RAT DER EUROPÄISCHEN UNION

Brüssel, den 12. Februar 2013 (13.02)
(OR. en)

6342/13
ADD 1

Interinstitutionelles Dossier: 2013/0027 (COD)

TELECOM	**24**
DATAPROTECT	**14**
CYBER	**2**
MI	**104**
CODEC	**313**

ÜBERMITTLUNGSVERMERK

Absender:	Herr Jordi AYET PUIGARNAU, Direktor, im Auftrag der Generalsekretärin der Europäischen Kommission
Eingangsdatum:	7. Februar 2013
Empfänger:	der Generalsekretär des Rates der Europäischen Union, Herr Uwe CORSEPIUS
Nr. Komm.dok.:	SWD(2013) 31 final
Betr.:	ARBEITSUNTERLAGE DER KOMMISSIONSDIENSTSTELLEN ZUSAMMENFASSUNG DER FOLGENABSCHÄTZUNG *Begleitunterlage zum* Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über Maßnahmen zur Gewährleistung einer hohen gemeinsamen Netz- und Informationssicherheit in der Union

Die Delegationen erhalten in der Anlage das Kommissionsdokument SWD(2013) 31 final.

Anl.: SWD(2013) 31 final

EUROPÄISCHE
KOMMISSION

Brüssel, den 7.2.2013
SWD(2013) 31 final

ARBEITSUNTERLAGE DER KOMMISSIONSDIENSTSTELLEN

ZUSAMMENFASSUNG DER FOLGENABSCHÄTZUNG

Begleitunterlage zum

Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates

über Maßnahmen zur Gewährleistung einer hohen gemeinsamen Netz- und Informationssicherheit in der Union

{COM(2013) 48 final}
{SWD(2013) 32 final}

ARBEITSUNTERLAGE DER KOMMISSIONSDIENSTSTELLEN

ZUSAMMENFASSUNG DER FOLGENABSCHÄTZUNG

Begleitunterlage zum

Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates

über Maßnahmen zur Gewährleistung einer hohen gemeinsamen Netz- und Informationssicherheit in der Union

1. GELTUNGSBEREICH

Die vorliegende Folgenabschätzung befasst sich mit Politikoptionen zur Verbesserung der Internetsicherheit sowie der Sicherheit anderer Netze und Informationssysteme für Dienste, die das gesellschaftliche Leben (u. a. öffentliche Verwaltungen, Finanz- und Bankenwesen, Energie-, Verkehrs-, Gesundheits- sowie bestimmte Internetdienste, die zentrale wirtschaftliche und gesellschaftliche Prozesse, wie Plattformen des elektronischen Geschäftsverkehrs und soziale Netzwerke ermöglichen) unterstützen. Dieser Bereich wird als Netz- und Informationssicherheit (NIS) bezeichnet.

2. POLITISCHER KONTEXT

Die Kommission erkannte die zunehmende Bedeutung der NIS für unsere Volkswirtschaften und Gesellschaften erstmals 2001 an. Im Jahr 2004 beschloss die Europäische Union die Gründung der Europäischen Agentur für Netz- und Informationssicherheit (ENISA), um eine hohe und wirksame Netz- und Informationssicherheit innerhalb der EU sicherzustellen. Der bisher von der Europäischen Union verfolgte Ansatz im Bereich der NIS bestand hauptsächlich in der Annahme verschiedener Aktionspläne und Strategien, in denen die Mitgliedstaaten dazu aufgefordert wurden, ihre NIS-Kapazitäten zu verbessern und bei der Bekämpfung von grenzüberschreitenden NIS-Problemen zusammenzuarbeiten.

Interessenträger sind zu den verschiedenen Aspekten der Initiative (Problemabgrenzung und Optionen zu Behebung bestehender Defizite) in folgender Weise konsultiert worden:

- **im Rahmen einer öffentlichen Online-Konsultation** zur „Verbesserung der NIS in der EU“, die vom 23. Juli bis zum 15. Oktober 2012 durchgeführt wurde; insgesamt gingen über das Online-Tool 169 Antworten sowie 10 weitere schriftliche Antworten bei der Kommission ein;
- in Gesprächen mit den **Mitgliedstaaten** im Rahmen des Europäischen Forums der Mitgliedstaaten (EFMS), in bilateralen Treffen und auf der von der Kommission und dem Europäischen Auswärtigen Dienst organisierten EU-Konferenz zum Thema Cybersicherheit, die am 6. Juli 2012 stattfand;
- in Gesprächen mit Unternehmen und Verbänden des **Privatsektors** im Rahmen der Europäischen öffentlich-privaten Partnerschaft für Robustheit (EP3R) und auf bilateralen Treffen;
- in Gesprächen mit **ENISA und CERT-EU**;

- in Gesprächen im Rahmen der **Versammlung 2012 zur Digitalen Agenda**.

