KOMMISSION DER EUROPÄISCHEN GEMEINSCHAFTEN

Brüssel, 30.3.2009
SEK(2009) 400

ARBEITSPAPIER DER KOMMISSIONSDIENSTSTELLEN

Begleitdokument zur

MITTEILUNG DER KOMMISSION AN DAS EUROPÄISCHE PARLAMENT, DEN RAT, DEN 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“

ZUSAMMENFASSUNG DER FOLGENABSCHÄTZUNG

{KOM(2009) 149}
{SEK(2009) 399}

ZUSAMMENFASSUNG DER FOLGENABSCHÄTZUNG

1. PROBLEMSTELLUNG

Der IKT-Sektor ist entscheidend für Wirtschaft und Gesellschaft in der EU

Die Informations- und Kommunikationstechnologien (IKT) haben sich zum Rückgrat der EU-Wirtschaft und der Gesellschaft insgesamt entwickelt. **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**. Auch für die **Arbeit von Regierungen und Verwaltungen sind die IKT immer unabdingbarer geworden**: Die Einführung elektronischer Behördendienste auf allen Ebenen führt zwar zu effizienteren Abläufen, gleichzeitig aber auch zu einer starken Abhängigkeit des öffentlichen Sektors von den IKT bei zahlreichen seiner Tätigkeiten. Auch die **Bürger stützen sich zunehmend auf Dienste der Informationsgesellschaft und verwenden in ihrem Alltag die IKT**. Neben den schädlichen Auswirkungen, die Computer- und Netzstörungen auf diese Aktivitäten hätten, ist auch zu berücksichtigen, dass personenbezogene Daten der Bürger in zunehmendem Maße elektronisch mitgeteilt und übertragen werden. Unzureichende Sicherheitsmaßnahmen könnten zum Verlust vertraulicher Informationen führen und die Gefahr des Identitätsdiebstahls oder anderer Betrugsformen in sich bergen[1]. **Deshalb ist die Verbesserung der Sicherheit und Robustheit dieser Infrastrukturen auch für den Schutz der personenbezogenen Daten der Bürger und die Durchsetzung des Rechts auf Privatsphäre entscheidend.**

IKT-Systeme und -Dienste stellen als solche bereits eine wichtige Infrastruktur dar und bilden zudem die Grundlage für andere kritische technische und gesellschaftliche Infrastrukturen. Darauf wurde bereits im Grünbuch der Kommission über ein Europäisches Programm für den Schutz kritischer Infrastrukturen hingewiesen, das unter dem Begriff **kritische Informationsinfrastrukturen (KII)** alle IKT-Systeme zusammenfasst, *die als solche kritische Infrastrukturen darstellen oder von wesentlicher Bedeutung für den Betrieb kritischer Infrastrukturen sind (Telekommunikation, Computer/Software, Internet, Satelliten usw.)*[2], was auch mit dem Ansatz der OECD[3] vergleichbar ist.

Ungeachtet der terminologischen Unterschiede **kommt es darauf an, dass das Konzept der KII zu einer systematischen Politik für einen sicheren und kontinuierlichen Betrieb der IKT-Systeme, -Dienste, -Netze und -Infrastrukturen** (kurz: IKT-Infrastrukturen) führt, von denen das **Internet** aufgrund seiner Verbreitung und der technologischen Konvergenz **ein äußerst wichtiger Teil ist**.

---

1 http://www.timesonline.co.uk/tol/news/uk/crime/article4211711.ece
2 KOM(2005) 576 endg.
3 Vgl. http://www.oecd.org/dataoecd/1/13/40825404.pdf

Was steht auf dem Spiel?

Die Verbreitung der KII hat zur Folge, dass Computer- und Netzstörungen **sich auf weite Bereiche der Gesellschaft auswirken können**.

Die auf menschliche Einwirkung, Naturkatastrophen oder technische Pannen zurückzuführenden Risiken sind häufig noch nicht vollständig verstanden oder analysiert worden. Unter den Beteiligten besteht daher noch kein ausreichendes Problembewusstsein, das zu angemessenen Sicherheitsmechanismen und Gegenmaßnahmen führen würde.

Cyber-Angriffe haben einen bis dato unbekannten Grad an Komplexität erreicht und sind häufig das Werk einzelner Personen oder krimineller Gruppierungen und durch Gewinnstreben oder politische Gründe motiviert. **Die jüngsten Cyber-Großangriffe auf Estland, Litauen und Georgien sind Beispiele für einen allgemeinen Trend.** Die große Anzahl von Viren, Würmern und anderen Schadprogrammen, die Ausweitung so genannter Botnets und die Zunahme von Spam bestätigen den Ernst der Lage[4]. **Die IKT-Infrastrukturen sind ständiger Bedrohung ausgesetzt** und die Folgen von Angriffen sind weitaus ernster, wenn Europa keine entsprechenden Vorkehrungen trifft.

