SPAM maschinell erkennen und behandeln

Claude Frantz

Dokument in Arbeit, Arbeitsstand vom 23. Juli 2009

Zusammenfassung

Maschinelle SPAM-Erkennung ist ein sehr komplexes Fachgebiet, das sehr oft stiefmütterlich behandelt wird. Die sehr große Menge an SPAM und Malware, die heute im Verkehr ist, führt dazu, dass diese Materie gar nicht mehr ignoriert werden kann. Hier ist eine kleine Einführung.

1 Grundlegendes

1.1 Was ist SPAM ?

Wikipedia definiert SPAM so:

> Als Spam oder Junk (englisch für *Abfall* oder *Plunder*) werden unerwünschte, in der Regel auf elektronischem Weg übertragene Nachrichten bezeichnet, die dem Empfänger unverlangt zugestellt werden und häufig werbenden Inhalt haben.

1.2 Warum heißt SPAM so ?

Aus Wikipedia erfahren wir:

> SPAM ist ursprünglich ein Markenname für Dosenfleisch[1], bereits 1936 entstanden aus *SPiced hAM*, fälschlich auch *Spiced Pork And Meat/hAM* oder *Specially Prepared Assorted Meat.*

Ferner klärt uns Wikipedia auf:

> Der Begriff Spam – als Synonym für eine unnötig häufige Verwendung und Wiederholung – entstammt dem Spam-Sketch der englischen Comedyserie Monty Python's Flying Circus: In einem Café besteht die Speisekarte ausschließlich aus Gerichten mit Spam, die Spam teilweise mehrfach hintereinander im Namen enthalten. Im Sketch wird das Wort *Spam* insgesamt 132 Mal erwähnt.

> In den Zusammenhang mit Werbung wurde das Phänomen Spam zum ersten Mal im Usenet gebracht. Dort bezeichnet man damit mehrfach wiederholte Artikel in den Newsgroups, die substanziell gleich sind oder für dieselbe Dienstleistung werben. Die erste Spam-E-Mail wurde wohl am 3. Mai 1978 versendet, allerdings erst im Jahr 1993 als solche bezeichnet.

1.3 Wo ist welches Problem ?

E-Mail ist ein Ersatz für die *gelbe Post*, so kann es nicht überraschen, dass viele Eigenschaften gleich oder sehr ähnlich sind. Empfänger können nicht nur empfänglich sein für Nachrichten, die sie erwarten, sondern es muss auch möglich sein, einem Empfänger eine Nachricht zuzusenden, die er nicht erwartet. Es gibt zahlreiche Gründe dies zu tun, ohne dass dieses Verhalten verwerflich wird. Leider kann diese Empfangsbereitschaft auch missbraucht werden. Das kennt wohl jeder, der täglich

[1] Die Firma Hormel Foods ist der Hersteller.

seinen Briefkasten leert. Überträgt man das auf E-Mail, so landet man bei der SPAM-Problematik.

1.4 Kurze geschichtliche Entwicklung

In den *guten alten Zeiten* von SPAM war die Sache noch ganz einfach. Der Absender war stets *cyber-promo.com*. Es war also eine leichte Übung, Nachrichten von diesem Absender gesondert zu behandeln. Diese Ära war jedoch nur von kurzer Dauer. Sehr bald sind Nachrichten, die wohl als SPAM einzustufen sind, mit sehr unterschiedlichen Absendern von sehr unterschiedlichen SMTP Clients versendet worden. Es war also nicht mehr trivial diese Nachrichten, auf der Seite des Empfängers, zu erkennen. In dieser Zeit konnte der Spammer noch anhand der verwendeten IP-Adresse des Clients ermittelt werden. Nachdem Spamming zunehmend als Straftatbestand eingestuft wurde, versuchten die Spammer zunehmend den wahren Ursprung der Nachrichten zu verschleiern. Nachdem es sich in einem anderen Zusammenhang gezeigt hatte, wie leicht es möglich ist Personal Computers (PC's) zu infizieren, ohne dass das den Betreibern auffällt, so gingen Spammer dazu über, solche Computer mit Zugang zum Internet zu infizieren, um sie für ihre Zwecke einzusetzen. Zunächst wurden die infizierten PC's noch einzeln zum spammen, eingesetzt. Später haben die Spammer diese PC's koordiniert eingesetzt und daraus sog. *Botnets*[2] gebildet. Immer mehr Aufwand haben die Spammers in Techniken eingebracht, um den Aufbau des Botnets und ihrer Betreiber zu verschleiern. Moderne Botnets sind recht komplex aufgebaut. Sie haben oft diverse Fähigkeiten Schäden zu verursachen, die nicht alle mit SPAM in Verbindung stehen. Sehr oft besteht eine dieser Fähigkeiten darin, andere PC's zu infizieren um sie dann in das Botnet zu integrieren. Daraus können sehr große Botnets entstehen, die über eine Million Mitglieder aufweisen können. Ihre Spamming-Fähigkeit ist dementsprechend sehr groß.