3. PROBLEMBESCHREIBUNG

3.1. Problemstellung

Das Problem besteht in einem generell ***unzureichenden Schutz vor Sicherheitsvorfällen, -risiken und -bedrohungen im Bereich der Netz- und Informationssicherheit in der EU, die das reibungslose Funktionieren des Binnenmarkts beeinträchtigen***.

Da Netze und Informationssysteme miteinander verbunden sind und das Internet in seinem Wesen ein globales Netz ist, geht die Tragweite vieler NIS-Vorfälle über nationale Grenzen hinaus, wodurch das ordnungsgemäße Funktionieren des Binnenmarkts gefährdet wird.

Wie im Falle der Angriffe gegen eBay und PayPal besteht die Gefahr, dass grenzüberschreitende Dienste aufgrund von Sicherheitsverletzungen nicht mehr verfügbar oder gestört werden bzw. ausgesetzt werden müssen. Im Zusammenhang mit den Angriffen gegen die niederländische Internet-Zertifizierungsstelle Diginotar wurde darauf hingewiesen, dass schnelles Handeln zur Lösung des Problems sowie der Informationsaustausch über wichtige Sicherheitsvorfälle von großer Bedeutung sind. Anlässlich bereits eingetretener Sicherheitsvorfälle haben die Mitgliedstaaten begonnen, eigene Vorschriften einzuführen. Unkoordinierte Regelungsmaßnahmen können jedoch zu einer Fragmentierung und zu Schranken im Binnenmarkt führen und die Befolgungskosten für Unternehmen erhöhen, die in mehr als einem Mitgliedstaat tätig sind.

Dieses Problem betrifft die Gesellschaft und die Wirtschaft (Behörden, Unternehmen und Verbraucher) als Ganzes. Insbesondere bestimmte Wirtschaftszweige spielen eine zentrale Rolle für die Bereitstellung unerlässlicher Dienste zur Unterstützung von Wirtschaft und Gesellschaft, weshalb die Sicherheit der von ihnen angebotenen Systeme von besonderem Interesse für einen gut funktionierenden Binnenmarkt ist. Zu diesen Wirtschaftszweigen gehören Banken, Börsen, die Energieerzeugung, -übertragung und -verteilung, der (Luft-, Schienen- und See-)Verkehr, das Gesundheitswesen, Betreiber von Infrastruktur für wichtige Internetdienstleistungen sowie öffentliche Verwaltungen. Im Rahmen der öffentlichen Konsultation sprachen sich die Betroffenen klar für ein Eingreifen im Bereich der NIS in diesen Wirtschaftszweigen und für die Ergreifung von Maßnahmen auf EU-Ebene aus.

Werden keine weiteren Maßnahmen ergriffen, um der zunehmenden Anzahl an Sicherheitsvorfällen entgegenzuwirken, könnte sich dies negativ auf das Vertrauen der Verbraucher in Online-Dienste auswirken, was die Erreichung der Ziele der Digitalen Agenda beeinträchtigen kann.

3.2. Problemfaktoren

Das festgestellte Problem ist auf verschiedene Faktoren zurückzuführen.

Erstens sind die **vorhandenen Kapazitäten innerhalb der EU auf nationaler Ebene unterschiedlich**, wodurch sich in Fachkreisen nur schwer Vertrauen bildet, das jedoch eine Voraussetzung für Zusammenarbeit und Informationsaustausch ist.

Zweitens ist der **Informationsaustausch über Sicherheitsvorfälle, -risiken und -bedrohungen unzureichend**. Die meisten NIS-Vorfälle werden nicht angezeigt und bleiben

unbemerkt. Dies liegt hauptsächlich daran, dass Unternehmen diese Informationen nur widerwillig herausgeben, weil sie negative Auswirkungen auf ihr Ansehen oder gar Haftungsansprüche befürchten. Der Informationsaustausch innerhalb der bestehenden öffentlich-privaten Partnerschaften/Plattformen wie EFMS und EP3R beschränkt sich auf den Austausch bewährter Verfahren.

