IT-SIcherheit und Datenschutz, Heft 05/2005

Ulrich Emmert

Spam-Abwehr: eine „unendliche Geschichte“

Mit der Novelle des *Gesetzes gegen den unlauteren Wettbewerb* (UWG) vom Juli 2004 wurde die Übermittlung unerwünschter Reklamebotschaften per E-Mail, Fax oder Telefon endlich auch in Deutschland verboten. Uneingeschränkter Grund zur Freude besteht damit allerdings nicht, denn nach wie vor stellt die Abwehr von Spam-Mails Unternehmen vor teils erhebliche technische, organisatorische und rechtliche Probleme.

Nach dem neuen Gesetz, das die Umsetzung einer EU-Richtlinie darstellt, die nur gegen den massiven Widerstand der Werbelobby überhaupt zustande kam, ist der unaufgeforderte Versand von Werbemails zwar nur noch in bestimmten eng umgrenzten Fällen erlaubt: So dürfen Firmen grundsätzlich nur noch ihre eigenen Kunden mit „Informationen“ zu Produkten oder Dienstleistungen versorgen, die sie so oder ähnlich schon einmal gekauft bzw. in Anspruch genommen haben. Verboten sind ferner gefälschte oder verschleierte Absenderadressen, zwingend erforderlich hingegen eine Möglichkeit für den Empfänger, sich auf normalen Kommunikationswegen (anstelle teurer Sonderrufnummern) von einem derartigen Service wieder abzumelden. Zudem können die Empfänger der Nutzung ihrer Mail-Adresse auch aus datenschutzrechtlichen Gründen widersprechen, womit ebenfalls ein Verbot wirksam wird.

Klare Regeln – wenig Schutz

Doch so erfreulich diese klaren Regelungen auch sein mögen, für die alltägliche Abwehr von Spam- und Phishing-Mails und die Durchsetzung der Rechtsansprüche Geschädigter bringen sie noch nicht viel. Das liegt zum einen daran, dass nach jüngsten Erhebungen die meisten professionellen Spam-Versender (zusammen 70 Prozent) von den USA oder Südkorea aus operieren, also in Ländern, wo deutsche Gesetze oder EU-Normen nicht gelten. Zum anderen fällt es auch einheimischen Übeltätern relativ leicht, die Herkunft ihrer Massensendungen zu verschleiern – sei es durch Manipulation der Absenderadresse oder durch die Zusammenarbeit mit Kriminellen, die mit Hilfe von Schadprogrammen die Rechner unbeteiligter Dritter „übernehmen“ und zu so genannten Botnetzen zusammenfassen, über deren Mail- bzw. IP-Adressen dann der Versand erfolgt, wodurch eine Rückverfolgung oft im Sande verläuft. Zudem haben allen lobenswerten Anstrengungen von Verbraucherschützern und Beschwerde-Hotlines[1] zum Trotz die meisten Unternehmen (und erst recht Privatanwender) weder Zeit noch Lust, sich auf einen womöglich langwierigen Rechtsstreit einzulassen. Sie verlassen sich daher lieber auf den Einsatz spezieller Filtersoftware, der allerdings wiederum seinerseits rechtliche Probleme mit sich bringt.[2]

Widerstreitende Normen

Das Kernproblem besteht dabei darin, dass bei der organisierten Spam-Abwehr im Unternehmen zwei unterschiedliche Rechtsansprüche aufeinander treffen: Zwar hat die Firma ein berechtigtes (und einklagbares!) Interesse an einem ungestörten Arbeitsablauf, dieses kollidiert aber in vielen Fällen mit der Pflicht zur Wahrung des Fernmeldegeheimnisses (vgl. § 354 StGB) und zur Übermittlung der Mails an die Empfänger gemäß § 88 Telekommunikationsgesetz (TKG). Einzig bei virenbehafteten „Sendungen“ ist das Ausfiltern juristisch kein Problem, da dies nach § 109 TKG als Maßnahme zu werten ist, die der Aufrechterhaltung des Betriebes gilt. In allen anderen Fällen stößt der Arbeitgeber jedoch zunächst auf Schwierigkeiten.

Das hat vor allem damit zu tun, dass er seinen Beschäftigten schon aus logischen Gründen nicht untersagen kann, private Mails zu empfangen, zumal sich diese nur schlecht dagegen wehren können. Darüber hinaus sind E-Mails, auch Spam, in der Regel an den Mitarbeiter persönlich und nicht an die Firma adressiert, wodurch erst recht die Regeln des Datenschutz- und Telekommunikationsgesetzes für private Mails gelten. § 88 TKG legt überdies fest, dass der Arbeitgeber in seiner Rolle als Telekommunikationsanbieter vor Weiterleitung keine Kenntnis vom Inhalt einer Mail nehmen darf – womit auch die vielfach gebräuchliche „Vorfilterung“ von Spam in sog. Sammelaccounts unzulässig ist.

---

[1] Vgl. hierzu den Artikel „Müllvermeidung statt Müllbeseitigung“ in diesem Heft.

