RAT DER EUROPÄISCHEN UNION

Brüssel, den 28. Februar 2003 (07.03)
(OR. en)

6946/03

Interinstitutionelles Dossier: 2002/0086 (CNS)

LIMITE

DROIPEN 12
TELECOM 31

BERATUNGSERGEBNISSE

des	Rates
vom	27./28. Februar 2003
Nr. Vordokument:	6671/1/03 REV 1 DROIPEN 11 TELECOM 25
Nr. Kommissionsvorschlag:	8586/02 DROIPEN 29 ECO 143 (COM (2002) 173 final)
Betr.:	Vorschlag für einen Rahmenbeschluss des Rates über Angriffe auf Informationssysteme

Der Rat (Justiz und Inneres) hat den oben genannten Vorschlag auf seiner Tagung am 28. Februar 2003 auf der Grundlage des Dokuments 6671/1/03 REV 1 DROIPEN 11 TELECOM 25 geprüft.

Der Rat (Justiz und Inneres) einigte sich auf eine allgemeine Ausrichtung zu dem in Anlage I enthaltenen Text, vorbehaltlich

- der Aufhebung der Parlamentsvorbehalte der irischen, der französischen, der schwedischen, der dänischen und der niederländischen Delegation,
- der Prüfung der Stellungnahme des Europäischen Parlaments im Lichte der vom Rat festgelegten allgemeinen Ausrichtung,
- der Prüfung der Erwägungsgründe auf der Grundlage des in Anlage I wiedergegebenen Texts, die in Einklang mit der Interinstitutionellen Vereinbarung über die Abfassung von Rechtsvorschriften erfolgen wird.

In Anlage II des vorliegenden Dokuments ist eine Erklärung der Kommission zu Artikel 6 enthalten. Änderungen des Texts im Vergleich zu Dokument 6671/1/03 REV 1 DROIPEN 11 TELECOM 25 sind unterstrichen.

ANLAGE I

Vorschlag für einen
RAHMENBESCHLUSS DES RATES
über Angriffe auf Informationssysteme

DER RAT DER EUROPÄISCHEN UNION -

gestützt auf den Vertrag über die Europäische Union, insbesondere auf Artikel 29, Artikel 30 Absatz 1 Buchstabe a, Artikel 31 und Artikel 34 Absatz 2 Buchstabe b,

auf Vorschlag der Kommission [1],

nach Stellungnahme des Europäischen Parlaments [2],

in Erwägung nachstehender Gründe:

(1) Dieser Rahmenbeschluss stellt darauf ab, durch Angleichung der einzelstaatlichen Strafrechtsvorschriften für Angriffe auf Informationssysteme die Zusammenarbeit zwischen den Justiz- und sonstigen zuständigen Behörden, einschließlich der Polizei und anderer spezialisierter Strafverfolgungsbehörden der Mitgliedstaaten zu verbessern.

(2) Es finden nachweislich - und insbesondere im Rahmen der organisierten Kriminalität - Angriffe auf Informationssysteme statt, und die Furcht vor Terroranschlägen auf Informationssysteme, die Teil der kritischen Infrastruktur der Mitgliedstaaten sind, wächst. Das Ziel des Aufbaus einer sichereren Informationsgesellschaft und eines Raumes der Freiheit, der Sicherheit und des Rechts wird hierdurch gefährdet. Daher bedarf es Gegenmaßnahmen auf Ebene der Europäischen Union.

---

[1] ABl. C ..., S. ... .
[2] ABl. C ..., S. ... .

(3) Um diesen Gefahren wirksam begegnen zu können, ist ein umfassender Ansatz zur Gewährleistung der Sicherheit der Netze und Informationen erforderlich, wie dies im Aktionsplan "*e*Europe", in der Mitteilung der Kommission "Sicherheit der Netze und Informationen: Vorschlag für einen europäischen Politikansatz" [1] und in der Entschließung des Rates vom 6. Dezember 2001 zu einem gemeinsamen Ansatz und spezifischen Maßnahmen im Bereich der Netz- und Informationssicherheit hervorgehoben wurde.

