Spam-Abwehr – Möglichkeiten und Grenzen

Burckhard Schmidt
bschmidt@cms.hu-berlin.de

Werbung, SPAM Filer, SPAM-Level, Spam-Status, Datenschutz, Virus, Telekommunikationsgesetz, Blacklist

Unerwünschte Werbung – SPAM – ist auf der einen Seite Geschäft, auf der anderen Seite schlicht eine erhebliche Beeinträchtigung der Arbeitsfähigkeit. Wie lässt sich die SPAM-Flut eindämmen oder wenigstens kanalisieren?

Die Zusendung von E-Mails mit unerwünschter Werbung (Spam) ist nach wie vor ein »boomender Geschäftszweig«. Ebenso der Handel mit verifizierten E-Mail-Adressen. Die Möglichkeiten zum Verschicken von Massenmails sind vielfältig. Es ist kein Problem, den eigenen PC zum Mailserver zu machen, der die Zustellung der Spam-Mails selbst durchführt. Zudem können für die Verbindung zum Internet meistens preiswerte Flatrates genutzt werden, also kein Problem. Weiterhin werden viele Mailserver im Internet betrieben, die im Gegensatz zu unseren Servern E-Mails von jedem x-beliebigen PC annehmen und verteilen (offenes Relay). Das kann so gewollt oder schlichtweg eine Nachlässigkeit in der Administration sein. Weitere Möglichkeiten bieten sich auf Web- und Proxy-Servern, auf denen oft Mailformulare vorhanden sind, die sich leicht zum Spammen missbrauchen lassen. Auch unsere Web-Server sind beständig Versuchen ausgesetzt, die entsprechenden Schutzmaßnahmen auszuhebeln.

Wie geht man mit Spam um?

Die einfachste Methode ist das Löschen, weil man visuell relativ schnell am Betreff und am Absender eine E-Mail als Spam klassifizieren kann. Leider unterliegt man hier leicht Täuschungen, weil im Betreff oft mit einer »sozialen Komponente« gearbeitet wird, so dass man sich persönlich angesprochen fühlen soll. »Re:« täuscht z. B. eine erwartete Antwort vor. Die »guten« E-Mails stehen natürlich gemischt zwischen den Spam-Mails. Das mit dem Löschen ist also leichter gesagt als getan, denn das bedeutet Aufwand und ist mit der Gefahr verbunden, wichtige E-Mails mitzulöschen. Selbst das Markieren von E-Mails zum Löschen kann, je nach verwendetem Mailtool und den eingestellten Parametern, schon schwierig sein und zum ungewollten Öffnen einer E-Mail führen.

Weiterhin macht es keinen Sinn, an den vermeintlichen Absender eine Beschwerde zu schicken, denn dieser ist eigentlich immer gefälscht. Das heißt aber nur, dass es nicht der Absender des Spam-Versenders ist, aber eine gültige Adresse kann es schon sein. Der ahnungslose reguläre Besitzer dieser missbrauchten E-Mail-Adresse sieht sich dann zu Unrecht den Beschwerden ausgesetzt und kämpft mit einer vollen Mailbox. Ein korrekter Absender würde ja zum Spammer führen, was also nicht zu erwarten ist. Um etwas über die Herkunft einer E-Mail zu erfahren, muss man die so genannten Received-Zeilen aus dem Kopf einer E-Mail (Header) analysieren, wobei auch gefälschte Received-Zeilen verwendet werden, um eine Analyse zu erschweren. Das Verfahren, nach dem E-Mails zu einem Mailserver übertragen werden (SMTP-Protokoll), stammt aus den Anfängen des Internet und ist von seinen Entwicklern »nur« hinsichtlich einer vernünftigen Nutzung entworfen worden. Aber so ist es ja mit vielen Dingen im Leben. Die Angaben in der From:- bzw. To:-Zeile sind beliebig fälschbar, weil die Zustellung von E-Mails anhand von Adressen vorgenommen wird, die auf dem fiktiven Umschlag (envelope) einer E-Mail stehen, dem Empfänger aber nicht mitgeteilt werden.

