KOMMISSION DER EUROPÄISCHEN GEMEINSCHAFTEN

Brüssel, den 15.11.2006
KOM(2006) 688 endgültig

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

über die Bekämpfung von Spam, Späh- und Schadsoftware

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

über die Bekämpfung von Spam, Späh- und Schadsoftware

(Text von Bedeutung für den EWR)

1. ZWECK DER MITTEILUNG

Immer stärker wächst in der Gesellschaft das Bewusstsein, welch große Bedeutung den modernen elektronischen Kommunikationsnetzen und –diensten im Alltag zukommt – im Berufsleben wie auch zu Hause. Sollen die angebotenen Dienste in breitem Umfang genutzt werden, bedarf es vertrauenswürdiger, sicherer und zuverlässiger Technologien. Die Mitteilung der Kommission über eine Strategie für eine sichere Informationsgesellschaft[1] zielt auf eine allgemeine Verbesserung der Netz- und Informationssicherheit ab. Der private Sektor wird aufgefordert, Sicherheitslücken in Netzen und Informationssystemen, die zur Verbreitung von Spam und Schadsoftware genutzt werden können, zu schließen. In der Mitteilung der Kommission über die Überprüfung des EU-Rechtsrahmens für elektronische Kommunikationsnetze und –dienste werden neue Vorschriften zur Erhöhung der Sicherheit und zum Schutz der Privatsphäre im Bereich der elektronischen Kommunikation vorgeschlagen.[2]

Die vorliegende Mitteilung befasst sich mit der Entwicklung im Bereich der unerwünschten elektronischen Werbung *(Spam)*[3] und den Bedrohungen durch Spähsoftware *(Spyware)* und Schadsoftware *(Malware)*. Es wird eine Bilanz der bisherigen Bemühungen zur Abwendung dieser Bedrohungen gezogen und aufgezeigt, welche weiteren Maßnahmen ergriffen werden können. Unter anderem sind dies:

– Ausbau der gemeinschaftlichen Rechtsvorschriften;

– Rechtsdurchsetzung;

– Zusammenarbeit innerhalb der Mitgliedstaaten und zwischen den Mitgliedstaaten;

– politischer und wirtschaftlicher Dialog mit Drittländern;

– Initiativen der Branche;

– Forschungs- und Entwicklungsaktivitäten.

---

1 KOM(2006) 251 endgültig.
2 KOM(2006) 334 endgültig.
3 KOM(2004) 28 endgültig.

2. DAS PROBLEM: EINE SICH ÄNDERNDE ART DER BEDROHUNGEN

Spam[4] hat in den vergangenen fünf Jahren erheblich zugenommen.[5] Wirtschaftsquellen berichten, dass Spam mittlerweile mit 50-80 % der an die Endnutzer adressierten Mitteilungen zu Buche schlägt.[6] Wenngleich der größte Teil der Spam-E-Mails aus Ländern außerhalb der EU stammt, haben die europäischen Länder inzwischen doch immerhin einen Anteil von 25 % an den verbreiteten Spam-Mitteilungen erreicht.[7] Für das Jahr 2005 werden die Kosten von Spam auf weltweit 39 Mrd. EUR geschätzt. Die durch Spam entstehenden Kosten werden für die großen europäischen Volkswirtschaften mit etwa 3,5 Mrd. EUR für Deutschland, 1,9 Mrd. EUR für das Vereinigte Königreich und 1,4 Mrd. EUR für Frankreich veranschlagt.[8] Spamming ist inzwischen schon gewissermaßen zu einem eigenen „Wirtschaftszweig" geworden. Spammer mieten oder verkaufen Listen mit „geernteten" E-Mail-Adressen zu Marketing-Zwecken an Unternehmen. Besonders lukrativ ist Internet-Spam. Die Gründe hierfür sind die große Reichweite des Mediums und die geringen Kosten des Massenversands. Andererseits können aber auch schon moderate Investitionen in die Spam-Bekämpfung gute Ergebnisse bringen. So konnte beispielsweise in den Niederlanden mit Investitionen in Anti-Spam-Werkzeuge in Höhe von **570 000 EUR** eine Reduzierung des niederländischen Spam-Aufkommes um 85 % bewirkt werden.

Waren sie früher einfach nur ein Ärgernis, sind die unerwünschten E-Mails heutzutage immer häufiger betrügerischer oder krimineller Natur. Ein bekanntes Beispiel sind Phishing-E-Mails, die die Endnutzer dazu verleiten sollen, sensible Daten preiszugeben, und zwar durch deren Eingabe auf gefälschten Websites, die den Anschein erwecken, als handele es sich um die Websites tatsächlich existierender Unternehmen. Hier besteht die Gefahr des Identitätsbetrugs und der Schädigung des Rufs der betreffenden Unternehmen. Die Verbreitung von Spähsoftware per E-Mail oder der Einsatz von Software, die geeignet ist, das Online-Verhalten eines Nutzers aufzuzeichnen und entsprechende Berichte zu versenden, stellt eine zunehmende Gefahr dar. Spähsoftware kann auch persönliche Daten wie Kennwörter und Kreditkartennummern ausspionieren.