4. WIRKSAMKEIT DER BISHERIGEN MASSNAHMEN

4.1. Lücken im vorhandenen Regelungsrahmen

Nach den derzeitigen Vorschriften gelten eine Verpflichtung zur Ergreifung von Maßnahmen im Bereich NIS-Risikomanagement und eine Meldepflicht für NIS-Vorfälle nur für Telekommunikationsunternehmen. Gleichwohl sind allen Wirtschaftsteilnehmern, die von Netzen und Informationssystemen abhängen, Sicherheitsrisiken ausgesetzt. Dies führt zu ungleichen Ausgangsbedingungen bei Telekommunikationsbetreibern und VoIP-Anbietern, weil z. B. Sicherheitsvorfälle gleicher Art vom Telekommunikationsbetreiber, nicht aber vom VoIP-Anbieter bei der zuständigen nationalen Behörden gemeldet werden müssten.

Alle für die Datenverarbeitung Verantwortlichen (z. B. Banken oder Krankenhäuser) sind nach dem Datenschutzrechtsrahmen verpflichtet, Sicherheitsmaßnahmen zu ergreifen, die hinsichtlich der bestehenden Risiken verhältnismäßig sind. Allerdings sind diese Verantwortlichen lediglich verpflichtet, Sicherheitsverletzungen zu melden, bei denen der Schutz personenbezogener Daten beeinträchtigt worden ist.

Die Richtlinie 2008/114/EG des Rates über die Ermittlung und Ausweisung europäischer kritischer Infrastrukturen und die Bewertung der Notwendigkeit, ihren Schutz zu verbessern gilt nur für den Energie- und den Verkehrssektor und bisher sind auch nur einige wenige europäische kritische Infrastrukturen von den Mitgliedstaaten ausgewiesen worden. Die Richtlinie sieht für Betreiber weder Meldepflichten für schwerwiegende Sicherheitsverletzungen noch Kooperations- und Reaktionsmechanismen für die Mitgliedstaaten vor.

Die Gesetzgeber verhandeln derzeit über den Vorschlag der Kommission für eine Richtlinie über Angriffe auf Informationssysteme[1]. Der Vorschlag soll lediglich die Strafbarkeit bestimmter Verhaltensweisen, nicht aber die Prävention von Risiken und Sicherheitsvorfällen im NIS-Bereich, die Reaktion darauf oder die Folgenminderung regeln.

4.2. Die Grenzen eines auf Freiwilligkeit basierenden Ansatzes

Der bisher verfolgte freiwillige Ansatz hat zu einem ungleichen Maß an Abwehrbereitschaft und zu einer nur begrenzten Zusammenarbeit geführt.

Der Aufgabenbereich des EFMS ist begrenzt, da die Mitgliedstaaten weder Informationen über Sicherheitsvorfälle, -risiken und -bedrohungen untereinander austauschen noch im Bereich der Bekämpfung grenzüberschreitender Bedrohungen zusammenarbeiten. Das EFMS ist nicht befugt, seine Mitglieder zur Schaffung bestimmter Mindestkapazitäten zu verpflichten.

[1] KOM(2010) 517 endg., http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0517:FIN:DE:PDF.

ENISA hat keine operativen Befugnisse und kann z. B. nicht eingreifen, um NIS-Probleme zu beheben.

Die EP3R hat formal keine Befugnisse und kann somit den Privatsektor nicht verpflichten, den nationalen Behörden Sicherheitsvorfälle zu melden; innerhalb der EP3R gibt es ferner keinen Rahmen für einen vertrauensvollen Informationsaustausch oder die Mitteilung von Informationen über NIS-Bedrohungen, -Risiken und -Vorfälle.

5. NOTWENDIGKEIT DES HANDELNS AUF EU-EBENE, SUBSIDIARITÄT UND VERHÄLTNISMÄSSIGKEIT

Die Gewährleistung der NIS ist für ein ordnungsgemäßes Funktionieren des Binnenmarkts und für das Gemeinwohl unverzichtbar. Artikel 114 AEUV bildet eine geeignete Rechtsgrundlage für die Harmonisierung von NIS-Vorgaben und die Einführung eines gemeinsamen Mindestsicherheitsniveaus in der EU.

Ein Handeln der Union im Bereich NIS ist aufgrund des grenzüberschreitenden Charakters des Problems und der höheren Wirksamkeit etwaiger Maßnahmen auf EU-Ebene (und somit ihres Mehrwerts) im Vergleich zu den bestehenden nationalen Strategien nach dem **Subsidiaritätsprinzip** gerechtfertigt.

