische Rahmen für die IKT-Sicherheitszertifizierung administrativ begleitet und technisch umgesetzt wird. Mithilfe eines solchen Rahmens würden Regeln für die Governance der IKT-Sicherheitszertifizierung in der EU eingeführt werden, die ein System der gegenseitigen Anerkennung der in den Mitgliedstaaten ausgestellten Zertifikate fördern würden. Die in der Kombination dieser Optionen bestehende Lösung wird als die Lösung betrachtet, mit der die EU die folgenden Ziele am effektivsten erreichen kann: Verbesserung der Cybersicherheitskapazitäten, der Abwehrbereitschaft, der Zusammenarbeit, der Sensibilisierung und der Transparenz sowie Vermeidung einer Marktfragmentierung. Diese Option weist zudem die größte Übereinstimmung mit den politischen Prioritäten auf, die in der Cybersicherheitsstrategie, in den damit verbundenen Strategien (z. B. NIS-Richtlinie) und in der Strategie für den digitalen Binnenmarkt festgelegt wurden. Darüber hinaus ließen sich die Ziele bei dieser Option durch einen angemessenen Ressourceneinsatz erreichen.

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

Trotz der Übernahme neuer Funktionen wäre die reformierte ENISA weiterhin eine flexible Organisation. Der erforderliche finanzielle Beitrag aus dem EU-Haushalt wäre höher als dies derzeit der Fall ist, er läge jedoch nach wie vor um einiges unter dem finanziellen Beitrag für andere Agenturen, die auch in kritischen Bereichen tätig sind.

Die Schaffung eines Rahmens für die europäische IKT-Sicherheitszertifizierung wäre für die Industrie (einschließlich KMU) nicht mit zusätzlichen Vorabkosten verbunden. Sie hätte vielmehr für Unternehmen, die ihre Produkte bereits zertifizieren, oder die bereit sind, eine Sicherheitszertifizierung durchzuführen, erhebliche Einsparungen mit positiven Auswirkungen auf ihre globale Wettbewerbsfähigkeit zur Folge. Sie würde andererseits einige Mittelbindungen für die Beibehaltung des Rahmens voraussetzen, die vor allem durch das Modell „reformierte ENISA“ bereitgestellt würden, was die technischen Aufgaben und die Sekretariatsaufgaben betrifft.

Wird es spürbare Auswirkungen auf nationale Haushalte und Behörden geben?

Nein. Die mit der Stärkung der ENISA verbundenen Kosten würden überwiegend aus dem EU-Haushalt getragen werden, die Mitgliedstaaten könnten der Agentur jedoch weiterhin finanzielle Beiträge zukommen lassen. Bei der Zertifizierung würden sich die Hauptauswirkungen auf die nationalen Haushalte und Verwaltungen aus der Einrichtung einer Zertifizierungsbehörde, soweit angezeigt, ergeben.

Wird es andere nennenswerte Auswirkungen geben?

Nein.

Verhältnismäßigkeit

Die bevorzugte Option umfasst ausgewogene Maßnahmen, die alle für notwendig erachtet werden, um die angestrebten Ziele zu erreichen, ohne den jeweiligen Interessenträgern übermäßige Belastungen aufzuerlegen. Daher wird davon ausgegangen, dass diese Initiative dem Grundsatz der Verhältnismäßigkeit entspricht.

D. FOLGEMASSNAHMEN

Wann wird die Maßnahme überprüft?

Es wird nun vorgeschlagen, dass die erste Bewertung fünf Jahre nach Inkrafttreten des Rechtsakts stattfindet. Anschließend wird die Kommission dem Europäischen Parlament und dem Rat über die Ergebnisse ihrer Bewertung Bericht erstatten, erforderlichenfalls zusammen mit einem Vorschlag zur Überarbeitung des Rechtsakts. Weitere Bewertungen müssen alle fünf Jahre stattfinden.