XXIII. GP.-NR
3931 /J
25. März 2008

Anfrage

der Abgeordneten Mag. Johann Maier
und GenossInnen
an den Bundesminister für Verkehr, Innovation und Technologie
betreffend „Spam-Mails – Strategien zur Bekämpfung"

Mit der AB 224/XXIII.GP vom 08.03.2007 wurden durch den Bundesminister sehr ausführlich die Fragen zur Bekämpfung von Spam-Mails (unerwünschte E-Mails) mit den Zahlen für das Jahr 2006 beantwortet und auf die grundsätzlichen (internationalen) Problemstellungen hingewiesen.

Die Situation hat sich für Internet-User auch 2007 nicht geändert: 91 Prozent aller E-Mails in Europa sind Spam! 171 Milliarden E-Mails werden jeden Tag verschickt. Die Überflutung mit elektronischer Post lässt die Produktivität der Mitarbeiter in Unternehmen deutlich sinken. Allein die US-Wirtschaft verliert so jährlich 588 Milliarden Dollar. Obwohl schon die meisten Spam-Mails firmenintern ausgefiltert werden, verschwendet ein Manager laut aktuellen Hochrechnungen britischer Forscher insgesamt 3,5 Jahre seiner Lebenszeit mit irrelevanten Mails.
Unerwünschte E-Mail (inkl. SMS) sind meist Werbeangebote für Pharmaprodukte, Parfüms, Erotikdienste, Viagra, Penisverlängerungen, Finanzierungen, Penny-stocks (Pumping stocks), Aktienkäufe, Arzneimittel etc.. Unerwünschte E-Mails widersprechen europäischem Recht, dem österreichischen TKG und sind wettbewerbswidrig. Jeder Versender könnte in den meisten europäischen Staaten auf Unterlassung geklagt werden. Trotzdem ist dies meist aussichtslos, da sich die Absender bzw. Werber meist außerhalb der nationalen und europäischen Jurisdiktion befinden. Der Kampf gegen Spams wird zurzeit international als fast aussichtslos beurteilt.

Diese Aussichtslosigkeit musste im Jahr 2006 der deutsche Bundesverband der Verbraucherzentralen eingestehen, der eine eigene Beschwerdestelle dazu sogar eingerichtet hatte:

2,4 Millionen Beschwerden waren unter **beschwerdestelle@spam.vzbv.de** bis Ende November 2006 eingegangen. Das waren rund 6.300 Emails am Tag, 85 Prozent davon waren internationale Spam-Emails. Das heißt, der Versender der Spam kam nicht aus Deutschland, er kam aus dem Ausland.

Damit waren aber den deutschen Behörden die Hände bei der Verfolgung gebunden. Der Bundesverband konnte in einem solchen Fall nichts anderes tun, als die Email an die jeweiligen nationalen Behörden weiterzuleiten - für die meisten Verbraucher eine Enttäuschung, weil nichts herauskam. Viele Spam-Warnungen und aufklärende Informationen für Internet-User kommen vom deutschen BSI bzw. von Bürger-CERT für Österreich ist keine vergleichbare Einrichtung bekannt.

Auch unter den österreichischen Unternehmen herrscht große Unsicherheit zu Spam-Mails. Bemerkenswert dazu eine aktuelle Umfrage der Wirtschaftskammer Österreich (WKÖ): Demnach ist der Schutz vor Spam-Mails für die Betriebe das mit Abstand wichtigste Thema im Zusammenhang mit IT-Fragen. Immerhin 59,7 % der befragten Unternehmen sehen dies als Riesenproblem an. Allerdings möchten 72,6 % den Erstkontakt zu Kunden auf dem Wege der elektronischen Kommunikation aufnehmen dürfen, am liebsten per E-Mail. Und zu guter letzt hält dennoch die überwältigende Mehrheit von 85,2 % die geltenden Regeln, die das unaufgeforderte Zusenden von E-Mails verbieten, für angemessen. Das das Internet kein rechtsfreier Raum ist, sei vielen leider noch immer nicht bewusst, warnte die WKÖ. Über die Verbotsbestimmungen des Telekommunikationsgesetzes weiß mit 47,6 % nicht einmal die Hälfte der Betriebe Bescheid. Bei Betrieben mit 10 bis 49 bzw. ab 250 Mitarbeitern ist das Wissen besonders schwach ausgeprägt (38,6 bzw. 39,6 %). Als eine Gegenmaßnahme wird – so die Presseinformation – das E-Center der Wirtschaftskammer Österreich der Aufklärung im Zusammenhang mit Spam und IT-Sicherheit 2008 besonderes Augenmerk schenken.

