3910/AB XXIII. GP

Eingelangt am 21.05.2008

BM für Verkehr, Innovation und Technologie

Anfragebeantwortung

GZ. BMVIT-12.000/0007-I/PR3/2008 DVR:0000175

An die
Präsidentin des Nationalrates
Mag.[a] Barbara Prammer

Parlament
1017 W i e n

Wien, am 21. Mai 2008

Sehr geehrte Frau Präsidentin!

Die schriftliche parlamentarische Anfrage Nr. 3931/J-NR/2008 betreffend Spam-Mails – Strategien zur Bekämpfung, die die Abgeordneten Mag. Johann Maier am 25. März 2008 an mich gerichtet haben, beehre ich mich wie folgt zu beantworten:

Frage 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)?

Antwort:
Die Ausforschung des tatsächlichen Versenders ist für die Fernmeldebehörden oft nicht möglich. Der Ursprung der Mails wird durch Manipulation der Header entsprechend verschleiert. Hier darf auf die Ausführungen in der Beantwortung der Anfrage Nr. 223/J-NR/2007, 224/AB XXIII.GP und auf jene zu Frage 2 verwiesen werden. Insofern stellen die Angaben über die vermeintlichen Ursprungsländer lediglich auf die übermittelten Header und die dort ersichtlichen echten oder gefälschten Informationen ab. Teilweise erfolgte die Zuordnung auch anhand der beworbenen Homepage über eine Abfrage des registrierten Inhabers der Domain. Angaben über den Ursprung aller angezeigten Mails sind nicht möglich.

Österreichweit, im örtlichen Wirkungsbereich aller vier in Österreich als Verwaltungsstrafbehörden zur Vollziehung des § 107 TKG 2003 zuständigen Fernmeldebüros, wurden im Jahr 2007 355 Anzeigen, davon 107 gegen ausländische Versender erstattet.

Die ausländischen Versender stammten insbesondere aus Belgien, der Türkei, Argentinien, der Schweiz, Hongkong, Kanada, dem amerikanischen Bereich (insbesondere USA), Ukraine, Mexiko, Brasilien, den Philippinen, China, Antigua und Barbuda, Japan, Brasilien, Israel, Korea, Russland, Marokko, Ungarn, Frankreich, Slowakei, den Niederlanden und Deutschland. Oftmals ist die wahre Herkunft der Mails auf Grund gefälschter IP-Adressen nicht feststellbar.

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

Antwort:
Abgesehen von der „Kurzlebigkeit" der verwendeten IP-Adresse handelt es sich zumeist um solche von gehackten Rechnern, sodass der tatsächliche Versender meist nicht ausforschbar ist. Aufgrund der Tatsache, dass der Großteil der Anzeiger die unerwünschten Mails nur weiterleitet, stehen die für die Ausforschung notwendigen Header nicht zur Verfügung. Wird eine Email weitergeleitet, verschwinden die im Hintergrund befindlichen Header-Informationen der weitergeleiteten Email und werden durch die Informationen des Anzeigeerstatters ersetzt. Da die Header auch entsprechend oft manipuliert sind, können keine gesicherten Angaben über die zur Versendung von Spam-Mails verwendeten Server gemacht werden. Zu den vermutlichen Standorten der Server/PCs, von denen Spam-Mails versendet werden, darf auf die Beantwortung der Frage 1 verwiesen werden.

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

Antwort:
Es wurde bzw. wird allen Beschwerden/Anzeigen nachgegangen.

Eine grenzüberschreitende Zusammenarbeit mit anderen Behörden bei der Verfolgung von aus dem Ausland stammenden Mails konnte aus Gründen der Wirtschaftlichkeit, Zweckmäßigkeit und Sparsamkeit nicht erfolgen, da der Großteil der ausländischen Mails nicht aus dem EU-Raum stammt und somit eine weitere Verfolgung, Vollstreckung oder entsprechende Hilfestellung durch die in Frage kommenden Behörden nicht zu erwarten war.

Frage 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?

Antwort:
Es konnten österreichweit 81 Strafen verhängt und 23 Ermahnungen ausgesprochen werden. Die übrigen Verfahren wurden entweder aus den in Antwort zu Frage 5 dargelegten Gründen nicht weiter verfolgt, endeten mit Einstellung oder sind noch anhängig.

