Neue Juristische Wochenschrift

In Verbindung mit dem Deutschen Anwaltverein

und der Bundesrechtsanwaltskammer herausgegeben von *Dr. Wolfgang Ewer,* Rechtsanwalt in Kiel – *Prof. Dr. Rainer Hamm,* Rechtsanwalt in Frankfurt a. M. – *Dr. Georg Maier-Reimer,* Rechtsanwalt in Köln – *Prof. Dr. Rudolf Nirk,* Rechtsanwalt beim BGH – *Prof. Dr. Hans-Jürgen Rabe,* Rechtsanwalt in Berlin – *Ingeborg Rakete-Dombek,* Rechtsanwältin und Notarin in Berlin – *Dr. Michael Streck,* Rechtsanwalt in Köln.

Schriftleitung: Rechtsanwalt *Martin W. Huff* und Rechtsanwalt *Dr. Achim Schunder*
Beethovenstraße 7 b, 60325 Frankfurt a. M.

49 2004
Seite 3513–3592
57. Jahrgang
29. November 2004

Professor Dr. Thomas Hoeren, Münster

Virenscanning und Spamfilter – Rechtliche Möglichkeiten im Kampf gegen Viren, Spams & Co.*

Internetuser sind zunehmend frustriert ob der Flut von Spams und Viren, die sie jeden Tag zugesandt bekommen. Rechtlich ist klar, dass solche Attacken unzulässig sind. Doch wie sich dagegen wehren? Der folgende Beitrag zeigt auf, welche legalen Möglichkeiten bestehen, effektiv gegen Datensicherheitsangriffe vorzugehen.

I. Abwehr von Spams

Provider und Internetnutzer werden zunehmend von Fluten unerbetener und unerwünschter Werbe-Mails, so genannter Spam-Mails, überrollt. Mittlerweile soll es sich – mit weiter steigender Tendenz – bei über der Hälfte aller durchs Datennetz versandten Botschaften um Spams handeln[1]. Allein die Kosten für den Download im Jahr 2003 werden weltweit auf über 12 Mrd. Euro geschätzt[2]. Den Versendern, die ihre Werbung meist massenweise auf den Weg bringen, entstehen dabei nur geringe Kosten. Den Löwenanteil tragen die Provider, deren Infrastruktur in Anspruch genommen wird und die für die Spamabwehr finanziellen, zeitlichen und personellen Aufwand erbringen müssen. Spams stellen deshalb für Provider nicht nur eine Belästigung dar, sondern auch einen erheblichen wirtschaftlichen Faktor. Schließlich können Spam-Mails auch Viren, Würmer und andere Schadprogramme transportieren und damit ein nicht zu unterschätzendes Gefahrenpotenzial für die IT-Infrastruktur mit sich bringen. Auch für die Inhaber von Mail-Accounts bedeutet das Sichten ihrer Mailbox durch längere Online- bzw. Downloadzeiten ein (arbeits-)zeitintensives und kostenaufwändiges Ärgernis. Wird durch Spams die Speicherkapazität der Mailbox des Nutzers überschritten, so können selbst erwünschte Mails den Empfänger nicht mehr erreichen.

1. Technische Grundlagen

Für den Versand der Massenwerbung benutzen Spammer oft gezielt so genannte offene Relays, also Mailserver, die Mails beliebiger Absender zur Beförderung annehmen. Werden dabei Rechenanlagen von Hochschulen als Spam-Server missbraucht, nimmt dies nicht nur deren Ressourcen in Anspruch; werden die betroffenen Hochschulserver auf Black Lists gesetzt und weisen deshalb andere Server deren Mails ab, behindert dies auch aktiv den E-Mail-Verkehr der betroffenen Hochschule. Inzwischen beschränken viele Provider den Mail-Versand auf authentifizierte Absender. Spammer wiederum missbrauchen neuerdings vermehrt tatsächlich existierende Domains in Spam-Absenderadressen. Dies bedeutet nicht nur eine Rufbeeinträchtigung für die entsprechende Institution, weil Adressaten die Spams zunächst der Institution als vermeintlichem Absender zuschreiben. Zudem führen Unmengen an Rückläufern und Fehlermeldungen zu einer weiteren Belastung der Systeme bzw. im Extremfall zu einer Überlastung. Auch das Unabhängige Landeszentrum für Datenschutz (ULD), Schleswig-Holstein, war wiederholt vom Missbrauch seiner Domain in Spam betroffen[3]; unter dessen Adresse „www.datenschutzzentrum.de" wurden Spams, die teilweise den Wurm „Sobig.E" enthielten, verschickt, wobei nicht nur die „From:"-Adresse, sondern auch die „envelope"-from-Adresse gefälscht wurden und die Mails meist über nicht offiziell vergebene IP-Adressen ohne DNS-Eintrag versandt wurden, so dass eine Rückverfolgung nicht möglich war.

