Rechtliche Aspekte der Spamfilterung für Unternehmen und Administratoren

Peer Heinlein (Dipl.jur.)
Heinlein Professional Linux Support GmbH
p.heinlein@heinlein-support.de

Abstract: Internet Service Provider, Arbeitgeber und Administratoren haben beim Einsatz von Spam- und Virenfiltern viele rechtliche Details zu beachten. Scheint der Einsatz entsprechender Filtermechanismen vordergründig selbstverständlich und notwendig zu sein droht dem Administrator die Strafbarkeit und dem Unternehmen die Haftungsfalle. Arbeitsrechtliche Vorschriften machen den Einsatz von Filtern innerhalb eines Unternehmen zum aufwändig abzustimmenden Unterfangen.

1 Grundlagen

Für die nachfolgende Betrachtung der rechtlichen Probleme müssen die verschiedenen Rechtsgebiete sauber voneinander getrennt werden:

Das Strafrecht, mit dem der Staat den allgemeinen Rechtsfrieden sichert, indem besondere als sozialschädlich erachtete Verhaltensweisen sanktioniert werden. Das Strafrecht wirkt sich damit nur indirekt auf das allgemeine Zusammenleben der Bürger aus.

Das Zivilrecht, dass das Verhältnis zwischen Kunde und Anbieter regelt, also der Nutzungsvertrag und damit die Frage, ob der Anbieter seine Leistung vertragsgerecht erbringt und demzufolge auch Anspruch auf angemessene Bezahlung hat.

Das Öffentliches Recht, das nur unter Umständen eine gewisse Rolle bei Spamfilterungen innerhalb eines Unternehmens spielt, beispielsweise wenn arbeits- und datenschutzrechtliche Vorschriften zu beachten sind.

2 Strafrechtliche Probleme

Aufgrund der Tatsache, dass die Sanktionierung im Strafrecht neben Geld- auch Haftstrafen für jeden Einzelnen nach sich ziehen kann, muß Konflikten mit dem Strafgesetzbuch besondere Aufmerksamkeit geschenkt werden.

§206 II StGB bedroht die unbefugte Unterdrückung anvertrauter Sendungen für Inhaber und Beschäftigte von geschäftsmäßigen Telekommunikationsanbietern mit bis zu fünf Jahren Gefängnis oder Geldstrafe. Der Begriff der „Sendung“ umfaßt dabei auch E-Mails ([TROEND06], §206 Rn. 13).

„Geschäftsmäßig“ ist der Anbieter schon dann, wenn er den Dienst nur nachhaltig betreibt, auf eine Gewinnerzielungsabsicht kommt es nicht an ([TROEND06], §206 Rn. 2). Auch Gratis-Dienste und geschlossene Benutzergruppen werden demnach vom Anwendungsbereich des §206 II StGB erfaßt. In der Praxis muß daher beim Betreiber eines Mailservers sehr schnell von einem „geschäftsmäßigen Telekommunikationsanbieter“ ausgegangen werden, so daß §206 StGB prinzipiell anwendbar ist.

„Anvertraut“ ist eine Nachricht, wenn der Absender davon ausgehen kann, dass der nächste Server die E-Mail sicher empfangen hat und zustellen wird. In der technischen Praxis ist dies dann der Fall, wenn der empfangende Server die erfolgreiche Übertragung der E-Mail mit dem SMTP-Statuscode „`250 OK`“ quittiert und das einliefernde System daraufhin die E-Mail aus seiner Mailqueue gelöscht hat. Ein Anvertrauen ist im Umkehrschluß dann zu verneinen, wenn das empfangene System durch einen entsprechenden Fehlercode („`4xx`“, bzw. „`5xx`“) kenntlich gemacht hat, daß die Mailübertragung aus welchen Gründen auch immer nicht erfolgreich war.