Spamversand ist für Kriminelle ein lukratives Geschäft, ein Ende der Spamflut ist weltweit nicht abzusehen:

„Laut Gdata kostet der Versand von 20 Millionen Werbemails lediglich 350 Euro. Für 140 Euro seien fünf Millionen E-Mail-Adressen und ein Selbstbau-Kit erhältlich, mit dem Werbetreibende selber die unerwünschten E-Mails verschicken können. Die Anbieter dieser Offerten setzen dabei zunehmend auf Kombi-Pakete: Zehn Minuten Distributed-Denial-of-Service (DDoS) gibt es kostenlos dazu, längere Attacken auf die Server des Wettbewerbs gebe es für rund 14 Euro (20 US-Dollar) die Stunde oder für etwa 70 Euro (100 US-Dollar) am Tag.
Auch E-Mail-Adressen sind günstig zu haben – zehn Millionen Adressen kosten den Sicherheitsforschern zufolge nur 100 Euro.

Am teuersten kommen Kaufwilligen Zugangsdaten zum Online-Spiel World of Warcraft zu stehen, hier kostet ein Kontodatensatz sechs Euro. Einen Kreditkarten-Datensatz gebe es für drei Euro" (heise.de 24.10.2007).

International haben sich in den letzten Jahren die Probleme weiter verschärft, wie nachstehende Beispiele zeigen:

Einer Analyse des **Instituts für Internet-Sicherheit** an der FH Gelsenkirchen (ifis) zufolge gelingt es Spam-Versendern mittlerweile in den weitaus meisten Fällen, IP-Adressen für so kurze Zeit zu nutzen, dass sich ein nachträgliches Eintragen auf **Blacklists** Stunden oder gar Tage später kaum mehr lohnt. Rund drei Viertel aller Adressen treten nach den Erkenntnissen des ifis überhaupt nur innerhalb eines einzigen Tages in Erscheinung. Zwei Tage lang sind es 13 Prozent, und über drei Tage hinweg ließen sich gerade noch 4 Prozent der IP-Adressen als aktiv erkennen. Mehr als drei Tage lang aktiv waren im analysierten Zeitraum Mitte Dezember 2007 lediglich die verbleibenden 8 Prozent aller IP-Adressen, inklusive derjenigen gewöhnlicher Mailserver, die ihre IP-Adressen üblicherweise nicht laufend wechseln (heise.de 18.01.2008).

Online-Kriminelle stellen sich vermehrt auf die individuellen Unterschiede zwischen verschiedenen Ländern und Kulturen ein.

So arbeiten sie zunehmend mit unterschiedlichen Sprachen und konzentrieren sich auf lokale Webangebote, einzelne Firmen oder bestimmte Software. Zu diesem Ergebnis kommt eine aktuelle Studie des IT-Sicherheitsunternehmens McAfee [http://www.mcafee.com/de]. Schadsoftware werde heutzutage speziell für den Einsatz in bestimmten Ländern programmiert, die dazugehörigen Spam-Mails in der Landessprache verfasst. Besonders beliebt zur Schadcodeverbreitung seien Web 2.0 Anwendungen und Peer-to-Peer-Netzwerke.

Versender von Spam-Mails scheuen keine Mühen, um ihre „Müll-Nachrichten" im World Wide Web zu verbreiten.