Die Inhalte solcher E-Mails sind »vielfältig« gestaltet, auch um die Spam-Bewertung auszutricksen: einfacher Text, HTML-Text, Texte mit HTML-Kommentaren zwischen je zwei Buchstaben, URL's, Grafiken, Animationen, WebBugs usw. Solche »Inhalte« können bereits beim Öffnen der E-Mail sofort Aktionen auslösen, die dem Spammer (und Auftraggeber) u. a. mitteilen, dass die E-Mail ihr Ziel erreicht hat. Analog verhält es sich mit angebotenen Links zum Abbestellen zukünftiger E-Mails. Es ist also am besten, solche E-Mails nicht zu öffnen, sondern nur zu löschen.

Spam-Abwehr durch Blacklists – Annahme verweigert

Im Internet gibt es Listen, auf denen die Netzadressen (IPAdresse) von Servern geführt werden, die im Zusammenhang mit Spam »auffällig« waren. Sie werden ständig aktualisiert und können für die Entscheidung genutzt werden, ob von einem konkreten Server/PC (ausgewiesen durch seine IP-Adresse) überhaupt eine E-Mail angenommen werden soll oder nicht. Es gibt verschiedene Organisationen, die nach unterschiedlichen Kriterien die IP-Adressen von Servern führen, von denen Spam verschickt wurde oder die sich prinzipiell dafür »eignen«. Diese Netzadressen werden z. B. nach der Methode klassifiziert, die sie Spammern »bieten« oder nach ihrem Verwendungszweck. Hier spielt insbesondere die IP-Adresse eine Rolle, die man (der PC) für die Dauer des telefonischen Zugangs zum Internet erhält. In der Regel sollte man nämlich seine E-Mails dann auch über den Mailserver des Providers verschicken, über den man sich eingewählt hat und nicht über einen anderen Mailserver. Nicht zuletzt aus diesem Grund bieten wir einen eigenen Einwahldienst für Angehörige unserer Universität an. Wenn man einen anderen Einwahldienst benutzt und über unseren Mailserver eine E-Mail »in die Welt« verschicken möchte, dann gibt es die bekannte Fehlernachricht »Relaying denied«. Im anderen Fall wäre unser Mailserver ein offenes Relay und stünde selbst auf einer Blacklist. Viele Provider lassen die Netzadressen, die sie für die telefonische Einwahl vergeben, in eine entsprechende Blacklist aufnehmen, um die missbräuchliche Nutzung einzudämmen. Bekannte Anti-Spam-Organisationen sind etwa *ordb.org*, *spamhaus.org* oder *sorbs.net*. Sie sehen sich übrigens selbst häufig Angriffen aus dem Internet ausgesetzt, indem der Dienst mit extrem vielen Anfragen praktisch blockiert wird (denial of service attack). In einem solchen Fall entstehen auch für Mailserver, die diese Dienste nutzen, erhebliche Verzögerungen bei der Zustellung von E-Mails.

Markierung von Spam durch den Mailserver

Eine Möglichkeit, dem Empfänger einer E-Mail Unterstützung bei der Spam-Bewertung zu geben, besteht darin, die E-Mail nach verschiedenen Kriterien zu analysieren und das Ergebnis als zusätzliche Information in den Kopf einer E-Mail einzufügen. Diese »Spam-Information« kann vom Empfänger ignoriert werden oder z. B. für eine Verteilung der eingehenden E-Mails in entsprechende (Spam-) Ordner benutzt werden. Damit erreicht man eine Entlastung bei der Bearbeitung seiner E-Mails.

