rapidsoft GmbH
Emmy-Noether-Str. 2, 79115 Freiburg

Spam und SPIT

(Aktuelle Schutzmöglichkeiten und Gegenmaßnahmen)

Moritz Mertinkat
mmertinkat AT rapidsoft DOT de
17.06.2007

Inhaltsverzeichnis

1 Einleitung

In der vorliegenden Arbeit geht es um den Themenkomplex *Spam* im E-Mail- sowie im Telefoniebereich, der vor allem von der technischen Seite beleuchtet wird. Zunächst werden in Kapitel 2 aktuelle Schutzmöglichkeiten und Gegenmaßnahmen gegen E-Mail-Spam beschrieben, darunter Greylisting oder SPF und DomainKeys (DKIM) zur Verifizierung von Absenderadressen. Aber auch auf ältere Techniken wie S/MIME und OpenPGP wird kurz eingegangen. Im darauffolgenden Kapitel 3 wird nach einer kurzen Vorstellung der rechtlichen Situation in Deutschland dann versucht, diese Techniken auf den Telefoniebereich, d.h. auf SPIT zu übertragen – soweit dies überhaupt möglich ist. Zudem werden auch für SPIT angepasste Konzepte wie Reputationssysteme oder Audio-CAPTCHAs diskutiert. Inwieweit die vorgestellten Lösungen bereits ihren Einsatz finden und ob sie sinnvoll genutzt werden (können), versucht der Autor schließlich im Ausblick in Kapitel 4 einzuschätzen.

2 Spam

2.1 Was ist Spam?

Der Begriff *Spam* ist dem Dosenfleisch SPAM (spiced ham) der Firma Hormel Foods entliehen und wurde durch einen Sketch der Komikertruppe Monty Python populär. In diesem Sketch versucht ein Gast ausdrücklich ein Gericht ohne SPAM zu bestellen, die Karte listet jedoch fast jedes Gericht mit SPAM auf. Als der Gast sich darüber aufregt setzt ein Chor mit einem Loblieb auf SPAM ein, bis der Sketch in Chaos verfällt [1]. Bezogen auf Kommunikation hat der Begriff seinen Ursprung vermutlich in Online-Rollenspielen, man bezeichnete dort das Flooding der Textinterfaces mit eigenen Nachrichten als SPAM. Später ging der Begriff vom Usenet auch auf E-Mails über, die ungewünschte (Werbe-)nachrichten enthielten. So wie in Monty Pythons Sketch ist auch hier – im übertragenen Sinne – die Kommunikation durch Spam gestört.
Spam bezieht sich jedoch nicht ausschließlich auf E-Mails, sondern meint generell die Störung bestimmter Kommunikationskanäle durch Überflutung selbiger mit ungewünschten bzw. unnötigen Informationen. Es gibt also verschiedene Arten von Spam, von denen hier aber nur auf zwei näher eingegangen werden soll. Zum einen der eben schon genannte E-Mail-Spam und zum anderen (in Kapitel 3) der Spam über Internet-Telefonie, auch *SPIT* genannt.

2.1.1 Verschiedene Arten

Im E-Mail-Bereich haben sich im Laufe der Jahre neben der vergleichsweise harmlosen „unerwünschten E-Mail-Werbung“ (Unsolicited Commercial E-Mail) einige besondere Formen herausgebildet, die im Folgenden kurz beschrieben werden sollen.

Viren- und Trojaner-Spam. Bei Viren- und Trojaner-Spam handelt es sich um E-Mails mit zumeist ausführbaren Anhängen, die entweder darauf abzielen Daten zu vernichten oder aber – und dies wird immer populärer [2] – Schadsoftware auf dem Computer des Empfängers zu installieren, um selbigen dann für eigene Zwecke zu benutzen.

Phishing-Spam. In eine etwas andere Richtung geht es beim *Phishing-Spam* – hier wird versucht, mittels fingierter E-Mails an vertrauliche Daten des Empfängers zu kommen. So handelt es sich in knapp 90 % [3] aller Fälle um gefälschte E-Mails von Kreditinstituten und anderen Bezahlsystemen wie z.B. PayPal, da die sogenannten Phisher hier mit dem größten Gewinnpotential rechnen. Symantecs *Internet Security Threat Report* [4] vom März 2007 gibt für den Finanzsektor immerhin noch 84 % an.

Aktienspam. Als *Aktienspam* bezeichnet man E-Mails mit Werbung für eine bestimmte Aktie. Dabei handelt es sich fast ausschließlich um sogenannte Penny-Stocks, d.h. Aktien mit einem Kurs im Centbereich und sehr geringem Handelsvolumen (von oftmals bereits insolventen Firmen). Der Spammer (oder dessen Auftraggeber) kauft vor dem Versand die beworbene Aktie und versucht diese nach Anstieg des Kurses wieder zu verkaufen. Aufgrund des geringen Handelsvolumens führen bereits wenige Käufe zu enormen Schwankungen und kurzfristigen Kursanstiegen. Sobald allerdings große Stückzahlen wieder verkauft werden, sinkt der Wert meist auf ein Niveau unterhalb des ursprünglichen Kurses. [5] Obwohl es Aktienspam schon einige Jahre gibt, ist ein enormen Anstieg seit Februar 2007 zu verzeichnen.

2.1.2 Herkunft des Spams

Noch vor wenigen Jahren kamen die meisten Spam E-Mails aus den USA, da dort bereits viele breitbandige Internetanschlüsse zu günstigen Preisen verfügbar waren. Zudem gab es in den USA lange kein Gesetz gegen unverlangte Massen-E-Mails, was sich aber mittlerweile mit dem *CAN-SPAM Act* [6] vom 01.01.2004 geändert hat.

Seitdem es auch in vielen anderen Ländern schnelle Internetanbindungen gibt, hat sich die Herkunft der Spam-E-Mails etwas verlagert; vor allem nach Osteuropa und Asien – nicht zuletzt um einer Strafverfolgung aus westlichen Länder zu entgehen bzw. diese zu erschweren.

Betrachtet man nur den Spam in Deutschland, so ist hier Polen die führende Spam-Nation mit 9 % Spam-Anteil, gefolgt von China und Frankreich, die jeweils 7 % beisteuern. [7]

2.1.3 Status quo

In den letzten fünf Jahren ist das Spam-Aufkommen deutlich angestiegen. Ging man bisher von 40-60 % des gesamten Mailverkehrs aus, so weisen neuere Statistiken Werte um 90 %

[8] auf (bei T-Online, so berichtete mir neulich ein dort für die Mailserver zuständiger Administrator, läge das Spam-Aufkommen sogar bei etwa 98-99 %).

50 Mrd. Dollar Schaden. Hierdurch entsteht weltweit ein enormer volkswirtschaftlicher Schaden, der im Jahr 2005 durch das Marktforschungsinstitut Ferris Research auf 50 Mrd. Dollar beziffert wurde, wobei 17 Mrd. Dollar alleine auf die USA entfallen. Als Hauptursache nennt die Studie das Absinken der Produktivität der Mitarbeiter, wenn diese ihren E-Mail-Account nach Spam durchsuchen müssten. Deshalb sei der Schaden in Industrieländern mit hohen Gehältern auch am größten.

Mehr Durchsatz. Seit 2005 ist das Spam-Aufkommen stark angestiegen, allerdings gibt es auch immer bessere Schutzmechanismen und -möglichkeiten. Das Problem ist hierbei, dass diese neuen Möglichkeiten zum einen oftmals nicht auf die spezifischen Anforderungen der Firmen abgestimmt werden und zum anderen für den Anwender ein trügerisches Sicherheitsgefühl entstehen kann. Aber auch durch die automatische Aussortierung von wichtigen E-Mails, die fälschlicherweise als Spam eingestuft wurden (*false-positives*), kann ein erheblicher Schaden entstehen.