(4) Das Europäische Parlament hat in seiner Entschließung vom 5. September 2001 [2] auf die Notwendigkeit einer stärkeren Sensibilisierung für die Probleme der Informationsgesellschaft und der Gewährung von praktischer Hilfe hingewiesen.

(5) Die Bekämpfung der organisierten Kriminalität und des Terrorismus wird durch beträchtliche Unterschiede und Diskrepanzen zwischen den einschlägigen Rechtsvorschriften der Mitgliedstaaten erschwert, die einer wirksamen polizeilichen und justiziellen Zusammenarbeit gegen Angriffe auf Informationssysteme im Wege stehen. Der länder- und grenzübergreifende Charakter moderner elektronischer Kommunikationsnetze führt dazu, dass Angriffe auf Informationssysteme häufig eine internationale Dimension annehmen, was den dringenden Bedarf an weiteren Maßnahmen zur Angleichung der einschlägigen Strafrechtsvorschriften unterstreicht.

(6) Der Aktionsplan des Rates und der Kommission zur bestmöglichen Umsetzung der Bestimmungen des Amsterdamer Vertrags über den Aufbau eines Raumes der Freiheit, der Sicherheit und des Rechts [3], der Europäische Rat (Tampere, 15./16. Oktober 1999 und Santa Maria da Feira, 19./20. Juni 2000), die Kommission im Anzeiger der Fortschritte [4] und das Europäische Parlament in seiner Entschließung vom 19. Mai 2000 [5] haben legislative Maßnahmen (einschließlich gemeinsamer Definitionen, Tatbestandsmerkmale und Sanktionen) gegen die Hightech-Kriminalität genannt oder gefordert.

---

1 KOM (2001) 298.
2 [2001/2098(INI)].
3 ABl. C 19 vom 23.1.1999.
4 KOM(2001) 278 endg.
5 A5-0127/2000.

(7) Die von internationalen Organisationen und insbesondere vom Europarat geleisteten Arbeiten zur Angleichung des Strafrechts sowie die Arbeiten der G8 zum Thema grenzüberschreitende Zusammenarbeit im Bereich der Hightech-Kriminalität müssen durch einen gemeinsamen Ansatz der Europäischen Union für diesen Bereich ergänzt werden. Diese Anforderung wurde in der Mitteilung der Kommission an den Rat, das Europäische Parlament, den Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen zur "Schaffung einer sichereren Informationsgesellschaft durch Verbesserung der Sicherheit von Informationsinfrastrukturen und Bekämpfung der Computerkriminalität" [1] näher ausgeführt.

(8) Das Strafrecht im Bereich schwerwiegender Angriffe auf Informationssysteme sollte angeglichen werden, um eine möglichst effiziente polizeiliche und justizielle Zusammenarbeit bei Straftaten in Verbindung mit Angriffen auf Informationssysteme sicherzustellen und einen Beitrag zur Bekämpfung der organisierten Kriminalität und des Terrorismus zu leisten.

(9) Die Bezugnahmen auf die Computerkriminalität im Rahmenbeschluss über den Europäischen Haftbefehl [2], im Anhang zum Europol-Übereinkommen und im Beschluss des Rates über die Einrichtung von Eurojust bedürfen einer genaueren Definition. Für die Zwecke dieser Instrumente sollte der Begriff "Computerkriminalität" so verstanden werden, dass er auch Angriffe gegen Informationssysteme im Sinne dieses Rahmenbeschlusses einschließt, denn auf diese Weise lässt sich eine viel stärkere Angleichung der Tatbestandsmerkmale dieser Delikte erreichen. Dieser Rahmenbeschluss ergänzt zudem den Rahmenbeschluss zur Terrorismusbekämpfung [3], der u.a. Terrorhandlungen abdeckt, die weit reichende Zerstörungen von Infrastruktureinrichtungen einschließlich Informationssystemen verursachen und dadurch menschliches Leben gefährden oder großen wirtschaftlichen Schaden anrichten können.

