BEKÄMPFUNG VON SPAM

Ratgeber zum Datenschutz 9

Datenschutz und Informationsfreiheit in Berlin

Herausgeber:
Berliner Beauftragter für Datenschutz und Informationsfreiheit

Verantwortlich:
Volker Brozio
Redaktion:
Laima Nicolaus

An der Urania 4-10, 10787 Berlin
Tel.: (030) 1 38 89 0
Fax.: (030) 2 15 50 50
Internet: www.datenschutz-berlin.de
Email: mailbox@datenschutz-berlin.de

Grafik Design: www.studiohiggins.com

Berlin

EINLEITUNG

Wer ein E-Mail-Konto bzw. eine E-Mail-Adresse besitzt, macht täglich die Erfahrung, dass neben der per E-Mail abgewickelten Korrespondenz ein großer Teil der empfangenen Nachrichten aus unangekündigter, in der Regel auch unerwünschter Werbung (SPAM) besteht. Vor allem aufgrund der Menge dieser Nachrichten stellt SPAM eine Belastung dar, von der eine Gefährdung der Nutzbarkeit des E-Mail-Systems ausgeht.

In technischer Hinsicht lässt sich derzeit nicht verhindern, dass unerwünschte Werbung unter falschen Absender- und Betreff-Angaben versandt wird. Aber selbst bei korrekten Angaben wird es trotz einer Reduzierung von SPAM nicht auszuschließen sein, dass einzelne E-Mails unerwünscht zum Adressaten gelangen.

In rechtlicher Hinsicht sind durch SPAM neben dem datenschutzrechtlichen Verstoß, der in der unberechtigten Nutzung von E-Mail-Adressen für den Versand unerwünschter Werbung besteht, vor allem wettbewerbsrechtliche Fragen berührt. Eine Verfolgung etwaiger Verstöße ist jedoch in der Mehrzahl der Fälle nicht möglich, da der Absender von SPAM unerkannt bleiben kann.

Neben den technischen und rechtlichen Aspekten wird Sie vor allem interessieren, wie Sie praktisch mit der großen Menge unerwünschter E-Mails fertig werden. Im WWW finden Sie dazu Hinweise von Datenschutzinstitutionen, Verbraucherschützern, Interessenvertretungen der IT-Wirtschaft und aus dem universitären Bereich. Wir haben auf Grundlage dieser Veröffentlichungen sowie unserer Erfahrungen die aus unserer Sicht wichtigsten Empfehlungen sowohl zum Versand als auch zum Empfang von E-Mails für Sie zusammengestellt.

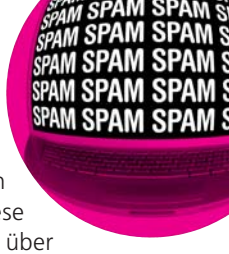
1. EMPFEHLUNGEN ZUM VERSAND VON E-MAILS

Wenn Sie E-Mails versenden, sollten Sie sich neben den gesetzlichen Vorgaben auch an den Regeln der „Netiquette“ orientieren, die keinesfalls veraltet sind: Es kommt weniger darauf an, welche Informationen Sie gerne versenden möchten, denken Sie bitte vielmehr darüber nach, welche Ihrer Informationen welchen Empfänger interessieren. Fassen Sie sich kurz; achten Sie auf die Reaktionen des Empfängers auf Ihre vorherigen E-Mails: Will er wirklich mehr?

Falls Sie sich entschließen, Informationen regelmäßig per E-Mail an mehrere Personen zu verteilen, lassen Sie sich die Einwilligung von jedem einzelnen Empfänger geben. Tragen Sie die Empfänger-Adressen niemals in das „To:“-Feld („An:“) Ihres E-Mail-Programms ein, sondern in das „BCC:“-Feld („Blindkopie an:“). Auf diese Weise können die Empfänger die Adressen der anderen Empfänger Ihrer E-Mail nicht feststellen.

