KOMMISSION DER EUROPÄISCHEN GEMEINSCHAFTEN

Brüssel, den 27.10.2008
SEK(2008) 2702

ARBEITSDOKUMENT DER KOMMISSIONSDIENSTSTELLEN

Begleitdokument zu dem

Vorschlag für eine

ENTSCHEIDUNG DES RATES

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

ZUSAMMENFASSUNG DER FOLGENABSCHÄTZUNG

{KOM(2008) 676 endgültig}
{SEK(2008) 2701}

Am 6. Juni 2008 gab der Ausschuss für Folgenabschätzung der Europäischen Kommission eine Stellungnahme zu einer vorläufigen Fassung dieses Folgenabschätzungsberichts ab. Darin heißt es, dass der Bericht in einer auch dem Nichtfachmann verständlichen Sprache abgefasst ist und eine eingehende Beschreibung der möglichen Systemkonfiguration enthält. Der Ausschuss empfiehlt im Wesentlichen, die bestehenden Warnsysteme präziser zu beschreiben und die Vorteile des CIWIN deutlicher hervorzuheben.

Der Ausschuss stellt darüber hinaus fest:

- Das Referenzszenario sollte ausführlicher dargestellt und der Mehrwert der CIWIN-Initiative stärker hervorgehoben werden.

- Es sollte stärker darauf eingegangen werden, wie die Initiative von den Mitgliedstaaten aufgegriffen wird.

1. DIE CIWIN-INITIATIVE

Die Initiative CIWIN (Warn- und Informationsnetz für kritische Infrastrukturen), die Teil des Europäischen Programms für den Schutz kritischer Infrastrukturen (EPCIP) ist, betrifft den Informationsaustausch zwischen den EU-Mitgliedstaaten und die dazu gehörige Informationstechnologie. In der EPCIP-Mitteilung (KOM(2006) 786 endg.) wird ein horizontaler Rahmen für den Schutz kritischer Infrastrukturen in der EU skizziert, zu dem auch Maßnahmen gehören, die die Durchführung des EPCIP erleichtern sollen. Zu diesen Maßnahmen zählt das CIWIN.

Der Rat hatte bereits 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“ die Einrichtung des CIWIN gebilligt[1].

Zurzeit stellen sich im Wesentlichen folgende Probleme:

- Notwendigkeit einer eingehenderen Analyse der Maßnahmen zum Schutz kritischer Infrastrukturen in der EU

- Notwendigkeit, die Zusammenarbeit und den Informationsaustausch zwischen den Mitgliedstaaten im Bereich der kritischen Infrastrukturen zu verbessern

- Doppelaufwand

- Unzureichendes Vertrauen und ungenügende Bereitschaft der Beteiligten zum Austausch sensibler Informationen.

2. ZIELE

Handlungsbedarf besteht auf EU-Ebene konkret, soweit es um die Erleichterung des Informationsaustauschs zwischen den mitgliedstaatlichen Behörden (z. B. über bewährte

[1] Dok. 14894/04.

Praktiken) und die Bereitstellung eines Schnellwarnsystems zum Schutz kritischer Infrastrukturen geht.

Ziel des CIWIN ist es, den Schutz kritischer Infrastrukturen in der EU zu verbessern und die Koordination und Kooperation in Bezug auf Informationen zu erleichtern, die den Schutz kritischer Infrastrukturen auf EU-Ebene betreffen.

Die operativen Ziele von CIWIN sind:

- Bereitstellung eines IT-Tools, das die Zusammenarbeit der hierzu bereiten Mitgliedstaaten erleichtert

- Angebot einer effizienten, zeitsparenden Alternative zu den häufig aufwändigen Verfahren, die für die Suche nach Informationen zur Verfügung stehen, d. h. Einrichtung einer einzigen Anlaufstelle für alle relevanten Informationen über kritische Infrastrukturen in der EU

- Gewährleistung eines sicheren Informationsaustauschs

- den Mitgliedstaaten die Möglichkeit zu bieten, direkt miteinander in Kontakt zu treten und Informationen ins Netz zu stellen, die sie als sachdienlich ansehen.

Da einige Mitgliedstaaten nur einen Teil der Funktionalitäten nutzen wollen, die das CIWIN bietet, muss eine Lösung gefunden werden, die den Mitgliedstaaten die Möglichkeit gibt, bestimmte Systemkomponenten nicht zu nutzen.

3. OPTIONEN

Bei der Folgenabschätzung wurden fünf Optionen in Betracht gezogen:

Beibehaltung des Status quo

Diese Option schließt ein allgemeines Vorgehen auf europäischer Ebene aus. Die Mitgliedstaaten bleiben auf sich gestellt.

CIWIN als verbessertes Schnellwarnsystem

Die bestehenden Schnellwarnsysteme werden in einem sektorübergreifenden Schnellwarnsystem für kritische Infrastrukturen zusammengefasst, auf das ein breiterer Kreis von Beteiligten, d. h. über Notfall- und Rettungsdienste hinaus, zugreifen könnte. Diese Option schließt allerdings den Austausch von Informationen allgemeiner Art und bewährten Praktiken aus.