Die starke Abhängigkeit von den KII, ihre grenzübergreifende Vernetzung und Verknüpfung mit anderen Infrastrukturen machen es erforderlich, **die Sicherheit und Robustheit dieser Infrastrukturen systematisch zu verbessern und sich damit an vorderster Front gegen Ausfälle und Angriffe zu verteidigen**, zusätzlich und ergänzend zu den Maßnahmen, durch die gegen KII gerichtete kriminelle und terroristische Aktivitäten verhütet, bekämpft und verfolgt werden sollen.

Die Problematik

Die Sicherheit und Robustheit von KII werden derzeit **kaum gesamteuropäisch koordiniert und überwiegend auf nationaler Ebene behandelt**. **Das Fehlen einer systematischen grenzübergreifenden Zusammenarbeit schränkt die Wirksamkeit nationaler Gegenmaßnahmen erheblich ein.** Zudem können durch **ein niedriges Niveau an Sicherheit und Robustheit der KII in einem Land die Anfälligkeit und die Risiken in anderen Ländern verstärkt werden**.

Angesichts des globalen Charakters der KII, ihrer engen Vernetzung mit und wechselseitigen Abhängigkeit von anderen Infrastrukturen ist es unmöglich, ihre Sicherheit und Stabilität **durch rein einzelstaatliche und unkoordinierte Strategien zu gewährleisten**. Zudem besteht die **allgemeine Ansicht, dass der Markt nicht genügend Anreize für den Privatsektor bietet, in den Schutz von KII in dem von staatlicher Seite normalerweise geforderten Maß zu investieren**.

Die Ursachen dieses generellen Problems sind:

- **uneinheitliches ordnungspolitisches Vorgehen der Mitgliedstaaten im Bereich der Sicherheit und Robustheit von KII**. Die von den Mitgliedstaaten verfolgten Strategien zur Gewährleistung der Sicherheit und Robustheit von KII sind unterschiedlich. Zudem gibt es offensichtlich Unterschiede in der Fachkompetenz und Abwehrbereitschaft, wie dies bereits in der von der Kommission durchgeführten Untersuchung nationaler Strategien festgestellt und in einem Bericht der **Europäischen Agentur für Netz- und Informationssicherheit (ENISA)** bestätigt wurde[5];

[4] KOM(2006) 688 endg.

[5] http://www.enisa.europa.eu/doc/pdf/resilience/stock_taking_final_report_2008.pdf

- **schwierige Übernahme neuer europaweiter Verwaltungsmodelle**. Die Verbesserung der Sicherheit und Zuverlässigkeit der KII ist mit besonderen **ordnungspolitischen Herausforderungen** verbunden. KII-Strategien werden zwar von den **Regierungen bestimmt, für ihre Umsetzung ist jedoch die Beteiligung des Privatsektors unverzichtbar**. Auf nationaler Ebene wurden als Referenzmodell **öffentlich-private Partnerschaften** (ÖPP) geschaffen, um diese Kombination von Verantwortlichkeiten zu bewältigen. Obwohl ÖPP auf europäischer Ebene generell als wünschenswert angesehen werden, sind bisher noch keine Partnerschaften dieser Art entstanden;
- **beschränkte Frühwarn- und Reaktionsfähigkeit in Europa**. Konsultationen haben gezeigt, dass die nationalen Frühwarn- und Krisenbewältigungssysteme sich voneinander unterscheiden. Einige Mitgliedstaaten erhalten keine regelmäßigen Berichte über Netzsicherheitsverletzungen (obwohl einige Betreiber dies durchaus auf informeller Basis praktizieren) und/oder haben keine entsprechende Meldestelle eingerichtet. Die Zusammenarbeit und der Informationsaustausch zwischen **Regierungsstellen** erscheint **unzureichend** und wird durch das Fehlen zuverlässiger Mechanismen hierfür erschwert. Deshalb wiederum **müssen sämtliche nationalen/staatlichen Computer-Notfallteams** (*Computer Emergency Response Teams, CERT*) **gut funktionieren, d. h. über gemeinsame Grundfähigkeiten verfügen**. Zudem sind **Übungen und praktische Simulationen auf EU-Ebene** als entscheidende Voraussetzungen für die Verbesserung der Sicherheit und Robustheit von KII noch im **Anfangsstadium** begriffen;
- **geringes Bewusstsein über die Gefährdungen für die Sicherheit und Robustheit des Internet.** Dank seiner verteilten, redundanten Gestaltung hat sich das Internet als **recht robuste und widerstandsfähige Infrastruktur** erwiesen. Angesichts seines **außerordentlichen Wachstums**, seiner **zunehmenden Komplexität** und der **Entstehung neuer Dienste** ist es jedoch legitim, seine Fähigkeit **anzuzweifeln**, der **zunehmenden Zahl** von Störungen und Cyber-Angriffen weiterhin standzuhalten.