2.2 Schutzmöglichkeiten

Auch wenn bereits Maßnahmen gegen den Versand von Spam ergriffen werden (Kapitel 2.3: Gegenmaßnahmen), so wird es trotzdem auf absehbare Zeit kein spam-freies Internet geben. Daher ist es wichtig, sich so gut wie möglich vor der ungewünschten E-Mail-Flut zu schützen – allerdings werden nicht nur die Schutzmechanismen immer intelligenter und ausgereifter, sondern auch die Automatismen (Bots) der Spammer.
Im folgenden wird nun versucht, einen möglichst umfassenden Überblick über die aktuell verfügbaren Schutzmechanismen zu geben.

2.2.1 Bayes-Filter

Ein Bayes-Filter ist ein statistischer, selbstlernender Filter, der sich des bayesschen Wahrscheinlichkeitsbegriffs bedient. Dieser geht auf den Pfarrer und Mathematiker Thomas Bayes zurück, der im 18. Jahrhundert in England lebte.

Für die Beurteilung der Spam-Wahrscheinlichkeit einer E-Mail wird diese zunächst in Worte zerlegt und dann für jedes dieser Worte eine Wahrscheinlichkeit berechnet, die die Häufigkeit des Auftauchens in dieser sowie in allen bereits eingegangenen E-Mails und die Wahrscheinlichkeit, dass eine E-Mail überhaupt Spam ist, berücksichtigt. Die neu errechneten Werte werden in einer Datenbank gespeichert und können so in die Bewertung der nächsten E-Mail eingehen, die wiederum diese Werte anpasst und neue hinzufügt.

Bogus? Als Beispiel für einen Bayes-Filter sei hier der ursprünglich von Eric S. Raymond entwickelte *bogofilter*[1] genannt, der nur kurz nach der Veröffentlichung des Artikels „A Plan for Spam“ [9] im August 2002 erschien. Seitdem wird er kontinuierlich weiterentwickelt und gilt mittlerweile als stabil.

Bayes-Filter werden normalerweise auf dem Mailserver des Empfängers eingesetzt, um bereits dort die E-Mails zu sortieren, aber auch ein Einsatz beim Endbenutzer selbst, wie bspw. der *Junk-Filter* in Mozillas Thunderbird, ist möglich.

Eine Weiterentwicklung des Bayes-Filter ist der sogenannte Markow-Filter [10], der nicht nur einzelne Worte, sondern ganze Satzteile (Wortkette, Markow-Kette) zur Bewertung der Spam-Wahrscheinlichkeit heranzieht.

2.2.2 Schwarze, weiße und graue Listen

Whitelisting und *Blacklisting* zählen zu den am häufigsten eingesetzten Schutzmechanismen gegen unerwünschte Nachrichten, sowohl server- als auch client-seitig. Allerdings sind diese Methoden auch die ineffizientesten. Beim Blacklisting wird der Inhalt oder der Absender einer E-Mail mit bestimmten Ausdrücken einer *Blacklist* verglichen. Werden ein oder mehrere Ausdrücke in der E-Mail gefunden, so wird diese aussortiert oder entsprechend gekennzeichnet zugestellt. Dabei ist die Erkennungsrate zumeist nicht so hoch wie beim Bayes-Filter, da die Blacklist je nach Umgebung manuell gepflegt werden muss und auch leicht umgangen werden kann (z.B. ‚V14gra‘ statt ‚Viagra‘). Allerdings können Blacklists in Zusammenhang mit anderen Methoden trotzdem sehr wirksam sein, da sich hierdurch mit wenig Rechenzeit eine grobe Vorsortierung realisieren lässt. So werden beim bekannten Spamfilter *SpamAssassin* u.a. DNS-Realtime-Blacklists (DNSRBLs [11]) für die Verifizierung von Absenderadressen eingesetzt, bevor der eigentliche (wesentlich rechenintensivere) Scanvorgang startet.
Whitelists wiederum stellen das Gegenstück zur Blacklist dar: E-Mails, die eine Übereinstimmung mit der Whitelist haben, werden auf jeden Fall zugestellt. Whitelists enthalten in der Regel gültige Absenderadressen von bekannten Kommunikationspartnern und sind den Blacklists vorgeschaltet.

Keine Schwarz-Weiß-Malerei. Mit dem Ausdruck *Greylisting* bezeichnet man ein relativ neues Verfahren zur Spam-Abwehr, das ähnlich der Blacklists und Whitelists funktioniert, aber Nachrichten nicht permanent zurückweist oder dauerhaft annimmt. Beim ersten Zustellungsversuch der E-Mail von einem unbekannten Absender antwortet der Mailserver mit einem temporären Fehler und nimmt die E-Mail erst beim zweiten Anlauf entgegen. Da die meiste Spam-Software (bislang noch) keinen zweiten Versuch unternimmt, ist auf diesem Weg eine effektive Spam-Abwehr möglich, die den Spam auf bis zu 10 % reduzieren

[1] bogofilter
http://bogofilter.sourceforge.net/

kann. [12] Das Verfahren ist insofern elegant, da es rein auf die bestehenden Möglichkeiten des Simple Mail Transfer Protocols (SMTP) aufsetzt und nur einen geringen Wartungsaufwand nach sich zieht. Zudem lässt sich hiermit die Whitelist automatisch trainieren.

Aufgeschlüsselt. Verbindet sich nun ein Client mit dem Mailserver und versucht eine E-Mail einzuliefern, so kann der Mailserver während der SMTP-Session folgende drei Merkmale in Erfahrung bringen: die IP-Adresse des Clients, die Absender- sowie die Empfängeradresse der E-Mail (`MAIL FROM` und `RCPT TO`). Ist dem Mailserver diese Kombination noch nicht bekannt, so verweigert er dem Client unter Rückgabe eines temporären Fehlers (451 bzw. 4.7.1 „You have been greylisted. We will accept this mail from you in 15 minutes.“) die Übermittlung der Nachricht, speichert aber die Kombination in einer Datenbank (der sogenannten Greylist). Handelt es sich um einen „guten“ Client, der sich an die RFC-Standards hält, so wird er eine erneute Zustellung der Nachricht versuchen. Dies geschieht meistens innerhalb der ersten Stunde mehrfach[2]. Existiert bei der erneuten Zustellung nun die Kombination aus IP-, Absender- und Empfängeradresse in der Greylist, so wird die E-Mail angenommen und zugestellt. Sinnvollerweise wird auch die Whitelist um diese Informationen ergänzt, um bei zukünftigen E-Mails mit dieser Kombination auf das Greylisting und somit auf eine Verzögerung bei der Zustellung verzichten zu können. Erfolgt keine weitere Zustellung innerhalb ersten Stunde, so wäre es denkbar die IP-Adresse des Clients für 24 Stunden zu blockieren oder erneute Verbindung dieses Clients künstlich zu bremsen.
Abbildung 1 zeigt beispielhaft eine SMTP-Session zum Mailserver der UNI Freiburg.

```
# telnet mailgateway2.uni-freiburg.de smtp

Trying 132.230.2.212...
Connected to mailgateway1.uni-freiburg.de.
Escape character is '^]'.

220 mailgateway1.uni-freiburg.de ESMTP I'm pleased to meet you.
HELO mertinkat.net
250 mailgateway1.uni-freiburg.de Hello mertinkat.net [xxx.xxx.xxx.xxx]
MAIL FROM: <trashcan@mertinkat.net>
250 OK
RCPT TO: <mmertinka@informatik.uni-freiburg.de>
451-You have been greylisted.
451 We will accept this mail from you in 15 minutes.
QUIT
221 mailgateway1.uni-freiburg.de closing connection
```

Abbildung 1: Erst beim zweiten Zustellversuch mit den gleichen Parametern wird die E-Mail angenommen.

[2] Retry schedule bei *qmail* berechnet sich nach der Formel: $(z-1)^2 * 400$ Sekunden, $z \in [1, 40]$, wobei z der Zustellungsversuch ist

2.2.3 Content-Scanner

Als Content-Scanner werden Methoden bezeichnet, die – zumeist während und kurz nach der Zustellung auf dem eingehenden Mailserver – den Inhalt der E-Mails näher analysieren. Dies erfolgt zwar auch durch White- und Blacklisting, allerdings wesentlich oberflächlicher.