CIWIN als offene Plattform für den (ungesicherten) Austausch von Informationen, die den Schutz kritischer Infrastrukturen betreffen

Diese Option sieht die Einrichtung eines IT-Tools vor, das für die breite Öffentlichkeit zugänglich wäre. Dies würde sicherlich dazu beitragen, das Bewusstsein für den Schutz kritischer Infrastrukturen in Europa zu schärfen und den direkten Informationsaustausch zwischen den Beteiligten zu erhöhen.

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.

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 CIWIN für alle Mitgliedstaaten verbindlich und jeder Mitgliedstaat wäre verpflichtet, die Informationen regelmäßig ins Netz zu stellen und zu aktualisieren.

4. VOR- UND NACHTEILE DER EINZELNEN OPTIONEN

Optionen	Vorteile	Nachteile
Option 1: Beibehaltung des Status quo	Kein zusätzlicher Legislativvorschlag. Den Mitgliedstaaten steht es völlig frei, den Schutz kritischer Infrastrukturen nach eigenen Vorstellungen zu organisieren.	Der Dialog und Informationsaustausch zwischen den Mitgliedstaaten bliebe wie gehabt. Kein kohärentes, sicheres und effizientes IT-System für den Austausch von Informationen über den Schutz kritischer Infrastrukturen in Europa. Keine Verbesserung der Sicherheit auf EU-Ebene. Keine Gewähr, dass alle Beteiligten in Europa Zugang zu relevanten Informationen haben.
Option 2: Verbesserung der vorhandenen Schnellwarnsysteme	Einrichtung eines sektorübergreifenden Schnellwarnsystems.	Interoperabilität der vorhandenen Schnellwarnsysteme würde hohe Kosten verursachen. Diese Option schließt den Austausch von Informationen und

		bewährten Praktiken aus. Für den Informationsaustausch müsste auf jeden Fall eine neue Plattform geschaffen werden.
Option 3: offene Plattform für den (ungesicherten) Informationsaustausch	Breiter Zugang zu Informationen über kritische Infrastrukturen. Der Privatsektor hätte direkten Zugriff. Das CIWIN würde einen effizienten, koordinierten, leichten Zugang zu öffentlich bereits verfügbaren Informationen bieten.	Verschlusssachen könnten nicht übermittelt werden. Da die Informationen, die für einen Austausch infrage kommen, bereits an anderer Stelle verfügbar sind, ist mit dieser Option nur ein geringer Mehrwert verbunden. Warnmeldungen könnten nicht ausgetauscht werden.
Option 4: gesichertes Mehrebenensystem, dem sich die Mitgliedstaaten freiwillig anschließen können	Das System würde eine gesicherte Umgebung für den Informationsaustausch bieten und so erheblich zur Vertrauensbildung unter den Beteiligten beitragen. Es würden auch Informationen ausgetauscht, die öffentlich nicht verfügbar sind. Über das System könnten Warnmeldungen ausgetauscht werden. CIWIN würde ein effizientes, benutzerfreundliches IT-System bieten. CIWIN würde zu mehr Sicherheit in der EU beitragen. CIWIN würde durch eine bessere Koordination und Kooperation dazu beitragen, Forschungsarbeiten, die den Schutz kritischer Infrastrukturen betreffen, zusammenzuführen.	Der Privatsektor hätte zum CIWIN keinen direkten Zugang. Der Erfolg des Systems hängt von der Bereitschaft der Mitgliedstaaten ab, es zu nutzen.

Option 5: gesichertes, obligatorisches Mehrebenensystem	Alle Mitgliedstaaten wären dem System angeschlossen. Es würden auch Informationen ausgetauscht, die öffentlich nicht verfügbar sind. Über das System könnten Warnmeldungen ausgetauscht werden. CIWIN würde ein effizientes, benutzerfreundliches IT-System bieten. CIWIN würde zu mehr Sicherheit in der EU beitragen. CIWIN würde durch eine bessere Koordination und Kooperation dazu beitragen, Forschungsarbeiten, die den Schutz kritischer Infrastrukturen betreffen, zusammenzuführen.	Die Mitgliedstaaten würden diesem Vorschlag nicht zustimmen. Ein System, das auf Verpflichtungen basiert, würde nicht zur Vertrauensbildung beitragen und kontraproduktiv wirken. Ein solches System wäre unter Umständen nicht mit dem Verhältnismäßigkeitsprinzip vereinbar.

5. BEVORZUGTE OPTION

Nach Prüfung der fünf Optionen ist festzustellen, dass Option 4 (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) eindeutig das günstigste Verhältnis zwischen Vor- und Nachteilen aufweist.

CIWIN wird die Sicherheit in der EU nicht von Grund auf umgestalten. Das Warn- und Informationsnetz ist nur einer von vielen Schritten zur Umsetzung des EPCIP. CIWIN ist ein IT-Tool, das die Kommunikation über Themen, die den Schutz kritischer Infrastrukturen betreffen, erleichtern soll und Funktionen bietet wie Nachrichtenboard, Diskussionsgruppen, kooperative Umgebungen, Dokumenten- und Vorgangsmanagement, die zum alltäglichen Umgang mit dem Internet oder Firmenintranet gehören. Die Arbeiten am CIWIN werden sich mit einer Vielzahl von Funktionen beschäftigen. Dabei wird jedoch darauf geachtet, dass diese Funktionen neutralisiert werden können, wenn sie keinen Mehrwert bieten oder herkömmlichen Vorgehensweisen entgegenstehen.