RAT DER EUROPÄISCHEN UNION

Brüssel, den 8. April 2011 (OR. en)

8795/11

Interinstitutionelles Dossier: 2010/0273 (COD)

DROIPEN 27
TELECOM 43
CODEC 609

VERMERK

des	Vorsitzes
für den	Rat
Nr. Vordokument	8508/11 DROIPEN 24 TELECOM 39 CODEC 561
Betr.:	Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über Angriffe auf Informationssysteme und zur Ersetzung des Rahmenbeschlusses 2005/222/JI des Rates – Orientierungsaussprache und Sachstand

I. ALLGEMEINE INFORMATIONEN

Die Kommission hat dem Europäischen Parlament und dem Rat am 30. September 2010 einen Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über Angriffe auf Informationssysteme und zur Aufhebung des Rahmenbeschlusses 2005/222/JI des Rates unterbreitet.

Gemäß Artikel 3 Absatz 1 des den Verträgen beigefügten Protokolls (Nr. 21) haben das Vereinigte Königreich und Irland dem Rat mitgeteilt, dass sie sich an der Annahme und Anwendung der Richtlinie beteiligen wollen. Gemäß dem den Verträgen beigefügten Protokoll (Nr. 22) beteiligt sich Dänemark nicht an der Annahme dieses Gesetzgebungsakts.

UK hat einen Parlamentsvorbehalt eingelegt. DE, SI, FR und SE haben einen allgemeinen Prüfungsvorbehalt eingelegt.

Der Vorschlag wurde der Gruppe "Allgemeine Angelegenheiten einschließlich Bewertung" am 13. Oktober 2010 und dem Rat auf seiner Tagung am 8./9. November 2010 vorgelegt.
Der Rat hat am 25. Februar 2011 Kenntnis vom Stand der Erörterungen genommen.

Der Koordinierungsausschuss für den Bereich der polizeilichen und justiziellen Zusammenarbeit in Strafsachen (CATS) wurde in drei seiner Sitzungen um strategische Vorgaben für die Beratungen in der Gruppe "Materielles Strafrecht" ersucht. Am 13. Dezember 2010, zu Beginn der Verhandlungen, wurden einige allgemeine Fragen behandelt. Am 11. Februar 2011 prüfte der CATS Artikel 10 Absatz 3 des Kommissionsvorschlags, mit dem ein neuer erschwerender Umstand bei Angriffen auf Informationssysteme eingeführt würde, nämlich der Umstand, dass sie unter Verschleierung der wahren Identität des rechtmäßigen Identitätseigentümers begangen wurden. Am 22. März 2011 schließlich wurde der CATS zu vier noch offenen Fragen betreffend leichte Fälle, die Strafbarkeit nach Artikel 3, das Strafmaß und die gerichtliche Zuständigkeit auf der Grundlage der Staatsangehörigkeit konsultiert.

Die Gruppe "Materielles Strafrecht" hat den Vorschlag in ihren Sitzungen vom 13./14. und 28. Januar sowie vom 2./3. und 29. März 2011 erörtert. Am 29. März 2011 hat sie eine dritte Lesung des Textes abgeschlossen und die Formulierungsvorschläge geprüft, die der Vorsitz eingebracht hatte, um die Beratungen voranzubringen.

Der Vorschlag wurde zudem am 4. April 2011 von den JI-Referenten geprüft.

II. FRAGEN, ZU DENEN POLITISCHE VORGABEN DER MINISTER ERBETEN WERDEN

Im Verlauf der Beratungen wurde der ursprüngliche Kommissionsvorschlag in einer Reihe von Punkten angepasst, um den Bedenken der Delegationen so weit wie möglich Rechnung zu tragen. Der Vorsitz nahm auch die Standpunkte der Delegationen zur Kenntnis, die sich für die Beibehaltung eines ehrgeizigen Textes ausgesprochen haben. Nach Ansicht des Vorsitzes zeichnete sich ein möglicher Kompromiss ab und am 7. April 2011 wurde dem AStV ein entsprechender Vorschlag übermittelt (siehe Anlage I).

Bei den Bratungen des AStV wurde allerdings auch deutlich, dass in einigen politischen Fragen noch weitere Vorgaben des Rates benötigt werden, um den politischen Rahmen festlegen zu können, innerhalb dessen die Gruppe ihre Beratungen fortsetzen soll. Vor diesem Hintergrund möchte der Vorsitz dem Rat die folgenden Fragen unterbreiten:

1. Strafmaß (Artikel 9 Absatz 2) im Verhältnis zur Strafbarkeit (Artikel 3 bis 7)

Infolge der Beratungen in der Gruppe wurden gegenüber dem ursprünglichen Kommissionsvorschlag einige bedeutende Kompromisse aufgenommen, die die Strafbarkeit betreffen. Mit diesen Änderungen soll den besonderen Anliegen einiger Mitgliedstaaten wie folgt Rechnung getragen werden:

- Die Bezugnahme auf "leichte Fälle" wurde auf alle in der Richtlinie aufgeführten Straftatbestände (Artikel 3 bis Artikel 7) ausgeweitet. Leichte Fälle werden daher vollständig vom Geltungsbereich der Richtlinie ausgenommen.
- Der Geltungsbereich des Artikels 3 "Rechtswidriger Zugang zu Informationssystemen" wurde auf Fälle beschränkt, in denen der Verstoß gegen eine Sicherheitsmaßnahme ein Tatbestandsmerkmal ist. Das Übereinkommen von Budapest sah diese Möglichkeit als Option vor, sie wurde jedoch nicht in den ursprünglichen Kommissionsvorschlag aufgenommen.
- Der Besitz von Instrumenten, die zu Angriffen auf Informationssysteme verwendet werden, wurde vom Geltungsbereich des Artikels 7 ausgenommen.

Nach Ansicht des Vorsitzes ist es angesichts dieser beschränkten Strafbarkeit gerechtfertigt, in Bezug auf das Strafmaß für Grundtatbestände (vgl. Artikel 9) den ursprünglichen Kommissionsvorschlag beizubehalten, d.h. Freiheitsstrafen im Höchstmaß von mindestens zwei Jahren. Ferner ist anzumerken, dass der Geltungsbereich der Vorschriften weiter beschränkt wurde, und zwar auf die Artikel 3 bis 6, während für Artikel 7 mithin nicht mehr die Verpflichtung gilt, dieses spezifische Strafmaß vorzusehen.

Allerdings hat eine Gruppe von Mitgliedstaaten nach wie vor ihre Ablehnung geäußert und weiterhin darauf bestanden, dass das Strafmaß auf ein Jahr gesenkt werden sollte. Als Alternative zu dem Strafmaß von einem Jahr ließe sich dieses Ziel auch dadurch erreichen, dass die im Rahmenbeschluss 2005/222/JI vorgesehenen Lösung einer Freiheitsstrafe im Höchstmaß von mindestens ein bis drei Jahren beibehalten wird, da dies in der Praxis bedeutet, dass die Mitgliedstaaten verpflichtet sind, eine Höchststrafe von mindestens einem Jahr vorzusehen.

