Effektivität und Effizienz von Anti-Spam-Maßnahmen

Seit vielen Jahren sitzen wir nun gemeinsam im Email-Boot und es dringt kontinuierlich Spam-Wasser ein. Um unser Boot zu retten, nutzen wir dabei eine Reihe von unterschiedlich starken und teuren (Spam-)Pumpen und diskutieren unermüdlich die Frage, welche dieser Pumpen wir uns leisten wollen. Dabei sollten wir aber nicht vergessen, das Leck zu stopfen.

1 Einleitung

Im Januar 2004 ließ sich Bill Gates hinreißen, das baldige Ende der Spam-Ära anzukündigen: „*Two years from now, spam will be solved*". Dass sich diese Äußerung nicht als „self-fulfilling prophecy" bewahrheitet hat, dokumentieren sowohl zahlreiche Statistiken von Providern und Marktforschungsunternehmen als auch der tägliche Blick in unsere Email-Postfächer. Sie zeigen, dass es uns trotz einer Fülle unterschiedlichster Anti-Spam-Maßnahmen (ASM) bislang nicht gelungen ist, Email-Spam in den Begriff zu bekommen. Damit erhebt sich zum einen die prinziporientierte Fragen, wie wirksam unterschiedliche Maßnahmen überhaupt sein können, zum anderen ist zu klären, welcher Preis im Sinne der Ressourcennutzung für die Maßnahmen zu zahlen ist. Der erste Aspekt wird üblicherweise mit dem Terminus „Effektivität" bezeichnet („doing the right things"), während der zweite mit dem Begriff „Effizienz" adressiert wird („doing the things right"). Dieser Beitrag widmet sich schwerpunktmäßig diesen Fragestellungen und bemüht sich um eine maßnahmenspezifische Einordnung, wobei ausschließlich technologische ASM betrachtet werden; primär rechtliche, organisatorische oder verhaltensorientierte Maßnahmen stehen hier nicht im Fokus.

2 Effektivität und Effizienz

Die Wirksamkeit (Effektivität) von ASM ist von deren Wirtschaftlichkeit (Effizienz) abzugrenzen. Die Effektivität von derartigen Maßnahmen, die meist als binäre Klassifikationsheuristiken (Spam oder Ham (Nicht-Spam)?) auftreten, wird in der Regel mit den beiden Kennzahlen „False-positiv-Rate" und „False-negative-Rate" gemessen. Die erste gibt an, wieviel Prozent der als Spam klassifizierten Emails Ham-Emails sind, die zweite bezeichnet den Prozentsatz der Spam-Emails, die nicht als solche erkannt wurden.

Die Wirtschaftlichkeitsanalyse widmet sich der Frage, welche Ressourcen zur Erzielung bestimmter Raten notwendig sind. Diese ist notwendig, da ASM ökonomische Ressourcen wie Personal, Hardware, Software oder Kommunikationsnetze binden und damit Kosten verursachen. Anwendern von ASM steht jedoch nur ein begrenztes Kostenbudget zur Verfügung.

Aspekte der Effektivität und Effizienz lassen sich nicht isoliert betrachtet. Wenn z.B. Anti-Spam-Filter aufgrund der enormen Spam-Menge im Sinne der Ressourceneinsparung weniger intensiv analysieren, dann schwindet auch die Präzision. Daher stellt sich Organisationen, insbesondere

Providern die zentrale Frage, wie mit vertretbaren Kosten eine möglichst zuverlässige Spam/Ham-Klassifizierung erzielt werden kann.

3 Anti-Spam-Maßnahmen

Eine Übersicht über praxisrelevante ASM zeigt die Abbildung 1, die neben einer funktionalen Klassifikation der Verfahren auch zum einen danach differenziert, ob sie nur bei bestimmten oder allen Varianten der Emailzustellung zum Einsatz kommen, und zum anderen die Phase bzw. den Akteur (Versender, versendender Email Service Provider (vESP), empfangender Email Service Provider (eESP), Empfänger) unterscheidet, in der/bei dem die Verfahren zur Anwendung kommen. Nur die dargestellten ASM werden im Folgenden näher betrachtet.