Von der Verständigung ausländischer Behörden bzw. der Erstattung von Anzeigen an ausländische Behörden wurde aus den zu Frage 1 dargelegten Gründen abgesehen. Siehe dazu auch Antwort auf Fragen 3 und 5.

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

Antwort:
Mit Ausnahme jener Anzeigen, die Mails aus Deutschland betrafen, wurden bezüglich der übrigen Länder folgende Anzeigen wegen Aussichtslosigkeit nicht weiter verfolgt: Fernmeldebüro für Oberösterreich und Salzburg: 25, Fernmeldebüro für Steiermark und Kärnten: 17, Fernmeldebüro für Tirol und Vorarlberg: 1, Fernmeldebüro für Wien, Niederösterreich und Burgenland: 64. Zur Länderaufschlüsselung siehe Antwort zu Frage 1.

Frage 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?

Antwort:
Siehe dazu auch die Ausführungen zu Frage 3.
Eine formelle grenzüberschreitende Zusammenarbeit erfolgte bis dato hinsichtlich der Vollziehung der verhängten Geldstrafen im Zusammenhang mit Spam nur mit Deutschland. Diese hat sich bestens bewährt.

Auf europäischer Ebene beschäftigt sich das CNSA (Netzwerk der Spam Bekämpfungsbehörden) mit der Entwicklung und Verbesserung von Verfahren der grenzüberschreitenden Zusammenarbeit und dem Austausch bewährter Praktiken. Europaweit gesehen hat diese Zusammenarbeit bereits in einigen Fällen Erfolge gebracht.

Frage 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?

Antwort:
Beworben wurden: diverse Warenangebote (HiFi-Produkte, Haushaltsgeräte, Fahrzeuge, Kleidung, Medikamente, Uhren, Software usw.), diverse Dienstleistungsangebote (Finanz- und Bankdienstleistungen, Erotik- und Kontaktdienste, Jobbörsen etc.). Rund 50 Spam-Mails betrafen Glückspielangebote.

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

Antwort:
Ich darf hiezu auf meine Ausführungen zu den Fragen 1 und 2 verweisen.

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

Antwort:
In Österreich ist die Verfolgung von Spammern im Rahmen eines Verwaltungsstrafverfahrens wegen einer Übertretung des § 107 iVm § 109 TKG 2003 möglich. Voraussetzung dafür ist das Vorliegen eines strafbaren Sachverhaltes. Diesen haben die Fernmeldebehörden von Amts wegen zu ermitteln. Eine Beschwerde/Anzeige stellt ein Indiz für das Vorliegen dar. Hier sind die Behörden natürlich auf die Mitarbeit der Anzeiger angewiesen, um zu klären, ob nicht in der einen oder anderen Form doch eine Zustimmung zum Erhalt einer angezeigten Werbeemail vorliegt.

Gerade die Ermittlung des jeweils entscheidungsrelevanten Sachverhaltes wirft in der Praxis häufig Probleme auf, da die Intention der AnzeigerInnen zumeist die sofortige Veranlassung der Einstellung weiterer Zusendungen durch die Behörde ist. Ein über die Anzeigeerstattung hinausgehender Zeitaufwand wird von den meisten als unzumutbar angesehen oder hält schon im Vorhinein von einer Beschwerde/Anzeige ab. Aus diesem Grund kommt es mangels des für eine Bestrafung notwendigen gesicherten Nachweises der Übertretung immer wieder zu einer Einstellung der eingeleiteten Verfahren.

Die bestehenden Sanktionen sind ausreichend. Als eher problematisch ist das Fehlen entsprechender Amtshilfe- und Verwaltungsübereinkommen zu sehen, das die Durchführung von Verwaltungsstrafverfahren gegen ausländische Versender und damit die Verhängung der vorgesehenen Sanktionen erschwert bzw. unmöglich macht. Über die allfälligen Auswirkungen des EU-Verwaltungsvollstreckungsregimes können noch keine Angaben gemacht werden.

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

Antwort:
Österreich hat durch die Regelung in § 107 TKG 2003 die Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation umgesetzt und gewährleistet damit aus rechtlicher Sicht ein hohes Schutzniveau. Unmittelbarer legislativer Handlungsbedarf in Österreich besteht nicht.

Frage 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?

Antwort:
Die Auswirkungen des EU-Verwaltungsvollstreckungsgesetzes bleiben abzuwarten. Gegebenfalls wären weitergehende Regelungen zur grenzüberschreitenden Verfolgung notwendig.