[2] Abkürzung für Robot Networks

1.5 SPAM ist subjektiv

Bereits aus der Definition von SPAM geht hervor (siehe 1.1), dass der Empfänger einer Nachricht selbst beurteilt, was in seinen Augen SPAM ist oder nicht. Welche Nachricht *unerwünscht* ist, kann nur der Empfänger beurteilen. Oft werden unterschiedliche Empfänger die gleiche Nachricht unterschiedlich beurteilen. Hier ist bereits das große Problem der SPAM-Erkennung zu sehen. Eine maschinelle Erkennung wird nur dann ihren Kundenkreis zufriedenstellen können, wenn sie die Möglichkeit bietet auf die Wünsche jedes Kundens einzugehen. Das heißt aber auch, dass jeder Kunde genau formulieren können muss, was er als SPAM ansieht und was nicht. Die maschinelle Bearbeitung von SPAM muss zunächst in der Lage sein, möglichst alle Aspekte einer Nachricht und ihres Absenders zu ermitteln. Sie muss das Ergebnis dieser Bearbeitung dem Empfänger zur Verfügung stellen, damit dieser weitere, eigene Bewertungen vornehmen kann. Aus dieser Bewertung kann die Maschine dann zusätzlich eine Bewertung nach allgemeinen und eigenen lokalen Regeln vornehmen. Diese Bewertung kann zwangsläufig nur recht allgemein vorgenommen werden, bezogen auf den Kundenkreis, den die Maschine bedient. Das heißt aber auch, dass die lokale Bewertungskriterien dem Kundenkreis angepasst sein müssen. Anhand der ermittelten Kriterien und anhand der Bewertung nach allgemeinen und lokalen Kriterien kann der Empfänger dann weitere, eigene Bewertungen vornehmen.

Zusammenfassend folgen die Vorgänge also so:

- Erkennung der Eigenschaften der Nachricht. Erkennung der Eigenschaften des SMTP Clients. Ergebnis festhalten.
- Bewertung nach allgemeinen Kriterien. Ergebnis festhalten.
- Bewertung nach Kriterien, die für den gegebenen Kundenkreis als *allgemein* anzusehen sind. Ergebnis festhalten.

- Bewertung nach den eigenen Kriterien, die vom Empfänger definiert worden sind.
- Nachricht gemäß dem Ergebnis der Bewertung behandeln (siehe 2.6).

1.5.1 Beispiele

- Werbung für Viagra, die an Frauen gerichtet ist, kann mit großer Sicherheit als SPAM anzusehen sein, weil Viagra für Frauen ungeeignet ist. Das Produkt kann höchstens für einen männlichen Partner in Frage kommen.
- Werbung für Viagra, die an die Mitglieder eines verarbeitendes Unternehmens der Elektroindustrie gerichtet ist, kann mit großer Sicherheit als SPAM anzusehen sein, weil sie ohne Zusammenhang mit dem Betrieb steht.
- Eine Nachricht, in der viele Markennamen von Medikamenten vorkommen, kann bei einer Universität mit einer pharmakologischen oder medizinischen Fakultät ganz normaler Alltag sein. Wenn eine solche Nachricht an die Mitglieder eines verarbeitendes Unternehmens der Elektroindustrie gerichtet ist, ist die Wahrscheinlichkeit recht groß, dass es sich um SPAM handelt.
- Die Tschibo-Newsletter, wenn sie an Empfänger gerichtet werden, die bei einem *Wald-und-Wiesen* Provider ihre Mailbox unterhalten, werden nicht als SPAM angesehen, wenn die Empfänger die Zusendung solcher Nachrichten abonniert haben. Hat der Empfänger die Zusendung solcher Nachrichten nicht abonniert, so wird er sie wahrscheinlich als SPAM ansehen. Werden die Tschibo-Newsletter an die Mitglieder eines verarbeitendes Unternehmens der Elektroindustrie gerichtet, so sind sie als SPAM anzusehen, weil sie ohne Zusammenhang mit dem Betrieb stehen. Ob ein Abonnement vorliegt, wird der Maschine nicht bekannt sein, die für die SPAM Behandlung zuständig ist. Jedoch kann (und sollte) der Empfänger die besondere Behandlung dieses Newsletter in seiner persönlichen Einstellungen vorsehen, falls er diese Newsletter abonniert hat.

  Unseriöse Vertriebsleute von Anbietern von kommerziellen SPAM-Abwehrlösungen gehen oft damit auf Kundenfang, dass sie eine *False Positive*-Quote präsentieren, die besonders gut erscheint. Sie unterlassen es aber, sorgfältig zu erklären, wie diese Zahl entstanden ist. Nachdem SPAM aber subjektiv ist, lässt sich so eine Zahl eigentlich gar nicht seriös ermitteln. Höchstens könnte man so eine Zahl für eine Umgebung ansetzen, in der ein sehr kundiger Empfänger sorgfältige persönliche Kriterien festgelegt hat, die er, in geeigneter Weise der Maschine zur Verfügung gestellt hat, die ihn bedient. Das ist aber eine recht idealisierte Welt.

