KOMMISSION DER EUROPÄISCHEN GEMEINSCHAFTEN

Brüssel, den 30.3.2009
KOM(2009) 149 endgültig

MITTEILUNG DER KOMMISSION AN DAS EUROPÄISCHE PARLAMENT, DEN RAT, DEN EUROPÄISCHEN WIRTSCHAFTS- UND SOZIALAUSSCHUSS UND DEN AUSSCHUSS DER REGIONEN

über den Schutz kritischer Informationsinfrastrukturen

„Schutz Europas vor Cyber-Angriffen und Störungen großen Ausmaßes: Stärkung der Abwehrbereitschaft, Sicherheit und Stabilität“

{SEK(2009) 399}
{SEK(2009) 400}

(von der Kommission vorgelegt)

MITTEILUNG DER KOMMISSION AN DAS EUROPÄISCHE PARLAMENT, DEN RAT, DEN EUROPÄISCHEN WIRTSCHAFTS- UND SOZIALAUSSCHUSS UND DEN AUSSCHUSS DER REGIONEN

über den Schutz kritischer Informationsinfrastrukturen

„Schutz Europas vor Cyber-Angriffen und Störungen großen Ausmaßes: Stärkung der Abwehrbereitschaft, Sicherheit und Stabilität“

1. EINLEITUNG

Die Informations- und Kommunikationstechnologien (IKT) sind in zunehmendem Maße mit unserem Alltagsleben verflochten. Einige dieser IKT-Systeme, -Dienste, -Netze und -Infrastrukturen (kurz: IKT-Infrastrukturen) sind ein unverzichtbarer Teil der europäischen Wirtschaft und Gesellschaft, weil sie entweder Güter und Dienste von grundlegender Bedeutung bereitstellen oder die Grundlage für andere kritische Infrastrukturen bilden. Sie gelten gemeinhin als kritische Informationsinfrastrukturen (KII)[1], da durch ihre Störung oder Zerstörung wichtige gesellschaftliche Funktionen ernsthaft beeinträchtigt würden. Aktuelle Beispiele sind u. a. die Cyber-Großangriffe gegen Estland 2007 und die Unterbrechung von Tiefseekabeln 2008.

Nach Schätzungen des Weltwirtschaftsforums aus dem Jahr 2008 besteht eine Wahrscheinlichkeit von 10 - 20 %, dass sich in den kommenden zehn Jahren ein größerer KII-Ausfall ereignen wird, der für die Weltwirtschaft Kosten von ca. 250 Mrd. US-Dollar verursachen könnte[2].

Die vorliegende Mitteilung konzentriert sich auf die Aspekte Prävention, Abwehrbereitschaft und Problembewusstsein und enthält einen Plan für Sofortmaßnahmen zur Stärkung der Sicherheit und Robustheit der KII. Diese Schwerpunkte stehen mit der vom Rat und dem Europäischen Parlament geforderten Debatte im Einklang, in der die Herausforderungen und Prioritäten der Politik für die Netz- und Informationssicherheit (NIS) sowie die auf EU-Ebene am besten dafür geeigneten Instrumente bestimmt werden sollen. Die Vorschläge ergänzen die Maßnahmen, durch die gegen KII gerichtete kriminelle und terroristische Aktivitäten verhütet, bekämpft und verfolgt werden sollen, und zielen auf Synergien mit laufenden und künftigen EU-Forschungsanstrengungen auf dem Gebiet der Netz- und Informationssicherheit sowie mit einschlägigen internationalen Initiativen ab.

2. POLITISCHES UMFELD

In dieser Mitteilung wird eine europäische Politik zur Verbesserung der Sicherheit in der Informationsgesellschaft und zur Stärkung des Vertrauens in sie entwickelt. Die Kommission wies bereits 2005 auf die dringende Notwendigkeit hin, die Bemühungen um ein stärkeres Vertrauen der Beteiligten in die elektronische Kommunikation und die dazugehörigen Dienste

---

1 Eine Definition für KII wurde in dem Dokument KOM(2005) 576 endg. vorgeschlagen.

2 Global Risks 2008.

zu koordinieren[3]. Zu diesem Zweck wurde 2006 eine Strategie für eine sichere Informationsgesellschaft[4] beschlossen. Ihre wichtigsten Elemente, darunter die Sicherheit und Robustheit von IKT-Infrastrukturen, wurden in der Entschließung des Rates 2007/068/01 gebilligt, wenngleich sie von den Beteiligten nur unzureichend übernommen und umgesetzt werden. Mit der Strategie wird auch die Rolle – auf taktischer wie auf operativer Ebene – der Europäischen Agentur für Netz- und Informationssicherheit (ENISA) gestärkt, die 2004 geschaffen wurde, um innerhalb der Gemeinschaft zu einer hohen und wirksamen Netz- und Informationssicherheit zum Nutzen der Bürger, Verbraucher, Unternehmen und Behörden beizutragen.