Die Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation sieht in ihrem Art. 13 bereits jetzt sehr strenge Bestimmungen gegen die Zusendung von Spam vor.

Derzeit wird auf europäischer Ebene die Überprüfung des EU Telekommunikations-Rechtsrahmens (review) behandelt. Im Zuge dessen wird auch der oben erwähnte Art. 13 überarbeitet, wobei das derzeit geltende Grundprinzip des „opt-in“ sicherlich beibehalten wird, da es aus rechtlicher Sicht das höchste Schutzniveau bietet.

Unter Vorsitz der Europäischen Kommission beschäftigt sich, wie bereits zu Frage 6 erwähnt, das CNSA (Netzwerk der Spam Bekämpfungsbehörden) mit der Entwicklung von Verfahren der grenzüberschreitenden Zusammenarbeit und dem Austausch bewährter Praktiken.

Die Schwierigkeiten bei der Spam Bekämpfung haben ihre Ursache jedoch nicht in mangelhaften rechtlichen Regelungen, sondern in den vielfältigen technischen Möglichkeiten und deren höchst professioneller Nutzung durch die Spammer.

So wird beispielsweise über sog. „Bot-.Netze“ (Computer, die durch das Einschleusen spezieller Software „ferngesteuert“ werden können) Spam von Rechnern versendet, deren Nutzer gar nichts davon wissen.

Eine weitere Methode, die die Identifizierung der Herkunft von Spam beinahe unmöglich macht, ist das sog. „Fast Flux hosting“, bei dem die Spam Server (IP-Adresse) dutzende Male binnen weniger Minuten wechseln und die Domains „offshore“ registriert sind. Durch diese und viele ähnliche Methoden wird es für handelnde Behörden äußerst schwierig die tatsächliche Herkunft von Spam zuverlässig zu bestimmen.

Abgesehen davon besteht ein grundsätzliches Verfolgungsproblem schon allein aufgrund des Umstandes, dass der überwiegende Teil von Spam nicht aus dem EU- Raum selbst kommt und damit einer innereuropäischen Verfolgung entzogen ist. In diesem Zusammenhang gilt es, wie auch im Rahmen des CNSA versucht wird, auf internationaler/globaler Ebene eine Verständigung mit den Staaten zu suchen, die als Spam Quellenländer gelten. Legistische Maßnahmen ausschließlich auf EU-Ebene können dieses Problem nicht ausreichend lösen.

Fragen 12 und 13, 14:
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)?

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)?

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?

Antwort:
Ich verweise auf meine Ausführungen in der AB 224/XXIII.GP.

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

Antwort:
Der volkswirtschaftliche Schaden durch Spammails für Österreich kann seriöser Weise nicht exakt beziffert werden. Auch die Wirtschaft selbst kann dazu keine fundierten Aussagen treffen.

Ungeachtet konkreter Zahlen steht außer Frage, dass es sich um ein globales Problem handelt, dem energisch begegnet werden muss.

Eine im Auftrag der europäischen Kommission erstellte Studie von Ferris Research (2005) kam zu dem Ergebnis, dass die durch Spam entstehenden Kosten 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 zu veranschlagen sind.

Frage 16:
Teilen auch Sie die Auffassung, dass es sich bei Spamming um einen „Untergrundwirtschafts-zweig" handelt und es dabei um „Verbrechen und Verbrechensbekämpfung" geht? Wenn nein, warum nicht?

Antwort:
Das aus Österreich versendete Spamaufkommen betrifft nach den Erfahrungen der Vollziehungsbehörden identifizierbare Versender aus dem Unternehmensbereich, die zumeist wegen mangelnder Information über die Rechtslage aktiv wurden und nach Durchführung eines Verwaltungsstrafverfahrens ihre diesbezügliche Tätigkeit – manchmal auch nur auf Grund einer bloßen Ermahnung - eingestellt haben.

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

Antwort:
Grundsätzlich ist ein sorgsamer, wohl überlegter Umgang mit dem Medium Internet notwendig. So ist von der unüberlegten Preisgabe persönlicher Daten im Internet dringend abzuraten. Für allfällige Registrierungen auf Internet Seiten sollten “alias“ Adressen oder sog. „Free mail“ Adressen verwendet werden.

