EUROPÄISCHE KOMMISSION

Brüssel, den 31.3.2011
KOM(2011) 163 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

„Ergebnisse und nächste Schritte: der Weg zur globalen Netzsicherheit”

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

über den Schutz kritischer Informationsinfrastrukturen

„Ergebnisse und nächste Schritte: der Weg zur globalen Netzsicherheit"

1. EINFÜHRUNG

Die Kommission verabschiedete am 30. März 2009 eine Mitteilung über den Schutz kritischer Informationsinfrastrukturen mit dem Titel „Schutz Europas vor Cyber-Angriffen und Störungen großen Ausmaßes: Stärkung der Abwehrbereitschaft, Sicherheit und Stabilität"[1], in der ein Plan – der Aktionsplan zum Schutz kritischer Informationsinfrastrukturen (CIIP-Aktionsplan) – dargelegt wurde, mit dem die Sicherheit und Robustheit kritischer Informations- und Kommunikations(IKT)-Infrastrukturen erhöht werden soll. Ziel war die Förderung und Unterstützung einer hohen Abwehrbereitschaft, Sicherheit und Robustheit auf nationaler Ebene und europaweit. Dieses Konzept fand 2009 im Rat breite Unterstützung[2].

Der CIIP-Aktionsplan hat fünf Schwerpunkte: Prävention und Abwehrbereitschaft, Erkennung und Reaktion, Folgenminderung und Wiederherstellung, internationale Zusammenarbeit und Kriterien für europäische kritische Infrastrukturen im IKT-Bereich. Er beschreibt die von der Kommission, den Mitgliedstaaten und/oder der Industrie mit Unterstützung der Europäischen Agentur für Netz- und Informationssicherheit (ENISA) im Rahmen der einzelnen Schwerpunkte durchzuführenden Maßnahmen.

In der im Mai 2010 verabschiedeten Digitalen Agenda für Europa[3] (DAE) und den diesbezüglichen Schlussfolgerungen des Rates[4] wurde das Einvernehmen darüber hervorgehoben, dass Vertrauen und Sicherheit grundlegende Voraussetzungen für eine breite Nutzung von IKT und damit für das Erreichen der Ziele des „intelligenten Wachstums" im Rahmen der Strategie Europa 2020[5] sind. Gemäß der Digitalen Agenda müssen alle Akteure sich mit vereinten Kräften um die Sicherheit und Robustheit der IKT-Infrastrukturen bemühen, wobei der Schwerpunkt auf Prävention, Abwehrbereitschaft und Aufklärung zu legen ist, sowie um die Entwicklung wirksamer koordinierter Mechanismen, um auf neue und immer raffiniertere Formen von Cyber-Angriffen und Cyber-Kriminalität reagieren zu können. Damit werden beide Dimensionen des Problems, Prävention und Reaktion, entsprechend berücksichtigt.

---

1 KOM(2009) 149.

2 Entschließung des Rates vom 18. Dezember 2009 über ein kooperatives europäisches Vorgehen im Bereich der Netz- und Informationssicherheit (NIS) (ABl. C 321 vom 29.12.2009, S. 1).

3 KOM(2010) 245.

4 Schlussfolgerungen des Rates zur Mitteilung „Eine digitale Agenda für Europa" vom 31. Mai 2010 (10130/10).

5 KOM(2010) 2020 und Schlussfolgerungen des Europäischen Rates vom 25./26. März 2010 (EUCO 7/10).

In den vergangenen Monaten wurden die folgenden, in der Digitalen Agenda bereits angekündigten Maßnahmen ergriffen: Die Kommission verabschiedete im September 2010 einen Vorschlag für eine Richtlinie über Angriffe auf Informationssysteme[6]. Mit dieser soll die Bekämpfung der Cyber-Kriminalität durch die Angleichung der einzelstaatlichen Strafvorschriften und die Verbesserung der Zusammenarbeit zwischen den Justizbehörden und sonstigen zuständigen Behörden verstärkt werden. Außerdem werden Bestimmungen für den Umgang mit neuen Formen von Cyber-Angriffen (insbesondere Botnetzen) eingeführt. Zur Ergänzung legte die Kommission gleichzeitig einen Vorschlag[7] für ein neues Mandat der Europäischen Agentur für Netz- und Informationssicherheit (ENISA) zu deren Stärkung und Modernisierung im Hinblick auf den Ausbau des Vertrauens und der Netzsicherheit vor. Die Stärkung und Modernisierung der ENISA wird der EU, den Mitgliedstaaten und den privaten Akteuren dabei helfen, ihre Kapazitäten und Vorsorgemaßnahmen für die Prävention, Aufdeckung und Reaktion im Bereich der Internetsicherheit zu verbessern.

Nicht zuletzt zeigen die DAE, das Stockholmer Programm/der Aktionsplan[8] und die EU-Strategie der inneren Sicherheit[9] (ISS) das Engagement der Kommission für die Schaffung eines digitalen Umfelds, in dem jeder Europäer sein wirtschaftliches und soziales Potenzial voll entfalten kann.

In der Mitteilung werden die seit der Verabschiedung des CIIP-Aktionplans 2009 erreichten Ergebnisse und die für die einzelnen Maßnahmen auf europäischer und internationaler Ebene geplanten Schritte beschrieben. Ein weiterer Schwerpunkt liegt auf der globalen Dimension der Herausforderungen und auf der Bedeutung einer stärkeren Zusammenarbeit der Mitgliedstaaten und des Privatsektors auf nationaler, europäischer und internationaler Ebene, um den globalen Interdependenzen gerecht zu werden.

2. EIN SICH WEITERENTWICKELNDES SZENARIO

Die Folgenabschätzung für den CIIP-Aktionsplan[10] sowie ein breites Spektrum von Analysen und Berichten privater und öffentlicher Akteure zeigen nicht nur, inwieweit Europa in gesellschaftlicher, politischer und wirtschaftlicher Hinsicht von IKT abhängig ist, sondern auch die stetige Zunahme der – natürlichen oder vom Menschen hervorgerufenen – Gefahren in Bezug auf Anzahl, Umfang, Komplexität und potenzielle Wirkung.

In jüngster Zeit sind neue, technologisch komplexere Bedrohungen aufgetreten. Ihre globale geopolitische Bedeutung wird immer deutlicher. Es ist die Tendenz festzustellen, IKT zur Erlangung politischer, wirtschaftlicher und militärischer Macht einzusetzen, auch durch Angriffe. In diesem Zusammenhang ist zuweilen von ‘Cyberkrieg’ oder ‘Cyberterrorismus’ die Rede.

