Das Anti-Spam-Arsenal

Wer sich nicht wehrt, hat schon verloren – beim Thema Spam passt diese Redewendung wie die Faust aufs Auge: Ohne Gegenwehr wäre der Untergang im Message-Müll sicher, sind doch mittlerweile drei von vier Mails oder noch mehr unerwünscht. Ein Blick in die Waffenkammer der Verteidiger. Jens-Christoph Brendel

Spam ist lästig, aber das allein triebe vielleicht noch nicht so viele Widerständler auf die Barrikaden. Der wahre Grund ist: Spam ist teuer, und zwar sehr. Spammer verpulvern jedes Jahr fremdes Geld in Milliardenhöhe und bereichern sich daran. Die hohe Summe ergibt sich zum einen aus den unmittelbaren Kosten für sinnlos konsumierte Bandbreite, die unnötige Nutzung der Mailserver samt ihrer Infrastruktur und die Personalkosten für Abwehrmaßnahmen. Zum anderen schlagen Zeitverschwendung und Produktivitätsverlust der Empfänger als indirekte Kosten zu Buche, daneben die womöglich eingeschränkte Erreichbarkeit oder Imageschäden. Nicht zu vergessen ist die Infektionsgefahr mit Viren und allerlei anderer Malware, die Spammer vorsätzlich in Umlauf bringen.

Konkrete Zahlen sind schwer zu ermitteln, die diversen Spam-Statistiken von Institutionen sowie Herstellern basieren auf keiner einheitlichen Definition und Methodik und erfassen lediglich Stichproben. Sie sind deshalb schwer vergleichbar. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) ermittelte 2005 im Rahmen einer Studie (1) für einen mittelständischen Betrieb ohne Schutzmaßnahmen durch Spam verursachte Kosten von 170 000 Euro pro Jahr. Noch härter trifft es der Studie zufolge Kleinbetriebe, die für jede Spam-Mail 66 Cent verausgaben müssen. Dabei ließen sich viele dieser unerwünschten Mails für nur 4 Cent das Stück verhindern, wenn man im Zuge einer durchdachten Strategie die richtigen Maßnahmen ergriffe. Im selben Jahr errechneten die Analysten von Ferris Research (2) einen jährlichen Schaden durch Spam weltweit von 50 Milliarden Dollar.

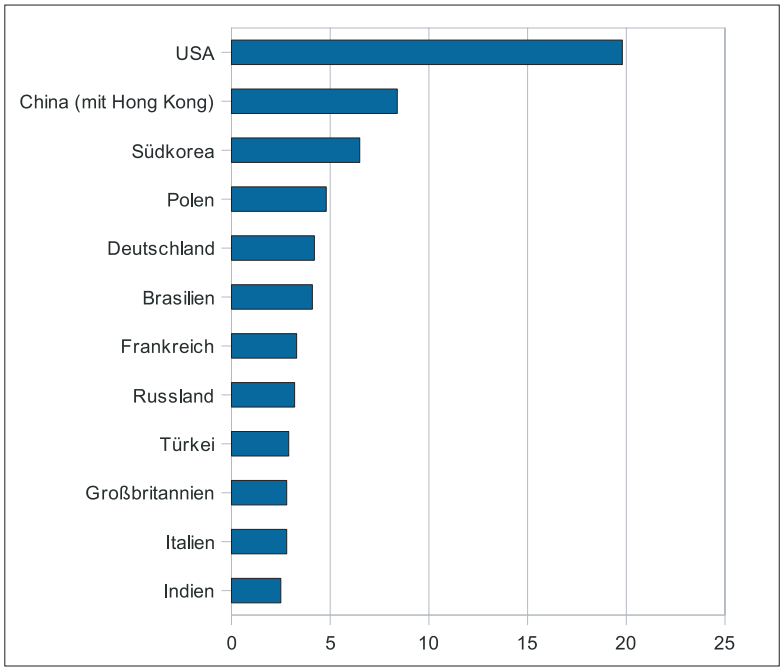

Abbildung 1: Aus diesen Ländern kam nach einer Statistik des Anti-Viren-Herstellers Sophos zwischen April und Juni 2007 der meiste Spam.