Abb.1: Klassifikation technologischer Anti-Spam-Maßnahmen

3.1 IP-Block

Beim IP-basierten Blockieren von Emails wird ausschließlich die IP-Adresse des SMTP-Clients des vESP genutzt. Dieser überprüft die Zulässigkeit der Client-IP mit Hilfe von Blacklists (Listen explizit verdächtiger IPs) und/oder Whitelists (Listen explizit unverdächtiger IPs), die entweder lokal vorgehalten werden oder online abgefragt werden. Der eESP trifft damit seine Entscheidung zur Annahme oder Ablehung der Email-Zustellung, noch bevor Daten des SMTP-Envelopes (alle Daten vor dem SMTP-Kommando „DATA „wie z.B. die Versender- und Empfänger-Adresse) oder gar Header und Body der Email übertragen wurden. Aufgrund dieser „Datenminimalität“ kann der SMTP-Server bereits frühestmöglich seine Entscheidung treffen, ohne dabei viel Rechenzeit zu verwenden, die Email übertragen zu lassen und damit Bandbreite des Kommunikationskanals zu nutzen. Ferner wird auf die serverseitige Speicherung einer Email verzichtet.

Die Ressourcen-Schonung des IP-Blocks ist auf dessen einfache Vorgehensweise zurückzuführen, bei der nur die IP-Adresse des Clients als verdächtig oder unverdächtig eingestuft wird. Damit verlassen sich IP-Blocks ausschließlich auf die Qualität der genutzten Blacklists oder/und Whitelists. Deren Qualität und Verfügbarkeit determinieren damit die Wirksamkeit der IP-Blocks, die im Folgenden betrachtet werden.

Umfangreiche Blacklists wie die von Spamhaus und SORBS stehen zahlreich zur Verfügung. Bei der Auswahl zu nutzender Blacklists ist nicht nur deren jeweilige Größe zu beachten, sondern darüber hinaus auch deren (zu vermeidende) Überschneidungen. Beispielsweise nutzt es wenig, die Blacklists XBL und CBL von Spamhaus zu kombinieren, da CBL in XBL enthalten ist (Rossow et al. 2008). Die praktische Relevanz von Blacklists ist weiterhin hoch: Nach (Bleich und Dölle 2008) blocken z.B. Provider wie 1&1 und Strato ca. 75% aller täglich eingehenden Emails (100 Mio. bis 1 Mrd.) mittels Blacklisting.

Mit dem Blacklisting sind jedoch auch Probleme verbunden, die deren Wirksamkeit stark einschränken. Zum einen stellen Blocks Klassifikationsheuristiken dar, die unter „false-positives“ und „false-negatives“ leiden. False-positives, also geblockte Ham-Emails, rühren oftmals daher, dass aufgrund einzelner Spam-Fälle ganze Adressbereiche von Providern temporär blockiert werden und damit eine „Sippenhaft“ vorgenommen wird, die zu enormen Kollateralschäden führen können. Hier kann die komplementäre Verwendung von Whitelists, z.B. die von

dnswl.org, helfen, die jedoch ebenfalls mit False-positives und False-negatives verbunden sein können. Ferner besteht die Gefahr, dass ein Spammer auf eine Whitelist gelangt und er damit Blacklists umgehen kann. Dieser Blacklist-Bypass ist beispielsweise gegeben, wenn Botnetze verwendet werden, die Rechner Dritter fernsteuern (Zombie PCs) und dabei Spam-Emails über die in Whitelists geführten ESP der betroffenen Nutzer versenden.

Neben dem konzeptionell-bedingten Problem der Missklassifikation besteht derzeit auch nur eine eingeschränkte Anwendbarkeit von Black- und Whitelists, da die relevantesten zusammen nur ungefähr 20% aller ca. 2 Mrd. nutzbaren IPv4-Adressen abdecken (Rossow et al.), damit verbleiben Spammern also 80% des nutzbaren IPv4-Adressraums, der unklassifiziert ist.