Ferner zeigte sich anlässlich der jüngsten Ereignisse im südlichen Mittelmeerraum, dass einige Regime auch bereit und in der Lage sind, aus politischen Gründen ihren eigenen Bürgern den Zugang zu elektronischen Kommunikationsmitteln – insbesondere zum Internet und zur Mobilfunkkommunikation – willkürlich zu verwehren oder diesen zu stören. Solche

---

6 KOM(2010) 517 endgültig.
7 KOM(2010) 521.
8 KOM(2010) 171.
9 KOM(2010) 673.
10 SEK(2009) 399.

einseitigen Maßnahmen eines Staates können schwerwiegende Auswirkungen für andere Teile der Welt haben[11].

Um zu einem umfassenderen Verständnis dieser unterschiedlichen Bedrohungen zu gelangen, kann man sie in folgenden Kategorien zusammenfassen:

– **kriminelle Ausnutzung,** z. B. durch „komplexe anhaltende Angriffe“ (advanced persistent threats, APT)[12] zur wirtschaftlichen oder politischen Spionage (z. B. GhostNet[13]), Identitätsdiebstahl, die jüngsten Angriffe auf das Emissionshandelssystem[14] oder Angriffe auf staatliche IT-Systeme[15];

– **Störung**, wie durch DDoS-Angriffe (Distributed Denial of Service - koordinierte Überlastungsangriffe auf Server) oder Spamming über Botnetze (z. B. das Conficker-Netz mit 7 Millionen Computern und das von Spanien ausgehende Mariposa-Netz mit 12,7 Millionen Computern[16]), Stuxnet[17] sowie das Unterbinden der Kommunikation über bestimmte Kommunikationsmittel;

– **Zerstörung**. Dieses Szenario wurde noch nicht verwirklicht, kann jedoch angesichts der immer stärkeren Durchdringung kritischer Infrastrukturen mit IKT (z. B. intelligente Netze und Wasserversorgungssysteme) in Zukunft nicht ausgeschlossen werden[18].

3. DIE EUROPÄISCHE UNION UND DER GLOBALE KONTEXT

Die zu erwartenden Herausforderungen sind weder EU-spezifisch noch können sie von der EU allein bewältigt werden. Die Allgegenwärtigkeit der IKT und des Internets ermöglicht eine effizientere, effektivere und wirtschaftlichere Kommunikation, Koordinierung und Zusammenarbeit zwischen den jeweiligen Akteuren und führt zu einem lebendigen Innovationsumfeld in allen Lebensbereichen. Gefahren können jedoch heute aufgrund der Vernetzung von jedem Teil der Welt ausgehen und jeden Teil der Welt treffen.

Ein Vorgehen Europas im Alleingang reicht nicht aus, um den neuen Herausforderungen zu begegnen. Es ist zwar nach wie vor wichtig, einen innerhalb der EU kohärenten und auf Zusammenarbeit beruhenden Ansatz zu verfolgen, dieser muss jedoch in eine Strategie der globalen Koordinierung eingebettet sein, in die wichtige Partner (einzelne Länder oder einschlägige internationale Organisationen) einbezogen werden.

---

11 Gemeinsame Mitteilung „Eine Partnerschaft mit dem südlichen Mittelmeerraum für Demokratie und gemeinsamen Wohlstand“, KOM(2011) 200 vom 8.3.2011.

12 Andauernde, koordinierte Angriffe auf Regierungsbehörden und den öffentlichen Sektor generell. Sie sind inzwischen auch ein Problem für den Privatsektor (siehe „RSA 2011 cybercrime trends report“).

13 Siehe Berichte des Projekts „Information Warfare Monitor": „Tracking GhostNet: investigating a Cyber Espionage Network” (2009) und „Shadows in the Cloud: Investigating Cyber Espionage 2.0” (2010).

14 Siehe Fragen und Antworten unter http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/11/34&format=HTML&aged=0&language=EN&guiLanguage=fr.

15 z. B. die jüngsten Angriffe auf die Systeme der französischen Regierung.

16 Siehe OECD/IFP-Projekt zu „Future Global Shocks”, Bericht „Reducing systemic cyber-security risks“, 14. Januar 2011, unter http://www.oecd.org/dataoecd/3/42/46894657.pdf.

17 Siehe http://www.enisa.europa.eu/media/press-releases/stuxnet-analysis.

18 Siehe Weltwirtschaftsforum, Global Risks 2011.

Wir müssen zu einer globalen Einschätzung der Risiken gelangen, die mit der allgemeinen und massiven Nutzung der IKT in allen Teilen der Gesellschaft verbunden sind. Außerdem müssen wir Strategien entwickeln, um diese Risiken angemessen und wirksam anzugehen (d. h. Strategien für Prävention, Bekämpfung, Eindämmung und Reaktion). Gemäß der DAE „*muss die Zusammenarbeit der einschlägigen Beteiligten auf globaler Ebene organisiert werden, um Sicherheitsbedrohungen wirksam bekämpfen und mindern zu können*“, und es wird das Ziel der „*Zusammenarbeit mit weltweiten Akteuren zur Stärkung des* ***globalen Risikomanagements*** *in der digitalen und physischen Sphäre und zur international koordinierten Durchführung gezielter Aktionen gegen Computerkriminalität und sicherheitsrelevante Angriffe*“ vorgegeben.

4. UMSETZUNG DES CIIP-AKTIONSPLANS: EINIGE ERFOLGE

Der vollständige Bericht über die Ergebnisse des CIIP-Aktionsplans und die nächsten Schritte ist im Anhang beigefügt. Nachstehend sind beispielhaft einige der bisherigen Erfolge aufgeführt.

4.1. Prävention und Abwehrbereitschaft

- Das **Europäische Forum der Mitgliedstaaten** (EFMS) hat beträchtliche Fortschritte bei der Förderung von Gesprächen und Austausch der zuständigen Behörden über bewährte Maßnahmen für die Sicherheit und Robustheit von IKT-Infrastrukturen aufzuweisen. Das EFMS wird von den Mitgliedstaaten als wichtiges Forum für solche Gespräche und den Austausch bewährter Maßnahmen anerkannt[19]. Bei seiner künftigen Tätigkeit wird es weiterhin von der ENISA unterstützt. Der Schwerpunkt der Arbeit wird auf der Zusammenarbeit zwischen nationalen/staatlichen CERT (Computer Emergency Response Teams – IT-Notfallteams), der Ermittlung finanzieller und rechtlicher Anreize für Sicherheit und Robustheit (bei Einhaltung der Vorschriften für Wettbewerb und staatliche Beihilfen), der Bewertung des Grades der Internetsicherheit in Europa, der Initiierung europaweiter Sicherheitsübungen sowie der Erörterung der Prioritäten für die internationale Zusammenarbeit in Fragen der Sicherheit und Robustheit liegen.