(10) Alle Mitgliedstaaten haben das Übereinkommen des Europarats zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten vom 28. Januar 1981 ratifiziert. Die im Zusammenhang mit der Umsetzung dieses Rahmenbeschlusses verarbeiteten Daten werden gemäss den Grundsätzen des Übereinkommens geschützt werden.

---

1 KOM (2000) 890.
2 ABl. C ..., S. ... .
3 ABl. C ..., S. ... .

(11) Gemeinsame Definitionen in diesem Bereich und insbesondere Definitionen von Informationssystemen und Computerdaten sind im Hinblick auf einen einheitlichen Ansatz in den Mitgliedstaaten für die Umsetzung dieses Rahmenbeschlusses von großer Bedeutung.

(12) Es gilt, einen gemeinsamen Straftatbestand des unberechtigten Zugangs zu Informationssystemen sowie des unrechtmäßigen Eingriffs in ein Informationssystem vorzusehen, um so zu einem gemeinsamen Ansatz im Hinblick auf die Tatbestandsmerkmale von Straftaten zu gelangen.

(13) Nach diesem Rahmenbeschluss sind die Mitgliedstaaten verpflichtet, den rechtswidrigen Zugang zu Informationssystemen als Straftatbestand zu definieren. Der Rahmenbeschluss verpflichtet die Mitgliedstaaten jedoch nicht, die unerlaubte Nutzung von Fernsehen und Kabelfernsehen an sich unter Strafe zu stellen.

(14) Zum Zwecke der besseren Bekämpfung der Cyberkriminalität sollte jeder Mitgliedstaat eine wirksame justizielle Zusammenarbeit bei Straftaten, die auf den in den Artikeln 2, 3, 4 und 5 beschriebenen Vorgehensweisen beruhen, gewährleisten.

(15) Eine Überkriminalisierung insbesondere von geringfügigen oder Bagatelldelikten ist zu vermeiden; ebenso gilt es zu verhindern, dass Rechteinhaber und Zugangsberechtigte (z.B. rechtmäßige private oder geschäftliche Nutzer, Verantwortliche, Aufsichtspersonen und Netz- oder Systembetreiber, rechtmäßige wissenschaftliche Forscher sowie unternehmensinterne oder extern ernannte Zugangsberechtigte, die die Erlaubnis besitzen, die Sicherheit eines Systems zu testen) als Kriminelle eingestuft werden.

(16) Die Mitgliedstaaten müssen Angriffe auf Informationssysteme unter Strafe stellen, wobei diese Strafen wirksam, angemessen und abschreckend sein und in schweren Fällen auch Freiheitsstrafen einschließen müssen.

(17) Für Fälle, in denen ein Angriff auf ein Informationssystem aufgrund der Begleitumstände eine noch größere Gefahr für die Gesellschaft darstellt, sind schwerere Strafen vorzusehen.

In solchen Fällen sollten die gegen die Täter verhängten Strafen so beschaffen sein, dass Angriffe auf Informationssysteme in den Anwendungsbereich der geltenden Rechtsakte zur Bekämpfung der organisierten Kriminalität fallen, so beispielsweise in den Anwendungsbereich der Gemeinsamen Maßnahme 98/733/JI vom 21. Dezember 1998 - vom Rat aufgrund von Artikel K.3 des Vertrags über die Europäische Union angenommen - betreffend die Strafbarkeit der Beteiligung an einer kriminellen Vereinigung in den Mitgliedstaaten der Europäischen Union [1].

(18) Es sind Maßnahmen zu treffen, damit juristische Personen für die von ihnen zu ihrem eigenen Vorteil begangenen Straftaten, auf die sich dieser Rechtsakt bezieht, zur Verantwortung gezogen werden und sichergestellt ist, dass jeder Mitgliedstaat für Straftaten zuständig ist, die gegen Informationssysteme in Situationen begangen werden, in denen sich der Straftäter physisch im Hoheitsgebiet dieses Mitgliedstaates aufhält bzw. in denen sich das Informationssystem im Hoheitsgebiet dieses Staates befindet.

