Bundesrat **Drucksache 846/08**
05.11.08

EU - A - In - U -
Vk - Wi

Unterrichtung
durch die Bundesregierung

Vorschlag für eine Entscheidung des Rates über ein Warn- und Informationsnetz für kritische Infrastrukturen (CIWIN)
KOM(2008) 676 endg.; Ratsdok. 15041/08

Vertrieb: Bundesanzeiger Verlagsgesellschaft mbH, Amsterdamer Straße 192, 50735 Köln
Telefon: 0221/97668-0, Telefax: 0221/97668-338
ISSN 0720-2946

Übermittelt vom Bundesministerium für Wirtschaft und Technologie am 05. November 2008 gemäß § 2 des Gesetzes über die Zusammenarbeit von Bund und Ländern in Angelegenheiten der Europäischen Union vom 12. März 1993 (BGBl. I S. 313), zuletzt geändert durch das Föderalismusreform-Begleitgesetz vom 5. September 2006 (BGBl. I S. 2098).

Die Kommission der Europäischen Gemeinschaften hat die Vorlage am 28. Oktober 2008 dem Bundesrat zugeleitet.
Die Vorlage ist von der Kommission am 28. Oktober 2008 dem Generalsekretär/Hohen Vertreter des Rates der Europäischen Union übermittelt worden.

Das Europäische Parlament wird an den Beratungen beteiligt.

Hinweis: vgl. Drucksache 851/05 = AE-Nr. 053205,
Drucksache 938/06 = AE-Nr. 061839 und
Drucksache 773/08 = AE-Nr. 080784

BEGRÜNDUNG

KONTEXT DES VORSCHLAGS

Gründe und Ziele des Vorschlags

Auf seiner Tagung vom Juni 2004 beauftragte der Europäische Rat die Kommission mit der Ausarbeitung einer umfassenden Strategie für den Schutz kritischer Infrastrukturen. Daraufhin nahm die Kommission am 20. Oktober 2004 eine Mitteilung mit dem Titel „Schutz kritischer Infrastrukturen im Rahmen der Terrorismusbekämpfung“ an, in der konkrete Vorschläge zur Stärkung der Prävention, Abwehrbereitschaft und Reaktionsfähigkeit in Europa bei terroristischen Anschlägen gegen wichtige Infrastrukturen formuliert wurden. In seinen Schlussfolgerungen vom Dezember 2004 zu „Prävention, Abwehrbereitschaft und Reaktionsfähigkeit bei terroristischen Anschlägen“ sowie zu dem „EU-Solidaritätsprogramm zu den Folgen terroristischer Bedrohungen und Anschläge“ billigte der Rat die Absicht der Kommission, ein europäisches Programm für den Schutz kritischer Infrastrukturen vorzuschlagen, und stimmte der von der Kommission geplanten Einrichtung eines Warn- und Informationsnetzes für kritische Infrastrukturen (CIWIN) zu.

Im Dezember 2006 schlug die Kommission eine Richtlinie über die Ermittlung und Ausweisung kritischer europäischer Infrastrukturen und die Bewertung der Notwendigkeit, ihren Schutz zu verbessern, vor. Gleichzeitig gab sie eine Mitteilung über das Europäische Programm für den Schutz kritischer Infrastrukturen (EPCIP) heraus. Beide Dokumente bilden zusammen den Rahmen für den Schutz kritischer Infrastrukturen in der EU. In der Mitteilung wird ein horizontaler Rahmen für den Schutz kritischer Infrastrukturen in der EU skizziert und erläutert, wie das EPCIP (zusammen mit CIWIN) realisiert werden könnte.

Die CIWIN-Initiative, die Teil des Europäischen Programms für den Schutz kritischer Infrastrukturen ist, betrifft den Informationsaustausch zwischen den EU-Mitgliedstaaten und die dazugehörige Informationstechnologie.

Allgemeiner Kontext

Die Sicherheit und Wirtschaft der Europäischen Union wie auch das Wohlergehen ihrer Bürger hängen von bestimmten Infrastrukturen und deren Diensten ab. So sind Telekommunikations- und Energienetze, Finanzdienstleistungen und Verkehrssysteme, Gesundheitsfürsorge und die Bereitstellung von sauberem Trinkwasser und unbedenklichen Lebensmitteln für die EU und ihre Mitgliedstaaten lebenswichtig. Jede Störung oder Zerstörung solcher wichtigen Infrastrukturen und jede unangemessene Reaktion darauf kann den Verlust von Menschenleben, Sachwerten und Vertrauen zur Folge haben. Komplexe Interdependenzen können dazu führen, dass ein bestimmtes Ereignis einen Kaskadeneffekt in anderen Sektoren und Lebensbereichen auslösen kann, die nicht unmittelbar und offenkundig miteinander verbunden sind. Wechselbeziehungen dieser Art sind nicht ausreichend erforscht, was einen unzureichenden Schutz der kritischen Infrastrukturen und der EU-Bürger zur Folge haben kann.

Die kritischen Infrastrukturen unterliegen zurzeit in der Europäischen Union einer Vielzahl unterschiedlicher Schutzmaßnahmen und Auflagen ohne allgemein geltende Mindeststandards. In einigen Mitgliedstaaten ist die Ermittlung nationaler kritischer Infrastrukturen bereits sehr weit gediehen. Strenge Sicherheitsmaßnahmen wurden ergriffen, und es sind Verfahren und Strukturen vorhanden, die den Schutz dieser Infrastrukturen

sicherstellen. Andere Mitgliedstaaten haben damit gerade erst begonnen. Sie würden erheblich von bewährten Verfahren wie Risikobewertungsmethoden profitieren. Die Problematik lässt sich räumlich (d. h. zwischen den Mitgliedstaaten) und sektorbezogen (d. h. zwischen den verschiedenen Sektoren, die kritische Infrastrukturen aufweisen) betrachten.

Der Informationsaustausch zwischen den Mitgliedstaaten ist eine sehr komplexe Aufgabe, die gut überlegt sein will. Es ist wichtig, Doppelarbeit zu vermeiden, die durch unzureichende Informationen über ähnliche Situationen in anderen Mitgliedstaaten bedingt ist. Mit der Weitergabe bewährter Praktiken könnten die Kosten für die Entwicklung ähnlicher Praktiken in anderen Mitgliedstaaten möglicherweise eingespart werden.

Unbehagen bereitet auch der Austausch sensibler Informationen. Ein effizienter Informationsaustausch ist hier nur möglich, wenn für eine Umgebung gesorgt ist, die Vertrauen und Flexibilität gewährleistet.

Bestehende Rechtsvorschriften auf diesem Gebiet

Der Austausch von Informationen und Warnmeldungen im Bereich des Schutzes kritischer Infrastrukturen ist in der EU nicht geregelt, obwohl die Kommission 2006 eine Richtlinie über die Ermittlung und Ausweisung kritischer europäischer Infrastrukturen und die Bewertung der Notwendigkeit, ihren Schutz zu verbessern, vorgeschlagen hat (KOM(2006) 787 endg.). Damit einher ging eine Mitteilung über das Europäische Programm für den Schutz kritischer Infrastrukturen (KOM(2006) 786 endg.). Im Juni 2008 erzielte der Rat eine politische Einigung über die Richtlinie, die in der zweiten Hälfte 2008 erlassen werden soll.