Das IT-Sicherheitsunternehmen McAfee [http://www.mcafee.com/de] berichtet, dass Cyberkriminelle die automatische Abwesenheitsnotiz von Webmail-Anbietern nutzen, um ihre Spam-Mails zu versenden. Dazu richten sie einen Webmail-Account ein und aktivieren die automatische Antwortfunktion. Die Betreffzeile mit dem „out of office"-Text wird durch eine eigene ersetzt und das Textfeld mit der Spam-Nachricht versehen. Nun wird über gefälschte Absenderadressen eine Unmenge an E-Mails an diesen Account versandt. Dieser "antwortet" dann automatisch auf alle eingehenden Mails - mit der Spam-Nachricht.

Der Vorteil für die Online-Kriminellen: Auf diese Art versandte Mails werden in der Regel von Spamfiltern nicht erkannt und gelangen ungehindert in die Postfächer der Nutzer. Mehr Infos zum Thema Spam gibt es auf der BSI-fuer-Buerger-Webseite [http://www.bsi-fuer-buerger.de/abzocker/05_06.htm].

Beispiele zur „Spam-Mafia" (Quelle: Buerger-Cert)

Besonders gefährlich sind die Phishingseiten im Internet:

„Während das BKA im Mai 2006 insgesamt 12.000 solcher Seiten zählte, waren es im November 2006 bereits 32.000 Seiten. **Besonders problematisch sind die „explodierenden Botnetze in Millionenhöhe", bei denen über Trojaner fremde Rechner zweckentfremdet werden, um Spam zu verschicken.** 20.000 Schadprogramme sollen laut Ziercke vom BSI gezählt worden sein. „Die Zahlen zeigen, die Internet-Täter keine psychologischen Hemmschwellen haben", lautete Zierckes Fazit (heise.de 13.02.2007).

Ende September 2007 wurden von Cyberkriminellen E-Mails im Netz verbreitet, die mit kostenlosen Spiele-Downloads locken, berichtete die Online-Ausgabe des Magazins PC Welt [http://www.pcwelt.de].

Klickt der Empfänger auf den angegebenen Link, wird er auf eine Webseite geführt, von der er sich die vermeintlichen Spiele herunterladen kann. Öffnet er die dort hinterlegte Datei namens „ArcadeWorld.exe" wird ein **Trojanisches Pferd auf den Rechner** geladen, der ihn an ein Bot-Netz anschließt.

Ein weiteres Spam-Mail der Bot-Netz-Betreiber, die vermehrt im Netz kursiert, bietet dem Empfänger einen Job als Geldwäscher.

Folgt man dem dazugehörigen Link, landet man auf einer Webseite, die ganz offen eine Provision von 10 Prozent für eine Geldwäsche offeriert. Die Experten von Symantec [http://www.symantec.de] gehen davon aus, dass diese Job-Mails von den bereits „gekaperten" Rechnern des Bot-Netzes aus verschickt werden. Das BSI rät dazu, Mails aus nicht vertrauenswürdigen Quellen umgehend zu löschen.

Besonders aktuell war 2007 der Versand von Massenmails mit PDF-Anhang:

Viele Anti-Spam-Programme sind noch nicht in der Lage, PDF-Inhalte auf Spam zu untersuchen – sie überprüfen lediglich die Signatur der Datei und der E-Mail.

Dies öffnet den Cyberkriminellen Tür und Tor – und die Zeit, in der PDF-Dokumente als halbwegs „sicher" galten, scheint endgültig vorbei. über eine Sicherheitslücke im Adobe Reader können Angreifer beliebigen Schadcode auf fremde Rechner schmuggeln und die vollständige Kontrolle über den Computer erlangen. Dazu genügt bereits das Öffnen manipulierter PDF-Dokumente. Bislang gibt es keinen Patch, der die Lücke schließt. Das BSI rät Nutzern dazu, keine PDF-Dateien aus unbekannten oder nicht vertrauenswürdigen Quellen zu öffnen und umgehend das Update einzuspielen, sobald dieses bereit steht.