2. Rechtslage

a) *Abwehransprüche von Spam-Adressaten.* Spezielle Gesetze, die Spamming verbieten oder unter Strafe stellen, gibt es in Deutschland derzeit nicht. In den USA ist zum 1. 1. 2004 mit dem so genannten „Can Spam Act" ein Gesetz auf Bundesebene in Kraft getreten, das Geldstrafen bis zu 750 US-Dollar pro Spam-Mail bzw. eine Gefängnishöchststrafe von fünf Jahren vorsieht. Dabei geht die Regelung vom so genannten „Opt out"-Prinzip aus, wonach kommerzielle Mails erlaubt sind, solange der Empfänger einer Zusendung nicht widerspricht. Die Zulässigkeit der Spam-Mails ist aber an bestimmte Kriterien geknüpft, unter anderem die Erkennbarkeit als Werbung, die Angabe einer zutreffenden und gültigen Absenderadresse und die tatsächliche Ermöglichung des „opt out". Bereits bisher gab es in einigen US-Bundesstaaten Anti-Spam-Gesetze, allerdings mit unterschiedlichen Regelungsansätzen; dabei wurde in Kalifornien in 2003 erstmals eine Geldstrafe von 2 Mio. US-Dollar gegen zwei Unternehmer verhängt, die via Internet Computerprogramme und Bücher für Spammer sowie Listen mit E-Mail-Adressen zum Kauf angeboten haben und Mails ohne die gesetzlich vorgeschriebene gültige Absenderadresse verschickt haben[4].

In Deutschland hat sich zwischenzeitlich eine gefestigte Rechtsprechung entwickelt, nach der eine Zusendung von Werbe-Mails ohne vorherige Zustimmung des Adressaten

---

* Der Autor ist Direktor des Instituts für Informations-, Telekommunikations- und Medienrecht der Universität Münster.

1 *Bleich/Heidrich*, Die Spammung steigt, c't 17/2003, http://www.heise.de/ct/03/17/134/default.shtml.

2 eco, Spam, S. 2, http://www.eco.de.

3 Warnung: Spam und Würmer in gefälschten „Datenschutz-E-Mail" verschickt, 1. 7. 2003, http://www.datenschutzzentrum.de/material/themen/divers/spamwurm.htm.

4 http://www.urheberrecht.org/news/?id=1524&w=&p=1, Meldung v. 27. 10. 2003.

grundsätzlich rechtswidrig ist. Zu Grunde gelegt wird dabei der „Opt in"-Ansatz. Der private Empfänger unerwünschter Werbe-Mails kann wegen Verletzung seines allgemeinen Persönlichkeitsrechts Unterlassung (§§ 823 I, 1004 BGB) verlangen[5]. Gewerbetreibenden stehen Abwehransprüche wegen Eingriffs in den so genannten „eingerichteten und ausgeübten Gewerbebetrieb"[6] zu, unter Mitbewerbern auch wegen wettbewerbswidrigen Verhaltens[7].

Eine ausdrückliche Regelung – derzufolge unverlangte Werbesendungen wettbewerbswidrig sind – wurde in das inzwischen novellierte UWG aufgenommen (§ 7 II Nrn. 3 u. 4 UWG). Damit wird übereinstimmend mit der europäischen Datenschutzrichtlinie[8] eine „Opt in"-Lösung vorgesehen, die auch der bisherigen Rechtspraxis in Deutschland zu Grunde lag. Nach dem Gesetzentwurf gilt künftig jede Werbezusendung von Unternehmern als „unzumutbare Belästigung" und damit als wettbewerbswidrig, wenn der Empfänger nicht vorher zugestimmt hat; dies kann beispielsweise auch durch Anforderung eines Newsletters geschehen. Eine wichtige Ausnahme betrifft Kundenbeziehungen: Daten, die ein Unternehmer „in Zusammenhang" mit dem Verkauf einer Ware oder Dienstleistung erhält, darf er zur Direktwerbung für eigene ähnliche Waren oder Dienstleistungen verwenden; dies gilt, solange der Kunde nicht widerspricht (Opt out-Regelung).

Die Neuregelung entspricht damit weitgehend der bisherigen Rechtsprechung zu Spam-Mails. Auch wird sich die Rechtsstellung von betroffenen Privatpersonen, Hochschulen und Unternehmen nicht verändern, denn klagebefugt gegen wettbewerbswidrige Mails sind nur direkte Mitbewerber, Verbraucherverbände sowie die Industrie- und Handelskammern. In allen übrigen Fällen verbleibt es bei den oben genannten Rechtsschutzmöglichkeiten.

Auch Anbieter, die eine E-Card-Funktion zur Verfügung stellen, können nach mehreren zwischenzeitlich ergangenen Entscheidungen[9] als Mitstörer auf Unterlassung der Zusendung unerwünschter Spam-Mails in Anspruch genommen werden. Dies gilt auch für politische Parteien, wenn diese es auf ihren Webseiten beliebigen Dritten ermöglichen, elektronische Grußkarten zu versenden[10]. Die dem Dienst innewohnende Missbrauchsmöglichkeit müsse der Anbieter unterbinden, notfalls durch das Einstellen des Dienstes. Das *LG* Leipzig[11] schließlich bejahte selbst Unterlassungsansprüche gegen den Subdomain-Vermieter eines Spam-Versenders.