Kein Land ist eine Insel. Die globale Verbreitung der KII, insbesondere des Internet, erfordert ein **gemeinsames globales Konzept** für die Gewährleistung ihrer Sicherheit und Robustheit. **Durch eine intensive Koordinierung auf EU-Ebene lassen sich international unmittelbare Erfolge erzielen.**

2. GRÜNDE FÜR EU-MAßNAHMEN

Für die Bewältigung der aufgezeigten Probleme ist ein rein nationaler Ansatz möglicherweise nicht ausreichend. Zahlreiche Bedrohungen für die Netz- und Informationssicherheit (NIS) können sich grenzübergreifend auswirken und zu Beeinträchtigungen führen, denen auf nationaler Ebene nicht wirksam begegnet werden kann und die in anderen Ländern Störungen verursachen können.

Ein integriertes EU-Konzept für sicherere und robustere KII würde die nationalen Programme zum Schutz kritischer Informationsinfrastrukturen sowie bestehende Kooperationsregelungen zwischen Mitgliedstaaten **sinnvoll ergänzen und verstärken**. Viele Herausforderungen und Fragen sind gleicher Natur und ein gemeinsames Konzept würde allen zugute kommen.

Diskussionen nach den Angriffen in Estland lassen erkennen, dass die Auswirkungen vergleichbarer Angriffe durch **Verhütungsmaßnahmen** – beispielsweise einen besser strukturierten Informationsaustausch auf europäischer Ebene – und ein **koordiniertes Vorgehen** während der Krise begrenzt werden können. Unter Beachtung des **Subsidiaritätsprinzips** ist die Kommission besonders geeignet, diese Anstrengungen in enger

Zusammenarbeit mit den Mitgliedstaaten und anderen internationalen Organisationen zu koordinieren.

Zudem können nationale Sicherheitsbedenken, die bei der Gestaltung von NIS-Maßnahmen und -Anforderungen eine wichtige Rolle spielen, zu einer Fragmentierung in der Regulierung führen und die Wettbewerbsfähigkeit der Europäischen Union insgesamt sowie die wohlstandsbildende Kraft des europäischen Binnenmarkts beeinträchtigen.

Die Kommission bekundete 2006 ihre Absicht[6], im Rahmen des Europäischen Programms für den Schutz kritischer Infrastrukturen[7] (EPSKI) eine auf den IKT-Sektor zugeschnittene Politik *„im Hinblick auf die Erhöhung der Sicherheit und der Widerstandsfähigkeit von Netzen und Informationssystemen“* zu entwickeln. Diese Ankündigung wurde vom Europäischen Rat 2007 begrüßt[8].

Diese Initiative würde auch internationalen Entwicklungen Rechnung tragen und auf anerkannten Grundsätzen aufbauen wie denen der G8 für den Schutz kritischer Informationsinfrastrukturen, 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 von KII.

Nicht zuletzt werden ohne Doppelarbeit auch die Bemühungen der NATO für Computer- und Netzsicherheit berücksichtigt, deren Schwerpunkt die militärische Verteidigung ist. Im Einzelnen handelt es sich dabei um eine gemeinsame Politik zur Computerverteidigung sowie um die Tätigkeiten der „Cyber Defence Management Authority“ (CDMA) und die Ergebnisse des „Cooperative Cyber Defence Centre of Excellence“ (CCD-COE).

3. WAS SIND DIE ZIELE?

Ziel dieses Vorschlags ist es, in Europa **die Abwehrbereitschaft und Reaktionsfähigkeit in Bezug auf die beschriebenen Risiken und Bedrohungen zu verbessern** und dabei ein uneinheitliches Vorgehen der Mitgliedstaaten zu vermeiden. Der Schwerpunkt wird dabei auf die Festlegung gemeinsamer Prozesse gelegt, um auf bekannte und unbekannte Bedrohungen flexibel reagieren zu können. Die Beteiligten des öffentlichen und des privaten Sektors würden verpflichtet, für die Einführung **geeigneter und einheitlicher Vorbeugungs-, Erkennungs-, Notfall- und Wiederherstellungsmaßnahmen** zu sorgen, um eine **angemessene Sicherheit und Robustheit der KII und die Kontinuität der Dienste** zu gewährleisten. Mehr Sicherheit und Robustheit würden sich auch **auf den Schutz der personenbezogenen Daten und der Privatsphäre der EU-Bürger positiv auswirken**.