Der Vorsitz möchte ausdrücklich darauf hinweisen, dass die Lösung für das Strafmaß an den Geltungsbereich des Vorschlags gebunden ist und dass daher im letztgenannten Fall bestimmte Teile des Kompromisspakets, das dem AStV am 7. April 2011 vorgelegt wurde, erneut geprüft werden müssen.

Die Minister werden angesichts der beschränkten Strafbarkeit gebeten, ihre Vorgaben zu folgenden Fragen zu machen:

- *Können Sie dem Strafmaß von zwei Jahren für die Grundtatbestände in Artikel 9 Absatz 2 – wie im Kommissionsvorschlag dargelegt – zustimmen?*
- *Oder unterstützen Sie den von einigen Delegationen vertretenen Standpunkt, das Strafmaß auf eine Freiheitsstrafe im Höchstmaß von mindestens einem Jahr zu senken.*

2. Erschwerende Umstände (Artikel 9 Absätze 3, 4 und 5)

Der Kommissionsvorschlag zielte darauf ab, zwei neue Gefahren der Cyber-Welt dadurch anzugehen, dass zwei erschwerende Umstände im Zusammenhang mit den Grundtatbeständen eingeführt werden. Dabei geht es um

- groß angelegte Cyber-Angriffe über die sogenannten Botnetze (derzeit in Artikel 9 Absatz 3 geregelt) und
- die missbräuchliche Verwendung personenbezogener Daten einer anderen Person, um das Vertrauen eines Dritten zu gewinnen, was in der Praxis die Durchführung von Cyber-Angriffen erleichtert (derzeit in Artikel 9 Absatz 5 geregelt).

Diese Bestimmungen wurden – obwohl es sich um grundsätzliche Aspekte der Zielsetzung der Kommission handelte – im Laufe der Beratungen erheblich geändert, um den Anliegen der Delegationen Rechnung zu tragen, wobei gleichzeitig der Vorschlag der Kommission zu diesen Fragen inhaltlich beibehalten wurde.

Was das Strafmaß für erschwerende Umstände anbelangt, so lässt der derzeitige Text mehr Flexibilität als der ursprüngliche Kommissionsvorschlag zu. Er sieht zwei verschiedene Schwellenwerte vor, und zwar Freiheitsstrafen im Höchstmaß von mindestens drei bzw. fünf Jahren, je nach Schwere der Straftat, wobei neue Bedingungen dazu aufgenommen wurden, in welchem Fall die Höchststrafe anzuwenden wäre. Falls der Angriff schweren Schaden verursacht oder ein Informationssystem beschädigt hat, das Teil der kritischen Infrastruktur ist, beträgt die vorgeschlagene Höchstfreiheitsstrafe demnach mindestens fünf Jahre.

Die missbräuchliche Verwendung der Identität eines Dritten wird als rein erschwerender Umstand in Artikel 9 Absatz 5 aufgenommen, ohne dass ein spezifisches Strafmaß vorgesehen würde, wobei es den Mitgliedstaaten überlassen bleibt, wie sie das gewünschte Ergebnis erreichen. Im Verlauf der Beratungen wurde wiederholt bemerkt, dass dieser Tatbestand von einem Identitätsdiebstahl, der eine teilweise anders gelagerte komplexe Erscheinung darstellt, abgegrenzt werden sollte. Gleichzeitig wäre in Bezug auf Cyberangriffe anzumerken, dass oftmals von diesem Modus operandi Gebrauch gemacht wird, um schwere Straftaten der Computerkriminalität zu begehen.

Einige Delegationen würden es nach wie vor bevorzugen, diese Komponente aus der Richtlinie herauszunehmen, da sie in einem eigenen Rechtsinstrument, das ganz generell den Identitätsdiebstahl erfasst, behandelt werden sollte. Was die andere neue Komponente des Kommissionsvorschlags, nämlich die Verwendung eines Instruments für quantitativ oder qualitativ besonders folgenreiche Angriffe (Artikel 9 Absatz 3) anbelangt, so stieß sie bei den Delegationen auf ein gewisses Maß an Widerstand.

Die Minister werden ersucht, eine Richtschnur in der Frage vorzugeben, ob das Konzept einer mithilfe von Botnetzen begangenen Straftat als erschwerender Umstand beibehalten oder aus dem Entwurf gestrichen werden sollte.

Die Minister werden ersucht, eine Richtschnur in der Frage vorzugeben, ob das Konzept der missbräuchlichen Verwendung der Identität eines Dritten als erschwerender Umstand beibehalten oder aus dem Entwurf gestrichen werden sollte.

> Sollte diese Frage bejaht werden, so wird die Formulierung auf Expertenebene entsprechend angepasst.

3. Gerichtliche Zuständigkeit (Artikel 13)

Der Aspekt der gerichtlichen Zuständigkeit war Gegenstand eingehender Beratungen der Gruppe. Der Kompromisstext in Artikel 13 weicht vom ursprünglichen Vorschlag der Kommission ab und orientiert sich am diesbezüglichen Ansatz der Richtlinie gegen Menschenhandel. Ferner wird als Mindeststandard die Anforderung einer positiven doppelten Strafbarkeitsüberprüfung aufgenommen, und zwar insbesondere in Bezug auf eigene Staatsangehörige, wenn die Straftat außerhalb des Staatsgebiets des betreffenden Mitgliedstaats begangen worden ist (Artikel 13 Absatz 1 Buchstabe b). Die Voraussetzungen für die Ausübung der einzelstaatlichen gerichtlichen Zuständigkeit sind nicht Gegenstand der Richtlinie, wie in dem neu aufgenommenen Erwägungsgrund 10a niedergelegt ist.

Die Minister werden um Bestätigung ersucht, dass die gerichtliche Zuständigkeit in Bezug auf die eigenen Staatsangehörigen im Anwendungsbereich des Vorschlags beibehalten wird.

4. Tatwerkzeuge – Strafbarkeit der Verwendung bestimmter Vorrichtungen (Artikel 7)

Die Gruppe bestätigte die Auslegung des Anwendungsbereichs des Artikels 7 des Entwurfs im Einklang mit Artikel 6 des Budapester Übereinkommens über Computerkriminalität.

In Artikel 6 Absatz 3 des Übereinkommens ist jedoch vorgesehen, dass jede Vertragspartei des Übereinkommens die Möglichkeit hat, einige Teile dieser Bestimmung nicht anzuwenden, und zwar auch, wenn es um eine Vorrichtung geht, die "in erster Linie dafür ausgelegt oder hergerichtet" worden ist, Cyberangriffe zu begehen. Der Umstand, dass eine derartige Ausnahme im Vorschlag der Kommission nicht vorgesehen ist, erweist sich für eine Delegation als problematisch.