In den letzten Jahren wurde mit dem Greylisting, das für viele Mailsystem wie z.B. Postfix und Sendmail verfügbar ist, ein weiteres Verfahren eingesetzt, das auf die Speicherung und die Analyse von Header- und Bodydaten einer Email verzichtet, jedoch Daten des SMTP-Envelopes benötigt und temporär speichert. Die grundlegende Idee, dass sich reguläre Email-Server von spammenden Email-Servern dadurch unterscheiden, dass letztere nach der ersten Ablehnung der Zustellung keinen erneuten Versuch unternehmen, mag anfangs praktisch nutzbar gewesen sein, greift jedoch auf ein nur temporär existierendes Charakteristikum zurück. Spammer werden sich hierauf zunehmend einstellen, des Weiteren besteht auch hier die Möglichkeit der Kompromittierung regulärer Email-Server über Botnetze. Neben den sich dadurch ergebenden False-negatives besteht ferner die Gefahr von False-positives, wenn reguläre Email-Server die Zustellung erst dann wiederholen, wenn der entsprechende Zustellversuch seitens des empfangenden Email-Servers aus der Tabelle, die diese Zustellversuche speichert, entfernt wurde. Schließlich kann es auch zu enormen Verspätungen bei der Zustellung von Emails kommen.

3.2 Filter

Mechanismen, die den Header und den Body einer Email in die Klassifikationsentscheidung einbeziehen, werden als Filter oder in expliziter Abgrenzung zu IP-Blocks auch als inhaltsbasierte Filter bezeichnet. Im Gegensatz zu IP-Blocks ist die Email vollständig zu übertragen und zu speichern, bevor sie analysiert wird. Die Analyse von Emails wird heute mit Algorithmen vorgenommen, die sich hinsichtlich der verwendeten Methode (z.B. Künstliche Neuronale Netze, statistische Verfahren), des untersuchten Email-Inhalts (Header, Body oder beides) und der Zusammenarbeit mit anderen (kollaborativen) Filtern unterscheiden können. Im Unterschied zu IP-Blocks können Filter nicht nur auf dem Email-Server des eESP zum Einsatz kommen, sondern auch komplementär in den lokalen Email-Clients der Empfänger. Obwohl Filter heute vielfach eingesetzt werden und bei der Klassifikation von Emails sehr nützliche Dienste erbringen, benötigen sie viele Ressourcen. Neben dem benötigten Speicherplatz und der Bandbreite zur Emailübertragung gehören Filter zu den rechenlastigen Verfahren. Diese Rechenlast erfordert oftmals auch den Einsatz dedizierter Server, so dass neben Softwarekosten auch Hardwarekosten entstehen.

Neben derartigen Effizienzproblemen sind ebenfalls Effektivitätsdefizite festzustellen, da es sich – ebenso wie bei IP-Blocks – auch bei Filtern um heuristische Klassifikatoren handelt, die False-positives und False-negatives mit sich bringen. Spammer versuchen, sich auf Filter einzustellen, indem sie diese mittels Texten oder beigefügten Bildern oder Audiodokumenten in die Irre zu führen versuchen. Gelingt dies in Testläufen, so können in einem begrenzten Zeitraum – bis die Filter sich entsprechend adaptiert haben – die Filter umgangen werden. Dieser Zeitraum kann

oftmals ausreichen, um viele Spam-Emails zu versenden. Haben die Filter sich adaptiert, ist das Kind oftmals schon in den Brunnen gefallen.

Im Unterschied zu IP-Blocks ist für die Klassifikationsqualität von Filtern deren Zuschnitt auf die Empfängerorganisation oder gar den Empfänger notwendig. Ein Krankenhaus oder ein Arzt mag Emails mit Medikamentennamen akzeptieren wollen, ein Finanzdienstleistungsunternehmen hingegen eher nicht. Daher kommen neben organisationsspezifischen Filtern auf Providerseite oft auch persönliche Filter auf der Clientseite zum Einsatz.

Es erhebt sich bei Filtern über die genannten Effektivitätsprobleme auch die Frage, ob der Einsatz von Filtern Spammer dazu bewegt, sogar mehr Emails zu versenden, um die gefilterten Nachrichten zu kompensieren. In diesem Fall hätten Filter gar eine kontraproduktive Facette.

Filter gehören zu den ASM, die sich im Strudel eines Wettrüstens bewegen, wobei die Filter-Anwender stets einen Schritt zurück sind und letztendlich im Wesentlichen reaktiv sind.