Spam-Prävention

Es lohnt sich demnach garantiert, den Datenmüll nicht kampflos hinzunehmen. Für die Gegenwehr lassen sich prinzipiell mindestens drei Verteidigungslinien ziehen, allerdings mit unterschiedlichen Erfolgsaussichten: Da wäre an vorderste Stellung die Prävention, die den Leidensdruck mindestens zu lindern vermag, zweitens die juristische Front – schließlich ist Spam fast überall Gesetzesbruch –, und drittens schützt das Hinterland schließlich eine ganze Batterie technologischer Anti-Spam-Maßnahmen.

Die erste Maßnahme zur Spam-Vermeidung ist die sichere Konfiguration der eigenen Systeme – sowohl der Mailserver wie der Clients. Gäbe es nicht nach wie vor schlecht konfigurierte Mailserver, welche Post von Fremden annehmen und an beliebige Empfänger weiterleiten (Open Relays), und ließen sich nicht gleichzeitig Abertausend angreifbare PCs in Botnetzen als Spam-Schleudern missbrauchen, dann wäre das Problem sehr viel kleiner.

Was zu tun ist, ist bekannt: Firewall und (zumindest für Windows-Clients) Virenschutz sollten obligatorisch sowie die Serverkonfiguration durchdacht sein. Ob sie wirklich wasserdicht ist, kann jeder selbst unter (3) überprüfen. Kein von außen erreichbarer Proxy sollte eine Verbindung zu dem SMTP-Host zulassen, und HTTP- oder PHP-Formulare mit Mailfunktion – ein häufiger Angriffspunkt für Spammer – sind besonders gründlich auf Sicherheitslücken abzuklopfen.

Die zweite Maßnahme betrifft den bewussten Umgang mit der oder den eigenen Mailadresse(n). Nur bekannte Adressen werden bespammt. Andererseits: Völlig unbekannte sind nutzlos. Ein Mittelweg kann darin bestehen, den automatischen Harvestern der Spammer ihr Handwerk zu erschweren, indem man die Mailadresse mit simplen HTML- oder JavaScript-Tricks auf der eigenen Webseite verschleiert. Im einfachsten Fall reicht dafür die hexadezimale Kodierung. Sie ändert nichts an der Lesbarkeit für Menschen, ist aber für automatische Adresssammler zumindest ein Stolperstein. ▶

Tabelle 1: Technologische Anti-Spam-Maßnahmen – Teil 1

Verfahren		Funktionsprinzip	Ort und Zeit
auf IP-Ebene			
	Blacklisting (DNSBLS)	Listen spamverdächtiger IP-Adressen	MTA vor Annahme
	Whitelisting	Listen vertrauenswürdiger IP-Adressen	MTA vor Annahme
	RHSBL	Right Hand Side Black Lists, als Filterkriterium wird die Absender-Domain herangezogen	MTA vor Annahme
	URI-Blacklisting (URIDNSBLS)	Listen von Domains, auf die Links im Spam verweisen	MTA vor Annahme
	Greylisting	SMTP-Verzögerung bei unbekanntem Einlieferer, die reguläre Mailserver tolerieren, Botnetze aber nicht	MTA vor Annahme
	Existenzprüfung von Absender- und Empfängeradresse	Überprüfen, ob Sender und Empfänger existieren – oder gefälscht bzw. geraten sind	MTA vor Annahme
	Frequenzanalysen und Begrenzung abgehender Mails	Provider bemerkt Massenmail-Versand, Begrenzung des abgehenden Mailvolumens	MTA des Providers während des SMTP-Dialogs
auf TCP-Ebene			
	Sperren von Port 25	Blockade abgehender Mails von nicht autorisierten Sendern	Firmen-Firewall vor Versand, auch Provider
Filter			
	heuristische Methoden (rule based filtering)	Erkennen spamtypischer Strings, etwa mittels regulärer Ausdrücke, regelbasierte Untersuchung von Header und/oder Body, meist Scoring-Technik	MTA/MDA nach Annahme
	statistische Methoden	Tests auf Grundlage von Worthäufigkeiten	MTA/MDA nach Annahme
	Prüfsummenvergleich	Abgleich aktueller Mails mit Spam-Fingerprints aus externen Datenbanken	MTA/MDA nach Annahme
Authentifizierung			
	SMTP-Erweiterung	Mailclient authentifiziert sich gegenüber dem Mailserver	MTA im SMTP-Dialog mit dem Client
	MTAMARK	Markierung im DNS für berechtigte Mailserver, die der Empfänger abfragen kann	MTA vor Annahme

