(In Anwendung von Titel VI des Vertrags über die Europäische Union erlassene Rechtsakte)

RAHMENBESCHLUSS 2005/222/JI DES RATES

vom 24. Februar 2005

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 Absatz 1 Buchstabe e) und Artikel 34 Absatz 2 Buchstabe b),

auf Vorschlag der Kommission,

nach Stellungnahme des Europäischen Parlaments [1],

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 es wächst die Besorgnis über das Potenzial an Terroranschlägen auf Informationssysteme, die Teil der kritischen Infrastruktur der Mitgliedstaaten sind. 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.

(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 „eEurope", in der Mitteilung der Kommission „Sicherheit der Netze und Informationen: Vorschlag für einen europäischen Politikansatz" und in der Entschließung des Rates vom 28. Januar 2002 zu einem gemeinsamen Ansatz und spezifischen Maßnahmen im Bereich der Netz- und Informationssicherheit [2] hervorgehoben wurde.

(4) Das Europäische Parlament hat in seiner Entschließung vom 5. September 2001 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 könnte durch beträchtliche Unterschiede und Diskrepanzen zwischen den einschlägigen Rechtsvorschriften der Mitgliedstaaten behindert werden, die eine wirksame polizeiliche und justizielle Zusammenarbeit beim Abwehren von Angriffen auf Informationssysteme erschweren könnten. Der länder- und grenzübergreifende Charakter moderner Informationssysteme führt dazu, dass Angriffe auf solche Systeme häufig eine grenzüberschreitende 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" und das Europäische Parlament in seiner Entschließung vom 19. Mai 2000 haben legislative Maßnahmen (einschließlich gemeinsamer Definitionen, Tatbestandsmerkmale und Sanktionen) gegen die Hightech-Kriminalität genannt oder gefordert.

(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" näher ausgeführt.

(8) Das Strafrecht im Bereich der 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.

[1] ABl. C 300 E vom 11.12.2003, S. 26.
[2] ABl. C 43 vom 16.2.2002, S. 2.
[3] ABl. C 19 vom 23.1.1999, S. 1.

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

(10) 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.

(11) Es gilt, gemeinsame Strafbestände des rechtswidrigen Zugangs zu Informationssystemen, des rechtswidrigen Systemeingriffs und der rechtswidrigen Bearbeitung von Daten vorzusehen, um so zu einem gemeinsamen Ansatz im Hinblick auf die Tatbestandsmerkmale von Straftaten zu gelangen.

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

(13) Eine Überkriminalisierung insbesondere von Bagatellfällen ist zu vermeiden; ebenso gilt es zu verhindern, dass Rechteinhaber und Zugangsberechtigte als Kriminelle eingestuft werden.

(14) Die Mitgliedstaaten müssen Angriffe auf Informationssysteme mit Sanktionen bedrohen. Diese Sanktionen müssen wirksam, verhältnismäßig und abschreckend sein.

(15) Schwerere Strafen sollten für Fälle vorgesehen werden, in denen ein Angriff auf ein Informationssystem 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 [1] begangen wurde. Es ist ferner angemessen, schwerere Strafen vorzusehen, wenn ein solcher Angriff schwere Schäden verursacht oder wesentliche Interessen beeinträchtigt hat.

(16) 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, auf das in der Empfehlung des Rates vom 25. Juni 2001 über Kontaktstellen mit einem rund um die Uhr erreichbaren Dauerdienst zur Bekämpfung der Hightech-Kriminalität [2] verwiesen wird, nutzen.

(17) Da die Ziele dieses Rahmenbeschlusses, nämlich Angriffe auf Informationssysteme in allen Mitgliedstaaten mit wirksamen, verhältnismäßigen und abschreckenden strafrechtlichen Sanktionen zu ahnden und die justizielle Zusammenarbeit durch Beseitigung möglicher Hemmnisse in ausreichendem Maße zu verbessern und zu fördern, auf Ebene der Mitgliedstaaten nicht ausreichend erreicht werden können, und — da es dazu gemeinsamer, miteinander zu vereinbarender Regeln bedarf — besser auf Unionsebene zu erreichen sind, kann die Union im Einklang mit dem in Artikel 5 des Vertrags niedergelegten Subsidiaritätsprinzip tätig werden. Entsprechend dem in demselben Artikel genannten Verhältnismäßigkeitsprinzip geht dieser Rahmenbeschluss nicht über das zur Erreichung dieser Ziele erforderliche Maß hinaus.

