EUROPÄISCHE KOMMISSION

Brüssel, den 30.9.2010
SEK(2010) 1123 final

ARBEITSDOKUMENT DER KOMMISSIONSDIENSTSTELLEN

ZUSAMMENFASSUNG DER FOLGENABSCHÄTZUNG

Begleitunterlage zum

Vorschlag für eine

RICHTLINIE DES EUROPÄISCHEN PARLAMENTS UND DES RATES

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

{KOM(2010) 517 final}
{SEK(2010) 1122 final}

ZUSAMMENFASSUNG DER FOLGENABSCHÄTZUNG

1. PROBLEMSTELLUNG

Die Zahl der Angriffe auf Informationssysteme hat seit dem Erlass des Rahmenbeschlusses über Angriffe auf Informationssysteme stark zugenommen. Laut einem Bericht eines der führenden Internetsicherheitsunternehmen stieg die Zahl der Attacken auf vertrauliche Informationen (im Gegensatz zu öffentlich verfügbaren Informationen) 2008 erheblich an: von 624 267 auf 1 656 227[1]. Zudem kam es zu einigen Angriffen von bis dahin ungekanntem Ausmaß und Gefahrenpotenzial wie denjenigen in Estland 2007 und Litauen 2008. Im März 2009 griff ein Netz infizierter Computer die Computersysteme staatlicher und privater Organisationen in 103 Ländern an und verschaffte sich Zugang zu sensiblen und vertraulichen Dokumenten[2]. Für den Angriff wurden sogenannte „Botnetze“[3]verwendet, d. h. Netze infizierter Computer, die ferngesteuert werden können. Derzeit erlebt die Welt die Ausbreitung des Botnetzes „Conficker“ (auch unter den Namen Downup, Downadup und Kido bekannt), das sich seit November 2008 in noch nie da gewesenem Maße verbreitet und mittlerweile Millionen Computer weltweit befallen hat[4].

Ferner erschwert die ungenügende Zusammenarbeit zwischen den Mitgliedstaaten und insbesondere zwischen den Strafverfolgungs- und Justizbehörden in der EU eine koordinierte und wirksame Reaktion auf die Angriffe. Aus dem Umsetzungsbericht zum Rahmenbeschluss geht zwar hervor, dass die Mehrzahl der Mitgliedstaaten – wie in Artikel 11 des Rahmenbeschlusses gefordert – ständige Kontaktstellen eingerichtet hat, doch bestehen nach wie vor Probleme hinsichtlich ihrer Einsatzbereitschaft und ihrer Fähigkeit, auf dringende Kooperationsersuchen zu reagieren[5].

Dass eine Kontaktstelle existiert, bedeutet nicht, dass sie auch reibungslos funktioniert. In ihren Mitteilungen an die Kommission gaben mehrere Mitgliedstaaten an, dass sie zwar ihre jeweiligen Kontaktstellen eingerichtet hatten, doch dass diese nicht – wie im Rahmenbeschluss über Angriffe gefordert – rund um die Uhr erreichbar seien. Dies deutet darauf hin, dass sie außerhalb der Dienstzeiten nicht auf dringende Anträge reagieren können. Die öffentlich-private Zusammenarbeit wird oft durch die geringe Effizienz der

---

1 http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xiv_04-2009.en-us.pdf, S.10.

2 http.www.theglobeandmail.com/servlet/story/RTGAM.20090328.wspy0328/BNStory/International/home?cid=al_gam_mostemail.

3 Der Ausdruck Botnetz bezeichnet ein Netz von Computern, die mit Schadsoftware (Computerviren) infiziert wurden. Ein solches Netzwerk aus infizierten Computern („Zombies“) kann ferngesteuert bestimmte Handlungen ausführen, beispielsweise Informationssysteme angreifen (Cyberangriffe). Diese „Zombies“ können von einem anderen Computer kontrolliert werden – häufig ohne Wissen der Nutzer dieser infizierten Computer. Die Kontrolle über ein Botnetz übt ein sogenannter „Master-Server“ – auch als „Command-and-Control-Server“ bezeichnet – aus. Die Personen, die diesen Server kontrollieren, sind zum Täterkreis zu rechnen, da sie die infizierten Computer zum Angriff auf Informationssysteme nutzen. Es ist sehr schwierig, diesen Tätern auf die Spur zu kommen, da sich das Botnetz, das die Attacke ausführt, an einem anderen Ort befinden kann als die Täter.

4 http://www.lemonde.fr/technologies/article/2009/03/31/virus-conficker-catastrophe-ou-poisson-d-avril_1174916_651865.html.

5 Bericht der Kommission an den Rat auf der Grundlage von Artikel 12 des Rahmenbeschlusses des Rates vom 24. Februar 2005 über Angriffe auf Informationssysteme, KOM (2008) 448 endgültig.