Diesbezüglich schlägt der Vorsitz folgende Kompromissformulierung vor:

Artikel 7

Tatwerkzeuge

(1) Die Mitgliedstaaten treffen die erforderlichen Maßnahmen, um sicherzustellen, dass das vorsätzliche unbefugte Herstellen, Verkaufen, Beschaffen zwecks Gebrauchs, Einführen, Verbreiten oder anderweitige Verfügbarmachen folgender Instrumente, die dazu bestimmt sind, eine Straftat im Sinne der Artikel 3 bis 6 zu begehen, zumindest dann unter Strafe gestellt wird, wenn kein leichter Fall vorliegt:

a) (…) eines Computerprogramms, <u>das</u> in erster Linie dafür ausgelegt oder hergerichtet worden ist, eine Straftat im Sinne der Artikel 3 bis 6 zu begehen;

b) eines Computerpassworts, eines Zugangscodes oder ähnlicher Daten, die den Zugang zu einem Informationssystem als Ganzem oder zu einem Teil davon ermöglichen.

<u>(2) Die Mitgliedstaaten können ferner die erforderlichen Maßnahmen treffen, um sicherzustellen, dass das Herstellen, Verkaufen, Beschaffen zwecks Gebrauchs, Einführen, Verbreiten oder anderweitige Verfügbarmachen aller anderen Vorrichtungen, die in erster Linie dafür ausgelegt oder hergerichtet worden sind, eine Straftat im Sinne der Artikel 3 bis 6 zu begehen, zumindest dann, wenn kein leichter Fall vorliegt, als Straftat unter Strafe gestellt wird, wenn die Vorrichtung vorsätzlich und unbefugt in der Absicht verwendet wurde, eine Straftat im Sinne der Artikel 3 bis 6 zu begehen.</u>

Die Minister werden ersucht, den Kompromissvorschlag des Vorsitzes zu Artikel 7 zu bestätigen.

III. SACHSTAND

Der Vorsitz vertritt die Auffassung, dass bei einer Reihe von Bestimmungen eine vorläufige Einigung erzielt wurde. Hierbei handelt es sich um folgende Bestimmungen: Artikel 1 bis 6 und Artikel 11 bis 19.

Daher wird der Rat ersucht, festzustellen, dass der Text der Artikel 1 bis 6 und der Artikel 11 bis 19 (siehe Anlage II) Gegenstand einer vorläufigen Einigung ist, wobei jedoch gilt, dass es sich im weiteren Verlauf der Beratungen durchaus als notwendig erweisen kann, jede einzelne dieser Bestimmungen erneut auf den Prüfstand zu stellen.

ANLAGE I

2010/0273 (COD)

Vorschlag für eine

RICHTLINIE DES EUROPÄISCHEN PARLAMENTS UND DES RATES

über Angriffe auf Informationssysteme und zur Ersetzung des Rahmenbeschlusses 2005/222/JI des Rates

DAS EUROPÄISCHE PARLAMENT UND DER RAT DER EUROPÄISCHEN UNION –
gestützt auf den Vertrag über die Arbeitsweise der Europäischen Union, insbesondere auf Artikel 83 Absatz 1,
auf Vorschlag der Europäischen Kommission[1],
nach Zuleitung des Entwurfs des Gesetzgebungsakts an die nationalen Parlamente,
nach Stellungnahme des Europäischen Wirtschafts- und Sozialausschusses,
nach Stellungnahme des Ausschusses der Regionen,
gemäß dem ordentlichen Gesetzgebungsverfahren,
in Erwägung nachstehender Gründe:

(1) Ziel dieser Richtlinie ist die Angleichung der einzelstaatlichen Strafvorschriften für Angriffe auf Informationssysteme sowie die Verbesserung der Zusammenarbeit zwischen den zuständigen Behörden einschließlich der Polizei und anderer spezialisierter Strafverfolgungsbehörden der Mitgliedstaaten.

[1] ABl. C […] vom […], S. […].

(2) Angriffe auf Informationssysteme – insbesondere im Rahmen der organisierten Kriminalität – werden zunehmend zu einer Bedrohung, und es wächst die Besorgnis über mögliche Terroranschläge oder politisch motivierte Attacken auf Informationssysteme, die Teil der kritischen Infrastruktur der Mitgliedstaaten und der Europäischen Union sind. Hierdurch wird das Ziel einer sichereren Informationsgesellschaft und eines Raums der Freiheit, der Sicherheit und des Rechts gefährdet, so dass Gegenmaßnahmen auf Ebene der Europäischen Union erforderlich sind.

(2a) "Es gibt in der Union eine Reihe wichtiger Infrastrukturen, deren Störung oder Zerstörung erhebliche grenzüberschreitende Auswirkungen hätte. Da die Fähigkeit zum Schutz kritischer Infrastrukturen in ganz Europa verbessert werden muss, sollte die Bekämpfung von Angriffen auf Informationssysteme durch schwere strafrechtliche Sanktionen, die der Schwere derartiger Angriffe Rechnung tragen, ergänzt werden. Als kritische Infrastrukturen sind in einem Mitgliedstaat gelegene Anlagen, Systeme oder Teile derselben zu verstehen, die beispielsweise von wesentlicher Bedeutung für die Aufrechterhaltung wichtiger gesellschaftlicher Funktionen, der Gesundheit, der Sicherheit und des wirtschaftlichen oder sozialen Wohlergehens der Bevölkerung sind und deren Störung oder Zerstörung erhebliche Auswirkungen auf einen Mitgliedstaat hätte, da diese Funktionen nicht aufrechterhalten werden könnten."

(3) Es besteht eine Tendenz zu immer gefährlicheren und häufigeren Großangriffen auf Informationssysteme, die für den Staat oder für bestimmte Funktionen im öffentlichen oder privaten Sektor unverzichtbar sind. Diese Tendenz geht einher mit der Entwicklung immer ausgefeilterer Instrumente, die von Kriminellen zu Cyberangriffen unterschiedlichster Art genutzt werden können.

(4) Für eine einheitliche Strategie in den Mitgliedstaaten bei der Anwendung dieser Richtlinie sind gemeinsame Definitionen in diesem Bereich und insbesondere Definitionen von Informationssystemen und Computerdaten wichtig.

(5) Es sollten gemeinsame Straftatbestände für den rechtswidrigen Zugang zu Informationssystemen, den rechtswidrigen Systemeingriff, den rechtswidrigen Eingriff in Daten und das rechtswidrige Abfangen von Daten festgelegt werden, wozu es einer Einigung über die Tatbestandsmerkmale bedarf.

(6) Angriffe auf Informationssysteme sollten von den Mitgliedstaaten unter Strafe gestellt werden. Die Sanktionen sollten wirksam, verhältnismäßig und abschreckend sein.

(6a) Diese Richtlinie sieht zumindest dann strafrechtliche Sanktionen vor, wenn kein leichter Fall vorliegt. Die Mitgliedstaaten können festlegen, was gemäß ihrem einzelstaatlichen Recht und ihrer einzelstaatlichen Praxis als leichter Fall gilt. Ein Fall kann beispielsweise dann als leicht eingestuft werden, wenn der damit verbundene Schaden und/oder die damit verbundene Gefahr für öffentliche oder private Interessen, wie etwa die Integrität eines Computersystems oder von Computerdaten oder die Integrität, die Rechte und andere Interessen einer Person geringfügig oder so geartet ist, dass die die Verhängung einer strafrechtlichen Sanktion innerhalb der gesetzlichen Grenzen oder die Begründung einer strafrechtlichen Verantwortung nicht notwendig ist.

