Verband der Internetwirtschaft e. V.

Auswahl einer DNSBL

eco Kompetenzgruppe E-Mail

Inhaltsverzeichnis

Autoren: Tobias Herkula (optivo GmbH), Gunther Nitzsche (NetCologne Gesellschaft für Telekommunikation mbH), Andreas Schulze (DATEV eG), Kerstin Espey (HeLi NET Telekommunikation GmbH & Co. KG), Sven Krohlas (1&1 Mail & Media GmbH), Florian Kunkel (Deutsche Telekom AG), Carsten Kühn (empaction GmbH), Olaf Petry (antispameurope GmbH), Alexander Schaefer (Host Europe GmbH), Florian Vierke (TERADATA)

Editor: Sven Krohlas (1&1 Mail & Media GmbH)

Abstract

Die Kompetenzgruppe E-Mail des eco e.V. gibt Hilfestellung für Mailserveradministratoren bei der Auswahl passender Blacklisten.

Motivation

Neben erwünschten Mitteilungen erreichen eine Vielzahl unerwünschter Nachrichten aller Art inzwischen die meisten Mailpostfächer. Die Empfänger erwartet beim Blick in den Posteingang eine Mischung aus per Mail verbreiteter Schadsoftware, unerwünschter Werbung, teilweise unregelmäßig erscheinende Newsletter sowie geschäftliche und private Korrespondenz.

Nutzer und ISPs versuchen sich an der Erkennung und Filterung von Spam. Eine Einteilung in erwünschte Ham- und unerwünschte Spamnachrichten ist jedoch aufwändig und mühsam. Zu dem dafür nötigen Zeitaufwand kommen Kosten für Speicherplatz, Bandbreite und Rechenkapazität für die Übermittlung und Verarbeitung von Spamnachrichten. Sie stellen somit einen nicht unerheblichen Kostenfaktor für die Empfängerseite dar. Je nach Erfolg der Filter gehen gewollte Nachrichten noch immer zwischen Spam unter, verschwinden fälschlicherweise im Spam-Ordner, werden gelöscht oder es werden ungewollte Nachrichten als legitim eingestuft.

Daher setzen die meisten Postmaster zusätzlich auf in Echtzeit gepflegte, DNS-basierte Blacklisten (DNS Based Realtime Blacklists; DNSBL) von IP-Adressen, ganzen Netzen oder Domänen. Von diesen nehmen sie Nachrichten gar nicht erst an oder lassen die Informationen aus einem Listing in das Spamscoring einfließen. Diese Verfahren sind auch technisch von der IETF beschrieben: https://tools.ietf.org/html/rfc5782

Inzwischen existiert eine große Anzahl an Blacklisten von diversen Betreibern, die nach verschiedenen Kriterien IP-Adressen oder Domains listen. Der praktische Austausch in der eco Kompetenzgruppe E-Mail hat hierbei gezeigt, dass die Auswahl der am besten geeigneten Listen für Postmaster allein schon auf Grund der großen Menge verfügbarer Listenanbieter schwer fällt. Daraus entstand der Wunsch Kriterien zum Blacklisteneinsatz zu sammeln und deren Folgen klar darzulegen. Wir erhoffen uns hiermit den Administratoren von Mailsystemen Hilfestellung zu geben und die Auswahl zu erleichtern.

Dennoch sind allein die Postmaster und nicht die Listenbetreiber für die Entscheidung eine Mail anzunehmen, abzulehnen oder als Spam zuzustellen verantwortlich. Daher ergänzen viele Postmaster ihr Filterkonzept zusätzlich durch den Einsatz von Whitelisten, um die Zustellung von Nachrichten bekannter seriöser Versender sicherzustellen.

Für eine ausführlichere Diskussion von Kriterien an seriöse Blacklisten verweisen wir auch auf https://tools.ietf.org/html/rfc6471.

