KOMMISSION DER EUROPÄISCHEN GEMEINSCHAFTEN

Brüssel, den 14.7.2008
KOM(2008) 448 endgültig

BERICHT DER KOMMISSION AN DEN RAT

auf der Grundlage von Artikel 12 des Rahmenbeschlusses des Rates vom 24. Februar 2005 über Angriffe auf Informationssysteme

1. EINLEITUNG

1.1. Hintergrund

In diesem Bericht soll bewertet werden, ob die Mitgliedstaaten den Rahmenbeschluss 2005/222/JI des Rates über Angriffe auf Informationssysteme[1] (nachstehend „RB“) ordnungsgemäß in innerstaatliches Recht umgesetzt haben.

Das Hauptziel[2] des RB besteht darin, 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. Aus diesem Grund soll sich der RB auf andere EU-Rechtsakte und internationale Instrumente (insbesondere das Übereinkommen des Europarates über Computerkriminalität[3]) stützen bzw. diese ergänzen.

Seit Annahme des RB haben diverse kriminelle Angriffe auf Informationssysteme wiederholt verdeutlicht, dass es in diesem Bereich einer intensiveren Koordinierung auf europäischer Ebene bedarf. Der massive Denial-of-service-Angriff auf die Informationsinfrastruktur Estlands im Mai 2007 führte erneut – und glücklicherweise rechtzeitig – vor Augen, welche schädlichen und destruktiven Auswirkungen solche Angriffe haben.

Nach Verabschiedung des RB hat sich noch stärker gezeigt, wie wichtig es ist, dass die einzelnen Mitgliedstaaten den RB vollständig und korrekt umsetzen. Dass dieser Bericht genau zum richtigen Zeitpunkt vorgelegt wird, bestätigt auch der ausdrückliche Hinweis auf die Bekämpfung der Internetkriminalität in den Schlussfolgerungen zu einer unlängst stattgefundenen Tagung des Rates „Justiz und Inneres“[4], in denen dieser unter anderem feststellte, dass er dem Bericht der Kommission über die Umsetzung des RB mit Interesse entgegensieht.

1.2. Mitteilungen und Reaktionen

Gemäß Artikel 12 Absatz 2 des RB sind die Mitgliedstaaten verpflichtet, bis zum 16. März 2007 den Wortlaut der Vorschriften zu übermitteln, mit denen sie ihre Verpflichtungen aus dem RB in innerstaatliches Recht umsetzen. Bis zu dem genannten Zeitpunkt hatte lediglich ein Staat (Schweden) der Kommission innerstaatliche Umsetzungsvorschriften übermittelt, die jedoch unvollständig waren. Daher sandte die Kommission den Mitgliedstaaten ein Mahnschreiben zu, in dem sie sie aufforderte, ihr den Wortlaut aller innerstaatlichen Bestimmungen zur Umsetzung des Rahmenbeschlusses und alle als sachdienlich erachteten diesbezüglichen Angaben zu übermitteln.

---

1 ABl. L 69 vom 16.3.2005, S. 67.
2 Erwägungsgrund 1.
3 http://conventions.coe.int/treaty/ger/treaties/html/185.htm.
4 Am 8./9. November 2007, siehe http://www.consilium.europa.eu/ueDocs/cms_Data/docs/pressData/de/jha/97235.pdf.

Bis zum 1. Juni 2008 haben 23 Mitgliedstaaten Umsetzungsvorschriften mitgeteilt bzw. auf das Mahnschreiben reagiert. Keine Antworten gingen von *Malta*, *Polen*[5], der *Slowakei* und *Spanien* ein. Außerdem ermöglichen die Antworten *Irlands*, *Griechenlands* und des *Vereinigten Königreichs* – wie die jeweiligen Regierungen eingeräumt haben – keinerlei Bewertung der Umsetzung in diesen Staaten, da sich die Umsetzung dort verzögert hat.

Die sieben genannten Mitgliedstaaten sind somit ihrer Mitteilungspflicht nach Artikel 12 Absatz 2 des RB nicht nachgekommen. In dem Bericht werden daher ausschließlich die Rechtsvorschriften der übrigen 20 Mitgliedstaaten bewertet.