- Die **Europäische öffentlich-private Partnerschaft für Robustheit** (European Public-Private Partnership for Resilience/EP3R) wurde als europaweiter Governance-Rahmen für die Robustheit von IKT-Infrastrukturen ins Leben gerufen. Sie unterstützt die Zusammenarbeit zwischen dem öffentlichen und dem privaten Sektor in strategischen Fragen der EU-Politik für Cybersicherheit und Robustheit. ENISA hat die Tätigkeit der EP3R erleichtert und würde bei Annahme des Kommissionsvorschlags aus dem Jahr 2010 zur Modernisierung der ENISA einen langfristigen und dauerhaften Rahmen hierfür bieten. Die EP3R wird auch als Forum für die internationale Zusammenarbeit in Fragen von öffentlichem Interesse sowie in wirtschaftlichen und marktbezogenen Fragen im Zusammenhang mit Sicherheit und Robustheit dienen, insbesondere mit Blick auf die Stärkung des globalen Risikomanagements bei IKT-Infrastrukturen.

---

[19] In der Antwort der britischen Regierung auf den fünften Bericht des EU-Ausschusses des britischen Oberhauses über den CIIP-Aktionsplan heißt es, das EFMS sei erfolgreich und entspreche einem echten Bedarf der politisch Verantwortlichen, ihre Erfahrungen auszutauschen.

- Es wurden **Mindestkapazitäten und -dienste**[20] beschrieben sowie entsprechende **Empfehlungen**[21] für die nationalen/staatlichen CERT ausgesprochen, damit diese effektiv arbeiten und in ihrem Land die zentrale Rolle im Hinblick die Abwehrbereitschaft, den Informationsaustausch, die Koordinierungsmöglichkeiten und die Reaktionsfähigkeit übernehmen können. Diese Dokumente werden dazu beitragen, bis 2012 mit Unterstützung der ENISA ein Netz gut funktionierender nationaler/staatlicher CERT in allen Mitgliedstaaten einzurichten. Dieses wird die Stütze des Europäischen Informations- und Warnsystems (EISAS) für Bürger und KMU sein und soll mit den Ressourcen und Kapazitäten der Mitgliedstaaten bis 2013 errichtet werden.

4.2. Erkennung und Reaktion

- Die ENISA erstellte einen übergeordneten Fahrplan für die Entwicklung des **EISAS** bis 2013[22], der auf der Einführung von *Basisdiensten* auf der Ebene der nationalen/staatlichen CERT und der Schaffung von *Interoperabilitätsdiensten* für die Integration der nationalen Informations- und Warnsysteme in EISAS beruht. Der angemessene Schutz personenbezogener Daten wird in diesem Rahmen eine zentrale Komponente sein.

4.3. Folgenminderung und Wiederherstellung

- Bisher haben nur zwölf Mitgliedstaaten Übungen zur Reaktionsfähigkeit bei Netzsicherheitsverletzungen großen Ausmaßes sowie zum Katastrophenmanagement[23] durchgeführt. Die ENISA hat einen **Leitfaden für die gute Praxis bei nationalen Übungen**[24] erstellt, außerdem **Empfehlungen** für die Entwicklung nationaler Strategien[25], um die Maßnahmen der Mitgliedstaaten – die verstärkt werden sollten – zu unterstützen.

- Die erste **europaweite Erprobung der Reaktionsfähigkeit bei Netzsicherheitsverletzungen großen Ausmaßes** (Cyber Europe 2010) fand am 4. November 2010 statt. Alle Mitgliedstaaten waren einbezogen, 19 Mitgliedstaaten nahmen aktiv teil. Die Schweiz, Norwegen und Island waren ebenfalls beteiligt. Für künftige europaweite Übungen zur Internetsicherheit wäre es zweifellos von Vorteil, wenn es einen gemeinsamen Rahmen gäbe, der auf den nationalen Notfallplänen aufbaut und diese miteinander verbindet; dadurch würden grundlegende Mechanismen und Verfahren für die Kommunikation und Zusammenarbeit der Mitgliedstaaten geschaffen.

4.4. Internationale Zusammenarbeit

- Im Rahmen des EFMS wurden **EU-Grundsätze und -Leitlinien für die Robustheit und Stabilität des Internets**[26] entwickelt und erörtert. Die Kommission wird diese mit den betroffenen Akteuren erörtern und für sie werben, insbesondere im Privatsektor (über die

---

20 Siehe: http://www.enisa.europa.eu/act/cert/support/files/baseline-capabilities-for-national-governmental-certs.

21 Siehe http://www.enisa.europa.eu/act/cert/support/files/baseline-capabilities-of-national-governmental-certs-policy-recommendations.

22 http://www.enisa.europa.eu/act/cert/other-work/eisas_folder/eisas_roadmap.

23 Quelle: ENISA.

24 Siehe: http://www.enisa.europa.eu/act/res/policies/good-practices-1/exercises/national-exercise-good-practice-guide/at_download/fullReport.

25 Siehe: http://www.enisa.europa.eu/act/cert/support/files/baseline-capabilities-of-national-governmental-certs-policy-recommendations.

26 Siehe http://ec.europa.eu/information_society/policy/nis/index_en.htm.

EP3R), in bilateralen Gesprächen mit wichtigen internationalen Partnern (insbesondere den USA), und in multilateralen Foren. Im Rahmen ihrer Zuständigkeit wird die Kommission dies u. a. in folgenden Foren tun: G8, OECD, NATO (insbesondere auf der Grundlage ihres im November 2010 verabschiedeten neuen strategischen Konzepts und der Tätigkeit des Cooperative Cyber-defense Center of Excellence), ITU (im Rahmen des Kapazitätsaufbaus im Bereich der Cybersicherheit), OSCE (im Rahmen ihres Forums für Sicherheitszusammenarbeit), ASEAN, Meridian[27]. Die Grundsätze und Leitlinien sollen einen für alle geltenden Rahmen für die gemeinsamen internationalen Bemühungen im Hinblick auf die langfristige Robustheit und Stabilität des Internets bilden.