Falls Sie regelmäßig bzw. geschäftsmäßig E-Mails an einen großen Empfängerkreis senden, legen Sie mit Hilfe von Newsletter-Software oder entsprechenden Angeboten Ihres Internet-Providers E-Mail-Listen an. Schützen Sie diese Daten vor unberechtigtem Zugriff. Machen Sie sich mit den Regelungen des Bundesdatenschutzgesetzes (BDSG) vertraut, insbesondere mit den technischen und organisatorischen Maßnahmen (§ 9 BDSG und Anlage). Der Versand eines E-Mail-Newsletters stellt gleichzeitig ein Telemedium im Sinne des Telemediengesetzes (TMG) dar. Machen Sie sich daher auch mit den Datenschutzregelungen dieses Gesetzes vertraut. Darüber hinaus sind die Bestimmungen des Gesetzes gegen den unlauteren Wettbewerb (UWG; hier insbesondere § 7) zu beachten.

Um bei einer größeren Menge von Adressaten den Überblick zu behalten und den Anforderungen des TMG, BDSG und des UWG zu genügen, sollten Sie E-Mail-Adressen nicht mit einfacher E-Mail-Software verwalten. Empfehlenswert ist die Verwendung von Newsletter-Software, die gleichzeitig eine Verwaltung der Einwilligung von Adressaten in den Empfang Ihres Newsletters ermöglicht. Beim derzeitigen Stand der Technik wird dies am besten durch ein Double-Opt-In-Verfahren gewährleistet: Wenn eine E-Mail-Adresse für den Empfang eines E-Mail-Newsletters eingegeben wurde, wird zunächst eine E-Mail an diese Adresse versandt, die eine Information über die Registrierung der Adresse, den Zweck der Speicherung, einen Hinweis darauf, dass die Einwilligung in den Empfang jederzeit widerrufen werden kann, und eine Beschreibung, wie dies einfach geschehen kann, enthält. Erst wenn der Empfänger diese E-Mail bestätigt, erhält er den angeforderten E-Mail-Newsletter regelmäßig.



Wenn Sie diese datenschutzrechtlichen Hinweise beachten, minimieren Sie das Risiko, sich dem Vorwurf auszusetzen, SPAM zu versenden. Sie vermeiden Ärger und vor allem Kosten, die durch Verstöße gegen das Datenschutz- und das Wettbewerbsrecht entstehen können. Zudem ist es empfehlenswert, sich im eigenen Interesse beim Versand von E-Mails dem Empfänger gegenüber so zu verhalten, wie man es als Empfänger von E-Mails selbst erwartet.

2. EMPFEHLUNGEN FÜR DEN EMPFANG VON E-MAILS

Wie reagiert man jedoch am besten, wenn das eigene Postfach mit E-Mails von Absendern gefüllt ist, die sich keinesfalls so rücksichtsvoll verhalten, wie man es selbst beim Versand von E-Mails wäre? Was kann man tun, um die Menge an unerwünschten E-Mails, die man erhält, möglichst gering zu halten?

Wenn Sie in der Presse oder im Internet Artikel über SPAM lesen, insbesondere über die Menge, in der unerwünschte E-Mails versandt werden, gewinnen Sie sicherlich den Eindruck, dass man nichts tun kann. Ein Blick in das eigene E-Mail-Postfach bestätigt zudem häufig diesen Eindruck.

UND TATSÄCHLICH IST DERZEIT
DIE BESTE REAKTION AUF SPAM:
NICHTS TUN!

Ignorieren Sie die vielen E-Mails, in denen Sie aufgefordert werden, Medikamente zu bestellen, Attachments mit angeblich wichtigen technischen oder juristischen Informationen anzuklicken, Ihre PIN und TAN in WWW-Formulare Ihrer Bank einzugeben oder in eine relativ geringe finanzielle Vorleistung zu treten, um an einem Millionengewinn beteiligt zu werden. Die Medikamente sind entweder gefälscht, überteuert oder werden von Ihnen nicht gebraucht, Systemadministratoren und Staatsanwaltschaften senden Ihnen wichtige Informationen nicht als Attachment, Ihre Bank fordert Sie nicht per E-Mail auf, Ihre PIN und TAN irgendwo einzugeben, und nach Überweisung der finanziellen Vorleistung für den Millionengewinn hören Sie nie wieder etwas von dem Absender.