Bei Spam-Mails, die 0190-Dienste bewerben, ist nach der neuen Regelung in § 13 a TKV[12] auch der Netzbetreiber in die Pflicht genommen, der Kunden Mehrwertdienstenummern überlässt. Er ist gehalten, unter anderem auf das Verbot hinzuweisen, Werbung gesetzeswidrig zu übermitteln; dies betrifft auch unerbetene rechtswidrige Werbung, sprich Spams. Wird die vergebene Rufnummer dennoch rechtswidrig beworben, so muss der Netzbetreiber bei gesicherter Kenntnis von einem wiederholten oder schwerwiegenden Verstoß den Nummerninhaber zunächst abmahnen und bei Erfolglosigkeit die Rufnummer sperren. Von einer gesicherten Kenntnis ist nach Ansicht des *LG Köln*[13] auszugehen, wenn wiederholt Verstöße unter Angabe einzelner Rufnummern mitgeteilt werden.

b) *Ansprüche des Providers gegen Spammer.* Benutzt ein Spammer zur Versendung der Mails unberechtigt fremde Mail-Server, so kommen seitens des Providers Unterlassungs- und Schadensersatzansprüche in Betracht. Die Nutzung fremder Ressourcen und Rechnerkapazitäten stellt eine rechtswidrige und schuldhafte Eigentumsverletzung (§ 823 I BGB) jedenfalls dann dar, wenn der Mail-Server infolge des erhöhten Mail-Aufkommens nicht mehr bestimmungsgemäß funktioniert. Der Missbrauch des Mail-Servers kann auch einen Anspruch wegen betriebsbezogenen Eingriffs in den Gewerbebetrieb des Server-Betreibers begründen. Denkbar sind auch Ansprüche wegen vorsätzlich sittenwidriger Schädigung (§ 826 BGB) sowie aus § 823 II BGB, wenn Straftatbestände verwirklicht werden, die auch den Schutz des Providers bezwecken, beispielsweise das Erschleichen von Leistungen (§ 265 a StGB), eine Datenveränderung (§ 303 a StGB), Computersabotage (§ 303 b StGB) oder eine Störung von Telekommunikationsanlagen (§ 317 StGB).

c) *Missbrauch der Domain in Spam-Absenderadressen.* Häufig benutzen Spammer gefälschte Absenderangaben und missbrauchen dazu vermehrt auch tatsächlich existierende Domains. Damit wir unter anderem versucht, die Abwehrmaßnahmen von Mailhosts zu konterkarieren, die bei eintreffenden Mails die Absenderdomain verifizieren und anderenfalls als Spam markieren. Infolge des Missbrauchs erhält der vermeintliche Spam-Absender zahllose Rückläufer wie Fehlermeldungen von Mailservern, was im Extremfall zum Zusammenbruch der Mailserver führen kann[14]. Mit juristischen Mitteln kann kaum dagegen vorgegangen werden. Zum einen agieren die meisten Versender aus außereuropäischen Ländern und sind damit für die deutsche Justiz kaum greifbar[15]. Selbst gegen Täter in Deutschland, soweit diese überhaupt identifizierbar sind, bestehen nur wenige rechtliche Möglichkeiten. Eine Strafbarkeit käme – etwa bei Nutzung von Hochschuldomains in Spam-Absenderadressen – allenfalls als Computersabotage, § 303 b StGB, in Betracht. Allerdings setzt dies voraus, dass die Funktionsfähigkeit der Datenverarbeitungsinfrastruktur einer Behörde oder eines Unternehmens beeinträchtigt wird, also der Mailserver unter der Last der Rückläufer vorübergehend zusammenbricht. Der Strafrechtstatbestand des § 143 MarkenG schließlich greift nur in Wettbewerbsverhältnissen und damit in Fällen, in denen eingetragene Marken oder Geschäftskennzeichen im geschäftlichen Verkehr unerlaubt vorsätzlich in verwechslungsfähiger Art und Weise benutzt werden.

Im Übrigen existiert kein strafrechtlicher Schutz der Betroffenen. Diese sind auf zivilrechtliche Ansprüche und damit auf Unterlassungs- und Schadensersatzklagen verwiesen.

3. Gegenmaßnahmen

Im Kampf gegen Spam-Mails suchen Rechenzentren an Hochschulen und andere Provider ebenso wie Nutzer nach effektiven Gegenstrategien. Die Maßnahmen der Provider reichen von der Blockierung von Absenderadressen über die

5 St. Rspr., s. *OLG Koblenz*, MMR 2003, 590 = JurPC Web-Dok. 196/2003; *KG*, CR 2003, 291 = JurPC Web-Dok. 31/2003.

6 S. *KG*, NJOZ 2002, 2203 = JurPC Web-Dok. 362/2002; *LG Berlin*, NJW 2002, 2569 = MMR 2002, 631.

7 *LG München I*, MMR 2003, 758 = JurPC Web-Dok. 230/2003.

8 Art. 13 der Richtlinie für den Schutz persönlicher Daten und der Privatsphäre auf dem Feld der elektronischen Kommunikation (Richtlinie 2002/58/EG) vom 12. 7. 2002, umzusetzen bis 31. 10. 2003.

9 *LG München I*, MMR 2003, 483; *AG Hamburg*, Urt. v. 4. 3. 2003 – 36A C 37/03, http://www.trademarx.de/urteile/aghh36a_C_37_03.html.

10 S. *OLG München*, MMR 2004, 324; *AG Rostock*, NJW-RR 2003, 1282 = MMR 2003, 345; *LG München I*, NJW-RR 2003, 764.

11 *LG Leipzig*, Urt. v. 13. 11. 2003 – 12 S 2595/03, JurPC Web-Dok. 66/2004; ebenso *AG Leipzig*, MMR 2003, 610 = JurPC Web-Dok. 205/2003.

12 Eingeführt durch die 2. Verordnung zur Änderung der Telekommunikations-Kundenschutzverordnung (TKV) v. 20. 8. 2002.

13 *LG Köln*, MMR 2003, 676.