Nach einer Welle von Spam-Mails mit PDF-Dateien im Anhang waren 2007 auch vermehrt Werbe-Mails mit angehängten Excel-Tabellen in Umlauf. Dies berichtet das IT-Sicherheitsunternehmen G Data (http:www.data.de). Die Dateien tragen Namen wie „investor-news-12345.xls" oder „news-12345.xls" und haben in erster Linie die Aufgabe, installierte Spamfilter zu umgehen, damit die Werbe-Mail auch wirklich im Postfach des Empfängers landet. Die meisten gängigen Filter sind nicht in der Lage, Excel-Dateien als Spam zu erkennen. Des Weiteren ist nicht auszuschließen, dass sich auch Schadcode in den Dateianhängen versteckt.

Für Unruhe im Netz sorgten auch E-Mails, die vermeintlich von Paypal stammen sollen. In der Mail heißt es, dass mit Paypal jetzt auch Online-Banking möglich sei. Um dieses so sicher wie möglich zu gestalten, könne man ab sofort TAN-Nummern für Transaktionen nutzen. Dazu befinde sich im Anhang ein spezieller TAN-Generator. Öffnet der Empfänger jedoch die angehängte Datei, installiert sich ein Trojanisches Pferd auf dem Rechner. Der Schädling spioniert Paypal-Zugangsdaten und möglicherweise weitere private Informationen aus.

„Sex sells" scheint nach wie vor das Motto der Online-Kriminellen zu sein.
So verbreiteten sich E-Mails im Netz, die ein vermeintlich pornografisches Promi-Computerspiel im Anhang haben, berichtet das Antivirenunternehmen Sophos [http://www.sophos.de]. In den vermeintlichen Games sollen beispielsweise Angelina Jolie, Luke Skywalker oder Harry Potter zu sehen sein. Mit Betreffzeilen wie „You ask me about this game, here it is!", „Hot game" oder „Something hot" soll der Empfänger der Nachricht dazu verleitet werden, die angehängte .zip-Datei zu öffnen. Kommt man der Aufforderung nach, wird ein Trojanisches Pferd auf den Rechner geladen. Der Schädling lädt weitere Malware aus dem Internet nach und verschickt sich selbst per E-Mail weiter. Empfänger sollten keinesfalls den Dateianhang öffnen und die Antivirensoftware stets auf dem aktuellen Stand halten.

Cyberkriminelle boten 2007 über Webseiten manipulierte Blog-Vorlagen an, die Spam-Links enthalten.

Dies berichtet das IT-Sicherheitsunternehmen Trend Micro [http://de.trendmicro-europe.com/]. Werden die angebotenen Templates in das eigene Weblog eingebunden, werden auch die Links übernommen - die allerdings für den Nutzer nicht sichtbar sind. Sichtbar sind sie lediglich für Suchmaschinen, die die Links finden und die dort angezeigten Webseiten in ihrer „"Trefferliste" durch das vermehrte Aufkommen weiter nach oben setzen.

Das IT-Sicherheitsunternehmen Panda Security [http://www.panda-software.de] berichtete über Spam-Mails, die das Online-Casino „Lux Imperial Casino" bewerben.

In der Nachricht heißt es, dass die Einzahlung des Nutzers von 350,50 Euro dem Spielkonto gutgeschrieben wurde und man den Kontoauszug über den angegebenen Link überprüfen könne. Wird dieser Link jedoch angeklickt, wird man auf eine Webseite geleitet, über die der Spam-Versender nach Sicherheitslücken auf dem Rechner des Anwenders sucht. Findet er eine ungepatchte Schwachstelle, wird diese dazu genutzt, um ein Trojanisches Pferd auf den Rechner zu schleusen. Dieses lädt einen weiteren Schädling nach, der Kontodaten ausspioniert. Empfänger der Mail sollten diese umgehend löschen und Betriebssystem und Software stets auf dem aktuellen Stand halten (Bürger-CERT 06.03.2008).

Cyberkriminelle nutzten die Neugier der Internetnutzer, um Schadsoftware zu verbreiten: Sie versendeten E-Mails laut mehrerer IT-Sicherheitsunternehmen mit Links zu vermeintlichen Enthüllungsvideos.