(19) Ferner sind Maßnahmen zur Zusammenarbeit zwischen den Mitgliedstaaten im Hinblick auf eine wirksame Vorgehensweise gegen Angriffe auf Informationssysteme vorzusehen. Die Mitgliedstaaten sollten daher das bestehende Netz der operativen Kontaktstellen für den Informationsaustausch nutzen.

(20) Die Mitgliedstaaten als solche können nicht hinreichend dafür sorgen, dass Angriffe auf Informationssysteme in allen Mitgliedstaaten mit wirksamen, angemessenen und abschreckenden Strafen geahndet werden, und die justizielle Zusammenarbeit durch Beseitigung möglicher Hindernisse in ausreichendem Maße verbessern und fördern. Es bedarf dazu gemeinsamer, miteinander zu vereinbarender Regeln. Diese Ziele können daher auf Unionsebene besser verwirklicht werden. Die Union kann somit in Übereinstimmung mit dem in Artikel 2 EUV genannten und in Artikel 5 EGV definierten Subsidiaritätsprinzip geeignete Maßnahmen treffen. Gemäß dem in Artikel 5 EGV definierten Grundsatz der Verhältnismäßigkeit geht dieser Rahmenbeschluss nicht über das für die Erreichung dieser Ziele erforderliche Maß hinaus.

[1] ABl. L 351 vom 29.12.1998, S. 1.

(21) Dieser Rahmenbeschluss berührt die Befugnisse der Europäischen Gemeinschaft nicht.

(22) Dieser Rahmenbeschluss wahrt die Grundrechte und achtet die Grundsätze, die insbesondere in der Charta der Grundrechte der Europäischen Union, vor allem in den Kapiteln II und VI, anerkannt werden –

HAT FOLGENDEN RAHMENBESCHLUSS ANGENOMMEN:

Artikel 1

Begriffsbestimmungen

Im Sinne dieses Rahmenbeschlusses bezeichnet der Ausdruck

a) *"Informationssystem"* eine Vorrichtung oder eine Gruppe miteinander verbundener oder zusammenhängender Vorrichtungen, die einzeln oder zu mehreren auf der Grundlage eines Programms automatische Verarbeitung von Computerdaten durchführen sowie die von ihr oder ihnen zum Zwecke des Betriebs, der Nutzung, des Schutzes und der Pflege gespeicherten, verarbeiteten oder übertragenen Computerdaten.

b) *"Computerdaten"* die Darstellung von Tatsachen, Informationen oder Konzepten in einer für die Verarbeitung in einem Informationssystem geeigneten Form, einschließlich eines Programms, das die Ausführung einer Funktion durch ein Informationssystem auslösen kann;

c) *"juristische Person"* jedes Rechtssubjekt, das diesen Status nach dem jeweils geltenden innerstaatlichen Recht besitzt, mit Ausnahme von Staaten oder anderen Körperschaften des öffentlichen Rechts in der Ausübung ihrer hoheitlichen Rechte, und von öffentlich-rechtlichen internationalen Organisationen;

d) *"unbefugt"* einen Zugang oder Eingriff, der vom Eigentümer oder einem anderen Rechtsinhaber des Systems oder eines Teils des Systems nicht gestattet wurde, oder der nach den einzelstaatlichen Rechtsvorschriften nicht zulässig ist.

Artikel 2

Rechtswidriger Zugang zu Informationssystemen

(1) Jeder Mitgliedstaat trifft die erforderlichen Maßnahmen, um sicherzustellen, dass der vorsätzliche und unbefugte Zugang zu einem Informationssystem oder einem Teil eines Informationssystems zumindest dann unter Strafe gestellt wird, wenn kein Bagatellfall vorliegt.

