KOMMISSION DER EUROPÄISCHEN GEMEINSCHAFTEN

Brüssel, den 31.5.2006
KOM(2006) 251 endgültig

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

Eine Strategie für eine sichere Informationsgesellschaft – „Dialog, Partnerschaft und Delegation der Verantwortung“

{SEK(2006) 656}

INHALTSVERZEICHNIS

1. Einleitung 3

2. Verbesserung der Sicherheit der Informationsgesellschaft: Die zentralen Herausforderungen 4

3. Der Weg zu einem dynamischen Ansatz für eine sichere Informationsgesellschaft ... 7

3.1. Dialog 8

3.2. Partnerschaft 9

3.3. Delegation der Verantwortung 10

4. Schlussfolgerungen 11

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

Eine Strategie für eine sichere Informationsgesellschaft – „Dialog, Partnerschaft und Delegation der Verantwortung“

1. EINLEITUNG

Die Mitteilung „i2010 - Eine europäische Informationsgesellschaft für Wachstum und Beschäftigung“[1] hat die Bedeutung von Netz- und Informationssicherheit für die Schaffung eines einheitlichen europäischen Informationsraums hervorgehoben. Verfügbarkeit, Zuverlässigkeit und Sicherheit von Netzen und Informationssystemen werden immer wichtiger für unsere Wirtschaft und Gesellschaft.

Die vorliegende Mitteilung hat zum Ziel, die Strategie der Europäischen Kommission, die im Jahre 2001 in der Mitteilung „Sicherheit der Netze und Informationen: Vorschlag für einen europäischen Politikansatz“[2] definiert wurde, neu zu beleben. Sie überprüft die gegenwärtigen Bedrohungen der Sicherheit der Informationsgesellschaft und legt dar, welche zusätzlichen Schritte unternommen werden sollten, um die Netz- und Informationssicherheit (NIS) zu verbessern.

Im Vordergrund steht dabei die Weiterentwicklung einer dynamischen, globalen Strategie in Europa auf der Grundlage von **Dialog, Partnerschaft und Delegation der Verantwortung**, die sich auf eine Sicherheitskultur sowie auf die Erfahrungen in den Mitgliedstaaten und auf Ebene der Europäischen Gemeinschaft stützt.

Zur Bewältigung der Herausforderungen an die Sicherheit der Informationsgesellschaft hat die Europäische Gemeinschaft einen dreifachen Ansatz entwickelt, der spezielle Maßnahmen für die Netz- und Informationssicherheit, den Rechtsrahmen für die elektronische Kommunikation (einschließlich Privatsphäre und Datenschutzfragen) und die Bekämpfung der Internet-Kriminalität umfasst. Obwohl diese drei Aspekte bis zu einem gewissen Grad getrennt voneinander ausgearbeitet werden können, erfordern die zahlreichen gegenseitigen Abhängigkeiten eine aufeinander abgestimmte Strategie. In dieser Mitteilung wird die Strategie erläutert und der Rahmen geliefert, um den in sich schlüssigen Ansatz bezüglich der NIS fortzusetzen und zu erweitern.

Die Mitteilung aus dem Jahre 2001 definiert NIS als „*die Fähigkeit eines Netzes oder Informationssystems, mit einem vorgegebenen Niveau Störungen oder böswillige Aktionen abzuwehren, die die Verfügbarkeit, Authentizität, Integrität und Vertraulichkeit von gespeicherten oder übermittelten Daten und damit zusammenhängenden Diensten, die über dieses Netz oder Informationssystem angeboten werden bzw. zugänglich sind, beeinträchtigen*“. In den letzten Jahren hat die Europäische Gemeinschaft mehrere Maßnahmen zur Verbesserung der NIS ergriffen.

---

[1] KOM(2005) 229 vom 1.6.2005.

[2] KOM(2001) 298 vom 6.6.2001.