Tiefgründiges. Beim Content-Scanning werden die einzelnen MIME-Parts der E-Mail überprüft und bewertet. So lässt sich zum Beispiel prüfen, ob die E-Mail eine korrekte Anrede und einen Namen in den Headern aufweist (die auf den jeweiligen Empfänger zutreffen) oder ob es einen HTML-Teil gibt, dessen Inhalt grob mit dem im Text-Teil übereinstimmt. Bei Spam-E-Mails gibt es meistens keinen Text-Teil, da sich mit Hilfe von HTML die Links besser verbergen lassen und zudem eingebettete Bilder direkt angezeigt werden können.
Weiterhin lässt sich überprüfen, ob z.B. JavaScript im HTML-Code vorkommt oder ob viele grelle Farben in Text und Hintergründen eingesetzt werden.

Fünf, setzen. Der bereits erwähnte Spamfilter *SpamAssassin* nutzt dafür ein Punktesystem und bewertet den Inhalt der E-Mail je nach Gesichtspunkt positiv oder negativ. Erhält die E-Mail mehr als fünf Punkte[3], so wird sie als Spam markiert und ggf. im weiteren Verlauf aussortiert.
Dabei schlägt ein falsches Encoding für den Textteil (Base64, um z.B. einfache Blacklists zu umgehen) gleich mit 1,9 Punkten zu Buche. Aber auch ein Abmeldelink in einem gewöhnlichen und erwünschten Newsletter kann bis zu 3,2 Punkte kosten. Mit die höchsten Strafpunkte vergibt SpamAssassin aber beim Auffinden einer in der E-Mail genannten Domain, die sich in der „Spam URI Realtime Blocklist“[4] befindet. Hierfür fallen je nach Art der Blocklist 3,0 bis 4,5 Punkte an.
Auszug aus den Headern einer von SpamAssassin gescannten E-Mail:

[3] Es handelt sich hier, wie auch bei den im folgenden genannten Werten, um die Standardeinstellung, die sich über Konfigurationsdateien leicht anpassen lässt.
[4] SURBL Lists
http://www.surbl.org/

```
X-Spam-Status: Yes, score=26.2 required=5.0 tests=BAYES_99,BODY_ENHANCEMENT2,
        HELO_DYNAMIC_HCC,HELO_DYNAMIC_IPADDR2,HTML_50_60,HTML_MESSAGE,
        URIBL_AB_SURBL,URIBL_JP_SURBL,URIBL_OB_SURBL,URIBL_SBL,URIBL_SC_SURBL,
        URIBL_WS_SURBL autolearn=spam version=3.1.7-deb
X-Spam-Report:
        *  3.5 BAYES_99 BODY: Bayesian spam probability is 99 to 100%
        *      [score: 1.0000]
        *  4.1 HELO_DYNAMIC_HCC Relay HELO'd using suspicious hostname (HCC)
        *  3.8 HELO_DYNAMIC_IPADDR2 Relay HELO'd using suspicious hostname (IP
        *      addr 2)
        *  0.7 BODY_ENHANCEMENT2 BODY: Information on getting larger body parts
        *  0.1 HTML_50_60 BODY: Message is 50% to 60% HTML
        *  0.0 HTML_MESSAGE BODY: HTML included in message
        *  1.6 URIBL_SBL Contains an URL listed in the SBL blocklist
        *      [URIs: tnens.com]
        *  3.8 URIBL_AB_SURBL Contains an URL listed in the AB SURBL blocklist
        *      [URIs: tnens.com]
        *  4.1 URIBL_JP_SURBL Contains an URL listed in the JP SURBL blocklist
        *      [URIs: tnens.com]
        *  4.5 URIBL_SC_SURBL Contains an URL listed in the SC SURBL blocklist
        *      [URIs: tnens.com]
```

Diese E-Mail wurde mit 26,2 Punkten bewertet und korrekterweise als Spam eingestuft (`X-Spam-Status: Yes`). Wie aus dem obigen Auszug ersichtbar, gibt es auch in SpamAssassin zusätzlich einen Bayes-Filter, der in den Standardeinstellungen ab 12 Punkten die E-Mail als Spam hinzulernt (`autolearn=spam`) und sich somit selbst trainiert. Bei einer Punktzahl von -1 und weniger wird die E-Mail als Ham hinzugelernt; im Bereich dazwischen findet kein Training des Bayes-Filters statt. Der Vorteil bei dieser Vorgehensweise ist, dass – bei gleichzeitiger Stabilisierung der Trennschärfe – die Wortliste des Filters nicht unnötig groß wird, weil nur E-Mails trainiert werden, die aufgrund von vorher angewendeten Regeln mit hoher Wahrscheinlichkeit Spam oder Ham sind. Ein Nachteil ist aber, dass bei harmloseren Spam-E-Mails kein Training des Filters stattfindet.

2.2.4 Virenscanner

Virenscanner funktionieren ähnlich den Content-Scannern und prüfen die E-Mail inklusive der Attachments auf Viren und Trojaner. SpamAssassin wird zumeist mit dem unter der GPL stehenden – und somit frei verfügbaren – Virenscanner *ClamAV* betrieben, es funktioniert aber auch jeder andere Virenscanner, der mit E-Mail-Daten umgehen kann.
Gerade in diesem Bereich gibt es immer wieder Exploits (also speziell präparierte E-Mails), um die Virenscanner ausser Gefecht zu setzen. Auch werden im Phishing-Bereich häufig Trojaner in Archiven mit gesetztem Kennwort verschickt, deren Inhalt der Virenscanner dann nicht prüfen kann. Je nach Einstellung und Virenscanner können solche Anhänge aber auch blockiert werden, ebenso wie unbekannte ausführbare Dateien.

2.2.5 Absenderverifizierung durch Freischalt-Link

Von den erwähnten Vorgehensweisen, Spam abzuwehren, ist das Whitelisting mit das wirksamste Mittel – allerdings auch in der Administration das aufwendigste. Bezieht sich die Whitelist auf die Absenderadresse, was den Normalfall darstellt, so muss die E-Mail-Adresse jenes Absenders vorab bekannt sein, um von diesem E-Mails zu empfangen. Was im privaten Bereich noch möglich erscheint, ist bei Firmen oder im öffentlichen Sektor ein Ding der Unmöglichkeit. Bei der Absenderverifizierung durch einen Freischalt-Link wird nun dem Absender im Falle, dass seine E-Mail Adresse noch nicht in der Whitelist existiert, eine Nachricht zugestellt, in der ihm mitgeteilt wird, dass die E-Mail beim Empfänger eingeliefert aber noch nicht zugestellt wurde. Weiterhin enthält die Nachricht einen Link sowie zumeist einen Code, mit dem sich der Absender verifizieren kann. Sobald dies geschehen ist, wird die bereits versandte E-Mail zugestellt und die Absenderadresse der Whitelist hinzugefügt.
Erfolgt keine Freischaltung der Absenderadresse, so wird die wartende E-Mail nach einer gewissen Zeit verworfen. Bei einem Spam-Bot ist die Wahrscheinlichkeit also sehr hoch, dass die E-Mail den Empfänger niemals erreicht.
Ein Problem stellen hierbei allerdings legitime E-Mails von einer automatisierten Quelle dar, also z.B. abonnierte Newsletter. Daher wird die Absenderverifizierung meistens mit einem Spamfilter kombiniert, so dass eine Freischaltung nur dann nötig wird, wenn der vorgeschaltete Filter die E-Mail nicht eindeutig als Spam oder Ham einstufen kann.

2.2.6 One-Time-E-Mail-Adressen

Für Registrierungen bei Foren oder für den Download von Software wird häufig eine E-Mail-Adresse benötigt, aber nicht alle Anbieter gehen mit den eingegebenen Adressen im Sinne des Bundesdatenschutzgesetzes (BDSG) um, sofern diese überhaupt daran gebunden sind. Aus diesem Grund haben sich einige kostenlose Dienste etabliert, die sogenannte One-Time- oder auch Wegwerf-E-Mail-Adressen anbieten. Einer der ältesten Dienste ist „Spamgourmet“[5], bei dem man sich eine E-Mail-Adresse registrieren kann, die nur eine bestimmte Anzahl E-Mails an die eigene Adresse weiterleitet. Andere Dienste bieten auch E-Mail-Adressen ohne Registrierung und Weiterleitung an – dort reicht meist die Eingabe eines beliebigen Account-Namens, um Zugriff auf dessen Inhalt zu bekommen. Da jeder andere, der den Namen des Accounts kennt, ebenso Zugriff auf die E-Mails hat, sollten solche Dienste unter keinen Umständen für wichtige E-Mails genutzt werden. Grundsätzlich ist aber auch bei Weiterleitungs-Diensten Vorsicht geboten, da hier E-Mails abgefangen werden könnten.