(7) Schwerere Strafen sollten vorgesehen werden bei Angriffen auf ein Informationssystem, die von einer kriminellen Vereinigung im Sinne des Rahmenbeschlusses 2008/841/JI des Rates vom 24. Oktober 2008 zur Bekämpfung der organisierten Kriminalität[2] verübt werden, bei groß angelegten oder schwere Schäden verursachenden Angriffen oder bei Straftaten, die unter missbräuchlicher Verwendung personenbezogener Daten einer anderen Person als des Täters begangen werden, um das Vertrauen eines Dritten zu gewinnen[3].

(8) In den Schlussfolgerungen des Rates vom 27./28. November 2008 wurde die Ausarbeitung einer neuen Strategie in Zusammenarbeit mit den Mitgliedstaaten und der Kommission angekündigt, in die auch das Übereinkommen des Europarats über Computerkriminalität aus dem Jahr 2001 einfließen soll. Dieses Übereinkommen ist der rechtliche Bezugsrahmen für die Bekämpfung der Cyberkriminalität und damit auch der Angriffe auf Informationssysteme. Die vorliegende Richtlinie baut auf dem Übereinkommen auf.

---

[2] ABl L 300 vom 11.11.2008, S. 42.

[3] Der Text wurde an die derzeitige Fassung des Vorschlags angepasst.

(9) Angesichts der unterschiedlichen Art und Weise, wie Cyberangriffe ausgeführt werden können, und der raschen Entwicklung bei der Hard- und Software ist in dieser Richtlinie die Rede von "Instrumenten", die zur Begehung der in dieser Richtlinie aufgeführten Straftaten verwendet werden können. Bei solchen Instrumenten kann es sich beispielsweise um Schadsoftware einschließlich Botnetzen handeln, die für Cyberangriffe verwendet werden[4].

(10) Mit dieser Richtlinie soll keine strafrechtliche Haftung in Fällen begründet werden, in denen die Handlungen ohne kriminelle Absicht, beispielsweise zum genehmigten Testen oder zum Schutz eines Informationssystems, vorgenommen werden, oder wenn die betreffende Person nicht wusste, dass sie kein Zugangsrecht hatte.

(10a) Diese Richtlinie enthält keine Bestimmungen über die Voraussetzungen, die erfüllt sein sollten, damit eine Verfolgung der in den Artikeln 3 bis 8 genannten Straftaten eingeleitet werden kann, wenn diese Straftaten außerhalb des Hoheitsgebiets des betreffenden Mitgliedstaats begangen wurden, wie etwa eine am Tatort erstattete Anzeige des Opfers oder eine Anzeige des Staats, in dem sich der Tatort befindet, oder wenn der Grundsatz *ne bis in idem* Anwendung findet.

(11) Diese Richtlinie stärkt die Rolle von Netzwerken wie des G8-Netzes oder des Netzes der Kontaktstellen des Europarats, die an sieben Wochentagen 24 Stunden täglich für den Informationsaustausch zur Verfügung stehen, um verfügbare einschlägige Informationen für Ermittlungen und Verfahren wegen Straftaten im Zusammenhang mit Informationssystemen und –daten, die den ersuchenden Mitgliedstaat betreffen, bereitstellen zu können. Angesichts der Schnelligkeit, mit der Großangriffe ausgeführt werden können, sollten die Mitgliedstaaten in der Lage sein, prompt auf dringende Ersuchen dieser Kontaktstellen um Unterstützung zu reagieren. In diesen Fällen kann es zweckmäßig sein, dass neben dem Informationsersuchen auch telefonisch Kontakt aufgenommen wird, um dafür zu sorgen, dass der ersuchte Staat das Ersuchen zügig bearbeitet und dass innerhalb der Frist von acht Stunden eine Rückmeldung erfolgt, mit der der Eingang des Ersuchens bestätigt und zugleich mitgeteilt wird, ob es beantwortet wird und wann mit Antwort zu rechnen ist.

---

[4] LT: Prüfungsvorbehalt, bis eine Einigung über Artikel 9 erzielt wird.

(12) Um sich ein vollständigeres Bild von der Problematik auf Ebene der Union machen und auf diese Weise zur Gestaltung effizienterer Lösungen beitragen zu können, müssen Daten über Straftaten, die unter diese Richtlinie fallen, erfasst werden. Diese Daten werden auch Agenturen wie Europol oder der Europäischen Agentur für Netz- und Informationssicherheit dabei helfen, das Ausmaß der Cyberkriminalität und den Stand der Netz- und Informationssicherheit in Europa besser einzuschätzen[5].

(13) Größere Abweichungen und Diskrepanzen zwischen den einschlägigen Rechtsvorschriften der Mitgliedstaaten können die Bekämpfung der organisierten Kriminalität und des Terrorismus behindern und unter Umständen eine wirksame polizeiliche und justizielle Zusammenarbeit bei der Abwehr von Angriffen auf Informationssysteme erschweren. Der länder- und grenzübergreifende Charakter moderner Informationssysteme bedeutet, dass auch Angriffe auf solche Systeme eine grenzüberschreitende Dimension annehmen, was den dringenden Bedarf an weiteren Maßnahmen zur Angleichung der einschlägigen Strafvorschriften unterstreicht. Die Koordinierung der Strafverfolgung bei solchen Angriffen sollte mithilfe des Rahmenbeschlusses 2009/948/JI des Rates zur Vermeidung und Beilegung von Kompetenzkonflikten in Strafverfahren erleichtert werden.

(14) Da die Ziele dieser Richtlinie, nämlich Angriffe auf Informationssysteme in allen Mitgliedstaaten mit wirksamen, verhältnismäßigen und abschreckenden strafrechtlichen Sanktionen zu ahnden und die justizielle Zusammenarbeit durch Beseitigung möglicher Hemmnisse zu verbessern und zu fördern, auf Ebene der Mitgliedstaaten nicht ausreichend erreicht werden können, sondern – da es dazu gemeinsamer, kompatibler Regeln bedarf – besser auf Unionsebene zu erreichen sind, kann die Union im Einklang mit dem in Artikel 5 des Vertrags über die Europäische Union niedergelegten Subsidiaritätsprinzip tätig werden. Diese Richtlinie geht nicht über das für die Erreichung dieser Ziele erforderliche Maß hinaus.

---

[5] NL: Prüfungsvorbehalt, bis eine Einigung über Artikel 15 erzielt wird.

(15) Alle im Zusammenhang mit der Anwendung dieser Richtlinie verarbeiteten Daten sollten nach Maßgabe des Rahmenbeschlusses 2008/977/JI des Rates vom 27. November 2008 über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden[6], soweit dieser Rahmenbeschluss einschlägig ist, und gemäß der Verordnung (EG) Nr. 45/2001 des Europäischen Parlaments und des Rates vom 18. Dezember 2000 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der Gemeinschaft und zum freien Datenverkehr[7] geschützt werden.