Der Rechtsrahmen für die elektronische Kommunikation, dessen Überprüfung derzeit stattfindet, beinhaltet Bestimmungen zur Sicherheit. Insbesondere enthält die Richtlinie über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation)[3] eine Verpflichtung für Anbieter öffentlich verfügbarer elektronischer Kommunikationsdienste, ihre Dienste abzusichern. Vorkehrungen gegen Spam[4] und Spyware[5] sind darin ebenfalls enthalten.

Vertrauen und Sicherheit spielen auch in den Programmen der Europäischen Gemeinschaft, die der Forschung und Entwicklung gewidmet sind, eine wichtige Rolle. Das 6. Forschungsrahmenprogramm befasst sich mit diesen Fragen in einer Vielzahl von Projekten. Sicherheitsbezogene Forschung wird im 7. Rahmenprogramm mit der Einrichtung eines Europäischen Sicherheitsforschungsprogramms (ESRP)[6] weiter gestärkt. Außerdem unterstützt das Programm „Mehr Sicherheit im Internet" die Vernetzung von Projekten und den Austausch bewährter Vorgehensweisen zur Bekämpfung schädlicher Inhalte, die in Netzen verbreitet werden.

Als einen Teil ihrer Antwort auf die Bedrohungslage beschloss die Europäische Gemeinschaft im Jahre 2004 die Errichtung der Europäischen Agentur für Netz- und Informationssicherheit (ENISA). Die ENISA trägt zur Entwicklung einer Kultur der Netz- und Informationssicherheit zugunsten von Bürgern, Verbrauchern, Unternehmen und der öffentlichen Verwaltung überall in der europäischen Union (EU) bei.

Die EU spielt auch in den internationalen Foren, die sich mit diesen Themen befassen, eine aktive Rolle, wie zum Beispiel in der OECD, im Europarat oder in den Vereinten Nationen. Auf dem Weltgipfel über die Informationsgesellschaft in Tunis hat sich die EU aktiv in die Diskussionen über Verfügbarkeit, Zuverlässigkeit und Netz- und Informationssicherheit eingebracht. Die Tunis-Agenda[7], die zusammen mit der Verpflichtung von Tunis die weiteren Schritte für den politischen Meinungsaustausch zur globalen Informationsgesellschaft liefert und von den Weltpolitikern unterstützt wird, spricht sich dafür aus, Internet-Kriminalität und Spam unter Wahrung der Privatsphäre und der Meinungsfreiheit weiterhin zu bekämpfen. Sie betont die Notwendigkeit eines gemeinsamen Verständnisses in Fragen der Internet-Sicherheit und der weiteren guten Zusammenarbeit. Ziel hierbei ist, das Sammeln und Verbreiten sicherheitsbezogener Informationen sowie den Austausch bewährter Vorgehensweisen zur Bekämpfung von Sicherheitsbedrohungen zu erleichtern.

2. VERBESSERUNG DER SICHERHEIT DER INFORMATIONSGESELLSCHAFT: DIE ZENTRALEN HERAUSFORDERUNGEN

Trotz der Bemühungen auf internationaler, europäischer und nationaler Ebene stellt die Sicherheit weiterhin eine Herausforderung dar.

---

3 Richtlinie 2002/58/EG.

4 oder unerbetene Werbenachrichten.

5 Spyware ist eine Software zum Aufspüren und Verfolgen von Benutzern, die ohne angemessene Mitteilung, Zustimmung oder Kontrolle des Benutzers eingesetzt wird.

6 Das ESPR ist im Zuge der vorbereitenden Aktion für die Sicherheitsforschung im Zeitraum 2004-2006 vorbereitet worden.

7 „Auf dem Wege zu einer globalen Partnerschaft in der Informationsgesellschaft - Folgemaßnahmen nach der Tunis-Phase des Weltgipfels über die Informationsgesellschaft (WSIS)" – KOM(2006) 181 vom 27.4.2006.