1.3. Vorgehensweise und Bewertungskriterien

Der Bericht stützt sich auf die von den Mitgliedstaaten übermittelten Informationen. Da in einigen Fällen aber noch nicht alle Daten vorlagen, beruhen die Bewertung und die Schlussfolgerungen dieses Berichts teilweise auf unvollständigen Angaben.

Nach Artikel 34 Absatz 2 Buchstabe b des Vertrags über die Europäische Union sind Rahmenbeschlüsse für die Mitgliedstaaten hinsichtlich des zu erreichenden Ziels verbindlich, überlassen jedoch den innerstaatlichen Stellen die Wahl der Form und der Mittel. Es wurden allgemeine Kriterien ausgearbeitet, anhand deren objektiv bewertet werden kann, ob eine Richtlinie von einem Mitgliedstaat vollständig umgesetzt wurde. Diese Kriterien können sinngemäß auf Rahmenbeschlüsse angewandt werden. Insbesondere müssen die Vorschriften zur Umsetzung des RB gewährleisten, dass dessen Zielen wirksam Rechung getragen wird, die Erfordernisse der Klarheit und der Rechtssicherheit erfüllt sind sowie der Wortlaut des RB hinreichend klar und präzise in vollem Umfang angewandt und innerhalb der vorgegebenen Frist umgesetzt wird.

Dieser Bericht befasst sich schwerpunktmäßig mit der formalen Umsetzung der strafrechtlichen Bestimmungen des RB. Die tatsächliche *Anwendung* dieser Bestimmungen ist jedoch nicht Gegenstand des Berichts.

2. BEWERTUNG

2.1. Allgemeines zur Umsetzung

Der RB wurde in den 20 Mitgliedstaaten auf sehr unterschiedliche Weise umgesetzt. In den meisten Staaten orientiert sich der Wortlaut der innerstaatlichen Rechtsvorschriften stark an dem des RB. In anderen wurde einer indirekteren und allgemeineren Umsetzungsmethode der Vorzug gegeben. In vielen Fällen bedeutet dies, dass die Rechtskonzepte und –begriffe nicht ohne Weiteres vergleichbar sind. Soweit möglich wird in dem Bericht das in den Mitgliedstaaten geltende allgemeine Strafrecht berücksichtigt und auf besondere Schwierigkeiten im Zusammenhang mit diesem Ansatz hingewiesen.

---

[5] Die polnische Mitteilung, die verspätet am 1. Juli 2008 eingegangen ist, kann wegen der strikten Veröffentlichungsfristen in dem vorliegenden Bericht zwar nicht berücksichtigt werden, es wird ihr aber später bei den Maßnahmen, die nach Veröffentlichung des Berichts getroffen werden, Rechnung getragen.

2.2. Begriffsbestimmungen (Artikel 1)

Die 20 Mitgliedstaaten haben keine klaren bzw. keine vollständigen Angaben dazu gemacht, wie die in dem RB enthaltenen Begriffsbestimmungen im innerstaatlichen Recht Anwendung finden. Generell ist den übermittelten Informationen jedoch eindeutig zu entnehmen, dass die Begriffsbestimmungen im innerstaatlichen Recht denen des RB entsprechen.

2.3. Rechtswidriger Zugang zu Informationssystemen (Artikel 2)

Nach Auffassung der Kommission sind alle 20 Mitgliedstaaten der Hauptverpflichtung nachgekommen, sicherzustellen, dass der vorsätzliche und unbefugte Zugang zu einem Informationssystem als Ganzes oder zu einem Teil eines Informationssystems unter Strafe gestellt wird.

Nach dem letzten Teil von Absatz 1 haben die Mitgliedstaaten die Option, solche Handlungen nur dann unter Strafe zu stellen, „wenn kein leichter Fall vorliegt". Folgende Mitgliedstaaten haben mehr oder weniger ausdrücklich von dieser Option Gebrauch gemacht, sofern die unten erläuterten Regelungen dieser Vorgabe entsprechen.

– In *Österreich* gilt der Vorsatz, Datenspionage zu begehen und die erlangten Daten zwecks Gewinnerzielung oder Schädigung zu verwenden, als rechtliches Kriterium dafür, dass der Betreffende strafrechtlich zur Verantwortung zu ziehen ist.

– Die *Tschechische Republik* hat den rechtswidrigen Zugang zu Informationssystemen nur in Fällen unter Strafe gestellt, in denen die Daten anschließend missbraucht oder beschädigt werden.