Ignorieren Sie alle E-Mails, die Sie nicht interessieren oder die Ihnen seltsam vorkommen. Falls Sie dies schon am Betreff oder am Absender feststellen können, löschen Sie die E-Mail am besten ungelesen. Wenn Sie nicht sicher sind, nehmen Sie Kontakt mit dem Absender auf. Benutzen Sie dazu am besten das Telefon oder schreiben Sie einen Brief. Auf keinen Fall sollten Sie eine verdächtige E-Mail per E-Mail beantworten. Wenn es keinen anderen Weg gibt, den Absender zu erreichen, stimmt meist etwas nicht.

Seien Sie gegenüber dem Inhalt und der Angabe des Absenders misstrauisch. Die Absenderadresse ist nicht nur, wie häufig zu lesen ist, leicht zu fälschen – sie ist im E-Mail-Programm frei wählbar. Ignorieren Sie alle E-Mails, bei denen Sie nicht prüfen können, ob sie wirklich vom vermeintlichen Absender stammen.

Verzichten Sie auch auf die Weiterleitung von Kettenbriefen. Die meisten sind üble Scherze, die darauf abzielen, massenhaft versandt das E-Mail-System zu stören. Ausführliche Informationen zu solchen „Hoaxes" finden Sie auf den WWW-Seiten der Technischen Universität Berlin unter http://www2.tu-berlin.de/www/software/hoax.shtml. Ignorieren Sie auch diese E-Mails.

3. HINWEISE ZUR BEKÄMPFUNG VON SPAM

Wir können nachvollziehen, dass Sie sich über den Aufwand für das Abrufen und das Aussortieren unerwünschter E-Mails ärgern. Und wir wissen, dass es Ihnen nicht genügt, die E-Mails zu ignorieren. Wir wollen wie Sie gegen die datenschutzrechtlichen Verstöße der Spammer vorgehen: Nicht nur, weil wir dafür zuständig sind, sondern vor allem, weil wir überzeugt sind, dass es sich bei der Verarbeitung einer E-Mail-Adresse für unerwünschte Werbung auf Kosten des Empfängers um eine für den Betroffenen besonders ärgerliche Form des datenschutzrechtlichen Verstoßes handelt – und bei der Verwendung der E-Mail-Adresse zu betrügerischen Zwecken umso mehr. Was können Sie also tun, wenn Sie gegen SPAM vorgehen wollen?

Schritt 1: E-Mails vollständig lesen lernen

Wenn Sie sich entschieden haben, rechtlich gegen den Versand von SPAM vorzugehen, kommen Sie nicht darum herum, die unerwünscht erhaltene E-Mail zu analysieren, vor allem um festzustellen, woher diese versandt wurde. Ein datenschutzrechtlicher Verstoß kann in der Regel nur dann verfolgt werden, wenn die E-Mail aus einem Staat der Europäischen Union oder einem Land mit vergleichbaren Datenschutzregelungen kommt. Auch um festzustellen, ob der Versand gegen weitere lokale Regelungen des Herkunftslandes verstößt, und um festzustellen, welche Behörden für die Verfolgung der Verstöße zuständig sind, sollten Sie zumindest einen Anhaltspunkt für die Herkunft der E-Mail haben.

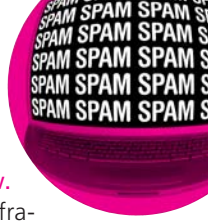
Dies setzt allerdings voraus, dass Sie die E-Mail zum Lesen öffnen. Wenn Sie dies tun, sollten Sie alle Maßnahmen getroffen haben, die Ihren Computer vor unberechtigten Manipulationen schützen, die durch das Lesen der E-Mail ausgelöst werden können: Das Betriebssystem und die Software zum Lesen von E-Mails sollten mit allen verfügbaren Sicherheits-Updates aktualisiert worden sein, Sie sollten ein Anti-Viren-Programm mit mindestens tagesaktuellen Informationen über bekannte Computerviren („Viren-Signaturen") aktiviert haben, das Sie beim Öffnen von E-Mails und Da-

teien vor Risiken warnt, und Sie sollten – da auch der beste Virenschutz nicht perfekt ist – eine Sicherheitskopie Ihrer Dateien angefertigt haben. Wir empfehlen außerdem, den Computer für die Zeit der Analyse vom Internet zu trennen, um keine in der E-Mail versteckten Empfangsbestätigungen zu versenden. Erst wenn diese Voraussetzungen gegeben sind, sollten Sie das Wagnis eingehen, die E-Mail mit Ihrem E-Mail-Programm zu öffnen und die „Kopfzeilen" („Header") der E-Mail zu analysieren, indem Sie sich die Kopfzeilen der E-Mail alle vollständig anzeigen lassen. Wenn Sie die Option nicht finden, gibt es in einigen E-Mail-Programmen auch die Möglichkeit, den „Quelltext" der E-Mail anzeigen zu lassen.