Auswahlkriterien

Bei der Auswahl einer passenden Blacklist sollte sich der Mailserveradministrator mindestens folgende Fragen stellen:

Wie gut ist die Qualität der betrachteten Liste?

Eine gute DNSBL hat zum einen eine hohe Trefferrate bei Spam einliefernden IP-Adressen, zum anderen – noch wichtiger! – eine sehr geringe Fehlerrate bei Ham. DNSBLs, die öfter falsche oder zu große IP-Ranges listen, werden natürlich in den üblichen Foren diskutiert. Ein Blick in die Suchmaschine des Vertrauens liefert hier erste Anhaltspunkte.

Wie verbreitet ist die Liste?

Eine DNSBL, die kaum bekannt ist, ist schwer gegenüber geblockten Absendern zu argumentieren. Ein erhöhter Supportaufwand ist daher zu erwarten, um geblockten Absendern das Prozedere zu erklären.

Wie seriös ist die Liste?

Eine seriöse DNSBL nimmt kein Geld für ein Delisting (Interessenkonflikt) und hat nachvollziehbare Listing- und Delisting-Kriterien.

Eine strukturierte Webseite zur DNSBL, die die jeweiligien Kriterien sowie auch den Einsatzzweck und evtl. Einschränkungen bei der Nutzung beschreibt, sollte bei der Auswahl berücksichtigt werden. Auch die Kontaktdaten zur jeweiligen DNSBL sollten aus der Webseite hervorgehen. Die Informationsseiten der DNSBL sollten auch nicht als "Honeypot" für weitere Listing-Aktivitäten dienen.

Bietet die Liste eine Inhouse-Lösung?

Durch die (DNS)-Abfrage bei einer DNSBL erhält der Listenbetreiber auch weitergehende Informationen über den Mailverkehr des Anfragenden. Die Nutzung von Listen, die zur Inhaltsfilterung gedacht sind, verraten dabei sogar Teile des Nachrichteninhalts. Über Listen, die auf Metadaten der Kommunikation wie beispielsweise IP-Adressen angewendet werden, erhält der Listenbetreiber diese Informationen. Sollten Listenbetreiber die Möglichkeit anbieten ihre Listen zu kopieren – beispielsweise mittels Rsync –, können sie als lokale Kopie ohne diese Datenschutzbedenken, die auch zu rechtlichen Problemen führen können, eingesetzt werden.

Welchen Einsatzzweck bietet die Liste?

Die meisten DNSBLs bieten IP-Adresslisten, die zum Reject von E-Mails genutzt werden können. Jedoch gibt es auch Listen, die etwa zur Inhaltsanalyse (z.B. beworbene URLs) genutzt werden können und/oder auf Basis von Domainnamen agieren. Der Mailserveradministrator muss sich über den von ihm präferierten Einsatzzweck im Klaren sein und sollte die Liste nur nach dem vorgegebenen Zweck einsetzen. Manche DNSBLs werden auch nicht durch den Betreiber selbst gefüllt, sondern nutzen Meldungen anderer ISPs, die bestimmte IP-Adressbereiche (etwa dynamische Einwahl-IPs), aus denen keine E-Mails direkt gesendet werden sollen, einpflegen. Sind beispielsweise die eigenen Kundenadressen dort gelistet, sollte man diese Liste nicht ungeprüft auf den Kundenmailservern einsetzen.

Hinweis:

Um dem deutschen TKG gerecht zu werden, darf eine Mail nicht mehr abgewiesen werden, nachdem dem Absender die Annahme im SMTP-Protokoll gemeldet wurde. Um ein Reject, basierend auf einer Inhaltsüberprüfung, zu senden, muss die E-Mail-Annahme bis vor der Statusmeldung verzögert werden.

Welche Listingkriterien werden angewendet?

Die Aufnahme in eine DNSBL erfolgt niemals ohne Grund, wobei die Verweildauer eines Eintrages auf einer DNSBL selbst von verschiedenen Faktoren wie der Reputation des Einlieferers und dem Listinggrund abhängig sein kann.