(2) Jeder Mitgliedstaat kann beschließen, dass Handlungen nach Absatz 1 nur geahndet werden, sofern sie durch einen Verstoß gegen eine Sicherheitsmaßnahme erfolgen.

Artikel 3

Rechtswidriger Systemeingriff

Jeder Mitgliedstaat trifft die erforderlichen Maßnahmen, um sicherzustellen, dass die unbefugte vorsätzliche schwere Behinderung oder Störung des Betriebs eines Informationssystems, durch Eingabe, Übermittlung, Beschädigung, Löschung, Verstümmelung, Veränderung, Unterdrückung oder Blockierung von Computerdaten, zumindest dann unter Strafe gestellt wird, wenn kein Bagatellfall vorliegt.

Artikel 4

Rechtswidrige Bearbeitung von Daten

Jeder Mitgliedstaat trifft die erforderlichen Maßnahmen, um sicherzustellen, dass die unbefugte vorsätzliche Löschung, Beschädigung, Verstümmelung, Veränderung, Unterdrückung oder Blockierung von Computerdaten eines Informationssystems zumindest dann unter Strafe gestellt wird, wenn kein Bagatellfall vorliegt.

Artikel 5

Anstiftung, Beihilfe und Versuch

(1) Jeder Mitgliedstaat stellt sicher, dass die Anstiftung oder Beihilfe zur Begehung einer der in den Artikeln 2, 3 und 4 beschriebenen Straftaten unter Strafe gestellt wird.

(2) Jeder Mitgliedstaat stellt sicher, dass der Versuch der Begehung einer der in den Artikeln 2, 3 und 4 beschriebenen Straftaten unter Strafe gestellt wird.

(3) Jeder Mitgliedstaat kann beschließen, Absatz 2 auf die in Artikel 2 genannten Straftaten nicht anzuwenden.

Artikel 6

Strafen

(1) Jeder Mitgliedstaat trifft die erforderlichen Maßnahmen, um sicherzustellen, dass die Handlungen nach Artikel 2, 3, 4 und 5 mit wirksamen, angemessenen und abschreckenden Strafen bedroht werden.

(2) Jeder Mitgliedstaat trifft die erforderlichen Maßnahmen, um sicherzustellen, dass die Handlungen nach Artikel 3 und 4 mit einer Freiheitsstrafe im Höchstmaß von mindestens einem bis drei Jahren geahndet werden.

Artikel 7

Erschwerende Umstände

(1) Jeder Mitgliedstaat trifft die erforderlichen Maßnahmen, um sicherzustellen, dass die Handlungen nach Artikel 2 Absatz 2 sowie die Handlungen nach den Artikeln 3 und 4 mit einer Freiheitsstrafe im Höchstmaß von mindestens zwei bis fünf Jahren geahndet werden, wenn sie im Rahmen einer kriminellen Vereinigung im Sinne der Gemeinsamen Maßnahme 98/733/JI vom 21. Dezember 1998 betreffend die Strafbarkeit der Beteiligung an einer kriminellen Vereinigung in den Mitgliedstaaten der Europäischen Union begangen wurden, unabhängig von dem dort vorgesehenen Strafmaß.

(2) Ein Mitgliedstaat kann die in Absatz 1 genannten Maßnahmen auch treffen, wenn durch die Handlungen schwere Schäden verursacht oder wesentliche Interessen beeinträchtigt wurden.

Artikel 8

Verantwortlichkeit juristischer Personen

(1) Jeder Mitgliedstaat trifft die erforderlichen Maßnahmen, um sicherzustellen, dass eine juristische Person für die in den Artikeln 2, 3, 4 und 5 aufgeführten Handlungen verantwortlich gemacht werden kann, die zu ihren Gunsten von einer Person begangen werden, die entweder allein oder als Teil eines Organs der juristischen Person gehandelt hat und die eine Führungsposition innerhalb der juristischen Person innehat aufgrund

a) einer Befugnis zur Vertretung der juristischen Person oder
b) einer Befugnis, Entscheidungen im Namen der juristischen Person zu treffen, oder
c) einer Kontrollbefugnis innerhalb der juristischen Person.