Die Versendung großer Mengen unerwünschter E-Mails wird durch die Verbreitung von bösartigen Programmcodes wie Würmern und Viren erheblich erleichtert. Sobald sie installiert wurden, ermöglichen sie einem Angreifer, die Kontrolle über ein infiziertes Computersystem zu übernehmen und es zu einem „Botnet"[9] zu machen, das die Identität des Spammers verschleiert. Botnets werden von Spammern, Phischern und Spyware-Anbietern für betrügerische und kriminelle Zwecke gemietet. Experten gehen davon aus, dass mehr als 50 % der missbräuchlichen E-Mails über Botnets weitergeleitet werden.[10] Die Verbreitung von Späh- und anderer Schadsoftware, die die Computer von privaten Nutzern und

---

4 Der Begriff „Spam" bezeichnet unerbetene Nachrichten, z. B. in Form von E-Mails, die zu kommerziellen Zwecken versandt werden. Unerwünschte E-Mails können auch Träger von Schadsoftware oder von Spyware sein.

5 Im Jahr 2001 hatte Spam einen Anteil von 7 % am weltweiten E-Mail-Aufkommen.

6 Symantec: 54 %; Messagelabs: 68,6 %; MAAWG: 80-85 %.

7 Q1 2006 (Sophos): Asien 42,8 %, Nordamerika 25,6 %, Europa 25,0 %, Südamerika: 5,1 %, Australasien: 0,8 %, Afrika: 0,6 %, sonstige: 0,1.

8 Ferris research, 2005.

9 Botnets sind infizierte, vernetzte Computer, die von Spammern zur Versendung von Massen-E-Mails genutzt werden. Zu diesem Zweck wird eine versteckte Software installiert, die den Computer ohne Wissen der Nutzer in Mail-Server umwandelt.

10 Am stärksten Botnet-infizierte Länder (Symantec, Q 3-4 2005): USA: 26 %, VK: 22 %, China: 9 %, Frankreich, Südkorea, Kanada: 4 %, Taiwan, Spanien, Deutschland: 3 %, Japan: 2 %.

Unternehmen angreift, hat beträchtliche wirtschaftliche Auswirkungen. Der durch solche Schadprogramme weltweit verursachte finanzielle Schaden wird für das Jahr 2005 auf etwa 11 Mrd. EUR beziffert.[11]

3. BISHERIGE ARBEITEN: MASSNAHMEN SEIT 2004

Die Europäische Union hat im Jahr 2002 eine **Richtlinie über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation** erlassen, die ein **Spam-Verbot** enthält[12]. Mit der Richtlinie wurde der Grundsatz der Zustimmungsbedürftigkeit von Werbung an natürliche Personen eingeführt. Im Januar 2004 legte die Kommission eine Mitteilung über Spam vor, in der Maßnahmen zur Ergänzung der Richtlinie vorgeschlagen wurden.[13] In der Mitteilung wurde die Notwendigkeit eines Tätigwerdens verschiedener Akteure in den Bereichen Aufklärung, Selbstregulierung / technische Maßnahmen, Zusammenarbeit und Rechtsdurchsetzung herausgestellt. Die Kommission hat damit begonnen, die Problematik der Bekämpfung von Spam, Späh- und Schadsoftware auch im Rahmen ihrer Gespräche mit Drittländern zum Thema zu machen. Im Übrigen werden die Verbraucher auch durch die Richtlinie über unlautere Geschäftpraktiken[14] vor aggressiven Geschäftspraktiken geschützt. In der Verordnung über die Zusammenarbeit im Verbraucherschutz[15] ist eine grenzüberschreitende Zusammenarbeit in der Bekämpfung entsprechender Praktiken vorgesehen.

3.1. Aufklärungsmaßnahmen

Die Kommissionsmitteilung hat dazu beigetragen, das Bewusstsein für das Phänomen Spam auf nationaler und internationaler Ebene zu schärfen. Auf EU-Ebene fördert das Programm **„Mehr Sicherheit im Internet“** eine sicherere Nutzung des Internets und den Einsatz neuer Online-Technologien – insbesondere für Kinder – im Rahmen eines innerhalb der Europäischen Union abgestimmten Vorgehens.

Die Mitgliedstaaten initiieren oder unterstützen **Kampagnen**, deren Ziel es ist, die Nutzer für die Spam-Problematik zu sensibilisieren und über den richtigen Umgang mit Spam aufzuklären. Generell stellen sich die Internet-Diensteanbieter (ISP) ihrer Verantwortung, indem sie ihre Kunden beraten, wie sie sich vor Spähsoftware und Viren schützen können, und sie entsprechend unterstützen. Im Februar 2004 war die Kommission Gastgeberin eines OECD-**Workshops** über Spam. Die Kommission hat auch einen aktiven Beitrag zum OECD-**Anti-Spam-Toolkit** geleistet. Dabei handelt es sich um ein umfassendes Paket ordnungspolitischer Maßnahmen, technischer Lösungen und Brancheninitiativen zur Spam-Bekämpfung.