– In *Finnland* erfolgt nur dann eine strafrechtliche Ahndung, wenn eine „Gefährdung" der Daten, auf die zugegriffen wurde, besteht.

– *Lettland* hat den rechtswidrigen Zugang zu Informationssystemen nur in Fällen unter Strafe gestellt, in denen eine erhebliche Schädigung verursacht wird.

Um bewerten zu können, ob diese Regelungen mit dem RB in Einklang stehen, muss näher erläutert werden, wie die Formulierung „wenn kein leichter Fall vorliegt" auszulegen ist. Nur anhand einer solchen Auslegung kann ermittelt werden, ob die Mitgliedstaaten zumindest der Kernaussage des RB formal Rechnung getragen haben. Artikel 2 zielt auf den Schutz des Zugangs zu Informationssystemen ab. Die Kommission ist der Ansicht, dass in diesem Zusammenhang unter minder schweren Fällen solche zu verstehen sind, in denen der rechtswidrige Zugang zu einem Informationssystem von geringer Bedeutung ist oder in denen nur in geringem Maße gegen die Sicherheit des Informationssystems verstoßen wurde. Die vorstehend genannten Vorschriften *Österreichs*, der *Tschechischen Republik*, *Finnlands* und *Lettlands* nehmen jedoch Bezug auf besondere Umstände wie das Vorliegen eines kriminellen Vorsatzes, spezieller Risiken oder einer Schädigung, die nicht als vereinbar mit der oben erläuterten Auslegung erachtet werden können. Die Kommission bezweifelt daher stark, dass die fraglichen *österreichischen*,

tschechischen, *finnischen* und *lettischen* Bestimmungen der RB-Bedingung „wenn kein leichter Fall vorliegt“ angemessen Rechnung tragen.

Generell ist die Verwirklichung des Ziels der Angleichung der einzelstaatlichen Strafrechtsvorschriften für Angriffe auf Informationssysteme durch derart divergierende Auslegungen und Anwendungen der Option, bestimmte Handlungen nicht unter Strafe zu stellen, ernsthaft gefährdet.

Dementsprechend ist die Kommission der Auffassung, dass lediglich 16 der 20 Mitgliedstaaten Artikel 2 des RB nachweislich ordnungsgemäß umgesetzt haben.

Gemäß Artikel 2 Absatz 2 kann jeder Mitgliedstaat beschließen, dass Handlungen nach Absatz 1 nur geahndet werden, sofern sie durch eine Verletzung von Sicherheitsmaßnahmen erfolgen. Von dieser Option haben sieben der 20 Mitgliedstaaten Gebrauch gemacht (*Österreich*, *Finnland*, *Deutschland*, *Ungarn*, *Italien*, *Lettland* und *Litauen*).

2.4. Rechtswidriger Systemeingriff (Artikel 3)

Nach Ansicht der Kommission sind alle 20 Mitgliedstaaten der Hauptverpflichtung nachgekommen, sicherzustellen, dass die vorsätzliche schwere Behinderung oder Störung des Betriebs eines Informationssystems durch Eingeben, Übermitteln, Beschädigen, Löschen, Verstümmeln, Verändern, Unterdrücken oder Unzugänglichmachen von Computerdaten unter Strafe gestellt wird.

Um eine wirklich fundierte Bewertung vornehmen zu können, müssen jedoch die Vorgehensweisen jener Mitgliedstaaten, die diesen ausführlichen RB-Artikel mit relativ allgemeinen Bestimmungen umgesetzt haben, genauer analysiert werden. Dies gilt zum Beispiel für *Dänemark*, das erklärt hat, dass eine sehr allgemeine Bestimmung über die Zerstörung, Beschädigung oder Beseitigung von Eigentum jeglicher Art alle in dem Artikel aufgezählten Kriterien abdeckt. Auch wenn ein solcher Ansatz grundsätzlich akzeptabel ist, stellt sich die Frage, inwieweit eine solche Bestimmung auf Angriffe auf den Zugang anwendbar ist, vor allem in Fällen, in denen die Beschädigung vielleicht nur vorübergehender Natur ist.[6]

Nach dem letzten Teil von Artikel 3 haben die Mitgliedstaaten die Option, solche Handlungen nur dann unter Strafe zu stellen, „wenn kein leichter Fall vorliegt“. Von dieser Option haben sechs Mitgliedstaaten Gebrauch gemacht, die mehr oder weniger ausdrücklich erklärt haben, dass die folgenden Regelungen diese Bedingung abdecken:

– Im *österreichischen* Recht werden Systemeingriffe nur in schweren Fällen unter Strafe gestellt.