[5] Spamgourmet
http://www.spamgourmet.com

2.3 Gegenmaßnahmen

Während in Kapitel 2.2 die Schutzmechanismen vorgestellt wurden, geht es in den folgenden Abschnitten darum, welche Maßnahmen bereits jetzt existieren, um sich nicht nur wirksam vor Spam zu schützen, sondern diesen möglichst effektiv zu unterbinden. Zugleich wird aber auch ein Ausblick auf neue Techniken gegeben, die in Zukunft eine wichtige Rolle in der Spam-Vermeidung spielen könnten.

2.3.1 Signierte E-Mails

Zum sicheren Signieren und Verschlüsseln von Daten im Internet haben sich asymmetrische Verschlüsselungsverfahren durchgesetzt, d.h. Verfahren bei dem jeder Kommunikationspartner ein Schlüsselpaar besitzt (einen *private* und *public key*). Was mit dem einen Schlüssel signiert bzw. kodiert wird, kann mit dem Gegenstück überprüft respektive dekodiert werden.

Im Bereich E-Mail haben sich diesbezüglich zwei Standards herausgebildet, die jedoch nicht zueinander kompatibel sind, obwohl beide Standards dieselben kryptographischen Verfahren nutzen. Zum einen gibt es S/MIME, das bereits 1995 als RFC veröffentlicht wurde, aber erst in Version 2 (ab 1998) eine nennenswerte Verbreitung fand. Zum anderen das seit 1996 existierende OpenPGP, das auf Phil Zimmermanns PGP aufbaut. Während S/MIME eine Erweiterung des MIME Formats darstellt und auf X.509-Zertifikaten basiert, nutzt OpenPGP ein „Netz des Vertrauens“. Hier gibt es keine *Certificate Authority* (CA) wie bei S/MIME, die mit einem Zertifikat die Identität des Besitzer beurkundet und diese an dessen öffentlichen Schlüssel bindet, sondern die PGP-Nutzer signieren selbst die Schlüssel anderer Nutzer (die sie kennen). Dabei kann ein Schlüssel (im Gegensatz zu einem X.509-Zertifikat) mehrfach signiert werden, was in etwa einem höheren Trustlevel bei den X.509-Zertifikaten entspricht.

Was beiden Standards gemein ist: Sie erfordern die Unterstützung des E-Mail-Clients. Unterstützt also der E-Mail-Client des Empfängers nicht den vom Sender verwenden Standard, so kann die Nachricht nicht (oder nur mit deutlichem Mehraufwand) auf eine gültige Unterschrift überprüft oder dechiffriert werden.

S/MIME und OpenPGP sind für sich selbst genommen noch keine Spam-Gegenmaßnahme, denn auch ein Spammer kann E-Mails signieren. Würde man allerdings nur solche E-Mails akzeptieren, die eine gültige Unterschrift aufwiesen, so könnte man damit sicherlich einen Großteil der Spam-E-Mails herausfiltern. Das Problem ist hierbei allerdings die mangelnde Akzeptanz, woran nicht zuletzt inkompatible Standards und unzureichende Unterstützung in den E-Mail-Clients eine Rolle spielen.

Selbst große Firmen, die wichtige und vertrauliche Dokumente wie Rechnungen oder Mahnungen an Kunden verschicken, nutzen meist noch keine digitale Signatur. Der Kunde kann im Zweifelsfall also nicht prüfen, ob die erhaltene Rechnung authentisch ist. Genau

diese (vermeidbare) Lücke machen sich nun Spammer als auch Phisher zunutze, indem sie gefälschte Dokumente verschicken, die den Originalen zum Verwechseln ähnlich sehen. Den Schaden hat meist der Empfänger solcher E-Mails, nicht der Absender. [13, 14]

Sender Policy Framework (SPF). Das Sender Policy Framework (kurz SPF) ist eine Technik, die das Fälschen von Absender-Adressen in E-Mails erschweren soll. Dazu wird im DNS einer Domain ein Resource Record (RR) hinterlegt, der bestimmt welche Mailserver für diese Domain E-Mails versenden dürfen. Der Resource Record kann dabei vom Typ *SPF* oder alternativ *TXT* sein. Beim Empfang einer E-Mail wird die `MAIL FROM`- und `HELO`-Identität ausgewertet und mittels einer DNS-Anfrage überprüft, ob der einliefernde Mailserver im SPF- bzw. TXT-RR der Absender-Domain hinterlegt ist. Die E-Mail-Header bleiben unbeachtet, da SPF nur auf SMTP-Ebene arbeitet. Ein Problem ergibt sich allerdings bei einer (legitimen) Weiterleitung der E-Mail, da hier die meisten Mailserver die ursprüngliche `MAIL FROM`-Identität beibehalten, der weiterleitende Mailserver aber im Allgemeinen nicht im SPF-RR der ursprünglichen Domain hinterlegt ist. Abbildung 2 verdeutlicht diesen Sachverhalt. Es gibt dafür zwei Lösungsansätze: Zum einen kann man auf eine SPF-Prüfung der umleitenden Domain verzichten, da diese dem Empfänger im Normalfall bekannt sein sollte. Zum anderen kann ein Mailserver beim Weiterleiten die `MAIL FROM`-Identität auf seine eigene Domain umschreiben und somit auch Verantwortung für etwaige Bounces übernehmen. Dieses *Sender Rewriting Scheme (SRS)* genannte Verfahren ist der vom SPF-Projekt präferierte Lösungsansatz.

Sender ID. Microsofts Sender ID baut auf SPF auf, bietet aber die Möglichkeit den Absender auch über die E-Mail-Header zu überprüfen. D.h. es wird neben der Überprüfung der `MAIL FROM`- bzw. `HELO`-Identität auf SMTP-Ebene auch die Überprüfung der Header auf RFC 2822-Ebene ermöglicht. Mittels des sogenannten *PRA-Algorithmuses*[6] wird zunächst versucht, die E-Mail-Adresse des letzten Senders[7] aus verschiedenen Headern (`Resent-Sender`, `Resent-From`, `Sender` und `From`) zu extrahieren. Danach wird eine DNS-Anfrage an die Domain des gefundenen Senders gestellt, die – wie auch bei SPF – diejenigen Mailserver zurückliefert, die für die gegebene Domain E-Mails versenden dürfen.

Ist einer dieser gültigen Mailserver identisch mit dem, der die E-Mail eingeliefert hat, so ist davon auszugehen, dass der Absender nicht gefälscht ist.

Da Sender ID nicht nur die `MAIL FROM`- bzw. `HELO`-Identität überprüft, ist die Forwarding-Problematik (wie bei SPF) nicht gegeben (Sender ID lässt sich jedoch auch so einstellen, dass es kompatibel zu SPF ist und nur die Daten aus dem SMTP-Layer auswertet). Insgesamt ist dieses Verfahren einfacher und auch weniger fehleranfällig als SPF, allerdings

[6] RFC 4407: Purported Responsible Address in E-Mail Messages

[7] Der „letzte Sender“ ist im Normalfall der ursprüngliche Absender, im Falle einer Weiterleitung kann es aber auch ein anderer Mailserver sein. Jeder weiterleitende Mailserver sollte dabei einen `Resent-From`-Header einfügen, damit der PRA-Algorithmus zuverlässig funktioniert.

```
MAIL FROM: <alice@domain1>
RCPT TO: <bob@domain2>
DATA
From: Alice <alice@domain1>
To: Bob <bob@domain2>
Subject: Discussion on SPF
[...]
```

Der Mailserver von *domain2* empfängt eine E-Mail von *alice@domain1*. Nun hat der Benutzer *bob* allerdings eine Weiterleitung an *bob@domain3* eingerichtet, an die der Mailserver diese E-Mail weiterleitet. Dabei benutzt er jedoch die ursprüngliche `MAIL FROM`-Identität (grün hervorgehoben).

```
MAIL FROM: <alice@domain1>
RCPT TO: <bob@domain3>
DATA
From: Alice <alice@domain1>
To: Bob <bob@domain2>
Subject: Discussion on SPF
[...]
```

Der Mailserver von *domain3* überprüft nun beim Empfangen dieser E-Mail mittels SPF, ob der sendende Mailserver (von *domain2*) berechtigt ist, E-Mails von *domain1* zu senden. Da im DNS SPF-RR von *domain1* korrekterweise auch *nur* der Mailserver von *domain1* hinterlegt ist, scheint der Absender gefälscht zu sein und die E-Mail wird abgelehnt.