Beispiel	Vorteile	Nachteile
Spamhaus, Uceprotect, SORBS, Spamcop u. v. m.	nur IP-Adresse nötig, deshalb geringe Ressourcenbelastung, einfach, gut kombinierbar, effektiv	nur 20 Prozent aller IPv4-Adressen durch Listen abgedeckt, Gefahr von False Positives und False Negatives, stark abhängig von Qualität der Liste, ständige Aktualisierung nötig, Gefahr, Unschuldige durch Sperren kompletter Adressbereiche zu treffen, teils unklare Policies der Betreiber
Certified Senders Alliance (Whitelist der Direktvermarkter)	nur IP-Adresse nötig, deshalb geringe Ressourcenbelastung, einfach, gut kombinierbar, effektiv	wie Blacklists
(http://rhsbl.sorbs.net)	kann Absender-Authentifizierung unterstützen	Domain-Angabe beliebig fälschbar, daher weitgehend ungeeignet
(http://www.surbl.org)	blockiert Spam-Variationen, die dieselbe Zieladresse bewerben	hilft nicht gegen Spam ohne Links
»postgrey«, »greylistd«	geringe Ressourcenbelastung, gut kombinierbar, effektiv gegen direkt sendende Botnetze	Gefahr von False Positives und False Negatives durch inkompatible Konfiguration bzw. Versand über missbrauchte Benutzeraccounts, Gewöhnung der Spammer denkbar
DNS-Abfrage der Absender-Domain/MX-Record, Empfängerabgleich mit lokaler User-DB	Schutz vor Adressfälschung und Spam auf Verdacht	erhöhter Ressourcenbedarf, Gefahr von False Positives: Adressabfrage nicht absolut sicher
Klassifizierung beim Provider	effektiv gegen einzelne Spam-Quellen, kurze Reaktionszeit, Kombination mit Whitelist empfehlenswert	Kooperation aller Provider nötig, E-Mail-Accounts dürfen sich nicht massenhaft automatisch erzeugen lassen, relativ aufwändig
Firewall	einfach, braucht kaum Ressourcen	Gefahr, legitime Sender zu blockieren, wirkt nur gegen Direktversand, nicht gegen Spam von Provideraccounts
RegEx-Filter	Einsatz auf Server und Client möglich, mit anderen Verfahren kombinierbar	ressourcenbelastend, komplette Mail nötig, Gefahr von False Positives und False Negatives durch Fehlklassifikation, hoher Aufwand für die Pflege der Konfiguration
Bayes-Filter	Einsatz auf Server und Client möglich, mit anderen Verfahren kombinierbar	ressourcenbelastend, Trainingsphase erforderlich, komplette Mail nötig, schwer nachvollziehbare Klassifikation, Gefahr von Fehlklassifikation
Vipul's Razor, Pyzor, DDC u. a.	Nutzen der kollektiven Intelligenz zahlreicher Anwender, kompakter als Inhaltsfilter	Gefahr von False Positives, wenn viele etwa einen Newsletter als Spam kennzeichnen, der legal ist, oft effizienter als Blacklists, Zwang zu bestimmter Software für die Prüfsummenbildung
SMTP-AUTH (RFC 2554), SMTP after POP, SMTP after IMAP	kann gegen Address Spoofing wirken	nötige Passworte auf vielen PCs nicht sicher, dann wirkungslos bei korrumpiertem Account
MTAMARK	einfacher als SPF, Intention ähnlich	kaum verbreitet, nicht so differenziert wie SPF