(16) Diese Richtlinie steht im Einklang mit den Grundrechten und Grundsätzen, die insbesondere mit der Charta der Grundrechte der Europäischen Union anerkannt wurden, namentlich der Schutz personenbezogener Daten, die Meinungs- und Informationsfreiheit, das Recht auf ein faires Verfahren, die Unschuldsvermutung und die Gewährleistung der Verteidigungsrechte sowie das Gesetzlichkeits- und Verhältnismäßigkeitsprinzip in Bezug auf Straftaten und Sanktionen. Diese Richtlinie, mit der die uneingeschränkte Wahrung dieser Rechte und Grundsätze gewährleistet werden soll, ist entsprechend umzusetzen.

(17) Gemäß den Artikeln 1, 2, 3 und 4 des Protokolls über die Position des Vereinigten Königreichs und Irlands hinsichtlich des Raums der Freiheit, der Sicherheit und des Rechts im Anhang zum Vertrag über die Arbeitsweise der Europäischen Union haben das Vereinigte Königreich und Irland mitgeteilt, dass sie sich an der Annahme und Anwendung dieser Richtlinie beteiligen wollen.

---

[6] ABl L 350 vom 30.12.2008, S. 60.
[7] ABl L 8 vom 12.1.2001, S. 1.

(18) Gemäß den Artikeln 1 und 2 des dem Vertrag über die Arbeitsweise der Europäischen Union beigefügten Protokolls über die Position Dänemarks beteiligt sich Dänemark nicht an der Annahme dieser Richtlinie, die daher für diesen Staat nicht verbindlich und ihm gegenüber nicht anwendbar ist.

(19) Mit dieser Richtlinie sollen die Bestimmungen des Rahmenbeschlusses 2005/222/JI geändert und ausgeweitet werden. Da die vorzunehmenden Änderungen sowohl bezüglich der Zahl als auch hinsichtlich des Inhalts erheblich sind, sollte der Rahmenbeschluss aus Gründen der Klarheit für die sich an der Annahme dieser Richtlinie beteiligenden Mitgliedstaaten vollständig ersetzt werden.

(20) Nach Nummer 34 der Interinstitutionellen Vereinbarung über bessere Rechtsetzung[8] sind die Mitgliedstaaten aufgefordert, für ihre eigenen Zwecke und im Interesse der Union eigene Tabellen aufzustellen, aus denen im Rahmen des Möglichen die Entsprechungen zwischen dieser Richtlinie und ihren Umsetzungsmaßnahmen zu entnehmen sind, und diese zu veröffentlichen[9] –

HABEN FOLGENDE RICHTLINIE ERLASSEN:

Artikel 1

Gegenstand

Mit dieser Richtlinie werden Mindestvorschriften für die Definition von Straftaten und für die Sanktionen bei Angriffen auf Informationssysteme festgelegt. Die Richtlinie soll überdies die Verhinderung derartiger Straftaten erleichtern und die Zusammenarbeit zwischen Justizbehörden und anderen zuständigen Behörden verbessern[10].

---

8 ABl. C 321 vom 31.12.2003, S. 1.
9 DE hat einen Prüfungsvorbehalt eingelegt.
10 ES hält an ihrem Prüfungsvorbehalt fest.

Artikel 2

Begriffsbestimmungen

Im Sinne dieser Richtlinie 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, abgerufenen oder übertragenen Computerdaten;

(b) "Computerdaten" jede 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;

(d) "unbefugt" einen Zugang, einen Eingriff, ein Abfangen von Daten oder jede andere in dieser Richtlinie genannte Handlung, die 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 3

Rechtswidriger Zugang zu Informationssystemen[11]

Die Mitgliedstaaten treffen die erforderlichen Maßnahmen, um sicherzustellen, dass der vorsätzliche unbefugte Zugang zu einem Informationssystem als Ganzem oder zu einem Teil davon zumindest dann unter Strafe gestellt wird, wenn er durch eine Verletzung von Sicherheitsmaßnahmen erfolgt und kein leichter Fall vorliegt.

Artikel 4

Rechtswidriger Systemeingriff

Die Mitgliedstaaten treffen die erforderlichen Maßnahmen, um sicherzustellen, dass die schwere Behinderung oder Störung des Betriebs eines Informationssystems durch Eingeben, Übermitteln, Beschädigen, Löschen, Beeinträchtigen, Verändern, Unterdrücken oder Unzugänglichmachen von Computerdaten zumindest dann unter Strafe gestellt wird, wenn sie vorsätzlich und unbefugt erfolgt und kein leichter Fall vorliegt.

Artikel 5

Rechtswidriger Eingriff in Daten

Die Mitgliedstaaten treffen die erforderlichen Maßnahmen, um sicherzustellen, dass das vorsätzliche unbefugte Löschen, Beschädigen, Beeinträchtigen, Verändern, Unterdrücken oder Unzugänglichmachen von Computerdaten eines Informationssystems zumindest dann unter Strafe gestellt wird, wenn kein leichter Fall vorliegt.

---

11 UK: Prüfungsvorbehalt.

Artikel 6

Rechtswidriges Abfangen von Daten

Die Mitgliedstaaten treffen die erforderlichen Maßnahmen, um sicherzustellen, dass das vorsätzliche, mit technischen Hilfsmitteln bewirkte unbefugte Abfangen nichtöffentlicher Computerdatenübermittlungen an ein Informationssystem, aus einem Informationssystem oder innerhalb eines Informationssystems einschließlich elektromagnetischer Abstrahlungen aus einem Informationssystem, das Träger solcher Computerdaten ist, zumindest dann unter Strafe gestellt wird, wenn kein leichter Fall vorliegt.

Artikel 7

Tatwerkzeuge[12]

(1) Die Mitgliedstaaten treffen die erforderlichen Maßnahmen, um sicherzustellen, dass das vorsätzliche unbefugte Herstellen, Verkaufen, Beschaffen zwecks Gebrauchs, Einführen, Verbreiten oder anderweitige Verfügbarmachen folgender Instrumente, die dazu bestimmt sind, eine Straftat im Sinne der Artikel 3 bis 6 zu begehen, zumindest dann unter Strafe gestellt wird, wenn kein leichter Fall vorliegt:

a) einer Vorrichtung einschließlich eines[13] Computerprogramms, die in erster Linie dafür ausgelegt oder hergerichtet worden ist, eine Straftat im Sinne der Artikel 3 bis 6 zu begehen;

b) eines Computerpassworts, eines Zugangscodes oder ähnlicher Daten, die den Zugang zu einem Informationssystem als Ganzem oder zu einem Teil davon ermöglichen.

(…)

---

12 UK erhält seinen Prüfungsvermerk aufrecht.

13 DE schlägt vor, "einer Vorrichtung einschließlich eines Computerprogramms, die" durch "eines Computerprogramms, das" zu ersetzen.

Artikel 8

Anstiftung, Beihilfe und Versuch

1. Die Mitgliedstaaten stellen sicher, dass die Anstiftung oder Beihilfe zur Begehung einer Straftat im Sinne der Artikel 3 bis 7 unter Strafe gestellt wird.

2. Die Mitgliedstaaten stellen sicher, dass der Versuch der Begehung einer Straftat im Sinne der Artikel 4 und 5 unter Strafe gestellt wird.