In der EU gibt es bereits mehrere sektorbezogene Schnellwarnsysteme. Das CIWIN unterscheidet sich von den bestehenden Schnellwarnsystemen in erster Linie durch seinen sektorübergreifenden Ansatz. Derzeit enthält keines der bestehenden Schnellwarnsysteme eine horizontale, sektorübergreifende Komponente, die einem breiteren Kreis von Beteiligten (z. B. nationalen Stellen und Ministerien, die für den Schutz kritischer Infrastrukturen zuständig sind) und nicht nur den Rettungs- und Notfalldiensten zur Verfügung stünde:

– Entscheidung 2007/779/EG, Euratom des Rates über ein Gemeinschaftsverfahren für den Katastrophenschutz (Neufassung)

– Entscheidung 87/600/Euratom des Rates über Gemeinschaftsvereinbarungen für den beschleunigten Informationsaustausch im Fall einer radiologischen Notstandssituation zur Einrichtung eines Systems der Europäischen Gemeinschaft für den Informationsaustausch in radiologischen Notsituationen

– Richtlinie 82/894/EWG des Rates vom 21. Dezember 1982 über die Mitteilung von Viehseuchen in der Gemeinschaft

– Richtlinie 2000/29/EG des Rates über Maßnahmen zum Schutz der Gemeinschaft gegen die Einschleppung und Ausbreitung von Schadorganismen der Pflanzen und Pflanzenerzeugnisse

– Entscheidung Nr. 2119/98/EG des Europäischen Parlaments und des Rates über die Schaffung eines Netzes für die epidemiologische Überwachung und die Kontrolle übertragbarer Krankheiten in der Gemeinschaft

– Richtlinie 2001/95/EG des Europäischen Parlaments und des Rates über die allgemeine Produktsicherheit

– Verordnung (EG) Nr. 178/2002 des Europäischen Parlaments und des Rates zur Festlegung der allgemeinen Grundsätze und Anforderungen des Lebensmittelrechts, zur Errichtung der Europäischen Behörde für Lebensmittelsicherheit und zur Festlegung von Verfahren zur Lebensmittelsicherheit

– Entscheidung 2003/623/EG der Kommission über die Entwicklung eines integrierten EDV-Systems für das Veterinärswesen (TRACES)

– Beschluss 2006/25/EG, Euratom der Kommission zur Änderung ihrer Geschäftsordnung.

Vereinbarkeit mit den anderen Politikbereichen und Zielen der EU

Dieser Vorschlag steht in völligem Einklang mit den Zielen der EU und insbesondere mit der angestrebten „Erhaltung und Weiterentwicklung der Union als Raum der Freiheit, der Sicherheit und des Rechts, in dem in Verbindung mit geeigneten Maßnahmen in Bezug auf die Kontrollen an den Außengrenzen, das Asyl, die Einwanderung sowie die Verhütung und Bekämpfung der Kriminalität der freie Personenverkehr gewährleistet ist“.

Er ist zudem mit anderen Politikbereichen vereinbar, da er nicht darauf abstellt, bestehende Maßnahmen zu ersetzen, sondern diese vielmehr mit Blick auf einen besseren Schutz kritischer europäischer Infrastrukturen ergänzen soll.

KONSULTATION VON INTERESSIERTEN KREISEN UND FOLGENABSCHÄTZUNG

Konsultation von interessierten Kreisen

Konsultationsmethoden, angesprochene Sektoren und allgemeines Profil der Befragten

Alle Beteiligten hatten Gelegenheit, sich im Rahmen der EPCIP-Konsultation zur Einführung eines Warn- und Informationsnetzes zu äußern. Dies geschah in folgender Form:

– Annahme des EPCIP-Grünbuchs am 17. November 2005 mit einer Konsultationsphase bis 15. Januar 2006: 22 Mitgliedstaaten haben im Rahmen der Konsultation geantwortet, und rund 100 Vertreter des Privatsektors haben sich zum Grünbuch geäußert. Der Vorschlag, ein Warn- und Informationsnetz für kritische Infrastrukturen einzurichten, stieß generell auf Zustimmung.

– Informelle Zusammenkünfte der mitgliedstaatlichen Kontaktstellen für den Schutz kritischer Infrastrukturen bei der Kommission (Dezember 2005, Februar 2006, Dezember 2006, November 2007, Februar 2008, März 2008).

– Studie von Unisys über die Einrichtung eines Warn- und Informationsnetzes für kritische Infrastrukturen (CIWIN) vom Januar 2008: Der Auftragnehmer führte hierzu in allen 27 Mitgliedstaaten Befragungen durch.

– Informelle Zusammenkünfte mit Vertretern des Privatsektors: Es wurden zahlreiche informelle Zusammenkünfte mit Vertretern von Privatunternehmen sowie mit Wirtschaftsverbänden veranstaltet.

Zusammenfassung der Antworten und Art ihrer Berücksichtigung

Im Rahmen des thematisch weit gefassten EPCIP-Grünbuchs wurden die Beteiligten zu zahlreichen Aspekten (z. B. Ziel und Grundprinzipien des EPCIP, Vorgehensweise) konsultiert, die auch das Warn- und Informationsnetz betrafen.

Die Antworten auf das EPCIP-Grünbuch und der Meinungsaustausch mit allen Beteiligten haben den Vorschlag zur Einrichtung eines Warn- und Informationsnetzes inhaltlich stark beeinflusst. Anfangs waren sich die Mitgliedstaaten uneins, wie das CIWIN aussehen sollte. Manche befürworteten ein Mehrebenen-Kommunikations- bzw. Warnsystem mit zwei verschiedenen Funktionen: Schnellwarnsystem und elektronische Plattform für den Austausch bewährter Praktiken und Ideen im Bereich des Schutzes kritischer Infrastrukturen. Einige Mitgliedstaaten neigten dagegen dazu, das CIWIN auf seine Rolle als Forum bzw. als Schnellwarnsystem zwischen den Mitgliedstaaten und der Kommission zu beschränken. Zwei Mitgliedstaaten sprachen sich in der Konsultationsphase gegen das CIWIN aus. Da es unterschiedliche Meinungen gab, wurde das Thema mit den Mitgliedstaaten auf den regelmäßigen Zusammenkünften der Kontaktstellen für den Schutz kritischer Infrastrukturen weiter erörtert. Das hier vorliegende Konzept ist das Ergebnis dieses Meinungsaustausches.

Einholung und Nutzung von Expertenwissen

Relevante wissenschaftliche/fachliche Bereiche

Das benötigte Expertenwissen ist bei zahlreichen Zusammenkünften und Seminaren in den Jahren 2006, 2007 und 2008 sowie im Rahmen der Konsultation zu dem EPCIP-Grünbuch eingeholt worden. Darüber hinaus haben alle Beteiligten Informationen beigesteuert.

Methodik

Im März 2006 vergab die Kommission einen Auftrag, der unter anderem eine Durchführbarkeitsstudie zum CIWIN einschloss. Dabei sollten Informationen über bewährte Praktiken für den Schutz kritischer Infrastrukturen eingeholt und Gespräche mit Sachverständigen in den Mitgliedstaaten über die Anforderungen eines Warn- und Informationsnetzes, und zwar sowohl für den Informationsaustausch als auch als Schnellwarnsystem geführt werden, wobei bestehende Infrastrukturen und Netze auf nationaler und internationaler Ebene berücksichtigt werden sollten.

Ein weiteres Ziel war die Einrichtung einer gemeinsamen Plattform für den Austausch von Informationen über den Schutz kritischer Infrastrukturen.

Konsultierte Organisationen/Sachverständige

Alle EU-Mitgliedstaaten.

Zusammenfassung der Stellungnahmen und Gutachten

Keine Hinweise auf potenziell schwerwiegende Risiken mit irreversiblen Folgen

Form der Veröffentlichung der Stellungnahmen

Mittels der Anhänge der Folgenabschätzung

Folgenabschätzung

Im Rahmen des EPCIP-Pakets – genauer in der diesbezüglichen Mitteilung der Kommission – wurde bereits die Annahme eines separaten Vorschlags für die Einrichtung eines Warn- und Informationsnetzes für kritische Infrastrukturen ins Auge gefasst. Bei der Folgenabschätzung wurden fünf Optionen in Betracht gezogen:

Option 1: Beibehaltung des Status quo. Diese Option schließt Querschnittsmaßnahmen auf europäischer Ebene aus. Die Mitgliedstaaten bleiben auf sich gestellt.

Option 2: Das CIWIN als verbessertes Schnellwarnsystem. Diese Option (die sowohl eine Überarbeitung der bestehenden IT-Architektur in funktionaler Hinsicht als auch eine Änderung ihrer Rechtsgrundlage erfordern würde) zielt darauf ab, mithilfe des CIWIN die Interoperabilität der bestehenden Schnellwarnsysteme sicherzustellen und den verschiedenen Diensten innerhalb der EU und in den Ministerien der Mitgliedstaaten den Zugriff auf diese Systeme zu ermöglichen. Da damit lediglich die Schnellwarnfunktion abgedeckt ist, würde jeder weitere Schritt in Richtung auf die Einführung eines Forums für den Austausch von Informationen und bewährten Praktiken nicht unerhebliche Änderungen an den bestehenden Schnellwarnsystemen erfordern, für die beträchtliche Ressourcen bereitgestellt werden müssten.