Um die Zusammenarbeit aller Mitgliedstaaten zu gewährleisten, muss sichergestellt werden, dass alle Mitgliedstaaten über die erforderlichen Mindestkapazitäten verfügen. Zudem wird sich eine abgestimmte und kooperative NIS-Politik zweifellos äußerst positiv auf die wirksame Wahrung der Grundrechte, insbesondere des Rechts auf den Schutz personenbezogener Daten und den Schutz der Privatsphäre, auswirken.

Die Maßnahmen im Rahmen der bevorzugten Option sind nach dem **Verhältnismäßigkeitsgrundsatz** gerechtfertigt, weil die von den Mitgliedstaaten zu erfüllenden Voraussetzungen bei dem Mindestmaß angesetzt werden, das erforderlich ist, um eine ausreichende Abwehrbereitschaft zu erzielen und eine auf Vertrauen gegründete Zusammenarbeit zu ermöglichen, und weil die von Unternehmen und staatlichen Stellen zu erfüllenden Voraussetzungen ausschließlich für kritische Einrichtungen gelten und Maßnahmen vorgeschrieben werden, die angesichts der Risiken angemessen sind und Sicherheitsvorfälle mit erheblichen Auswirkungen betreffen. Außerdem verursachen die Maßnahmen der bevorzugten Option keine unverhältnismäßig hohen Kosten.

6. ZIELE

Das allgemeine Ziel besteht in einem erhöhten Schutz vor Sicherheitsvorfällen, -risiken und -bedrohungen im Bereich der Netz- und Informationssicherheit in der gesamten EU. Die besonderen Ziele sind folgende:

- **Ziel 1** – Einführung eines gemeinsamen Mindestniveaus der NIS in den Mitgliedstaaten, durch das sich die Abwehrbereitschaft und Reaktionsfähigkeit insgesamt erhöhen.
- **Ziel 2** – Verbesserte Zusammenarbeit im NIS-Bereich auf EU-Ebene, damit grenzüberschreitende Sicherheitsvorfälle und -bedrohungen wirksam bewältigt werden können.
- **Ziel 3** – Schaffung einer Risikomanagementkultur und Verbesserung des Informationsaustauschs zwischen dem privaten und dem öffentlichen Sektor.

7. OPTIONEN

In dieser Folgenabschätzung werden die folgenden Optionen erwogen: Der „Business as usual"-Ansatz, der Regulierungsansatz und der gemischte Ansatz. Die Option, jegliches Handeln der EU im NIS-Bereich einzustellen, bleibt unberücksichtigt.

7.1. Option 1 – Business as usual („Ausgangsszenario")

Mit Hilfe der ENISA würde die Kommission den derzeitigen freiwilligen Ansatz fortführen und die Mitgliedstaaten aufrufen, auf nationaler Ebene NIS-Kapazitäten aufzubauen (z. B. CERTs, nationale Notfallpläne für Cybervorfälle, nationale Cybersicherheitsstrategien) und auf EU-Ebene zusammenzuarbeiten (z. B. über ein europäisches CERT-Netz und einen europäischen Notfall- und Kooperationsplan für Cybervorfälle).

7.2. Option 2 – Regulierungsansatz

Die Kommission würde alle Mitgliedstaaten verpflichten, wenigstens ein Mindestmaß an nationalen Kapazitäten aufzubauen (CERTs, zuständige Behörden, nationale Notfallpläne für Cybervorfälle, nationale Cybersicherheitsstrategien).

Im Rahmen dieses Regulierungsansatzes wären die zuständigen nationalen Behörden und CERTs Teil eines **Netzes** zur Zusammenarbeit auf EU-Ebene. Über dieses Netz würden die Behörden und CERTs Informationen austauschen und zusammenarbeiten, um nach dem **Europäischen Notfall- und Kooperationsplan für Cybervorfälle**, auf den sich die Mitgliedstaaten einigen müssten, NIS-Bedrohungen und -Vorfällen zu begegnen.

In besonders kritischen Wirtschaftszweigen tätige Unternehmen (mit Ausnahme von Kleinstunternehmen), d. h. Banken, Energieversorger (Strom und Erdgas), Verkehrsunternehmen, Unternehmen des Gesundheitssektors, Betreiber von Infrastrukturen für wichtige Internetdienstleistungen sowie öffentliche Verwaltungen, wären gehalten, die für sie bestehenden Risiken zu bewerten und geeignete, angemessene Maßnahmen zu ergreifen, um die tatsächlichen Risiken abzuschätzen. Außerdem müssten diese Einrichtungen den zuständigen Behörden alle Sicherheitsvorfälle melden, die den Betrieb ihrer Netze und Informationssysteme ernsthaft beeinträchtigen und somit beträchtliche Auswirkungen auf die Betriebskontinuität und auf Warenlieferungen haben, die von Netzen und Informationssystemen abhängen. Dieser Ansatz entspricht Artikel 13a und 13b der Rahmenrichtlinie für elektronische Kommunikation.

