IP-Blacklisting zur Spam-Abwehr

Spam-Vermeidung ist besser als Spam-Erkennung

Christian J Dietrich, Prof. Dr. Norbert Pohlmann

Mehr als 45% aller Einrichtungen, die E-Mail einsetzen, nutzen dieses Medium für kritische Geschäftsprozesse. Über 61,5% Spam im Internet bedeuten jedoch, dass deutlich mehr als die Hälfte der zugestellten E-Mails unerwünschte Nachrichten darstellen – ohne dass sich die Nutzer dieser Flut grundsätzlich erwehren können. IP-Blacklisting setzt im Gegensatz zu vielen anderen Anti-Spam-Technologien bereits im SMTP-Dialog an und hilft damit effizient Spam zu vermeiden.

Einleitung

Der E-Mail Dienst ist einer der am weitesten verbreiteten und meist genutzten Dienste des Internets und wird heutzutage als Mittel zur einfachen, nachrichtenbasierten und zuverlässigen Kommunikation im Internet eingesetzt. Er ist für unsere vernetzte Wissens- und Informationsgesellschaft inzwischen eine nicht mehr wegzudenkende Anwendung.

Seit einigen Jahren jedoch beeinträchtigt insbesondere Spam das Medium E-Mail derart stark, dass die Frage erlaubt ist, ob E-Mail in der Zukunft noch genauso einfach, unkonventionell, produktiv und vielfältig eingesetzt werden kann.

Um letztlich das Gefahrenpotential für die E-Mail Nutzung genauer einschätzen zu können, hat das Institut für Internet-Sicherheit der Fachhochschule Gelsenkirchen eine Erhebung bei diversen Firmen, Organisationen und großen europäischen Internet Service Providern durchgeführt, die sowohl die aktuelle Bedrohungslage durch Spam und Viren als auch Maßnahmen zu deren Gefahrenabwehr analysiert (vgl. [DiPo05]). Die Untersuchung ist repräsentativ für über 40 Mio. E-Mail-Accounts und ein durchschnittliches monatliches E-Mail-Volumen von mehr als 2,3 Mrd. E-Mails.

Zurzeit wenden 27,6% aller Befragten Filtermechanismen auf IP-Schicht an. Der größte Anteil dieser Mechanismen sind Blacklists. Durch eine größere Verbreitung sowie eine effektivere Anwendung von Blacklists kann unserer Meinung nach Spam im Internet um ein Vielfaches reduziert werden.

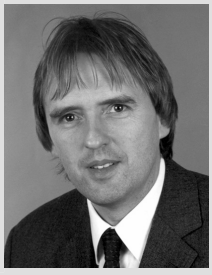
Die Ergebnisse der Untersuchung zeigen, dass neben den weit verbreiteten Spam-Erkennungsmechanismen insbesondere das Blacklist-Verfahren in seiner konkreten Anwendung in vielen Institutionen noch deutlich optimiert werden kann und dadurch bessere Ergebnisse in der Spam-Vermeidung erzielt werden können.

Einzelne Provider eliminieren durch aufwendig gepflegte Blacklists bis zu 70% Spam. Die Tatsache, dass der aktuelle