Option 3: Das CIWIN als offene Plattform für den (ungesicherten) Austausch von Informationen über kritische Infrastrukturen. Diese Option erfordert ein IT-Tool, das wie eine normale Website funktionieren würde und für die breite Öffentlichkeit zugänglich wäre. Dies würde zwar das Bewusstsein für den Schutz kritischer Infrastrukturen in Europa schärfen und den direkten Informationsaustausch zwischen den Beteiligten erhöhen, doch da derjenige, der die Informationen ins Netz stellt, nicht wissen kann, wer die Informationen letztlich nutzt, dürfte sich der Umfang dieser Informationen in Grenzen halten.

Option 4: Das CIWIN als gesichertes Mehrebenen-Kommunikations- bzw. Warnsystem mit zwei verschiedenen Funktionen, dem sich die Mitgliedstaaten freiwillig anschließen können: Schnellwarnsystem und elektronische Plattform für den Austausch bewährter Praktiken und Ideen im Bereich des Schutzes kritischer Infrastrukturen. Nach dieser Option würde das CIWIN als IT-Tool eingerichtet, mit dem sensible, vertrauliche Informationen bis zur Stufe UE RESTREINT gespeichert und übermittelt werden könnten. Das System hätte zwei Hauptfunktionen: 1) ein gesichertes Forum für den Informationsaustausch mit Schwerpunkt auf der Vermittlung bewährter Praktiken, Dialog und Vertrauensbildung auf EU-Ebene; 2) Schnellwarnsystem für kritische Infrastrukturen. Den Mitgliedstaaten stünde es frei, das System vollständig, nur eine der beiden Funktionen oder gar nicht anzuwenden.

Option 5: Das CIWIN als verbindliches Mehrebenen-Kommunikations- bzw. Warnsystem mit zwei verschiedenen Funktionen: Schnellwarnsystem und elektronische Plattform für den Austausch bewährter Praktiken und Ideen im Bereich des Schutzes kritischer Infrastrukturen. Nach dieser Option wäre das CIWIN für alle Mitgliedstaaten verbindlich, und jeder Mitgliedstaat wäre verpflichtet, die Informationen regelmäßig ins Netz zu stellen und zu aktualisieren.

Die Kommission hat, wie in ihrem Arbeitsprogramm vorgesehen, eine Folgenabschätzung vorgenommen. Option 4 (das CIWIN als gesichertes Mehrebenen-Kommunikations- bzw. Warnsystem mit zwei verschiedenen Funktionen: Schnellwarnsystem und elektronische Plattform für den Austausch bewährter Praktiken und Ideen im Bereich des Schutzes

kritischer Infrastrukturen) ergab eindeutig das günstigste Verhältnis zwischen Vor- und Nachteilen. Diese Option würde eine gesicherte Umgebung für den Informationsaustausch bieten, das Vertrauen der Beteiligten untereinander erheblich stärken und den Austausch von Warnmeldungen ermöglichen.

Die CIWIN-Folgenabschätzung ist als Anhang beigefügt.

RECHTLICHE ASPEKTE

Zusammenfassung der vorgeschlagenen Maßnahmen

Die Einrichtung des Warn- und Informationsnetzes soll den Mitgliedstaaten den Austausch von Informationen über gemeinsame Bedrohungen und Schwachstellen sowie über geeignete Maßnahmen und Strategien zur Risikominimierung im Hinblick auf den Schutz kritischer Infrastrukturen erleichtern.

Rechtsgrundlage

Der Vorschlag stützt sich auf Artikel 308 des Vertrags zur Gründung der Europäischen Gemeinschaft und auf Artikel 203 des Vertrags zur Gründung der Europäischen Atomgemeinschaft.

Subsidiaritätsprinzip

Das Subsidiaritätsprinzip gelangt zur Anwendung, da der Vorschlag nicht unter die ausschließliche Zuständigkeit der Gemeinschaft fällt.

Die Ziele des Vorschlags können von den Mitgliedstaaten aus folgendem Grund nicht ausreichend verwirklicht werden:

Dem Subsidiaritätsgrundsatz wird insofern entsprochen, als die Mitgliedstaaten die aus diesem Vorschlag resultierenden Maßnahmen allein nicht erfolgreich durchführen können, so dass ein Tätigwerden auf EU-Ebene erforderlich ist.

Zwar ist jeder Mitgliedstaat für den Schutz der in seinem Hoheitsgebiet gelegenen kritischen Infrastrukturen verantwortlich, doch kann eine alle EU-Mitgliedstaaten umfassende, grenzübergreifende Plattform, die gewährleistet, dass die Informationen allen Mitgliedstaaten, denen sie nützen können, zur Verfügung stehen, nur auf EU-Ebene eingerichtet werden.

Die Ziele des Vorschlags können aus folgenden Gründen besser durch Maßnahmen der Gemeinschaft erreicht werden:

Kein Mitgliedstaat kann allein einen europaweiten Austausch von Informationen oder Schnellwarnungen gewährleisten. Es liegt somit auf der Hand, dass auf EU-Ebene durch die Koordination von Informationen, die zwar unter Umständen bereits verfügbar sind, aber nicht mit anderen geteilt werden, ein Mehrwert erzielt wird.

Nur mit einem Vorgehen auf europäischer Ebene kann gewährleistet werden, dass die Mitgliedstaaten, die bereit sind, Informationen weiterzugeben und entgegenzunehmen, gleichbehandelt werden, dass Mitgliedstaaten nicht aufgrund ihrer geografischen Lage benachteiligt werden und dass die Informationen bei denen ankommen, die sie haben wollen.

Zwischen interdisziplinärer Kooperation auf europäischer Ebene und nationaler Sicherheit besteht ein direkter Zusammenhang. Die heutigen sowohl länder- als auch sektorübergreifenden Interdependenzen haben zur Folge, dass Mitgliedstaaten Dienstleistungen von anderen Mitgliedstaaten beziehen oder dass ihre eigenen Dienstleistungen durch andere Mitgliedstaaten beeinflusst werden. Es besteht die Gefahr, dass ein Mitgliedstaat geschädigt wird, weil ein anderer seine Infrastrukturen im eigenen Land nicht ausreichend geschützt hat.

Immer mehr Infrastrukturen haben europäische Ausmaße angenommen, so dass eine rein nationale Strategie nicht ausreicht. Es ist eindeutig notwendig, sich mit den vielfältigen Gefahren auseinanderzusetzen, die Europas kritische Infrastrukturen bedrohen.

Der Vorschlag steht daher mit dem Subsidiaritätsprinzip im Einklang.

Grundsatz der Verhältnismäßigkeit

Der Vorschlag entspricht aus folgenden Gründen dem Grundsatz der Verhältnismäßigkeit.

Dieser Vorschlag geht nicht über das hinaus, was notwendig ist, um die der mitgliedstaatlichen Zusammenarbeit in diesem Bereich zugrunde liegenden Ziele zu erreichen, insbesondere im Hinblick auf die Kooperationsbereitschaft der Mitgliedstaaten. Den Mitgliedstaaten steht die Teilnahme an dem Warn- und Informationsnetz frei.

Betrachtet man den Nutzen des Warn- und Informationsnetzes, wird das CIWIN weder den EU-Haushalt noch die Finanzen der Mitgliedstaaten in nennenswertem Umfang direkt belasten. Die Instandhaltungskosten dürften sich beispielsweise auf 550 000 € jährlich belaufen, während Störfälle, die das CIWIN verhindern oder beschränken könnte, sehr viel höhere Kosten verursachen würden.

Wahl des Instruments

Vorgeschlagene Instrumente: Entscheidung des Rates

Andere Instrumente wären aus folgenden Gründen nicht angemessen.