Das Mandat der ENISA wurde 2008 unverändert bis März 2012 verlängert[5]. Zugleich riefen der Rat und das Europäische Parlament dazu auf, *„weitergehende Überlegungen über die Zukunft der ENISA und die allgemeine Ausrichtung der europäischen Bemühungen um eine verbesserte Netz- und Informationssicherheit anzustellen.“* Zur Unterstützung dieser Debatte führte die Kommission im November letzten Jahres eine Online-Konsultation[6] durch, deren Auswertung demnächst veröffentlicht wird.

Die in dieser Mitteilung vorgesehenen Maßnahmen erfolgen im Rahmen des und parallel zum Europäischen Programm für den Schutz kritischer Infrastrukturen (EPSKI)[7]. Ein Kernelement des EPSKI ist die Richtlinie[8] über die Ermittlung und Ausweisung europäischer kritischer Infrastrukturen[9], in der der IKT-Sektor als ein vorrangiger Sektor für die Zukunft genannt wird. Ein weiteres wichtiges Element des EPSKI ist das Warn- und Informationsnetz für kritische Infrastrukturen (CIWIN)[10].

Was die Regulierung anbelangt, enthält der Kommissionsvorschlag zur Reform des Rechtsrahmens für elektronische Kommunikationsnetze und -dienste[11] neue Bestimmungen in Bezug auf die Sicherheit und Integrität, insbesondere um höhere Anforderungen an die Betreiber zu stellen, damit den ermittelten Risiken angemessen begegnet und die fortlaufende Verfügbarkeit der Dienste gewährleistet wird sowie Sicherheitsverletzungen gemeldet werden[12]. Dieser Ansatz deckt sich mit dem allgemeinen Ziel, die Sicherheit und Robustheit der KII zu verbessern. Diese Bestimmungen werden vom Europäischen Parlament und dem Rat weitgehend unterstützt.

Mit den in dieser Mitteilung vorgeschlagenen Maßnahmen werden bestehende und künftige Maßnahmen im Bereich der polizeilichen und der justiziellen Zusammenarbeit ergänzt, durch die gegen KII gerichtete kriminelle und terroristische Aktivitäten verhütet, bekämpft und verfolgt werden sollen, wie dies u. a. der Rahmenbeschluss des Rates über Angriffe auf Informationssysteme[13] und dessen geplante Überarbeitung[14] vorsehen.

---

3 KOM(2005) 229 endg.
4 KOM(2006) 251 endg.
5 Verordnung (EG) Nr. 1007/2008.
6 http://ec.europa.eu/information_society/newsroom/cf/itemlongdetail.cfm?item_id=4464
7 KOM(2006) 786 endg.
8 2008/114/EG.
9 http://www.consilium.europa.eu/ueDocs/cms_Data/docs/pressData/en/gena/104617.pdf
10 KOM(2008) 676 endg.
11 KOM(2007) 697, KOM(2007) 698, KOM(2007) 699.
12 Artikel 13 der Rahmenrichtlinie.
13 2005/222/JHA.
14 KOM(2008) 712 endg.

Bei dieser Initiative werden Bemühungen der NATO für eine gemeinsame Politik zur Computerverteidigung berücksichtigt, insbesondere im Rahmen der „Cyber Defence Management Authority“ und des „Cooperative Cyber Defence Centre of Excellence“.

Schließlich wird auch internationalen politischen Entwicklungen angemessen Rechnung getragen, insbesondere den Grundsätzen der G8 für den Schutz kritischer Informationsinfrastrukturen[15], der Resolution der Generalversammlung der Vereinten Nationen Nr. 58/199 über die Schaffung einer globalen Kultur der Computer- und Netzsicherheit und den Schutz kritischer Informationsinfrastrukturen *(Creation of a global culture of cybersecurity and the protection of critical information infrastructures)* sowie der jüngsten Empfehlung der OECD über den Schutz kritischer Informationsinfrastrukturen.

3. WAS STEHT AUF DEM SPIEL?

3.1. Kritische Informationsinfrastrukturen sind entscheidend für das wirtschaftliche und gesellschaftliche Wachstum in der EU

In aktuellen Berichten über Innovation und Wirtschaftswachstum wird auf die Rolle hingewiesen, die der IKT-Sektor und die IKT-Infrastrukturen für Wirtschaft und Gesellschaft spielen. Zu nennen sind hier u. a. die Mitteilung zur i2010-Halbzeitüberprüfung[16], der Bericht der Aho-Gruppe[17] sowie die Jahreswirtschaftsberichte der Europäischen Union[18]. Die OECD unterstreicht die Bedeutung der IKT und des Internet, wenn es darum geht, *die Wirtschaftsleistung und den sozialen Wohlstand zu fördern und die Fähigkeit der Gesellschaft zur Verbesserung der Lebensqualität der Bürger weltweit zu stärken*[19]. Sie empfiehlt darüber hinaus Maßnahmen, die das Vertrauen in die Internet-Infrastruktur stärken sollen.