Außerdem empfiehlt sich ein eigenes Mailkonto für öffentliche Foren, Newsletter und dergleichen. Fällt diese Adresse dann in die Hände von Spammern, bleibt wenigstens der Account verschont, welchen man im Regelfall für dienstliche oder private Mails nutzt. Dessen Adresse gibt man wiederum nur an vertrauenswürdige Partner weiter.

Wer es auf die Spitze treiben möchte, verwendet für die Kommunikation, bei der die Adresse besonders leicht publik wird, Wegwerfadressen, welche man beispielsweise mit (4) oder (5) generieren kann. Damit verbreitet sich die eigentliche Adresse ebenfalls nur in einem kontrollierten Rahmen.

Der Eintrag in eine Robinsonliste (6) schützt womöglich vor unerwünschten Botschaften seriöser Werber. Die Schattenseite: Wer sich einträgt, der veröffentlicht auch seine Mailadresse, und ein hartnäckiger Spammer schert sich sicherlich nicht um Robinsonlisten.

Antworten sollte man übrigens auf eine Spam-Mail unter keinen Umständen, denn so verrät man dem Spammer nur, dass es sich um einen wertvollen, aktiv genutzten Account handelt – und noch mehr Spam ist der sichere Lohn.

Rechtsmittel gegen Spam

Prinzipiell kann man sich auch juristisch gegen Spam wehren (die Details erläutern zwei weitere Beiträge von spezialisierten Rechtsanwälten in dieser Ausgabe) – allerdings muss man hierbei mit diversen Schwierigkeiten rechnen. So ist der Spam-Versender meistens schwer zu ermitteln, weil er seine Identität in aller Regel bewusst verschleiert und Rechner unbeteiligter Dritter missbraucht. Selbst wenn er auszumachen ist, lebt er in vielen Fällen im Ausland, wohin der Arm des Gesetzes womöglich nicht reicht, auch wenn es theoretisch ebenfalls für ihn gilt. Ist aber nicht sicher, ob es zu einer Verurteilung kommt, sitzt der Kläger auf dem Kostenrisiko eines Prozesses.

Auch die Strafverfolgungsbehörden – die Redaktion hatte bei der Vorbereitung der Ausgabe Kontakt zu Experten eines Landeskriminalamts – sehen im Spam derzeit keine Priorität und verweisen auf die im Einzelfall geringe Schadenshöhe und Schwierigkeiten bei der Verfolgung ausländischer Mailversender.

Etwas günstiger gestalten sich die Erfolgsaussichten womöglich bei einer Beschwerdestelle. Privatleute können sich beispielsweise per

Tabelle 1: Technologische Ant-Spam-Maßnahmen – Teil 2

Verfahren		Funktionsprinzip	Ort und Zeit
Authentifizierung			
	Pfad-Authentifizierung	Verzeichnis sendeberechtigter Mailserver pro DNS-Domain	MTA vor Annahme
	Krypto-Authentifizierung	Mailsignatur, Key zum Verifizieren im DNS	MTA nach Annahme
Challenge-Response-Verfahren			
		Sender erhält zunächst eine Bounce-Mail, die ihn auffordert, die Sendung zu wiederholen, dabei aber ein bestimmtes Token anzuhängen, oder über einen zweiten Kanal (WWW) z. B. ein Captcha zu lösen	implementiert im MTA
Bezahlverfahren/Proof-of-Work-Verfahren			
		Geld oder Ressourcen gegen Mails	verschieden
Reputationsbasierte Verfahren			
		Bewertung des Senders aufgrund dessen Spam-Aktivität bzw. seiner Zuverlässigkeit als Spam-Melder	im MTA vor Annahme