Vor dem Inhalt der E-Mail sehen Sie viele Zeilen, die ein kurzes Stichwort, einen Doppelpunkt und dann einen meist langen Eintrag enthalten. Aus den Zeilen, die mit „Received:" beginnen, kann man schließen, über welche E-Mail-Server die Nachricht weitergeleitet wurde, wobei die unterste Zeile zuerst und die oberste zuletzt hinzugefügt wurde. Sie finden im Internet Anleitungen, wie diese Informationen ausgewertet werden können, um die Herkunft einer E-Mail festzustellen.

Da einige dieser Zeilen gefälscht sein können und die Analyse einige Erfahrung voraussetzt, ziehen Sie am besten jemanden zu Rate, der sich damit auskennt. Umgekehrt heißt das: Wenn Sie sich wegen einer E-Mail, die wahrscheinlich einen rechtlichen Verstoß darstellt, an eine Behörde oder eine andere Institution wenden, senden Sie bitte immer die gesamten Kopfzeilen der E-Mail mit; ansonsten ist eine Analyse der E-Mail-Herkunft nicht möglich.

Lesen Sie die E-Mail auch ansonsten sorgfältig durch: Gibt es Hinweise darauf, dass unabhängig von der Herkunft der E-Mail für ein Produkt, eine Dienstleistung oder ein sonstiges Angebot einer bestimmten Firma geworben wird, stellen Sie nach Möglichkeit fest, wo diese Firma ihren Sitz hat. Neben einer Recherche mit einer WWW-Suchmaschine stehen Ihnen dazu auch die „Whois"-Datenbanken im Internet zur Verfügung: Wenn Sie ein berechtigtes Interesse haben zu erfahren, welche Firma oder Institution eine deutsche Domain (z. B. „datenschutz-berlin.de") reserviert hat, können Sie unter http://www.denic.de/de/whois/index.jsp eine Abfrage bei der deutschen Registrierungsstelle „DENIC eG" durchführen. Für internationale Domains finden Sie entsprechende Informationen beispielsweise unter http://www.internic.net/whois.html. Es ist davon auszugehen, dass die beworbene Firma zumindest den Versand der E-Mail an Ihre Adresse veranlasst hat, so dass anzunehmen ist, dass Ihre E-Mail-Adresse dort gespeichert und verarbeitet wird.



Es gibt allerdings auch Fälle, in denen Dritte Werbe-E-Mails im Namen von Firmen oder Institutionen versenden, denen sie schaden wollen. Opfer solcher „Joe-Jobs" sind häufig Aktivisten oder Organisationen, die gegen den Versand von SPAM vorgehen. Spammer versenden gerne in deren Namen eine große Menge unerwünschter E-Mails, damit sie nicht dazu kommen, gegen Spammer vorzugehen, sondern sich selbst des Vorwurfs erwehren müssen, Urheber dieser E-Mails zu sein.

Auch sind Absenderadressen von E-Mails, die einen Computervirus oder andere Schadsoftware wie Würmer oder Trojaner enthalten, fast immer gefälscht. Heutige Computerwürmer, die sich per E-Mail verbreiten, analysieren das Windows-Adressbuch des „infizierten" Computers und entnehmen diesem Adressbuch nicht nur Adressen, an die sie E-Mails weiter versenden, die denselben Wurm als Attachment enthalten, sondern entnehmen dem Adressbuch zusätzlich die Adressen, die sie als vermeintliche Absender der E-Mails einsetzen.

Am häufigsten werden Sie jedoch feststellen, dass die Herkunft der E-Mail nicht feststellbar ist oder dass die E-Mail aus einem Land kommt, das den Versand von SPAM nicht verfolgt. In diesem Fall besteht die einzige Möglichkeit darin, die E-Mail zu ignorieren und ansonsten präventive Maßnahmen gegen den SPAM-Empfang zu treffen, die weiter unten beschrieben werden.