Der IKT-Sektor spielt für alle gesellschaftlichen Bereiche eine wichtige Rolle. Die Unternehmen sind sowohl im Hinblick auf ihre direkten Umsätze als auch auf die Effizienz ihrer internen Abläufe vom IKT-Sektor abhängig. Die IKT sind ein wichtiger Baustein der Innovation und für fast 40 % des Produktivitätsanstiegs verantwortlich[20]. Auch für die Arbeit von Regierungen und öffentlichen Verwaltungen sind die IKT unverzichtbar: Infolge der Einführung elektronischer Behördendienste auf allen Ebenen sowie neuer Anwendungen, beispielsweise innovativer Lösungen in den Bereichen Gesundheit, Energie und politische Mitbestimmung, ist der öffentliche Sektor stark auf die IKT angewiesen. Auch die Bürger benötigen und verwenden in ihrem Alltag zunehmend die IKT, so dass durch mehr KII-Sicherheit das Vertrauen der Bürger in die IKT gestärkt würde, nicht zuletzt dank eines besseren Schutzes der personenbezogenen Daten und der Privatsphäre.

3.2. Risiken für kritische Informationsinfrastrukturen

Die auf menschliche Einwirkung, Naturkatastrophen oder technische Pannen zurückzuführenden Risiken sind häufig noch nicht vollständig bekannt oder noch nicht hinreichend analysiert worden. Unter den Beteiligten besteht daher noch kein ausreichendes

---

15 http://www.usdoj.gov/criminal/cybercrime/g82004/G8_CIIP_Principles.pdf

16 KOM(2008) 199 endg.

17 http://ec.europa.eu/invest-in-research/action/2006_ahogroup_en.htm

18 Die Wirtschaft der EU: Bilanz 2007 http://ec.europa.eu/economy_finance/publications/publication10130_en.pdf

19 http://www.oecd.org/dataoecd/1/29/40821707.pdf

20 http://epp.eurostat.ec.europa.eu/ - Wissenschaft und Technologie/Informationsgesellschaft

Problembewusstsein, das zu wirksamen Sicherheitsmechanismen und Gegenmaßnahmen führen würde.

Cyber-Angriffe haben einen bis dato unbekannten Grad an Komplexität erreicht. Einfache Experimente haben sich inzwischen zu komplizierten Tätigkeiten entwickelt, die entweder durch Gewinnstreben oder politische Gründe motiviert sind. Die jüngsten Cyber-Großangriffe auf Estland, Litauen und Georgien sind die bekanntesten Beispiele für einen allgemeinen Trend. Die große Anzahl von Viren, Würmern und anderen Schadprogrammen, die Ausweitung so genannter Botnets und die stetige Zunahme von Spam bestätigen den Ernst der Lage[21].

Die starke Abhängigkeit von den KII, ihre grenzübergreifende Vernetzung und Verknüpfung mit anderen Infrastrukturen sowie ihre Anfälligkeit und Bedrohungen machen es umso dringender, die Sicherheit und Robustheit dieser Infrastrukturen systematisch zu verbessern und sich damit an vorderster Front gegen Ausfälle und Angriffe zu verteidigen.

3.3. Sicherheit und Robustheit kritischer Informationsinfrastrukturen für mehr Vertrauen in die Informationsgesellschaft

Um die IKT-Infrastrukturen und damit die wirtschaftlichen und gesellschaftlichen Chancen der Informationsgesellschaft in vollem Maße nutzen zu können, müssen alle Beteiligten ein hohes Maß an Vertrauen in diese Infrastrukturen setzen. Dies hängt von verschiedenen Faktoren ab, vor allem von der Gewährleistung ihrer Sicherheit und Robustheit. Zudem sind Diversität, Offenheit, Interoperabilität, Benutzerfreundlichkeit, Transparenz, Verantwortlichkeit, Überprüfbarkeit der einzelnen Komponenten sowie Wettbewerb weitere Schlüsselfaktoren, wenn es darum geht, die Sicherheit zu fördern und den Einsatz sicherheitsverbessernder Produkte, Verfahren und Dienste zu stimulieren. Dabei handelt es sich, wie von der Kommission bereits betont wurde[22], um eine gemeinsame Aufgabe: Keiner der Beteiligten kann allein die Sicherheit und Robustheit aller IKT-Infrastrukturen gewährleisten und die sich daraus ergebende Verantwortung tragen.