Das übergeordnete Ziel dieses Vorschlags, nämlich **an vorderster Front für die Sicherheit und Robustheit der KII zu sorgen**, lässt sich durch vier spezifische Ziele erreichen:

(1) Überbrückung von Unterschieden in den nationalen Strategien für die Sicherheit und Robustheit von KII

(2) Besseres Regieren in Europa im Hinblick auf sicherere und robustere KII

(3) Stärkung der operativen Reaktionsfähigkeit Europas

---

6 KOM(2006) 251 endg.
7 KOM(2006) 786 endg.
8 Entschließung des Rates 2007/C 68/01.

(4) Verbesserung der Sicherheit und Robustheit des Internet.

4. WELCHE HANDLUNGSMÖGLICHKEITEN GIBT ES?

Option 1: Fortsetzung der heutigen Politik

Das Unterlassen weiterer Maßnahmenvorschläge ist keine praktikable Option. Ohne horizontale Maßnahmen auf EU-Ebene würden die Mitgliedstaaten weiterhin einzeln oder aufgrund von Absprachen unter wenigen Beteiligten handeln. Dies birgt die **Gefahr, dass unterschiedliche, miteinander inkompatible nationale Strategien entstehen**. Darüber hinaus käme es nur fallweise zu einer grenzübergreifenden Zusammenarbeit, die angesichts der Komplexität und des Ausmaßes von Cyber-Angriffen unter Umständen erfolglos bliebe.

Da die Mitgliedstaaten diese Fragen weiterhin unterschiedlich schnell angingen, würden die Beteiligten **eventuell darauf verzichten, in die Sicherheit und Robustheit zu investieren**, und angesichts der Vielzahl an Normen und Anforderungen an Wettbewerbsfähigkeit einbüßen. Da es sich um ein grenzübergreifendes Problem handelt, würden sich die Unterschiede in der Sicherheit, Robustheit und Abwehrbereitschaft in Europa noch stärker bemerkbar machen. Die Anfälligkeit der KII in Europa wäre weiterhin groß und könnte trotz individueller Anstrengungen noch zunehmen.

Option 2: Unverbindlicher Rechtsrahmen

Die Kommission würde in Form einer Mitteilung und eines Aktionsplans den **Rahmen für Koordinierung und Zusammenarbeit schaffen**, in den die Mitgliedstaaten, der Privatsektor und die Zivilgesellschaft einbezogen würden. Die Mitteilung könnte vom Rat gebilligt werden, und auch das Europäische Parlament könnte beschließen, sich an der Diskussion zu beteiligen.

Die Initiative würde auf die vorgenannten Ziele ausgerichtet sein und im Einzelnen folgende Vorschläge enthalten:

(1) **Förderung kohärenter nationaler Strategien für die Sicherheit und Robustheit von KII** durch

- die Ermittlung übertragbarer Beispiele für ordnungspolitische Praktiken und Gemeinsamkeiten;
- die Schaffung eines Europäischen Forums für die Mitgliedstaaten für den Austausch von Informationen und bewährten politischen Praktiken bezüglich der Sicherheit und Robustheit von KII.

(2) **Besseres Regieren in Europa im Hinblick auf sicherere und robustere KII** durch

- die Schaffung einer **Europäischen öffentlich-privaten Partnerschaft für Robustheit (EÖPPR)**, um die Zusammenarbeit zwischen dem öffentlichen und dem privaten Sektor in Bezug auf Zielsetzungen für Sicherheit und Robustheit, grundlegende Anforderungen, bewährte politische Praktiken und sonstige Maßnahmen zu fördern.