– Nach *tschechischem* Recht muss der Vorsatz, eine Schädigung oder einen Verlust zu verursachen, vorliegen.[7]

---

6 Wie ein anderer Mitgliedstaat in einer Mitteilung an die Kommission betont hat.

7 Laut Auskunft der tschechischen Regierung wird diese Bedingung nach Verabschiedung des neuen Strafrechts fallen gelassen.

– Das *deutsche* Recht sieht die Bedingung vor, dass das Informationssystem, das Gegenstand eines Systemeingriffs war, „für einen anderen von wesentlicher Bedeutung“ ist.

– Nach *estnischem* Recht erfolgt nur dann eine strafrechtliche Ahndung, wenn erheblicher Schaden … verursacht wird.

– Im *litauischen* Recht werden nur Handlungen unter Strafe gestellt, durch die … ein Schaden verursacht wird.

– Nach *lettischem* Recht sind Systemeingriffe nur dann strafbar, wenn die Schutzsysteme geschädigt oder zerstört werden oder ein umfangreicher Verlust verursacht wird.

Damit bewertet werden kann, ob die oben erwähnten Regelungen mit dem RB in Einklang stehen, bedarf es auch hier einer näheren Erläuterung der Formulierung „wenn kein leichter Fall vorliegt“. Hierauf wurde bereits in Abschnitt 2.3 im Zusammenhang mit Artikel 2 hingewiesen.

Artikel 3 zielt auf den Schutz der Integrität der Informationssysteme ab. Daher ist die Kommission der Ansicht, dass unter minder schweren Fällen solche zu verstehen sind, in denen der Systemeingriff als solcher von geringer Bedeutung ist oder in denen die Integrität des Informationssystems nur in geringem Maße angetastet wurde. Die oben erwähnten einschlägigen *österreichischen*, *tschechischen*, *estnischen* und *litauischen* Vorschriften stellen offensichtlich genau auf solche Fälle ab. Es ist davon auszugehen, dass sie der Vorgabe, dass nur geringfügige Systemeingriffe nicht geahndet werden brauchen, Rechnung tragen.

Allerdings verweisen die einschlägigen *deutschen* Vorschriften auf die Bedeutung für einen anderen und die *lettischen* Vorschriften auf eine Schädigung der Schutzsysteme oder einen umfangreichen Verlust. Nach Auffassung der Kommission weisen diese Vorschriften einen unzureichenden Bezug zur Integrität der Informationssysteme auf, so dass nicht bewertet werden kann, ob sie mit der RB-Option vereinbar sind, wonach minder schwere Fälle nicht geahndet werden brauchen. Außerdem ist die Kommission der Ansicht, dass dies nicht in Einklang mit dem Ziel des RB steht, die einzelstaatlichen Strafrechtsvorschriften für Angriffe auf Informationssysteme anzugleichen.

Generell ist die Verwirklichung des Ziels der Angleichung der einzelstaatlichen Strafrechtsvorschriften für Angriffe auf Informationssysteme durch derart divergierende Auslegungen und Anwendungen der Option, bestimmte Handlungen nicht zu ahnden, ernsthaft gefährdet.

Dementsprechend ist die Kommission der Auffassung, dass lediglich 18 der 20 Mitgliedstaaten Artikel 3 des RB nachweislich ordnungsgemäß umgesetzt haben.

2.5. Rechtswidriger Eingriff in Daten (Artikel 4)

Nach Auffassung der Kommission sind alle 20 Mitgliedstaaten der Hauptverpflichtung nachgekommen, sicherzustellen, dass das vorsätzliche Löschen, Beschädigen, Verstümmeln, Verändern, Unterdrücken oder Unzugänglichmachen von Computerdaten eines Informationssystems unter Strafe gestellt wird. Viele

Mitgliedstaaten haben die Artikel 3 und 4 in einer einzigen innerstaatlichen Bestimmung umgesetzt. Im Falle *Dänemarks* kann nach Auffassung der Kommission auch hier nicht unbedingt davon ausgegangen werden, dass eine sehr allgemein gehaltene Bestimmung über die Zerstörung, Beschädigung oder Beseitigung von Eigentum jeglicher Art alle in dem Artikel aufgezählten Handlungen in Bezug auf Computerdaten abdeckt. In diesem Zusammenhang ist auf die Anmerkungen zu Artikel 3 in Abschnitt 2.4 zu verweisen.