Auf dem Weltgipfel der Vereinten Nationen über die Informationsgesellschaft[16] (WSIS) wurde die **Notwendigkeit anerkannt**, die Spam-Problematik auf der jeweils geeigneten nationalen oder internationalen Ebene in Angriff zu nehmen. Die ITU hat in den Jahren 2004 und 2005 WSIS-Themenkonferenzen organisiert. In der im November 2005 in Tunis

---

11 Computer Economics: The 2005 Malware Report.
12 Artikel 13 der Richtlinie 2002/58.
13 Siehe Fußnote 3.
14 Richtlinie 2005/29/EG, Anhang 1, Ziffer 26.
15 Verordnung (EG) Nr. 2006/2004.
16 WSIS, Genf, Dezember 2003.

angenommenen WSIS-Agenda wird dazu aufgerufen, das Spam-Problem, das zunehmend an Bedeutung gewinnt, wirksam anzugehen.[17]

3.2. Internationale Zusammenarbeit

Spam ist ein grenzüberschreitendes Problem. Es wurden bereits verschiedene Kooperationsinitiativen ergriffen und grenzüberschreitende Durchsetzungsmechanismen eingeführt. Die Kommission hat ein **Kontaktnetz der für die Spam-Bekämpfung zuständigen Behörden** ***(Contact Network of Spam Authorities,*** *CNSA)* eingerichtet, das regelmäßige Zusammenkünfte organisiert, bewährte Verfahren austauscht und im Bereich der Rechtsdurchsetzung grenzüberschreitend zusammenarbeitet. Das CNSA hat ein Kooperationsverfahren[18] festgelegt, um die grenzüberschreitende Verfolgung von Spam-Beschwerden zu erleichtern. Die Dienststellen der Kommission unterstützen den **Londoner Aktionsplan** (LAP) und nehmen als Beobachter an den Arbeiten teil. Auf der Grundlage des Aktionsplans arbeiten die zuständigen Behörden von 20 Ländern zusammen. Im Rahmen des LAP wurde ein Verfahren für die grenzüberschreitende Zusammenarbeit beschlossen. Im November 2005 fand ein gemeinsamer EU-CNSA/LAP-Workshop statt. Die **OECD** hat im April 2006 eine Empfehlung zur grenzüberschreitenden Zusammenarbeit bei der Durchsetzung der Rechtsvorschriften zur Bekämpfung von Spam[19] verabschiedet. Darin werden die zuständigen Behörden zum Informationsaustausch und zur Zusammenarbeit aufgefordert.

Die Kommission setzt sich auch weiterhin für **internationale Kooperationsinitiativen** ein. Die USA und die Europäische Union haben vereinbart, im Rahmen gemeinsamer Initiativen zur Rechtsdurchsetzung bei der Bekämpfung von Spam zusammenzuarbeiten und nach Lösungen zur Bekämpfung illegaler Späh- und Schadprogramme zu suchen. Des Weiteren arbeitet die Kommission in der kanadischen Arbeitsgruppe für internationale Zusammenarbeit im Bereich Spam mit. Es finden Gespräche mit wichtigen internationalen Partnern, z. B. mit China und Japan, statt. Was Asien betrifft, gab die Kommission den Anstoß zu einer gemeinsamen Erklärung über die internationale Zusammenarbeit zur Bekämpfung von Spam. Die Erklärung wurde im Februar 2005 auf der ASEM-Konferenz über den elektronischen Geschäftsverkehr[20] verabschiedet.

In der auf dem Weltgipfel über die Informationsgesellschaft im November 2005 angenommenen Tunis-Agenda wurde hervorgehoben, dass die Internetsicherheit ein Bereich ist, in dem eine bessere internationale Zusammenarbeit vonnöten ist, und dass diese Frage im Rahmen des Modells für eine verstärkte Zusammenarbeit im Bereich der Internet-Verwaltung, das als Folgemaßnahme zum Gipfel geschaffen werden soll,[21] aufzugreifen sein wird.

3.3. Forschung und technologische Entwicklung

Innerhalb des 6. Rahmenprogramms für Forschung und technologische Entwicklung hat die Kommission Projekte auf den Weg gebracht, die darauf abzielen, die Betroffenen bei der

---

17 Tunis-Agenda, Ziffer 41.

18 http://europa.eu.int/information_society/policy/ecomm/doc/todays_framework/privacy_protection/spam/cooperation_procedure_cnsa_final_version_20041201.pdf

19 http://www.oecd-antispam.org/

20 http://www.asemec-london.org/

21 Tunis-Agenda, Ziffern 39-47, http://www.itu.int/wsis/docs2/tunis/off/6rev1.doc.

Bekämpfung von Spam und anderen Formen von Schadsoftware zu unterstützen. Die Projekte[22] decken ein breites Spektrum von Tätigkeiten ab – von einer allgemeinen Netzüberwachung und dem Aufspüren von Angriffen bis hin zur konkreten Entwicklung von Technologien für die Installation von Filtern, die Spam, Phishing-Angriffe und Schadcodes abfangen. Ergebnisse waren unter anderem die Einrichtung einer Forschungsgemeinschaft, die sich mit dem Problem der Schadcode-Abwehr befasst, sowie der Aufbau einer europäischen Infrastruktur zur Überwachung des Internetverkehrs. Arbeiten zur Entwicklung adaptiver Phishing-Filter, die in der Lage sind, unbekannte Bedrohungen und Cyber-Angriffe aufzudecken, wurden in jüngster Zeit in Angriff genommen. Für diese Aktivitäten werden Mittel in Höhe 13,5 Mio. EUR bereitgestellt.