Es gibt verschiedenste Listinggründe, z.B.:

- Belege für eine Infektion mit Malware.
- Spamtrap-Hits.
- Verhalten, dass auf Missbrauch hindeutet, wie beispielsweise die auffällig häufige Adressierung nicht existenter Adressen.
- Policy-Gründe: Die gelisteten IPs, Netze oder Domänen dürfen laut Besitzer bzw Betreiber keine Mails versenden. Dies ist insbesondere bei dynamisch vergebenen Adressbereichen oft der Fall. Auch IPs oder ganze Netze von Betreibern, die Spamprobleme nicht oder nicht zeitnah beseitigen, können per Policy gelistet werden.

Diese Liste ist nicht abschließend.

Wozu muss ich als Nutzer der Liste die Listingkriterien so genau kennen?

Wenn der Listenbetreiber den oder die Gründe, die zu einer Aufnahme in die Liste geführt haben, klar kommuniziert, werden Supportanfragen von Nutzern und Versendern einfacher und schneller zu bearbeiten sein.

Der Postmaster kann direkt (bereits in der Reject-Meldung) auf den Listinggrund verweisen. Voraussetzung hierfür ist, dass der Listenbetreiber Belege für den Listinggrund für einen angemessenen Zeitraum vorhält. Dies können, abhängig vom Grund des Listings, beispielsweise Samples eingegangener Spammails oder Zustellstatistiken sein.

Auch eine Anleitung zur Entfernung oder zum Auffinden eventuell an ihrem Verhalten erkannter Schadsoftware wäre als Hinweis an den geblockten Nutzer denkbar.

Belege für den Listinggrund müssen nicht zwingend automatisiert abrufbar sein. Falls der Abruf jedoch nur von der gelisteten IP aus möglich wäre, können diese Informationen nicht mehr für Supportanfragen genutzt werden. Auch kann der Administrator des gelisteten Systems möglicherweise selbst nicht auf die Begründung zugreifen, denn nicht jeder Mailserver ist mit Software zur Kommunikation über andere Protokolle ausgestattet. Üblich ist eine Abfrage auf der Webseite der DNSBL unter Angabe der betroffenen IP.

Wenn ein Listenbetreiber eine Möglichkeit der Benachrichtigung über ein Listing anbietet, ermöglicht dies dem Betroffenen eine schnelle Analyse des Vorfalls. Zudem kann dies auf Empfängerseite Supportanfragen reduzieren, da der betroffene Einlieferer schneller und ohne weitere Rückfragen reagieren kann.

Wie funktioniert ein Delisting?

Der Weg zum Delisting selbst sollte dokumentiert sein, um Supportaufwände zu reduzieren. Hierbei sollte darauf geachtet werden, dass technische Hürden niedrig und umsetzbar sind, andernfalls werden geblockte Einlieferer nicht den Listenbetreiber, sondern den Postmaster des Empfangssystems um Hilfe bitten.

Was kostet die Liste?

Im professionellen Umfeld sind einige DNSBLs aktiv, die für Ihren Einsatz Geld nehmen; andere sind kostenfrei. Um abschätzen zu können, ob die gewünschte DNSBL ihr Geld wert ist, sei insbesondere auf die Punkte Qualität und Verbreitung der Liste verwiesen. Im Einzelfall sollte eine Testphase mit dem Anbieter vereinbart werden.

Listings sollten nicht nur ausschließlich fachlich begründet vorgenommen, sondern auch nur fachlich begründet erhalten bleiben. Sollte ein Delisting beispielsweise von Geldzahlungen abhängig sein, kann dies einen Interessenkonflikt darstellen. Denn schließlich würde der Betreiber durch ein Listing und dem darauf folgenden Delisting finanziell profitieren.

Wie sind die Listenbetreiber erreichbar?