Artikel 9

Sanktionen

1. Die Mitgliedstaaten treffen die erforderlichen Maßnahmen, um sicherzustellen, dass die Straftaten im Sinne der Artikel 3 bis 8 mit wirksamen, angemessenen und abschreckenden strafrechtlichen Sanktionen geahndet werden.

2. Die Mitgliedstaaten treffen die erforderlichen Maßnahmen, um sicherzustellen, dass Straftaten im Sinne der Artikel 3 bis 6 mit Freiheitsstrafen im Höchstmaß von mindestens zwei Jahren geahndet werden.

3. Die Mitgliedstaaten treffen die erforderlichen Maßnahmen, um sicherzustellen, dass Straftaten im Sinne der Artikel 4 und 5 mit Freiheitsstrafen im Höchstmaß von mindestens drei Jahren geahndet werden, wenn sie vorsätzlich mit einem Instrument begangen wurden, das in erster Linie dazu bestimmt ist, Angriffe auszulösen, die eine beträchtliche Anzahl von Informationssystemen schädigen oder einen schweren Schaden verursachen.

4. Die Mitgliedstaaten treffen die erforderlichen Maßnahmen, um sicherzustellen, dass Straftaten im Sinne der Artikel 4 und 5 mit Freiheitsstrafen im Höchstmaß von mindestens fünf Jahren geahndet werden, wenn[14]

a) sie im Rahmen einer kriminellen Vereinigung im Sinne des Rahmenbeschlusses 2008/841/JI ungeachtet des dort genannten Strafmaßes verübt wurden oder

b) einen schweren Schaden verursachen oder

c) gegen ein Informationssystem verübt wurden, das Teil der kritischen Infrastruktur ist.

5. Sofern die nachstehenden Umstände nicht bereits ein Tatbestandsmerkmal der in den Artikeln 3 bis 5 genannten Straftaten sind, treffen die Mitgliedstaaten die erforderlichen Maßnahmen, um sicherzustellen, dass sie als erschwerende Umstände gelten können, wenn diese Straftaten unter missbräuchlicher Verwendung personenbezogener Daten einer anderen Person als des Täters begangen werden, um das Vertrauen eines Dritten zu gewinnen.

(…)

Artikel 11

Verantwortlichkeit juristischer Personen

1. Die Mitgliedstaaten treffen die erforderlichen Maßnahmen, um sicherzustellen, dass eine juristische Person für eine Straftat im Sinne der Artikel 3 bis 8 verantwortlich gemacht werden kann, die zu ihren Gunsten von einer Person begangen wurde, 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,

b) einer Befugnis, Entscheidungen im Namen der juristischen Person zu treffen, oder

c) einer Kontrollbefugnis innerhalb der juristischen Person.

[14] RO: Prüfungsvorbehalt zu Artikel 9 Absatz 4 Buchstaben b und c.

2. Die Mitgliedstaaten treffen 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 einer Straftat nach den Artikeln 3 bis 8 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 als Täter, Anstifter oder Gehilfen bei einer Straftat im Sinne der Artikel 3 bis 8 nicht aus.

Artikel 12

Sanktionen gegen juristische Personen

1. Die Mitgliedstaaten treffen die erforderlichen Maßnahmen, um sicherzustellen, dass gegen eine im Sinne von Artikel 11 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,
   d) richterlich angeordnete Eröffnung des Liquidationsverfahrens oder
   e) vorübergehende oder endgültige Schließung von Einrichtungen, die zur Begehung der Straftat genutzt wurden.
2. Die Mitgliedstaaten treffen die erforderlichen Maßnahmen, um sicherzustellen, dass gegen eine im Sinne von Artikel 11 Absatz 2 verantwortliche juristische Person wirksame, angemessene und abschreckende Sanktionen oder Maßnahmen verhängt werden können.

Artikel 13

Gerichtliche Zuständigkeit[15]

1. Jeder Mitgliedstaat begründet seine Zuständigkeit für die in den Artikeln 3 bis 8 genannten Straftaten, wenn diese

[15] UK und ES halten an ihrem Prüfungsvorbehalt zu diesem Artikel fest.

a) ganz oder teilweise in seinem Hoheitsgebiet oder

b) von einem seiner Staatsangehörigen begangen wurden, zumindest in den Fällen, in denen die Tat an dem Ort, an dem sie begangen wurde, eine Straftat darstellt.

(…)[16]

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) sich der Täter bei der Begehung der Straftat physisch im Hoheitsgebiet dieses Mitgliedstaats aufhält, unabhängig davon, ob sich die Straftat gegen ein Informationssystem innerhalb oder außerhalb seines Hoheitsgebiets richtet, oder

b) sich die Straftat gegen ein Informationssystem in seinem Hoheitsgebiet richtet, unabhängig davon, ob sich der Täter bei der Begehung der Straftat physisch im Hoheitsgebiet dieses Mitgliedstaats aufhält.

3. Ein Mitgliedstaat unterrichtet die Kommission über seine Entscheidung, eine weitere gerichtliche Zuständigkeit für Straftaten nach den Artikeln 3 bis 8, die außerhalb seines Hoheitsgebiets begangen wurden, zu begründen, zum Beispiel in Fällen, in denen

a) der gewöhnliche Aufenthalt des Straftäters in seinem Hoheitsgebiet liegt oder

b) die Straftat zugunsten einer in seinem Hoheitsgebiet niedergelassenen juristischen Person begangen wird.

---

[16] Auf Wunsch mehrerer Delegationen wurde Artikel 13 Absatz 1a als neuer Erwägungsgrund 10a in den Einleitungsteil aufgenommen.

Artikel 14

Informationsaustausch[17]

1. Zum Zwecke des Informationsaustauschs über Straftaten nach den Artikeln 3 bis 8 nutzen die Mitgliedstaaten das bestehende Netz der operativen Kontaktstellen, die an sieben Wochentagen 24 Stunden täglich zur Verfügung stehen. Die Mitgliedstaaten sorgen dafür, dass Verfahren vorhanden sind, mit sie denen bei dringenden Ersuchen binnen höchstens acht Stunden zumindest mitteilen können, ob das Ersuchen um Unterstützung beantwortet wird und in welcher Form und wann dies voraussichtlich erfolgen wird.

2. Die Mitgliedstaaten teilen der Kommission ihre Kontaktstelle für den Informationsaustausch über Straftaten im Sinne der Artikel 3 bis 8 mit. Die Kommission leitet diese Information an die anderen Mitgliedstaaten weiter.

Artikel 15

Kontrolle und Statistiken[18]

1. Die Mitgliedstaaten sorgen dafür, dass ein System für die Aufzeichnung, Erstellung und Bereitstellung statistischer Daten zu den Straftaten im Sinne der Artikel 3 bis 7 bereitsteht.

2. Die statistischen Daten gemäß Absatz 1 umfassen zumindest die vorhandenen Daten über die Anzahl der in den Mitgliedstaaten erfassten Straftaten im Sinne der Artikel 3 bis 7 und die Anzahl der Personen, die wegen einer Straftat im Sinne der Artikel 3 bis 7 verfolgt und verurteilt worden sind.