3.4. Maßnahmen der Branche

Die Kommission begrüßt, dass die Branche eine proaktive Rolle in der Spam-Bekämpfung übernommen hat. Generell haben die Diensteanbieter **technische Vorkehrungen** zur Bekämpfung von Spam, insbesondere durch bessere Spam-Filter, getroffen. Die ISP bieten eine **Helpdeskunterstützung** und stellen den Nutzern Programme zur Bekämpfung von Spam, Späh- und Schadsoftware zur Verfügung. Viele ISP wenden **Vertragsklauseln** an, die missbräuchliche Online-Praktiken untersagen. Kürzlich verhängte ein Zivilgericht im Vereinigten Königreich gegen einen Spammer eine Geldstrafe in Höhe von umgerechnet 68 800 EUR wegen Vertragsbruchs. Wirtschaftsverbände haben bewährte Verfahren eingeführt, um Online-Phishing zu verhindern und Filtermethoden zu optimieren[23].

Die Mobilfunkbetreiber haben für die Branche Verhaltensregeln eingeführt, die Maßnahmen zur Abwehr unerwünschter Nachrichten vorsehen. Die GSMA hat im Jahr 2006 einen Verhaltenskodex zum Umgang mit über Mobilfunknetze verbreitetem Spam herausgegeben. Die Kommission kofinanziert derzeit die Spotspam-Initiative – eine Partnerschaft zwischen privaten und öffentlichen Einrichtungen. Zweck dieser Initiative ist es, eine Datenbank aufzubauen, die eine grenzüberschreitende Untersuchung und Verfolgung von Spam-Fällen erleichtert.[24]

3.5. Rechtsdurchsetzung

Offensichtlich zeigen die Spam-Bekämpfungsmaßnahmen Wirkung. Dank der in Finnland verordneten Filtermaßnahmen konnte der Spam-Anteil am E-Mail-Aufkommen von 80 % auf etwa 30 % reduziert werden. Zahlreiche Behörden haben Strafverfolgungsmaßnahmen eingeleitet, um den Spammern das Handwerk zu legen.[25]

Zwischen den einzelnen Mitgliedstaaten bestehen jedoch erhebliche Unterschiede, was die Zahl der verfolgten Fälle anbelangt. Einige Behörden haben hundert oder mehr Untersuchungen eingeleitet, die erfolgreich abgeschlossen wurden und in denen Spam-Aktivitäten bestraft wurden. In anderen Mitgliedstaaten wurden lediglich einige wenige – oder auch gar keine – Fälle untersucht.

---

22 www.diademhttp://cordis.europa.eu/fp6/projects.htm#search

23 http://www.maawg.org/home/

24 http://www.spotspam.net

25 Eine Umfrage des CNSA hat ergeben, dass 15 der 18 Mitglieder, die geantwortet haben, im Zeitraum 2003 bis 2006 Strafverfolgungsmaßnahmen eingeleitet haben.

Die meisten Maßnahmen zielen auf **„traditionelle" Formen** von Spam ab; **andere festgestellte Bedrohungen wurden kaum verfolgt**, obwohl sie große Risiken bergen.

4. DAS WEITERE VORGEHEN: ANSTEHENDE ARBEITEN

4.1. Maßnahmen auf der Ebene der Mitgliedstaaten

In diesem Abschnitt geht es um Maßnahmen, die auf Regierungen und nationale Behörden abstellen, insbesondere auf Rechtsdurchsetzung und Zusammenarbeit.

4.1.1. Kritische Erfolgsfaktoren

Angesichts der Hartnäckigkeit des Problems und der sich ändernden Art der Bedrohungen sind ein größeres Engagement und eine entsprechende Prioritätensetzung seitens der Mitgliedstaaten erforderlich. Die zu planenden Maßnahmen sollten insbesondere auf „professionelle" Spammer und Phisher und auf die Verbreitung von Späh- und Schadsoftware abzielen. Kritische Erfolgsfaktoren sind:

– die feste Entschlossenheit der Regierungen, gegen missbräuchliche Online-Praktiken vorzugehen;

– die klare Zuweisung der Verantwortlichkeiten für die Durchführung der Maßnahmen im Bereich der Rechtsdurchsetzung;

– eine angemessene Ausstattung der für die Rechtsdurchsetzung zuständigen Behörden.

Derzeit sind diese Voraussetzungen nicht in allen Mitgliedstaaten erfüllt.