7.3. Option 3 – Gemischter Ansatz

Die Kommission würde freiwillige, auf der Grundlage der jeweiligen Bereitschaft der Mitgliedstaaten basierende Initiativen zum Aufbau oder zur Stärkung der nationalen NIS-Kapazitäten und zur Einrichtung von Mechanismen für die Zusammenarbeit auf EU-Ebene mit den rechtlichen Vorgaben für wichtige private Wirtschaftsteilnehmer und öffentliche Verwaltungen verbinden.

Freiwillige Initiativen würden im Wesentlichen denen der Option 1 ähneln, während die rechtlichen Vorgaben sowohl im Hinblick auf die betroffenen Einrichtungen als auch den Inhalt der Verpflichtungen mit den unter Option 2 aufgeführten identisch wären.

ENISA würde die Kommission, die Mitgliedstaaten und den Privatsektor unterstützen und ihnen technisches Know-how bereitstellen, z. B. in Form von technischen Leitlinien und Empfehlungen.

8. FOLGENABSCHÄTZUNG

Gegenstand der Folgenabschätzung sind neben dem Sicherheitsniveau auch die wirtschaftlichen und sozialen Auswirkungen der drei Optionen. Ferner werden die im Rahmen der Optionen 2 und 3 entstehenden Kosten beurteilt.

Keine der Optionen hat genau abschätzbare Umweltauswirkungen.

8.1. Option 1 – Business as usual („Ausgangsszenario“)

Sicherheitsniveau: Es ist unwahrscheinlich, dass alle Mitgliedstaaten in vergleichbarem Maße nationale Kapazitäten und Abwehrbereitschaft aufbauen würden, was jedoch erforderlich wäre, um die Sicherheit zu erhöhen, eine Basis für die Zusammenarbeit zu schaffen und einen vertrauensvollen Informationsaustausch auf EU-Ebene zu ermöglichen. In den Bereichen Risikomanagement und Verbesserung der Transparenz bei Sicherheitsvorfällen würden keine gleichen Ausgangsbedingungen erzielt, so dass Rechtslücken nicht geschlossen würden.

Wirtschaftliche Folgen: Die wirtschaftlichen Auswirkungen würden davon abhängen, in welchem Maß die Mitgliedstaaten den Empfehlungen der Kommission folgen. Ein unzureichendes Sicherheitsniveau in den weniger entwickelten Mitgliedstaaten würde deren Wettbewerbsfähigkeit und Wachstum beeinträchtigen und sie Risiken und Sicherheitsstörungen aussetzen. Angesichts der derzeitigen Trends würden NIS-Vorfälle stärker in den Blick von Unternehmen und Verbrauchern rücken und ein Hindernis für die Vollendung des Binnenmarkts darstellen.

Soziale Folgen: Weitere und voraussichtlich schwerwiegendere Sicherheitsvorfälle, -risiken und -bedrohungen würden das Vertrauen der Bürger in Online-Dienste untergraben.

8.2. Option 2 – Regulierungsansatz

Sicherheitsniveau: Durch die für die Mitgliedstaaten geltenden Verpflichtungen wäre sichergestellt, dass alle Mitgliedstaaten angemessen gerüstet sind; dies würde ein Klima gegenseitigen Vertrauens als Voraussetzung für eine wirksame Zusammenarbeit auf EU-Ebene schaffen.

Mit der Einführung von Vorschriften zur Durchführung eines NIS-Risikomanagements für öffentliche Verwaltungen und wichtige private Wirtschaftsteilnehmer würde ein starker Anreiz geschaffen, Sicherheitsrisiken wirksam zu managen und zu bemessen. Die von allen Wirtschaftszweigen in der EU insgesamt zur Einhaltung dieser Vorschriften zu tragenden Mehrkosten würden sich auf **1 bis 2 Mrd. EUR** belaufen. Die Befolgungskosten **für kleine und mittlere Unternehmen** würden **jeweils zwischen 2500 und 5000 EUR** liegen.