2 Technologie der maschinellen SPAM Erkennung

Wie soeben dargestellt, besteht der erste Schritt darin, die Eigenschaften der Nachricht und des SMTP Clients zu erkennen und festzuhalten. Die Anzahl solcher erkennbaren Eigenschaften ist sehr groß. Sie kann mehrere Tausende umfassen. Je mehr solche Eigenschaften ermittelt worden sind, je genauer können sie beurteilt werden und so genauer kann erkannt werden, ob es sich um SPAM handelt. Spammer arbeiten sehr unterschiedlich, deswegen müssen zahlreiche Situationen erkannt werden. Der Zeitpunkt, an dem die Tests durchgeführt werden können sind:

- Während der SMTP Sitzung,
- Nach der Übernahme der Nachricht vom Client durch den Server.

Prinzipiell ist es möglich an nur einem dieser Zeitpunkte alle Tests durchzuführen, es ist aber sinn-

voller beide Zeitpunkte zu nutzen. Zeitaufwendige Tests sind während der SMTP nicht empfehlenswert. Ungeduldige Clients können vermuten, dass die Sitzung abgebrochen wurde, selbst dann, wenn die Vermutung nicht angebracht ist (zu kurze Timeouts sind keine Seltenheit). Für den SMTP Server ist schwer vorauszusagen, wie lange eine Überprüfung dauern kann, weil diese von zahlreichen Faktoren abhängt, wie z.B. die Auslastung der Maschine oder die Algorithmen, die eingesetzt werden müssen, abhängig von dem Inhalt der Nachricht. Wenn externe Dienste abgefragt werden müssen (was der Regelfall ist), wie z.B. DNS, LDAP oder DCC, ist die Dauer nicht vorhersagbar bis zu der eine externe Anfrage ein Ergebnis liefern wird. Die Gefahr eines *echten* Timeouts ist immer gegeben. Wenn ein solcher auftreten sollte, ist immer mit einer Verzögerung zu rechnen weil der Client, in aller Regel, den nächsten Versuch verzögern wird und zwar um so mehr, wie erfolglose Zustellversuche bereits durchgeführt wurden. Gerade wenn ein Schub von SPAM den Server erreicht, ist es günstiger die Dauer der SMTP Sitzung kurz zu halten. Wenn Tests während der SMTP Sitzung bereits erkennen lassen, dass die Nachricht abgelehnt werden wird, ist es besser es dann sofort zu tun, weil somit eine weitere Behandlung der Nachricht entfallen kann.

Die Untersuchung auf SPAM erfolgt in aller Regel zusammen mit der Untersuchung auf Malware. Auf letzteres wird hier in diesem Rahmen nicht näher eingegangen. Hier sind nur einige der Kriterien, die untersucht werden können, bzw. sollten:

- Erfüllung der Vorgaben aus RFC-1912, Punkt 2: Konsistenz und Vollständigkeit der DNS-Eintragungen ausgehend von der IP-Adresse des Clients.
- Präsenz der IP-Adresse des Clients auf diversen RBLs (dynamische Blacklists).
- Mitgliedschaft der IP-Adresse des Clients in bekannten Botnets.
- Untersuchung der Host-Angabe, in der HELO bzw. EHLO Anweisung, die vom Client abgegeben wurde.
- Vergleich des Inhalts der Nachricht mit dem Inhalt anderer Nachrichten, die zuvor bearbeitet wurden. Der Vergleich muss so durchgeführt werden, dass ähnliche Inhalte auch erkannt werden können.
- Vergleich des Urteils bezüglich anderer Nachrichten, die zuvor bearbeitet wurden, die vom gleichen Client kamen oder von einem Client mit ähnlicher Adresse und die den gleichen Absender hatten (Auto Whitelist).
- Abfrage externer, kooperativer SPAM Erkennungsdienste, aufgrund diverser Signaturen, die aus der Nachricht gebildet wurden (DCC, Vipul's Razor2, pyzor).
- Test auf bestimmte Inhalte, z.B. Vorschussbetrug gemäß § 419 (SCAM), fiktive Liebesgeschichten (Internet Love Scam), Auswanderungsbetrug, Anwerbung von Boten für betrügerische Transaktionen, Einladung zum Glücksspiel, Aufforderungen vertrauliche Informationen mitzuteilen (Phishing), Aufforderungen infizierte Inhalte zu öffnen (Klicken Sie hier !), Angebot von Raubkopien von Software, usw., usw. Die Kreativität der Betrüger ist offensichtlich grenzenlos. Die Untersuchung muss in allen Sprachen durchgeführt werden, die beim Empfänger vorkommen können.
- Test auf bestimmte Formulierungen im Text.
- Test auf korrekten Empfänger in der "To:"-Zeile und während der SMTP-Sitzung.
- Test auf Glaubwürdigkeit der Adresse des Absenders.
- Test des Aufbaus der Nachricht: Bilder, Sprache, verwendete Kodierung der Zeichensätze,

Anhänge, verwendete Zeichensätze, Verwendung von HTML, Verhältnis der Anhänge zu einander, usw.