3. Die Mitgliedstaaten übermitteln der Kommission die nach Maßgabe dieses Artikels erfassten Daten. Die Kommission sorgt dafür, dass eine konsolidierte Zusammenfassung dieser statistischen Berichte veröffentlicht wird.

---

17 ES: Prüfungsvorbehalt.

18 ES: Prüfungsvorbehalt.

Artikel 16

Ersetzung des Rahmenbeschlusses 2005/222/JI[19]

Der Rahmenbeschluss 2005/222/JI wird in Bezug auf die Mitgliedstaaten ersetzt, die sich an der Annahme dieser Richtlinie beteiligen, unbeschadet der Pflichten der Mitgliedstaaten im Zusammenhang mit den Fristen für die Umsetzung des Rahmenbeschlusses in innerstaatliches Recht.

In Bezug auf die Mitgliedstaaten, die sich an der Annahme dieser Richtlinie beteiligen, gelten Verweise auf den Rahmenbeschluss 2005/222/JI als Verweise auf die vorliegende Richtlinie.

Artikel 17

Umsetzung

1. Die Mitgliedstaaten setzen die erforderlichen Rechts- und Verwaltungsvorschriften in Kraft, um dieser Richtlinie bis [zwei Jahre nach ihrem Erlass] nachzukommen.

2. Die Mitgliedstaaten übermitteln der Kommission den Wortlaut der innerstaatlichen Rechtsvorschriften zur Umsetzung ihrer Verpflichtungen aus dieser Richtlinie.

3. Bei Erlass dieser Vorschriften nehmen die Mitgliedstaaten in den Vorschriften selbst oder durch einen Hinweis bei der amtlichen Veröffentlichung auf diese Richtlinie Bezug. Die Mitgliedstaaten regeln die Einzelheiten dieser Bezugnahme.

19 UK erhält seinen Prüfungsvorbehalt aufrecht.

Artikel 18

Berichterstattung

1. Die Kommission berichtet dem Europäischen Parlament und dem Rat bis [VIER JAHRE NACH ERLASS DER RICHTLINIE], inwieweit die Mitgliedstaaten die zur Einhaltung dieser Richtlinie notwendigen Maßnahmen ergriffen haben, und unterbreitet erforderlichenfalls Gesetzgebungsvorschläge.

2. Die Mitgliedstaaten übermitteln der Kommission alle Angaben, die für die Erstellung des in Absatz 1 genannten Berichts dienlich sind. Dazu gehört auch eine ausführliche Beschreibung der zur Umsetzung dieser Richtlinie verabschiedeten gesetzgeberischen und sonstigen Maßnahmen[20].

Artikel 19

Inkrafttreten

Diese Richtlinie tritt am Tag ihrer Veröffentlichung im *Amtsblatt der Europäischen Union* in Kraft.

Artikel 20

Adressaten

Diese Richtlinie ist gemäß den Verträgen an die Mitgliedstaaten gerichtet.

Geschehen zu Brüssel am

Im Namen des Europäischen Parlaments	*Im Namen des Rates*
Der Präsident	*Der Präsident*

---

[20] ES äußerte Vorbehalte zu Absatz 2, der in der Richtlinie gegen Menschenhandel nicht enthalten ist.

ANLAGE II

2010/0273 (COD)

Vorschlag für eine

RICHTLINIE DES EUROPÄISCHEN PARLAMENTS UND DES RATES

über Angriffe auf Informationssysteme und zur Ersetzung des Rahmenbeschlusses 2005/222/JI des Rates

Artikel 1

Gegenstand

Mit dieser Richtlinie werden Mindestvorschriften für die Definition von Straftaten und für die Sanktionen bei Angriffen auf Informationssysteme festgelegt. Die Richtlinie soll überdies die Verhinderung derartiger Straftaten erleichtern und die Zusammenarbeit zwischen Justizbehörden und anderen zuständigen Behörden verbessern.

Artikel 2

Begriffsbestimmungen

Im Sinne dieser Richtlinie 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, abgerufenen oder übertragenen Computerdaten;

b) "Computerdaten" jede 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;

d) "unbefugt" einen Zugang, einen Eingriff, ein Abfangen von Daten oder jede andere in dieser Richtlinie genannte Handlung, die 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 3

Rechtswidriger Zugang zu Informationssystemen

Die Mitgliedstaaten treffen die erforderlichen Maßnahmen, um sicherzustellen, dass der vorsätzliche unbefugte Zugang zu einem Informationssystem als Ganzem oder zu einem Teil davon zumindest dann unter Strafe gestellt wird, wenn er durch eine Verletzung von Sicherheitsmaßnahmen erfolgt und kein leichter Fall vorliegt.

Artikel 4

Rechtswidriger Systemeingriff

Die Mitgliedstaaten treffen die erforderlichen Maßnahmen, um sicherzustellen, dass die schwere Behinderung oder Störung des Betriebs eines Informationssystems durch Eingeben, Übermitteln, Beschädigen, Löschen, Beeinträchtigen, Verändern, Unterdrücken oder Unzugänglichmachen von Computerdaten zumindest dann unter Strafe gestellt wird, wenn sie vorsätzlich und unbefugt erfolgt und kein leichter Fall vorliegt.

Artikel 5

Rechtswidriger Eingriff in Daten

Die Mitgliedstaaten treffen die erforderlichen Maßnahmen, um sicherzustellen, dass das vorsätzliche unbefugte Löschen, Beschädigen, Beeinträchtigen, Verändern, Unterdrücken oder Unzugänglichmachen von Computerdaten eines Informationssystems zumindest dann unter Strafe gestellt wird, wenn kein leichter Fall vorliegt.

Artikel 6

Rechtswidriges Abfangen von Daten

Die Mitgliedstaaten treffen die erforderlichen Maßnahmen, um sicherzustellen, dass das vorsätzliche, mit technischen Hilfsmitteln bewirkte unbefugte Abfangen nichtöffentlicher Computerdatenübermittlungen an ein Informationssystem, aus einem Informationssystem oder innerhalb eines Informationssystems einschließlich elektromagnetischer Abstrahlungen aus einem Informationssystem, das Träger solcher Computerdaten ist, zumindest dann unter Strafe gestellt wird, wenn kein leichter Fall vorliegt.

Artikel 11

Verantwortlichkeit juristischer Personen

1. Die Mitgliedstaaten treffen die erforderlichen Maßnahmen, um sicherzustellen, dass eine juristische Person für eine Straftat im Sinne der Artikel 3 bis 8 verantwortlich gemacht werden kann, die zu ihren Gunsten von einer Person begangen wurde, 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,

   b) einer Befugnis, Entscheidungen im Namen der juristischen Person zu treffen, oder

   c) einer Kontrollbefugnis innerhalb der juristischen Person.

2. Die Mitgliedstaaten treffen 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 einer Straftat nach den Artikeln 3 bis 8 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 als Täter, Anstifter oder Gehilfen bei einer Straftat im Sinne der Artikel 3 bis 8 nicht aus.