Die Analyse der E-Mails wird mit dem Programm SpamAssassin vorgenommen (*www.spamassassin.org*). Im Ergebnis der Analyse können mehrere »X-Spam«-Zeilen in den Kopf einer E-Mail (Header) eingefügt werden. Dieser Bereich ist sowieso zur Aufnahme von Bearbeitungsmerkmalen jener Mailserver gedacht, die eine E-Mail auf ihrem Weg vom Sender zum Empfänger passiert hat.

Das Ergebnis der Spam-Bewertung ist eine Zahl, die eine Art Spam-Wahrscheinlichkeit ausdrückt. Je größer sie ist, um so wahrscheinlicher ist es, dass eine E-Mail als Spam zu bewerten ist. Dieses Ergebnis ist in der »X-Spam-Status:«-Zeile als »hits« zu finden. Um eine einfache Möglichkeit zur Auswertung in nutzerdefinierten Filterregeln im Mailtool zu ermöglichen, wird auch eine »X-Spam-Level:«-Zeile eingefügt, die diese Zahl in der entsprechenden Anzahl von »*«-Zeichen darstellt. Damit kann man im eigenen Mailtool Filterregeln[1] definieren, die diese »X-Spam-Level:«-Zeile auswerten. So könnte z. B. bei Vorhandensein von mindestens 12 Sternen die E-Mail gelöscht werden und bei mehr als 5 Sternen in einen Spam-Ordner einsortiert werden.

Die Status-Zeile enthält noch weitere Angaben, u. a. zu den durchgeführten Tests, die zur entsprechenden Spam-Bewertung geführt haben. Die Beschreibungen der Tests sind beim Entwickler (sehr) kurz gehalten. Da SpamAssassin sehr verbreitet ist, muss man auch daran denken, dass eine E-Mail, die man selbst verschickt, gleichermaßen bewertet wird. Schon eine »ungeschickt« gestaltete Betreff-Zeile mit vielen Großbuchstaben, Ausrufezeichen oder Bindestrichen führt zu Spam-Punkten.

Löschen von Spam durch den Mailserver

Ein generelles Löschen von Spam-Mails auf dem zentralen Mailserver wird es nicht geben, auch wenn man damit den »größten« Effekt erreichen würde (vgl. rechtliche Aspekte). Die Spam-Bewertung durch Programme, also auch durch den Mailserver, wird nie mit absoluter Sicherheit erfolgen können, zumal bei der »Gestaltung« der Spam-Mails versucht wird, bekannte Filtermethoden möglichst zu umgehen. Darum sind z. B. die Texte im Betreff oft so eigenartig gestaltet! Also kann das Löschen von Spam nur eigenverantwortlich vom Empfänger selbst veranlasst werden.

Einsatz »intelligenter« Mailtools

Eine Alternative kann die Verwendung eines modernen, bezüglich Spam intelligenten, selbstlernenden Mailtools[2] sein, z. B. Mozilla oder Netscape. Die Filterregeln lassen sich auf die eigenen Kommunikationsbeziehungen einstellen, wobei man die »Entscheidungen« des Tools auch korrigieren kann, wenn falsche Bewertungen (positiv wie negativ) bezüglich Spam erfolgt sind.

Filtern – alles was Recht ist

Im Rahmen des Deutschen Forschungsnetzes arbeitet eine Forschungsstelle »Recht im DFN« an der Universität Münster, die Betreiber von Maildiensten in rechtlichen Fragen unterstützt. Sie hat z. B. Handlungsempfehlungen zu Spam und Viren veröffentlicht[3]. Der Betreiber eines Mail-Dienstes ist an eine Reihe von gesetzlichen Bestimmungen gebunden. So wird der Mailverkehr auch für die Individualkommunikation benutzt, wodurch schützenswerte Interessen der beteiligten Kommunikationspartner bestehen. Insbesondere sind das Telekommunikationsgeheimnis (§ 206 StGB und Telekommunikationsgesetz), die Datenintegrität (§ 303a StGB) und die datenschutzrechtlichen Gesichtspunkte zu beachten. Neben den möglichen Unterscheidungen zwischen dienstlicher und privater Nutzung des Maildienstes ist in unserem Bereich auch die Lehr- und Wissenschaftsfreiheit zu beachten. Andererseits haben die Betreiber universitärer Netze und Dienste (landläufig Rechenzentren) auch die Aufgabe, die Infrastruktur vor Missbrauch zu schützen. Bezüglich Viren und deren Filterung (im Sinne einer Unterdrückung) ist zwischen den genannten Aspekten eine Interessenabwägung vorzunehmen. Bei den Viren wird eine Unterdrückung eher tolerierbar sein als bei einer möglichen Unterdrückung von Spam. Viren sind zudem relativ sicher definierbar und erkennbar, was man