Die Betreffzeilen lauten beispielsweise „Download and watch the stupid Britney video!" („Lad dir das Video von der dummen Britney herunter!" oder „Sensation. New Video – make haste to look!" („Sensation. Neues Video. Schau es dir schnell an!"). Auch Pamela Anderson, Michael Jackson oder vermeintliche Foltervideos der CIA werden als Lockmittel eingesetzt. Klickt der Empfänger auf den angegebenen Link – der häufig als Yahoo oder Google-Link getarnt ist – wird er auf eine präparierte Webseite geleitet. Wird die dort hinterlegte .exe-Datei geöffnet, installiert sich ein Trojanisches Pferd auf dem Rechner, das weitere Schädlinge nachlädt. Diese spionieren unter anderem private Daten aus oder löschen Systemdateien von Windows. Empfänger sollten keinesfalls den Links folgen, sondern solche Mails umgehend löschen.

Das BSI warnte vor kurzem vor E-Mails, die Empfänger mit vermeintlichen Haus-Gewinnen in die Schadsoftware-Falle locken wollen.
In der Nachricht heißt es, die Zeitschrift Haus & Bau verlose zum 25-jährigen Jubiläum ein Traumhaus im Wert von 250.000 Euro. Wenn man dem angegebenen Link folge, könne man am Gewinnspiel teilnehmen. Klickt man jedoch auf den Link und öffnet die auf der Webseite zum Download angebotene exe-Datei, installiert sich schädliche Software auf dem Rechner. Die Betreffzeilen der Mails lauten unter anderem „Mahnung" oder „Ihre Bank Überweisung", auch die Absenderadressen variieren. Empfänger sollten keinesfalls dem Link folgen und die Mail umgehend löschen. Außerdem sollte die Virenschutzsoftware auf dem aktuellen Stand gehalten und die Firewall aktiviert werden.

Aus systematischen Gründen werden zum einem ähnliche Fragen wieder gestellt, um die aktuellen Vergleichszahlen für 2007 zu erhalten, sowie anderseits neue Fragen, um Antworten auf die angesprochenen Problemstellungen zu erhalten.

Die unterzeichneten Abgeordneten richten daher an den Bundesminister für Verkehr, Innovation und Technologie nachstehende

Anfrage

1. Wie viele Beschwerden über „Spam-Mails" wurden 2007 an das BMVIT herangetragen?
   Wie viele Anzeigen wurden erstattet?
   Wie viele dieser Beschwerden betrafen Spam-Mails (Absender bzw. Server) aus anderen Ländern (Aufschlüsselung auf Länder)?

2. Haben Sie Informationen von welchen Servern die meisten Spam-Mails stammen?
   Wenn ja, von welchen (Aufschlüsselung nach Ländern)?

3. Wie vielen dieser Beschwerden wurde 2007 durch das BMVIT konkret nachgegangen und diese in Zusammenarbeit mit den Fernmeldebehörden anderer Länder grenzüberschreitend verfolgt?

4. Welche konkreten Ergebnisse liegen dazu vor?
   Welche behördlichen Maßnahmen wurden durch die zuständigen Fernmeldebehörden jeweils ergriffen?
   In welchen Fällen andere zuständige Behörden verständigt?
   Wie viele Anzeigen wurden 2007 durch die österreichische Fernmeldebehörde erstattet?

5. Wie viele wurden wegen Aussichtslosigkeit **nicht** weiter verfolgt (Aufschlüsselung jeweils auf Länder bzw. Fernmeldebehörden)?

6. Haben sich der vereinbarte Datenaustausch und die grenzüberschreitende Verfolgung diesbezüglicher Beschwerden zumindest 2007 aus Sicht des BMVIT bewährt?
   Wie funktionierte bei der Spam-Bekämpfung die grenzüberschreitende Zusammenarbeit mit den Behörden anderer EU-Mitgliedsstaaten?
   Wenn ja, welche Erfolge wurden konkret gemeinsam mit diesen anderen Fernmeldebehörden erreicht?