Erstens sind Angriffe auf Informationssysteme zunehmend durch Gewinnstreben motiviert und weniger durch den Wunsch, Störungen um ihrer selbst willen hervorzurufen. Gezielte Datensuche findet zunehmend ohne das Wissen der Benutzer statt, während die Anzahl (und Entwicklungsgeschwindigkeit) der Varianten von Schadprogrammen schnell wächst. Spam ist ein gutes Beispiel für diese Entwicklung: Spam dient zunehmend als Transportmittel für Viren sowie betrügerische und kriminelle Handlungen wie zum Beispiel Spyware, Phishing[8] oder andere Formen von Schadprogrammen[9]. Seine weite Verbreitung beruht zunehmend auf Botnets[10], d. h. kompromittierten Servern und PCs, die ohne Kenntnis ihrer Eigentümer als Schaltstelle genutzt werden.

Der zunehmende Einsatz mobiler Geräte (einschließlich Mobiltelefone der dritten Generation, tragbare Videospiele usw.) und von Mobiltelefon-Netzdiensten führt aufgrund der schnellen Entwicklung IP-gestützter Dienste zu neuen Herausforderungen. Diese könnten möglicherweise bald Angriffe mittels PC in den Hintergrund drängen, da letztere schon über ein gewisses Sicherheitsniveau verfügen. Tatsächlich eröffnen alle neuen Arten von Kommunikationsplattformen und Informationssystemen unvermeidlich neue Gelegenheiten für böswillige Angriffe.

Eine andere wichtige Entwicklung ist das Aufkommen intelligenter Umgebungen, wo intelligente Endgeräte mit Hilfe von Rechner- und Netztechnik allgegenwärtig sein werden (z. B. durch Funketiketten - RFID[11], IPv6 und Sensor-Netze). Ein vernetztes Alltagsleben bietet enorme Möglichkeiten. Jedoch entstehen dadurch auch zusätzliche Risiken für Sicherheit und Privatsphäre. Weit verbreitete Plattformen und Anwendungen tragen zwar einerseits zur Interoperabilität und Inanspruchnahme von Informations- und Kommunikationstechnologien (IKT) bei, erhöhen aber andererseits auch die Risiken. Je stärker z. B. Standardprogramme zum Einsatz kommen, desto mehr wirken sich ausgenutzte Schwachstellen und aufgetretene Fehlfunktionen aus. Die Zunahme von „Monokulturen“ bei Plattformen und Anwendungen begünstigt die Zunahme und Ausbreitung von Sicherheitsbedrohungen wie z. B. Schadprogrammen und Viren. **Verschiedenartigkeit, Offenheit und Interoperabilität sind integrale Bestandteile der Sicherheit und sollten entsprechend gefördert werden.**

Die Bedeutung der IKT-Branche für die europäische Wirtschaft und die europäische Gesellschaft als Ganzes ist unbestreitbar. Die IKT sind ein wichtiger Baustein der Innovation und für fast 40 % des Produktivitätswachstums verantwortlich. Außerdem entfallen auf diese hoch innovative Branche mehr als ein Viertel der gesamten europäischen Forschungs- und Entwicklungstätigkeiten, und sie spielt eine Schlüsselrolle beim Wirtschaftswachstum und bei der Schaffung von Arbeitsplätzen in allen Wirtschaftszweigen. Immer mehr Europäer leben in einer wesentlich auf Informationen gestützten Gesellschaft, in der sich die Nutzung der IKT schnell zu einem zentralen Element des menschlichen Miteinanders und des Gesellschafts- und Wirtschaftslebens entwickelt. Laut Eurostat nutzten im Jahre 2004 89 % der EU-Unternehmen und etwa 50 % der Verbraucher das Internet[12].

---

8 Phishing ist eine Form des Internetbetrugs, der darauf abzielt, wertvolle Informationen wie zum Beispiel Kreditkartennummern, Bankkontonummern, Benutzerkennungen und Passworte zu stehlen.