Nach dem letzten Teil des Artikels haben die Mitgliedstaaten die Option, solche Handlungen nur dann unter Strafe zu stellen, „wenn kein leichter Fall vorliegt". Von dieser Option haben drei Mitgliedstaaten Gebrauch gemacht, die mehr oder weniger ausdrücklich erklärt haben, dass die folgenden Regelungen diese Bedingung abdecken:

– Nach *tschechischem* Recht muss der Vorsatz, eine Schädigung oder einen Verlust zu verursachen, vorliegen.[8]

– Nach *estnischem* Recht erfolgt nur dann eine strafrechtliche Ahndung, wenn erheblicher Schaden … verursacht wird.

– Im *lettischen* Recht (Artikel 234 des Strafrechts) gilt als Kriterium, ob die Schutzsysteme geschädigt oder zerstört werden oder ein umfangreicher Verlust verursacht wird.

Wie bereits in Abschnitt 2.4 in Bezug auf die entsprechenden Bestimmungen zur Umsetzung von Artikel 3 des RB erläutert, ist die Kommission der Ansicht, dass das tschechische Recht in dieser Hinsicht mit dem RB vereinbar ist und davon auszugehen ist, dass dies auch für das estnische Recht gilt. Dagegen kann auch hier nicht davon ausgegangen werden, dass Lettland seinen Verpflichtungen bezüglich dieses Aspekts des RB vollständig nachgekommen ist.

Nach Auffassung der Kommission haben 19 der 20 Mitgliedstaaten Artikel 4 des RB nachweislich ordnungsgemäß umgesetzt.

2.6. Anstiftung, Beihilfe und Versuch (Artikel 5)

Nach Ansicht der Kommission sind 18 der 20 Mitgliedstaaten der Hauptverpflichtung grundsätzlich nachgekommen, sicherzustellen, dass die Anstiftung oder Beihilfe zur Begehung einer Straftat sowie der Versuch der Begehung einer Straftat unter Strafe gestellt wird. *Finnland* und *Portugal* haben lediglich die innerstaatlichen Vorschriften betreffend den Versuch mitgeteilt und somit nicht nachgewiesen, inwiefern die Verpflichtungen betreffend die Anstiftung und die Beihilfe im innerstaatlichen Recht abgedeckt sind. Das *schwedische Recht* sieht keine Ahndung für minder schwere Fälle von Anstiftung, Beihilfe oder Versuch vor. Dieser Ansatz ist nicht mit den Vorgaben des RB vereinbar.

Die Mitgliedstaaten können beschließen, die Verpflichtung sicherzustellen, dass der Versuch der Begehung der Straftat des rechtswidrigen Zugangs zu

[8] Laut Auskunft der tschechischen Regierung wird diese Bedingung nach Verabschiedung des neuen Strafrechts fallen gelassen.

Informationssystemen unter Strafe gestellt wird, nicht umzusetzen. *Deutschland* und *Slowenien* haben mitgeteilt, dass sie von dieser Möglichkeit Gebrauch machen.

Die Kommission ist daher der Ansicht, dass Artikel 5 in 17 der 20 Mitgliedstaaten ordnungsgemäß umgesetzt wurde.

2.7. Sanktionen und erschwerende Umstände (Artikel 6 und 7)

Nach Auffassung der Kommission haben alle 20 Mitgliedstaaten sichergestellt, dass die Straftaten nach den Artikeln 2 bis 5 des RB mit wirksamen, verhältnismäßigen und abschreckenden strafrechtlichen Sanktionen bedroht werden.[9] Die für rechtswidrige Systemeingriffe und rechtswidrige Eingriffe in Daten vorgesehenen Sanktionen erfüllen auch die besonderen Vorgaben von Artikel 6 Absatz 2 des RB.

Stärkere Abweichungen gibt es hinsichtlich der Verpflichtung, den „erschwerenden Umständen" im Falle von Straftaten, die im Rahmen einer kriminellen Vereinigung begangen wurden, Rechnung zu tragen (Artikel 7).