- Test auf Inhalt von Bildern wenn diese Texte beinhalten. Es könnte auch SPAM sein.
- Test auf Fälschungen in den Headers, z.B.: unmögliche "Received:"-Zeilen, vorgetäuschte Version der verwendeter Software, beim Absender, usw.
- Sendung von Kommandos vom Client an den SMTP-Server, bevor letzterer die Begrüßung abgegeben hat (Verletzung der Regeln des SMTP-Protokolls).
- Auswertung der Details der SMTP Sitzung (p0f).
- Test auf URLs in der Nachricht, die häufig bei SPAM angetroffen werden.

Jeder hier aufgelistete Punkt kann auch auf eine ganze Gruppe von Tests hinweisen, die jeweils auch mehrere hundert Tests beinhalten kann.

Die Tests müssen gewisse lokale Gegebenheiten berücksichtigen (siehe 1.5), wie z.B. die Sprachen, die im Hause verwendet werden, Begriffe, die in der Organisation gängig und typisch sind (z.B. Markennamen, Fachbegriffe).

2.1 Zusammenfügen der Testergebnisse

Gängige SPAM-Erkennungssoftware vergibt für jeden einzelnen bestandenen Test ein numerisches Ergebnis zurück. Das Vorzeichen zeigt an ob damit der Verdacht auf SPAM sich bestätigt oder, im Gegenteil, ob er sich reduziert. Am Ende wird summiert und die Summe wird gegenüber lokal definierten Grenzwerte verglichen. Daraus wird die SPAM-Wahrscheinlichkeit abgeleitet. Es ist wünschenswert, dass jeder Empfänger seine eigene Schwelle definieren kann, wenn er es wünscht.

Ein derart primitives Zusammenfügen der Ergebnisse lässt viele Wünsche offen. Durch ganz gezielte Bewertung der einzelnen Tests gegenüber anderen könnte ein deutlich besseres und zuverlässigeres Urteil gewonnen werden. Statt simpler Summierung müsste die Auswertung algorithmisch geschehen wie in einem Programm. Ein einfaches Beispiel lässt das Problem gut erkennen:

Um erkennen zu können, ob ein SMTP-Client zu einem Subnet gehört, aus dem heraus bisher viel SPAM versendet wurde und bei dem dies auch weiterhin zu erwarten ist, so sind zahlreiche Tests notwendig, um sich ernsthaft ein Bild machen zu können. Würde man die Ergebnisse einfach summieren, so würde daraus, wegen der vielen Tests, ein starker SPAM-Verdach entstehen. Wenige Tests wären aber auch nicht sinnvoll, weil die Erkennungssicherheit stark darunter leiden würde. Handelt es sich aber, bei dem Client in einen solchen Subnet, um einen, der leichtsinnigerweise seine Nachrichten direkt an den MX-Host des Empfänger zu senden versucht, obwohl er eigentlich gar kein Spammer ist, so läuft er Gefahr als Spammer eingestuft zu werden. Sicher werden zahlreiche andere Tests den SPAM-Verdacht herabsetzen, es wird ihnen aber schwer fallen, gegen die hohe Summe, die aus den Tests bezüglich des Subnets entstanden ist, anzukommen.

Dieses kleine Beispiel lässt das Problem der einfachen Summierung gut erkennen. Viel besser wäre es hier gewesen, wenn die Ergebnisse der Tests bezüglich des Subnets als solches deutlich gekennzeichnet gewesen wären und wenn daraus ein Wert abgeleitet worden wäre, der angibt, wie hoch die Wahrscheinlichkeit ist, dass der Client zu einem Subnet gehört, aus dem heraus bisher viel SPAM versendet wurde und bei dem dies auch weiterhin zu erwarten ist. Auch das Ergebnis der anderen Tests müsste jeweils zu einem Wert zusammengefasst werden, der angibt, wie hoch die Wahrscheinlichkeit ist, dass bestimmte Dinge zutreffen, die für die SPAM-Bewertung von Bedeutung sind. Soweit dann die Wahrscheinlichkeit dieser Dinge ermittelt worden wäre, müssten diese Ergebnisse dann so zusammengefasst werden, dass dann, als Endergebnis, die SPAM-Wahrscheinlich der vorliegen-

den Nachricht ermittelt werden könnte. Genauer gesagt, müssten diese Wahrscheinlichkeiten in einer Hierarchie (Baum-Struktur) ermittelt werden, so dass am Ende dieser Hierarchie (Wurzel des Baumes) die SPAM-Wahrscheinlichkeit der vorliegenden Nachricht steht. Die Zusammenfassung mehrerer Wahrscheinlichkeiten zu einer *Gruppenwahrscheinlichkeit* müsste algorithmisch erfolgen, unter genauer Berücksichtigung des Inhalts der durchgeführten Tests.