Abbildung 2: Problem bei SPF mit E-Mail-Weiterleitungen.

bisher kein Standard.

Anmerkung: Die Arbeitsgruppe *MARID* der IETF, die 2004 ins Leben gerufen wurde, um aus Microsofts Caller ID, SPF und einigen weiteren Vorschlägen ein Standardverfahren zur Überprüfung von Mailabsendern im DNS zu verabschieden, wurde mittlerweile aufgrund interner Auseinandersetzungen [15] wieder aufgelöst. Bis zuletzt versuchte man an Sender ID (Zusammenschluss von Caller ID und SPF) festzuhalten, obwohl es heftige Kritik aus den eigenen Reihen bzgl. des von Microsoft patentrechtlich geschützten PRA-Algorithmuses gab, was schlussendlich zur Ablehnung dieses Verfahrens führte.

DomainKeys Identified Mail (DKIM). Das Konzept hinter DomainKeys stammt ursprünglich von Yahoo! und wurde im Mai 2007 als RFC 4871 veröffentlicht. Mit DomainKeys lässt sich dabei nicht nur der Absender überprüfen, sondern auch, ob die E-Mail unversehrt beim Empfänger angekommen ist. Realisiert wird dies durch ein asymmetrisches Verschlüsslungsverfahren, dessen privater Schlüssel (private key) nur dem Mailserver[8] bekannt ist und dazu genutzt wird, die ausgehende E-Mail digital zu signieren. Der öffentlich Schlüssel (public key) wird im DNS der Absender-Domain (als TXT-RR unterhalb

[8] Es besteht auch die Möglichkeit mehrere Mailserver mit demselben private key zu betreiben.

_domainkey.domain) publiziert und kann beim eingehenden Mailserver dazu verwendet werden, die E-Mail auf Echtheit zu überprüfen. [16, 17]

Abbildung 3 zeigt eine mit DomainKeys signierte E-Mail. Beim Empfang der E-Mail wird zunächst überprüft, ob die Domain aus dem From-Header der Domain im d=-Feld der DKIM-Signature entspricht. Ist dies der Fall, wird versucht den öffentlichen Schlüssel im DNS abzufragen; im Beispiel also aus dem TXT-RR unterhalb von dkim-enabled-mails._domainkey.mertinkat.net. Anschließend wird ein Hash (SHA256) aus den Header-Feldern im h=-Feld und der Nachricht errechnet und mit dem RSA-dechiffrierten Wert aus dem b=-Feld verglichen. Nur wenn diese Werte übereinstimmen ist sichergestellt, dass der Absender authentisch ist.

```
DKIM-Signature: v=1; a=rsa-sha256; s=dkim-enabled-mail; d=mertinkat.net;
  c=simple/simple; q=dns/txt;
  h=received:from:to:subject:date:message-id;
  b=AuUoFEfDxTDkHlLXSZEpZj79LICEps6eda7W3deTVFOk4yAUoqOB
    4nujc7YopdG5dWLSdNg6xNAZpOPr+kHxt1IrE+NahM6L/LbvaHut
    KVdkLLkpVaVVQPzeRDI009SO2Il5Lu7rDNH6mZckBdrIx0orEtZV
    4bmp/YzhwvcubU4=;
Received: from mail.mertinkat.net (mail.mertinkat.net [217.160.111.22])
  by mail.rapidsoft.de with SMTP; 12 Jun 2007 19:07:55 -0000
From: Moritz Mertinkat <moritz@mertinkat.net>
To: Stefan Becker <sbecker@rapidsoft.de>
Subject: Ist DKIM bereits eingerichtet?
Date: Tue, 12 Jun 2007 21:07:53 +0200
Message-ID: <466EEF09.6050508@mertinkat.net>

Wie ist der Stand?

Gruß Moritz
```

Abbildung 3: DKIM-signierte E-Mail.

2.3.2 Neue E-Mail-Protokolle

Das aktuelle E-Mail-Protokoll *SMTP* stammt in seiner Ursprungsfassung aus dem Jahr 1982, als sich das Internet noch in der frühen Entwicklungsphase befand und lediglich Forschungseinrichtungen und wenigen Universitäten zugänglich war. Damals ahnte wohl niemand, dass dieses Protokoll ganze 25 Jahre später in kaum abgewandelter Form noch immer existieren würde.

Das Problem ist, dass die Ausgangslage heute eine völlig andere ist — statt weniger Universitäten benutzen mehrere 100 Millionen Menschen täglich das Netz. Die Entwickler der Protokolle hatten damals aber vor allem eins im Sinn: einfache und möglichst kleine Strukturen. An sichere Kommunikation und Authentifizierung von Daten sowie deren Herkunft dachte zunächst niemand, es ging eher um die grundsätzliche Funktionalität, zumal die Benutzer ja zunächst noch einem kleinen Kreis von bekannten Einrichtungen angehörten. Genau dies führt aber heute dazu, dass E-Mail-Spam in dieser Art und Weise überhaupt möglich ist (unabhängig von Sicherheitslücken in der Implementation). Zwar gibt es Weiterentwicklungen wie das „Authenticated Mail Transfer Protocol“ [18] (s.u.), allerdings ist

dies bislang kein offizieller Standard, ganz davon abgesehen, dass man solche Protokolle nicht einfach austauschen kann.

Extended SMTP. Bei Extended SMTP (ESMTP) handelt es sich um eine Erweiterung des SMTP Standards, die 1995 als RFC veröffentlicht wurde und mittlerweile in die die neueste SMTP Spezifikation von 2001 eingegangen ist. Dabei bietet ESMTP ansich keine neue Funktionalität, sondern stellt nur die Möglichkeit bereit, über ein modulares Konzept weitere Befehle zu definieren. Meldet sich der Client beim Mailserver nun mit `EHLO` (statt `HELO`), so teilt ihm der Server mit, welche Erweiterungen des Protokolls er unterstützt.

Die wohl wichtigsten Erweiterungen, die sich ESMTP zu nutze machen, sind *AUTH* und *STARTTLS*. Erstere dient der Zugangskontrolle zum Mailserver und verhindert so den nicht-authorisierten Spam-Versand[9], während letztere die Verbindung zwischen Client und Mailserver TLS-verschlüsselt und zudem die Möglichkeit bietet, den Mailserver auf Echtheit zu überprüfen (sofern der Mailserver ein von einer Certificate Authority ausgestelltes Zertifikat einsetzt).

```
220 mail.rapidmaurice.de ESMTP
EHLO mertinkat.net
250-mail.rapidmaurice.de
250-STARTTLS
250-PIPELINING
250-8BITMIME
250-SIZE 0
250 AUTH LOGIN PLAIN CRAM-MD5
QUIT
221 mail.rapidmaurice.de
```

Abbildung 4: EHLO Antwort eines ESMTP Mailservers.

AMTP – Authenticated Mail Transfer Protocol. Dieses von Bill Weinman erdachte Authenticated Mail Transfer Protocol basiert im Wesentlichen auf dem oben erwähnten SMTP, ermöglicht aber die Echtheitsprüfung des einliefernden Mailservers mittels X.509-Zertifikaten und führt einen sogenannten Mail Policy Code ein, mit dem ein Server Regeln für den Empfang und Versand von E-Mails festlegen kann. Die Übertragung der Daten zwischen den Mailservern findet ausschließlich TLS-verschlüsselt statt; ebenso wie dies bei der STARTTLS-Erweiterung [19] für SMTP möglich ist.

