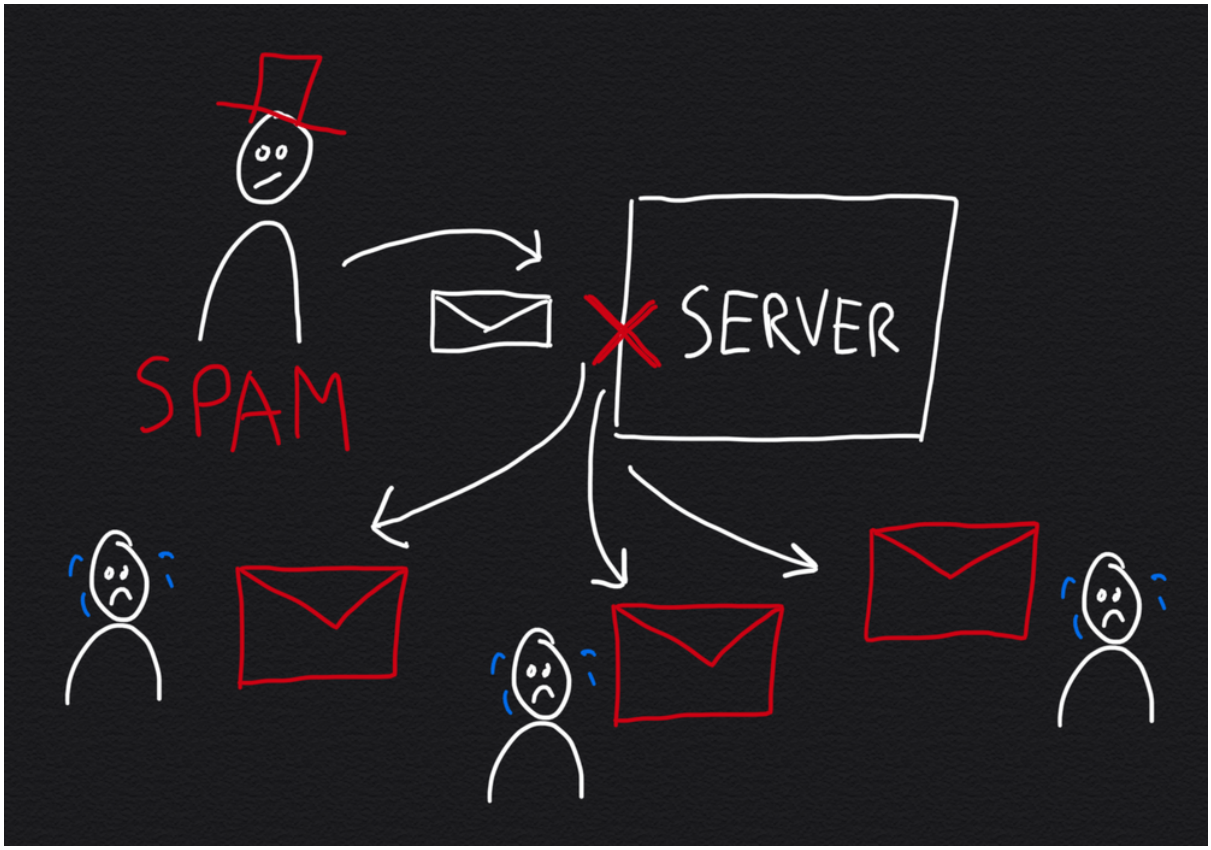
Bekämpfung von Backscatter-Spam auf Serverebene

Postfix so konfigurieren, dass Spam blockiert wird, bevor er den Server erreicht

Willem L. Middelkoop
Sep. 10, 2019



Diesen Monat hatte ich mit Backscatter-Spam zu kämpfen, der einen der von mir verwalteten Mailserver betraf. Als Server-Engineer stelle ich sicher, dass Server keinen Spam versenden und eingehende E-Mails gefiltert werden. Trotz aller Bemühungen wurde dieser Server immer wieder auf die Blacklist gesetzt, weil er Spam an iCloud, Office 365 und Google Gmail for Business (G Suite) gesendet hat. Lesen Sie weiter, um herauszufinden, was die Ursache dafür war und wie man das Problem behebt.

Das Problem

Der Server ist ein Postfix-Mailserver unter Debian GNU/Linux, auf dem die neuesten Updates und Sicherheitspatches ausgeführt werden. Der Server wird von legitimen Kunden

verwendet, die ihn nur mit ordnungsgemäßer Authentifizierung verwenden können.