2.2 Absenderrückversicherung

Im Laufe der Zeit wurden verschiedene Verfahren eingeführt, mit denen ein SMTP-Server überprüfen kann, ob der Client überhaupt ermächtigt ist, Nachrichten mit dem gegebenen Absender zu versenden.

Das erste und einfache SPF-Verfahren (Sender Policy Framework) sieht vor, dass die notwendige Information, die notwendig ist um die Überprüfung durchzuführen, im DNS gespeichert wird. Trotz der Einfachheit des Verfahrens ist es technisch sehr wirksam. Es ist aber davon abhängig, dass die nötige Information im DNS hinterlegt wird. Liegt keine vor, besteht Zweifel und Unsicherheit.

Das zweite und viel aufwendigere Verfahren wurde in Zusammenarbeit von mehreren Unternehmen entwickelt und von Microsoft eingeführt. Es heißt DKIM (DomainKeys Identified Mail). Es setzt einen sehr viel größeren Aufwand beim Absender voraus.

Beide Verfahren leiden unter dem gleichen Problem, das diese Verfahren letztendlich kaum brauchbar macht. Würden alle Organisationen, die hinter den Absendern stecken, zuverlässig nur den Systemen das Vertrauen schenken, die das wirklich verdienen, so würden sich die Missbrauchsmöglichkeiten auf die Fälle beschränken, in denen Unbefugte sich einen Zugang zu diesen Systemen verschaffen konnten. Leider ist die Wirklichkeit ganz anders. U.a. gehen viele Provider sehr unkritisch damit um, so dass es für einen Spammer sehr einfach ist, das Vertrauen ausgesprochen zu bekommen, ohne einer ernsthaften Prüfung zu unterliegen. Wenn der Missbrauch auffliegt, hat der Spammer schon mehrere andere Alternativen in Betrieb.

2.3 Lokale Blacklists und Whitelists

Unkundigen mag nichts näher liegen als einen Absender in eine Whitelist zu übernehmen, wenn Nachrichten von ihm einen zu großen SPAM-Verdacht aufkommen lassen. Entsprechendes gilt auch für Blacklists. Aber Unkundige überblicken die Komplexität der Materie nicht und sie übersehen dabei, welche Probleme auftreten können. Empfängerbezogene lokale Blacklists und Whitelists, die vom Empfänger selbst gepflegt werden, sind hier durchaus möglich und sinnvoll. Eine Aufklärung und Beratung der Empfänger ist jedoch sehr ratsam. Für andere Empfänger haben sie keine Wirkung, so dass eine falsche Eintragungen sich nur bei dem Empfänger auswirkt, der sie angelegt hat.

Lokale Blacklists und Whitelists mit Auswirkung auf alle Empfänger, die das System bedient, sind mit sehr großer Vorsicht zu genießen. Nur wenn sie wirklich von allgemeiner Bedeutung sind, sind sie sinnvoll. Die Praxis hat gezeigt, dass eine weiche Entscheidung, bei der nur Punkte vergeben werden, die in die Bewertung eingehen, viel besser ist als eine harte Entscheidung, bei der die bedingungslose Annahme oder Ablehnung der Nachricht dekretiert werden würde.

2.4 Greylisting (oder graylisting)

Greylisting ist ein recht einfaches SPAM-Abwehrverfahren, bei dem der SMTP-Server eine angebotene Nachricht zunächst temporär ablehnt, in der berechtigen Annahme, dass ein *sauberer* SMPT-Client es später wieder probieren wird. Dann würde der Server sie annehmen. Greylisting vertraut darauf, dass Clients aus Botnets diese Situation nicht korrekt handhaben würden und nicht wieder versuchen würden, die Nachricht

erneut zu senden.

Zu Beginn der Einführung von Greylisting zeigte das Verfahren eine große Wirksamkeit, weil die Clients tatsächlich die Fähigkeit zu einem weiteren Versuch nicht hatten. Spammer sind nicht blöd, ganz im Gegenteil. So kommen heute nahezu alle Spammer-Clients mit der temporären Ablehnung zurecht und sie versuchen es später wieder. Besonders pikant ist die Tatsache, dass die Server, die Greylisting verwenden, dies während der SMTP-Sitzung meistens noch deutlich ankündigen, so dass der Spammer-Client die Information zu seinem Vorteil nutzen kann.

Die Wirksamkeit von Greylisting ist heute gegen Null gesunken. Nur noch sehr alte, vor langem infizierte Spammer-Clients (PC's) können damit abgewehrt werden. Die Mehrheit der Botnet-PC's sind mit einer relativ modernen Software ausgestattet, die viele Schadmöglichkeiten aufweist und über viele Funktionen verfügt. Diese Malware wird meistens sehr viel öfters aktualisiert (durch die Spammer gesteuert) als das Betriebsystem.