Kontaktstellen oder ihre Unfähigkeit, Kooperationsanträge aus dem Privatsektor zu bearbeiten, erschwert.

Darüber hinaus gibt es immer noch zu wenig Daten zu Cyberangriffen und den entsprechenden polizeilichen und strafrechtlichen Folgemaßnahmen. Nicht alle Mitgliedstaaten erheben Daten zu Cyberangriffen. Wo dies getan wird, eignen sich die erhobenen Daten aufgrund der unterschiedlichen statistischen Methoden in den verschiedenen Mitgliedstaaten nicht zum Vergleich.

Zu den Opfern der groß angelegten Angriffe auf Informationssysteme zählen sowohl die allgemeine Öffentlichkeit, d. h. die Benutzer der Informationssysteme, als auch zentrale und lokale Regierungsstellen, internationale Organisationen und Privatunternehmen.

Es ist möglich, von Drittstaaten aus Ziele innerhalb der EU anzugreifen und umgekehrt.

2. SUBSIDIARITÄT

Die Cyberkriminalität ist ein internationales Problem, das nur selten in einem rein einzelstaatlichen Rahmen bekämpft werden kann. Es ist allgemein anerkannt, dass Maßnahmen auf internationaler und auf EU-Ebene erforderlich sind, um diese Art von Kriminalität zu verhindern und zu bekämpfen. Die meisten Angriffe erfolgen über die Grenzen der EU hinweg. Sie betreffen alle Mitgliedstaaten, und es liegen Belege dafür vor, dass bei einem erheblichen Anteil der Angriffe grenzübergreifende Aktivitäten zwischen mehreren Mitgliedstaaten eine Rolle spielen. Informationssysteme sind oft über Grenzen hinweg technisch miteinander verbunden und voneinander abhängig. Unter den Sachverständigen herrscht daher Einigkeit darüber, dass Maßnahmen sowohl auf internationaler als auch auf EU-Ebene notwendig sind und dass die Mitgliedstaaten allein diese Art von Kriminalität nicht hinreichend effektiv bekämpfen können.

Eine einzelstaatliche Strategie gegenüber der Cyberkriminalität birgt die Gefahr von Uneinheitlichkeit und Effizienzverlust in Europa. Unterschiedliche einzelstaatliche Strategien und das Fehlen einer systematischen grenzübergreifenden Zusammenarbeit schränken die Wirksamkeit einzelstaatlicher Gegenmaßnahmen erheblich ein. Dies liegt teilweise daran, dass aufgrund der Vernetzung von Informationssystemen ein niedriges Sicherheitsniveau in einem Land die Anfälligkeit in anderen Ländern verstärken kann.

3. ZIELSETZUNG

3.1 Allgemeine, spezifische und operative Ziele

Das grundlegende Ziel der Maßnahmen der EU besteht gemäß Artikel 67 des Vertrags über die Arbeitsweise der Europäischen Union darin, organisierte und andere Kriminalität zu bekämpfen und zu verfolgen, indem groß angelegte Cyberangriffe auf Informationssysteme bekämpft werden.

A Spezifisches Ziel: Strafverfolgung und Verurteilung von Kriminellen, die für groß angelegte Angriffe verantwortlich sind, durch Angleichung der Strafvorschriften im Bereich der Angriffe auf Informationssysteme

B Spezifisches Ziel: Verbesserung der grenzübergreifenden Zusammenarbeit zwischen Strafverfolgungsbehörden

C Spezifisches Ziel: Einrichtung wirksamer Überwachungssysteme und Datenerhebung

4. OPTIONEN

4.1 Option 1 – Status quo / keine neuen Maßnahmen auf EU-Ebene

Bei dieser Option würde die EU keine weiteren Maßnahmen ergreifen, um gegen diese besondere Form der Cyberkriminalität vorzugehen. Laufende Maßnahmen – insbesondere die Programme zur Stärkung des Schutzes kritischer Informationsinfrastrukturen und zur Verbesserung der öffentlich-privaten Zusammenarbeit bei der Bekämpfung der Cyberkriminalität – würden fortgesetzt.

4.2 Option 2 – Ausarbeitung eines Programms zur Stärkung der Abwehr von Angriffen auf Informationssysteme durch nichtlegislative Maßnahmen

Nichtlegislative Maßnahmen würden zusätzlich zu dem Programm zum Schutz kritischer Informationsinfrastrukturen bei der grenzübergreifenden Strafverfolgung und der Zusammenarbeit zwischen dem öffentlichen und dem privaten Sektor ansetzen und ein weiteres koordiniertes Vorgehen auf EU-Ebene erleichtern. Ein nichtlegislativer Vorschlag könnte Maßnahmen umfassen wie die Stärkung des bestehenden rund um die Uhr erreichbaren Kontaktnetzes der Strafverfolgungsbehörden, die Einrichtung eines EU-Netzes öffentlich-privater Kontaktstellen für Sachverständige im Bereich Cyberkriminalität und Strafverfolgungsbehörden sowie die Ausarbeitung eines EU-Mustervertrags für die Zusammenarbeit der Strafverfolgungsbehörden mit dem Privatsektor.