E-Mail (beschwerdestelle@spam.vzbv.de) an den Bundesverband der Verbraucherzentralen (vzbv) wenden, Firmen an die Wettbewerbszentrale (7). Solche Organisationen können Beschwerden bündeln und effizienter gegen die Verursacher vorgehen.
Auch ein Protest bei dem Provider, aus dessen Netz heraus der Spammer agiert, ist sinnvoll. Ist dieser kooperationsbereit, so ist es unter Umständen möglich, dem Spammer den Zugang zu verlegen oder aber Dritte darauf hinzuweisen, dass sie unfreiwillig Schützenhilfe leisten. Die meisten Provider haben dafür inzwischen auch spezielle E-Mail-Adressen nach dem Muster abuse@provider.org eingerichtet.

Technologische Maßnahmen

Schließlich bleibt dem Verteidiger auch noch ein ganzes Arsenal technologischer Waffen, denen zahlreiche Beiträge der vorliegenden Ausgabe gewidmet sind. Ihre wichtigsten Stärken und Schwächen fasst **Tabelle 1** zusammen. Sie können sowohl zentral beim Mailserver ansetzen wie dezentral beim E-Mail-Client oder auch an beiden Stellen gleichzeitig.

Nur auf Serverebene sinnvoll sind listenbasierte Filter, die spamverdächtige Absender abweisen können, bevor der Server ihre Mails annimmt. Zwar sind sie kein Allheilmittel und können sich auch irren, aber sie arbeiten sehr effektiv, weil allein die – schwer fälschbare – IP-Adresse des Absenders oder der Domain-Name für die Beurteilung ausreichen. Daher verbrauchen sie auch kaum Ressourcen und eignen sich am besten für die massenhafte Vorauswahl.
Anders sieht die Sache bei allen Spielarten von inhaltsbasierten Filtern aus, die sich entweder heuristischer oder statistischer Methoden bedienen. Da sie die gesamte E-Mail vor der Analyse empfangen müssen, um sie danach einer meist rechenintensiven Prüfung zu unterziehen, belasten sie die Ressourcen von Client oder Server deutlich stärker. Dafür erkennen sie auch Spam von bisher unbekannten Absendern.
Häufig kommen hier verschiedene Techniken gemeinsam zum Einsatz, die zusammen einen Score-Wert bilden, der die Spam-Wahrscheinlichkeit einer bestimmten Mail angibt. Das bekannteste freie Anti-Spam-Programm SpamAssasin arbeitet beispielsweise mit einem solchen Scoring-Verfahren. ▶

Beispiel	Vorteile	Nachteile
SPF/SenderID	nur geringer bis mittlerer Ressourcenbedarf, verhindert lokale SMTP-Server	Probleme bei Weiterleitung von Mails, Spammer registrieren Wegwerf-Domains mit SPF-Eintrag
DKIM	gesamte Mail vor Fälschung geschützt	PKI nötig, unwirksam, wenn Private Key nicht gut geschützt, Missbrauch durch Spammer möglich, hoher Ressourcenbedarf
	verteuert Spam	starke Modifikation von SMTP nötig, verschwendet Ressourcen, erschwert Kommiunikation, trifft u. U. den Falschen
E-Mail-Briefmarke, Hashcash, Camram-Projekt	verteuert Spam	Infrastruktur fehlt, trifft u. U. den Falschen, Effizienz unklar, problematisch für legitime Massenversender
viele DNSBLs und kollaborative Inhaltsfilter, zahlreiche Vorschläge für MTA-Registrierung (z. B. ICANN, Lumos)	gut kombinierbar	Gefahr ungerechtfertigter Sippenhaft, schützt nur bedingt gegen Bots

Abbildung 2: Die Startseite eines Anbieters von Wegwerf-E-Mail-Adressen: Solche Adressen leiden nicht unter Spam, sind dafür etwas umständlich in der Handhabung.