(2) Neben den in Absatz 1 vorgesehenen Fällen trifft jeder Mitgliedstaat die erforderlichen Maßnahmen, um sicherzustellen, dass eine juristische Person verantwortlich gemacht werden kann, wenn mangelnde Überwachung oder Kontrolle durch die in Absatz 1 genannte Person die Begehung der in den Artikeln 2, 3, 4 und 5 genannten Straftaten zugunsten der juristischen Person durch eine ihr unterstellte Person ermöglicht hat.

(3) Die Verantwortlichkeit der juristischen Personen nach den Absätzen 1 und 2 schließt die strafrechtliche Verfolgung natürlicher Personen, die als Täter, Anstifter oder Gehilfe an Handlungen nach den Artikeln 2, 3, 4 und 5 beteiligt sind, nicht aus.

Artikel 9

Sanktionen gegen juristische Personen

(1) Jeder Mitgliedstaat trifft die erforderlichen Maßnahmen, um sicherzustellen, dass gegen eine im Sinne von Artikel 8 Absatz 1 verantwortliche juristische Person wirksame, angemessene und abschreckende Sanktionen verhängt werden können, zu denen Geldbußen oder Geldstrafen sowie andere Sanktionen gehören können, beispielsweise:

a) Ausschluss von öffentlichen Zuwendungen oder Hilfen,
b) vorübergehendes oder ständiges Verbot der Ausübung einer Handelstätigkeit,
c) richterliche Aufsicht oder
d) richterlich angeordnete Eröffnung des Liquidationsverfahrens.

(2) Jeder Mitgliedstaat trifft die erforderlichen Maßnahmen, um sicherzustellen, dass gegen eine im Sinne von Artikel 8 Absatz 2 verantwortliche juristische Person wirksame, angemessene und abschreckende Sanktionen oder Maßnahmen verhängt werden können.

Artikel 10

Gerichtliche Zuständigkeit

(1) Jeder Mitgliedstaat begründet seine gerichtliche Zuständigkeit in Bezug auf die Handlungen nach den Artikeln 2, 3, 4 und 5, wenn diese

a) ganz oder teilweise in seinem Hoheitsgebiet oder
b) von einem seiner eigenen Staatsangehörigen oder
c) zugunsten einer juristischen Personen, deren Hauptsitz sich im Hoheitsgebiet dieses Mitgliedstaates befindet,

begangen wurden.

(2) Bei der Begründung der Zuständigkeit gemäß Absatz 1 Buchstabe a stellt jeder Mitgliedstaat sicher, dass sich diese auch auf Fälle erstreckt, in denen

a) der Täter die Straftat begeht, während er sich physisch im Hoheitsgebiet dieses Staates aufhält, unabhängig davon, ob sich die Straftat gegen ein Informationssystem in seinem Hoheitsgebiet richtet, oder
b) sich die Straftat gegen ein Informationssystem in seinem Hoheitsgebiet richtet, unabhängig davon, ob der Täter die Straftat begeht, während er sich physisch im Hoheitsgebiet dieses Staates aufhält.

(3) Ein Mitgliedstaat, der aufgrund seiner Rechtsvorschriften eigene Staatsangehörige noch nicht ausliefert oder überstellt, trifft die erforderlichen Maßnahmen, um seine gerichtliche Zuständigkeit in Bezug auf die in den Artikeln 2 bis 5 genannten Handlungen zu begründen und gegebenenfalls die Strafverfolgung einzuleiten, sofern diese Handlungen von einem seiner Staatsangehörigen außerhalb seines Hoheitsgebiets begangen wurden.