14 *Mansmann/Heidrich*, Mail-Überlauf, c't 21/2003, S. 58, http://www.heise.de/ct/03/21/058/.

15 BfD, 19. TB, 2001/2002, S. 74.

automatische Abweisung von Mails von offenen Relays oder Filtermaßnahmen bis zur Markierung nach Spam-Wahrscheinlichkeit und nachfolgender Zustellung oder auch Löschung.

Nicht alle Abwehrmethoden sind jedoch rechtlich unbedenklich. Zu differenzieren ist, wie beim Umgang mit vireninfizierten Mails, zwischen der Durchsuchung auf Spam-Merkmale (Filterung) und den weiteren Schritten wie dem Löschen, Blockieren oder Umleiten in spezielle Folder. Ebenso wie bei der Virenabwehr sind bei der Beurteilung der Zulässigkeit einzelner Maßnahmen die widerstreitenden Belange abzuwägen. Dabei kommen auf Seiten der Nutzer vor allem das Telekommunikationsgeheimnis, das Persönlichkeitsrecht und gegebenenfalls die Wissenschaftsfreiheit zum Tragen. Die unterschiedlichen Schutzziele der Virenabwehr und der Spam-Bekämpfung stecken den Rahmen für zulässige Maßnahmen ab. Deshalb können zur Virenabwehr weiter reichende Maßnahmen zulässig sein, weil es sich dabei um notwendige Maßnahmen des Datenschutzes und der Datensicherheit zur Abwehr akuter Gefährdungen der Daten und der TK-Infrastruktur handelt[16], während die Bekämpfung von Spam zumeist dem Schutz vor Belästigung und Ressourcenverbrauch dient.

a) *Zentrale Blockierung*. Bei der Blockierung werden Mails bestimmter IP-Bereiche, ganzer Domänen oder Mails von Servern, die auf so genannten Black Lists stehen, nicht zur Zustellung angenommen. In den Black Lists werden vor allem Mailserver geführt, die als offenes Relay nicht oder nicht ausreichend gegen Missbrauch geschützt sind oder deren Betreiber Spam passiv oder aktiv unterstützen. Die betreffenden Mails werden zum Teil gelöscht, zum Teil auch mit einer entsprechenden Fehlermeldung zurückgeschickt, wenn sie beispielsweise von offenen Relays stammen, die unter anderem von der ORDB, der Non-Profit-Organisation „Open Relay Database", geführt werden[17].

Ohne vorherige Zustimmung des Nutzers zu diesem Vorgehen ist eine zentrale Blockierung rechtlich problematisch. Grundsätzlich sind Provider bereits vertraglich verpflichtet, Mails – und damit auch Spam-Mails – zuzustellen. Schließlich kann der Empfänger auch ein Interesse am Erhalt einer Werbe-Mail haben; gerade im Hochschulbereich können Spams auch aus legitimem wissenschaftlichem Interesse erwünscht sein. Ferner ist nicht auszuschließen, dass die Blockierung auch seriöse Mitteilungen wie Rechnungen etc. erfassen kann, deren Nichtzustellung für den Adressaten nachteilig sein kann. Das Zurückschicken oder Löschen von Mails ohne vorherige Nutzerzustimmung[18] kann insbesondere einen strafbaren Eingriff in das Fernmeldegeheimnis bedeuten, § 206 II Nr. 2 StGB, jedenfalls, soweit in Unternehmen, Behörden oder Hochschulen den Beschäftigten und Studenten die private Nutzung erlaubt ist oder geduldet wird. Das Unterdrücken von Nachrichten, die für den Nutzer bestimmt sind, kann schließlich auch als Datenunterdrückung, § 303 a I Alt. 2 StGB, strafbar sein.

b) *Die Filterung*. Ziel einer Filterung ist es, anhand charakteristischer Merkmale die Nachricht als Spam zu identifizieren, um sie im nächsten Schritt beispielsweise zu löschen oder in spezielle Ordner zu verschieben. Eine Filterung ist bereits in tatsächlicher Hinsicht problematisch; aus rechtlicher Sicht sollte eine zentrale Filterung jedenfalls nicht ohne Einwilligung des Nutzers erfolgen.

Um Kennzeichen einer Spam-Mail auszumachen, werden entweder Absenderangaben nach bestimmten Domains oder IPs durchsucht oder Mail-Inhalte auf bestimmte Schlüsselwörter gecheckt. Da Adressangaben häufig gefälscht sind, bieten sie schon a priori kein brauchbares Filterkriterium. Eine zentrale inhaltliche Filterung läuft nicht nur dem Persönlichkeitsrecht der Betroffenen zuwider, sondern eignet sich auch tatsächlich kaum für eine effektive Spam-Erkennung. So kann schon durch einfache Änderungen (z. B. ersetzen von „for you" durch „4u" oder „Access for all" durch „xs4all"[19]) das Aussondern bestimmter Wörter leicht umgangen werden. Gerade in Institutionen wie Hochschulen mit breitem Fächerspektrum lassen sich kaum Schlüsselwörter definieren, die eindeutig nur auf Spam hinweisen und nicht in einer der Fakultäten wissenschaftlich von Belang sein können. Denn das Vorhandensein eines bestimmten Schlüsselworts sagt noch nichts über dessen Kontext aus. Solche Erfahrungen machten auch Abgeordnete des britischen Unterhauses, die infolge des Versuchs der Parlamentsverwaltung, unerwünschte und pornografische Werbebotschaften auszufiltern, Teile ihrer regulären Mail-Kommunikation nicht mehr erhielten, insbesondere als ein Gesetzentwurf über Sexualdelikte zur Diskussion stand[20]. Die Unzulänglichkeit wortbasierter Filter führte auch zu Protesten gegenüber amerikanischen Providern, die Nachrichten mit dem Wort „Breast(s)" sperren wollten – denn dadurch vereitelte der Wortfilter auch den Erfahrungsaustausch brustkrebskranker Frauen in einer Newsgroup[21] und unterdrückte gleichzeitig das Angebot von Kochrezepten über „chicken breast"[22].