Eine gewisse Sonderstellung nimmt das Greylisting ein, das Mails von Unbekannten zunächst verzögert und darauf baut, dass ein legitimer Mailserver den Zustellversuch in diesem Fall wiederholt, ein vom Spammer gekaperter PC hingegen nicht. Entsprechend wirkt es am besten gegen die gefährlichen Botnetze, die zudem oft auch Viren und Trojaner verbreiten. Ein spezieller Greylisting-Artikel in dieser Ausgabe verrät, wie man es am wirkungsvollsten einsetzt.

Abbildung 3: Mit Tricks wie dieser in ein Bild eingebetteten Mail versuchen Spammer, die Filter zu überlisten, glücklicherweise oftmals erfolglos – auch diese Spam-Mail wurde erkannt und aussortiert.

Bei dem Provider fallen Spammer ebenfalls durch ihr Verhalten auf und lassen sich durch Analyse der Mailfrequenz aller Clients entdecken. Provider können schließlich auch durch Blockieren des SMTP-Ports 25 dafür sorgen, dass unberechtigte Clients keine Mail verschicken können.

Ein anderer wesentlicher Angriffspunkt ist die Überprüfung der Absender- und Empfängeradressen auf Existenz sowie auf mögliche Fälschungen. Zwei konkurrierende Techniken für die Absender-Authentifizierung – SPF und DKIM – stellt jeweils ein prominenter Verfechter der jeweiligen Technik in dieser Ausgabe vor.

Schließlich ist es im Kampf gegen den Spam möglich, die kollektive Intelligenz vieler Internetnutzer einzuspannen, die etwa Fingerabdrücke einmal als Spam erkannter Mails sammeln und zentral zur Verfügung stellen oder die Reputation der Absender gemeinsam bewerten. Weitere Beiträge auf den folgenden Seiten erläutern auch diese Technik im Detail.

Am sinnvollsten ist es, alle diese Maßnahmen geschickt zu kombinieren. Das ist etwa auch die Strategie der großen Mailprovider. (Einzelheiten finden sich in einem Beitrag über den Anti-Spam-Kampf des Großproviders Web.de in dieser Ausgabe.) Auch die meisten Anti-Spam-Appliances, von denen ein weiterer Artikel etliche bekannte Vertreter vorstellt, machen sich diesen Vorteil zu Nutze.

Fazit

Spam zählt heute zu den größten Problemen des Internets und vernichtet jedes Jahr gewaltige Geldbeträge, an denen sich wenige skrupellose Gesetzesbrecher bereichern. Hand in Hand geht außerdem ein erhebliches Sicherheitsrisiko durch Malware, die Spammer verbreiten.

Aber die Internetgemeinde ist keineswegs wehrlos. Auf vielen Ebenen ist Widerstand möglich, und jeder kann dazu beitragen. Zwar wird sich das Problem nicht kurzfristig aus der Welt schaffen lassen, aber zumindest seine Folgen lassen sich entscheidend lindern. Schließlich geht es um nicht mehr und nicht weniger als darum, eines der wichtigsten Kommunikationsmedien unserer Zeit benutzbar zu halten. ■■■

Infos

(1) BSI-Spam-Studie: Antispam-Strategien: Unerwünschte E-Mails erkennen und abwehren: (http://www.bsi.de/literat/studien/antispam/antispam.pdf)

(2) Ferris Research: The global economic impact of spam: (http://www.ferris.com/2005/02/24/the-global-economic-impact-of-spam-2005/)

(3) Mail relay testing: (http://www.abuse.net/relay.html)

(4) Spamgourmet: (http://www.spamgourmet.com)

(5) Spam Motel: (http://www.spammotel.com/)

(6) Deutsche Robinsonlisten: (http://www.robinsonlisten.de)

(7) Wettbewerbszentrale: (http://www.wettbewerbszentrale.de)