Der CIWIN-Prototyp muss auf eine Rechtsgrundlage gestützt werden, um voll einsatzfähig zu sein und von allen EU-Mitgliedstaaten genutzt werden zu können. Da ein spezieller Gegenstand geregelt werden soll und kein Sachverhalt allgemeiner Natur, ist eine Entscheidung des Rates das am besten geeignete Rechtsinstrument, zumal die Nutzer des Systems (Mitgliedstaaten und Kommission) auf diese Weise zur Wahrung der Vertraulichkeit der ausgetauschten Informationen verpflichtet werden können.

AUSWIRKUNGEN AUF DEN HAUSHALT

Der beiliegende Finanzbogen enthält eine Schätzung der Auswirkungen auf den EU-Haushalt. In die Durchführung der Entscheidung wird auch das Programm „Prävention, Abwehrbereitschaft und Folgenbewältigung im Zusammenhang mit Terrorakten und anderen sicherheitsbezogenen Risiken“ (2007-2013) einbezogen.

WEITERE ANGABEN

Simulation, Pilotphase und Übergangszeit

Es gab oder es wird eine Simulation oder eine Pilotphase für den Vorschlag geben.

Überprüfungs-/Revisions-/Verfallsklausel

Der Vorschlag enthält eine Überprüfungsklausel.

Der Vorschlag enthält eine Revisionsklausel.

2008/0200 (CNS)

Vorschlag für eine

ENTSCHEIDUNG DES RATES

über ein Warn- und Informationsnetz für kritische Infrastrukturen (CIWIN)

DER RAT DER EUROPÄISCHEN UNION -

gestützt auf den Vertrag zur Gründung der Europäischen Gemeinschaft, insbesondere auf Artikel 308,

gestützt auf den Vertrag zur Gründung der Europäischen Atomgemeinschaft, insbesondere auf Artikel 203,

auf Vorschlag der Kommission[1],

nach Stellungnahme des Europäischen Parlaments[2],

in Erwägung nachstehender Gründe:

(1) In seinen Schlussfolgerungen vom Dezember 2004 zu „Prävention, Abwehrbereitschaft und Reaktionsfähigkeit bei terroristischen Anschlägen“ sowie zu dem „EU-Solidaritätsprogramm zu den Folgen terroristischer Bedrohungen und Anschläge“ billigte der Rat die Absicht der Kommission, ein europäisches Programm für den Schutz kritischer Infrastrukturen vorzuschlagen, und stimmte der von der Kommission geplanten Einrichtung eines Warn- und Informationsnetzes für kritische Infrastrukturen (CIWIN) zu[3].

(2) Im November 2005 nahm die Kommission ein Grünbuch über ein Europäisches Programm für den Schutz kritischer Infrastrukturen (EPCIP) an, in dem eine Reihe von Optionen vorgeschlagen wurden, wie das Programm für den Schutz kritischer Infrastrukturen und das Warn- und Informationsnetz realisiert werden könnten. Bei der Konsultation zu diesem Grünbuch bekundete die Mehrzahl der Mitgliedstaaten Interesse an der Einrichtung eines Warn- und Informationsnetzes.

(3) Im Dezember 2006 nahm die Kommission eine Mitteilung über das Europäische Programm für den Schutz kritischer Infrastrukturen[4] an, in der sie für das Warn- und Informationsnetz, das als Plattform für den gesicherten Austausch bewährter Praktiken dienen soll, einen separaten Vorschlag ankündigte.

---

1 ABl. C […] vom […], S. […].
2 ABl. C […] vom […], S. […].
3 Dok. 14894/04.
4 KOM(2006) 786 endg.

(4) Mehrere Zwischenfälle bei kritischen Infrastrukturen in Europa wie beispielsweise der Stromausfall in mehreren EU-Ländern im Jahr 2006 machten die Notwendigkeit eines besseren und effizienteren Informationsaustauschs deutlich, um solche Zwischenfälle zu verhindern oder in ihrem Ausmaß zu beschränken.

(5) Es sollte ein Informationssystem eingerichtet werden, das zur Förderung der Integration und besseren Koordinierung der unabhängig voneinander durchgeführten nationalen Forschungsprogramme im Bereich des Schutzes kritischer Infrastrukturen beiträgt und das es den Mitgliedstaaten und der Kommission ermöglicht, Informationen und Warnmeldungen, die den Schutz kritischer Infrastrukturen betreffen, auszutauschen und ihren Dialog in diesem Bereich zu intensivieren.

(6) Das CIWIN sollte durch die Bereitstellung eines Informationssystems, das den Mitgliedstaaten die Zusammenarbeit erleichtern kann, zur Verbesserung des Schutzes kritischer Infrastrukturen in der EU beitragen und eine effiziente, zeitsparende Alternative zu den aufwändigen Verfahren bieten, die für die Suche nach Informationen über kritische Infrastrukturen in der Gemeinschaft zur Verfügung stehen.

(7) Das CIWIN sollte insbesondere die Entwicklung geeigneter Maßnahmen fördern, die den Austausch bewährter Praktiken erleichtern, und gleichzeitig als sicheres Medium für die Mitteilung von unmittelbaren Bedrohungen und die Übermittlung von Warnmeldungen dienen.

(8) Das CIWIN sollte den Besonderheiten, dem Wissensstand, den Vereinbarungen und Zuständigkeiten der sektoralen Schnellwarnsysteme (RAS) Rechnung tragen und Überschneidungen vermeiden.

(9) Die Kommission hat im Wege sektorspezifischer Schnellwarnsysteme, die sich an spezialisierte Stellen innerhalb der EU wenden, über die Jahre die operationellen Kapazitäten aufgebaut, um bei Notfällen der unterschiedlichsten Art Hilfe leisten zu können. Die bestehenden Schnellwarnsysteme verfügen jedoch nicht über eine den Schutz kritischer Infrastrukturen betreffenden Komponente, auf die ein breiterer Kreis von Beteiligten, der über Behörden oder Notfall- und Rettungsdienste hinausgeht, zugreifen könnte.

(10) Angesichts der Interdependenz der kritischen Infrastrukturen in den Mitgliedstaaten und ihres unterschiedlichen Schutzniveaus würde die Einrichtung eines allgemeinen, sektorübergreifenden Gemeinschaftsinstruments für den Austausch von Informationen und Warnmeldungen zum Schutz kritischer Infrastrukturen die Sicherheit der Bürger erhöhen.

(11) Die Kommission sollte unter Berücksichtigung des künftigen Einsatzes des Netzes für gesicherte transeuropäische Telematikdienste für Behörden (s-TESTA) oder anderer von ihr betriebener gesicherter Netze entscheiden, welche technologische Plattform für das CIWIN am besten geeignet ist, und die Endnutzer verpflichten, den von der Kommission festgelegten technischen Anforderungen nachzukommen.

(12) Der Informationsaustausch über kritische Infrastrukturen setzt ein Vertrauensverhältnis zwischen den Beteiligten voraus, so dass geschützte oder

sensible Informationen, die Gegenstand eines freiwilligen Austausches waren, nicht veröffentlicht und angemessen geschützt werden.

(13) Der Zugang zum CIWIN sollte Nutzungsberechtigten gemäß den festgelegten Modalitäten, Verfahren und Sicherheitsmaßnahmen vorbehalten sein. In den Mitgliedstaaten sollte der Zugang den zuständigen nationalen Behörden und in der Kommission den zuständigen Dienststellen vorbehalten sein.

(14) Kosten, die aus dem Betrieb des Warn- und Informationsnetzes auf Gemeinschaftsebene entstehen, sollten aus Gemeinschaftsmitteln und/oder einschlägigen Gemeinschaftsprogrammen bestritten werden.

(15) Kosten, die aus dem Betrieb des Warn- und Informationsnetzes auf nationaler Ebene entstehen, sollten von den Mitgliedstaaten selbst getragen werden, sofern eine Gemeinschaftsvereinbarung nicht etwas anderes bestimmt.