1 Generieren von Filterregeln: vgl. www.hu-berlin.de/cms/, Index »A-Z«, Mail
2 selbstlernende Mailfilter: vgl. www.hu-berlin.de/cms/, Index »A-Z«, Mail
3 www.dfn.de, »Recht im DFN«

von Spam nicht behaupten kann. International gibt es noch viele Länder, die Spam in ihren Gesetzen bisher überhaupt nicht betrachten, in anderen ist Spam ein legitimes Mittel innerhalb der gesellschaftlichen Kommunikationsbeziehungen. Das Europäische Parlament hatte eine Richtlinie (Datenschutzrichtlinie für elektronische Kommunikation) beschlossen, die im letzten Jahr in nationales Recht umgesetzt wurde. Das erfolgte leider nur im Rahmen des Wettbewerbsrechts, so dass z. B. eine Einzelperson keine Klagemöglichkeit gegen einen Spammer hat, sofern dieser »greifbar« wäre.

Fazit: Die rechtliche Situation ist hinreichend kompliziert und die Gesetze gegen Spam haben ihre Alltagstauglichkeit sowieso noch nicht bewiesen, weil es bisher keine entsprechenden Gerichtsverfahren gab. Auf der sicheren Seite stehen Nutzer und Betreiber eines Dienstes (generell), wenn der Nutzer entsprechende Nutzungsbedingungen gegenzeichnet (nachweisbar Kenntnis hat), einem bestimmten Verfahren nachweisbar zustimmt oder selbst in Kommunikationsprozesse steuernd eingreifen kann. Das ist einerseits natürlich einleuchtend, andererseits sind vom Betreiber solche Möglichkeiten zur individuellen Steuerung (hier z. B. die Gestaltung von Spam-Filtern auf dem Mailserver) in der Regel erst zu schaffen bzw. den konkreten Gegebenheiten anzupassen. Das erfordert personelle Kapazitäten und ist nicht immer sofort umsetzbar.

Das Analysieren von E-Mails bzg. Viren und Spam durch automatische Verfahren wird unter der Maßgabe, dass keine personenbezogenen Daten protokolliert werden, datenschutzrechtlich als zulässig angesehen. Die eingesetzten Programme (bei uns Virenscanner von NAI, Spam-Bewertung mit SpamAssassin) sind den Datenschutzbeauftragten ebenfalls bekannt, so dass auch eine weitere »Instanz« eingreifen könnte, wenn der Datenschutz durch den Einsatz fragwürdiger Programme oder Verfahren ernsthaft bedroht wäre.

Nicht zuletzt aus diesem Grund beziehen wir den Datenschutzbeauftragten der HU bei der Planung von Verfahren, die z. B. in den Kommunikationsprozess eingreifen, mit ein. Teilweise sind Ordnungen/Verfahren durch universitäre Gremien zu beschließen.

Verfahrensfragen

Blacklists

Der Einsatz von Blacklists bewirkt die Verweigerung jeglicher Annahme von E-Mails von einem konkreten Server (PC), worüber der Absender informiert wird. Darum müssen die wenigen von uns eingesetzten Blacklists wiederholt überprüft werden. Zum einen müssen die Regeln (Policy), nach denen Adressen oder Adressbereiche gelistet bzw. gelöscht werden, hinreichend plausibel sein. Zum anderen können Situationen auftreten (denial of service attack), die zu erheblichen Verzögerungen im Mailaustausch führen können, so dass die Nutzung eingestellt werden muss. Einige Betreiber bieten solche Dienste kostenpflichtig an.