– Die von *Österreich* mitgeteilten Vorschriften erfüllen diese Vorgabe des RB eindeutig nicht.

– Das *dänische* Recht enthält keinen direkten Verweis auf kriminelle Vereinigungen.

– Die einschlägigen *finnischen* Vorschriften enthalten keinen Verweis auf kriminelle Vereinigungen.

– Um dem RB vollständig nachzukommen, muss *Portugal* einige Anpassungen an seinen Vorschriften vornehmen.

In den Vorschriften, die andere Mitgliedstaaten (*Bulgarien, Italien, Lettland* und *Schweden*) der Kommission mitgeteilt haben, findet sich kein Verweis auf das Kriterium „kriminelle Vereinigungen". Allerdings ist den übermittelten Angaben zu entnehmen, dass die Verpflichtung zur Verhängung schwererer Sanktionen für Straftaten, an denen eine kriminelle Vereinigung beteiligt ist, bereits in vollem Umfang – wenn auch indirekt – durch die innerstaatlichen Vorschriften *Bulgariens, Italiens* und *Lettlands* abgedeckt ist. Die in diesen Mitgliedstaaten für die fraglichen Straftaten geltenden Vorschriften sehen die in Artikel 7 des RB genannten schwereren Mindestsanktionen vor. Die schwedische Regierung hat erklärt, dass Straftaten, die im Rahmen einer kriminellen Vereinigung begangen wurden, im schwedischen Recht durch den erschwerenden Umstand „schwere Straftat" vollständig abgedeckt sind, und hat dies eingehend erläutert.

Daher ist die Kommission der Ansicht, dass Artikel 6 von allen 20 Mitgliedstaaten ordnungsgemäß umgesetzt wurde und dass 16 von ihnen den Verpflichtungen aus Artikel 7 des RB nachgekommen sind.

---

[9] In diesem Zusammenhang ist zu erwähnen, dass Österreich selbst zu bezweifeln scheint, dass die im österreichischen Recht vorgesehenen Sanktionen für rechtswidrige Systemeingriffe ausreichend abschreckend sind.

2.8. Verantwortlichkeit juristischer Personen und Sanktionen gegen juristische Personen (Artikel 8 und 9)

Nach Auffassung der Kommission haben 16 der 20 Mitgliedstaaten eindeutig die erforderlichen Maßnahmen getroffen, um sicherzustellen, dass juristische Personen unter den in Artikel 8 Absatz 1 beschriebenen Umständen für die in den Artikeln 2 bis 5 aufgeführten Straftaten verantwortlich gemacht werden können.

Die *Tschechische Republik*[10], *Lettland* und *Luxemburg*[11] sind ihrer Verpflichtung zur Übermittlung der entsprechenden Vorschriften an die Kommission nicht nachgekommen.

Estland hat erklärt, dass seine Vorschriften über die zivilrechtliche Verantwortlichkeit alle in Artikel 8 Absatz 1 beschriebenen Fälle abdecken, hat aber der Kommission keine näheren Angaben dazu gemacht. Es gibt keine Vorgabe hinsichtlich der Art der Verantwortlichkeit juristischer Personen; innerstaatliche Vorschriften über die verwaltungs- oder zivilrechtliche Verantwortlichkeit, die vollständig mit Artikel 8 vereinbar sind, können also theoretisch durchaus genügen. Allerdings hat *Estland* nicht erläutert, inwiefern sein Gesetz über die zivilrechtliche Verantwortlichkeit die Vorgaben des RB vollständig erfüllt.

Gemäß Artikel 8 Absatz 2 sind die Mitgliedstaaten verpflichtet sicherzustellen, dass eine juristische Person verantwortlich gemacht werden kann, wenn mangelnde Überwachung oder Kontrolle durch die in Absatz 1 genannte Person die Begehung der Straftat zugunsten der juristischen Person durch eine ihr unterstellte Person ermöglicht hat. Nach Ansicht der Kommission sind 10 der 20 Mitgliedstaaten dieser Forderung nachgekommen. Neben der *Tschechischen Republik*, *Estland*, *Lettland* und *Luxemburg*, in deren Fall die Schlussfolgerungen hinsichtlich Artikel 8 Absatz 1 auch auf Artikel 8 Absatz 2 zutreffen, haben *Dänemark*, *Finnland*, *Frankreich* und *Portugal* keine einschlägigen Vorschriften über die Verantwortlichkeit juristischer Personen vorgelegt. *Frankreich* hat erklärt, dass sich eine solche Verantwortlichkeit aus den Vorschriften über die zivilrechtliche Verantwortlichkeit ergibt, hat aber den genauen Inhalt dieser Verantwortlichkeit nicht erläutert.