4.1.2. Koordinierung und Integration auf nationaler Ebene

Gemäß der Datenschutzrichtlinie für die elektronische Kommunikation und der allgemeinen Datenschutzrichtlinie[26] verfügen die nationalen Behörden über die Befugnis, gegen folgende illegale Praktiken vorzugehen:

– Versand unerbetener Nachrichten (**Spam**)[27];

– unrechtmäßiger Zugriff auf Endgeräte, sei es, um Informationen abzuspeichern, wie dies bei **Adware-** und **Spyware**-Programmen der Fall ist, oder um auf Informationen zuzugreifen, die im Endgerät gespeichert sind[28];

– Infizierung von Endgeräten durch Installieren von **Schadsoftware** wie Würmern und Viren und Umfunktionieren von PCs zu **Botnets** oder Missbrauch für andere Zwecke[29];

– Täuschung der Nutzer und Verleitung zur Weitergabe sensibler Daten[30], wie etwa Kennwörtern und Kreditkartenangaben, durch so genannte **„Phishing"**-Nachrichten.

---

26 Richtlinie 95/46/EG.
27 Artikel 13 der Datenschutzrichtlinie für elektronische Kommunikation.
28 Artikel 5 Absatz 3 der Datenschutzrichtlinie für elektronische Kommunikation.
29 Siehe Fußnote 28.
30 Artikel 6 Buchstabe a der allgemeinen Datenschutzrichtlinie.

Einige dieser Praktiken sind Straftatbestände und fallen unter die Bestimmungen des Rahmenbeschlusses über Angriffe auf Informationssysteme[31]. Gemäß diesem Beschluss haben die Mitgliedstaaten Freiheitsstrafen im Höchstmaß von mindestens drei Jahren bzw. fünf Jahren im Falle organisierter Kriminalität vorzusehen.

Auf nationaler Ebene kann die Einhaltung dieser Bestimmungen von Verwaltungsbehörden und Strafverfolgungsbehörden durchgesetzt werden. Wo dies der Fall ist, müssen die jeweiligen **Verantwortlichkeiten** der verschiedenen Behörden und die Verfahren der Zusammenarbeit klar festgelegt sein. Dies kann es erforderlich machen, dass Entscheidungen auf höherer Ebene innerhalb der nationalen Regierungen getroffen werden.

Bisher hat die zunehmende Verflechtung der strafrechtlichen und administrativen Aspekte von Spam und anderen Bedrohungen noch nicht zu einem entsprechenden Ausbau der Kooperationsverfahren in den Mitgliedstaaten geführt, die eine Bündelung der technischen und der Ermittlungskompetenzen der verschiedenen Stellen ermöglichen würde. Notwendig sind Kooperationsprotokolle, die Bereiche abdecken wie Austausch von Informationen und Ermittlungsergebnissen, Angaben zu Kontaktstellen, Unterstützung und Fallübertragung.

Eine enge Zusammenarbeit mit den zuständigen Behörden, den Netzbetreibern und den ISP auf nationaler Ebene kommt auch dem Informationsaustausch, dem technischen Know-how und der Verfolgung missbräuchlicher Online-Praktiken zugute. Die Behörden in Norwegen und den Niederlanden berichten, wie nützlich derartige öffentlich-private Partnerschaften sind.

4.1.3. Ressourcen

Zur Sammlung von Beweisen, zur Durchführung von Untersuchungen und zur Einleitung einer Strafverfolgung sind ausreichende Ressourcen erforderlich. Die Behörden benötigen eine angemessene technische Ausstattung und juristisches Personal und müssen sich mit den Vorgehensweisen der Täter vertraut machen, wenn sie deren Praktiken ein Ende setzen wollen.

Zu einem wichtigen Instrument können hier Online-Beschwerdeverfahren werden, die ein System zur Aufzeichnung und Analyse der berichteten missbräuchlichen Praktiken vorsehen. Die Erfahrung hat gezeigt, dass bereits **moderate Investitionen gute Ergebnisse** erbringen können. Die Reduzierung von Spam in den Niederlanden wurde bewerkstelligt durch Einrichtung eines Teams von fünf Vollzeitbeschäftigten bei der OPTA, der zuständigen niederländischen Behörde, und einen Mitteleinsatz in Höhe von **570 000 EUR** für Anti-Spam-Werkzeuge. Dank dieser Investition ist es nun möglich, die in der Spam-Bekämpfung gewonnenen Erfahrungen für die Entwicklung von Lösungen in anderen Problembereichen zu nutzen.

4.1.4. Grenzüberschreitende Zusammenarbeit

Spam ist ein globales Problem. Die nationalen Behörden werden bei der strafrechtlichen Verfolgung von Spammern häufig auf die Zusammenarbeit mit Behörden anderer Länder

[31] Rahmenbeschluss 2005/222/JI des Rates.

angewiesen sein. Umgekehrt werden sie selbst unter Umständen auf Ermittlungsersuchen aus anderen Ländern hin tätig werden müssen.

Zwar ist mit einer gewissen Zurückhaltung zu rechnen, wenn es darum geht, die knappen nationalen Ressourcen einzusetzen, um den Problemen anderer nachzugehen, doch müssen die Mitgliedstaaten erkennen, dass die wirksame grenzüberschreitende Zusammenarbeit ein wesentlicher Faktor bei der Spam-Bekämpfung ist. Unlängst ist es den für die Spam-Bekämpfung zuständigen australischen und niederländischen Behörden dank ihrer Zusammenarbeit gelungen, eine groß angelegte Spam-Aktion zu verhindern.