Über die tatsächlichen Unzulänglichkeiten einer – insbesondere zentralen – textbasierten Filterung hinaus ist diese rechtlich unzulässig. Ohne ausdrückliche Einwilligung der Nutzer verbietet sich eine inhaltliche, stichwortbasierte Kontrolle von Mails als unzulässige Inhaltskontrolle aus datenschutzrechtlichen Gründen und als strafbare Verletzung des Telekommunikationsgeheimnisses, soweit eine private Mailnutzung gestattet ist[23].

c) *Zulässige Maßnahmen*. Vor dem Hintergrund des Fernmeldegeheimnisses, das Inhalte wie auch Verbindungsdaten vor Kenntnisnahme schützt, ist eine Filterung allenfalls zulässig, wenn sie automatisiert erfolgt und eine Kenntnisnahme auch durch Administratoren ausgeschlossen ist. Unbedenklich ist insoweit die Praxis, im automatisierten Verfahren[24] einer Mail eine (Punkt-)Bewertung ihrer Spam-Wahrscheinlichkeit zuzuordnen und diese Bewertung an den Mail-Header anzufügen. Im Gegensatz zur Veränderung oder Ergänzung der Subjektzeile begegnet ein automatisiertes Hinzufügen eines X-Headers sowohl datenschutzrechtlich als auch strafrechtlich keinen Bedenken, da jeder E-Mail ohnehin zumindest ihr Transport-Header hinzugefügt wird und die X-Header-Daten der Mail keinen anderen Informationsgehalt[25] bekommen und damit nicht i. S. des § 303 a StGB verändert werden.

Der weitere Umgang mit der Mail sollte nur mit Einwilligung – das heißt vorheriger Zustimmung – des Nutzers erfolgen. Dem User können beispielsweise Programme angeboten wer-

16 LfD Nordrhein-Westfalen, 16. TB, 2003, S. 101.
17 *Bleich/Heidrich* (o. Fußn. 1), c't 17/2003, http://www.heise.de/ct/03/17/134/default.shtml.
18 *Büchner*, in: *Büchner/Ehmer/Geppert*, Beck'scher TKG-Kommentar, 2. Aufl. (2002), § 85 Rdnr. 19.
19 *Hoeren/Sieber/Sieber*, Hdb. MultimediaR, Stand: Juni 2004, Teil 19, Rdnr. 152.
20 *Gundermann* (ULD Schleswig-Holstein), Großbritannien: Spam-Filter behindert Parlamentsarbeit, 5. 2. 2003, http://www.datenschutz.de/news/alle/detail/?nid=759.
21 *Hoeren/Sieber/Sieber* (o. Fußn. 19), Teil 19, Rdnr. 152.
22 *Hoeren/Sieber/Sieber* (o. Fußn. 19), Teil 19, Rdnr. 152.
23 *Hanau/Hoeren*, Private Internetnutzung durch Arbeitnehmer, 2003, S. 66; BfD, 19. TB, 2001/2002, S. 74.
24 BfD, 19. TB, 2001/2002, S. 74.
25 *Stree*, in: *Schönke/Schröder*, StGB, 26. Aufl. (2001), § 303 a Rdnr. 4 a. E.

den, die ihm ein Filtern nach selbstdefinierten Stichwörtern und Kriterien ermöglichen[26] und mittels derer er seine Mails je nach Ergebnis des Scanvorgangs in verschiedenen Foldern ablegen lassen oder ab einem bestimmten Schwellenwert auch automatisch löschen lassen kann. Auch können nach Nutzervorgaben einzelne Mail-Adressen, die bereits durch Spam-Versendung aufgefallen sind, blockiert und gelöscht werden[27]. Einem Nutzer, der die zur Verfügung gestellten Konfigurationsmöglichkeiten nicht wahrnehmen möchte, müssen selbst Spam-Mails vom Provider zugestellt werden, will dieser sich nicht Unterlassungs- und Schadensersatzansprüchen oder gar strafrechtlichen Konsequenzen aussetzen.

Nur derartige Lösungen, die auf einer umfassenden vorherigen Einwilligung des Nutzers beruhen und ihm die eigene Entscheidung überlassen, bei welchem Schwellwert er welche Aktion unternimmt, sind datenschutzrechtlich, zivil- und strafrechtlich unbedenklich. Allerdings sollten die Nutzer darüber informiert werden, dass bei der automatisierten Filterung immer auch das Risiko einer Fehlbewertung (false positives) besteht. So können unter Umständen auch seriöse Mails als Spam gekennzeichnet werden mit der Folge, dass der Absender irrtümlich für einen Spam-Versender gehalten wird und damit dessen Persönlichkeitsrechte beeinträchtigt werden.