Schritt 2: Den Absender kontaktieren

Stellt sich heraus, dass der Absender feststellbar und sogar erreichbar ist, schreiben Sie ihm. Verlangen Sie gemäß § 34 BDSG Auskunft über die zu Ihrer Person gespeicherten Daten, die Herkunft dieser Daten, Empfänger oder Kategorien von Empfängern, an die Daten weitergegeben werden oder wurden, und den Zweck der Speicherung. Beziehen Sie sich dabei ausdrücklich auf die Werbe-E-Mail und geben Sie Ihre E-Mail-Adresse an. Widersprechen Sie einer Nutzung oder Übermittlung Ihrer Daten für Zwecke der Werbung oder der Markt- oder Meinungsforschung gemäß § 28 Absatz 4 BDSG. Verlangen Sie auf Grundlage von § 35 Absatz 2 BDSG die Löschung Ihrer Daten unverzüglich nach Erteilung der geforderten Auskunft. Setzen Sie dem Unternehmen eine Frist. Angemessen sind zwei Wochen.

Wenn Sie die E-Mail als Unternehmer an eine geschäftlich genutzte Adresse erhalten haben, lassen Sie sich beraten, wie Sie wettbewerbsrechtlich gegen den Versand dieser E-Mails vorgehen können.

Um Kontakt mit dem Versender von SPAM aufzunehmen, antworten Sie auf keinen Fall auf die SPAM-E-Mail. Meist erhalten Sie eine Fehlermeldung, dass Ihre Antwort nicht zustellbar ist. Außerdem bestätigen Sie gegenüber Spammern, die nicht vorhaben, auf Ihr Auskunftsbegehren zu antworten oder Ihre Daten zu löschen, dass die E-Mail-Adresse gültig ist und dass Sie Ihre E-Mails lesen. Sie erreichen nichts, außer dass der Wert Ihrer E-Mail-Adresse beim Verkauf an andere Spammer mehr einbringt als eine unbestätigte E-Mail-Adresse.

Klicken Sie auch nicht auf einen ggf. in der E-Mail vorhandenen Link zum Abbestellen der E-Mails. Dies können Sie tun, wenn Sie einen Newsletter bestellt haben und eine E-Mail zur Bestätigung erhalten. Auch wenn Sie diesen Newsletter später abbestellen wollen, können Sie den entsprechenden Link anklicken. Falls Sie jedoch eine E-Mail unaufgefordert erhalten haben, die mit einem Link zum Abbestellen versehen ist, bestätigen Sie durch das Anklicken des Links in der Regel nur gegenüber dem Spammer, dass Sie die E-Mail erhalten und gelesen haben – siehe oben.

Wenn Sie vorhaben, zum Schein auf die Angebote der Spammer einzugehen, sollten Sie sehr genau wissen, was Sie tun. Es entspricht nicht jedermanns Geschmack, beispielsweise der seit Jahren im Bereich betrügerischen E-Mail-Versands tätigen „Nigeria Connection" nachzujagen (siehe dazu http://www2.tu-berlin.de/www/software/hoax/419.shtml und http://www.419eater.com/)

Schritt 3: Den Absender zur Reaktion zwingen

Reagiert der Absender auf Ihre Aufforderung, indem er sich für den Fehler entschuldigt, Ihnen die erwünschten Auskünfte erteilt und Ihre E-Mail-Adresse aus seinem Verteiler löscht, können Sie dies als Erfolg verbuchen. Im Zweifelsfall wird der Absender zukünftig nicht nur Sie verschonen, sondern hat sich nun etwas genauer mit den rechtlichen Bestimmungen beschäftigt und versendet seine E-Mails nur an Adressaten, die wirklich in den Empfang eingewilligt haben. Wir haben die Erfahrung gemacht, dass dies gar nicht so selten vorkommt.