Grundsätzlich ist AMTP also ein guter Ansatz, um SMTP den Rang streitig zu machen – vor allem weil „nur“ Änderungen an der Mailserver-Infrastruktur erforderlich sind, nicht aber die Mailclients berührt werden müssen. Eine große Hürde sind allerdings die X.509-Zertifikate, die durch eine Certificate Authority ausgestellt werden müssen, um die Echtheit

[9] Mailserver, die ohne Zugangskontrolle auch E-Mails für fremde Domains annehmen und weiterleiten, nennt man Open-Relays. Diese sind besonders für Spammer attraktiv, da sie dessen Herkunft verschleiern und zudem eine (mehr oder weniger) kostenlose Versandmöglichkeit darstellen.

des Serverbetreibers zu beurkunden. Sie kosten meist zwischen US$100 und US$300 pro Jahr und sind somit für Mailserver von Privatpersonen oder gemeinnützigen Organisationen häufig nicht lohnend.

2.3.3 Teergruben

Unter einer Teergrube versteht man einen Mailserver, der versucht eine Verbindung möglichst lange aufrecht zu erhalten, um damit Resourcen des Spammers zu blockieren. Das Idee dazu stammt von Axel Zinser und wurde erstmal 1997 in einer Newsgroup diskutiert. Die Betreiber solche Teergruben veröffentlichen meistens hunderte von E-Mail-Adressen, in der Hoffnung, dass ein *address harvester* sie findet und der Spammer mit der E-Mail-Zustellung beginnt. Was vor 10 Jahren sicherlich keine schlechte Idee war (obgleich sich hierfür niemals eine breite Unterstützung fand), ist heute kaum mehr ein Hindernis für Spammer. Die Spam-Bots sind meist multithreadingfähig oder multiplexen[10] über die geöffneten Verbindungen, so dass langsame Verbindungen kaum bis gar nicht ins Gewicht fallen. Zudem wird mit aggressiven Timeouts gearbeitet, um genau solche Szenarios zu vermeiden. [20]

3 SPIT

3.1 Was ist SPIT?

Das Akronym SPIT steht für „Spam over Internet Telephony“ und bezeichnet die Störung der Internet-Telefonie (VoIP) mittels unerwünschter Werbeanrufe, ähnlich wie dies – im übertragenenen Sinne – auch beim Medium E-Mail der Fall ist.

3.1.1 Status quo

Werbeanrufe von Call-Centern, sogenannte Initiativanrufe oder Cold-Calls, sind seit langem bekannt und zumindest in Deutschland grundsätzlich verboten, weil sie „eine besonders schwerwiegende Beeinträchtigung der verfassungsrechtlich geschützten Privatsphäre des Angerufenen darstellen“, so der BGH in einer Entscheidung vom 16.03.1999 [21]. „Die Anrufe werden im allgemeinen von [...] besonders geschulten Personen vorgenommen, deren psychologisch geschickt eingesetzter Redegewandtheit sich der aus seiner gegenwärtigen Tätigkeit Gerissene meist nur unter peinlicher Verletzung der Regeln der Höflichkeit entziehen kann.“, so das Urteil weiter.

Ausnahmsweise erlaubt sind Cold-Calls nur dann, wenn der Angerufene mit dem Werbeanruf einverstanden ist. Handelt es sich um eine Privatperson, so muss diese hierzu ausdrücklich oder durch konkludentes Verhalten dem Anruf zugestimmt haben. Bei Unternehmen sind Werbeanrufe auch ohne Zustimmung erlaubt („mutmaßliche Einwilligung“,

[10] Postfix multiplexed unter Linux mit epoll:
http://archives.neohapsis.com/archives/postfix/2007-04/0062.html

nach § 7 Abs. 2 Nr. 2 UWG)[11], wenn der Anrufer davon ausgehen kann, dass der Angerufene ein konkretes Interesse an dessen Dienstleistungen haben könnte. [22]

Bei Werbeanrufen über VoIP (SPIT) handelt es sich jedoch bisher um ein eher theoretisches Problem, was nicht zuletzt damit zusammenhängt, dass VoIP-Netze noch nicht die Größe herkömmlicher Telefonnetze erreicht haben. Mit der stetig steigenden Verbreitung von VoIP verlagert sich das Call-Center-Geschäft aber zunehmens auf diese Technik, weil hierdurch große Einsparungen für die Betreiber möglich sind. Zugleich ebnet das kostengünstige VoIP aber auch den sogenannten Call-Bots, d.h. automatisierten „Call-Center-Agents“, den Weg.

3.2 Unterschiede zu Spam

Spam und SPIT sind so verschieden wie die ihnen zugrunde liegende Art der Kommunikation; gleich ist ihnen nur, dass sie den Benutzer belästigen. Während es sich bei E-Mail um ein asynchrones Medium handelt, hat man es bei der Telefonie mit einem synchronen Medium zu tun. Daraus resultiert auch, dass sich die oben vorgestellten Spam-Schutzmechanismen und -Gegenmaßnahmen nicht direkt auf SPIT übertragen lassen. Eine E-Mail liegt nach Annahme durch den Mailserver komplett vor und lässt sich zeitverzögert auf Spam überprüfen, wohingegen ein evtl. unerwünschter Anrufer noch vor der Annahme des Gesprächs überprüft werden muss – es stehen also weitaus weniger Informationen zur Überprüfung und Bewertung zur Verfügung.

3.3 Schutzmöglichkeiten

Obwohl es sich deutlich schwieriger gestaltet SPIT zu erkennen, gibt es doch einige Schutzmöglichkeiten, die einerseits vom Provider und andererseits auf Benutzerebene implementiert werden könnten. Dabei sollten die verschiedenen Möglichkeiten nicht nur als eigenständige Komponenten betrachtet, sondern vielmehr dazu genutzt werden, den Anrufer anhand eines Punktesystems zu bewerten (ähnlich wie dies der Spam-Filter *SpamAssassin* vormacht und ähnlich wie dies auch im *SPIT-AL (SPIT-Abwehr-Lösung)* Projekt[12] [23] geplant ist).

3.3.1 Weiße und schwarze Listen

Die einfachste Art der Filterung wird mittels White- und Blacklists erreicht, die sowohl erwünschte als auch unerwünschte Rufnummern enthalten. Ein Anrufer, dessen Rufnummer auf der Whitelist steht, wird in jedem Falle durchgestellt, wohingegen Anrufer, deren

[11] § 7 UWG: Unzumutbare Belästigungen
http://bundesrecht.juris.de/uwg_2004/__7.html
[12] SPIT-AL:
http://www.spit-abwehr.de

Rufnummern in der Blacklist enthalten sind, sofort abgewiesen werden. Übermittelt der Anrufer keine Rufnummer (was bei vielen Werbeanrufen der Fall ist), so ließe sich das Konzept auch auf IP-Adressen oder ganze IP-Subnetze erweitern, von denen die Anrufe stammen.

Pflegeleicht? Um White- und Blacklists sinnvoll einzusetzen, müssen diese jedoch kontinuierlich aktualisiert werden. Eine gewisse Problematik besteht zudem darin, dass erst *nach* einem Werbeanruf die jeweiligen Informationen in die Blacklist aufgenommen werden können, die Wahrscheinlichkeit aber deutlich sinkt nochmals einen Werbeanruf von diesem Anrufer zu bekommen. Um dem Problem entgegenzuwirken, könnte man entweder White- und Blacklists im Internet publizieren (ähnlich den bei E-Mail-Spam eingesetzten DNS-RBLs) oder aber auch die White- und Blacklists anderer VoIP-Teilnehmer mitbenutzen (*shared white-/blacklists*).