II. Abwehr von Viren

Zum Schutz vor Viren und anderen Schadprogrammen führen TK-Betreiber regelmäßig ein Virenscanning durch. Dies wirft zunächst die Frage auf, ob und inwieweit eine zentrale, inhaltliche Überprüfung von E-Mails überhaupt zulässig ist. Besonderes Augenmerk ist weiter darauf zu richten, wie mit einer erkannt virenbehafteten Mail zulässigerweise verfahren werden darf.

Bei allen Maßnahmen sind die widerstreitenden Interessen sorgfältig abzuwägen. Auf der einen Seite muss die Datensicherheit gewährleistet und die IT-Systeme vor Schäden durch Viren geschützt werden. Über das Eigeninteresse des Anlagenbetreibers am Schutz seiner Systeme hinaus treffen ihn vertragliche und gesetzliche Pflichten, das Fernmeldegeheimnis und den Schutz personenbezogener Daten technisch und organisatorisch sicherzustellen; für Mailbox-Betreiber ergibt sich dies insbesondere aus § 89 TKG[28]. Schutzmaßnahmen dürfen jedoch andererseits das Fernmeldegeheimnis und das informationelle Selbstbestimmungsrecht der am Mailverkehr Beteiligten nicht außer Acht lassen. Im Hochschulbereich muss darüber hinaus die grundgesetzlich garantierte Wissenschafts- und Forschungsfreiheit berücksichtigt werden.

Beim Scanning und allen weiteren Maßnahmen der Virenabwehr ist zu bedenken, dass das Telekommunikationsgeheimnis jegliche Kenntnisnahme von Inhalten wie von Verbindungsdaten verbietet. Dies gilt jedenfalls dann, wenn den Beschäftigten in Unternehmen, Behörden und Hochschulen (und Studenten) die private Mailnutzung erlaubt ist[29]. Das TK-Geheimnis ist darüber hinaus für dienstliche wie private Nachrichten gleichermaßen zu berücksichtigen, wenn sich technisch der Eingang privater und dienstlicher Mails nicht trennen lässt, beispielsweise durch getrennte Mail-Adressen oder dadurch, dass die Privatnutzung nur über einen (kostenlosen) Free-Mail-Dienst zugelassen ist[30]. Eine Verletzung des TK-Geheimnisses ist über zivilrechtliche Ansprüche hinaus auch strafbar.

Überdies muss im Hinblick auf die dienstliche Nutzung bei Kontrollmaßnahmen – und damit auch für Logdateien eines Virenscanners – immer auch der Betriebsrat bzw. Personalrat zustimmen. Allerdings ist die Personalvertretung nicht befugt, den Zugriff auf private Mails und damit einen Eingriff ins Fernmeldegeheimnis zu gestatten.

1. Virenscanning

Bereits das Scannen von Mails muss so gestaltet sein, dass das Fernmeldegeheimnis gewahrt wird[31]. Unbedenklich ist ein Virenscanning von ein- und ausgehenden Mails[32] dienstlicher oder privater Natur, solange es automatisiert abläuft und keine Kenntnisnahme des Kontrollvorgangs oder -ergebnisses etwa durch Administratoren stattfindet[33]. Das zentrale Virenscanning stellt vielmehr eine notwendige Maßnahme der Datensicherheit dar, die interne Netze, Dateien und damit auch personenbezogene Daten gegen Angriffe von außen durch Viren, Würmer und Trojanische Pferde schützt[34]. Allerdings muss das Inhalts-Scanning auf fest definierte Virensignaturen begrenzt bleiben und darf ein Scanning nach frei wählbaren Stichwörtern nicht zulassen[35]. Ein Inhalts-Scan verstößt bei privaten Mails gegen das TK-Geheimnis; bei ausgehenden geschäftlichen Mails kommt es einer unzulässigen Verhaltens- und Leistungskontrolle gleich[36]. Jegliche Kenntnisnahme von Inhalten oder Verbindungsdaten privater Mails ist aber nur durch eine Einwilligung, das heißt eine vorherige Zustimmung des Nutzers, legitimierbar; dies gilt selbst für eine Identifikation der Herkunft der Mail durch den Systemadministrator[37]. Im Übrigen kann ein zentraler Virencheck die dezentrale Überprüfung durch den Nutzer nicht gänzlich ersetzen, da beim automatisierten Scan Viren in verschlüsselten Mails nicht erkannt werden und daher eine Prüfung erst nach Entschlüsselung beim Empfänger geboten ist[38].

Auch beim weiteren Umgang mit virenverseuchten Anlagen in Mails sind die genannten Aspekte sorgfältig abzuwägen. Um datenschutzrechtliche, straf- und zivilrechtliche Bedenken auszuräumen, muss das weitere Vorgehen bei auffälligen Mails sorgfältig abgewogen werden.

2. Löschen von Mails bzw. Mailanhängen

Problematisch ist es, virenverseuchte Mails ohne Abstimmung mit dem Mailadressaten zu löschen. Denn grundsätzlich liegt die alleinige Verfügungsbefugnis über Mails beim Nutzer eines Maildienstes. E-Mails dürfen diesem nicht – auch nicht zeitweilig – vorenthalten werden und auch nur entsprechend dem Vertrag mit dem Nutzer gelöscht werden[39].