4.5. Kriterien für europäische kritische Infrastrukturen im IKT-Sektor

- Die technischen Erörterungen im Rahmen des EFMS ergaben einen **ersten Entwurf spezifischer Kriterien für den IKT-Sektor** zur Ermittlung europäischer kritischer Infrastrukturen. Der Schwerpunkt lag auf der **Festnetz- und Mobilfunkkommunikation sowie auf dem Internet**. Die technischen Diskussionen werden fortgesetzt und von den Konsultationen profitieren, die auf nationaler und europäischer (EP3R) Ebene mit dem Privatsektor über die Kriterienentwürfe geführt werden. Die Kommission wird ferner mit den Mitgliedstaaten die für den IKT-Sektor spezifischen Punkte erörtern, die 2012 im Rahmen der Überarbeitung der Richtlinie über die Ermittlung und Ausweisung europäischer kritischer Infrastrukturen und die Bewertung der Notwendigkeit, ihren Schutz zu verbessern[28] zu beachten sind.

5. DAS WEITERE VORGEHEN

Bei der Umsetzung des CIIP-Aktionsplans sind positive Ergebnisse zu verzeichnen, insbesondere im Hinblick darauf, dass anerkannt wurde, dass im Bereich der Netz- und Informationssicherheit ein auf der Zusammenarbeit aller Akteure beruhendes Konzept erforderlich ist. Sie entspricht ferner weitgehend den Meilensteinen und dem Zeitplan, die 2009 festgelegt wurden. Wir sollten uns damit jedoch nicht begnügen, denn es ist sowohl auf nationaler als auch auf europäischer Ebene noch viel zu tun.

Es ist ferner besonders wichtig, unsere Bemühungen in eine Strategie der globalen Koordinierung einzubetten und deshalb, unter Einbeziehung aller relevanten Akteure, auch auf internationaler Ebene tätig zu werden, mit anderen Regionen, Ländern und Organisationen, die mit ähnlichen Themen befasst sind, zusammenzuarbeiten und Partnerschaften aufzubauen, um so Informationen über Vorgehensweisen und Maßnahmen auszutauschen und Doppelarbeit zu vermeiden.

Wir müssen eine globale Kultur des Risikomanagements fördern. Der Schwerpunkt sollte auf der Unterstützung koordinierter Maßnahmen zur Prävention, Erkennung und Eindämmung aller natürlichen oder vom Menschen hervorgerufenen Störungen und zur entsprechenden Reaktionsbereitschaft liegen, ferner auf Maßnahmen zur Strafverfolgung der kriminellen Handlungen. Hierzu gehören auch gezielte Aktionen gegen Computerkriminalität und sicherheitsrelevante Angriffe.

---

[27] Mit dem Meridian-Prozess sollen die Regierungen weltweit ein Forum erhalten, in dem sie erörtern können, wie sie beim Schutz kritischer Informationsinfrastrukturen (CIIP) zusammenarbeiten wollen. Siehe http://meridianprocess.org/.

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

Zu diesem Zweck **wird die Kommission**

- **Grundsätze für die Robustheit und Stabilität des Internets fördern.** Internationale Grundsätze für die Robustheit und Stabilität des Internets sollten gemeinsam mit anderen Ländern, internationalen Organisationen und gegebenenfalls mit den weltweit tätigen Akteuren des Privatsektors entwickelt werden; dies sollte über bestehende Foren und Verfahren geschehen, z. B. solche, die für die Internetverwaltung (Internet Governance) existieren. Diese Grundsätze sollten ein Instrument für alle Akteure sein, das ihnen in Bezug auf die Stabilität und Robustheit des Internets einen Rahmen für ihre Tätigkeit vorgibt. Die EU-Grundsätze und -Leitlinien könnten hierfür die Grundlage sein;

- **strategische internationale Partnerschaften aufbauen**. Strategische Partnerschaften sollten auf bereits existierenden Maßnahmen in kritischen Bereichen (wie dem Management von Netzstörungen) aufbauen und Übungen sowie die Zusammenarbeit zwischen CERT einschließen. Die Beteiligung des Privatsektors, bei dem es sich um weltweit tätige Unternehmen/Organisationen handelt, ist entscheidend. Die Arbeitsgruppe EU-USA zum Thema Cybersicherheit und Cyberkriminalität, eingerichtet anlässlich des EU-USA-Gipfels im November 2010, ist ein wichtiger Schritt in diese Richtung. Der Schwerpunkt der Arbeit der Gruppe wird auf dem Management von Netzstörungen, öffentlich-privaten Partnerschaften, Sensibilisierung und Cyberkriminalität liegen. Sie kann ferner gegebenenfalls Möglichkeiten für eine Zusammenarbeit mit anderen Regionen oder Ländern, insbesondere solchen mit ähnlichen Problemen, prüfen, um Konzepte und damit verbundene Maßnahmen auszutauschen sowie Doppelarbeit zu vermeiden. In internationalen Foren, insbesondere im Rahmen der G8, sollte man sich um eine weitere Zusammenarbeit und Koordinierung bemühen. In Europa ist eine gute Koordinierung zwischen den EU-Institutionen, den zuständigen Agenturen (vor allem ENISA und Europol) und den Mitgliedstaaten entscheidend;

- **Vertrauen in das Cloud-Computing aufbauen**. Die Erörterungen über die besten Verwaltungsstrategien für neu aufkommende Technologien mit globaler Wirkung (wie Cloud-Computing) sind unbedingt zu intensivieren. Sie sollten einen angemessenen Governance-Rahmen für den Schutz personenbezogener Daten behandeln, sich jedoch nicht auf diese Frage beschränken. Um die Vorteile voll nutzen zu können, ist Vertrauen unerlässlich[29];

Da jeder seinen Teil der Verantwortung für die Sicherheit trägt, müssen alle Mitgliedstaaten sicherstellen, dass ihre nationalen Maßnahmen und Bemühungen zu einem koordinierten Vorgehen auf EU-Ebene zur Prävention, Erkennung und Eindämmung aller Arten von Netzstörungen und Cyber-Angriffen sowie zur entsprechenden Reaktionsfähigkeit beitragen. Im Hinblick darauf **sollten sich die Mitgliedstaaten verpflichten**,

- **die Abwehrbereitschaft der EU zu stärken, indem sie bis 2012 ein Netz gut funktionierender nationaler/staatlicher CERT einrichten.** Die EU-Institutionen werden für ihren Bereich bis 2012 ebenfalls ein CERT einrichten. Bei all diesen Maßnahmen sollten die von der ENISA beschriebenen Mindestkapazitäten und -dienste sowie die

[29] Siehe z. B. die Berichte der ENISA „Cloud Computing Information Assurance Framework“ (2009), unter http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-information-assurance-framework/at_download/fullReport), und „Security and resilience in governmental clouds“ (2011), unter http://www.enisa.europa.eu/act/rm/emerging-and-future-risk/deliverables/security-and-resilience-in-governmental-clouds/).

entsprechenden Empfehlungen zugrunde gelegt werden. Die ENISA wird auch in Zukunft diese Initiativen unterstützen. Hierdurch wird auch die Entwicklung eines Europäischen Informations- und Warnsystems (EISAS) für die Bürger bis 2013 vorangetrieben.