Bisher haben 21 europäische Behörden das vom CNSA festgelegte Verfahren der Zusammenarbeit[32] für die grenzüberschreitende Bearbeitung von Beschwerden übernommen. Die übrigen Behörden sind aufgefordert, diesem Beispiel in den kommenden Monaten zu folgen. Insbesondere werden die Mitgliedstaaten und die zuständigen Behörden aufgefordert, aktiv darauf hinzuarbeiten, dass

– die gemeinsamen CNSA-LAP-Pro-forma-Dokumente verwendet werden,

– die OECD-Empfehlung umgesetzt wird und das OECD-Toolkit zur Rechtsdurchsetzung im Bereich Spam zum Einsatz kommt.

4.1.5 Vorgeschlagene Maßnahmen

Die Mitgliedstaaten und ihre zuständigen Behörden werden aufgefordert,

– die Verantwortlichkeiten der für die Spam-Bekämpfung zuständigen nationalen Stellen klar abzugrenzen;

– eine effektive Koordinierung zwischen den zuständigen Behörden zu gewährleisten;

– die Marktteilnehmer auf nationaler Ebene einzubinden und ihr Know-how sowie die verfügbaren Informationen nutzbar zu machen;

– dafür zu sorgen, dass die für die Rechtsdurchsetzung erforderlichen Ressourcen zur Verfügung stehen;

– an Verfahren der internationalen Zusammenarbeit mitzuwirken und auf entsprechende Ersuchen hin grenzüberschreitend Unterstützung zu leisten.

4.2. Maßnahmen der Branche

In diesem Abschnitt geht es um Maßnahmen, die die Branche treffen kann, um das Verbrauchervertrauen zu fördern und die Versendung missbräuchlicher E-Mails einzudämmen.

4.2.1. Softwarelieferung und -installation

Spähsoftware *(Spyware)* stellt eine ernsthafte Bedrohung der Privatsphäre der Nutzer dar. Eine inzwischen weit verbreitete Methode zur **Verteilung von Spähsoftware und deren**

[32] Siehe Fußnote 18.

Installation auf den Endgeräten der Nutzer besteht darin, Softwareprodukte online anzubieten. Spähfunktionen können auch in Software-Produkten verborgen sein, die über andere Medien, wie CD-ROMs für die Installation auf einem Computer, vertrieben werden. Zusammen mit der vom Nutzer erworbenen Software können unerwünschte Spionageprogramme installiert werden.

Im Folgenden werden einige spezifische Maßnahmen genannt, mit denen verhindert werden kann, dass Spähsoftware die Endnutzer erreicht.

4.2.2. Aufklärung der Verbraucher

Software-Angebote können die Installation zusätzlicher Programme beinhalten. Sofern diese zusätzliche Software Spähfunktionen enthält und das Verhalten der Endnutzer überwacht (z. B. für Marketing-Zwecke), bedeutet dies, dass personenbezogene Daten verarbeitet werden, was ohne Information und Einwilligung des Nutzers unzulässig ist. Vielfach wird die Zustimmung des Nutzers zur Installation solcher Software nicht eingeholt oder die Einwilligung ist im Kleingedruckten einer langen Endnutzerlizenzvereinbarung versteckt.

Anbieter von Software-Produkten sollten klar und deutlich sämtliche Bedingungen nennen und insbesondere Angaben dazu machen, ob von irgendwelchen in den Software-Paketen enthaltenen Überwachungskomponenten personenbezogene Daten verarbeitet werden.

Selbstregulierung und die Verwendung einer Art „Gütesiegel“ wären eine Möglichkeit, vertrauenswürdige Anbieter von nicht vertrauenswürdigen Anbietern zu unterscheiden. Verhaltenskodizes, deren Zweck es ist, die Nutzer über Bedingungen zu informieren, die eine Verarbeitung personenbezogener Daten vorsehen, können der Datenschutzgruppe nach Artikel 29 zur Prüfung vorgelegt werden.

4.2.3 Vertragsklauseln in der Lieferkette

Häufig sind sich Unternehmen **gar nicht dessen bewusst**, mithilfe welcher technischen Lösungen die Werbung für ihre Produkte und Dienstleistungen die Adressaten erreicht. Spähsoftware kann im Paket mit unbedenklicher Software eingeschleust werden, um Zugang zu sensiblen Daten, wie etwa Kreditkartendaten, vertraulichen Dokumenten, usw. zu erlangen.

Unternehmen, die für Produkte werben oder Produkte verkaufen, müssen sich vergewissern, dass ihre Vertragspartner mit legitimen Mitteln arbeiten. Ein Unternehmen muss die innerhalb einer Vertragskette bestehenden Beziehungen durchschauen, es muss sicherstellen, dass die geltenden Rechtsvorschriften eingehalten werden, und es muss missbräuchliche Praktiken innerhalb der Kette unterbinden, damit weitere Geschäftsverbindungen mit Unternehmen, die derartige Praktiken anwenden, unverzüglich beendet werden.