(16) Da das Ziel dieser Entscheidung, nämlich ein sicherer und rascher Informationsaustausch zwischen den Mitgliedstaaten, auf Ebene der Mitgliedstaaten nicht in genügendem Maß erreicht werden kann und wegen der Wirkungen der geplanten Maßnahme besser auf Gemeinschaftsebene zu erreichen ist, kann die Gemeinschaft im Einklang mit dem Subsidiaritätsprinzip gemäß Artikel 5 EG-Vertrag tätig werden. Entsprechend dem in demselben Artikel genannten Verhältnismäßigkeitsprinzip geht diese Entscheidung nicht über das für die Erreichung dieses Ziels erforderliche Maß hinaus.

(17) Die Entscheidung steht im Einklang mit den Grundrechten und Grundsätzen, die insbesondere mit der Charta der Grundrechte der Europäischen Union anerkannt wurden –

HAT FOLGENDE ENTSCHEIDUNG ERLASSEN:

Artikel 1
Gegenstand

Mit dieser Entscheidung wird ein gesichertes Informations-, Kommunikations- und Warnsystem – Warn- und Informationsnetz für kritische Infrastrukturen (CIWIN) – eingerichtet, um den Mitgliedstaaten den Austausch von Informationen über gemeinsame Bedrohungen und Schwachstellen sowie über geeignete Maßnahmen und Strategien zur Risikominimierung im Hinblick auf den Schutz kritischer Infrastrukturen zu erleichtern.

Artikel 2
Begriffsbestimmungen

Für die Zwecke dieser Entscheidung gelten folgende Begriffsbestimmungen:

„Kritische Infrastruktur“: die in den Mitgliedstaaten gelegenen Anlagen, Systeme oder Teile davon, die von wesentlicher Bedeutung für die Aufrechterhaltung vitaler gesellschaftlicher Funktionen, der Gesundheit, der Sicherheit und des wirtschaftlichen oder sozialen Wohlergehens der Bevölkerung sind und deren Störung oder Zerstörung sich auf einen

Mitgliedstaat infolge der Unmöglichkeit, diese Funktionen aufrechtzuerhalten, erheblich auswirken würde;

„Teilnehmende Mitgliedstaaten“: die Mitgliedstaaten, die die Vereinbarung mit der Kommission unterzeichnet haben;

„CIWIN-Beauftragter“: die CIWIN-Kontaktstelle eines Mitgliedstaats oder der Kommission, die gewährleistet, dass das CIWIN vorschriftsgemäß genutzt und dass der Nutzerleitfaden in dem betreffenden Mitgliedstaat oder in der Kommission beachtet wird;

„Bedrohung“: Anzeichen, Umstände oder Ereignisse, die kritische Infrastrukturen oder deren Bestandteile stören oder zerstören können.

Artikel 3
Teilnahme

Die Teilnahme am CIWIN und seine Nutzung steht allen Mitgliedstaaten offen. Voraussetzung für die Teilnahme am CIWIN ist die Unterzeichnung einer Vereinbarung, in der die technischen Spezifikationen sowie die Sicherheitsanforderungen für das CIWIN und die Informationen über die an das CIWIN anzuschließenden Standorte festgelegt sind.

Artikel 4
Funktionalitäten

(1) Das CIWIN ist mit den folgenden zwei Funktionalitäten ausgestattet:

(a) elektronisches Forum für den Austausch von Informationen über den Schutz kritischer Infrastrukturen;

(b) Schnellwarnfunktionalität, die es den teilnehmenden Mitgliedstaaten und der Kommission ermöglicht, Warnmeldungen über kritische Infrastrukturen betreffende unmittelbare Gefahren und Bedrohungen zu übermitteln.

(2) Das elektronische Forum besteht aus festen und je nach Zweck einzurichtenden dynamischen Bereichen.

Feste Bereiche sind dauerhaft in das System integriert. Ihr Inhalt kann geändert werden, sie selbst können jedoch weder entfernt noch umbenannt, noch durch neue Bereiche ergänzt werden. Anhang I enthält eine Liste der festen Bereiche.

Dynamische Bereiche werden nach Bedarf für bestimmte Zwecke geschaffen. Haben sie ihren Zweck erfüllt, werden sie entfernt. Anhang II enthält eine Liste der dynamischen Bereiche, die bei Einrichtung des Warn- und Informationsnetzes vorzusehen sind.

Artikel 5
Aufgaben der Mitgliedstaaten

(1) Die teilnehmenden Mitgliedstaaten benennen einen CIWIN-Beauftragten und setzen die Kommission davon in Kenntnis. Der CIWIN-Beauftragte ist für die Gewährung und Ablehnung von CIWIN-Zugangsrechten in seinem Mitgliedstaat zuständig.

(2) Die teilnehmenden Mitgliedstaaten stellen den Zugang zum CIWIN nach Maßgabe der von der Kommission angenommenen Leitlinien her.

(3) Die teilnehmenden Mitgliedstaaten stellen Informationen von gemeinsamem Interesse, die für den Schutz kritischer Infrastrukturen relevant sind, bereit und aktualisieren sie regelmäßig.

Artikel 6
Aufgaben der Kommission

(1) Die Kommission ist zuständig für

(a) die technische Entwicklung und Verwaltung des CIWIN einschließlich für dessen IT-Struktur und die Elemente für den Informationsaustausch;

(b) die Erstellung eines Leitfadens für die Nutzung des Systems mit Anweisungen, die die Vertraulichkeit, Übermittlung, Speicherung, Archivierung und Löschung von Informationen betreffen. Die Kommission legt überdies die Modalitäten und Verfahren für die Gewährung des unbeschränkten oder selektiven Zugangs zum CIWIN fest.

(2) Die Kommission ernennt einen CIWIN-Beauftragten, der in der Kommission für die Gewährung und Ablehnung von CIWIN-Zugangsrechten zuständig ist.

(3) Die Kommission stellt Informationen von gemeinsamem Interesse, die für den Schutz kritischer Infrastrukturen relevant sind, bereit und aktualisiert sie regelmäßig.

Artikel 7
Sicherheit

(1) Das CIWIN wird als gesichertes System eingerichtet, das Informationen bis zur Stufe „RESTREINT UE“ verarbeiten kann.

Die Kommission entscheidet, welche technologische Plattform am besten für das CIWIN geeignet ist, und die Nutzer werden verpflichtet, den von der Kommission festgelegten technischen Spezifikationen nachzukommen.

Die Sicherheitseinstufung des CIWIN wird bei Bedarf erhöht.

(2) Das Zugriffsrecht der Nutzer bestimmt sich nach dem Umfang, in dem sie Kenntnis von den betreffenden Dokumenten haben müssen, wobei sie jederzeit den Anweisungen des Urhebers, die den Schutz und die Verbreitung der Dokumente betreffen, nachkommen müssen.

(3) Die Mitgliedstaaten und die Kommission treffen die erforderlichen Sicherheitsmaßnahmen, um

(a) Unbefugten den Zugang zum CIWIN zu verwehren;

(b) sicherzustellen, dass Nutzungsberechtigte bei der Nutzung des CIWIN nur Zugriff auf Daten aus ihrem Zuständigkeitsbereich haben;

(c) zu verhindern, dass Unbefugte Informationen im Netz lesen, kopieren, ändern oder löschen.

(4) Das Hochladen von Informationen in das Netz berührt nicht das Eigentum an den betreffenden Informationen. Die Zugangsberechtigten sind allein verantwortlich für die von ihnen bereitgestellten Informationen und müssen sicherstellen, dass deren Inhalt in vollem Umfang mit dem Gemeinschaftsrecht und den innerstaatlichen Vorschriften vereinbar ist.

Artikel 8
Nutzerleitfaden

Die Kommission erstellt einen regelmäßig zu aktualisierenden Nutzerleitfaden, der die Aufgaben und Funktionalitäten des CIWIN umfassend beschreibt.

Artikel 9
Kosten

Die Kosten, die durch den Betrieb, die Instandhaltung und zentrale Funktionen des CIWIN verursacht werden, gehen zulasten des Gemeinschaftshaushalts. Kosten, die mit dem Zugang der Nutzer zum CIWIN in den teilnehmenden Mitgliedstaaten verbunden sind, gehen zulasten der teilnehmenden Mitgliedstaaten.