Häufiger jedoch reagiert der Absender nicht auf Ihr erstes Schreiben. Verlieren Sie dann nicht zu viel Zeit. Wenn Sie meinen, dass ein Verstoß gegen das Wettbewerbsrecht vorliegt, wenden Sie sich, wenn die E-Mail Sie auf Ihrer privaten E-Mail-Adresse erreicht hat, per E-Mail an das Aktionsbündnis SPAM (beschwerdestelle@spam.vzbv.de) des „Verbraucherzentrale Bundesverbandes e.V." (http://www.vzbv.de/), das dieser in Zusammenarbeit mit dem Verband der deutschen Internetwirtschaft e.V. (eco: http://www.eco.de/) und der Zentrale zur Bekämpfung des unlauteren Wettbewerbs e.V. („Wettbewerbszentrale" WBZ: http://www.wettbewerbszentrale.de/) betreibt. Wenn Sie die unerwünschte Werbung als Unternehmer an eine geschäftlich genutzte E-Mail-Adresse erhalten haben, wenden Sie sich am besten direkt an die Wettbewerbszentrale.

Wegen etwaiger Verstöße gegen datenschutzrechtliche Bestimmungen wenden Sie sich an die jeweilige Aufsichtsbehörde für den Datenschutz im privaten Bereich. Die zuständige Stelle hängt vom Bundesland ab, in dem das Unternehmen, das für die E-Mail verantwortlich ist, seinen Sitz hat. Eine Liste aller Aufsichtsbehörden finden Sie auf unseren WWW-Seiten in der Rubrik „Adressen".

Schritt 4: Den Ausgang abwarten

Manchmal haben wir bei der Verfolgung von datenschutzrechtlichen Verstößen, die eine Grundlage für den Versand von SPAM bilden, Erfolg. Das ist meist der Fall, wenn ein Berliner Unternehmen unerwünschte E-Mails versendet, weil den Verantwortlichen die Rechtslage unbekannt ist oder sie darauf vertrauen, dass ein Verstoß nicht verfolgt wird. Dann wird der Versand von SPAM eingestellt und das Verfahren zum Versand von E-Mails so geändert, dass es den rechtlichen Anforderungen genügt. Manchmal muss ein Unternehmen mit einem Ordnungswidrigkeitenverfahren rechnen, insbesondere bei wiederholten Verstößen gegen das Datenschutzrecht.

Häufig jedoch fällt das Ergebnis unserer Nachforschungen mager aus: Wenn sich der Urheber von SPAM doch nicht einwandfrei feststellen lässt, das Unternehmen inzwischen nicht mehr existiert oder wenn sich kein datenschutzrechtlicher Verstoß nachweisen lässt. Es kommt auch vor, dass ein Unternehmen bei der Reservierung einer Internet-Domain eine Adresse in Berlin angibt und dort nicht einmal mit einem Briefkasten vertreten ist.

In diesen Fällen bleibt Ihnen und uns nur zu hoffen, dass dem Spammer beim nächsten Mal ein Fehler unterläuft, der zu einem befriedigenderen Ergebnis führt.

4. PRÄVENTIVE MASSNAHMEN ZUR ABWEHR VON SPAM

Es gibt eine Vielzahl einfacher Maßnahmen, mit denen Sie das Risiko deutlich reduzieren können, dass Ihre E-Mail-Adresse von Spammern missbraucht wird. Die wichtigsten davon möchten wir Ihnen nennen; weitere finden Sie im Internet, insbesondere auf WWW-Seiten zum Thema SPAM.

1. Seien Sie geizig bei der Herausgabe Ihrer E-Mail-Adresse. Geben Sie die Adresse so selten wie möglich weiter. Tragen Sie Ihre E-Mail-Adresse nicht in Formulare ein, wenn es sich vermeiden lässt. Geben Sie Ihre E-Mail-Adresse auf keinen Fall in zweifelhafte WWW-Seiten ein, die Ihnen die Teilnahme an nicht näher spezifizierten Gewinnspielen oder Ähnliches versprechen. Geben Sie auch nicht die E-Mail-Adresse von Freunden und Bekannten in WWW-Formulare ein, die unter dem Vorwand, freundliche oder lustige Grußbotschaften zu versenden, zum Sammeln von E-Mail-Adressen eingerichtet wurden – Ihre Freundschaften bleiben dann länger erhalten.