4.2.4 Sicherheitsvorkehrungen seitens der Diensteanbieter

Eine im Jahr 2006 von der ENISA durchgeführte Umfrage[33] bestätigt, dass die Diensteanbieter in der Regel Maßnahmen zur Spam-Bekämpfung treffen. Festgestellt wird aber auch, dass sie mehr tun könnten, um die allgemeine Netzsicherheit zu erhöhen. Es wird empfohlen, größeres Augenmerk auf die Filterung der E-Mails, die das Netz eines

[33] http://www.enisa.eu.int/doc/pdf/deliverables/enisa_security_spam.pdf

Diensteanbieters verlassen, zu richten **(*Egress*-Filterung)**. Die Kommission möchte die Diensteanbieter ermutigen, dieser Empfehlung zu folgen.

Die Datenschutzgruppe nach Artikel 29 hat eine Stellungnahme zu Datenschutzfragen bei Filterdiensten für elektronische Post[34] abgegeben. Die Stellungnahme enthält Informationen zu Fragen der Vertraulichkeit des E-Mail-Verkehrs und insbesondere zum Filtern von Online-Nachrichten zum Schutz vor Viren, Spam und illegalen Inhalten.

4.2.5. Vorgeschlagene Maßnahmen

Die Kommission

– fordert die Unternehmen auf sicherzustellen, dass die beim Erwerb von Software-Anwendungen standardmäßig erteilten Informationen den datenschutzrechtlichen Bestimmungen entsprechen;

– fordert die Unternehmen auf, die illegale Softwarenutzung zu Werbezwecken vertraglich zu untersagen, zu überwachen, wie ihre Werbung zum Verbraucher gelangt, und missbräuchliche Praktiken zu verfolgen;

– fordert E-Mail-Diensteanbieter auf, eine Filterpolitik anzuwenden, die gewährleistet, dass die einschlägige Empfehlung sowie die Leitlinien zur Filterung von E-Mails umgesetzt werden.

4.3. Maßnahmen auf europäischer Ebene

Die Kommission wird auch künftig Fragen im Zusammenhang mit Spam, Späh- und Schadsoftware in internationalen Foren, auf bilateralen Sitzungen und – soweit erforderlich – im Rahmen von Vereinbarungen mit Drittländern aufgreifen und wird auch weiterhin die Zusammenarbeit zwischen allen Beteiligten fördern, insbesondere zwischen den Mitgliedstaaten, den zuständigen Behörden und der Branche. Auch wird sie neue Initiativen in den Bereichen Rechtsetzung und Forschung auf den Weg bringen und damit neue Anstöße zur Bekämpfung missbräuchlicher Praktiken geben, die die Informationsgesellschaft aushöhlen. Die Kommission arbeitet derzeit an der Weiterentwicklung einer kohärenten Strategie zur Bekämpfung der Cyber-Kriminalität. Die Strategie wird Gegenstand einer Mitteilung sein, die Anfang 2007 zur Annahme vorgelegt werden soll.

4.3.1. Überprüfung des Rechtsrahmens

In der Mitteilung der Kommission[35] über die Überprüfung des Rechtsrahmens für elektronische Kommunikation wird vorgeschlagen, die den Schutz der Privatsphäre und die Sicherheit betreffenden Rechtsvorschriften auszubauen. Der Vorschlag sieht vor, Netzbetreiber und Diensteanbieter zu verpflichten,

– der zuständigen Behörde in einem Mitgliedstaat jeden Sicherheitsverstoß zu melden, der einen Verlust personenbezogener Daten oder Unterbrechungen der Kontinuität der Leistungserbringung zur Folge gehabt hat;

---

34 Stellungnahme 2/2006, WP 118.

35 http://europa.eu.int/information_society/policy/ecomm/implementation_enforcement/index_en.htm

– ihre Kunden über jeden Sicherheitsverstoß zu unterrichten, der einen Verlust, eine Änderung oder eine Vernichtung personenbezogener Kundendaten zur Folge gehabt oder den Zugriff auf solche Daten ermöglicht hat.

Die nationalen Regulierungsbehörden wären in der Lage, dafür zu sorgen, dass die Betreiber ausreichende Sicherheitsmaßnahmen treffen, und es könnten neue Vorschriften festgelegt werden, die **spezifische Rechtsmittel** vorsehen oder Angaben zur Höhe der im Falle eines Verstoßes zu erwartenden **Strafe** enthalten.

4.3.2. Die Rolle der ENISA

Unter anderem wird vorgeschlagen, in einer Vorschrift die beratende Rolle der ENISA in Sicherheitsfragen zu erwähnen. In der Kommissionsmitteilung über eine Sicherheitsstrategie[36] werden der ENISA noch weitere Aufgaben zugedacht, wie etwa:

– Aufbau einer vertrauensvollen Partnerschaft mit den Mitgliedstaaten und allen Beteiligten mit dem Ziel, einen geeigneten **Rahmen für die Erfassung von Daten** über Sicherheitsvorfälle und das Verbrauchervertrauen zu entwickeln.