Artikel 10
Überprüfung

Die Kommission überprüft und bewertet den Betrieb des CIWIN alle drei Jahre und erstattet den Mitgliedstaaten regelmäßig Bericht.

Im ersten Bericht, der innerhalb von drei Jahren nach Inkrafttreten dieser Entscheidung vorzulegen ist, ist auf die Elemente des Gemeinschaftsnetzes hinzuweisen, die verbessert oder angepasst werden sollten. Hält die Kommission eine Änderung oder Anpassung der Entscheidung für erforderlich, fügt sie dem Bericht entsprechende Vorschläge bei.

Artikel 11
Beginn der Geltungsdauer

Diese Entscheidung gilt ab dem 1. Januar 2009.

Artikel 12
Adressaten

Diese Entscheidung ist an die Mitgliedstaaten gerichtet.

Geschehen zu Brüssel am

Im Namen des Rates
Der Präsident

ANHANG I

FESTE CIWIN-BEREICHE

Folgende Bereiche gelten im Sinne von Artikel 4 als feste Bereiche:

(1) Bereiche der Mitgliedstaaten: Jeder teilnehmende Mitgliedstaat kann sich im CIWIN-Portal einen eigenen Bereich schaffen. Für die Organisation, Verwaltung und den Inhalt des Bereichs sind allein die Mitgliedstaaten verantwortlich. Zugangsberechtigt sind nur die Nutzer aus dem betreffenden Mitgliedstaat.

(2) Elf sektorbezogene Bereiche: chemische Industrie, Energie, Finanzsektor, Lebensmittel, Gesundheit, IKT, Kernbrennstoffkreislauf-Industrie, Forschung, Raumfahrt, Verkehr und Wasser. Für allgemeine Themen und Fragen, die für mehrere Sektoren relevant sind, wird ein sektorübergreifender Bereich eingerichtet.

(3) Bereich „CIWIN-Beauftragte“: strategische Plattform für Koordinierung und Zusammenarbeit, die der Förderung und Intensivierung der Arbeiten und der Kommunikation dient, die den Schutz kritischer Infrastrukturen betreffen. Zugangsberechtigt sind nur die CIWIN-Beauftragten.

(4) Zusammenarbeit mit Drittländern: Sensibilisierung für die Zusammenarbeit mit Ländern außerhalb der EU beim Schutz kritischer Infrastrukturen und bei den Schutzstandards.

(5) Adressverzeichnis: In diesem Verzeichnis sind die Namen und Anschriften anderer CIWIN-Nutzer und der Sachverständigen für den Schutz kritischer Infrastrukturen aufgeführt.

ANHANG II

DYNAMISCHE CIWIN-BEREICHE

Folgende Bereiche gelten im Sinne von Artikel 4 als dynamische Bereiche:

(1) Arbeitsgruppen der Sachverständigen: Dieser Bereich dient der Unterstützung der Expertengruppen für den Schutz kritischer Infrastrukturen.

(2) Projekt-Bereich: Dieser Bereich enthält Informationen über Projekte, die von der Kommission finanziert werden.

(3) Bereiche für Warnmeldungen: Wird eine Warnmeldung über das Schnellwarnsystem übermittelt, kann für diese Meldung ein Bereich geschaffen werden, der in der Zeit, in der Maßnahmen zum Schutz kritischer Infrastrukturen laufen, als Kommunikationsweg genutzt wird.

(4) Thematischer Bereich: Bereich, der einzelnen Themen gewidmet ist.

FINANZBOGEN

1. BEZEICHNUNG DES VORGESCHLAGENEN RECHTSAKTS

Entscheidung des Rates über ein Warn- und Informationsnetz für kritische Infrastrukturen (CIWIN)

2. ABM/ABB-RAHMEN

Maßnahme 18.05: Sicherheit und Schutz der Freiheitsrechte

Ziel 2: Schutz kritischer Infrastrukturen

3. HAUSHALTSLINIEN

3.1. Haushaltslinien (operative Linien sowie Linien für entsprechende technische und administrative Unterstützung (vormalige BA-Linien)), mit Bezeichnung:

Haushaltslinie: 18.050800

Rubrik: Prävention, Abwehrbereitschaft und Folgenbewältigung im Zusammenhang mit Terrorakten

3.2. Dauer der Maßnahme und ihrer finanziellen Auswirkungen:

Ab 2009

3.3. Haushaltstechnische Merkmale:

Haushaltslinie	Art der Ausgaben		Neu	EFTA-Beitrag	Beiträge von Bewerberländern	Rubrik des mehrjährigen Finanzrahmens
18.050800	NOA	GM[5]	NEIN	NEIN	NEIN	3A

[5] Getrennte Mittel.

4. RESSOURCEN IM ÜBERBLICK

4.1. Mittelbedarf

4.1.1. Überblick über die erforderlichen Verpflichtungsermächtigungen (VE) und Zahlungsermächtigungen (ZE)

in Mio. EUR (3 Dezimalstellen)

Art der Ausgaben	Abschnitt		2009	2010	2011	2012	2013	Insgesamt
Operative Ausgaben[6]								
Verpflichtungsermächtigungen (VE)	8.1.	a	0,95	0,55	0,55	0,55	0,55	3,15
Zahlungsermächtigungen (ZE)		b	0,95	0,55	0,55	0,55	0,55	3,15
Im Höchstbetrag enthaltene Verwaltungsausgaben[7]								
Technische und administrative Unterstützung (NGM)	8.2.4.	c	n.z.	n.z.	n.z.	n.z.	n.z.	n.z.
HÖCHSTBETRAG								
Verpflichtungsermächtigungen		a+c	0,95	0,55	0,55	0,55	0,55	3,15
Zahlungsermächtigungen		b+c	0,95	0,55	0,55	0,55	0,55	3,15
Im Höchstbetrag <u>nicht</u> enthaltene Verwaltungsausgaben[8]								
Personal- und Nebenkosten (NGM)	8.2.5.	d	0,117	0,117	0,117	0,117	0,117	0,585
Sonstige im Höchstbetrag nicht enthaltene Verwaltungskosten, außer Personal- und Nebenkosten (NGM)	8.2.6.	e	0,015	0,015	0,015	0,015	0,015	0,075
VE INSGESAMT, einschließlich Personalkosten		a+c+d+e	1,082	0,682	0,682	0,682	3,81	

6 Ausgaben, die nicht unter Kapitel XX 01 des betreffenden Titels XX fallen.

7 Ausgaben, die unter Artikel XX 01 04 des Titels XX fallen.

8 Ausgaben, die unter Kapitel XX 01 – außer Artikel XX 01 04 und XX 01 05 – fallen.

ZE INSGESAMT, einschließlich Personalkosten		b+c +d +e	1,082	0,682	0,682	0,682	3,81

4.1.2. Vereinbarkeit mit der Finanzplanung

☒ Der Vorschlag ist mit der derzeitigen Finanzplanung vereinbar.

☐ Der Vorschlag macht eine Anpassung der betreffenden Rubrik des mehrjährigen Finanzrahmens erforderlich.

☐ Der Vorschlag erfordert möglicherweise eine Anwendung der Interinstitutionellen Vereinbarung[9] (z. B. Inanspruchnahme des Flexibilitätsinstruments oder Änderung des mehrjährigen Finanzrahmens).

4.1.3. Finanzielle Auswirkungen auf die Einnahmen

☒ Der Vorschlag hat keine finanziellen Auswirkungen auf die Einnahmen.

☐ Folgende finanzielle Auswirkungen auf die Einnahmen sind zu erwarten:

4.2. Personalbedarf (Vollzeitäquivalent - Beamte, Zeitbedienstete und externes Personal) - Einzelheiten hierzu siehe Abschnitt 8.2.1

Jährlicher Bedarf	2009	2010	2011	2012	2013
Personalbedarf insgesamt	1	1	1	1	1

5. MERKMALE UND ZIELE

5.1. Kurz- oder längerfristig zu deckender Bedarf:

Das CIWIN soll der Koordination und Kooperation in Bezug auf Informationen dienen, die den Schutz kritischer Infrastrukturen auf EU-Ebene betreffen. Das CIWIN soll in erster Linie einen sicheren, strukturierten Informationsaustausch gewährleisten und seinen Nutzern auf diese Weise bewährte Praktiken in anderen EU-Mitgliedstaaten schnell und effizient vermitteln und den Mitgliedstaaten als Schnellwarnsystem für den Schutz kritischer Infrastrukturen zur Verfügung stehen.