2. Veröffentlichen Sie Ihre E-Mail-Adresse auch nicht ohne weiteren Schutz auf WWW-Seiten. Ersetzen Sie z.B. das „@"-Zeichen in der Adresse, das Spammern hilft, die Adresse auf WWW-Seiten automatisiert mit Hilfe von Software zu suchen, durch den Begriff „(at)" oder durch die Kodierung „@". Etwas sicherer ist das Ersetzen aller Buchstaben der E-Mail-Adresse durch eine kleine Bilddatei, die den gesamten Schriftzug der E-Mail-Adresse zeigt.

3. Legen Sie sich mehrere E-Mail-Adressen zu. Verwenden Sie eine Adresse für Kontakte mit Freunden, Behörden und seriösen Unternehmen. Verwenden Sie andere E-Mail-Adressen, die keinen direkten Bezug zu Ihrem Namen zulassen, wenn Sie nicht sicher sind, ob Ihre E-Mail-Adresse nicht zweckentfremdet benutzt wird. Wechseln Sie diese Adressen gelegentlich. Solange es kostenlose E-Mail-Adressen gibt, belastet diese Maßnahme noch nicht einmal Ihr Konto. Es gibt auch Internetangebote (z.B www.trashmail.net oder www.spamgourmet.com), die sich auf Wegwerf-E-Mail-Adressen spezialisiert haben, die nur eine festge-

legte Zeit gültig sind oder nur eine festgelegte Anzahl E-Mails weiterleiten. Bei manchen Diensten können Sie über eine Browsererweiterung komfortabel jedes Mal eine neue Wegwerf-E-Mail-Adresse erstellen, wenn Sie sie irgendwo auf einer Webseite eintragen müssen. Auf diese Weise behalten Sie zudem den Überblick und können u.U. nachweisen, dass eine Firma Ihre E-Mail-Adresse weitergegeben hat.

4. Seien Sie misstrauisch gegenüber E-Mail-Inhalten und -Absendern. Klicken Sie kein Attachment und keinen Link an, wenn Sie nicht absolut sicher sind, dass es sich weder um eine Malware noch um eine E-Mail mit betrügerischem Hintergrund handelt, die Sie zur Herausgabe von Informationen verleiten soll („Phishing"-E-Mail). Beantworten Sie zweifelhafte E-Mails nicht, sondern schreiben Sie einen Brief oder rufen Sie den angeblichen Absender an – allerdings nicht über eine ggf. angegebene besonders teure Mehrwertdienste- oder Mobilfunknummer. Unterschätzen Sie die Intelligenz und den Einfallsreichtum von E-Mail-Betrügern und Spammern auf keinen Fall.

5. Halten Sie Ihren Computer frei von nicht vertrauenswürdiger oder schädlicher Software. Computerviren und Trojaner werden heute häufig mit dem Ziel programmiert, den „infizierten" Computer zum ferngesteuerten SPAM-Versand oder zum Angriff auf Server im Internet nutzen zu können. Zudem gibt es Software, die speziell dafür programmiert wurde, Ihr Nutzerverhalten, Ihre Kennwörter oder Ihre E-Mail-Adresse auszuforschen. Gelegentlich installieren Sie solche Software selbst, wenn Sie kostenlose Software zweifelhafter Herkunft installieren und dabei das „Kleingedruckte" nicht aufmerksam lesen. Benutzen Sie Software zur Erkennung von „Adware" und Software zum Erkennen von Computerviren, „Trojanern" und anderer „Malware". Aktivieren Sie eine „Firewall" und halten Sie das Betriebssystem und jede andere installierte Software, insbesondere den Webbrowser, laufend auf dem neuesten Stand. Falls Sie diese Begriffe und die technischen Hintergründe nicht verstehen, informieren Sie sich zumindest grundlegend über das Thema Computersicherheit. Einen guten Einstieg bieten hier die WWW-Seiten des Bundesamtes für Sicherheit in der Informationstechnik (BSI: http://www.bsi-fuer-buerger.de/), des Virtuellen Datenschutzbüros (http://www.datenschutz.de/technik/) und der Datenschutzbeauftragten des Bundes und der Länder.