(18) Dieser Rahmenbeschluss wahrt die Grundrechte und achtet die Grundsätze, die in Artikel 6 des Vertrags über die Europäische Union und 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 die 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 geltendem Recht besitzt, mit Ausnahme von Staaten oder anderen Körperschaften des öffentlichen Rechts in der Ausübung ihrer hoheitlichen Rechte, und von öffentlich-rechtlichen internationalen Organisationen;

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

[2] ABl. C 187 vom 3.7.2001, S. 5.

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 als Ganzes oder zu einem Teil eines Informationssystems zumindest dann unter Strafe gestellt wird, wenn kein leichter Fall vorliegt.

(2) Jeder Mitgliedstaat kann beschließen, dass Handlungen nach Absatz 1 nur geahndet werden, sofern sie durch eine Verletzung von Sicherheitsmaßnahmen 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 Eingeben, Übermitteln, Beschädigen, Löschen, Verstümmeln, Verändern, Unterdrücken oder Unzugänglichmachen von Computerdaten, zumindest dann unter Strafe gestellt wird, wenn kein leichter Fall vorliegt.

Artikel 4

Rechtswidriger Eingriff in Daten

Jeder Mitgliedstaat trifft die erforderlichen Maßnahmen, um sicherzustellen, dass das unbefugte vorsätzliche Löschen, Beschädigen, Verstümmeln, Verändern, Unterdrücken oder Unzugänglichmachen von Computerdaten eines Informationssystems zumindest dann unter Strafe gestellt wird, wenn kein leichter Fall 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

Sanktionen

(1) Jeder Mitgliedstaat trifft die erforderlichen Maßnahmen, um sicherzustellen, dass die Straftaten nach den Artikeln 2, 3, 4 und 5 mit wirksamen, verhältnismäßigen und abschreckenden strafrechtlichen Sanktionen bedroht werden.

(2) Jeder Mitgliedstaat trifft die erforderlichen Maßnahmen, um sicherzustellen, dass die Straftaten 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 Straftaten nach Artikel 2 Absatz 2 sowie die Straftaten 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 begangen wurden, unabhängig von dem dort vorgesehenen Strafmaß.

(2) Ein Mitgliedstaat kann die in Absatz 1 genannten Maßnahmen auch treffen, wenn durch die Straftaten 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 Straftaten 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 nicht aus, die als Täter, Anstifter oder Gehilfe an der Begehung der in den Artikeln 2, 3, 4 und 5 genannten Straftaten beteiligt sind.

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, verhältnismäßige und abschreckende Sanktionen verhängt werden können, zu denen Geldbußen oder Geldstrafen gehören und zu denen 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, verhältnismäßige und abschreckende Sanktionen oder Maßnahmen verhängt werden können.

Artikel 10

Gerichtliche Zuständigkeit

(1) Jeder Mitgliedstaat begründet seine gerichtliche Zuständigkeit in Bezug auf die Straftaten 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 Mitgliedstaats befindet,

begangen wurden.

(2) Bei der Begründung seiner Zuständigkeit gemäß Absatz 1 Buchstabe a) stellt jeder Mitgliedstaat sicher, dass sich die Zuständigkeit 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, 3, 4 und 5 genannten Straftaten zu begründen und gegebenenfalls die Strafverfolgung einzuleiten, sofern sie 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 Mitgliedstaaten gemeinsam, welcher 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 Ebene der Europäischen Union 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 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 den Bestimmungen dieses Rahmenbeschlusses bis zum 16. März 2007 nachzukommen.

(2) Die Mitgliedstaaten übermitteln dem Generalsekretariat des Rates und der Kommission bis zum 16. März 2007 den Wortlaut der Vorschriften, mit denen ihre Verpflichtungen aus diesem Rahmenbeschluss in innerstaatliches Recht umgesetzt werden. Der Rat prüft bis zum 16. September 2007 anhand eines auf der Grundlage der Informationen und eines schriftlichen Berichts der Kommission erstellten Berichts, inwieweit die Mitgliedstaaten den Bestimmungen dieses Rahmenbeschlusses nachgekommen sind.

Artikel 13

Inkrafttreten

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

Geschehen zu Brüssel am 24. Februar 2005.

Im Namen des Rates

Der Präsident

N. SCHMIT