4.3 Option 3 – Gezielte Aktualisierung des Rahmenbeschlusses, um die Bedrohung abzuwenden, die von groß angelegten Angriffen auf Informationssysteme ausgeht

Diese Option beinhaltet die Einführung spezifischer (d. h. begrenzter) Rechtsvorschriften gegen besonders gefährliche, groß angelegte Angriffe auf Informationssysteme. Solche zielgerichteten Rechtsvorschriften wären mit Maßnahmen zur Verstärkung der operativen grenzübergreifenden Zusammenarbeit gegen Angriffe auf Informationssysteme verbunden und würden eine Erhöhung der bereits vorgesehenen Mindeststrafen bedeuten. Die Option würde in einer Aktualisierung des bestehenden Rahmenbeschlusses bestehen, die durch eine Reihe nichtlegislativer Maßnahmen ergänzt würde. Zu diesen würde eine Stärkung der Abwehrbereitschaft, Sicherheit und Stabilität kritischer Informationsinfrastrukturen sowie der Instrumente und Verfahren für die grenzübergreifende Zusammenarbeit bei der Strafverfolgung und des Austauschs bewährter Verfahren zählen.

4.4 Option 4 - Einführung einer umfassenden EU-Regelung gegen Cyberkriminalität

Die Feststellung, dass rasch gegen die Entwicklung ausgeklügelter Angriffe auf Informationssysteme vorgegangen werden muss, wirft die Frage auf, ob die Einführung umfassenderer EU-Rechtsvorschriften gegen Cyberkriminalität allgemein angebracht wäre. Solche Rechtsvorschriften würden sich nicht nur gegen Angriffe auf Informationssysteme

richten, sondern beispielsweise auch gegen Finanzkriminalität mithilfe des Internet und illegale Webinhalte. Geregelt würden auch die Erhebung, Speicherung und Weitergabe elektronischer Beweismittel, und es würden detailliertere Zuständigkeitsvorschriften festgelegt. Derartige EU-Rechtsvorschriften würden parallel zum Übereinkommen des Europarats über Computerkriminalität gelten, das insbesondere durch neue Bestimmungen ergänzt würde, die in der EU für erforderlich gehalten werden.

4.5 Option 5 – Aktualisierung des Übereinkommens des Europarats über Computerkriminalität

Diese Option erfordert eine grundlegende Neuverhandlung des geltenden Übereinkommens, was allerdings sehr viel Zeit erfordern würde und deshalb mit den Zeitvorgaben in der Folgenabschätzung nicht vereinbar wäre. Auf internationaler Ebene ist derzeit keine Bereitschaft zur Neuverhandlung des Übereinkommens erkennbar. Eine Aktualisierung des Übereinkommens stellt keine realistische Option dar, da diese den vorgegebenen Zeitrahmen sprengen würde.

5. ABSCHÄTZUNG DER FOLGEN

Optionen	Wirtschaftliche Folgen	Gesellschaft-liche Folgen	Folgen für Grundrechte	Folgen für Drittländer	Relevanz für die Ziele A, B und C	Kohärenz mit internationalem Recht
Option 1: Status quo / keine neuen Maßnahmen auf EU-Ebene	0	0	0	-	0	0
Option 2: Ausarbeitung eines Programms zur Stärkung der Abwehr von Angriffen auf Informationssysteme durch nichtlegislative Maßnahmen	-/+	++	-/+	++	A + B ++ C +	-/+
Option 3: Gezielte Aktualisierung des Rahmenbeschlusses, um die Bedrohung abzuwenden, die von groß angelegten Angriffen auf Informationssysteme ausgeht	--/++	-/+++	-/++	+++	A +++ B +++ C +++	++

Option 4: Einführung einer umfassenden EU-Regelung gegen Cyberkriminalität	---/+++	+++	--/++	++	A ++ B ++ C ++	-/++
Bevorzugte Option (Optionen 2 und 3) Kombination aus nichtlegislativen Maßnahmen und einer gezielten Aktualisierung des Rahmenbeschlusses	--/+++	+++	-/++	+++	A +++ B +++ C +++	++

6. WIE STELLEN SICH DIE OPTIONEN IM VERGLEICH DAR?

6.1 Option 1 – Status quo

Diese Option wird angesichts der Art und der Zunahme der Cyberkriminalität unweigerlich zu einer schwächeren Position privater Akteure, der Mitgliedstaaten und der Europäischen Union insgesamt führen. Selbst bei einer Beibehaltung des derzeit bestehenden Maßnahmenniveaus wäre eine europäische Koordinierung erforderlich.