Verhindern Sie, dass ein Open Relay entsteht

Die individuelle Benutzerauthentifizierung auf einem Mailserver ist eine wichtige Maßnahme gegen den Missbrauch des Mailservers. Wenn Spam versendet wird, können Sie anhand der Mailserver-Protokolle feststellen, welcher Benutzer das Problem verursacht. Technisch gesehen bedeutet dies, dass Sie verhindern, dass der Server zu einem „Open Relay“ wird. Postfix bietet viele Einstellungen, um _SMTP_Relay_mit_Zugriffskontrolle einzuschränken.

Ratenbegrenzung für (gehackte) E-Mail-Konten

Servermissbrauch durch einzelne Benutzer tritt auf, wenn ihr Computer mit einem Virus infiziert wird oder ihr Passwort abgefangen wird. Dies kann passieren, wenn Sie über ein unsicheres WLAN ohne Verschlüsselung (TLS/SSL) auf Ihre E-Mails zugreifen. In solchen Situationen ist es ratsam, die Anzahl der E-Mails, die einzelne Benutzer senden dürfen, zu begrenzen. Sie können individuelle Postfix Konfigurationsparameter (wie *smtpd_client_message_rate_limit, smtpd_client_connection_rate_limit* und *smtpd_client_recipient_* verwenden oder eine Postfix-Firewall wie Postwfd verwenden.

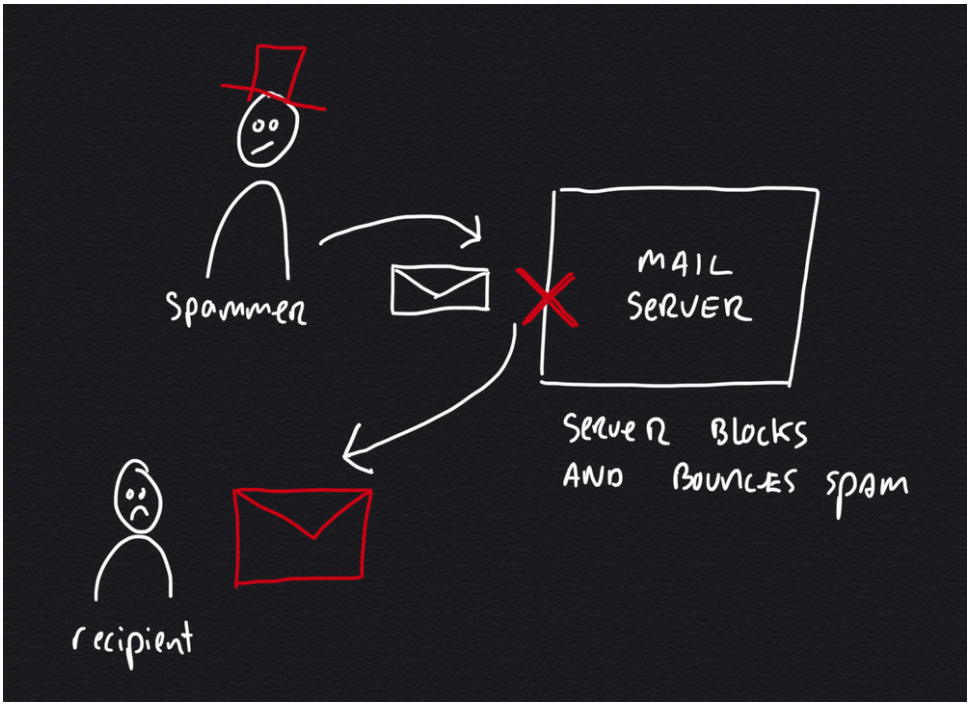
Der Server wird auf der schwarzen Liste von 'backscatterer.org' geführt

Trotz aller Maßnahmen gegen Spam-Missbrauch wurde der Server immer noch auf `http://backscatter.org` wegen des Versendens von Spam aufgeführt. Wenn ein Server auf einer schwarzen Liste aufgeführt wird, vertrauen ihm andere Server nicht mehr und betrachten alle Nachrichten als verdächtig. Dies kann dazu führen, dass Ihre (legitimen) Nachrichten von anderen Servern als Spam angesehen werden (falsch positive Ergebnisse). Um zu verstehen, warum dies geschah, müssen Sie zunächst verstehen, was Backscatter-Spam ist.