Dagegen wirken sich die Nachteile von Greylisting weiterhin voll aus. Sie bestehen in einer Verzögerung des SMTP-Verkehrs in einer Weise, die nicht kontrollierbar ist. Ein *sauberer* SMPT-Client wird es nach einer Ablehnung wieder probieren. Der Zeitpunkt ist jedoch kaum vorhersehbar, denn er ist von vielen Dingen abhängig auf der Seite des Clients. Es kann dann vorkommen, dass der Server mit Greylisting davon ausgeht, dass es ein Erstversuch ist, weil der Client nach der Einschätzung des Servers zu lange gewartet hat. Der Client andererseits wird aus den Ablehnungen auch Schlüsse ziehen, nämlich die, dass der Server schlecht erreichbar ist. Das kann und wird häufig dazu führen, dass der Client oft Nachrichten an gut erreichbare Ziele vorziehen wird und nur viel seltener versuchen wird, schlecht erreichbare Ziele zu versorgen wie z.B. Server mit Greylisting. In seinem Artikel "The Next Step in the Spam Control War: Greylisting", hatte der Greylisting-Verfechter Evan Harris, im Jahr 2003, bereits auf diese Probleme hingewiesen. Offensichtlich hatte man ihnen nur wenig Beachtung geschenkt oder man hat sie wenig ernst genommen.

2.5 Reputation Datenbanken

Gerade kommerzielle SPAM-Abwehrlösungen bauen oft sehr stark auf *Reputation Datenbanken* auf, deren Inhalt der Postmaster nicht beeinflussen kann und von denen er nicht wirklich weiß, wie der Inhalt zustande gekommen ist. Auch das Gewicht der Bewertung dieser Reputation Datenbanken ist oft nicht oder nur wenig zu beeinflussen.

Prinzipiell ist es recht vernünftig sich ein Bild darüber zu machen, wie andere eine vorliegende Nachricht oder eine Client-Adresse beurteilen. Die Bewertung solcher Dinge sollte aber stets recht kritisch vorgenommen werden. Das trifft unverändert genauso auf RBLs wie kooperative SPAM-Beurteilungssysteme zu. Wie bereits erwähnt, ist eine gute SPAM-Bewertung nur dann möglich, wenn ein umfassendes Bild vorliegt.

Soweit Anbieter einen Einblick in ihre Reputation Datenbanken erlauben, fallen dem erfahrenen Postmaster gewisse Dinge auf. So z.B., dass die Hosts gewisser Provider als erstaunlich *sauber* angesehen werden, obwohl die Erfahrung des Postmasters zu einer ganz anderen Einschätzung führt. Auch gewisse kommerzielle *E-Mail-Versender* sehen da sehr sauber aus, obwohl der erfahrene Postmaster, aufgrund seiner Erfahrung, diese bedingungslos als *SPAM-Schleuder* einstufen würde. Über den Grund dieser *Merkwürdigkeiten* lässt es sich spekulieren. Kann man eine *gute* Reputation kaufen ? Haben die Pfleger dieser Reputation Datenbanken ganz andere Clients und Nachrichten gesehen und andere nicht ?

Ganz gefährlich wäre es, den *allgemeinen* Bekanntheitsgrad eines Unternehmens oder einer Organisation in der SPAM-Bewertung zu berücksichtigen. Es gibt viel zu viele Beispiele, wo sehr bekannte Unternehmen eine katastrophale E-Mail-Infrastuktur betreiben und wo, ganz in Gegenteil, völlig unbekannte Unternehmen oder Organisationen musterhafte Infrastrukturen betreiben.

2.6 Differenzierte Behandlung von Nachrichten, abhängig von dem SPAM-Verdacht

Der primäre Zweck der SPAM-Analyse ist es, untersuchte Nachrichten anders zu behandeln wenn sie SPAM verdächtig sind. Die einfachste Form einer solchen Behandlung ist es, SPAM-verdächtige Nachrichten mit einem besonderen Kennzeichen zu versehen. Sehr sinnvoll kann auch sein, solche Nachrichten in einen besonderen E-Mail Ordner abzulegen, zu dem der Empfänger, mittels IMAP, Zugang hat. Der Empfänger hat dann noch die Möglichkeit zu prüfen, ob nicht doch Nachrichten als SPAM gekennzeichnet wurden, die er nicht als SPAM ansieht. Darauf hin kann und sollte er seine persönlichen Regeln anpassen oder anlegen. Mehrere Möglichkeiten sind denkbar, wie solche SPAM-verdächtige Nachrichten behandelt werden könnten. Nicht alle sind jedoch sinnvoll. So wäre es sicher wenig sinnvoll, den Absender zu benachrichtigen, dass seine Nachricht als SPAM angesehen wurde, wenn die Einstufung kaum einen Zweifel offen lässt.