9 Schadprogramme werden auch als „bösartige Software“ bezeichnet.

10 Botnets sind Netze von *Bots* (kleinen automatischen Programmen), die als auf einer Opfermaschine installierte getarnte Anwendungen Aktionen im Auftrag eines Fernsteuernden ausführen.

11 Radio Frequency Identification.

12 Eurostat, *Internet-Aktivitäten in der Europäischen Union*, 40/2005.

Lücken in der Netz- und Informationssicherheit können Auswirkungen haben, die weit über den wirtschaftlichen Schaden hinausreichen. Tatsächlich herrscht allgemeine Besorgnis, dass Sicherheitsprobleme die Nutzer entmutigen und von der Inanspruchnahme der IKT abhalten könnten. Deshalb gelten Verfügbarkeit, Zuverlässigkeit und Sicherheit als Voraussetzung dafür, dass die Grundrechte auch online gewahrt bleiben.

Außerdem hängen andere entscheidende Infrastrukturen (wie Verkehr, Energie usw.) wegen ihrer stärkeren Vernetzung immer mehr von der Unversehrtheit ihrer jeweiligen Informationssysteme ab.

Sowohl Wirtschaftsunternehmen als auch Bürger in Europa unterschätzen immer noch die Risiken. Hierfür gibt es verschiedene Gründe, aber für Unternehmen scheint am wichtigsten zu sein, dass sich Investitionen in Sicherheit kaum rechnen, während sich Privatpersonen ihrer Verantwortung in der weltweiten „Sicherheitskette“ nicht bewusst sind.

Tatsächlich stellt die Netz- und Informationssicherheit, angesichts der Allgegenwärtigkeit von IKT und Informationssystemen, eine Herausforderung für alle dar:

- **Öffentliche Verwaltungen** sollten sich um die Sicherheit ihrer Systeme kümmern, und zwar nicht nur um die Informationen des öffentlichen Sektors zu schützen, sondern auch um mit gutem Beispiel für andere voranzugehen.

- **Unternehmen** sollten Netz- und Informationssicherheit eher als Wirtschaftsgut und Wettbewerbsvorteil ansehen denn als „negativen Kostenfaktor“.

- **Privatpersonen** sollten verstehen, dass ihre Heimsysteme ein wichtiges Glied in der gesamten „Sicherheitskette“ darstellen.

Um die oben beschriebenen Probleme erfolgreich zu bewältigen, brauchen alle Beteiligten zuverlässige Daten über Sicherheitsvorfälle und zukünftige Entwicklungsrichtungen. Jedoch sind zuverlässige und umfassende Daten über solche Vorfälle aus vielen Gründen schwierig zu erhalten. Dabei reichen die Gründe von der Geschwindigkeit, mit der sich Sicherheitsvorfälle ereignen können, bis hin zur Abneigung einiger Organisationen, ihre Sicherheitslücken offen zu legen und zu veröffentlichen. Trotzdem ist ein **besseres Problemverständnis** ein Eckpfeiler der Entwicklung einer Sicherheitskultur.

Sensibilisierungsprogramme, die Sicherheitsbedrohungen bewusst machen sollen, dürfen nicht das Vertrauen von Verbrauchern und Nutzern untergraben, indem sie nur auf die negativen Gesichtspunkte abstellen. Deshalb sollte die **Netz- und Informationssicherheit wo immer möglich als Vorteil und Chance** anstatt als Haftungs- und Kostenfaktor dargestellt werden. Sie muss als Wert zur Schaffung von Vertrauen und Verbraucherzuversicht, als Wettbewerbsvorteil für Unternehmen, die Informationssysteme betreiben, und als Merkmal der Qualität von Dienstleistern des öffentlichen und des privaten Sektors angesehen werden.