In Deutschland wird bei Geschäftspartnern üblicherweise eine ladungsfähige Adresse erwartet. Insbesondere bei Listen aus dem Ausland kann dies problematisch werden. Inländische Listen sollten auf jeden Fall eine ladungsfähige Adresse vorweisen. Es darf nicht vergessen werden: Der Postmaster, nicht der Betreiber der DNSBL, ist für die Annahme eingehender Mails verantwortlich. Falls ein Einlieferer schon wegen Kontaktproblemen kein Delisting erreichen kann, wird er sich möglicherweise mit Rechtsmitteln gegen den Postmaster wenden.

Eine kommunizierte Support-Adresse mit kurzen Antwort- und Reaktionszeiten ist auf jeden Fall ratsam. Ein Kontakt, z.B. nur über bestimmte Usenet-Gruppen mit unbestimmten Ansprechpartnern, ist sicherlich nicht für einen schnellen gezielten Support hilfreich.

Kann man die DNSBL testen?

Besitzt eine DNSBL die in https://tools.ietf.org/html/rfc5782#section-5 spezifizierten Testeinträge, so können Administratoren die korrekte Funktionalität ihres Mailsystems sowie der DNSBL selbst prüfen. Dies ermöglicht eine schnelle Reaktion, beispielsweise falls die DNSBL eines Tages abgeschaltet werden soll.

Ein Vergleich der Wirksamkeit von Blacklisten für bekannte Usecases lässt sich auch durch den Abgleich bekannter guter und schlechter IP-Adressen mit verschiedenen DNSBLs umsetzen.

Über http://www.anti-abuse.org/multi-rbl-check/, http://mxtoolbox.com/blacklists.aspx, http://rbl-check.org/ oder auch andere Anbieter lässt sich einfach verifizieren, ob eine Spam sendende IP-Adresse wie erwartet gelistet und gute IP-Adressen nicht gelistet werden. Durch Wiederholung des Tests mit IP-Adressen verschiedener aktueller Angriffe lässt sich die Wirksamkeit der einzelnen Listen durch den Postmaster abschätzen.

Quellen und Verweise

DNS Blacklists and Whitelists

https://tools.ietf.org/html/rfc5782l

Overview of Best Email DNS-Based List (DNSBL) Operational Practices

https://tools.ietf.org/html/rfc6471

Die neueste Version dieses Dokuments ist online im Blog der Kompetenzgruppe E-Mail zum Download verfügbar.

https://e-mail.eco.de/downloads.html

Über eco - Verband der Internetwirtschaft e.V.

Mit mehr als 800 Mitgliedsunternehmen ist eco der größte Verband der Internetwirtschaft in Europa. Seit 1995 gestalten wir maßgeblich die Entwicklung des Internets in Deutschland, fördern neue Technologien, Infrastrukturen sowie Märkte und formen Rahmenbedingungen. In den eco Kompetenzgruppen sind alle wichtigen Experten und Entscheidungsträger der Internetwirtschaft vertreten und treiben aktuelle und zukünftige Internetthemen voran, gemeinsam mit einem Team von über 60 Mitarbeitern.

Spezielle eco Services helfen, den Markt für Anbieter und Anwender transparenter zu machen, unsere Gütesiegel sorgen für Qualitätsstandards. Mit Beratungsangeboten für Mitglieder und unseren Services für Internetnutzer unterstützen wir bei Fragen zur Rechtslage, erhöhen die Sicherheit und verbessern den Jugendschutz.

Als Verband ist es eine unserer wichtigsten Aufgaben, die Interessen der Mitglieder gegenüber der Politik und in nationalen sowie internationalen Gremien zu vertreten. Neben unserer Hauptgeschäftsstelle in Köln haben wir ein eigenes Hauptstadtbüro in Berlin und sind bei allen relevanten politischen Entscheidungsprozessen in Brüssel vor Ort.

Mehr Informationen über die eco Kompetenzgruppe E-Mail auf dem offiziellen Blog unter https://e-mail.eco.de/