Gemäß Artikel 9 müssen die Mitgliedstaaten außerdem die erforderlichen Maßnahmen treffen, um sicherzustellen, dass gegen eine im Sinne von Artikel 8 Absatz 1 und Artikel 8 Absatz 2 verantwortliche juristische Person wirksame, verhältnismäßige und abschreckende Sanktionen verhängt werden können. Die 14 Mitgliedstaaten, die Vorschriften zur ordnungsgemäßen Umsetzung von Artikel 8 Absatz 1 übermittelt haben, und die 10 Mitgliedstaaten, die ihren Verpflichtungen nach Artikel 8 Absatz 2 nachgekommen sind, haben auch diese Vorgaben erfüllt.

Dementsprechend ist die Kommission der Auffassung, dass lediglich 12 der 20 Mitgliedstaaten Artikel 8 und 9 des RB nachweislich vollständig umgesetzt haben.

---

[10] Die tschechische Regierung hat erklärt, dass das tschechische Recht einige einschlägige Bestimmungen über die zivilrechtliche Verantwortlichkeit enthält, hat aber weder den Wortlaut dieser Bestimmungen übermittelt noch deren Inhalt erläutert.

[11] Dem luxemburgischen Parlament wurde 2007 ein Vorschlag für Vorschriften, die diese Verpflichtung abdecken, vorgelegt, der Kommission ist jedoch nicht bekannt, ob der Vorschlag angenommen wurde.

2.9. Gerichtliche Zuständigkeit (Artikel 10)

Nach Ansicht der Kommission sind 17 der 20 Mitgliedstaaten ihrer Verpflichtung nachgekommen, ihre gerichtliche Zuständigkeit in Bezug auf die Straftaten nach den Artikeln 2 bis 5 des RB (auf der Grundlage der in Artikel 10 genannten besonderen Kriterien) zu begründen. Obwohl die unterschiedlichen Verfahren der Mitgliedstaaten zur Regelung der gerichtlichen Zuständigkeit einen Vergleich erschweren, ist die Kommission der Auffassung, dass der Artikel korrekt umgesetzt wurde. *Lettland* und *Portugal* sind ihrer Verpflichtung, die Kommission von den innerstaatlichen Vorschriften zur Umsetzung von Artikel 10 in Kenntnis zu setzen, nicht nachgekommen.

Von der in Absatz 5 vorgesehenen Option, wonach die Mitgliedstaaten beschließen können, die Zuständigkeitsregelung gemäß Absatz 1 Buchstaben b und c nicht oder nur in bestimmten Fällen oder unter bestimmten Umständen anzuwenden, haben *Frankreich* (im Falle von Absatz 1 Buchstabe b) sowie *Österreich*, *Finnland*, *Deutschland*, *Ungarn* und *Litauen* (im Falle von Absatz 1 Buchstabe c) Gebrauch gemacht und die Kommission entsprechend informiert. Offensichtlich haben *Italien* (in Bezug auf Absatz 1 Buchstaben b und c) sowie *Estland* und *Rumänien* (in Bezug auf Absatz 1 Buchstabe c) diese Option ebenfalls in Anspruch genommen, auch wenn sie dies nicht formal bestätigt haben. *Österreich* hat die Kommission davon in Kenntnis gesetzt, dass es noch prüft, ob es von der Option weiterhin Gebrauch machen wird.

Dementsprechend ist die Kommission der Ansicht, dass Artikel 10 in 17 der 20 Mitgliedstaaten ordnungsgemäß umgesetzt wurde.

2.10. Informationsaustausch (Artikel 11)

Die Mitgliedstaaten sind verpflichtet sicherzustellen, dass sie das bestehende Netz der operativen Kontaktstellen, die rund um die Uhr und sieben Tage pro Woche erreichbar sind, nutzen. Die Kommission hat keinerlei Informationen erhalten, anhand deren sie bewerten könnte, ob dies in Bezug auf den RB in *Belgien*, der *tschechischen Republik*, *Deutschland*, *Italien*, *den Niederlanden*, *Portugal* und *Slowenien* der Fall ist.