Wichtigste Herausforderung für die Entscheidungsträger ist es, einen ganzheitlichen Ansatz zu verfolgen. Dieser Ansatz muss den verschiedenen Beteiligten und ihren Rollen Rechnung tragen. Er muss eine sachgerechte Koordinierung der öffentlichen Politik und der ordnungspolitischen Bestimmungen sicherstellen, die entweder direkt oder indirekt die Netz- und Informationssicherheit beeinflussen. Liberalisierung, Deregulierung und Konvergenz haben zu einer Vielzahl an Mitspielern in den verschiedenen Interessengruppen geführt, was diese Aufgabe nicht leichter gestaltet. Die ENISA kann in diesem Zusammenhang einen

wichtigen Beitrag liefern. Die Agentur könnte als Zentralstelle für den Informationsaustausch, die Zusammenarbeit zwischen allen Beteiligten und den Austausch bewährter Vorgehensweisen sowohl in Europa als auch mit der restlichen Welt fungieren, um zur Wettbewerbsfähigkeit unserer IKT-Unternehmen und zu einem funktionsfähigen Binnenmarkt beizutragen.

3. DER WEG ZU EINEM DYNAMISCHEN ANSATZ FÜR EINE SICHERE INFORMATIONSGESELLSCHAFT

Eine sichere Informationsgesellschaft muss auf einer erhöhten **Netz- und Informationssicherheit (NIS)** und einer weit verbreiteten **Sicherheitskultur** aufbauen. Dazu schlägt die Europäische Kommission einen **dynamischen und integrierten Ansatz** vor, der alle Beteiligten einbezieht und auf **Dialog, Partnerschaft und Delegation der Verantwortung** setzt. Angesichts der sich gegenseitig ergänzenden Rollen des öffentlichen und privaten Sektors bei der Entwicklung einer Sicherheitskultur müssen sich einschlägige politische Initiativen auf **offene und umfassende Gespräche mit allen Beteiligten** stützen.

Dieser Ansatz und seine zugehörigen Maßnahmen werden den Plan der Kommission ergänzen und bereichern, die Entwicklung eines umfassenden und dynamischen politischen Rahmens im Jahre 2006 mittels mehrerer Initiativen weiter zu führen:

(1) Befassung mit Spam und Bedrohungen wie Spyware und anderen Formen von Schadprogrammen in einer besonderen Mitteilung.

(2) Vorschläge zur Verbesserung der Zusammenarbeit zwischen den Strafverfolgungsbehörden und zur Bekämpfung neuer Formen krimineller Aktivitäten, die das Internet ausnutzen und den Betrieb kritischer Infrastrukturen untergraben. Dies wird der Gegenstand einer besonderen Mitteilung über Internet-Kriminalität sein.

Diese politischen Initiativen ergänzen ebenfalls die Aktivitäten, die zur Erreichung der Ziele des Grünbuchs der Kommission über ein europäisches Programm für den Schutz kritischer Infrastrukturen[13] geplant sind und die als Reaktion auf eine Anfrage des Rates im Dezember 2004 entwickelt wurden. Das Grünbuch-Verfahren wird voraussichtlich zu einem Aktionsplan führen, der einen übergreifenden Gesamtrahmen zum Schutz kritischer Infrastrukturen mit den erforderlichen branchenbezogenen Strategien – einschließlich einer Strategie für die IKT-Branche – verbindet. Im Rahmen dieser speziellen IKT-Strategie würden auf der Grundlage von **Gesprächen mit allen Beteiligten** die entsprechenden volks- und betriebswirtschaftlichen sowie gesellschaftlichen Antriebskräfte im Hinblick auf die Erhöhung der Sicherheit und der Widerstandsfähigkeit von Netzen und Informationssystemen untersucht.

Darüber hinaus wird die Überprüfung des Rechtsrahmens für die elektronische Kommunikation im Jahre 2006 auch Elemente zur Verbesserung von NIS beinhalten, wie zum Beispiel technische und organisatorische Maßnahmen der Diensteanbieter, Bestimmungen zur Bekanntgabe von Sicherheitslücken sowie besondere Rechtsmittel und Strafmaßnahmen bei Pflichtverstößen.