In Problemfällen sind durchaus auch »Ausnahmen von der Regel« realisierbar.

Spam-Bewertung

Im obigen Abschnitt wurde beschrieben, wie Spam markiert wird und es dem Empfänger selbst überlassen ist, wie er diese Markierungen anwendet. Teilweise sind Zusatzprogramme erforderlich, weil z. B. Outlook Express diese zusätzlichen Kopfzeilen ignoriert.

Ein anderer Aspekt spielt hier auch noch hinein. Spam kann durchaus zu einer Denial of Service Attacke werden:

Häufig sind Zieladressen (Bestandteil vor dem »@«) für Spam-Mails einfach nur aus allen möglichen Zeichenkombinationen gebildet und werden von verschiedenen Servern aus zum »Ziel«, also zu unserem Mailserver, geschickt. Hier durchläuft jede E-Mail die üblichen Prüfungen. Für jede falsche Adresse wird eine Fehlernachricht an den vermeintlichen Absender geschickt, der entweder nicht erreichbar ist, falsch ist oder bereits zu viele E-Mails erhalten hat und nichts mehr annimmt. Darüber wird dann der »Postmaster« mit je einer E-Mail informiert, am 19./20.2. innerhalb von 12 Stunden fast 40 000 Stück, ausgelöst durch die Werbung für eine »URL«. In so einer Situation kann es sogar dazu kommen, dass der zuständige Mailserver des vermeintlichen Absenders von unserem Mailserver schließlich überhaupt keine E-Mails mehr annimmt! In solchen Fällen werden Kapazitäten auf dem Mailserver gebunden und die Grundlast ist deutlich erhöht. Die Frage entsteht zwangsläufig, wie stark die Mailserver überdimensioniert sein müssen, um bei anhaltenden Lastspitzen (sowohl Spam als auch Virus) die Zustellung nicht zu sehr zu verzögern? Das ist schließlich auch eine finanzielle Frage. Oder schaltet man die Spam-Bewertung oder den Virenscan in solchen Situationen einfach ab? Lieber nicht – meine ich.

Virencheck – der Vollständigkeit halber

Die Basis für den Virencheck sind Virusdefinitionen, die in definierten Abständen (z. B. wöchentlich) bereitgestellt werden. Bei aktuellen Gefahren hofft man auf eine möglichst schnelle Reaktion durch den Anbieter der genutzten Antivirensoftware. Das bedeutet aber, dass zwischen dem Auftreten eines Virus und der Bereitstellung seiner Erkennungsmerkmale eine Zeitspanne liegt, in der er sich »frei« verbreiten kann. Selbst eine nahezu optimale Verzögerung von nur 2 Stunden (Administrator vor Ort, Hinweise zu einem neuen Virus und Virusmerkmale verfügbar) haben nicht ausgereicht, die Verteilung des Virus ganz zu verhindern. Der Schutz ist also nicht absolut und nicht alle Schädlinge kommen per E-Mail!

Was passiert, wenn ein Virus per E-Mail eintrifft? Die Zustellung erfolgt nicht und der Absender erhält nur dann darüber eine Benachrichtigung, wenn der Virus nicht als »Fälscher« von Absenderadressen für den Virenscanner bekannt ist. Das muss manuell durch den Administrator erfolgen, so dass zeitweilig durchaus Benachrichtigungen verschickt werden können. Was passiert, wenn eine virenbehaftete E-Mail »beantwortet« wird?