5.2. Durch die Gemeinschaftsintervention bedingter Mehrwert, Kohärenz des Vorschlags mit anderen Finanzinstrumenten sowie mögliche Synergieeffekte:

Zwar ist jeder Mitgliedstaat für den Schutz der in seinem Hoheitsgebiet gelegenen kritischen Infrastrukturen verantwortlich, doch kann eine alle EU-Mitgliedstaaten umfassende, grenzübergreifende Plattform, die gewährleistet, dass die Informationen allen Mitgliedstaaten, denen sie nützen können, zur Verfügung stehen, nur auf EU-Ebene eingerichtet werden. Kein Mitgliedstaat kann allein einen europaweiten Austausch von Informationen oder Schnellwarnungen gewährleisten. Es liegt somit auf der Hand, dass auf EU-Ebene durch die

[9] Siehe Nummern 19 und 24 der Interinstitutionellen Vereinbarung.

Koordination von Informationen, die zwar unter Umständen bereits verfügbar sind, aber nicht mit anderen geteilt werden, ein Mehrwert erzielt wird. Nur mit einem Vorgehen auf europäischer Ebene kann gewährleistet werden, dass die Mitgliedstaaten, die bereit sind, Informationen weiterzugeben und entgegenzunehmen, gleichbehandelt werden, dass Mitgliedstaaten nicht aufgrund ihrer geografischen Lage benachteiligt werden und dass die Informationen bei denen ankommen, die sie haben wollen.

5.3. Ziele, erwartete Ergebnisse und entsprechende Indikatoren im Rahmen der ABM-Methodik:

Das CIWIN soll die Entwicklung geeigneter Maßnahmen fördern, die den Austausch bewährter Praktiken erleichtern sollen, und gleichzeitig als sicheres Medium für die Mitteilung von unmittelbaren Bedrohungen und die Übermittlung von Warnmeldungen dienen. Auf diese Weise soll dafür gesorgt werden, dass die richtigen Leute die richtigen Informationen rechtzeitig erhalten.

In der Mitteilung der Kommission über ein Europäisches Programm für den Schutz kritischer Infrastrukturen ist die Einrichtung des CIWIN bereits vorgesehen. Als IT-Tool gehört das CIWIN zu den operativen Zielen des Programms. Das operative (Teil-)Ziel, das mit dem Warn- und Kommunikationsnetz erreicht werden soll, lässt sich wie folgt umreißen:

- Bereitstellung eines IT-Tools, das die Zusammenarbeit der Mitgliedstaaten beim Schutz kritischer Infrastrukturen erleichtert, das eine effiziente, zeitsparende Alternative zu den häufig aufwändigen Verfahren bietet, die für die Suche nach Informationen zur Verfügung stehen, und das den Mitgliedstaaten die Möglichkeit bietet, direkt miteinander in Kontakt zu treten und Informationen ins Netz zu stellen, die sie als sachdienlich ansehen.

5.4. Durchführungsmodalitäten (indikative Angaben):

☒ ***Zentrale Verwaltung***

- ☒ direkt durch die Kommission
- ☐ indirekt im Wege der Befugnisübertragung an:
  - ☐ Exekutivagenturen
  - ☐ die von den Gemeinschaften geschaffenen Einrichtungen im Sinne von Artikel 185 der Haushaltsordnung
  - ☐ einzelstaatliche öffentliche Einrichtungen bzw. privatrechtliche Einrichtungen, die im öffentlichen Auftrag tätig werden

☐ ***Geteilte oder dezentrale Verwaltung***

- ☐ mit Mitgliedstaaten
- ☐ mit Drittländern

☐ ***Gemeinsame Verwaltung mit internationalen Organisationen (bitte auflisten)***

Bemerkungen:

6. ÜBERWACHUNG UND BEWERTUNG

6.1. Überwachungssystem

Zur Beurteilung der durch das CIWIN erzielten Fortschritte sind folgende Indikatoren heranzuziehen:

– Anzahl der am CIWIN teilnehmenden Mitgliedstaaten (damit das System als erfolgreich gelten kann, sollte es von mindestens 20 Mitgliedstaaten regelmäßig genutzt werden)

– Grad der Vertraulichkeit der ausgetauschten Informationen (stellen die Mitgliedstaaten auch Verschlusssachen ins Netz oder nur Informationen, die nicht vertraulich sind?)

– Nutzt die Gruppe der Experten für ihren Meinungsaustausch in erster Linie das CIWIN (z. B. für die Festlegung der Kriterien zur Ermittlung kritischer Infrastrukturen in bestimmten Sektoren)?

6.2. Bewertung

6.2.1. Ex-ante-Bewertung:

Nach Abschluss der Testphase (CIWIN-Pilotprojekt) 2009 wird die Kommission den Behörden der Mitgliedstaaten kurze Fragebögen zusenden, um ihre Zufriedenheit mit dem System zu bewerten und um festzustellen, ob es zu den allgemeinen Zielen der CIWIN-Initiative beiträgt (dabei besteht die Möglichkeit, die Einführung neuer oder die Entfernung nicht zufriedenstellend arbeitender Funktionalitäten vorzuschlagen).

Darüber hinaus wurde eine Folgenabschätzung vorgenommen, die diesem Vorschlag beigefügt ist.

6.2.2. Maßnahmen im Anschluss an Zwischen-/Ex-post-Bewertungen (unter Zugrundelegung früherer Erfahrungen):

Bei der Überwachung und Bewertung sollte auf die „Kundenzufriedenheit“ abgestellt werden.

– Die Funktionsweise des Systems sollte alle drei Jahre von der Kommission überprüft werden. Die Kommission stützt ihre Überprüfung auf die Einschätzung der Mitgliedstaaten, die diese bei den regelmäßigen Zusammenkünften der Kontaktstellen für den Schutz kritischer Infrastrukturen kundtun.

6.2.3. Modalitäten und Periodizität der vorgesehenen Bewertungen:

Drei Jahre nach seiner Einrichtung wird das CIWIN erstmals einer Bewertung anhand der unter 6.1 aufgeführten Indikatoren unterzogen.

7. BETRUGSBEKÄMPFUNGSMAßNAHMEN

Der Schutz der finanziellen Interessen der Gemeinschaft und die Bekämpfung von Betrug und Unregelmäßigkeiten sind Bestandteil dieser Entscheidung.

Die administrative Überwachung der Verträge und Zahlungen obliegt der zuständigen Kommissionsdienststelle. Jede auf der Grundlage dieser Entscheidung finanzierte Maßnahme wird in allen Phasen des Projektzyklus von den zuständigen Kommissionsdienststellen überwacht. Dabei wird den vertraglichen Verpflichtungen sowie den Grundsätzen der Kosten-Nutzen-Analyse und der Wirtschaftlichkeit der Haushaltsführung Rechnung getragen.

Darüber hinaus ist in allen Vereinbarungen oder Verträgen, die nach Maßgabe dieser Entscheidung geschlossen werden, ausdrücklich vorzusehen, dass die im Rahmen der Projekte/Programme genehmigten Ausgaben überwacht, die Maßnahmen ordnungsgemäß durchgeführt und die Finanzkontrolle durch die Kommission, einschließlich durch das Europäische Amt für Betrugsbekämpfung (OLAF), und die Prüfungen des Rechnungshof nötigenfalls vor Ort vorgenommen werden. Die Kommission (OLAF) wird ermächtigt, Kontrollen und Überprüfungen gemäß der Verordnung (Euratom, EG) Nr. 2185/96 des Rates vom 11. November 1996 betreffend die Kontrollen und Überprüfungen vor Ort durch die Kommission zum Schutz der finanziellen Interessen der Europäischen Gemeinschaften vor Betrug und anderen Unregelmäßigkeiten vorzunehmen.