Die Übernahme dieser Verantwortung erfordert eine Kultur des Risikomanagements, die es ermöglicht, auf bekannte Gefahren zu reagieren und neue Bedrohungen frühzeitig zu erkennen, ohne dass es dabei zu Überreaktionen kommt und die Entstehung innovativer Dienste und Anwendungen verhindert wird.

3.4. Die Herausforderungen für Europa

Zusätzlich und ergänzend zur Umsetzung der Richtlinie über die Ermittlung und Ausweisung europäischer kritischer Infrastrukturen, insbesondere zur Bestimmung spezifischer Kriterien für den IKT-Sektor, sind eine Reihe größerer Herausforderungen anzugehen, um die Sicherheit und Robustheit der KII zu stärken.

3.4.1. Uneinheitliche und unkoordinierte nationale Strategien

Trotz der Gemeinsamkeiten bei den zu behandelnden Problemen und Aspekten gibt es in den Mitgliedstaaten Unterschiede sowohl was die Maßnahmen und Regelungen zur

---

21 KOM(2006) 688 endg.

22 KOM(2006) 251 endg.

Gewährleistung der Sicherheit und Robustheit der KII, als auch was die Fachkompetenz und Abwehrbereitschaft anbelangt.

Eine rein nationale Strategie birgt die Gefahr von Uneinheitlichkeit und Effizienzverlust in Europa. Unterschiedliche nationale Strategien und das Fehlen einer systematischen grenzübergreifenden Zusammenarbeit schränken die Wirksamkeit nationaler Gegenmaßnahmen erheblich ein, u. a. weil durch die Vernetzung der KII ein niedriges Niveau an Sicherheit und Robustheit in einem Land die Anfälligkeit und die Risiken in anderen Ländern verstärken kann.

Zur Überwindung dieser Situation bedarf es einer gesamteuropäischen Anstrengung zur Verstärkung der nationalen Strategien und Programme. Dies soll dadurch geschehen, dass ein Problembewusstsein und gemeinsames Verständnis der Herausforderungen gefördert werden, die Vereinbarung gemeinsamer politischer Ziele und Prioritäten angeregt werden, die Zusammenarbeit zwischen den Mitgliedstaaten verstärkt wird und nationale Strategien in einen stärker auf Europa und die Welt ausgerichteten Rahmen gestellt werden.

3.4.2. Notwendigkeit eines neuen europäischen ordnungspolitischen Modells für KII

Die Verbesserung der Sicherheit und Robustheit der KII ist mit besonderen ordnungspolitischen Herausforderungen verbunden. KII-Strategien werden zwar letztendlich von den Mitgliedstaaten bestimmt, ihre Umsetzung erfordert allerdings die Beteiligung des Privatsektors, der eine große Zahl von KII besitzt oder kontrolliert. Zudem bieten die Märkte dem Privatsektor nicht immer hinreichend Anreize, in den Schutz von KII in dem von staatlicher Seite normalerweise geforderten Maß zu investieren.

Zur Lösung dieses Governance-Problems wurden auf nationaler Ebene als Referenzmodell öffentlich-private Partnerschaften (ÖPP) geschaffen. Obwohl ÖPP auf europäischer Ebene als wünschenswert angesehen werden, sind bisher noch keine Partnerschaften dieser Art entstanden. Durch die Schaffung eines europäischen ordnungspolitischen Rahmens unter Mitwirkung aller Beteiligten, in dem gegebenenfalls auch der ENISA eine wichtigere Rolle zukommt, könnte der Privatsektor stärker an der Festlegung ordnungspolitischer Ziele sowie von operativen Prioritäten und Maßnahmen beteiligt werden. Ein solcher Rahmen würde die Kluft zwischen nationalen politischen Entscheidungsprozessen und der operativen Wirklichkeit überwinden.

3.4.3. Beschränkte Frühwarn- und Reaktionsfähigkeit in Europa

Ordnungspolitische Instrumente sind nur dann wirksam, wenn alle Beteiligten ihr Handeln auf zuverlässige Informationen stützen können. Dies gilt vor allem für die Regierungen, die letztlich für die Sicherheit und das Wohlergehen der Bürger verantwortlich sind.

Die Prozesse und Vorgehensweisen für die Überwachung der Netzsicherheit und die Meldung von Störungen sind in den Mitgliedstaaten jedoch sehr unterschiedlich. Manche Staaten verfügen über keine zuständige Überwachungsstelle. Noch stärker ins Gewicht fällt die unzureichende Zusammenarbeit und der mangelnde Austausch zuverlässiger und konkreter Informationen über Sicherheitsvorfälle zwischen den Mitgliedstaaten, der entweder nur informell oder aufgrund von Absprachen weniger Beteiligter erfolgt. Störungssimulationen und Übungen zur Erprobung der Reaktionsfähigkeit sind im Hinblick auf sicherere und robustere KII von strategischem Belang. Dabei sollen insbesondere flexible Strategien und Prozesse für den Umgang mit der Unvorsehbarkeit möglicher Krisen in den Mittelpunkt

gestellt werden. In der EU sind Übungen zur Computer- und Netzsicherheit noch im Anfangsstadium begriffen. Grenzübergreifende Übungen finden nur in sehr begrenztem Maße statt. Wie jüngste Ereignisse[23] belegen, ist die gegenseitige Hilfe ein ausschlaggebender Faktor, um auf Cyber-Bedrohungen und -Großangriffe angemessen reagieren zu können.