Christian J Dietrich

Forschungsschwerpunkt E-Mail-Sicherheit, Institut für Internet-Sicherheit

E-Mail: dietrich@internet-sicherheit.de



Prof. Dr.
Norbert Pohlmann

Direktor, Institut für Internet-Sicherheit

E-Mail: pohlmann@internet-sicherheit.de

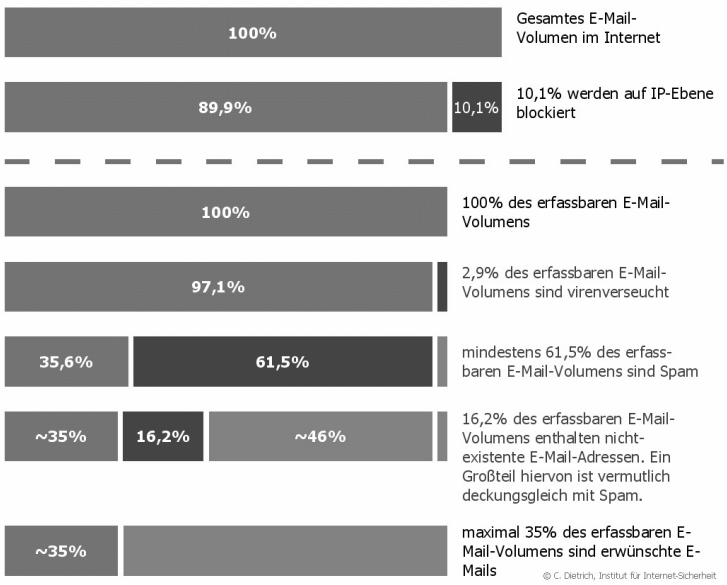


Abb. 1: Generalisierte Sichtweise, Anteilsverteilung des E-Mail-Traffics

Durchschnittswert des zu blockierenden Anteils lediglich rund 10% beträgt, zeigt, welches Potential in der Filterung auf IP-Schicht noch möglich ist.

Im Folgenden wird unter den Begriffen Sender und Empfänger der jeweilige Partner im SMTP-Dialog verstanden. Die Absender und Empfänger einer E-Mail-Nachricht werden als E-Mail-Absender bzw. E-Mail-Empfänger bezeichnet.

1 Spam-Vermeidung ist besser als Spam-Erkennung

Generell kann man die Verfahren zur Bekämpfung von Spam in erster Linie dahingehend unterscheiden, auf welchen unterschiedlichen Ebenen sie ansetzen. Während einige Verfahren – wie beispielsweise Hash- oder Signatur-Abgleich oder Wort-Analysen – darauf angewiesen sind, dass eine komplette E-Mail-Nachricht vorliegt, setzen andere Verfahren – u.a. das o.g. Blacklisting - bereits im Verbindungsaufbau zwischen SMTP-Sender und SMTP-Empfänger an.

Soll eine E-Mail zugestellt werden, so bauen zwei E-Mail-Server eine SMTP-Verbindung auf. Wenn auf Seiten des empfangenden Servers bereits anhand von Merkmalen des Verbindungsaufbaus – wie z.B. der IP-Adresse – erkannt wird, dass der Zulieferer Spam einliefern möchte, muss der empfangende Server den Verbindungsaufbau gar nicht erst vollständig durchführen, sondern kann den Aufbau unter Angabe einer Fehlermeldung abbrechen. Hierdurch wird der Empfang von Spam frühzeitig unterbunden und es werden keine CPU-, Personal-Ressourcen sowie Bandbreite und Speicherplatz verschwendet. Da die SMTP-Verbindung bei dem o.g. Verfahren sofort wieder beendet wird, ergibt sich für den Empfänger ein Kostenvorteil, da kaum Daten übertragen werden.

Ein solches Verfahren ist darüber hinaus deutlich ressourcenschonender als die üblicherweise rechenintensiven, inhaltsbasierten Scoringverfahren. Für den E-Mail-Server bedeutet die Entscheidung, ob die Verbindung erlaubt wird, meistens nur eine Anfrage an ein Verzeichnis mit (IP-)Adressen bekannter Spam-Quellen. Auf diese Art wird eruiert, ob der aktuelle Kommunikationspartner bereits als Spam-Quelle bekannt ist.

Bei der Nutzung von Blacklisting im Verbindungsaufbau fällt die Entscheidung für oder gegen die Kommunikation bei jeder einzelnen Verbindung. Über eine SMTP-Verbindung können mehrere Nachrichten zugestellt werden. Falls eine SMTP-Verbindung einer Spam-Quelle zugelassen wird, könnten innerhalb dieser Verbindung sehr viele Spam-Nachrichten eingeliefert werden. Eine abgewiesene Verbindung, die von einer bestimmten Spam-Quelle ausgeht, bedeutet also häufig die Vermeidung von deutlich mehr als einer Spam-Nachricht.