Wirtschaftliche Folgen: Durch das erhöhte Sicherheitsniveau würden sich die durch NIS-Risiken und -Vorfälle verursachten finanziellen Verluste verringern. Das Vertrauen der Unternehmen und Verbraucher in die digitale Welt würde gestärkt und dies würde dem

Binnenmarkt zugute kommen. Die Förderung einer verbesserten Risikomanagementkultur würde auch die Nachfrage nach sicheren IKT-Produkten und -Lösungen beleben.

Soziale Folgen: Ein erhöhtes Sicherheitsniveau würde den Bürgern mehr Vertrauen in Online-Dienste geben und es ihnen ermöglichen, uneingeschränkt vom digitalen Angebot (soziale Medien, elektronisches Lernen, elektronische Gesundheitsdienste usw.) zu profitieren.

8.3. Option 3 – Gemischter Ansatz

Sicherheitsniveau: Wie in Option 1 gibt es keine Garantie dafür, dass sich das auf den NIS-Kapazitäten basierende Sicherheitsniveau und die Zusammenarbeit auf EU-Ebene durch freiwillige Initiativen verbessern würden. Andererseits würde durch die Einführung von Sicherheitsanforderungen für öffentliche Verwaltungen und wichtige private Wirtschaftsteilnehmer ein starker Anreiz geschaffen, Sicherheitsrisiken zu managen und zu bestimmen. Dieses System wäre allerdings in denjenigen Mitgliedstaaten unwirksam, die die Empfehlungen der Kommission zum Aufbau von NIS-Kapazitäten nicht umsetzen würden.

Wirtschaftliche Folgen: Das Tempo der Entwicklung wäre in den einzelnen Mitgliedstaaten sehr unterschiedlich. Ein unzureichendes Sicherheitsniveau in den weniger entwickelten Mitgliedstaaten würde deren Wettbewerbsfähigkeit und Wachstum beeinträchtigen und sie den negativen Folgen von Sicherheitsrisiken und -vorfällen aussetzen.

Soziale Folgen: Weitere und voraussichtlich gravierende Sicherheitsvorfälle, -risiken und -bedrohungen würden das Vertrauen in Online-Dienste vor allem in jenen Mitgliedstaaten schwächen, die die NIS nicht als Priorität ansehen.

9. VERGLEICH DER OPTIONEN

Die Optionen 1 und 3 werden zur Erreichung der politischen Ziele als nicht geeignet angesehen und werden folglich nicht empfohlen, weil ihre Wirksamkeit davon abhängen würde, ob der auf Freiwilligkeit basierende Ansatz in der Praxis tatsächlich zu einem Mindestmaß an NIS führen würde; bei Option 3 hängt es von der Bereitschaft der Mitgliedstaaten ab, den Kapazitätenaufbau und die grenzüberschreitende Zusammenarbeit zu fördern.

Bevorzugt wird die Option 2, weil sich durch sie der Schutz der Verbraucher, Unternehmen und Behörden in der EU gegen NIS-Vorfälle, -Bedrohungen und -Risiken erheblich verbessern ließe. Die Bewältigung der internen Herausforderungen würde sich ferner positiv auf die Wirkungskraft der EU auf internationaler Ebene auswirken, so dass die EU zu einem noch glaubwürdigeren Partner in der Zusammenarbeit auf bilateraler und multilateraler Ebene würde. Auch wäre sie in einer besseren Position, um Grundrechte und die Grundwerte der EU jenseits ihrer Grenzen zu fördern.

10. MONITORING UND EVALUIERUNG

In Kapitel 10 der Folgenabschätzung sind ein Reihe von Schlüsselindikatoren für Fortschritte zur Erreichung der Ziele genannt, u. a. folgende:

- für Ziel 1: die Anzahl der Mitgliedstaaten, die eine für die NIS zuständige Behörde und ein CERT benannt oder eine nationale Cybersicherheitsstrategie und einen nationalen Notfall- und Kooperationsplan für Cybervorfälle angenommen haben;
- für Ziel 2: die Anzahl der zuständigen Behörden und CERTs der Mitgliedstaaten, die am Netzwerk teilnehmen sowie die Menge der im Rahmen des Netzwerks für NIS-Risiken und -Vorfälle ausgetauschten Informationen;
- für Ziel 3: die Höhe der von wichtigen privaten Wirtschaftsteilnehmern und öffentlichen Verwaltungen getätigten Investitionen in die NIS und die Anzahl der Meldungen von NIS-Vorfällen mit beträchtlichen Auswirkungen.