3.3.2 Graue Listen

Ähnlich wie im E-Mail-Bereich (dort wird der einliefernde Mailserver mit einem temporären Fehler abgewiesen) funktioniert auch das Greylisting bei VoIP: Beim ersten Anruf erhält der Anrufende ein Besetztzeichen und wird erst beim zweiten Anruf durchgestellt und zugleich für eine bestimmte Zeit auf eine Whitelist gesetzt. Es bleibt abzuwarten in wie weit sich die Call-Bots diesem Schema anpassen. Vorerst dürfte es jedoch kostengünstiger sein, gleich mit der nächsten Nummer fortzufahren.

3.3.3 Der gute Ruf

Menschen, die man nicht kennt, kann man auch nicht selbst einschätzen, geschweige denn bewerten. Man ist also auf die Bewertung dieser Menschen durch andere angewiesen. Genau hier setzen die sogenannten Reputations- oder Bewertungssysteme an, die es erlauben einen Mitmenschen zu bewerten. Praktisch alle zentral verwalteten Instant Messenger implementieren mit ihren *Buddy Lists* bereits ein solches Reputationssystem in Form eines sozialen Netzwerks. Dabei hat derjenige Benutzer die höchste Reputation, der auf den meisten Buddy Lists vertreten ist. Bei dem ansich dezentral organisierten VoIP-Netz (sieht man einmal von großen Providern ab), gestaltet sich ein derartiges Bewertungssystem allerdings schwieriger. Hier könnte man auf das Konzept von OpenPGP (*Web of Trust* für öffentliche Schlüssel) zurückgreifen und auch für VoIP-Teilnehmer ein Netzwerk gegenseitigen Vertrauens aufbauen, das im Idealfall die persönliche Whitelist ersetzt. [24]

3.3.4 Anruferfreischaltung durch Ansage

Eine weitere Möglichkeit besteht darin, den Anrufer vor Annahme des Gesprächs zunächst mit einem Sprachmenü zu verbinden, bei dem er aufgefordert wird eine Zahlenkombination

einzugeben. Nur wenn diese korrekt ist, wird er zum gewünschten Teilnehmer durchgestellt. Die gesprochene Zahlenkombination dient hier als Audio-CAPTCHA [25]. Mit dieser Methode lässt sehr wirksam automatisierter, d.h. durch Call-Bots verursachter SPIT vermeiden, da Spracherkennung auch in der nahen Zukunft eine sehr schwierige und rechenintensive Aufgabe bleiben wird. Anrufe von Call-Center-Agents lassen sich hiermit natürlich nicht verhindern, allerdings werden diese in ihrer Arbeit etwas gebremst, was dem Call-Center-Betreiber zusätzliche Kosten verursacht. Als Problem könnte sich herausstellen, dass ein (legitimer) Anrufer das Sprachmenü nicht versteht, da es nicht in seiner Sprache angeboten wird. Für den private Bereich dürfte dies aber vermutlich vernachlässigbar sein.

3.3.5 Anruferherkunft

SPIT ensteht einerseits aus der Tatsache, dass das Telefongespräch kostenlos geführt werden kann und sich andererseits eine Rückverfolgung als schwierig erweist. Kommt der Anrufer allerdings aus einem herkömmlichen Telefonnetz, das auf Vermittlungstechnik basiert (ATM, ISDN, Mobilfunk), so ist die Wahrscheinlichkeit deutlich geringer, dass es sich um einen unerwünschten Anruf handelt. Gleiches gilt für Anrufer aus VoIP Netzen, die vom VoIP-Provider dahingehend reglementiert sind, dass die Teilnehmer des Netzes mit dem VoIP-Provider einen Vertrag abgeschlossen haben. Ein Anrufer aus einem solchen Netz sollte eine positive Bewertung erhalten, wohingegen Anrufer aus unbekannten Netzen oder von Dial-In-Verbindungen negativ bewertet werden sollten. [23]

3.4 Gegenmaßnahmen

Da SPIT ein bislang praktisch nicht-existentes Problem darstellt, ist es schwierig wirksame Gegenmaßnahmen zu definieren. Im folgenden sollen trotzdem drei Gegenmaßnahmen diskutiert werden, die sicherlich nicht unwirksam, aber auch nur bedingt alltagstauglich sind.

3.4.1 Erkennung sehr aktiver VoIP-Teilnehmer

Die Filterung von SPIT muss nicht nur beim Angerufenen bzw. im Zielnetz geschehen, sondern auch die Provider der Quellnetze können zur Erkennung von SPIT im eigenen Netz beitragen. So wäre es denkbar, dass der Provider aufgrund der VoIP-Aktivität Listen „kritischer Teilnehmer“ erstellt. Schenkt man einer Meldung auf onlinekosten.de [26] glauben, so wird dieses Mittel bereits eingesetzt, auch wenn die Motivation dahinter eine andere ist und nichts mit SPIT zu tun hat. Zudem stellt sich hier die Frage nach einer rechtlichen Grundlage für die Erhebung und vor allem Speicherung dieser Daten.

3.4.2 Erkennung auffallender Anrufeigenschaften

Neben der Erkennung sehr aktiver VoIP-Teilnehmer könnte der Provider auch aufgrund anderer Anrufeigenschaften und mit Hilfe statistischer Verfahren Rückschlüsse auf die Natur eines VoIP-Teilnehmers ziehen. Bei vielen Telefonate ähnlicher bis gleicher Länge innerhalb einer bestimmte Zeitspanne ist z. B. davon auszugehen, dass es sich bei diesem Teilnehmer um einen Call-Bot handelt und nicht um eine Privatperson. Denkbar wäre auch eine Auswertung der angerufenen Teilnehmer, um daraus eventuell ein Schema abzuleiten, was auf einen Call-Bot hindeuten könnte [27]. Auch hier muss sich die Frage nach der rechtlichen Grundlage gestellt werden.

3.4.3 Teergruben

Ein andere Gegenmaßnahme, die auch aus dem Spam-Bereich kommt, ist das Einrichten von Teergruben. Dabei wird versucht einen Call-Bot oder möglicherweise auch Call-Center-Agent so lange wie möglich in ein simuliertes „Gespräch“ zu verwickeln, um Kapazitäten des Call-Bots (respektive des Call-Centers) zu binden. Eine Modellimplementation[13] könnte so aussehen, dass immer dann, wenn der Anrufer gerade nichts sagt und potentiell auf eine Antwort wartet, vorher aufgenommene Audio-Sequenzen in einer mehr oder weniger sinnvollen Reihenfolge abgespielt werden. Eine Flashanimation dieser Idee ist hier zu finden: `http://www.deviantart.com/view/22995489/`. Dabei wird gezeigt wie sich ein (naiver) Call-Center-Agent fiktiv mit einem Computer unterhält, der das Frage-Antwort-Spiel geradezu rumdreht, bis der Agent, augenscheinlich genervt, aber dennoch freundlich das Telefonat beendet – nach mehr als drei Minuten.

4 Ausblick

Ungeachtet aller Sicherheitsmaßnahmen und des langsamen Abnehmens der Open-Relay-Mailserver[14] hat sich das Spam-Aufkommen – wie in Kapitel 2 beschrieben – in den letzten Jahren mehr als verdoppelt. Es scheint also für die Spammer trotz erschwerter Voraussetzungen (und teilweise empfindlicher Geld- und Haftstrafen) immernoch rentabel zu sein, mit ihren Werbebotschaften für billiges Geld und bunte Pillen die Postfächer vieler Internetnutzer überquellen zu lassen.

Eine gewisse Mitschuld daran tragen aber auch diejenigen, die ihre Mailserver und somit ihre Nutzer nur unzureichend vor Spam schützen. Dabei wäre es schon mit einfachsten Mitteln (DNSRBLs) möglich, viele Werbenachrichten auf SMTP-Ebene zu blocken (und den Spammer dazu zu veranlassen die jeweiligen E-Mail-Adressen als ungültig zu erklären).