Eine ausgeprägte europäische Frühwarn- und Reaktionsfähigkeit auf Zwischenfälle erfordert gut funktionierende nationale/staatliche Computer-Notfallteams (*Computer Emergency Response Teams, CERT*), die über gemeinsame Grundfähigkeiten verfügen. Diese Stellen müssen als nationale Katalysatoren für die Belange der Beteiligten und ihre ordnungspolitische Handlungsfähigkeit agieren (einschließlich Tätigkeiten im Zusammenhang mit Informationsaustauschs- und Warnsystemen für Bürger und KMU) und auf eine wirksame grenzübergreifende Zusammenarbeit und den Austausch von Informationen hinwirken, wovon auch bestehende Organisationen wie die europäische EGC-Gruppe[24] (*European Governmental CERTs Group, EGC*) profitieren können.

3.4.4. Internationale Zusammenarbeit

Angesichts des Aufstiegs des Internet zur wesentlichen KII muss auf seine Robustheit und Stabilität besonders geachtet werden. Dank seiner verteilten, redundanten Gestaltung hat es sich als äußerst widerstandsfähige Infrastruktur bewährt. Sein außerordentliches Wachstum führte jedoch zu einer zunehmenden physischen und logischen Komplexität und zur Entstehung neuer Dienste und Anwendungsarten. Daher ist es legitim, die Fähigkeit des Internet anzuzweifeln, der zunehmenden Zahl von Störungen und Cyber-Angriffen standzuhalten.

Der Umstand, dass die Ansichten über die Kritikalität der das Internet ausmachenden Komponenten voneinander abweichen, erklärt zum Teil die unterschiedlichen Standpunkte, die von den Regierungen in internationalen Foren zum Ausdruck gebracht werden, sowie die häufig widersprüchlichen Auffassungen über den Stellenwert dieser Frage. Dadurch könnte es schwieriger werden, Bedrohungen des Internet vorzubeugen, sie abzuwehren und ihre Folgen zu bewältigen. Beispielsweise sollten die Auswirkungen des Übergangs vom IPv4 zum IPv6 auch unter dem Aspekt der KII-Sicherheit beurteilt werden.

Das Internet ist ein globales, hochgradig verteiltes Netz von Netzen, dessen Kontrollzentren sich nicht notwendigerweise nach nationalen Grenzen richten. Zur Gewährleistung seiner Robustheit und Stabilität ist daher ein gezieltes Konzept notwendig, das auf zwei einander ergänzenden Maßnahmen aufbaut. Dies ist erstens die Herstellung eines Konsenses über die Prioritäten Europas im Hinblick auf ein robustes und stabiles Internet, und zwar unter den Aspekten der Ordnungspolitik sowie des Einsatzes und des Betriebs. Zweitens ist es die Einbeziehung der Weltgemeinschaft in die Ausarbeitung einer Reihe von Grundsätzen für ein robustes und stabiles Internet, die die zentralen Werte Europas widerspiegeln, und zwar im Rahmen unseres strategischen Dialogs und der Zusammenarbeit mit Drittländern und internationalen Organisationen. Diese Maßnahmen würden auf die Anerkennung der fundamentalen Bedeutung der Stabilität des Internet durch den Weltgipfel über die Informationsgesellschaft[25] aufbauen.

---

23 http://ec.europa.eu/information_society/policy/nis/strategy/activities/ciip/large_scale/

24 http://www.egc-group.org/

25 Tunis-Agenda für die Informationsgesellschaft, http://www.itu.int/wsis/docs2/tunis/off/6rev1.html

4. MEHR KOORDINIERUNG UND ZUSAMMENARBEIT IN DER EU

In Anbetracht der gemeinschaftlichen und internationalen Dimension des Problems würden nationale Programme sowie bestehende bilaterale und multilaterale Kooperationsregelungen zwischen Mitgliedstaaten durch ein integriertes EU-Konzept für sicherere und robustere KII ergänzt und verstärkt.

Politische Grundsatzdiskussionen nach den Ereignissen in Estland lassen erkennen, dass die Auswirkungen ähnlicher Angriffe durch Verhütungsmaßnahmen und ein koordiniertes Vorgehen während der Krise begrenzt werden können. Durch einen besser strukturierten Austausch von Informationen und vorbildlichen Praktiken in der EU könnte die Bekämpfung grenzübergreifender Bedrohungen wesentlich erleichtert werden.