3.3 TCP-Block

Im Gegensatz zum IP-Block setzt der TCP-Block auf der Versenderseite an, indem der für die Emailzustellung verwendete TCP-Port 25 von Internet Service Providern (ISP) geblockt wird. Dies hindert Spammer daran, einen eigenen SMTP-Server aufzusetzen und Emails unter Umgehung von Providern direkt zum Email-Server des eESP zu senden. Diese Maßnahme trifft aber gleichermaßen auch die Email-Server von nicht spammenden Kunden, zu denen auch Unternehmen gehören. Um diese nicht von der Verwendung eigener Emailserver auszuschließen, wurden authentifizierende Maßnahmen eingesetzt wie z.B. „Message submission“, das üblicherweise den Port 587 nutzt, oder SMTP-AUTH. Auch diese Maßnahmen finden ihre Grenzen, wenn Spam webbasiert versendet wird oder die Rechner Dritter samt Authentifizierungsdaten im Rahmen von Botnetzen kompromittiert werden.

3.4 Authentifizierung

Zur Authentifizierung des Email-Versenders oder des vESP wurden bislang zahlreiche Varianten vorgeschlagen. Diese lassen sich danach klassifizieren, ob es sich um SMTP-Erweiterungen, Pfadauthentifizierungen oder kryptographische Authentifizierungen handelt.

Protokollerweiterungen von SMTP wie „SMTP-AUTH“, „SMTP after POP" und „SMTP after IMAP" dienen der Authentifizierung von Benutzern, die einen SMTP-Client (z.B. Mozilla Mail) verwenden. Neben der Einschränkung auf SMTP-basierten Emailverkehr hat das Verfahren den Nachteil, auf dem Schutz der SMTP-Authentifizierungsdaten vor unautorisiertem Zugriff zu basieren. Dieser ist bei infizierten PCs hingegen kaum gegeben.

Der Grundgedanke von Pfadauthentifizierungen besteht darin, dass sich in einer Kette von an der Kommunikation beteiligten Knoten jeder Knoten gegenüber dem Nachfolger authentifizieren muss. Dadurch entsteht eine Vertrauenskette bzw. ein Vertrauenspfad. Eine (im Wesentlichen DNS-basierte) Familie von Methoden zur Pfadauthentifizierung bei der Email-Versendung ist das (generische) Lightweight Message Authentication Protocol (LMAP) (deKok 2004). LMAP-Verfahren wie z.B. Sender Policy Framework (SPF) kommen auf der Serverseite einer SMTP-Verbindung zum Einsatz und überprüfen, ob beispielsweise eine Nachricht mit dem Absender buffy@sunnydale.com von einem SMTP-Knoten (Mail Transfer Agent (MTA)) zugestellt wird, der zur Zustellung von Emails der Subdomäne sunnydale.com legitimiert ist. Die zur Email-Zustellung zugelassenen IP-Adressen werden mittels entsprechender Einträge im DNS vermerkt

(analog zu MX-Einträgen). LMAP-basierte Verfahren benötigen zur Überprüfung der Autorisierung des SMTP-Clients nur den SMTP-Envelope und arbeiten daher ähnlich ressourcenschonend wie das Greylisting. Sie greifen beispielsweise dann, wenn ein Bot versucht, von einem infizierten Rechner aus eine direkte TCP-Verbindung zum Email-Server des eESP aufzubauen, da der infizierte Rechner in der Regel nicht zur direkten Versendung von Emails legitimiert ist. LMAP-basierte Verfahren verhindern Spamming jedoch dann nicht, wenn Spammer sich beispielsweise SPF-markierte Domains zulegen oder Bots den vESP eines Benutzers verwenden, dessen Email-Kontodaten auf dem infizierten Rechner kompromittiert wurden. Neben dem dadurch bedingten Auftreten von False-negatives kommt es auch zu False-positives im Kontext der Email-Weiterleitung. In diesem Fall passen der Rechner der weiterleitenden Domäne und die Domäne der Versenderadresse nicht mehr zusammen (im LMAP-Kontext).