Komplexer wird die Sache, wenn der Empfänger eine Weiterleitung der Nachrichten wünscht. Diesem Wunsch kann entsprochen werden wenn die Nachricht nicht SPAM-verdächtig ist. Diesem Wunsch kann auch noch entsprochen werden wenn eine SPAM-verdächtige Nachricht an einen Empfänger gehen soll, der ebenfalls von dem gleichen Server bedient wird. Dem Wunsch sollte besser nicht entsprochen werden wenn eine SPAM-verdächtige Nachricht an einen anderen Empfänger gehen soll, der von dem Server nicht bedient wird. Der Vorgang wäre dann als Versendung von SPAM anzusehen und das würden sich fremde Systeme durchaus merken. Würde das zu oft passieren, kann der lokale Server als SPAM-Schleuder eingestuft werden. Er kann sich dann auf RBLs finden, was mit erheblichen Nachteilen verbunden ist.

Ein weiterer komplexer Fall liegt vor, wenn der Server die Nachricht an einen anderen Server weitergegeben hat und wenn dieser die Annahme dadurch verweigert, dass er eine eigenerzeugte Ablehnungsnachricht versendet, nachdem er zunächst die SPAM verdächtige Nachricht angenommen hat. Prinzipiell wäre es sehr viel sinnvoller wenn der zweite Server selbst den angebrachten SPAM-Status beachten würde und ggf. auf die Versendung einer solchen Ablehnungsnachricht verzichten würde. In komplexen Umgebungen sind die Postmaster der Server in der zweiten Linie oft von der Aufgabe überfordert. Der erste Server kann dann versuchen, eine solche Situation zu erkennen und die Versendung der Ablehnungsnachricht verweigern.

2.7 Backscattering

Diese Spammer-Technik besteht darin eine SPAM-Nachricht an einen nicht existierenden Empfänger bei einer existierenden Domain zu versenden, wobei die *Return-Path:*-Zeile auf den Empfänger zeigt, den der Spammer eigentlich erreichen will. Der Spammer hofft, dass die Nachricht von einem der Server abgelehnt werden wird, die die Domain bedienen, und dass dann die Ablehnung an die Adresse gesendet wird, die in der *Return-Path:*-Zeile steht.

SPAM-Backscattering kann dadurch unterbunden werden, dass die Benachrichtigung an *Return-Path:* unterbunden wird, wenn die Nachricht als SPAM erkannt worden ist oder wenn sie Malware beinhaltet.

3 Zukunftsaussichten

Obwohl gegenwärtige SPAM-Abwehrsysteme oft bereits sehr gute Dienste leisten, so sind sie doch sehr verbesserungsfähig. Einige Möglichkeiten wurde hier bereits erwähnt. Die Notwendigkeit der Weiterentwicklung ist hier ganz besonders dringend, weil Spammer sehr dynamisch sind und sehr erfolgreich ihre Entwicklungen vorantreiben. Provider nehmen oft nur recht zögerlich die Ernsthaftigkeit der SPAM-Problematik wahr. Vieles ist

bei vielen von ihnen recht verbesserungsfähig. Das mag auch daran liegen, dass in der Bundesrepublik Deutschland die Bekämpfung der Straftaten, die mit SPAM und Malware in Verbindung stehen, praktisch nicht existiert, obwohl gleich mehrere Straftaten vorliegen.

In technischer Hinsicht ist auch einiges zu verbessern, obwohl bereits eine gute Grundlage vorhanden ist. Bei der Inhaltserkennung sind bessere Verfahren notwendig als Ergänzung zu dem klassischen Bayes'che Verfahren. Der CRM114-Discriminator bietet zwar einen guten Ansatz, seine Stabilität ist jedoch gegenwärtig völlig unzureichend. Es ist auch angebracht die Quellen von SPAM, ausgehend von dem Inhalt, besser zuzuordnen. So z.B. zu den Subnets, in denen sich die Clients betätigen. In diesem Rahmen zeigt sich auch, dass eine bessere Kenntnis dieser Subnets wünschenswert wäre.

Noch nahezu ungelöst ist das Problem der Anhänge im pdf-Format. Basierend auf einer Untermenge von PostScript, stellt es, so wie PostScript, eine große Menge von Möglichkeiten zur Verfügung um Texte und Graphiken darzustellen. Es ist nicht besonders schwer eine Art der Darstellung zu finden, für die es höchstwahrscheinlich keine Ausrüstung bei er SPAM-Erkennungssoftware gibt. Eine kurze Zeit lang waren SPAM-Nachrichten mit pdf-Anhang anzutreffen. Sie sind dann aber wieder verschwunden. Der genaue Grund dafür ist nicht erkennbar. Vielleicht liegt es u.U. auch daran, dass nicht jeder Empfänger eine Software hat, um pdf-Dokumente lesen zu können. Damals wurden Versuche gemacht, SPAM in pdf-Dokumenten zu erkennen, es wurde aber schnell klar welchen Aufwand dies bedeutet.