7. Was ergab eine inhaltliche Analyse dieser Spam-Mails?
   Welche Produkte und Dienstleistungen werden und wurden 2007 mit Spam-Mails angeboten?
   Wie viele davon waren Onlinewett- und Glückspielangebote?

8. Welche Länder waren von diesen Spam-Beschwerden betroffen?
   Wo befanden sich in diesen Fällen die Server?

9. Wie und unter welchen Voraussetzungen können Spammer (Spamversender) zurzeit in Österreich rechtlich verfolgt werden?
   Halten Sie die bestehenden Sanktionen für ausreichend?

10. Sehen Sie zur Bekämpfung von Spam-Mails einen zusätzlichen legislativen Handlungsbedarf in Österreich?
    Wenn ja, worin liegt dieser?

11. Sehen Sie zur Bekämpfung von Spam-Mails einen legislativen Handlungsbedarf in der EU?
    Wenn ja, worin liegt dieser?
    Was ist zurzeit auf europäischer Ebene dazu geplant?

12. In welchen Mitgliedsstaaten der EU ist „Spamming" mit Verwaltungsstrafen oder Pönalen bedroht?
    Welche konkreten Sanktionen gibt es?
    Gibt es Änderungen zur diesbezüglichen Antwort in der AB 224/XXIII.GP (Aufschlüsselung der Staaten und der jeweiligen Sanktionen)?

13. In welchen Mitgliedsstaaten der EU ist Spamming mit gerichtlichen Strafen bedroht?
    Welche konkreten Sanktionen gibt es?
    Gibt es Änderungen zur diesbezüglichen Antwort in der AB 224/XXIII.GP (Aufschlüsselung der Staaten und der jeweiligen Sanktionen)?

14. In welchen Mitgliedsstaaten der EU können auch die Unternehmen, die durch die Spam-Mails letztendlich wirtschaftlich profitieren (Werbung, Verkauf etc.) rechtlich zur Verantwortung gezogen werden?
    Welche Sanktionen sind jeweils vorgesehen?

15. Wie hoch schätzen Sie den volkswirtschaftlichen Schaden durch Spam-Mails für Österreich?

16. Teilen auch Sie die Auffassung, dass es sich bei Spamming um einen „Untergrundwirtschaftszweig" handelt und es dabei um „Verbrechen und Verbrechensbekämpfung" geht?
    Wenn nein, warum nicht?

17. Was empfehlen Sie aktuell Internet-UserInnen in Österreich zur Spamabwehr?
    Welche Maßnahmen sollen ergriffen werden?

18. Welche konkreten Maßnahmen werden Sie nun vorschlagen, um das Spam-Aufkommen in Österreich zu senken bzw. effektiv zu bekämpfen?

19. In welcher Form werden Sie der Aufforderung der EU-Kommission nachkommen, energisch gegen Spam, Spy- und Malware vorzugehen?
    Welche Maßnahmen sind für 2008 geplant?

20. Wie beurteilt das Ressort die in der Einleitung zitierte Umfrage der WKÖ?
    Welche Schlussfolgerungen zieht das Ressort daraus?

21. Wie viele gerichtliche Strafanzeigen wurden in diesem Zusammenhang (z.B. bei Spams in Form von Phising-Mails) von den Fernmeldebüros und der RtR 2005, 2006 und 2007 erstattet (Aufschlüsselung auf Jahre, Fernmeldebüros und RtR)?

22. Wie beurteilen Sie die im Einleitungstext dargestellten Beispiele von Spam-Mails (und Schädlingen)?

23. Wer hat in Österreich die Aufgabe, die Internet-UserInnen über die Risiken von Spam-Mails zu informieren?

24. Gibt es vergleichbare Einrichtungen wie das BSI oder Bürger-CERT?
    Wenn nein, warum nicht?

25. Mit welchen IT-Sicherheitsunternehmen wird seitens Ihres Ressorts zusammen gearbeitet?