Artikel 12

Sanktionen gegen juristische Personen

1. Die Mitgliedstaaten treffen die erforderlichen Maßnahmen, um sicherzustellen, dass gegen eine im Sinne von Artikel 11 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,
   d) richterlich angeordnete Eröffnung des Liquidationsverfahrens oder
   e) vorübergehende oder endgültige Schließung von Einrichtungen, die zur Begehung der Straftat genutzt wurden.

2. Die Mitgliedstaaten treffen die erforderlichen Maßnahmen, um sicherzustellen, dass gegen eine im Sinne von Artikel 11 Absatz 2 verantwortliche juristische Person wirksame, angemessene und abschreckende Sanktionen oder Maßnahmen verhängt werden können.

Artikel 13

Gerichtliche Zuständigkeit[21]

1. Jeder Mitgliedstaat begründet seine Zuständigkeit für die in den Artikeln 3 bis 8 genannten Straftaten, wenn diese

[21] Der folgende Erwägungsgrund ist in der partiellen allgemeinen Ausrichtung enthalten: "Diese Richtlinie enthält keine Bestimmungen über die Voraussetzungen, die erfüllt sein sollten, damit eine Verfolgung der in den Artikeln 3 bis 8 genannten Straftaten eingeleitet werden kann, wenn diese Straftaten außerhalb des Hoheitsgebiets des betreffenden Mitgliedstaats begangen wurden, wie etwa eine am Tatort erstattete Anzeige des Opfers oder eine Anzeige des Staats, in dem sich der Tatort befindet, oder die Tatsache, dass der Täter am Tatort nicht verfolgt wurde."

a) ganz oder teilweise in seinem Hoheitsgebiet oder

b) von einem seiner Staatsangehörigen begangen wurden, zumindest in den Fällen, in denen die Tat an dem Ort, an dem sie begangen wurde, eine Straftat darstellt.

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) sich der Täter bei der Begehung der Straftat physisch im Hoheitsgebiet dieses Mitgliedstaats aufhält, unabhängig davon, ob sich die Straftat gegen ein Informationssystem innerhalb oder außerhalb seines Hoheitsgebiets richtet, oder

b) sich die Straftat gegen ein Informationssystem in seinem Hoheitsgebiet richtet, unabhängig davon, ob sich der Täter bei der Begehung der Straftat physisch im Hoheitsgebiet dieses Mitgliedstaats aufhält.

3. Ein Mitgliedstaat unterrichtet die Kommission über seine Entscheidung, eine weitere gerichtliche Zuständigkeit für Straftaten nach den Artikeln 3 bis 8, die außerhalb seines Hoheitsgebiets begangen wurden, zu begründen, zum Beispiel in Fällen, in denen

a) der gewöhnliche Aufenthalt des Straftäters in seinem Hoheitsgebiet liegt oder

b) die Straftat zugunsten einer in seinem Hoheitsgebiet niedergelassenen juristischen Person begangen wird.

Artikel 14

Informationsaustausch

1. Zum Zwecke des Informationsaustauschs über Straftaten nach den Artikeln 3 bis 8 nutzen die Mitgliedstaaten das bestehende Netz der operativen Kontaktstellen, die an sieben Wochentagen 24 Stunden täglich zur Verfügung stehen. Die Mitgliedstaaten sorgen dafür, dass Verfahren vorhanden sind, mit sie denen bei dringenden Ersuchen binnen höchstens acht Stunden zumindest mitteilen können, ob das Ersuchen um Unterstützung beantwortet wird und in welcher Form und wann dies voraussichtlich erfolgen wird.

2. Die Mitgliedstaaten teilen der Kommission ihre Kontaktstelle für den Informationsaustausch über Straftaten im Sinne der Artikel 3 bis 8 mit. Die Kommission leitet diese Information an die anderen Mitgliedstaaten weiter.

Artikel 15

Kontrolle und Statistiken

1. Die Mitgliedstaaten sorgen dafür, dass ein System für die Aufzeichnung, Erstellung und Bereitstellung statistischer Daten zu den Straftaten im Sinne der Artikel 3 bis 7 bereitsteht.

2. Die statistischen Daten gemäß Absatz 1 umfassen zumindest die vorhandenen Daten über die Anzahl der in den Mitgliedstaaten erfassten Straftaten im Sinne der Artikel 3 bis 7 und die Anzahl der Personen, die wegen einer Straftat im Sinne der Artikel 3 bis 7 verfolgt und verurteilt worden sind.

3. Die Mitgliedstaaten übermitteln der Kommission die nach Maßgabe dieses Artikels erfassten Daten. Die Kommission sorgt dafür, dass eine konsolidierte Zusammenfassung dieser statistischen Berichte veröffentlicht wird.

Artikel 16

Ersetzung des Rahmenbeschlusses 2005/222/JI

Der Rahmenbeschluss 2005/222/JI wird in Bezug auf die Mitgliedstaaten ersetzt, die sich an der Annahme dieser Richtlinie beteiligen, unbeschadet der Pflichten der Mitgliedstaaten im Zusammenhang mit den Fristen für die Umsetzung des Rahmenbeschlusses in innerstaatliches Recht.

In Bezug auf die Mitgliedstaaten, die sich an der Annahme dieser Richtlinie beteiligen, gelten Verweise auf den Rahmenbeschluss 2005/222/JI als Verweise auf die vorliegende Richtlinie.

Artikel 17

Umsetzung

1. Die Mitgliedstaaten setzen die erforderlichen Rechts- und Verwaltungsvorschriften in Kraft, um dieser Richtlinie bis [zwei Jahre nach ihrem Erlass] nachzukommen.

2. Die Mitgliedstaaten übermitteln der Kommission den Wortlaut der innerstaatlichen Rechtsvorschriften zur Umsetzung ihrer Verpflichtungen aus dieser Richtlinie.

3. Bei Erlass dieser Vorschriften nehmen die Mitgliedstaaten in den Vorschriften selbst oder durch einen Hinweis bei der amtlichen Veröffentlichung auf diese Richtlinie Bezug. Die Mitgliedstaaten regeln die Einzelheiten dieser Bezugnahme.

Artikel 18

Berichterstattung

1. Die Kommission berichtet dem Europäischen Parlament und dem Rat bis [VIER JAHRE NACH ERLASS DER RICHTLINIE], inwieweit die Mitgliedstaaten die zur Einhaltung dieser Richtlinie notwendigen Maßnahmen ergriffen haben, und unterbreitet erforderlichenfalls Gesetzgebungsvorschläge.

2. Die Mitgliedstaaten übermitteln der Kommission alle Angaben, die für die Erstellung des in Absatz 1 genannten Berichts dienlich sind. Dazu gehört auch eine ausführliche Beschreibung der zur Umsetzung dieser Richtlinie verabschiedeten gesetzgeberischen und sonstigen Maßnahmen.

Artikel 19

Inkrafttreten

Diese Richtlinie tritt am Tag ihrer Veröffentlichung im *Amtsblatt der Europäischen Union* in Kraft.

Artikel 20

Adressaten

Diese Richtlinie ist gemäß den Verträgen an die Mitgliedstaaten gerichtet.

Geschehen zu Brüssel am