Überdies sollte der Computer durch eine auf aktuellem Stand gehaltene Anti-Virensoftware sowie eine „Firewall“ und einen Spamfilter vor unerwünschten Zugriffen geschützt werden.

In diesem Zusammenhang darf auch auf entsprechende Informationen auf der Internetseite meines Ressorts (www.bmvit.gv.at/telekommunikation/Internet/spam.html), sowie die Broschüre „Information betreffend unerwünschte Werbung mittels elektronischer Post“ von der meinem Wirkungsbereich unterstehenden Rundfunk- und Telekom Regulierungs- GmbH hingewiesen werden (www.rtr.at/de/tk/faq120). (Siehe dazu auch Antwort zu Frage 23)

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

Antwort:
In Österreich wurden bereits alle im Einklang mit der Datenschutzrichtlinie für elektronische Kommunikation zu treffende Maßnahmen umgesetzt. Weiters hat die Rundfunk- und Telekom Regulierungs GmbH, die meinem Wirkungsbereich untersteht, die Broschüre „Information betreffend unerwünschte Werbung mittels elektronischer Post (Spam)“ erarbeitet und auf ihrer Website veröffentlicht (www.rtr.at/de/tk/faq120). Damit stehen für jedermann umfassende Informationen sowohl über die Vermeidung als auch über das richtige Verhalten für von Spam Betroffene zur Verfügung.

Auch die österreichischen Internet Service Provider tragen mittels einer freiwilligen Selbstverpflichtung (Spam Code of Conduct, www.ispa.at/coc/), in der geregelt ist, wie ISPs mit Spam in ihren Netzen verfahren, dazu bei, das Spam Aufkommen bei ihren Kunden gering zu halten.

Frage 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?

Antwort:
In Österreich wird Spam schon bisher im Rahmen des Möglichen effektiv verfolgt. Es bestehen dazu klare rechtliche Vorgaben. Das grundsätzliche Problem stellt jedoch der bereits dargelegte Umstand dar, dass Spam nur in Ausnahmefällen in Österreich selbst generiert wird. Dies ist jedoch eine zentrale Voraussetzung für eine Erfolg versprechende Strafverfolgung durch österreichische Behörden.

Hinsichtlich der Notwendigkeit einer stärkeren internationalen Zusammenarbeit darf ich auf die Beantwortung der Fragen 9 und 11 verweisen.

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

Antwort:
Wie aus den bisherigen Ausführungen ersichtlich wird, ist Spam ein Problem, das nicht durch einzelstaatliche Maßnahmen oder rechtliche Regelungen allein in den Griff zu bekommen ist. Vielmehr ist ein stetiges Zusammenwirken folgender Faktoren erforderlich:

- adäquater rechtlicher Rahmen (siehe Antwort zu Frage 10 und 11)
- Schaffung von Problembewusstsein bei den Nutzern (Information über technische und rechtliche Möglichkeiten der Spam Bekämpfung)
- Verbreitung technischer Mittel zur Spam Bekämpfung (i.d.R. bieten Betreiber ihren Kunden entsprechende Software an)
- Selbstregulierungsmaßnahmen (z.B.: „code of conduct“ der österreichischen ISP’s zur gemeinsamen Spam Bekämpfung)
- Entwicklung von Verfahren der grenzüberschreitenden Zusammenarbeit und dem Austausch bewährter Praktiken

Der Umstand, dass der Schutz vor Spam-Mails das mit Abstand wichtigste Thema für österreichische Unternehmen im Zusammenhang mit IT Fragen darstellt zeigt, dass bei den Unternehmen ein Problembewusstsein vorhanden ist. Dies ist im Hinblick auf das vorhin Erwähnte ein wichtiger Punkt.

Die Schaffung angemessener rechtlicher Regeln im Bereich der unerbetenen elektronischen Kommunikation stellt einen Balanceakt zwischen wirtschaftlichen Interessen der Unternehmen einerseits und dem Recht auf Schutz der Privatsphäre und Datenschutz andererseits dar. Die Umfrage der WKÖ zeigt erfreulicherweise deutlich, dass dieser Balanceakt offensichtlich gelungen ist (72,6% wollen Erstkontakt zum Kunden per e-mail, 85,2% halten geltende Regeln für angemessen).

Im Hinblick auf den Punkt Schaffung von Problembewusstsein wird die Initiative des E-Centers der WKÖ zur Aufklärung im Zusammenhang mit Spam und IT - Sicherheit begrüßt.