„Unterdrückt“ wird eine Nachricht dann, wenn sie gelöscht, fehlgeleitet oder zurückgehalten wird ([TROEND06], §206 Rn. 15). Das einfache Verwerfen von erkannten Spam- und Virennachrichten (”DISCARD”) verbietet sich demnach, während das Einfügen eines SPAM-TAGs im Betreff oder ein Bounce an den Absender keine Unterdrückung im Sinne des §206 II StGB darstellt. Das Parken einer solchen E-Mail in einem Quarantäne-System ist wohl dann keine Unterdrückung, wenn der Empfänger darüber informiert wird und jederzeit leicht die Auslieferung der E-Mail veranlassen kann.

Allerdings sanktioniert §206 II StGB lediglich die „unbefugte“ Unterdrückung anvertrauter Nachrichten. Es ist das gute Recht des Empfängers darüber zu entscheiden, wie mit seinem Eigentum – den Nachrichten – umgegangen werden soll. Liegt das Einverständnis des Empfänger vor, ist selbst das spurlose Löschen der Nachrichten zulässig.

3 Zivilrechtliche Probleme

3.1 Zwischen Nutzer und Anbieter

Zwischen Provider und Nutzer liegt i.d.R. ein -wie auch immer gearteter- Dienstvertrag vor, wonach der Provider den Mailtransport zu erbringen hat. Filtert der Provider ohne Einverständnis des Nutzers Spam und Viren heraus, könnte dies prinzipiell als mangelhafte Dienstleistung des Anbieters zu bewerten sein. Sofern der Nutzer nicht explizit einer entsprechenden Filterung zugestimmt hat, könnte er theoretisch vom Anbieter ein filterfreies Postfach fordern.

Andererseits muß anerkannt werden, daß der Betrieb eines komplexen Netzwerkes wie dem Internet nur mit klaren Regeln, technisch sauber eingehaltenen Protokollen und einigen Schutzmaßnahmen sicherzustellen ist. Die Grundlage dafür bilden die sogenannten „Request for Comments“ (RFC), die auch festlegen wie E-Mails übertragen werden und wie Mailserver konfiguriert sein müssen. Eine umfangreiche Beleuchtung aller Details liefert [HEINL04]. Spam-Versender verstoßen häufig absichtlich oder unabsichtlich gegen

diese RFCs, beispielsweise weil DNS-Daten der Botnetze falsch konfiguriert sind oder weil sich der einliefernde Mailserver zur Tarnung mit einem falschen Namen anmeldet.

Es ist unbestritten, dass Mailserver nicht alle E-Mail annehmen können, gleich wie regel- und protokollwidrig sich der einliefernde Mailclient verhält. Spätestens wenn die technische Kommunikation zwischen Client und Mailserver nicht mehr funktioniert, wird der Mailserver die Mail nicht mehr empfangen können.

Das Recht des Nutzers auf Empfang seiner E-Mails findet demnach seine Grenzen in den technisch notwendigen Anforderungen zum Betrieb des Netzwerkes und damit dem Schutz einzelner Server, aber auch der Allgemeinheit seiner Nutzer. Es ist nicht unumstritten, aber gut nachvollziehbar, dass Mailserver bei eklatanten RFC-Verstößen die Annahme von E-Mails auch verweigern können müssen, selbst wenn technisch gesehen der Empfang der E-Mail noch möglich wäre. Auch im normalen Postverkehr wird analog der Transport von Sendungen mit Sicherheitsrisiken (Beispiel: Chemikalien) oder bei fehlender Transportfähigkeit (Beispiel: Fehlende Verpackung) vom Postdienstleister abgelehnt werden dürfen.

Der Nutzer kann damit mitnichten von seinem Anbieter unumstößlich und unbegrenzt den Empfang „aller“ E-Mails fordern kann, sofern der Anbieter im Rahmen der Abwägung beider Interessen nachvollziehbare und objektiv überprüfbare technische Kriterien vorbringen kann. Die Prüfung des Clients gegen einschlägige und durch Dritte verifizierte IP-Sperrlisten (RBL) mag je nach Auslegung darunter fallen.