6.2 Option 2 – Ausarbeitung eines Programms zur Stärkung der Abwehr von Angriffen auf Informationssysteme durch nichtlegislative Maßnahmen

Diese Option hat alle Vor- und Nachteile eines nicht rechtsverbindlichen Instruments („Soft-Law-Instrument“). Positiv ist, dass die Möglichkeit besteht, jede Option so zu gestalten, dass sie den bewährten nationalen Verfahren entspricht, und es somit einfacher wird, die wirksamsten Maßnahmen zu ermitteln.

Allerdings ist diese Option im Hinblick auf das Erreichen der Ziele weniger effektiv.

6.3 Option 3 – Gezielte Aktualisierung des Rahmenbeschlusses, um die Bedrohung abzuwenden, die von groß angelegten Angriffen auf Informationssysteme ausgeht

Diese Option ermöglicht eine rechtzeitige und zielgerichtete Reaktion auf die festgestellten Probleme. Sie behandelt die strafrechtlichen Fragen, die beantwortet werden müssen, damit eine wirksame Strafverfolgung der Täter bei dieser Art von Kriminalität möglich wird. Sie verbessert auch die internationale Zusammenarbeit durch die Einführung eines Mechanismus für internationale Soforthilfe bei dringenden Kooperationsersuchen und fördert die Zusammenarbeit mit dem privaten Sektor durch Begleitmaßnahmen wie Expertentreffen. Zudem werden mit dieser Option mehrere erschwerende Umstände eingeführt, u. a. der große Umfang der Angriffe sowie Angriffe, bei denen die wahre Identität des Täters verschleiert und der rechtmäßige Inhaber der Identität geschädigt werden.

Um das Problem in seinem ganzen Ausmaß erfassen zu können, sind Überwachungspflichten vorgesehen.

6.4 Option 4 - Einführung einer umfassenden EU-Regelung gegen Cyberkriminalität

Diese Option bringt wie Option 3 den zusätzlichen Nutzen der Festlegung verbindlicher Vorschriften. Bei vollständiger Umsetzung ist somit eine größere Wirksamkeit zu erwarten. Zudem wird die Option voraussichtlich die positiven Auswirkungen sowohl der legislativen als auch der nichtlegislativen Instrumente nicht nur im Bereich der groß angelegten Angriffe, sondern auch in weiteren Bereichen der Cyberkriminalität maximieren. Zusätzlich würde der strafrechtliche Rechtsrahmen angegangen und gleichzeitig die grenzübergreifende strafrechtliche Zusammenarbeit verbessert. Auf diesen ganzheitlichen Ansatz können sich die Beteiligten zum jetzigen Zeitpunkt jedoch nicht einigen, auch wenn seine Umsetzung die Bekämpfung der Cyberkriminalität einen Schritt weiter voranbringen würde als alle anderen Optionen.

7. BEVORZUGTE OPTION

Eine Analyse der wirtschaftlichen und gesellschaftlichen Folgen sowie der Auswirkungen auf die Grundrechte ergab, dass sich die Probleme im Hinblick auf die Verwirklichung der festgelegten Ziele am wirkungsvollsten mit den Optionen 2 und 3 angehen lassen.

Insgesamt wäre die bevorzugte Option eine Kombination der Optionen 2 und 3, da sie einander ergänzen und die festgelegten Ziele in Bezug auf sowohl die inhaltlichen als auch die zeitlichen Vorgaben am besten erfüllen.

8. ÜBERWACHUNG UND BEWERTUNG

Binnen zwei Jahren nach Inkrafttreten der Richtlinie soll ein Bericht über ihre Umsetzung veröffentlicht werden. In diesem Bericht sollte auf die genaue Umsetzung der Richtlinie durch die Mitgliedstaaten geachtet werden.

Zudem sollte regelmäßig bewertet werden, wie und in welchem Maße die Richtlinie zur Verwirklichung ihrer Ziele beiträgt. Die erste Bewertung sollte innerhalb von fünf Jahren nach Inkrafttreten der Richtlinie durchgeführt werden. In der Folge wird die Kommission alle fünf Jahre einen Bewertungsbericht veröffentlichen, der auch Informationen über die Umsetzung enthalten wird. Auf der Grundlage der Schlussfolgerungen und Empfehlungen der Bewertungen sollte die Kommission weitere Änderungen an der Richtlinie oder weitere mögliche Entwicklungen berücksichtigen.