Black- und Whitelist

Unter einer Blacklist wird eine Liste negativ aufgefallener Adressen in Bezug auf die E-Mail-Nutzung verstanden. Ebenso können in einer Blacklist Adressen von Rechnern, die nicht für die direkte E-Mail-Einlieferung vorgesehen sind – wie beispielsweise dynamische IP-Adressen – aufgeführt werden. Eine Blacklist entscheidet damit nicht zwangsläufig über Zulassung oder Ablehnung einer Verbindung. Die Entscheidung, ob eine Kommunikation aufgrund eines Eintrags einer entfernten Partei in einer Blacklist abgebrochen wird, liegt weiterhin beim Empfänger und muss durch eine eigene Policy auf der Empfängerseite bestimmt werden. Der Eintrag eines Adressdatums in einer Blacklist kann – wenn ein Missbrauch des eigenen E-Mail-Dienstes durch Spam verhindert werden soll – als Indiz gegen eine Verbindung gewertet werden.

Darüber hinaus spielt die Policy des Blacklist-Betreibers eine entscheidende Rolle. Sie formuliert, wann und wie ein Adressdatum in seine Blacklist aufgenommen bzw. wieder entfernt wird. Man unterscheidet manuelle und automatische Aufnahme sowie manuelles und automatisches Entfernen aus einer Blacklist.

In vielen Fällen sind die Policies auf Empfängerseite derart definiert, dass ein Eintrag der einliefernden Partei auf einer oder mehreren Blacklists zum Abbruch der Verbindung unter Angabe einer Fehlermeldung auf SMTP-Ebene führt.

Mit Hilfe einer sog. Whitelist lässt sich demgegenüber zuverlässige, gewünschte Kommunikation von der Überprüfung auf Spam ausnehmen.

Ansatzpunkte der Vermeidung von Spam im SMTP-Dialog

Im Rahmen des SMTP-Verbindungsaufbaus erfährt der Empfänger frühzeitig bestimmte Merkmale der entfernten Partei sowie Adressdaten der E-Mail-Nachricht, bevor der eigentliche Inhalt der Nachricht übermittelt wird. Der SMTP-Dialog kann praktisch an jeder Stelle durch den Server abgebrochen werden. Es bietet sich jedoch an, die Verbindung spätestens vor Übermittlung des Inhalts (SMTP Kommando DATA) abzubrechen, um keine unnötigen Ressourcen zu verbrauchen.

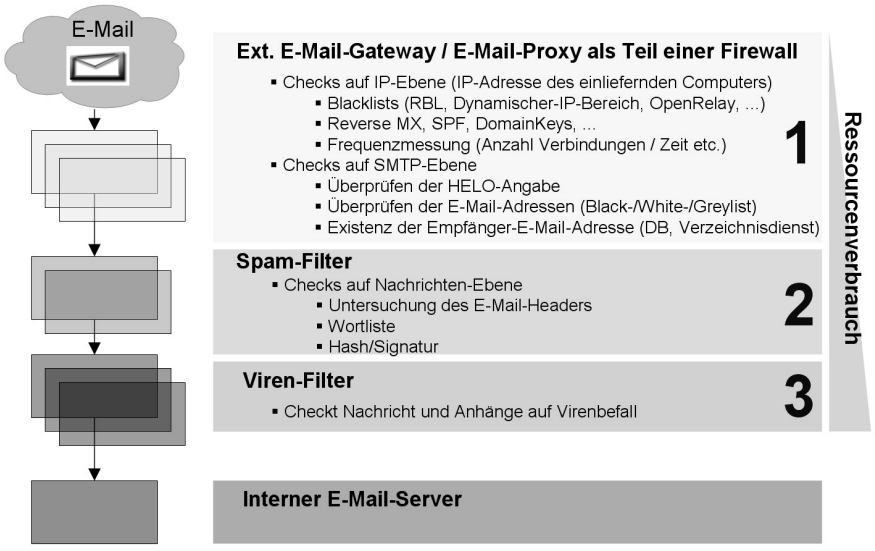


Abb. 2: Das Ebenen-Modell: Spam-Abwehr kann auf verschiedenen Ebenen ansetzen.