[13] THE TELECRAPPER 2000 TELEMARKETER INTERCEPTION SYSTEM: `http://www.pagerealm.com/tc2k/`

[14] Das mittlerweile nicht mehr existierende „Spamhaus“ listete im Dezember 2006 immernoch über 250.000 Open-Relay-Mailserver

Selbst größere Firmen setzen teilweise völlig unzureichende und schlecht abgestimmte Anti-Spam-Lösungen[15] ein, die im schlimmsten Fall mehr Arbeit und damit wirtschaftlichen Schaden verursachen, als ohne Filterung. Grundsätzlich sind moderne Spam-Filter mittlerweile in der Lage weit über 95 % des Spams auszusortieren, bei einer false-positives-Rate im Promillebereich – es gibt also doch Lösungen (noch dazu frei verfügbare), um sich effektiv vor Spam zu schützen.

Damit es bei der Internet-Telefonie nicht zu einem ähnlichen Szenario kommt wie im E-Mail-Bereich, werden schon jetzt Schutzmechanismen und Gegenmaßnahmen diskutiert – mit mehr oder weniger großem Erfolg. Ein in der Diskussion bislang vernachlässigter Punkt: Die Absicherung des VoIP hauptsächlich zugrunde liegenden Protokolls *SIP*, das für den Verbindungsaufbau zuständig ist. Hier bestehen ähnliche Probleme wie bei SMTP bzgl. der Überprüfung der Echtheit des Absenders bzw. des Anrufers.

Allerdings ist – meiner Meinung nach – mit dem Problem SPIT auch nicht in den nächsten Jahren zu rechnen. Die Call-Center-Betreiber werden zwar immer stärker auf VoIP setzen, um Kosten zu sparen, aber solange es keine vollautomatisierten Call-Bots gibt, wird sich SPIT nicht so weit verbreiten wie Spam. Der Anruf eines Call-Bot benötigt auf Seiten des Betreibers weitaus mehr Resourcen (da es sich um ein synchrones Medium handelt) als im asynchronen E-Mail-Bereich. Ist der Call-Bot noch dazu nicht erfolgreich, da er vielleicht beim Angerufenen lediglich eine 20-sekündige Nachricht abspielt und keinerlei Interaktion bietet, so entstehen dem Betreiber wesentlich höhere Kosten als beim Versand einer E-Mail, nicht zuletzt durch angefallenen Traffic.

Trotzdem ist es natürlich sinnvoll, sich bereits jetzt mit diesen Problemen auseinanderzusetzen und aus der Spam-Tragödie im E-Mail-Bereich zu lernen. Ob VoIP-Netzbetreiber und Anbieter von Endgeräten aber letztendlich die vorgestellten Schutzmechanismen und Gegenmaßnahmen auch rechtzeitig umsetzen, wird sich noch zeigen.

5 Literatur

[1] Monty Python. Spam-Sketch. http://video.google.com/videoplay?docid=5627694446211716271, zuletzt besucht am 17.06.2007.

[2] BBC News. Criminals 'may overwhelm the web'. http://news.bbc.co.uk/1/hi/business/6298641.stm, zuletzt besucht am 17.06.2007.

[3] Heise Verlag. Phishing - Der Kampf geht weiter. http://www.heise.de/newsticker/meldung/70547, zuletzt besucht am 17.06.2007.

[15] Beispiel für einen schlecht abgestimmten Filter: ein Teil des Spams wird aussortiert, muss aber aufgrund etlicher false-positives manuell überprüft werden, wohingegen der andere Teil noch immer im Posteingang verweilt. Der Anwender muss jetzt zwei Ordner nach *guten* E-Mails durchsuchen, bei den aussortieren E-Mails im Spam-Ordner steigt allerdings die Wahrscheinlichkeit einige false-positives zu übersehen, da hier oft nur oberflächlich kontrolliert wird.

[4] Symantec. Symantec Internet Security Threat Report, Volume XI, März 2007. http://eval.symantec.com/mktginfo/enterprise/white_papers/ent-whitepaper_internet_security_threat_report_xi_03_2007.en-us.pdf, zuletzt besucht am 17.06.2007.

[5] Heise Verlag. Untersuchung: Aktien-Spams beeinflussen Kursverläufe. http://www.heise.de/newsticker/meldung/71973, zuletzt besucht am 17.06.2007.

[6] David E. Sorkin. CAN-SPAM Act. http://www.spamlaws.com/federal/can-spam.shtml, zuletzt besucht am 17.06.2007.

[7] tecChannel. Spam-Herkunft: Polen schiebt sich auf Platz 2 nach den USA. http://www.tecchannel.de/news/themen/sicherheit/460036, zuletzt besucht am 17.06.2007.

[8] Heise Verlag. E-Mails: 90 Prozent sind Spam. http://www.heise.de/newsticker/meldung/89672, zuletzt besucht am 17.06.2007.

[9] Paul Graham. A Plan for Spam. http://www.paulgraham.com/spam.html, zuletzt besucht am 17.06.2007.

[10] Wikipedia. Markow-Filter. http://de.wikipedia.org/wiki/Markow-Filter, zuletzt besucht am 17.06.2007.

[11] Jeff Markey. Blacklists Compared. http://www.sdsc.edu/~jeff/spam/Blacklists_Compared.html, zuletzt besucht am 17.06.2007.

[12] Evan Harris. The Next Step in the Spam Control War: Greylisting. http://projects.puremagic.com/greylisting/whitepaper.html, zuletzt besucht am 17.06.2007.

[13] Steffen Heyde and Matthias Bartels. Am Scheideweg. *c't Magazin*, 26:220–222, 2003.

[14] Axel Kossel. Schlüsselfrage. *c't Magazin*, 23:142 ff., 2002.

[15] Marshall T. Rose and Andrew Norton. Radio-free RFC podcast: The MARID fiasco. http://podcast.resource.org/rf-rfc/index.html#item0003, zuletzt besucht am 17.06.2007.

[16] Yahoo! DomainKeys: Proving and Protecting Email Sender Identity. http://antispam.yahoo.com/domainkeys, zuletzt besucht am 17.06.2007.

[17] Allman, et al. RFC 4871: DomainKeys Identified Mail (DKIM) Signatures. http://tools.ietf.org/html/rfc4871, zuletzt besucht am 17.06.2007.

[18] Bill Weinman. AMTP - a replacement for SMTP. http://amtp.bw.org, zuletzt besucht am 17.06.2007.

[19] P. Hoffman. RFC 3207: SMTP Service Extension for Secure SMTP over Transport Layer Security. http://tools.ietf.org/html/rfc3207, zuletzt besucht am 17.06.2007.

[20] Tobias Eggendorfer. Spam-Boykott. *Linux Magazin*, 01/07:31–64, 2007.

[21] BGH. Urteil vom 16.03.1999, Az. XI ZR 76/98. http://lexetius.com/1999,799, zuletzt besucht am 17.06.2007.

[22] Kai Mielke. Bei Anruf Werbung. *c't Magazin*, 5:194, 2006.

[23] Markus Hansen, Marit Hansen, Jan Möller, Thomas Rohwer, Carten Tolkmit, and Henning Waack. Developing a Legally Compliant Reachability Management System as a Countermeasure against SPIT. This article was reviewed and accepted for the Third Annual VoIP Security Workshop, Berlin, June 2006.

[24] J. Rosenberg and C. Jennings. Internet-Draft: The Session Initiation Protocol (SIP) and Spam. http://www.ietf.org/internet-drafts/draft-ietf-sipping-spam-04.txt, zuletzt besucht am 17.06.2007.

[25] Wikipedia. CAPTCHA. http://de.wikipedia.org/wiki/Captcha, zuletzt besucht am 17.06.2007.

[26] Aleksandra Leon. VoIP: 1&1 schmeißt Power-Quassler raus. http://www.onlinekosten.de/news/artikel/21091, zuletzt besucht am 17.06.2007.

[27] Bertrand Mathieu, Yvon Gourhant, and Quentin Loudier; France Telekom R&D. SPIT Mitigation by a Network-Level Anti-Spit Entity. Vorgestellt auf dem Third Annual VoIP Security Workshop in Berlin im Juni 2006: http://www.iptel.org/voipsecurity/doc/08%20-%20Mathieu%20-%20SPIT%20Mitigation%20by%20a%20Networ-Level%20Anti-Spit%20Entity.pdf, zuletzt besucht am 17.06.2007.