Hinsichtlich der Verpflichtung, das Generalsekretariat des Rates und die Kommission davon in Kenntnis zu setzen, welche Kontaktstelle benannt wurde (Artikel 11 Absatz 2), ist der Kommission keine klare Mitteilung von *Österreich*, *Bulgarien*, *Italien* und *Portugal* zugegangen.

Dementsprechend ist die Kommission der Auffassung, dass lediglich 11 der 20 Mitgliedstaaten nachweislich allen Verpflichtungen aus Artikel 11 vollständig nachgekommen sind.

3. SCHLUSSFOLGERUNGEN

3.1. Umsetzungsstand

Dieser Bericht liefert einen ersten Überblick über die Umsetzung des RB durch die Mitgliedstaaten. Er bestätigt, dass die Mitgliedstaaten Strafrechtsvorschriften sehr

unterschiedlich umsetzen und es daher schwierig ist, die innerstaatlichen Vorschriften eingehend zu bewerten, ohne zu prüfen, wie sie in der Praxis angewandt werden.

Die Umsetzung des RB in den Mitgliedstaaten ist noch nicht abgeschlossen. In nahezu allen 20 Mitgliedstaaten, die in diesem Bericht bewertet werden, sind beachtliche Fortschritte erzielt worden, so dass der Umsetzungsstand relativ gut ist.

Bedenken hat die Kommission *vor allem* wegen der sieben Mitgliedstaaten, die die Umsetzungsvorschriften noch mitteilen müssen. Sie ersucht die Mitgliedstaaten, die den RB noch nicht in innerstaatliches Recht umgesetzt haben, dies so bald wie möglich nachzuholen. Sie fordert die Mitgliedstaaten außerdem auf, ihre Rechtsvorschriften sorgfältig im Hinblick darauf zu überprüfen, wie ihre Anstrengungen zur Bekämpfung von Angriffen auf Informationssysteme verstärkt werden können.

3.2. Künftige Entwicklungen

Nach Annahme des RB haben in jüngster Zeit Angriffe auf Informationssysteme in Europa mehrere neue Gefahren verdeutlicht, insbesondere massive gleichzeitige Angriffe auf Informationssysteme und eine zunehmende kriminelle Nutzung so genannter Botnets[12]. Diese Angriffe standen nicht im Mittelpunkt des Interesses, als der RB angenommen wurde. Um diesen Entwicklungen entgegenzutreten, wird die Kommission prüfen, mit welchen Maßnahmen besser auf die Bedrohung durch Botnets reagiert werden kann. So könnte unter anderem erwogen werden, bestimmte Aktivitäten, die die kriminelle Nutzung von Botnets erleichtern, auf besondere Weise zu ahnden sowie härtere Mindestsanktionen für Straftaten in Form von massiven und besonders gefährlichen Angriffen auf Informationssysteme zu verhängen.

Die Kommission erwägt auch, Maßnahmen zu treffen, mit denen eine wirksame und rechtzeitige Inanspruchnahme der rund um die Uhr erreichbaren Kontaktstellen nach Artikel 11 gefördert werden soll. Schwerwiegende Vorfälle haben 2007 verdeutlicht, dass auf internationaler Ebene rasch gemeinsame Maßnahmen – häufig unter Einbeziehung privater Akteure – getroffen werden müssen, um gegen massive Angriffe auf Informationssysteme vorzugehen. Im Hinblick auf eine bessere Koordinierung und Kohärenz eines solchen Reaktionssystems sollten die Mitgliedstaaten weiter prüfen, ob dieselben Kontaktstellen wie im Rahmen der Netzwerke des Europarats[13] und der G8 herangezogen werden sollten. Die Kommission wird insbesondere erwägen, EU-Leitlinien zur Nutzung der verschiedenen internationalen Netze zur Bekämpfung der Hightech-Kriminalität festzulegen.

---

[12] Unter dem Begriff „Botnet“ oder „Bot-Netz“ (Kurzform von Roboter-Netzwerk) ist ein fernsteuerbares Netz von infizierten Rechnern zu verstehen.

[13] Artikel 35 des Europarat-Übereinkommens.