(3) **Stärkung der operativen Reaktionsfähigkeit Europas** durch

- die Einrichtung gut funktionierender nationaler/staatlicher CERT[9] als Kernelemente der nationalen Kapazitäten in Bezug auf Abwehrbereitschaft, Informationsaustausch, Koordinierung und Reaktion;
- die Vereinbarung eines Mindestniveaus an Kapazitäten und Diensten der nationalen/staatlichen CERT;
- Förderung der Zusammenarbeit zwischen den nationalen/staatlichen CERT, Erleichterung von Austausch und Kooperation zwischen nationalen Reaktionskapazitäten, europaweite und/oder regionale Simulationen von Störungen großes Ausmaßes und Durchführung entsprechender Übungen;
- Förderung von Notfallplänen für die Reaktion auf Netzsicherheitsverletzungen und für Wiederherstellungsmaßnahmen;
- Finanzierung der Organisation europäischer Simulationsübungen zu Netzsicherheitsverletzungen großen Ausmaßes;
- Förderung der Entwicklung und Einführung eines Europäischen Informations- und Warnsystems (EISAS), das sich gleichermaßen effektiv an Bürger und KMU richtet.

(4) **Verbesserung der Sicherheit und Robustheit des Internet** durch

- die Festlegung von EU-Prioritäten für die langfristige Stabilität und Robustheit des Internet;
- die Vereinbarung einer Reihe von zunächst europäischen und später internationalen Grundsätzen für die Sicherheit und Robustheit des Internet.

Option 3: Verbindlicher Rechtsrahmen

Die meisten der vorgenannten Themen würden durch eine Reihe verbindlicher Maßnahmen geregelt werden, gegebenenfalls in Form einer Richtlinie, einer Verordnung oder einer Entscheidung.

Die Kommission kann verbindliche Maßnahmen vorschlagen, um

(1) **eine Grundlage zur Harmonisierung nationaler Strategien festzulegen**. Diese Maßnahmen können auch auf zusätzliche Sicherheit und Robustheit von KII außerhalb des Rahmens der bereits vorgeschlagenen Marktvorschriften abzielen;

(2) **die Rolle und die Verantwortlichkeiten der öffentlichen und privaten Akteure** im Hinblick auf die Sicherheit und Robustheit von KII **zu bestimmen**;

(3) **die operative Abwehrbereitschaft zu verbessern**, z. B. durch

(a) Mindeststandards für ein einheitliches Funktions- und Diensteniveau der nationalen/staatlichen CERT;

(b) eine Grundlage für nationale Notfallpläne im Hinblick auf die Schaffung eines europaweiten Notfallplans.

5. WIE STELLEN SICH DIE OPTIONEN IM VERGLEICH DAR?

Die Option „Fortsetzung der heutigen Politik“ **verfügt über kein klares Potenzial** zur Verbesserung der Sicherheit und Robustheit der KII in Europa. Somit muss zwischen einem

[9] Computer-Notfallteams (*Computer Emergency Response Teams*).

unverbindlichen und einem verbindlichen Rechtsrahmen entschieden werden. Derzeit scheint ein „verbindlicher Rechtsrahmen“ kein gangbarer Weg zu sein, u. a. aus folgenden Gründen:

- die Existenz souveräner Staaten als **politische Realität**, die im Rahmen einer gemeinschaftlichen NIS-Politik stets zu berücksichtigen ist;
- die zu berücksichtigende weit zerstreute operationelle Zuständigkeit des Privatsektors;
- mangelnde Erfahrungen im Informationsaustausch und der Zusammenarbeit zwischen dem öffentlichen und dem privaten Sektor auf dem Gebiet der KII.

Zudem steht die **geringe Qualität der** verfügbaren **Daten** über Sicherheitsstörungen – bedingt durch Informationsasymmetrien und nationale Sicherheitsbedenken – der Festlegung wirtschaftlich und ordnungspolitisch kohärenter Regulierungsmaßnahmen sowie der **Einhaltung des Grundsatzes der Verhältnismäßigkeit im Wege**, da unmöglich angemessene Maßnahmen vorgeschlagen werden können, wenn kein hinlängliches Verständnis über das genaue Ausmaß des Problems besteht.

Schließlich ist ein verbindlicher Rechtsrahmen aufgrund der langwierigen Annahmeverfahren zu zeitaufwändig, was dem Erfordernis eines raschen Handelns aller Beteiligten zuwiderläuft.

Zusammenfassend lässt sich aus der Folgenabschätzung ableiten, dass die Option 2 kurz- bis mittelfristig vorzuziehen ist, wobei die vorgeschlagenen Maßnahmen umgehend eingeleitet und die Ergebnisse, einschließlich der sich aus der Debatte über eine intensivierte und modernisierte NIS-Politik in Europa ergebenden Ergebnisse, zu gegebener Zeit geprüft werden. Diese würden anschließend als Grundlage dienen, um die Notwendigkeit und die Möglichkeiten etwaiger künftiger Vorschriften zu beurteilen.

Es könnten dann mit der Option 3 vergleichbare Maßnahmen vorgeschlagen werden.