---

[13] KOM(2005) 576 vom 17.11.2005.

Es obliegt größtenteils der privaten Wirtschaft, den Endnutzern Lösungen, Dienste und Sicherheitsprodukte zu liefern. Es ist deshalb von strategischer Bedeutung, dass die **europäische Industrie sowohl ein anspruchsvoller Nutzer** von Sicherheitsprodukten und -diensten **als auch ein wettbewerbsfähiger Lieferant** von NIS-Produkten und -Diensten ist.

Die nationalen Regierungen müssen in der Lage sein, bewährte Verfahren der Entscheidungsfindung zu erkennen und anzuwenden. Ebenso müssen sie sich erkennbar mit diesen politischen Zielen verbinden, indem sie ihre eigenen Informationssysteme auf eine sichere Art und Weise handhaben. Die Behörden in den Mitgliedstaaten und auf EU-Ebene spielen eine Schlüsselrolle bei der Unterrichtung der Nutzer dahingehend, dass diese zur eigenen Sicherheit beitragen können. Vorrang haben sollten die Schärfung des Bewusstseins für Fragen der NIS und die Bereitstellung von Sicherheitsportalen mit angemessenen und rechtzeitigen Informationen über Bedrohungen, Risiken und Warnungen ebenso wie zu bewährten Vorgehensweisen. Daher könnte es ein Hauptziel der ENISA sein zu untersuchen, ob sich ein **mehrsprachiges, europäisches Informationsaustauschs- und Warnsystem** aufbauen lässt, welches bestehende oder geplante private oder öffentliche nationale Initiativen berücksichtigt und diese miteinander verknüpft.

Die weltweite Dimension der Netz- und Informationssicherheit bildet eine Herausforderung für die Kommission, auf internationaler Ebene und in Abstimmung mit den Mitgliedstaaten ihre Bemühungen zu verstärken, eine **weltweite Zusammenarbeit in Fragen der NIS** - insbesondere bei der Umsetzung der auf dem Weltgipfel über die Informationsgesellschaft im November 2005 angenommenen Agenda - **zu fördern**.

Forschung und Entwicklung vor allem auf EU-Ebene tragen zum Aufbau neuer und innovativer Partnerschaften mit dem Ziel bei, das Wachstum der europäischen IKT-Industrie im Allgemeinen sowie der europäischen IKT-Sicherheitsindustrie im Besonderen anzukurbeln. Die Kommission wird sich deshalb im 7. EU-Rahmenprogramm um Finanzmittel in angemessener Höhe für die Forschung über NIS und Techniken zur Erhöhung der Zuverlässigkeit bemühen.

3.1. Dialog

3.1.1. Zur Verbesserung der Abstimmung zwischen den Behörden schlägt die Kommission zunächst eine **vergleichende Bewertung der nationalen, mit der NIS in Zusammenhang stehenden Strategien** einschließlich bestimmter Sicherheitspolitiken für den öffentlichen Sektor vor. Dies dürfte zur Ermittlung der wirksamsten Verfahren beitragen, die dann - wo immer dies möglich ist - verbreitet überall in der EU eingesetzt werden können, so dass die öffentliche Verwaltung bei bewährten Verfahren auf dem Gebiet der Sicherheit zum Vorreiter wird. Die Arbeiten zur elektronischen Identifizierung, etwa als Teil des neuen Aktionsplan für elektronische Behördendienste (E-Government), könnten dabei eine wichtige Rolle spielen.

Bei entsprechender Aufgliederung lassen sich aus den Ergebnissen einer solchen vergleichenden Bewertung **bewährte Verfahren** herauslesen, **mit denen sich das Problembewusstsein kleiner und mittlerer Unternehmen (KMU) sowie der Bürger schärfen** und deren Fähigkeit verbessern lässt, die für sie geltenden Herausforderungen und Anforderungen auf dem Gebiet der NIS anzupacken. Die ENISA sollte in diesen Gesprächen sowie bei der Zusammenführung und dem Austausch bewährter Verfahren eine aktive Rolle übernehmen.