Als dritte Möglichkeit zur Authentifikation stehen kryptographische Systeme zur Verfügung, die es dem Empfänger oder dem eESP gestatten, den Versender oder den vESP zu authentifizieren. Die Public-Key-Kryptographie stellt die mathematischen und algorithmischen Grundlagen der digitalen Signatur zur Verfügung. Die digitale Signatur einer Email kann zum einen personenbezogen sein, zum anderen sich auf eine Organisation bzw. einen Provider beziehen. In beiden Fällen ist eine Public-Key-Infrastruktur (PKI) notwendig, die u.a. die öffentlichen Schlüssel der Teilnehmer speichert. Die erste Form setzt voraus, dass die Email-Teilnehmer über ein persönliches Schlüsselpaar verfügen, die geheimen Schlüssel vor unautorisiertem Zugriff geschützt sind und eine weltweit kooperierende PKI existiert. Keine dieser Prämissen ist derzeit erfüllt. Daher beziehen Verfahren wie DomainKeys Identified Mail (DKIM) die digitale Signatur ausschließlich auf Organisationen bzw. Provider, die die o.g. Bedingungen mit deutlich geringerem Aufwand erfüllen können. Die öffentlichen Schlüssel sollen im DNS gespeichert werden, wobei sich hier sofort die Frage erhebt, inwiefern deren Authentizität gewährleistet ist. Digitale Zertifikate stellen hier eine funktionale Möglichkeit dar, sind aber mit weiterem Administrationsaufwand verbunden. DKIM und verwandte Verfahren sind jedoch in einigen Fällen unwirksam, die sich Spammer zu Nutze machen (werden): Zum einen können Spammer eigene DKIM-Domänen verwenden, zum anderen können Spammer mittels Bots Email-Konten kompromittieren. In beiden Fällen werden Spam-Emails dann mit einer gültigen digitalen Signatur versehen, so dass empfangende Server diese False-Negatives annehmen.

Wenn sich Signaturen wie im Fall von DKIM auf den Header und den Body einer Nachricht beziehen, dann muss der annehmende SMTP-Server wie bei der Filterung die vollständige Email übertragen lassen, speichern und verarbeiten. Damit benötigen derartige Verfahren umfangreiche Ressourcen.

Sowohl für LMAP- als auch für kryptographische Verfahren gilt, dass diese solange nicht als alleiniges Kriterium zur Klassifikation einer Email herangezogen werden können, solange sich die jeweiligen Verfahren noch nicht als praktischer Standard etabliert haben. Systeme wie SpamAssassin, die mehrere ASM miteinander kombinieren, sollten in der Zwischenzeit eingesetzt werden.

3.5 Verifizierung

Verfahren zur Verifizierung des Absenders (z.B. SAVE, Bless et al. 2005) sehen vor, dass vor der endgültigen Annahme einer Email der Versender ein „Challenge-Response-Verfahren“ zu absolvieren hat. Dies kann darin bestehen, dass der Mailserver des eESP dem Email-Client des vESP ein mathematisches Problem vorlegt, dessen Lösung Rechenzeit benötigt oder aber eine Aufgabe vorlegt, die von einem Menschen zu lösen ist (z.B. CAPTCHA-Verfahren). Derartige

Systeme haben kaum Praxisrelevanz, da sie mit vielen relevanten Nachteilen verbunden sind: (1) Das SMTP-Protokoll ist stark zu modifizieren bzw. zu erweitern. (2) Der emailbedingte Verkehr steigt enorm. (3) Es werden im Falle von Bots die Ressourcen des infizierten Rechners und nicht die des Spammers in Anspruch genommen, so dass diese Verfahren sich dann als kontraproduktiv erweisen.

3.6 Bezahlmechanismen

Spam-Emails lassen sich aufgrund sehr niedriger Grenzkosten pro Email mit geringen finanziellen Ressourcen massenhaft versenden. Zur Erhöhung der Grenzkosten sind Bezahlmechanismen vorgeschlagen worden, die vor der Versendung einer Email die Ressource „CPU“ (z.B. hashcash.org), „Speicher“ (z.B. Abadi et. al 2003) oder „Geld“ (z.B. Fahlmann 2002) des Versenders in Anspruch nehmen. Der gemeinsame Nachteil aller derartigen Verfahren besteht ähnlich wie bei Verfahren zur Verifizierung darin, dass bei deren Verwendung die Ressourcen Dritter ver(sch)wendet werden. Darüber hinaus ist das SMTP-Protokoll stark zu modifizieren. Die unterschiedlichen Verfahren finden sich bei (Schryen 2007) ausführlich beschrieben und diskutiert.

3.7 Begrenzung ausgehender Emails

Viele ESP sind dazu übergegangen, die Anzahl der pro Zeiteinheit und Email-Konto zu versendenden Emails zu beschränken. Diese Verfahren lassen sich leicht implementieren, dürften aber aufgrund folgender Phänomene letztendlich nur begrenzt effektiv sein: (1) Die Maßnahme ist bei den vESP einzusetzen. Ob sich ESP in Spam-freundlichen Ländern daran halten, ist sehr fraglich. (2) Neben der o.g. Email-Anzahl ist auch die Menge der Konten relevant, über die ein Spammer verfügt. Steht ihm eine Vielzahl infizierter PCs zur Verfügung oder lassen sich bei einem ESP (z.B. bei automatischer Lösung von CAPTCHA-Verfahren) automatisiert Email-Konten einrichten, so wird das Spamming nicht nachhaltig begrenzt.