Was ist Backscatter-Spam?

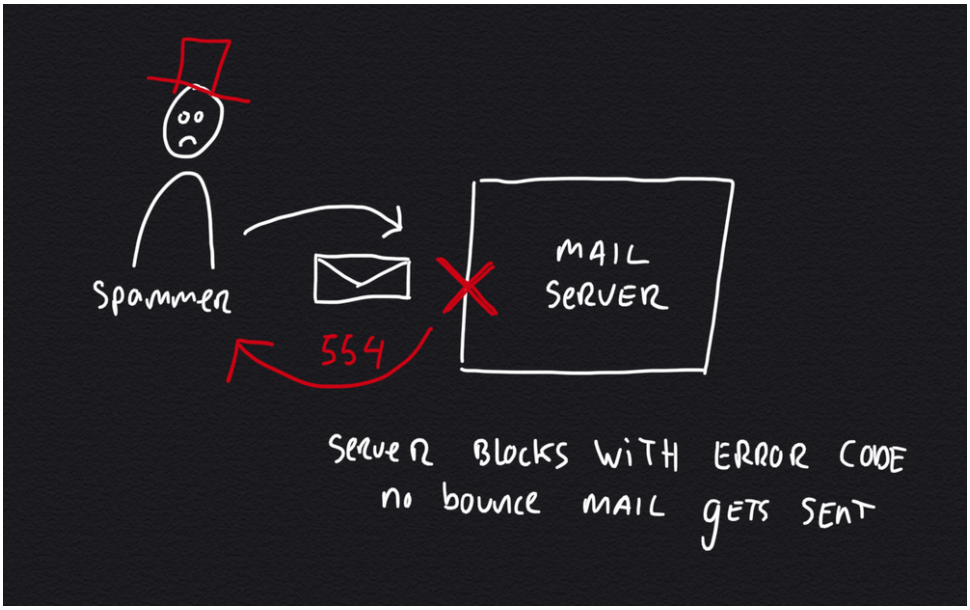
Backscatter-Spam sind falsch automatisierte Unzustellbarkeitsmeldungen, die vom Mailserver gesendet werden, normalerweise als Nebeneffekt von eingehendem Spam.

Backscatter tritt auf, wenn Spammer die Absenderadresse fälschen. Sie senden eine E-Mail-Nachricht, von der sie erwarten, dass sie mit der Adresse einer anderen Person als Absender zurückgewiesen wird. Wenn die E-Mail-Nachricht zurückgewiesen wird, sendet der Mailserver die Nachricht an den gefälschten Absender zurück... wodurch der Server effektiv Spam an die Absenderadresse liefert.



Einfaches Backscatter-Szenario, Mailserver sendet Bounce-Nachricht an eine gefälschte Absenderadresse

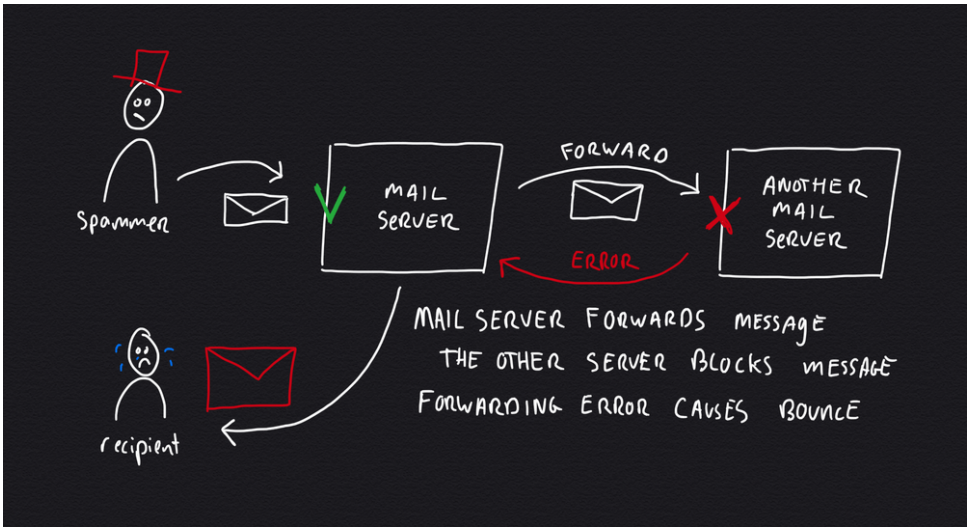
Das einfache Backscatter-Szenario ist, dass eine Nachricht an den falschen Absender zurückgewiesen wird. Dieses Szenario lässt sich einfach lösen, indem der Server so konfiguriert wird, dass er keine Unzustellbarkeitsmeldungen sendet, sondern stattdessen mit einem SMTP-Fehlercode antwortet.