3.1.2. Es ist ein **strukturierter Meinungsaustausch zwischen allen Beteiligten** darüber nötig, wie sich die bestehenden Werkzeuge und ordnungspolitischen Instrumente am besten nutzen lassen, um zu einem angemessenen gesellschaftlichen Gleichgewicht zwischen Sicherheit einerseits und Schutz der Grundrechte einschließlich der Privatsphäre andererseits zu gelangen. Die geplante Tagung „i2010 - Auf dem Weg zu einer allgegenwärtigen europäischen Informationsgesellschaft", die unter dem bevorstehenden finnischen Vorsitz veranstaltet wird, sowie die Anhörung zu den Auswirkungen von Funketiketten auf die Sicherheit und den Schutz der Privatsphäre, die Teil einer breiter angelegten, kürzlich von der Kommission gestarteten Anhörung ist, werden zu diesem Meinungsaustausch beitragen. Des Weiteren plant die Kommission:

- eine Veranstaltung für Unternehmen, um eine feste Verpflichtung der Industrie zu erreichen, wirksame Ansätze zur Umsetzung einer Sicherheitskultur in der **Wirtschaft** einzuführen;

- eine Veranstaltung, die Wege zur Weckung des Sicherheitsbewusstseins und der Stärkung des Vertrauens der **Endnutzer** in den Gebrauch elektronischer Netze und Informationssysteme aufzeigt.

3.2. Partnerschaft

3.2.1 Sinnvolle Entscheidungen können nur getroffen werden, wenn Art und Umfang der Herausforderungen wirklich verstanden wurden. Hierfür werden nicht nur zuverlässige, aktuelle statistische und wirtschaftliche Daten zu Sicherheitsvorfällen und zum Grad des Verbraucher- und Nutzervertrauens benötigt, sondern auch aktuelle Daten über Umfang und Entwicklungsrichtung der IKT-Sicherheitsbranche in Europa. Die Kommission will die ENISA ersuchen, eine **vertrauensvolle Partnerschaft mit den Mitgliedstaaten und den Interessenvertretern** zu entwickeln, um einen Rahmen zu entwerfen, der auch Verfahren und Mechanismen einbezieht, die der EU-weiten Erhebung von Daten über Sicherheitsvorfälle und Verbrauchervertrauen und deren Auswertung dienen.

Wegen des stark zersplitterten Marktes in der EU und seiner besonderen Ausprägung wird die Kommission parallel hierzu die Mitgliedstaaten, die Privatwirtschaft und die Wissenschaft auffordern, eine **strategische Partnerschaft** einzugehen, um die Verfügbarkeit von Daten über die IKT-Sicherheitsbranche und die Entwicklungsrichtungen des Marktes für Produkte und Dienste in der EU sicherzustellen.

3.2.2 Zur Verbesserung der europäischen Reaktionsfähigkeit auf Bedrohungen der Netzsicherheit wird die Kommission die ENISA weiterhin ersuchen, die **Verwirklichbarkeit eines europäischen Informationsaustauschs- und Warnsystems** zu untersuchen, damit bestehenden und künftigen Bedrohungen elektronischer Netze leichter begegnet werden kann. Insbesondere muss ein solches System ein **mehrsprachiges EU-Portal** umfassen, das maßgeschneiderte Informationen zu Bedrohungen, Risiken und Warnungen liefert.

3.3. Delegation der Verantwortung

Nur wenn den einzelnen Interessengruppen mehr Verantwortung übertragen wird, lässt sich deren Bewusstsein für die Notwendigkeit von Schutzmaßnahmen und Sicherheitsrisiken schärfen und sich somit die NIS fördern.