Der Virus trifft per E-Mail ein und wird entdeckt. Der Absender ist gefälscht, was aber nicht erkennbar ist. Die Benachrichtigung erhält der bisher unbeteiligte »Dritte«, sofern der Absender existiert, ansonsten geht eine Fehlernachricht an den Postmaster. Dieser »Dritte« wundert sich seinerseits und fragt per E-Mail oder per Telefon beim Postmaster an. Da es nicht bei einer Virenmail bleibt, entsteht ein »babylonisches Mail- und Sprachgewirr«, das auf der Ebene individueller Kommunikation nicht beherrschbar ist. Zudem bauen sich Warteschlangen von E-Mails auf, wenn z. B. dieser »Dritte« als vermeintlicher Absender von sehr vielen Maildiensten mit Virenscannern diese Information über die nicht zugestellte E-Mail erhält. Damit hat er schließlich selbst ein Problem mit seiner Mailbox, die sehr viele E-Mails enthalten kann.

Eine andere Variante ist die sogenannte Quarantänelösung, bei der eine virenbehaftete E-Mail separat und befristet abgespeichert wird. Das wird dem Empfänger dann per E-Mail mitgeteilt, einschließlich

der Möglichkeit, wie er (und nur er) selbständig an diese E-Mail gelangen kann. Dieses Verfahren ist bei uns nicht implementiert, weil eine programmtechnische Lösung erst zu realisieren wäre (personeller Aufwand) und in der Handhabung der befallenen E-Mail beim Empfänger natürlich Gefahren lauern.

Die Belastung durch Viren ist zeitweise erheblich. So hatten wir in einer »normalen« Woche Ende Januar durchschnittlich alle 3 Minuten einen Virus erhalten, in den ersten beiden Wochen im Februar pro Minute 7 Viren! Das Mailaufkommen war durch die sich selbst verschickenden Viren (hier Mydoom) extrem angestiegen, wodurch schließlich die Mailzustellung insgesamt verzögert wurde.

Fazit

Zu 100% »saubere« E-Mails gibt es nicht zum »Nulltarif«. Durch die schrittweise Erneuerung der Mail-Infrastruktur im CMS seit dem letzten November (mehrere neue Server, neue Software) konnte der Maildienst den deutlich gestiegenen Anforderungen angepasst und stabilisiert werden. Damit ist man aber eigentlich nie »fertig«, so dass wir am CMS stets bemüht sind, notwendige Verbesserungen oder auch Funktionserweiterungen zu realisieren. Das Thema SPAM beschäftigt inzwischen auch die großen E-Mail-Provider und Hersteller der entsprechenden Software, wobei es um die Modernisierung des »guten alten« SMTP-Protokolls geht. Spammer werden auch weiterhin nach neuen Möglichkeiten für ihre Tätigkeit suchen. Eine davon scheint die Ausnutzung von PC's zu sein, die durch einen Virenbefall feindliche Software (back door) enthalten können, mit der ein PC für »Dritte« unbemerkt nutzbar wird. Neben einer guten Mailinfrastruktur ist man aber auch von konkreten Situationen im Internet abhängig, die man mitunter kaum beeinflussen kann. Dann heißt es z. B. warten, bis der (Viren-) Sturm vorüber ist.

Die Betreiber von Maildiensten im Bereich des DFN-Vereins schätzen die gegenwärtige Situation bezüglich einer stabilen E-Mail-Versorgung als ziemlich kritisch ein. »Radikale« Lösungen verbieten sich von selbst, weil natürlich gesetzliche Vorgaben für eine freizügige Kommunikation zu beachten sind. Es gibt Lösungsansätze, die aber nicht den »durchschlagenden« Erfolg haben oder wegen ihrer ungewollten »Nebenwirkungen« nicht einsetzbar sind. Der Ressourcenbedarf für die Sicherstellung der Mailversorgung steigt überproportional an. Und der Nutzer? Er sieht sich weiterhin einem steigenden Aufkommen von Spam und Viren ausgesetzt. Diese Probleme werden wir nur in gewissem Grade mildern, aber nicht abschaffen können. Ein nicht gerade optimistischer Ausblick!