Ein wichtiges Problem besteht darin, dass die Software, die zu SPAM und Malware-Erkennung verwendet wird, aus verschiedene Quellen stammt. Schnittstellen wurden nie wirklich definiert und es ist an der Zeit, dies nachzuholen. Zwar ist die Programmiersprache PERL die meistverwendete hier. Die Schnittstellen wurden aber oft im kleinen Rahmen, ad-hoc definiert. Sie haben dann keine allgemeine Tragweite. Gerade im Fall des Versagens einer Komponente zeigen sich dann die Probleme besonders. Es ist dringend notwendig, bessere, allgemeine und sinnvolle Schnittstellen zu definieren, so dass die Weiterentwicklung der Software erleichtert wird. Es wäre dann auch leichter Komponenten auszutauschen, die von unterschiedlichen Quellen stammen.

Auch sehr wichtig ist die Speicherung von Nachrichten, ganz egal ob sie noch in Arbeit sind oder ob sie langfristig gespeichert sein sollen. Gegenwärtig werden Nachrichten völlig anders gespeichert, je nachdem ob sie in den Warteschlangen vom MTA, oder in Warteschlangen der SPAM-Erkennungssoftware, in Quarantäne oder in der Mailbox des Empfänger liegen. Das mag historisch verständlich sein, für die Verarbeitung ist das sehr hinderlich. Moderne Datenbankverwaltungssysteme haben die Fähigkeit, solche Daten in geeigneter Weise zu verwalten und zu speichern. Von diesen Fähigkeiten wurde bisher nur selten Gebrauch gemacht. Auch das Backup-Problem könnte hier gut gelöst werden, soweit das Datenbankverwaltungssystem solche Mechanismen bereits zur Verfügung stellt.

Ein Empfänger verfügt meistens über eine Software, die mittels POP3 oder IMAP Kontakt zu einem Server aufnimmt, der ihm seine Nachrichten zur Verfügung stellt. In einigen Fällen, erlaubt dieser Server dann auch die Einrichtung von Filtern bzw. Scripten (z.B. sieve). Weitere Funktionen, wie z.B. die Verwaltung von Quarantäne, sind nicht vorgesehen oder, wenn überhaupt, dann über zusätzliche Mittel, die nicht mit POP3 oder IMAP in Zusammenhang stehen. Diese Situation ist nicht länger tragbar, denn der Empfänger will verständlicherweise alles was E-Mail angeht, in einem Software-Rahmen vorfinden, der sich für ihn einheitlich darstellt, unabhängig vom Server, den er jeweils verwendet. Hier ist noch vieles zu tun. Wenn IMAP nur indirekt angesprochen wird, so z.B. über eine WWW-Applikation, so kann sich die Sache einheitlicher darstellen, ohne dass die Probleme wirklich gelöst wurden. Dafür kommen die

Probleme einer WWW-Applikation hinzu. E-Mail über WWW kann eigentlich nur als Hilfslösung angesehen werden.

4 Juristisches

SPAM Erkennung erfordert die maschinelle Analyse von Nachrichten. Letztere gehören zu der Privatsphäre des Empfängers, so wie ein normaler Brief auch. Es muss also sichergestellt werden, dass der Empfänger dem Verfahren zustimmt. Eine solche Zustimmung kann bereits in einem Arbeitsvertrag enthalten sein. In einem Unternehmen oder einer Organisation ist es auch ratsam die Personalvertretung zu Rate zu ziehen. Letztendlich muss sie dem Verfahren zustimmen. Relativ unproblematisch liegt der Fall, wenn die Analyse kaum Spuren hinterlässt, die auf den Inhalt der Nachricht schließen lassen. Erste Probleme sind bereits zu erkennen, wenn Nachrichten in Quarantäne gestellt werden und vom Postmaster analysiert werden müssen. Der Postmaster hat jedoch die gleichen Pflichten wie ein Briefträger. Quarantäne kann jedoch angebracht sein, wenn besondere Situationen auftreten, die eine weitere Beachtung erfordern. Sehr problematisch wird die Sache jedoch, wenn routinemäßig Kopien von Nachrichten abgespeichert werden.

Wie der Fall von Zango gegen Kaspersky gezeigt hat, so kann es auch vorkommen, dass sich Absender gegen eine vorgenommene Behandlung von Nachrichten wehren wollen. Auch hier zeigt sich, dass die Zustimmung des Empfängers wichtig sein kann.

Sehr problematisch kann es werden, wenn SPAM-verdächtige Nachrichten gar nicht an den Empfänger abgegeben werden.

Es ist sicher ratsam, dass sich die Postmaster einer Organisation oder eines Unternehmens den Rat von Juristen einholen, die diese ganz besondere Materie sehr gut kennen. Vor Scharlatanen wird ausdrücklich gewarnt.

Inhaltsverzeichnis