3.3.1 Deshalb fordert die Kommission die **Mitgliedstaaten** auf,

- sich aktiv an der vorgeschlagenen vergleichenden Bewertung der nationalen NIS-Politiken zu beteiligen;
- in enger Zusammenarbeit mit der ENISA Programme zu fördern, die zur Sensibilisierung hinsichtlich der Vorteile beitragen, die sich aus der Einführung wirksamer Sicherheitstechniken, Verfahren und Verhaltensweisen ergeben;
- der Einführung elektronischer Behördendienste zum Durchbruch zu verhelfen, um über bewährte Verfahren zu informieren und deren Anwendung zu fördern, so dass diese auf andere Branchen übertragen werden können;
- die Entwicklung von NIS-Programmen als Teil der Lehrpläne von Hochschulen anzuregen.

3.3.2 Die Kommission fordert auch die Akteure aus der **Wirtschaft** auf, Initiativen zu ergreifen, um

- eine geeignete Festlegung der Verantwortlichkeiten von Softwareproduzenten und Internet-Diensteanbietern zu entwickeln, und zwar in Verbindung mit Bestimmungen für ausreichende und prüffähige Sicherheitsniveaus; unterstützend müssen hierzu einheitliche Verfahren treten, die allgemein anerkannten Sicherheitsstandards und Regeln entsprechen;
- Verschiedenartigkeit, Offenheit, Interoperabilität, Benutzerfreundlichkeit und Wettbewerb als Schlüsselfaktoren für die Sicherheit zu fördern sowie den Einsatz die Sicherheit erhöhender Produkte, Verfahren und Dienste anzuregen, um Identitätsdiebstahl und andere Angriffe auf die Privatsphäre zu verhindern und zu bekämpfen;
- bewährte Verfahren für Netzbetreiber, Diensteanbieter und KMU zu verbreiten, die als grundlegendes Sicherheitsniveau dienen, das gleichzeitig den Fortbestand der Geschäftstätigkeiten dieser Unternehmen sichert;
- Ausbildungsprogramme im Unternehmensbereich insbesondere für KMU zu fördern, die Arbeitnehmern die notwendigen Fähigkeiten und Fertigkeiten vermitteln, damit sie bewährte Verfahren wirksam einsetzen können;
- auf erschwingliche Sicherheits-Zertifizierungsprogramme für Produkte, Verfahren und Dienste hinzuarbeiten, die bestimmte EU-Anforderungen abdecken (insbesondere in Bezug auf die Privatsphäre);
- die Versicherungswirtschaft an der Entwicklung von Instrumenten und Methoden zum Risikomanagement zu beteiligen, die der Beherrschung der mit der IKT

verbundenen Risiken und der Pflege einer Kultur des Risikomanagements in Behörden und Unternehmen (insbesondere in KMU) dienen.

4. SCHLUSSFOLGERUNGEN

Die Ermittlung der Probleme in Bezug auf die Sicherheit von Netzen und Informationssystemen in der EU und deren Bewältigung erfordern ein **umfassendes Engagement aller Beteiligten**. Der in dieser Mitteilung umrissene Politikansatz stützt sich dafür auf ein Gespräch zwischen allen Beteiligten. Dies würde auf gegenseitige Interessen aufbauen, es würden die jeweiligen Rollen ermittelt sowie ein dynamischer Rahmen entworfen werden mit dem Ziel, eine wirksame öffentliche Entscheidungsfindung und private Initiativen zu fördern.

Die Kommission wird dem Rat und dem Europäischen Parlament Mitte 2007 über die eingeleiteten Tätigkeiten, die ersten Ergebnisse und den Stand einzelner Initiativen berichten, darunter die der ENISA und die der Mitgliedstaaten und der Privatwirtschaft. Gegebenenfalls wird die Kommission eine Empfehlung zur Netz- und Informationssicherheit (NIS) vorlegen.