Es ist notwendig, die vorhandenen Kooperationsmechanismen, einschließlich der ENISA, zu stärken und erforderlichenfalls neue Instrumente zu schaffen. Unverzichtbar ist ein europäisches Konzept, das sich über verschiedene Ebenen erstreckt und sämtliche Beteiligten einbezieht, wobei die nationalen Zuständigkeiten vollständig gewahrt und ergänzt werden.

Zudem ist ein gründliches Verständnis des Umfelds und der Beschränkungen erforderlich. Problematisch ist beispielsweise die verteilte Struktur des Internet, bei der Randknoten als Angriffsvektoren, z. B. für Botnets, verwendet werden können. Die verteilte Struktur ist allerdings auch für die Gewährleistung von Stabilität und Robustheit entscheidend und kann zu einer schnelleren Folgenbewältigung beitragen, als dies normalerweise bei übermäßig formalisierten, streng hierarchischen Verfahren der Fall wäre. Deshalb müssen ordnungspolitische Maßnahmen und betriebliche Verfahren sorgfältig und fallweise analysiert werden.

Auch der Zeitrahmen spielt eine wichtige Rolle. Ohne Frage müssen sofort Maßnahmen ergriffen und die notwendigen Elemente für einen Rahmen geschaffen werden, der es ermöglicht, auf aktuelle Herausforderungen zu reagieren, und der in eine künftige Strategie für Netz- und Informationssicherheit übernommen werden kann.

Zur Bewältigung dieser Herausforderungen werden fünf Handlungsschwerpunkte vorgeschlagen:

(1) Prävention und Abwehrbereitschaft: Gewährleistung der Abwehrbereitschaft auf allen Ebenen

(2) Erkennung und Reaktion: Schaffung geeigneter Frühwarnsysteme

(3) Folgenminderung und Wiederherstellung: Stärkung der EU-Instrumente zur Verteidigung der KII

(4) Internationale Zusammenarbeit: Förderung der EU-Prioritäten auf internationaler Ebene

(5) Kriterien für den IKT-Sektor: Unterstützung der Durchführung der Richtlinie über die Ermittlung und Ausweisung europäischer kritischer Infrastrukturen[26].

[26] Richtlinie 2008/114/EG des Rates.

5. DER AKTIONSPLAN

5.1. Prävention und Abwehrbereitschaft

Gemeinsame Kapazitäten und Dienste für eine europaweite Zusammenarbeit. Die Kommission fordert die Mitgliedstaaten und Beteiligten auf,

- zur Förderung der europaweiten Zusammenarbeit gemeinsam mit der ENISA ein Mindestniveau an Kapazitäten und Diensten für nationale/staatliche CERT und Krisenbewältigungsmaßnahmen festzulegen;

- dafür zu sorgen, dass die nationalen/staatlichen CERT das Kernelement der nationalen Kapazitäten in Bezug auf Abwehrbereitschaft, Informationsaustausch, Koordinierung und Reaktion bilden.

Ziele: Vereinbarung von Mindeststandards bis Ende 2010; Schaffung gut funktionierender nationaler/staatlicher CERT in allen Mitgliedstaaten bis Ende 2011.

Europäische öffentlich-private Partnerschaft für Robustheit (EÖPPR). Die Kommission wird

- die Zusammenarbeit zwischen dem öffentlichen und dem privaten Sektor in Bezug auf Ziele für die Sicherheit und Robustheit, grundlegende Anforderungen, bewährte politische Praktiken und sonstige Maßnahmen fördern. Die EÖPPR soll vornehmlich der europäischen Dimension unter strategischen (z. B. bewährte politische Praktiken) und taktisch-operativen Aspekten (z. B. industrielle Umsetzung) gewidmet sein. Sie sollte auf bestehenden nationalen Initiativen und den operativen Tätigkeiten der ENISA aufbauen und diese ergänzen.

Ziele: Erstellung eines EÖPPR-Plans bis Ende 2009; Einrichtung der EÖPPR bis Mitte 2010; erste Ergebnisse der EÖPPR bis Ende 2010.

Europäisches Forum für den Informationsaustausch zwischen den Mitgliedstaaten. Die Kommission wird

- für die Mitgliedstaaten ein Europäisches Forum für den Austausch von Informationen und bewährten politischen Praktiken in Bezug auf die Sicherheit und Robustheit von KII einrichten. Auch die Tätigkeiten anderer Organisationen, insbesondere der ENISA, sollen darin einbezogen werden.

Ziele: Einrichtung des Forums bis Ende 2009; Lieferung erster Ergebnisse bis Ende 2010.