IP-Adresse der entfernten Partei

Um zu ermitteln, welcher E-Mail-Server für den E-Mail-Empfang einer bestimmten Domäne zuständig ist, wird der MX-Eintrag des Domain Name Systems (DNS) abgefragt. Da SMTP auf TCP/IP basiert, wird zunächst eine TCP-Verbindung hergestellt. Empfänger und Sender müssen also ihre IP-Adressen gegenseitig kennen.

Das Fälschen der IP-Adressen (IP spoofing) ist für Spammer meist mit einem hohen Aufwand verbunden und tritt daher zurzeit nahezu nicht auf.

IP-Adressen sind zumindest für die aktuelle Verbindung eindeutig einem Computer im Internet zuzuordnen. Über den Whois-Dienst kann für eine IP-Adresse die zuständige Organisation ermittelt werden. Die IP-Adresse ist damit ein verlässliches Merkmal zur Identifikation der entfernten Partei.

Darüber hinaus protokollieren Mail-Server heutzutage meistens IP-Adressen. Sie sind daher zur Ableitung des Kommunikationsverhaltens gut geeignet.

HELO-Argument

Das erste Kommando des SMTP-Clients ist das HELO/EHLO. Das HELO-/EHLO-Argument soll laut [RFC2821] der vollständige Hostname des einliefernden Clients sein. Allerdings verhalten sich über 60% der Client-Software an dieser Stelle falsch und übermitteln ein nicht standardkonformes HELO-Argument (vgl. [CLAY04]). Infolge dessen sowie aufgrund der Tatsache, dass es im SMTP-Dialog mit geringen Mitteln gefälscht werden kann, dient das HELO-/EHLO-Argument nicht als Identifikationsmerkmal. Gängige Mail-Provider messen dieser Angabe ebenfalls wenig Bedeutung bei.

Envelope-Absender-E-Mail-Adresse

Die Absender-E-Mail-Adresse kann im Simple Mail Transfer Protocol ebenfalls leicht durch ein beliebiges Argument des „MAIL FROM“-Kommandos gefälscht werden. Spammer machen hiervon häufig Gebrauch und übermitteln E-Mail-Nachrichten mit zufällig gewählten Envelope-Absender-E-Mail-Adressen.

Erst in letzter Zeit tauchen Spam-Nachrichten auf, die absichtlich Absender-Adressen nutzen, die dem Empfänger bekannt sind, in der Hoffnung, damit die Antispam-Mechanismen zu umgehen. Hierbei nutzen Spammer die Tatsache, dass viele E-Mail-Nutzer wichtige E-Mail-Kontakte in einer Whitelist aufgeführt haben, um E-Mails von diesen Kontaktadressen in jedem Fall zugestellt zu bekommen. Die Untersuchungs-Ergebnisse bestätigen dies. Insgesamt nutzen 43% der Befragten eine Whitelist, also lediglich rund 3% weniger, als jene, die eine Blacklist einsetzen. Dies ist typisch, denn der Einsatz einer Blacklist erfordert in fast allen Fällen auch den Einsatz einer Whitelist, um gewollte Kommunikation explizit zu erlauben und vor Fehlentscheidungen der Blacklist zu schützen.

Envelope-Empfänger-E-Mail-Adresse

Die Envelope-Empfänger-Adresse ist das Merkmal, das bestimmt, in welches Postfach die E-Mail zugestellt wird. Sie kann also für die reguläre E-Mail-Kommunikation nicht als Merkmal zur Bestimmung von Spam herangezogen werden.

Es gibt Ansätze, die spezielle, für die reguläre E-Mail-Kommunikation nicht genutzte E-Mail-Adressen quasi als Spam-Fallen, sog. spam traps, reservieren (vgl. [Hone05] oder http://wiki.fastmail.fm/wiki/index.php/SpamTraps). Diese E-Mail-Adressen werden je nach Zweck gar nicht oder nur selten sehr gezielt publiziert. Wird auf einer solchen E-Mail-Adresse eine E-Mail empfangen, so kann meistens auf Spam geschlossen werden.