Besonderes Augenmerk wird dabei auf die Art der Ausgaben (Förderfähigkeit der Ausgaben), die Einhaltung der Budgets (tatsächliche Ausgaben) und die Prüfung der Ausgabenbelege und sonstigen diesbezüglichen Unterlagen (Nachweis der Ausgaben) gelegt.

8. RESSOURCEN IM EINZELNEN

8.1. Ziele des Vorschlags und Finanzbedarf

Verpflichtungsermächtigungen, in Mio. EUR (3 Dezimalstellen)

Ziele, Maßnahmen und Outputs (bitte angeben)	**Art der Outputs**	**Durchschnittskosten**	2009		**2010**		**2011**		**2012**		**2013**		**INSGESAMT**	
			Zahl der Outputs	Gesamtkosten	Zahl der Outputs	Gesamtkosten	Zahl der Outputs	Gesamtkosten	Zahl der Outputs	Gesamtkosten	Zahl der Outputs	Gesamtkosten	Zahl der Outputs	Gesamtkosten
OPERATIVES ZIEL Nr.1 [10] **Bereitstellung eines IT-Tools, das die Zusammenarbeit der Mitgliedstaaten beim Schutz kritischer Infrastrukturen erleichtert**														
Maßnahme: Einrichtung und Verwaltung eines Schnellwarnsystems sowie eines Forums für den Austausch bewährter Praktiken														
- Output 1	Hosting der Schnellwarnfunktionalität des CIWIN (gesicherte Umgebung)	0,3	1	0,3	1	0,3	1	0,3	1	0,3	1	0,3	5	1,5

[10] Wie in Abschnitt 5.3 beschrieben.

Ziele, Maßnahmen und Outputs (bitte angeben)	Art der Outputs	Durchschnittskosten	2009		2010		2011		2012		2013		INSGESAMT	
			Zahl der Outputs	Gesamtkosten	Zahl der Outputs	Gesamtkosten	Zahl der Outputs	Gesamtkosten	Zahl der Outputs	Gesamtkosten	Zahl der Outputs	Gesamtkosten	Zahl der Outputs	Gesamtkosten
- Output 2	Unterstützung und Instandhaltung des Systems	0,25	1	0,25	1	0,25	1	0,25	1	0,25	1	0,25	5	1,25
- Output 3	Notwendige technische Unterstützung für die Sicherheitsakkreditierung, Instandhaltung, Bereitstellung eines Helpdesk und Schulung	0,07	1	0,4									1	0,4
GESAMTKOSTEN 1		0, 617	1	0,95	1	0,55	1	0,55	1	0,55	1	0,55	5	3,15

8.2. Verwaltungskosten

8.2.1. Art und Anzahl des erforderlichen Personals

Art der Stellen		Zur Verwaltung der Maßnahme einzusetzendes, vorhandenes und/oder zusätzliches Personal (**Stellenzahl/Vollzeitäquivalent**)									
		2009		2010		2011		2012		2013	
(18)	(20) AD	(21)	0,5	(22)	0,5	(23)	0,5	(24)	0,5	(25)	0,5
(19) Beamte oder Bedienstete auf Zeit[11] (XX 01 01)	AST	0,5		0,5		0,5		0,5		0,5	
Aus Artikel XX 01 02 finanziertes Personal[12]											
Sonstiges, aus Artikel XX 01 04/05 finanziertes Personal[13]											
INSGESAMT		1		1		1		1		1	

8.2.2. Beschreibung der Aufgaben, die im Zuge der vorgeschlagenen Maßnahme auszuführen sind

Den Kommissionsbeamten fällt in erster Linie die Aufgabe des CIWIN-Systemverwalters zu. Die Kommissionsbeamten sind daher zuständig für die Systemkonfiguration, sie nehmen Anträge auf Einrichtung dynamischer Bereiche entgegen, richten diese Bereiche ein und entfernen nicht genutzte oder aufgegebene Bereiche. Die Kommission nimmt die Aufgaben des Systemverwalters wahr.

8.2.3. Zuordnung der Stellen des damit betrauten Statutspersonals

☒ derzeit für die Verwaltung des Programms, das ersetzt oder verlängert werden soll, zugewiesene Stellen

☐ im Rahmen des JSP/HVE-Verfahrens für das Jahr n vorab zugewiesene Stellen

☐ im Rahmen des anstehenden neuen JSP/HVE-Verfahrens anzufordernde Stellen

---

11 Die Kosten hierfür sind NICHT im Höchstbetrag enthalten.

12 Die Kosten hierfür sind NICHT im Höchstbetrag enthalten.

13 Die Kosten hierfür sind im Höchstbetrag enthalten.

☐ innerhalb des für die Verwaltung zuständigen Dienstes neu zu verteilende vorhandene Stellen (interne Personalumsetzung)

☐ für das Jahr n erforderliche, jedoch im Rahmen des JSP/HVE-Verfahrens für dieses Jahr nicht vorgesehene neue Stellen

8.2.4. Sonstige im Höchstbetrag enthaltene Verwaltungsausgaben (XX 01 04/05 - Verwaltungsausgaben)

in Mio. EUR (3 Dezimalstellen)

Haushaltslinie (Nummer und Bezeichnung)	2009	2010	2011	2012	2013	INSGESAMT
1 Technische und administrative Unterstützung (einschließlich Personalkosten)						
Exekutivagenturen[14]	n.z.	n.z.	n.z.	n.z.	n.z.	n.z.
Sonstige technische und administrative Unterstützung	n.z.	n.z.	n.z.	n.z.	n.z.	n.z.
- *intra muros*						
- *extra muros*						
Technische und administrative Unterstützung insgesamt	n.z.	n.z.	n.z.	n.z.	n.z.	n.z.

8.2.5. Im Höchstbetrag nicht enthaltene Personal- und Nebenkosten

in Mio. EUR (3 Dezimalstellen)

Art des Personals	2009	2010	2011	2012	2013
Beamte und Bedienstete auf Zeit (XX 01 01)	0, 117	0, 117	0,117	0,117	0,117
Aus Artikel XX 01 02 finanziertes Personal (Hilfskräfte, ANS, Vertragspersonal usw.) (Angabe der Haushaltslinie)					
Personal- und Nebenkosten insgesamt (NICHT im Höchstbetrag enthalten)	0,117	0,117	0,117	0,117	0,117

Berechnung – *Beamte und Bedienstete auf Zeit*

Vgl. Abschnitt 8.2.1

[14] Hier ist auf den Finanzbogen zum Gründungsrechtsakt der Agentur zu verweisen.

Berechnung – *Aus Artikel XX 01 02 finanziertes Personal*

n.z.

	2009	2010	2011	2012	2013	INSGESAMT
XX 01 02 11 01 – Dienstreisen	0,01	0,01	0,01	0,01	0,01	0,05
XX 01 02 11 02 – Sitzungen & Konferenzen	0,005	0,005	0,005	0,005	0,005	0,025
XX 01 02 11 03 – Ausschüsse[15]	n.z.	n.z.	n.z.	n.z.	n.z.	n.z.
XX 01 02 11 04 – Studien und Konsultationen	n.z.	n.z.	n.z.	n.z.	n.z.	n.z.
XX 01 02 11 05 – Informationssysteme	n.z.	n.z.	n.z.	n.z.	n.z.	n.z.
2 Gesamtbetrag der sonstigen Ausgaben für den Dienstbetrieb (XX 01 02 11)	n.z.	n.z.	n.z.	n.z.	n.z.	n.z.
3 **Sonstige Ausgaben administrativer Art** (Angabe mit Hinweis auf die betreffende Haushaltslinie)	n.z.	n.z.	n.z.	n.z.	n.z.	n.z.
Gesamtbetrag der Verwaltungsausgaben ausgenommen Personal- und Nebenkosten (NICHT im Höchstbetrag enthalten)	0,015	0,015	0,015	0,015	0,015	0,075

Berechnung - *Sonstige nicht im Höchstbetrag enthaltene Verwaltungsausgaben*

n.z.

[15] Angabe des jeweiligen Ausschusses sowie der Gruppe, der dieser angehört.