Backscatter-Bounce-Nachrichten verhindern, indem mit SMTP-Fehlercodes geantwortet wird

Leider gibt es ein weiteres (schwierigeres) Szenario, das dazu führt, dass Ihr Mailserver Backscatter-Spam sendet. Dies geschieht, wenn jemand auf Ihrem Server sein E-Mail-Konto so konfiguriert, dass E-Mails an eine andere Adresse weitergeleitet werden. Der

zweite Server verfügt möglicherweise über einen strengeren Spamfilter, der dazu führt, dass Nachrichten bei der Weiterleitung blockiert werden. Ihr Mailserver informiert dann den ursprünglichen Absender darüber, dass die Weiterleitung fehlgeschlagen ist, was zu Backscatter-Spam führt.

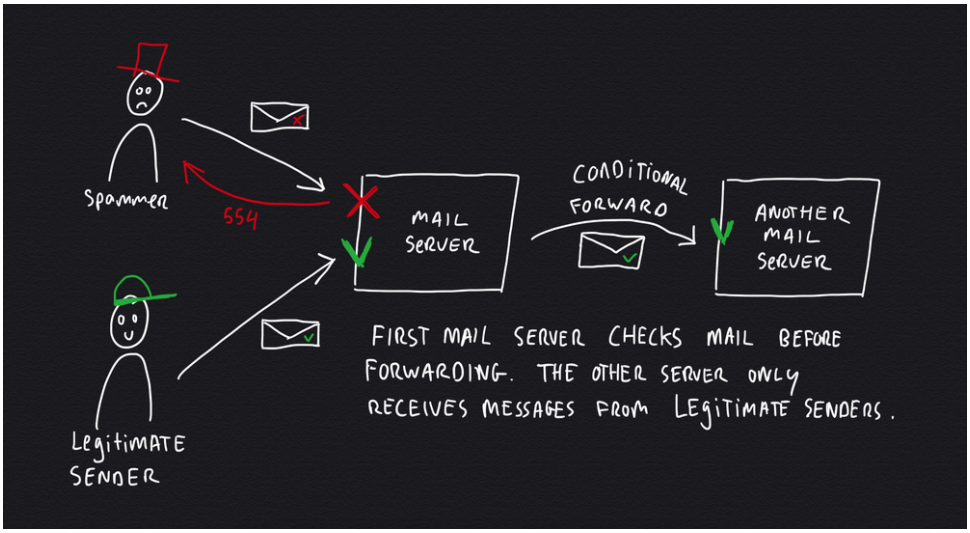


Verursacht Backscatter-Spam, wenn der erste Mailserver E-Mails an einen anderen Server weiterleitet, der die Nachricht blockiert

Das Weiterleitungsszenario ist viel schwieriger zu lösen, da Sie möglicherweise keine Kontrolle über den anderen Mailserver oder dessen Spamfiltereinstellungen haben. Schlimmer noch, es gibt oft eine gewisse Verzögerung zwischen dem Annehmen der Nachricht und ihrer Weiterleitung, wodurch es unmöglich ist, auf eine Antwort des anderen Mailservers zu warten.

Verhindern Sie Backscatter-Spam

Die einzige Möglichkeit, Backscatter-Spam vollständig zu verhindern, besteht darin, beim ersten Mailserver, in der anfänglichen SMTP-Verbindungsphase, sehr streng zu sein. Dies löst das schwierige „Weiterleitungsszenario“, indem sehr selektiv vorgegangen wird, welche Nachrichten weitergeleitet werden.