[2] Siehe dazu u. a.: Dirk-Michael Barton, Internetkontrolle und betriebliche Mitbestimmung: Kollektivrechtliche Aspekte, S & D Heft 7/2005, S. 36ff.

Allerdings sind die Rechte aus dem Fernmeldegeheimnis und dem Teledienstedatenschutzgesetz für die Mitarbeiter in vielen Fällen verzichtbar: Wer schon im Privatleben mit der unaufhörlich steigenden Flut elektronischen Werbemülls kämpft, ist möglicherweise ganz froh, wenn er wenigsten am Arbeitsplatz seine Ruhe hat. „Verzichtbar" bedeutet in diesem Zusammenhang aber hauptsächlich, dass der Beschäftigte tatsächlich auf sein Recht verzichten kann, etwa indem er sich mit der Ausfilterung von Spam-Mails einverstanden erklärt, bevor diese sein Postfach erreichen. Um diesen Verzicht tatsächlich wirksam werden zu lassen, reicht die häufig gewählte Form einer Betriebsvereinbarung aus meiner Sicht jedoch nicht aus: Da es hier um ein grundgesetzlich geschütztes Recht geht, ist eine individuelle Erklärung des einzelnen Mitarbeiters in jedem Fall vorzuziehen.

Technik vs. Recht

Eine weitere Grauzone tut sich auf, wenn technisch effektive Verfahren der „Müllvermeidung", sprich Filterung, in einen möglichen Widerspruch zu rechtlichen Normen treten. Das ist zum Beispiel dann der Fall, wenn Spam-Mails gar nicht erst angenommen, d. h. schon vor der Übermittlung an den Adressaten vom Provider oder Arbeitgeber blockiert werden. Darunter fallen etwa all jene Verfahren, bei denen Blacklists mit bekannten Spammern oder sog. Dynablocklisten, die Mail-Relays mit dynamischen IP-Adressen erkennen, den Empfang von Mails verhindern. Juristisch kaum anfechtbar wäre auch hier, eine Filterung nur mit Zustimmung der Empfänger vorzunehmen und einschlägige elektronische Post ansonsten in einem gesonderten Verzeichnis zu sammeln.

Damit jedoch nicht genug: Gerade bei den wirksamsten Software-Lösungen zur Spam-Abwehr tritt oft die paradoxe Situation auf, dass Schwierigkeiten gerade durch diese Wirksamkeit entstehen. Denn bei allzu scharfer Einstellung filtern diese ein ums andere Mal auch solche Mails aus, die wichtige Geschäftsdokumente enthalten – z. B. weil bestimmte Formate von Dateianhängen grundsätzlich nicht angenommen werden. Neben dem reinen Verlust der Daten und damit möglicherweise verbundenen finanziellen Schäden bergen derartige *false positives* auch handels- und steuerrechtliche Risiken, denn auf diese Weise sind weder die organisatorischen noch die technischen Voraussetzungen gegeben, den einschlägigen Archivierungspflichten zu genügen. Gewinnt ein Gericht den Eindruck, die Verantwortlichen im Unternehmen hätten dabei absichtlich oder fahrlässig gegen ihre Buchführungspflichten verstoßen, drohen gemäß § 283 b StGB Geldstrafen oder bis zu zwei Jahren Haft. Auf keinen Fall unterschätzen sollten Vorstand und IT-Leitung auch die haftungsrechtlichen Konflikte, die sich aus der Frage ergeben, ob der Softwarehersteller, das für die Installation verantwortliche Dienstleistungsunternehmen oder der Anwender selbst dafür verantwortlich ist, wenn wichtige Aufträge auf diese Weise verloren gehen oder nicht fristgerecht erledigt werden können. Anwendern, die eine solche Lösung einführen wollen, ist daher aus juristischer Sicht anzuraten, auf jeden Fall auf eine niedrige *false-positives*-Rate zu achten.

Was hilft?

Die bisherigen Ausführungen zeigen deutlich, dass die Abwehr von Spam trotz der durch die UWG-Novelle entstandenen anwenderfreundlicheren Gesetzeslage wohl auch weiterhin alle Merkmale einer „unendlichen Geschichte" aufweisen wird. Angesichts der vielfältigen rechtlichen Einschränkungen, denen die Spam-Opfer unterliegen, scheint es fast, als würden sie bei ihrer Gegenwehr ein größeres Risiko eingehen als die professionellen Spammer selbst – zumal diese mit ihrer Tätigkeit wirklich Geld verdienen: Neueren Erhebungen zufolge haben allein in den USA rund 30 Prozent aller E-Mail-User schon einmal in Spam-Sendungen beworbene Waren bestellt. Eine vergleichbare Entwicklung zeichnet sich auch in Europa ab. Wirklich hilfreich scheint vor diesem Hintergrund nur die Verhängung strafrechtlicher Sanktionen inklusive Haft. Die Diskussion darüber hat allerdings gerade erst begonnen.

Zum Autor: Ulrich Emmert ist Partner bei *esb Rechtsanwälte* in Stuttgart und Lehrbeauftragter für Internet an der Hochschule für Wirtschaft und Umwelt in Nürtingen. E-Mail-Kontakt: ulrich.emmert@kanzlei.de.