> Letztendlich bleibt also nur die IP-Adresse des einliefernden Clients als verlässliches Merkmal zur Identifikation möglicher Spam-Quellen.

Blockieren dynamischer IP-Adressen

Internet Service Provider vergeben IP-Adressen für Dial-Up-Kunden in der Regel nicht statisch, sondern es wird bei jeder Einwahl einem Kunden – hauptsächlich aufgrund von Managementaspekten – dynamisch eine IP-Adresse aus einem Pool zugeteilt. Für solche Adressbereiche der Internet Service Provider findet also eine ständige Rekombination von IP-Adressen und ihren Nutzern statt.

Für die Sperrung von IP-Adressen spielt die Häufigkeit der Rekombination eine Rolle, denn sie hilft, eine sinnvolle Dauer der Speicherung einer IP-Adresse in einer Blacklist zu bestimmen.

Dial-Up-Rechner bzw. Rechner mit dynamischen Dial-Up-IP-Adressen sind deswegen eine ernst zu nehmende Spam-Quelle, weil mittlerweile durch Trojaner infizierte Computer mit Internetverbindung, sog. Zombie PCs, in großem Stil zum Spam-Versand genutzt werden. Solche Rechnerverbünde werden auch als Botnetze bezeichnet.

Der reguläre Versand von E-Mails von einem Dial-Up-Rechner erfolgt durch Übermittlung an den SMTP-Server des Service Providers, einen sog. Smarthost. Ein Indiz für den Spam-Versand ist also eine direkte Einlieferung von E-Mails auf verschiedenen Ziel-E-Mail-Servern.

In Ausnahmefällen betreiben IT-Spezialisten unter einer dynamischen IP-Adresse einen eigenen E-Mail-Server, der E-Mails nicht über einen Smarthost, sondern direkt an den entsprechenden Ziel-E-Mail-Server ausliefert. Die Erfahrung aus der Praxis mehrerer großer Service Provider für E-Mail zeigt jedoch, dass sich solche Fälle bei Bedarf problemlos mit den entsprechenden Personen klären lassen.

Teilweise reagieren Internet Service Provider auf das Zombie-Problem, indem sie ihren Kunden direkte Verbindungen zu dem Standard-SMTP-Port (25) auf anderen Adressen als derjenigen des eigenen Smarthosts unterbinden.

Einige – aber bei weitem nicht alle – Service Provider führen eine Authentifizierung durch, bevor die E-Mail vom Smarthost entgegengenommen wird. In der ifis-Untersuchung wurde unter Service Providern für die SMTP-Erweiterung SMTP AUTH [RFC2554] ein Verbreitungsgrad von unter 50% ermittelt.

Ein weit verbreiteter Einsatz von Blacklists, sog. DUL-Lists, ist daher die Sperrung fremder dynamischer Dial-Up-IP-Adressen für die direkte E-Mail-Einlieferung auf Mail-Servern.

Realisierungen von Blacklists

Blacklists sind die ältesten Mechanismen zur Bekämpfung von Spam. Die Methode, ungewollte Kommunikation zu verhindern, indem von einer Quelle keine Nachrichten

angenommen werden, ist seit langem bekannt und sehr erfolgreich. Allerdings haben Spammer ihre Techniken weiterentwickelt, sodass heutzutage viele verschiedene Quellen mit unterschiedlichen Adressen Spam in das Internet einspeisen, die nicht mehr einfach und insbesondere nicht auf Dauer zu blockieren sind. Eine statische Liste hilft allenfalls in wenigen Sonderfällen gegen Spam mit bekannten Adressen von Spammern. Demgegenüber muss eine zeitgemäße Blacklist einen dynamischen Charakter haben. Man bezeichnet solche dynamischen Blacklists auch als Realtime Black Lists oder Realtime Blackhole Lists (RBL).