- **einen europäischen Notfallplan für Netzstörungen zu erstellen (bis 2012) und regelmäßig europaweite Übungen zur Internetsicherheit durchzuführen.** Solche Übungen sind ein wichtiger Aspekt einer kohärenten Strategie für die Notfallplanung im Hinblick auf Netzstörungen und die Wiederherstellung auf nationaler und auf europäischer Ebene. Künftige europaweite Übungen sollten auf einem europäischen Notfallplan für Netzstörungen beruhen, der seinerseits auf den nationalen Notfallplänen aufbaut und mit diesen verbunden ist. Ein solcher Notfallplan sollte die grundlegenden Mechanismen und Verfahren für die Kommunikation zwischen den Mitgliedstaaten festlegen und nicht zuletzt bei der Bestimmung des Gegenstands und der Organisation der künftigen europaweiten Übungen von Nutzen sein. Die ENISA wird zusammen mit den Mitgliedstaaten an der Entwicklung eines europäischen Notfallplans für Netzstörungen bis 2012 arbeiten. Gleichzeitig sollten alle Mitgliedstaaten regelmäßig nationale Notfallpläne erstellen und Übungen zur Reaktionsfähigkeit und Wiederherstellung durchführen.

- **den europäischen Beitrag in internationalen Foren und Diskussionen über die Stärkung der Sicherheit und Robustheit des Internets zu koordinieren.** Die Mitgliedstaaten sollten miteinander und mit der Kommission bei der Förderung eines grundsatz- oder normengestützten Konzepts für das Problem der globalen Stabilität und Robustheit des Internets zusammenarbeiten. Ziel sollte die Unterstützung der Prävention und Abwehrbereitschaft auf allen Ebenen und bei allen Akteuren sein, entgegen der derzeitigen Tendenz, die Diskussionen hauptsächlich aus der militärischen Perspektive und/oder der Perspektive der nationalen Sicherheit zu führen.

6. FAZIT

Die Erfahrung hat gezeigt, dass ein rein nationales oder regionales Vorgehen in der Frage der Netzsicherheit und -robustheit nicht ausreicht. Die europäische Zusammenarbeit hat sich seit 2009 beträchtlich und auf ermutigende Weise verbessert. Insbesondere ist auf die Übung „Cyber Europe 2010“ hinzuweisen. Europa sollte jedoch seine Anstrengungen fortsetzen, eine europaweit kohärente und kooperative Vorgehensweise zu entwickeln. Die ENISA sollte modernisiert werden und ihre Unterstützung für die Mitgliedstaaten, die EU-Institutionen und den Privatsektor bei diesen langfristigen Aufgaben ausbauen.

Die europäischen Bemühungen müssen jedoch, wenn sie von Erfolg gekrönt sein sollen, in eine koordinierte Vorgehensweise auf globaler Ebene eingebettet sein. Im Hinblick darauf wird die Kommission Diskussionen zur Internetsicherheit in allen geeigneten internationalen Foren vorantreiben.

Am 14./15. April 2011 wird der ungarische Ratsvorsitz der EU eine Ministerkonferenz zum Thema „Schutz kritischer Informationsinfrastrukturen“ organisieren. Diese wird eine wichtige Gelegenheit für die Verstärkung des Engagements für eine bessere Zusammenarbeit und Koordinierung zwischen den Mitgliedstaaten sowohl auf europäischer als auch auf internationaler Ebene bieten.

ANHANG

Der CIIP-Aktionsplan: Ergebnisse und nächste Schritte im Einzelnen

Insgesamt entsprechen die Ergebnisse der im Rahmen des CIIP-Aktionsplans durchgeführten Maßnahmen weitgehend den Meilensteinen und dem Zeitplan, die von der Kommission 2009 festgelegt wurden. Nachstehend werden für alle Schwerpunktbereiche die Ergebnisse und die nächsten Schritte ausgeführt. Bei dieser Bestandsaufnahme wird berücksichtigt, dass einige Maßnahmen in der Digitalen Agenda für Europa (DAE) und in der EU-Strategie der inneren Sicherheit (ISS) weiter präzisiert worden sind.

1. Prävention und Abwehrbereitschaft

Gemeinsame Kapazitäten und Dienste für eine europaweite Zusammenarbeit.

Ergebnisse

– 2009 legte die ENISA gemeinsam mit den europäischen CERT Mindestkapazitäten und -dienste fest, über die die nationalen/staatlichen CERT verfügen müssen, um im Interesse der europaweiten Zusammenarbeit effektiv arbeiten zu können. Man einigte sich auf eine Liste von obligatorischen Anforderungen in den Bereichen Betrieb, technische Kapazitäten, Auftrag und Zusammenarbeit[30].

– 2010 arbeitete die ENISA gemeinsam mit den europäischen CERT an Empfehlungen[31], die die genannten betriebsbezogenen Anforderungen in Empfehlungen für die nationalen/staatlichen CERT umsetzen, damit diese in ihrem Land die zentrale Rolle für die Abwehrbereitschaft, den Informationsaustausch, die Koordinierungsmöglichkeiten und die Reaktionsfähigkeit übernehmen können.

– Bisher haben 20 Mitgliedstaaten[32] nationale/staatliche CERT eingerichtet, und fast alle übrigen planen dies. Wie bereits in der DAE angekündigt und in der ISS ausgeführt, hat die Kommission Maßnahmen zur Einrichtung eines CERT für die EU-Institutionen bis 2012 vorgeschlagen.