3.8 Reputation

Neben den IP-Blocks gibt es eine Reihe weiterer Verfahren, die auf der Reputation des vESP basieren (z.B. sTLD, ICANN 2004). Diese sind oftmals mit einer starken Modifikation der bestehenden Email-Infrastrukur verbunden. Ein weiterer wesentlicher Nachteil dieser Verfahren tritt auf, wenn Bots verwendet werden, die ESP mit hoher Reputation (aus)nutzen und nach der Spam-bedingten Reduktion der Reputation alle Nutzer dieses ESP in „Sippenhaft“ nehmen. Die Granularität derartiger Ansätze ist folglich providerspezifisch und damit recht grob.

3.9 Modelltheoretische Betrachtung

Die bislang in diesem Artikel vorgenommene Analyse der ASM ist ausschließlich informell. Ein formales Modell der Internet-Email-Infrastruktur, das die formale Analyse routenspezifischer Maßnahmen erlaubt, findet sich bei (Schryen 2007).

4 Fazit

Die Analyse der vorgestellten ASM zeigt ein insgesamt ernüchterndes Bild, das mit dem Blick in unsere Email-Postfächer konsistent ist. Spammer gelingt es weiterhin trotz teilweise ressourcenintensiver Abwehrmechanismen nicht nur, die Heuristiken zu umgehen (False-negatives), sondern auch legitime Emails (Ham) als Spam behandeln zu lassen (False-positives).

Als eine der größten Herausforderungen stellt sich dabei die Nutzung von Botnetzen dar, mit der auch andere Sicherheitsprobleme wie die Verbreitung von Viren und Trojanern verbunden sind. Darüber hinaus ist die Absenderauthentizität, die eine Identifizierung und rechtliche Verfolgung von Spammern ermöglichen würde, bislang in Ermangelung einer weltweit verfügbaren PKI nicht möglich. Es fällt auf, dass sich der praktische Einsatz von ASM der Hochrüstung hingegeben hat und sich im wesentlichen auf reaktive Maßnahmen konzentriert, die erst nach der Nutzung vieler Ressourcen zum Einsatz kommen. Präventive Maßnahmen hingegen fristen weiterhin ein Schattendasein. Dies mag zum einen an dem Umstand liegen, dass sich über vermiedenen Spam keine spektakulären Statistiken führen lassen, zum anderen auch daran, dass größere Eingriffe in das SMTP-Protokoll und die Email-Infrastruktur notwendig sind, bei deren Entwicklung die Sicherheit kein primäres Ziel war. Der Diskurs über die Spam-Plage und die zu verwendenden Verfahren erinnert derzeit oftmals an das Sprichwort „Wasch mich, aber mach mich nicht nass."

Quellen:

M. Abadi, M. Burrows, M. Manasse, und T. Wobber: Moderately Hard, Memory-Bound Functions, Proceedings of the 10th Annual Network and Distributed System Security Symposium, S. 25-39, 2003

H. Bleich, M. Dölle: Spam-Golem – Warum der Mail-Versand zum Glücksspiel zu verkommen droht, c't 8/2008, S. 118-123, 2008

R. Bless, M. Conrad und H.-J.:Spam Protection by using Sender Address Verification Extension (SAVE), http://doc.tm.uka.de/2005/SAVE.pdf, 2005

A. DeKok: Lightweight MTA Authentication Protocol (LMAP), Discussion and Applicability Statement, Internet draft, IETF Network Working Group, 2004

S. Fahlmann: Selling interrupt rights: A way to control unwanted e-mail and telephone calls, IBM Systems Journal 41(4), S. 759-766, 2002

ICANN: new sTLD RFP Application .mail, Part B. Application Form, Technischer Bericht, 2004

C. Rossow, C. Dietrich, N. Pohlmann: IP-Blacklists sinnvoll kombinieren – Blockwerk, iX 1/2008, S. 56-61, 2008

G. Schryen (2007):Anti-Spam Measures – Analysis and Design, Springer, Berlin, Heidelberg, 2007