Um die Rechtssicherheit zu steigern sollte der Anbieter unbedingt entsprechende Klausen zum Eigenschutz in den Individualvertrag oder die allgemeinen Nutzungsbedingungen (AGBs) aufnehmen.

Ob in den AGBs eines Anbieters die grundsätzliche Festlegung einer allgemeinen Zustimmung zur Spam- und Virenfilterung auch nach inhaltsbewertenden Methoden zulässig ist, ist umstritten. Im Zweifel sollte hier jeweils eine individualvertragliche Vereinbarung („Opt-In“) angestrebt werden. Diese sollte sprachlich so gestaltet sein, daß der Anbieter nicht einfach nur „Spam“ herausfiltern darf, sondern etwas weiter formuliert die Erlaubnis erhält, Spam- und Virenfilter einzusetzen. Ansonsten könnte gut argumentiert werden, daß sich das Einverständnis des Nutzers lediglich auf „echten“ Spam bezogen hat. Das versehentliche Filtern einer echten E-Mail („false positive“) wäre sonst nicht vom Einverständnis des Nutzers gedeckt gewesen.

3.2 Zwischen Empfänger und Absender

Häufig werden als Spam erkannte Nachrichten von den Servern angenommen und lediglich markiert an den Empfänger weitergeleitet. Auch echte E-Mails können so versehentlich in den Spamverdachts-Ordner gelangen. Wird auf Empfängerseite der Verdachtsordner nicht richtig kontrolliert oder werden die als Spam markierte E-Mail pauschal gelöscht, sind zivilrechtliche Haftungsprobleme zwischen Empfänger und Absender denkbar, wenn der Absender von einer erfolgreichen Zustellung ausgehen durfte.

4 Besonderheiten bei Unternehmens-Netzwerken

4.1 Filterung ausschließlich geschäftlich genutzter E-Mail-Postfächer

Relativ unproblematisch ist die Spam-Filterung geschäftlicher E-Mails. Nicht der einzelne Mitarbeiter ist juristischer Eigentümer der empfangenen E-Mails, sondern der Geschäftsinhaber oder Dienstherr als Stellvertreter der juristischen Person. Ein Einverständnis zur Filterung der geschäftlichen E-Mails ist demnach einfach zu erteilen und juristisch unproblematisch.

Sofern vorhanden ist allerdings der Betriebs- oder Personalrat mit einem Kontrollrecht einzubeziehen, um einen Missbrauch der Filterfunktionen auszuschließen.

4.2 Filterung auch privat genutzter E-Mail-Postfächer

Bei privater Mail-Nutzung am Arbeitsplatz ist der Arbeitgeber i.d.R. als „geschäftsmäßiger Telekommunikationsanbieter“ mit allen geschilderten Auswirkungen anzusehen. Dies gilt auch dann, wenn der Arbeitnehmer für die Nutzung kein Entgelt zu entrichten hat.

Der Nutzer müßte einer Filterung seiner privaten E-Mails zustimmen. Ist eine klare technische Trennung zwischen privaten und geschäftlichen E-Mails nicht mehr möglich, wird dem Arbeitgeber ggf. die Filterung seiner eigenen E-Mails zu versagen sein, sollte der Nutzer seine Zustimmung verweigern.

Eine Filterung nach Viren und anderer Schadsoftware muß aufgrund des vorrangigen Schutzes des Unternehmensnetzwerkes stets möglich sein.

4.3 Die betriebliche Praxis bezüglich privater E-Mail-Nutzung

Oft fehlen Regelungen zur private E-Mail-Nutzung am Arbeitsplatz. Sollten innerhalb eines Betriebes tatsächlich keinerlei Regelungen zur privaten E-Mail-Nutzung vorhanden sein, ist grundsätzlich von einem Verbot auszugehen. Der Arbeitgeber müßte die private Nutzung seiner Infrastruktur erlauben.