Nicht abschließend geklärt ist, ob auch virenbehaftete Mails zugestellt werden müssen[40]. Die Datenschutzbeauftragten des Bundes und der Länder haben sich dafür ausgesprochen, dass aus Gründen der Datensicherheit Teilinhalte privater wie dienstlicher Mails oder Anlagen von Mails unterdrückt werden dürfen, die gefährlichen oder verdächtigen ausführbaren

26 BfD, 17. TB, 1997/1998, Nr. 10.2.13; BfD, 19. TB, 2001/2002, S. 74.
27 LfD Nordrhein-Westfalen, 16. TB, 2003, S. 20.
28 *Bizer*, Das Internetcafé im Jugendzentrum, http://medien-paedagogik.de/down/MD386.pdf, Nr. 3.1.3.
29 S. o. Fußn. 23 und die dortigen Belege.
30 Arbeitskreis (Ak) Technik der Konferenz der DSB des Bundes und der Länder, Orientierungshilfe zu Datenschutzfragen des Anschlusses von Netzen der öffentlichen Verwaltung an das Internet, Überarbeitete Fassung vom Mai 2000, abrufbar unter http://www.datenschutz-berlin.de/to/ak-tech.htm, Nr. 4.2.1.; *Däubler*, Internet und ArbeitsR, 2. Aufl. (2002), Rdnr. 238.
31 *Hanau/Hoeren* (o. Fußn. 23), S. 66; *Rieß*, in: *Roßnagel*, Recht der Multimediadienste, Stand: Juni 2003, Teil 6.4, Rdnr. 35.
32 So auch LfD Nordrhein-Westfalen, 15. TB, 2001, S. 21; Ak Technik (o. Fußn. 30), Nr. 4.2.1.
33 LfD Nordrhein-Westfalen, 16. TB, 2003, S. 100; Orientierungshilfe der 63. Konferenz zur datenschutzgerechten Nutzung von E-Mail und anderen Internetdiensten am Arbeitsplatz, Nr. III 2 c.
34 LfD Nordrhein-Westfalen, 16. TB, 2003, S. 101.
35 *Hanau/Hoeren* (o. Fußn. 23), S. 66; Ak Technik (o. Fußn. 30), Nr. 4.4.
36 Ak Technik (o. Fußn. 30), Nrn. 4.2.1 und 4.2.4 und 4.3.1.
37 *Schaar*, RDV 2003, 59 (60); Ak Technik (o. Fußn. 30), Nr. 4.2.1; Orientierungshilfe der 63. Konferenz der DSB (o. Fußn. 33), Nrn. II i, III 2 c; *Rieß*, in: *Roßnagel* (o. Fußn. 31), Rdnr. 35.
38 Ak Technik (o. Fußn. 30), Nr. 4.2.1.
39 *Bär*, Anm. zu *LG Ravensburg*, MMR 2003, 680.
40 Keine Zustellpflicht: *Rieß*, in: *Roßnagel* (o. Fußn. 31), Rdnr. 35.

Code enthalten (insb. html-Seiten als Mail-body, Dateien mit den Erweiterungen *.exe, *.bat, *.com oder gepackte Dateien wie *.zip, *.arj, *.lha)[41]. Allerdings muss diese Verfahrensweise ebenso wie der einzelne Zustellversuch virenbehafteter Mails den Mailempfängern zuvor bekannt gegeben sein.

Rechtsprechung zu diesem Problemkreis existiert noch nicht. Deshalb sollte vorsorglich, gerade im Hochschulbereich, wo es auch die Forschungsfreiheit zu berücksichtigen gilt, ein Procedere bevorzugt werden, das den Adressaten mit einbezieht. Ansonsten besteht beim Löschen von Mails ohne Einbeziehung des Nutzers nicht nur das Risiko einer Vertragsverletzung, sondern vor allem auch eines strafbaren Verstoßes gegen das Fernmeldegeheimnis (§ 206 II Nr. 2 StGB) sowie einer strafbaren Datenveränderung (§ 303 a StGB) durch Unterdrücken bzw. Unbrauchbarmachen von Daten, die für den Mailempfänger bestimmt sind.

3. Vorgehensweise unter Einbeziehung des Adressaten

Auch bei Maßnahmen der Datensicherheit gebietet der Grundsatz der Verhältnismäßigkeit, immer das am wenigsten einschneidende Mittel zu wählen. Deshalb sind, insbesondere im Hochschulbereich, Lösungen zu favorisieren, die den Mailadressaten in das weitere Vorgehen mit einbeziehen. Im wissenschaftlichen Kontext kann selbst der Erhalt virenbehafteter Mails von Interesse sein, der damit nicht von vornherein abgeschnitten wird.

Unzulässig ist jedenfalls die Praxis, dem Adressaten nach einer Mitteilung über den Eingang einer virenbehafteten Mail den Header nur auf Anfordern manuell weiterzuleiten. Denn mit dieser Vorgehensweise ist zwangsläufig eine Kenntnisnahme verbunden, die aber das Fernmeldegeheimnis strikt untersagt.

Einen zulässigen Weg bietet die so genannte Quarantänelösung. Die virenverseuchten E-Mails werden zunächst nicht zugestellt, sondern in einen gesonderten Ordner umgeleitet. Der Adressat wird jeweils darüber informiert, wenn eine an ihn gerichtete Nachricht Viren enthält und wie die Mail für ihn zugänglich ist. Zum Schutz der TK-Systeme kann dabei der Zugriff etwa an den Einsatz eines lokalen Virenscanners oder an Haftungsregelungen geknüpft werden. Dieses Verfahren bietet zum einen den Vorteil, dass es ausschließlich automatisiert abläuft und daher datenschutzrechtlich unbedenklich ist. Zum anderen ermöglicht es dem Adressaten, selbst abzuwägen, ob er unter Übernahme etwaiger Haftungsrisiken tatsächlich Zugriff nehmen oder eventuell den Absender kontaktieren will, um sich die Nachricht gegebenenfalls erneut zustellen zu lassen, oder ob er die Nachricht löscht.