Bei der Festlegung des Rahmens wird sich die ENISA um eine enge Abstimmung mit Eurostat bemühen – mit Blick auf die gemeinschaftliche Statistik zur Informationsgesellschaft und auf den i2010-Benchmarking-Rahmen[37].

– Prüfung der **Praktikabilität eines Europäischen Informations- und Warnsystems**, das ein wirksames Vorgehen gegen aktuelle und künftige Bedrohungen für elektronische Netze erleichtern soll.

4.3.3. Forschung und Entwicklung

Ein Ziel des künftigen 7. Forschungsrahmenprogramms wird es sein, in enger Abstimmung mit einschlägigen politischen Initiativen Wissen und Technologien, die eine höhere Sicherheit im Bereich der Informationsdienste und –systeme gewährleisten, kontinuierlich weiterzuentwickeln. Was Schadsoftware anbelangt, werden die Arbeiten unter anderem die Aspekte versteckte Botnets und Viren sowie Angriffe auf Mobilfunk- und Sprachtelefondienste abdecken.

4.3.4. Internationale Zusammenarbeit

Das Internet ist ein weltweites Netz. Somit ist bei der Bekämpfung von Spam, Späh- und Schadsoftware ein weltweites Engagement erforderlich. Daher beabsichtigt die Kommission, im Kampf gegen diese Bedrohungen und die damit verbundenen kriminellen Aktivitäten den Dialog und die Zusammenarbeit mit Drittländern zu verstärken. Zu diesem Zweck wird die Kommission sich dafür einsetzen, dass Spam, Späh- und Schadsoftware zum Gegenstand von zwischen der EU und Drittländern geschlossenen Vereinbarungen gemacht werden. Sie wird sich um verbindliche Zusagen der am stärksten betroffenen Drittländer bemühen, zusammen mit den EU-Mitgliedstaaten wirksamer gegen diese Bedrohungen vorzugehen, und sie wird die Durchsetzung der gemeinsam vereinbarten Ziele aufmerksam verfolgen.

---

[36] Siehe Fußnote 1.

[37] Von der Hochrangigen Gruppe „i2010“ am 20. April 2006 beschlossener Benchmarking-Rahmen.

4.3.5. Vorgeschlagene Maßnahmen

Die Kommission wird

- ihre Anstrengungen in den Bereichen Sensibilisierung und Förderung der Zusammenarbeit zwischen den Beteiligten fortsetzen;
- weiterhin den Abschluss von Vereinbarungen mit Drittländern über die Bekämpfung von Spam, Späh- und Schadsoftware anstreben;
- darauf hinarbeiten, Anfang 2007 neue Legislativvorschläge zur Weiterentwicklung der Vorschriften vorzulegen, die den Schutz der Privatsphäre und die Sicherheit im Kommunikationssektor betreffen, und eine Strategie zur Bekämpfung von Cyber-Kriminalität ausarbeiten;
- in Sicherheitsfragen auf die Fachkompetenz der ENISA zurückgreifen;
- innerhalb ihres 7. Forschungsrahmenprogramms Arbeiten in den Bereichen Forschung und Entwicklung unterstützen.

5. FAZIT

Bedrohungen durch Spam, Späh- und Schadsoftware untergraben das Vertrauen in die Informationsgesellschaft, stellen deren Sicherheit in Frage und haben beträchtliche finanzielle Auswirkungen. Einige Mitgliedstaaten haben zwar Initiativen auf den Weg gebracht, doch wird – insgesamt gesehen – in der EU **zu wenig getan, um dieser Entwicklung Einhalt zu gebieten**. In Wahrnehmung ihrer Mittlerrolle ist die Kommission bestrebt, das Bewusstsein für die Notwendigkeit eines stärkeren politischen Engagements im Kampf gegen diese Bedrohungen zu schärfen.

Es sind verstärkte Anstrengungen zur Rechtsdurchsetzung zu unternehmen, damit den Aktivitäten derjenigen, die wissentlich gegen geltendes Recht verstoßen, ein Ende gesetzt wird. Vonseiten der Branche sollten ergänzende Maßnahmen getroffen werden. Auf nationaler Ebene ist sowohl innerhalb der Regierung als auch zwischen Regierung und Wirtschaft eine Zusammenarbeit erforderlich. Die Kommission wird den Dialog und die Zusammenarbeit mit Drittländern intensivieren und prüfen, inwieweit es angebracht erscheint, neue Legislativvorschläge auszuarbeiten. Des Weiteren wird sie Forschungsarbeiten in Angriff nehmen, die darauf abstellen, einen besseren Schutz der Privatsphäre und eine höhere Sicherheit im Bereich der elektronischen Kommunikation zu gewährleisten.

Eine integrierte und möglichst parallel verlaufende Umsetzung der in der vorliegenden Mitteilung genannten Maßnahmen kann dazu beitragen, die festgestellten Bedrohungen zu reduzieren, die derzeit der Informationsgesellschaft ebenso wie der Wirtschaft zum Schaden gereichen.
Die Kommission wird die Umsetzung der Maßnahmen aufmerksam verfolgen und bis 2008 bewerten, ob weitere Maßnahmen erforderlich sind.