5.2. Erkennung und Reaktion

Europäisches Informations- und Warnsystem (EISAS). Die Kommission unterstützt

- die Entwicklung und Einführung des EISAS, das sich an Bürger und KMU richtet und auf bestehenden staatlichen und privaten Informationsaustauschs- und Warnsystemen aufbaut. Die Kommission leistet finanzielle Unterstützung für zwei ergänzende Prototyp-

Vorhaben[27]. Die ENISA soll eine Bestandsaufnahme der Ergebnisse dieser Vorhaben und anderer nationaler Initiativen vornehmen und einen Fahrplan erstellen, um die Entwicklung und Einführung des EISAS zu unterstützen.

Ziele: Abschluss der Prototyp-Vorhaben bis Ende 2010; Fahrplan zur Errichtung eines europäischen Systems bis Ende 2010.

5.3. Folgenminderung und Wiederherstellung

Nationale Notfallplanung und -übungen. Die Kommission fordert die Mitgliedstaaten dazu auf,

- nationale Notfallpläne aufzustellen und regelmäßige Übungen durchzuführen, um die Reaktionsfähigkeit auf Netzsicherheitsverletzungen großen Ausmaßes sowie das Katastrophenmanagement zu erproben und so auf eine engere europaweite Koordinierung hinzuarbeiten. Nationale/staatliche CERT/CSIRT können mit der Leitung nationaler Notfallplanungen und -übungen, an denen die Akteure des öffentlichen und des Privatsektors teilnehmen, beauftragt werden. Die ENISA wird aufgefordert, den Austausch bewährter Praktiken zwischen den Mitgliedstaaten zu unterstützen.

Ziel: Durchführung von mindestens einer nationalen Übung in jedem Mitgliedstaat bis Ende 2010.

Europaweite Erprobung der Reaktionsfähigkeit auf Netzsicherheitsverletzungen großen Ausmaßes. Die Kommission wird

- die Entwicklung europaweiter Übungen zur Internet-Sicherheit[28] finanziell fördern, was auch als operative Plattform für die Teilnahme Europas an entsprechenden internationalen Übungen zur Netzsicherheit, z. B. Cyber Storm in den USA, dienen kann.

Ziele: Ausarbeitung und Durchführung der ersten europaweiten Übung bis Ende 2010; Teilnahme Europas an internationalen Übungen bis Ende 2010.

Stärkere Zusammenarbeit zwischen nationalen/staatlichen CERT. Die Kommission fordert die Mitgliedstaaten auf,

- die Zusammenarbeit zwischen nationalen/staatlichen CERT zu stärken, u. a. durch die Förderung und Ausweitung bestehender Kooperationsmechanismen wie der EGC-Gruppe[29]. Die ENISA wird zur aktiven Mitwirkung aufgefordert, um die europaweite Zusammenarbeit zwischen den nationalen/staatlichen CERT anzuregen und im Hinblick auf eine verstärkte Abwehrbereitschaft und Reaktionsfähigkeit Europas und die Durchführung europaweiter (und/oder regionaler) Übungen zu unterstützen.

---

27 Im Rahmen des Gemeinschaftsprogramms „Prävention, Abwehrbereitschaft und Folgenbewältigung im Zusammenhang mit Terrorakten und anderen sicherheitsbezogenen Risiken“, http://ec.europa.eu/justice_home/funding/cips/funding_cips_en.htm

28 Siehe Fußnote 27.

29 Siehe Fußnote 24.

Ziele: Verdopplung der Zahl der an der EGC-Gruppe beteiligten nationalen Stellen bis Ende 2010; Erarbeitung von Referenzmaterial durch die ENISA zur Unterstützung der europaweiten Zusammenarbeit bis Ende 2010.

5.4. Internationale Zusammenarbeit

Robustheit und Stabilität des Internet. Geplant sind drei einander ergänzende Tätigkeiten:

- Europäische Prioritäten für die langfristige Robustheit und Stabilität des Internet. Die Kommission wird eine europaweite Debatte vorantreiben, in die alle öffentlichen und privaten Akteure einbezogen werden und deren Ziel es ist, die EU-Prioritäten für die langfristige Robustheit und Stabilität des Internet festzulegen.

Ziel: Festlegung der EU-Prioritäten zu kritischen Internet-Komponenten und –Aspekten bis Ende 2010.

- Grundsätze und Leitlinien für die Robustheit und Stabilität des Internet (europaweit). Die Kommission wird zusammen mit den Mitgliedstaaten Leitlinien für die Robustheit und Stabilität des Internet aufstellen und dabei u. a. folgende Schwerpunkte setzen: regionale Abhilfemaßnahmen, Vereinbarungen über gegenseitige Hilfeleistung, koordinierte Wiederherstellung der Betriebskontinuität, geografische Verbreitung kritischer Internetressourcen, technische Sicherheitsmechanismen in der Architektur des Internet und seinen Protokollen, Nachbildung und Vielfalt von Diensten und Daten. Die Kommission finanziert bereits eine *Task Force* zur Stabilität des Domänennamensystems, die zusammen mit anderen einschlägigen Projekten zur Konsensfindung beitragen wird[30].