Frage 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)?

Antwort:
Durch die Fernmeldebüros wurden in den genannten Jahren keine Strafanzeigen erstattet.

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

Antwort:
Die im Einleitungstext erwähnten Beispiele von Spam und Schädlingen zeigen, dass die Problematik in vielen Bereichen weit über den verwaltungsstrafrechtlichen Horizont des Telekommunikationsgesetzes hinausgeht. Es handelt sich dann nicht mehr „nur“ um die Zusendung unerbetener Nachrichten, sondern mitunter um strafrechtlich relevante

Tatbestände wie z.B. Betrug oder Datenmissbrauch. Ersichtlich wird auch, wie hoch professionell die Spammer ihre Methoden weiter entwickeln und damit zusehends die Verfolgung erschweren.

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

Antwort:
Spam tangiert unterschiedliche Bereiche wie den Datenschutz, den Konsumentenschutz, das Telekommunikationsrecht sowie das Strafrecht. Informationen sind daher in Österreich über verschiedene Wege erhältlich.

Selbstregulierung hat in diesem Bereich einen hohen Stellenwert. So tragen die österreichischen Internet Service Provider mittels einer freiwilligen Selbstverpflichtung, in der geregelt ist, wie ISPs mit Spam in ihren Netzen verfahren, dazu bei, das Spam Aufkommen bei ihren Kunden gering zu halten.

Der Wunsch nach Informationen zur sicheren Nutzung des Internet in Österreich ist hoch. Auf diesen Bedarf reagierte die Bundesregierung mit einer Informationsoffensive und setzte dabei auf die Zusammenarbeit mit Saferinternet.at (www.saferinternet.at). Saferinternet.at wird vom Österreichischen Institut für angewandte Telekommunikation (ÖIAT) in Kooperation mit dem Verband der Internet Service Provider Austria (ISPA) koordiniert und in Zusammenarbeit mit der öffentlichen Hand, NGO´s und der Wirtschaft umgesetzt. Neben kostenlosen Unterrichtsmaterialien zum Erkennen und Vermeiden von "Abzock-Angeboten" im Internet werden die wichtigsten "10 Tipps für Konsumenten im Internet" vorgestellt. Weiters sind viele praktische Informationen zur sicheren Internetnutzung ab sofort auch auf help.gv.at veröffentlicht.

Ich weise überdies nochmals auf die bereits erwähnten Informationsangebote auf der Homepage meines Ressorts sowie der RTR GmbH hin.

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

Antwort:
CERT.at ist das österreichische nationale CERT (Computer Emergency Response Team), das im März 2008 den Probebetrieb aufgenommen hat. CERT.at ist eine Initiative von „nic.at“, der österreichischen Domain - Registrierungsstelle.

Die klassischen Aufgaben eines Computer Emergency Response Teams sind mit denen der Feuerwehr vergleichbar: Es geht primär um die Behandlung sicherheitsrelevanter Störfälle (Analyse, Gegenmaßnahmen, Nachbereitung), aber auch um vorbeugende Maßnahmen wie z.B. Früherkennung, Vorbereitung für Notfälle, Öffentlichkeitsarbeit und Beratungen.

Als nationales CERT hat CERT.at kein Durchgriffsrecht auf die Netzwerkinfrastruktur Österreichs und kann daher bei Störfällen nur koordinierend und beratend aktiv werden.

CERT.at wird Österreich in den relevanten Bereichen repräsentieren und als zentraler Ansprechpartner für die CERTs anderer Länder fungieren. Die effektive Behandlung von so eingehenden Meldungen wird den jeweils lokalen Sicherheitsteams von ISPs und Firmen überlassen, wobei natürlich CERT.at diesen gerne beratend zur Seiten stehen wird. Die Rolle von CERT.at ist hier primär die einer Informationsdrehscheibe.

Bei Angriffen auf Rechner auf nationaler Ebene koordiniert CERT.at und informiert die jeweiligen Netzbetreiber und die zuständigen lokalen Security Teams.

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

Antwort:
Wir arbeiten abhängig von den jeweiligen IKT-Projekten mit österreichischen IT-Sicherheitsunternehmen, wie z.B. dem BRZ, Siemens oder Devoteam Consulting GmbH zusammen.

Mit freundlichen Grüßen

Werner Faymann