Die nächsten Schritte

– Die ENISA wird auch in Zukunft diejenigen Mitgliedstaaten unterstützen, die noch keine den oben genannten vereinbarten Mindestanforderungen genügenden nationalen/staatlichen CERT eingerichtet haben, um sicherzustellen, dass das Ziel, in allen Mitgliedstaaten bis Ende 2011 über gut funktionierende nationale/staatliche CERT zu verfügen, erreicht wird. Wird dieser Meilenstein erreicht, ist der Weg geebnet für die Schaffung eines gut funktionierenden Netzes nationaler CERT **bis 2012**, wie es in der DAE vorgesehen ist.

---

30 Siehe: http://www.enisa.europa.eu/act/cert/support/files/baseline-capabilities-for-national-governmental-certs.

31 Siehe http://www.enisa.europa.eu/act/cert/support/files/baseline-capabilities-of-national-governmental-certs-policy-recommendations.

32 Quelle: ENISA.

– Die ENISA wird mit den nationalen/staatlichen CERT erörtern, ob und gegebenenfalls wie die Mindestkapazitäten zu erweitern sind, damit die CERT die Mitgliedstaaten bei der Sicherung der Robustheit und Stabilität kritischer IKT-Infrastrukturen besser unterstützen und die Grundlage des Europäischen Informations- und Warnsystems (EISAS) für Bürger und KMU bilden können, das mit den Ressourcen und Kapazitäten der Mitgliedstaaten wie in der ISS angekündigt **bis 2013** errichtet werden soll.

Europäische öffentlich-private Partnerschaft für Robustheit (EP3R)

Ergebnisse

– 2009 wurde die EP3R als europaweiter Governance-Rahmen für die Robustheit von IKT-Infrastrukturen ins Leben gerufen. Sie unterstützt die Zusammenarbeit zwischen dem öffentlichen und dem privaten Sektor bei den Zielen für Sicherheit und Robustheit, den Mindestanforderungen und bewährten Maßnahmen. Wie in der ISS ausgeführt, wird die EP3R auch „*mit Partnern aus Drittländern zusammenarbeiten, um das globale Risikomanagement bei IT-Netzen zu verstärken.*“ Die ENISA hat die Tätigkeit der EP3R erleichtert.

– Öffentliche und private Akteure wurden konsultiert, um Ziele, Grundsätze und Aufbau der EP3R festzulegen und Anreize für eine aktive Beteiligung der betroffenen Akteure zu finden[33]. In dem Vorschlag zur Modernisierung der ENISA wurden vorrangige Bereiche für die EP3R genannt[34].

– Parallel zur Festlegung der Struktur der EP3R wurden Ende 2010 drei Arbeitsgruppen zu folgenden Themen eingerichtet: a) wesentliche Komponenten, Ressourcen und Funktionen für eine fortlaufende und sichere Bereitstellung grenzübergreifender elektronischer Kommunikationsdienste; b) Mindestanforderungen für die Sicherheit und Robustheit der elektronischen Kommunikation; c) Koordinierungs- und Kooperationsbedarf und -mechanismen zur Vorbereitung auf Störungen der elektronischen Kommunikation in großem Ausmaß und die Reaktion darauf.

– Der Vorschlag der Kommission zur Modernisierung der ENISA aus dem Jahr 2010 enthält einen langfristigen und dauerhaften Rahmen für die EP3R. Darin wird vorgeschlagen, dass die ENISA „*die Zusammenarbeit zwischen öffentlichen und privaten Akteuren auf Unionsebene [unterstützt], indem sie u. a. den Informationsaustausch und die Sensibilisierung fördert und Hilfestellung bei deren Bemühungen um die Entwicklung und Einführung von Normen für das Risikomanagement und die Sicherheit in Bezug auf elektronische Produkte, Netze und Dienste leistet.*“

Die nächsten Schritte

– 2011 wird die EP3R die Zusammenarbeit zwischen Akteuren des öffentlichen und des privaten Sektors weiter ausbauen, um Sicherheit und Robustheit durch innovative Maßnahmen und Instrumente zu verbessern und die Verantwortlichkeiten der Akteure festzulegen. Unter Rückgriff auf die Hilfe der ENISA werden die EP3R-Arbeitsgruppen erste Ergebnisse vorlegen. Gegenstand künftiger Arbeiten werden auch Probleme der

[33] Siehe http://ec.europa.eu/information_society/policy/nis/strategy/activities/ciip/impl_activities/index_en.htm.

[34] KOM(2010) 521.

Cybersicherheit intelligenter Netze sein; Grundlage hierfür sind derzeit laufende Vorarbeiten der Kommission und der ENISA.

– Die EP3R wird als Forum für die internationale Zusammenarbeit in Fragen des öffentlichen Interesses, in wirtschaftlichen und in marktbezogenen Fragen im Zusammenhang mit Sicherheit und Robustheit dienen. Die Kommission will sich bei der Tätigkeit der Arbeitsgruppe EU-USA zum Thema Cybersicherheit und Cyberkriminalität auf die EP3R stützen, um ein kohärentes Umfeld für die Zusammenarbeit zwischen dem öffentlichen und dem privaten Sektor zu schaffen, wobei gleichzeitig das Wettbewerbsrecht und die Vorschriften für staatliche Beihilfen beachtet werden.

– Langfristig ist entsprechend dem Vorschlag für eine neue ENISA-Verordnung vorgesehen, dass die EP3R einer der zentralen Tätigkeitsbereiche der modernisierten ENISA werden soll.

Europäisches Forum der Mitgliedstaaten (EFMS)

Ergebnisse

– 2009 wurde das EFMS zur Förderung von Gesprächen und Austausch über bewährte Praktiken zwischen den zuständigen Behörden mit dem Ziel eingerichtet, gemeinsame politische Ziele und Prioritäten hinsichtlich der Sicherheit und Robustheit von IKT-Infrastrukturen zu vereinbaren und dabei unmittelbar von der Arbeit und Unterstützung der ENISA zu profitieren; Das EFMS, das vierteljährlich zusammentritt, wird seit Mitte 2010 durch ein eigenes, von der ENISA verwaltetes Internetportal unterstützt.

– Das EFMS hat in folgenden Bereichen beträchtliche Fortschritte aufzuweisen: a) Festlegung von Kriterien zur Ermittlung europäischer IKT-Infrastrukturen im Rahmen der Richtlinie über die Ermittlung und Ausweisung europäischer kritischer Infrastrukturen[35]; b) Festlegung europäischer Prioritäten, Grundsätze und Leitlinien für die Robustheit und Stabilität des Internets; c) Austausch bewährter Maßnahmen, insbesondere in Bezug auf Übungen zur Internetsicherheit.