Die vermutlich am weitesten verbreitete Realisierung von Blacklists ist die DNS basierte Blacklist, sog. DNS Blacklist (DNSBL). Solche Blacklists nutzen zur Abfrage das DNS-Protokoll und bieten den Vorteil, dass vorhandene DNS-Resolver-Bibliotheken zur Abfrage genutzt werden können. Um in Erfahrung zu bringen, ob eine bestimmte IP-Adresse a.b.c.d in einer DNS-basierten Blacklist aufgeführt ist, wird üblicherweise eine Abfrage der Art d.c.b.a. [DNSBL-Domäne] gestartet. Die Antwort des Servers kodiert in der Regel mit einer Antwort im Bereich 127.0.0.0/24 den Grund des Eintrags in der Blacklist.

Informationsquellen für IP-Blacklists

Eine wichtige Frage in Bezug auf IP-Blacklists muss sein, wer die Informationen gewinnt und auf welche Art und Weise sie gewonnen werden. Je mehr E-Mail-Traffic zur Beobachtung bereitsteht, umso qualifizierter kann eine Einschätzung bezüglich einer fremden IP-Adresse gemacht werden. Große ISPs mit einem hohen E-Mail-Verkehr können daher relativ sicher beispielsweise über Mustererkennung in der E-Mail-Nutzung (siehe auch [CLAY04]) mögliche Spam-Quellen extrapolieren. Gezielte Kooperationen unter ISPs können diese Ergebnisse sogar noch weiter verbessern. Ebenso helfen spam traps, um Spam-Versender aufzuspüren. Diese IP-Adressen können dann auf einer Blacklist verzeichnet werden.

Aber auch für das Entfernen von zum Beispiel fälschlicherweise eingetragenen IP-Adressen müssen Mechanismen etabliert sein, die ein versehentliches Sperren so zügig wie möglich wieder aufheben.

IP-Blacklisting aus der Perspektive des Senders

Aus der Perspektive des Absenders einer E-Mail wird relativ schnell deutlich, dass eine E-Mail aufgrund eines Blacklist-Eintrags abgeblockt wurde. Der MTA, der blockiert wurde, erhält im SMTP-Dialog üblicherweise eine Fehlermeldung, die den Grund für die Blockade enthält, beispielsweise in welcher Blacklist seine IP-Adresse gerade als Spam-Quelle aufgeführt wird. Die Non-Delivery Notification, die vom sendenden Mail-Server an den E-Mail-Absender generiert wird, enthält diese Fehlermeldung in der Nachricht, sodass der Absender den Grund für die fehlgeschlagene Zustellung erfährt und ggf. Gegenmaßnahmen einleiten kann. Ein Verlust von Information findet daher nicht statt.

Service Provider sollten allerdings wichtige Blacklists häufig konsultieren und abfragen, ob ihre sendenden E-Mail-Server dort aufgelistet werden.

Fazit

Die Ergebnisse der Untersuchung bestätigen, dass sich IP-Blacklisting als beste und effizienteste Möglichkeit der Spam-Abwehr cxy ausschließliche Anwendung von Blacklisting Spam nicht vollständig vermieden. Es ist ein erster Schritt in die entscheidende Richtung, um Spam im Internet auf ein erträgliches Maß zu reduzieren und langfristig zu verhindern.

> Ein effektives Blacklisting ist darauf angewiesen, dass alle wichtigen Parteien im Internet zusammenarbeiten und gegenseitig Informationen bereitstellen.

Eine größere Verbreitung von IP-Blacklisting und eine effektivere Anwendung sind aus unserer Sicht dringend notwendig, um den E-Mail-Dienst in Zukunft weiterhin nutzen zu können.

Literatur

[RFC2821] J. Klensin: Simple Mail Transfer Protocol, RFC 2821, 2001

[CLAY04] R. Clayton: Stopping Spam by Extrustion Detection, 2004, http://www.cl.cam.ac.uk/users/rnc1/extrusion.pdf

[RFC2554] J. Myers: SMTP Service Extension for Authentication, RFC2554, 1999

[DiPo05] C. Dietrich, N. Pohlmann: E-Mail-Verlässlichkeit: Auswertung der Umfrage Ende 2004, 2005, http://www.internet-sicherheit.de/center-berichte.html

[Hone05] Honeyd project, Honeyd Research: Honeypots Against Spam, Stand: 1.März 2005, http://www.honeyd.org/spam.php