Doch auch bei einem schriftlich fixierten Verbot ist die aktuell ausgeübte betriebliche Praxis entscheidend: Auch schriftliche Regelungen können durch schlüssiges „konkludentes“ Handeln fortlaufend abgeändert werden. Das Verbot muß demnach eingehalten und durchgesetzt werden. Vorgesetzte und IT-Verantwortliche dürfen eine private Nutzung nicht schweigsam dulden, geschweige denn fördern, sonst ist alsbald von einer erlaubten privaten Nutzung auszugehen.

4.4 Arbeitsrechtliche Probleme für den Administrator

Ebenso wie bei anderen Straftaten – wie Diebstahl oder Totschlag – kann der Administrator gegen §206 StGB nicht anführen, er habe "lediglich auf Anweisung seines Vorgesetzten"gehandelt. Denn ob Anweisung, oder nicht: Was strafrechtlich durch den Staat verboten ist, kann nicht durch Anweisung eines Vorgesetzten legalisiert werden.

Rechtswidrigen Anweisungen des Vorgesetzten müßte sich der Administrator verweigern, was zu schweren Konflikten im Arbeitsleben führen kann. Dabei kann von keinem Beteiligten ein umfassendes Rechtswissen verlangt werden. Hier muss ggf. auf externen juristischen Sachverstand zurückgegriffen werden, um die Beteiligten abzusichern. Eine gute Übersicht bietet [STROEM02].

5 Quintessenz

Um die zivilrechtlichen Haftungsrisiken und strafrechtlichen Probleme zu vermeiden, sollten Spam und Viren vom Mailserver gar nicht erst erfolgreich angenommen werden. Auch das allseits beliebte markieren der Spamnachrichten („Tagging“) schafft keine ausreichende Rechtssicherheit.

Filtertechniken wie Greylisting ([HEINL04a]) oder RBL können diese Überprüfungen in Echtzeit leisten. Auch gute Anti-Spam-Software kann schon jede E-Mail während des Annahmeprozesses in Echtzeit filtern ([HEINL04]). Erkannter Spam kann dann direkt gegenüber dem einliefernden Mailserver mit einem SMTP-Code „`4xx`“, bzw. „`5xx`“ abgelehnt werden.

Auch für Absender und Empfänger ist das Ablehnen der E-Mais im Falle eines „false positive“ am erstrebenswertesten, da der Absender dann umgehend eine Unzustellbarkeitsmeldung erhält und über die nicht erfolgte Zustellung seiner Nachricht eindeutig informiert ist.

Im weiteren Ergeben sich bei privater Nutzung einer geschäftlichen E-Mail-Adresse unabwägbare Risiken für den Arbeitgeber, die zum Verlust seines Handlungsspielraumes führen können. Auch außerhalb der Spam- und Virenfilterung hat die erlaubte private Nutzung schwerwiegende Konsequenzen: Aus datenschutzrechtlichen Erwägungen wird der Zugriff des Arbeitgebers auf Mitarbeiterpostfächer selbst bei langer Krankheit oder einem Ausscheiden des Arbeitnehmers zu verneinen sein. Auch die neuerdings geforderte revisionssichere Archivierung aller ein- und ausgehenden Handelsbriefe kann nicht mehr umgesetzt werden, wenn die Gefahr besteht, daß auch private E-Mails archiviert werden könnten.

Hier kann einem Arbeitgeber nur geraten werden, die private E-Mail-Nutzung zu untersagen und durchzusetzen, oder aber eine weitere technisch klar getrennte Mailserver-Infrastruktur ausschließlich für die private Nutzung durch seine Mitarbeiter zu installieren und damit eine klare Trennung vorzunehmen.

6 Literatur

[TROEND06] Herbert Tröndle, Thomas Fischer, Strafgesetzbuch, Beck Juristischer Verlag, München 2006

[STROEM02] Tobias H. Strömer, Online-Recht, dpunkt.verlag, Heidelberg 2002

[HEINL04] Peer Heinlein, Das Postfix-Buch, Open Source Press, München 2004

[HEINL04a] Peer Heinlein, Verzögerungstaktik, Linux-Magazin 09/04, Linux New Media, München 2004