– Das EFMS wird von den Mitgliedstaaten als wichtiges Forum für solche Gespräche und den Austausch bewährter Maßnahmen anerkannt[36].

Die nächsten Schritte

– 2011 wird das EFMS die technischen Erörterungen zu den Kriterien für europäische kritische IKT-Infrastrukturen abschließen und langfristige Leitlinien und Prioritäten für europaweite Übungen in großem Maßstab zur Netz- und Informationssicherheit liefern.

– Das EFMS wird außerdem an der Erörterung der Prioritäten für die internationale Zusammenarbeit in Fragen der Sicherheit und Robustheit beteiligt sein, insbesondere im Zusammenhang mit der Tätigkeit der Arbeitsgruppe EU-USA zum Thema Cybersicherheit und Cyberkriminalität.

---

35 Richtlinie 2008/114/EG des Rates.

36 In der Antwort der britischen Regierung auf den fünften Bericht des EU-Ausschusses des britischen Oberhauses über den CIIP-Aktionsplan heißt es, das EFMS sei erfolgreich und entspreche einem echten Bedarf der politisch Verantwortlichen, ihre Erfahrungen auszutauschen.

– Vorrangige Bereiche der künftigen EFMS-Tätigkeit, bei der auf die unmittelbare Unterstützung der ENISA zurückgegriffen werden kann, sind u. a[37].: Entwicklung von Methoden für eine wirksame Zusammenarbeit zwischen den nationalen/staatlichen CERT; Nutzung von Mindestanforderungen bei der öffentlichen Auftragsvergabe zur Erhöhung der Internetsicherheit; Ermittlung finanzieller und rechtlicher Anreize für Sicherheit und Robustheit (bei Einhaltung der Vorschriften für Wettbewerb und staatliche Beihilfen); Bewertung des Grades der Cybersicherheit in Europa.

2. Erkennung und Reaktion

Europäisches Informations- und Warnsystem (EISAS)

Ergebnisse

– Die Kommission finanzierte zwei Prototypprojekte (FISHAS und NEISAS), für die die Ergebnisse demnächst vorliegen werden.

– Auf der Grundlage ihres Berichts über die Durchführbarkeit (2007)[38] und der Analyse der relevanten Projekte auf nationaler und europäischer Ebene erstellte die ENISA einen übergeordneten Fahrplan für die Entwicklung des EISAS bis 2013[39].

Die nächsten Schritte

– 2011 wird die ENISA die Mitgliedstaaten bei der Umsetzung des EISAS-Fahrplans unterstützen, indem sie „Basisdienste“ entwickelt, die die Mitgliedstaaten für die Einrichtung ihrer nationalen Informations- und Warnsysteme (ISAS) auf der Grundlage der Kompetenzen ihrer nationalen/staatlichen CERT benötigen.

– 2012 wird die ENISA „Interoperabilitätsdienste“ entwickeln, die es ermöglichen, die ISAS funktional in das EISAS zu integrieren. Die ENISA wird ferner die Mitgliedstaaten bei der Prüfung dieser Dienste im Rahmen einer schrittweisen Integration der nationalen Systeme unterstützen.

– Während des Zeitraums 2011-2012 wird die ENISA die nationalen/staatlichen CERT auffordern, die ISAS in ihre Dienste aufzunehmen.

3. Folgenminderung und Wiederherstellung

Nationale Notfallplanung und -übungen

Ergebnisse

– Ende 2010 hatten zwölf Mitgliedstaaten einen nationalen Notfallplan erstellt und/oder Übungen zur Reaktionsfähigkeit bei Netzsicherheitsverletzungen großen Ausmaßes sowie zum Katastrophenmanagement durchgeführt[40].

---

37 KOM(2010) 251.

38 Siehe http://www.enisa.europa.eu/act/cert/other-work/files/EISAS_finalreport.pdf.

39 http://www.enisa.europa.eu/act/cert/other-work/eisas_folder/eisas_roadmap.

40 Siehe: http://www.enisa.europa.eu/act/res/policies/good-practices-1/exercises/national-exercise-good-practice-guide/at_download/fullReport.

– Auf der Grundlage der Erfahrungen in den Mitgliedstaaten und auf internationaler Ebene entwickelte die ENISA einen Leitfaden für die gute Praxis bei nationalen Übungen[41]. Sie organisierte Veranstaltungen mit den Mitgliedstaaten und außereuropäischen CERT zu nationalen Übungen. In jüngster Zeit veröffentlichte sie ferner Empfehlungen für die Entwicklung nationaler Strategien, bei denen die nationalen/staatlichen CERT/CSIRT eine zentrale Rolle als Leiter der nationalen Notfallplanung und der entsprechenden Tests – unter Einbeziehung der Akteure aus dem öffentlichen und dem privaten Sektor – übernehmen[42].

Die nächsten Schritte

– Die ENISA wird auch in Zukunft die Mitgliedstaaten dabei unterstützen, nationale Notfallpläne aufzustellen und regelmäßige Übungen durchzuführen, um die Reaktionsfähigkeit bei Netzsicherheitsverletzungen großen Ausmaßes sowie das Katastrophenmanagement zu erproben, und so auf eine engere europaweite Koordinierung hinarbeiten.

Europaweite Erprobung der Reaktionsfähigkeit bei Netzsicherheitsverletzungen großen Ausmaßes

Ergebnisse

– Die erste europaweite Erprobung der Reaktionsfähigkeit bei Netzsicherheitsverletzungen großen Ausmaßes (*Cyber Europe 2010*) fand am 4. November 2010 statt. Alle Mitgliedstaaten waren einbezogen, 19 Mitgliedstaaten nahmen aktiv teil. Die Schweiz, Norwegen und Island waren ebenfalls beteiligt. Die Übung wurde von der ENISA organisiert und evaluiert[43], die aktive Hilfe von einem Planungsteam aus acht Mitgliedstaaten erhielt und von der Gemeinsamen Forschungsstelle (JRC) technisch unterstützt wurde.

Die nächsten Schritte

– 2011 werden die Mitgliedstaaten Ziel und Gegenstand der nächsten europaweiten Übung zur Internetsicherheit, die für 2012 geplant ist, erörtern. Die Option eines schrittweisen Vorgehens, bei dem eingehendere Prüfungen vorgenommen werden, eine kleinere Gruppe von Mitgliedstaaten beteiligt ist und gegebenenfalls nicht-europäische Akteure teilnehmen könnten, wird in Erwägung gezogen. Die ENISA wird diesen Prozess weiter unterstützen.