Eine ähnlich eigenverantwortliche Entscheidungsfreiheit verbleibt dem Nutzer, wenn er in einem benutzerspezifischen Profil im Voraus festlegen kann, wie mit virenbehafteten E-Mails zu verfahren ist. Unter Abwägung des Haftungsrisikos kann er darin bestimmen, ob entsprechende E-Mails gelöscht, gesäubert oder ganz normal zugestellt werden sollen. Dabei kann auch insoweit die Zustellung abhängig gemacht werden von Bedingungen wie dem Einsatz eines lokalen Anti-Viren-Programms oder von Haftungsbestimmungen.

Zusammenfassend ist festzustellen, dass in jedem Fall dem Nutzer vorher bekannt gegeben werden muss, wie mit auffälligen Mails verfahren wird[42]. Ferner sind Mailadressaten grundsätzlich zu benachrichtigen, wenn an sie gerichtete oder von ihnen abgesendete E-Mails ganz oder teilweise unterdrückt werden oder virenverseucht sind[43]. Ist private Mailnutzung zugelassen, so kann die Vorgehensweise sinnvollerweise in die Nutzungserlaubnis zur privaten Mailnutzung aufgenommen werden. Eine Kenntnisnahme von Verbindungsdaten und Inhalten verbietet das Fernmeldegeheimnis. Daher ist eine Einsichtnahme in virenverseuchte E-Mails durch den Systemadministrator auch zur Identifikation der Quelle immer nur unter Einbeziehung des Adressaten bzw. mit dessen Einwilligung zulässig. Das Fernmeldegeheimnis kann auch nicht durch Betriebsvereinbarungen eingeschränkt werden. Auch soweit die Mailnutzung auf ausschließlich dienstliche Zwecke beschränkt ist, ist das Vorgehen ebenfalls – aus Gründen des Persönlichkeitsrechts – transparent zu gestalten[44] und mit der Personalvertretung abzustimmen. ■

41 Orientierungshilfe der 63. Konferenz der DSB (o. Fußn. 33), Nrn. II i, III 2 c; ebenso BfD, Datenschutzrechtliche Grundsätze bei der dienstlichen/privaten Internet- und E-Mail-Nutzung am Arbeitsplatz, Stand: März 2003, Nr. 2.4., http:// www.bfd.bund.de/information/Leitfaden.pdf.

42 Orientierungshilfe der 63. Konferenz der DSB (o. Fußn. 33), Nr. II i, III 2 c.

43 Orientierungshilfe der 63. Konferenz der DSB (o. Fußn. 33), Nr. II i, III 2 c.

44 Orientierungshilfe der 63. Konferenz der DSB (o. Fußn. 33), Nr. II i, III 2 c.

Wiss. Assistent Dr. Andreas Popp, Passau

Von „Datendieben" und „Betrügern" – Zur Strafbarkeit des so genannten „phishing"*

Der folgende Beitrag widmet sich dem Phänomen des „password fishing" – kurz: „phishing" –, das im Bereich des so genannten Online-Banking in zunehmendem Maß Vermögensschädigungen von zum Teil erheblichem Umfang bewirkt. Im Mittelpunkt der Untersuchung steht die Frage, ob das „phishing" als solches von einem geltenden Straftatbestand erfasst ist.

I. Der „phishing"-Angriff als neue Form der Vermögensschädigung

Der Erledigung von Bankgeschäften im Wege des für beide Seiten bequemeren und kostengünstigeren Online-Banking droht Gefahr: Viele Banken warnen ihre Kunden neuerdings vor so genannten „phishing"-Attacken „in betrügerischer Absicht", durch die für Zugang und Benutzung erforderliche, ausschließlich dem Kunden bekannte Daten wie Passwort, Identifikationsnummer (PIN) oder Transaktionsnummern (TAN) in falsche Hände geraten können[1]. Und dies nicht ohne Grund: Schätzungen des dadurch bislang verursachten Schadens bewegen sich für die USA zwischen 500 Mio. und 2,4 Mrd. US-Dollar, auch in Deutschland wurden bereits erste Geschädigte bekannt[2].

Die Täter gehen dabei folgendermaßen vor: Zunächst wird irgendwo im Internet eine Website eingerichtet, die derjenigen der betreffenden Bank täuschend ähnlich sieht. Dann werden

* Der Autor ist Wissenschaftlicher Assistent am Lehrstuhl für Straf- und Strafprozessrecht, Rechtsphilosophie und Rechtssoziologie (Prof. *Dr. Berhard Haffke)* der Universität Passau.

1 Z. B. https://www.dresdner-privat.de/fb/sicherheit/sicherheit_aktuell_home.html; http://www.postbank.de (Stand: 4. 10. 2004). Das Kunstwort „phishing" geht auf den Ausdruck „password fishing" zurück.

2 Quelle: http:/heise.de/newsticker/meldung/50398, unter Berufung auf die Financial Times Deutschland v. 26. 8. 2004.