(4) Fällt eine Straftat in die gerichtliche Zuständigkeit von mehreren Mitgliedstaaten und kann jeder dieser Staaten auf der Grundlage desselben Sachverhalts die Strafverfolgung übernehmen, so entscheiden diese Länder gemeinsam, welches von ihnen die Strafverfolgung gegen den Täter vornimmt, um das Verfahren nach Möglichkeit auf einen Mitgliedstaat zu konzentrieren. Zu diesem Zweck können die Mitgliedstaaten auf jedes Gremium oder jeden Mechanismus auf EU-Ebene zurückgreifen, um die Zusammenarbeit zwischen ihren Justizbehörden und die Koordinierung ihrer Maßnahmen zu erleichtern. Nacheinander kann nachstehenden Anknüpfungspunkten Rechnung getragen werden:

– es handelt sich um den Mitgliedstaat, in dessen Hoheitsgebiet die Straftat begangen wurde, nach Maßgabe von Absatz 1 Buchstabe a und Absatz 2 ;
– es handelt sich um den Mitgliedstaat, dessen Staatsangehöriger der Täter ist;
– es handelt sich um den Mitgliedstaat, in dem der Täter ergriffen wurde.

(5) Ein Mitgliedstaat kann beschließen, die Zuständigkeitsregelung gemäß Absatz 1 Buchstaben b und c nicht oder nur in bestimmten Fällen oder unter bestimmten Umständen anzuwenden.

(6) Beschließen die Mitgliedstaaten die Anwendung des Absatzes 5, so unterrichten sie das Generalsekretariat des Rates und die Kommission entsprechend und teilen gegebenenfalls mit, in welchen speziellen Fällen oder unter welchen speziellen Umständen der Beschluss gilt.

Artikel 11

Informationsaustausch

(1) Zum Zwecke des Informationsaustauschs über die in den Artikeln 2, 3, 4 und 5 genannten Straftaten und im Einklang mit den Datenschutzbestimmungen nutzen die Mitgliedstaaten das bestehende Netz der operativen Kontaktstellen, die rund um die Uhr und sieben Tage pro Woche erreichbar sind.

(2) Jeder Mitgliedstaat setzt das Generalsekretariat des Rates und die Kommission darüber in Kenntnis, welche Kontaktstelle für den Informationsaustausch über Straftaten im Zusammenhang mit Angriffen auf Informationssysteme benannt wurde. Das Generalsekretariat leitet diese Informationen an die übrigen Mitgliedstaaten weiter.

Artikel 12

Umsetzung

(1) Die Mitgliedstaaten treffen die erforderlichen Maßnahmen, um diesem Rahmenbeschluss bis spätestens [...] [1] nachzukommen.

(2) Die Mitgliedstaaten übermitteln dem Generalsekretariat des Rates und der Kommission bis zu diesem Zeitpunkt den Wortlaut der Vorschriften, mit denen ihre Verpflichtungen aus diesem Rahmenbeschluss in innerstaatliches Recht umgesetzt werden. Der Rat prüft bis spätestens 31. Dezember 2004 anhand eines auf der Grundlage dieser Informationen erstellten Berichts und eines schriftlichen Berichts der Kommission, inwieweit die Mitgliedstaaten die erforderlichen Maßnahmen getroffen haben, um diesem Rahmenbeschluss nachzukommen.

Artikel 13

Inkrafttreten

Dieser Rahmenbeschluss tritt am Tag seiner Veröffentlichung im *Amtsblatt der Europäischen Union* in Kraft.

Geschehen zu Brüssel am

Im Namen des Rates
Der Präsident

---

[1] Datum ist noch einzufügen.

ANLAGE II

Erklärung für das Protokoll über die Ratstagung, auf der der Entwurf eines Rahmenbeschlusses über Angriffe auf Informationssysteme angenommen wird

Die Kommission bedauert, dass in Artikel 2 Absatz 2 des Rahmenbeschlusses kein Mindeststrafmaß für die in Artikel 2 genannte Straftat des rechtswidrigen Zugangs vorgesehen ist.