Ziele: europäischer Fahrplan für die Erarbeitung von Grundsätzen und Leitlinien für die Robustheit und Stabilität des Internet bis Ende 2009; Vereinbarung eines ersten Entwurfs von Grundsätzen und Leitlinien bis Ende 2010.

- Grundsätze und Leitlinien für die Robustheit und Stabilität des Internet (weltweit). Die Kommission wird zusammen mit den Mitgliedstaaten einen Fahrplan zur Förderung von Grundsätzen und Leitlinien auf globaler Ebene ausarbeiten. Als Mittel zur globalen Konsensbildung wird die strategische Zusammenarbeit mit Drittstaaten gefördert, vor allem in den Dialogen zu Themen der Informationsgesellschaft[31].

Ziele: Erstellung eines Fahrplans für die internationale Zusammenarbeit bei der Aufstellung von Grundsätzen und Leitlinien für die Robustheit und Stabilität des Internet bis Anfang 2010; erster Entwurf international anerkannter Grundsätze und Leitlinien, die mit Drittstaaten und in einschlägigen Foren, einschließlich des Internet Governance Forums, diskutiert werden bis Ende 2010.

Globale Übungen zur Wiederherstellung und Folgenminderung nach Internet-Störungen großen Ausmaßes. Die Kommission fordert die Beteiligten in Europa auf,

30 Siehe Fußnote 27.
31 KOM(2008) 588 endg.

- einen praktischen Weg aufzuzeigen, wie die zur Krisenabschwächung und Folgenbewältigung durchgeführten Übungen auf der Grundlage regionaler Notfallpläne und -kapazitäten global ausgeweitet werden können.

Ziele: Kommissionsvorschlag für eine Grundlage und einen Fahrplan zur Beteiligung Europas an globalen Übungen zur Wiederherstellung und Folgenminderung nach Internet-Störungen großen Ausmaßes bis Ende 2010.

5.5. Kriterien für europäische kritische Infrastrukturen im IKT-Sektor

Besondere Kriterien für den IKT-Sektor. Aufbauend auf ihren anfänglichen Aktivitäten von 2008 wird die Kommission

- gemeinsam mit den Mitgliedstaaten und allen Beteiligten weiter an der Ausarbeitung der Kriterien zur Bestimmung der europäischen kritischen Infrastrukturen im IKT-Sektor arbeiten. Zu diesem Zweck werden einschlägige Informationen aus einer aktuellen Studie[32] herangezogen.

Ziele: Festlegung der Kriterien zur Bestimmung der europäischen kritischen Infrastrukturen im IKT-Sektor durch die Kommission im ersten Halbjahr 2010.

6. FAZIT

Die Sicherheit und Robustheit der kritischen Informationsinfrastrukturen sind entscheidende Voraussetzungen, um gegen Ausfälle und Angriffe gewappnet zu sein. Ihre Verbesserung in der gesamten EU ist ausschlaggebend für die volle Erschließung der mit der Informationsgesellschaft verbundenen Vorteile. Um dieses ehrgeizige Ziel zu erreichen, wird ein Aktionsplan vorgeschlagen, durch den die taktische und operative Zusammenarbeit auf europäischer Ebene verstärkt werden soll. Der Erfolg dieser Maßnahmen hängt davon ab, wie wirkungsvoll die Aktivitäten des öffentlichen und des Privatsektors zugrunde gelegt und genutzt werden können, sowie vom Engagement und der vollen Teilnahme der Mitgliedstaaten, der europäischen Institutionen und der Beteiligten.

Zu diesem Zweck findet am 27. und 28. April 2009 eine Ministerkonferenz statt, die das Ziel hat, die Maßnahmenvorschläge mit den Mitgliedstaaten zu erörtern und deren Engagement in der Debatte über eine modernisierte und intensivierte NIS-Politik in Europa zu bekräftigen.

Die Verbesserung der Sicherheit und Robustheit der KII ist ein langfristiges Ziel, und die dafür aufzuwendenden Strategien und Maßnahmen bedürfen einer regelmäßigen Überprüfung. Da dieses Ziel mit der allgemeinen Debatte über die Zukunft der Politik auf dem Gebiet der Netz- und Informationssicherheit in der EU nach 2012 im Einklang steht, wird die Kommission Ende 2010 eine Bestandsaufnahme einleiten, um die erste Aktionsphase einer Bewertung zu unterziehen und gegebenenfalls weitere Maßnahmen auszuarbeiten und vorzuschlagen.

[32] Siehe Fußnote 27.