6. Nehmen Sie sich die Zeit, Ihre Software datenschutzgerecht zu konfigurieren, bevor Sie sie benutzen. Insbesondere E-Mail-Programme sind häufig geradezu fahrlässig und datenschutzwidrig vorkonfiguriert: Beispielsweise gelingt es Spammern, über winzige, in E-Mails eingebettete Bilder, die beim Lesen der E-Mail von einem Server heruntergeladen werden, den Empfang bzw. das Lesen der E-Mail sekundengenau nachzuvollziehen. Daher sollte die Funktion, Bilder in E-Mails automatisch zu laden, deaktiviert werden. Auf keinen Fall sollte es Spammern möglich sein, ein Programm in die E-Mail zu integrieren, das beim Lesen der E-Mail automatisch gestartet wird. Leider ist beispielsweise die Funktion, „Java-Script"-Programme in E-Mails automatisch zu starten, in einigen E-Mail-Programmen nach der Installation aktiviert und muss manuell deaktiviert werden. Auch die HTML-Vorschau auf E-Mails und die Aktivierung von Scriptsprachen und PlugIns in E-Mails können im Zusammenhang mit fehlerhafter E-Mail-Software zum Einschleusen von Schadsoftware führen, teilweise ohne dass die E-Mail geöffnet und gelesen werden muss. Übrigens sind nicht alle Betriebssysteme und E-Mail-Programme in gleichem Maße anfällig für Sicherheitsprobleme. Im Internet finden Sie viele Hinweise zu diesem Thema, die vielleicht dazu führen, dass Sie zukünftig eine andere Software als bisher für die Internet- und E-Mail-Nutzung bevorzugen werden.

7. Da es sich kaum ganz vermeiden lässt, dass Spammer in den Besitz Ihrer E-Mail-Adresse gelangen, können Sie Ihre E-Mails mit Hilfe spezieller Software automatisch filtern lassen. Das kann sowohl auf einem E-Mail-Server geschehen – einige Provider bieten diesen Dienst kostenlos an, andere lassen sich diesen Dienst fürstlich entlohnen und verdienen so auf legale Weise am hohen SPAM-Aufkommen mit – als auch auf Ihrem Computer: Moderne E-Mail-Software bietet eine „Filter"-Funktion, und es gibt Software, die E-Mail-Software um „Filter"-Funktionen ergänzt. Seien Sie

sich dabei allerdings bewusst, dass es schon Menschen zum Teil schwerfällt, erwünschte und unerwünschte bzw. seriöse und unseriöse E-Mails zu unterscheiden. Umso schwieriger ist es für Software, deren Bewertung Sie daher hinterfragen sollten. Schlimmer als das Übersehen unerwünschter Software ist dabei das unerwünschte Aussortieren wichtiger E-Mails – die Software sollte vermeintlich unerwünschte E-Mails daher besser automatisch in einem besonderen Postordner speichern, statt sie automatisch zu löschen.

5. FAZIT: WAS TUN?

Solange es keine geeigneten Mittel gibt, um den Versand von beim Empfänger unerwünschten E-Mails zu verhindern oder zumindest das Risiko zu minimieren, ist es lediglich möglich, die eben beschriebenen präventiven Maßnahmen anzuwenden, um möglichst wenig SPAM zu empfangen. Die unerwünschten Nachrichten, die trotzdem ankommen, sollten ignoriert und gelöscht werden. Nur wenn Aussicht auf Erfolg besteht, kann man versuchen, den Versand von SPAM wegen der in diesem Zusammenhang begangenen wettbewerbsrechtlichen und datenschutzrechtlichen Verstöße zu verfolgen.

Dazu bedarf es einiger Anstrengung und Ausdauer; und es bedarf des Gleichmuts, wenn das Ergebnis der Anstrengung im Einzelfall unbefriedigend sein sollte. Bei der Entscheidung, ob sich der Versuch lohnt, den Missbrauch Ihrer E-Mail-Adresse zum Versand unerwünschter E-Mails zu unterbinden, sind wir Ihnen gerne mit unserem Rat behilflich.

Herausgeber:
Berliner Beauftragter für Datenschutz und Informationsfreiheit

Verantwortlich:
Volker Brozio
Redaktion:
Laima Nicolaus

An der Urania 4-10, 10787 Berlin
Tel.: (030) 1 38 89 0
Fax.: (030) 2 15 50 50
Internet: www.datenschutz-berlin.de
Email: mailbox@datenschutz-berlin.de

Grafik Design: www.studiohiggins.com

Stand: Juli 2008