– Die Kommission unterstützt das EuroCybex-Projekt finanziell, in dessen Rahmen im zweiten Halbjahr 2011 eine Simulationsübung durchgeführt wird.

– Übungen zur Internetsicherheit sind ein wichtiger Teil einer kohärenten Strategie für die Notfallplanung im Hinblick auf Netzstörungen auf nationaler und auf europäischer Ebene. Daher sollten künftige europaweite Übungen auf einem europäischen Notfallplan für Netzstörungen beruhen, der seinerseits auf den nationalen Notfallplänen aufbaut und mit

41 Siehe: http://www.enisa.europa.eu/act/res/policies/good-practices-1/exercises/national-exercise-good-practice-guide/at_download/fullReport.

42 Siehe: http://www.enisa.europa.eu/act/cert/support/files/baseline-capabilities-of-national-governmental-certs-policy-recommendations.

43 Siehe http://www.enisa.europa.eu/.

diesen verbunden ist. Ein solcher Notfallplan sollte die grundlegenden Mechanismen und Verfahren für die Kommunikation zwischen den Mitgliedstaaten festlegen und nicht zuletzt bei der Bestimmung des Gegenstands und der Organisation der künftigen europaweiten Übungen von Nutzen sein. Die ENISA wird zusammen mit den Mitgliedstaaten an der Entwicklung eines europäischen Notfallplans für Netzstörungen bis 2012 arbeiten. Gleichzeitig sollten alle Mitgliedstaaten regelmäßig nationale Notfallpläne erstellen und Übungen zu Reaktionsfähigkeit und Wiederherstellung entwickeln. Die hierfür notwendige Koordinierung übernimmt das EFMS.

Stärkere Zusammenarbeit zwischen nationalen/staatlichen CERT

Ergebnisse

– Die Zusammenarbeit zwischen nationalen/staatlichen CERT wurde verstärkt. Die Arbeiten der ENISA zu Mindestkapazitäten für die nationalen/staatlichen CERT, CERT-Übungen und nationalen Übungen sowie zum Management von Netzstörungen haben zu einer intensiveren europaweiten Zusammenarbeit zwischen nationalen/staatlichen CERT beigetragen und diese unterstützt.

Die nächsten Schritte

– Die ENISA wird die Zusammenarbeit zwischen nationalen/staatlichen CERT auch in Zukunft unterstützen. In diesem Zusammenhang wird sie 2011 eine Analyse der Anforderungen durchführen und Ratschläge im Hinblick auf einen geeigneten, sicheren Kommunikationskanal zu den CERT formulieren (einschließlich Fahrplan für die Umsetzung und künftige Entwicklung). Die ENISA wird auch die operativen Unterschiede auf europäischer Ebene analysieren und einen Bericht über die Möglichkeiten des Ausbaus der grenzüberschreitenden Zusammenarbeit zwischen CERT und relevanten Akteuren vorlegen, insbesondere im Hinblick auf die Koordinierung der Reaktionen auf Netzsicherheitsverletzungen.

– In der DAE werden die Mitgliedstaaten aufgefordert, **bis 2012** ein gut funktionierendes Netz nationaler/staatlicher CERT einzurichten.

4. Internationale Zusammenarbeit

Robustheit und Stabilität des Internets

Ergebnisse

– Auf der Grundlage der Arbeiten des EFMS wurden EU-Grundsätze und -Leitlinien für die Robustheit und Stabilität des Internets[44] entwickelt.

Die nächsten Schritte

– Die Kommission wird 2011 die Grundsätze im Rahmen der bilateralen Zusammenarbeit mit internationalen Partnern, insbesondere den USA, und in multilateralen Gesprächen im Rahmen der Foren G8, OECD, Meridian und ITU erörtern; mit relevanten Akteuren, insbesondere des Privatsektors, auf europäischer Ebene (über die EP3R) und weltweit

[44] Siehe http://ec.europa.eu/information_society/policy/nis/index_en.htm.

(über das Internet Governance Forum und andere geeignete Foren) Konsultationen durchführen; Diskussionen mit wichtigen Akteuren/Organisationen des Internets unterstützen.

– 2012 werden die internationalen Partner aufgefordert, die Grundsätze und Leitlinien als gemeinsamen Rahmen für die internationalen Bemühungen um die langfristige Robustheit und Stabilität des Internets festzulegen.

Weltweite Übungen zur Wiederherstellung und Folgenminderung nach Internetstörungen großen Ausmaßes

Ergebnisse

– Sieben Mitgliedstaaten[45] nahmen als ausländische Partner an der US-amerikanischen Sicherheitsübung „Cyber Storm III" teil. Die Kommission und die ENISA nahmen als Beobachter teil.

Die nächsten Schritte

– 2011 wird die Kommission gemeinsam mit den USA im Rahmen der Arbeitsgruppe EU-USA zum Thema Cybersicherheit und Cyberkriminalität ein gemeinsames Programm und einen Fahrplan für gemeinsame/abgestimmte transkontinentale Übungen zur Internetsicherheit in den Jahren 2012/2013 entwickeln. Ferner werden Optionen für die Zusammenarbeit mit anderen Regionen oder Ländern erwogen, die mit ähnlichen Themen befasst sind, um Konzepte und damit verbundene Maßnahmen auszutauschen.

5. Kriterien für europäische kritische Infrastrukturen im IKT-Sektor

Spezifische Kriterien für den IKT-Sektor zur Ermittlung europäischer kritischer Infrastrukturen

Ergebnisse

– Bei den technischen Diskussionen über sektorspezifische Kriterien für IKT im Rahmen des EFMS wurden Kriterienentwürfe für Festnetz- und Mobilfunkkommunikation sowie für das Internet erstellt.

Die nächsten Schritte

– Das EFMS wird die technischen Diskussionen über sektorspezifische Kriterien für IKT mit dem Ziel fortsetzen, ihre Formulierung bis Ende 2011 abzuschließen. Gleichzeitig planen einige Mitgliedstaaten und die EU (über die EP3R) Konsultationen mit dem Privatsektor zu den Kriterienentwürfen für den IKT-Sektor.

– Die Kommission wird die für den IKT-Sektor spezifischen Aspekte, die 2012 bei der Überarbeitung der Richtlinie 2008/114/EG über die Ermittlung und Ausweisung europäischer kritischer Infrastrukturen zu beachten sein werden, mit den Mitgliedstaaten erörtern.

[45] FR, DE, HU, IT, NL, SE und UK.