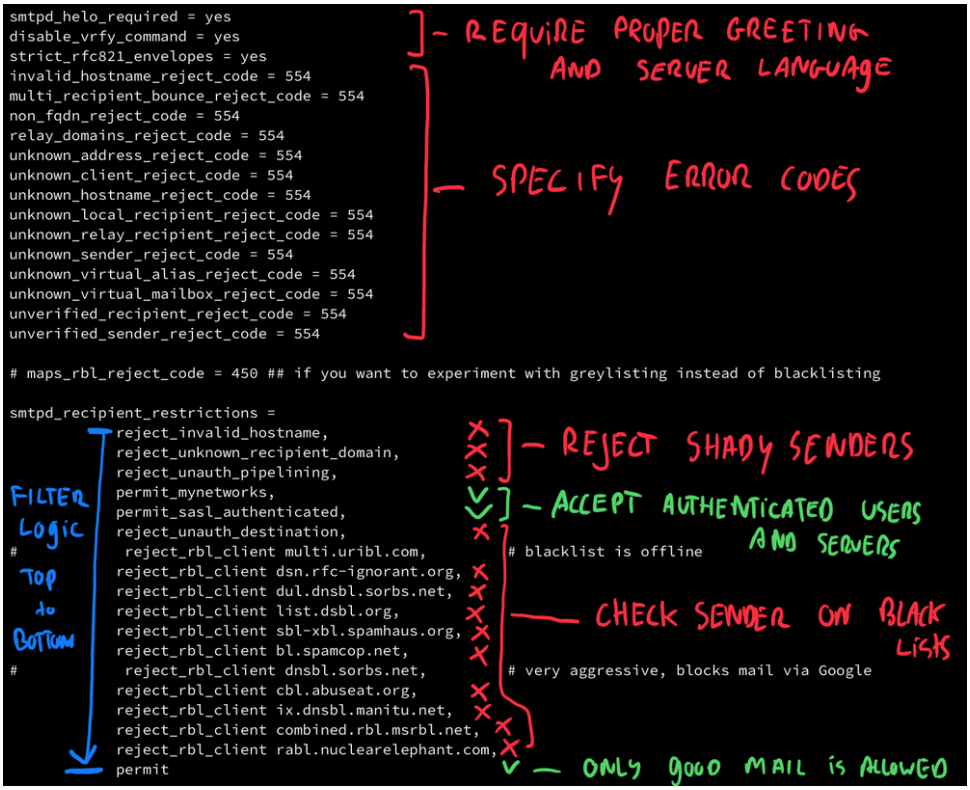
Backscatter-Spam verhindern, indem alle Nachrichten überprüft werden, bevor sie an einen anderen Server weitergeleitet werden

So blockieren Sie Spam, bevor er in den Server gelangt

Der beste Weg, Backscatter-Spam zu verhindern, besteht darin, ihn zu blockieren, bevor er in die (Kette von) Server(n) gelangt.

Traditionell verwenden Server fortschrittliche Spamfilter wie SpamAssasin, um Nachrichten einzeln zu analysieren. Dies verursacht zusätzliche Belastung für den Mailserver.

Es ist viel einfacher, sich den Absender anzusehen (z. B. ob er einen roten Hut trägt), um eine erste Filterung durchzuführen. Steht der Absender auf einer schwarzen Liste? Verwendet er eine „normale“ Mail-App, oder werden Nachrichten von einem Virus oder Malware gesendet? Sie können viele Dinge feststellen, indem Sie sich die „Sprache“ ansehen, die der Absender spricht.



Implementierung strenger SMTP-Einschränkungen in Postfix - kommentierter Screenshot aus main.cf

In Postfix können Sie SMTP-Einschränkungen in der Konfigurationsdatei *main.cf* festlegen. Es gibt Prüfungen, die verwendet werden können, um Nachrichten zu blockieren. Es ist ratsam, in der Filterlogik von „einfach zu schwer“ zu arbeiten, beginnend mit Dingen, die ohne Rücksprache mit externen Servern überprüft werden können. Dies reduziert den Netzwerkverkehr und die Belastung. Nur wenn eine Nachricht alle Prüfungen besteht, wird sie zur Zustellung (oder Weiterleitung) zugelassen.

Bei der Zustellung können Sie zusätzliche komplexe (und benutzerspezifische) Spamfilterung mithilfe von Tools wie SpamAssasin oder Bayes_Filterung (https://de.wikipedia.org/wiki/Rekur Schätzung) implementieren. Durch die Reduzierung des Zustroms offensichtlicher Spam-Nachrichten können diese ressourcenintensiven Filter ihre Arbeit viel effizienter erledigen.

Fazit

Die Bekämpfung von Spam auf Serverebene ist ein herausforderndes Spiel, da Spammer immer kreativer werden, wenn es darum geht, die Mechanismen von Mailservern zu missbrauchen. Wenn Ihr Server wegen Backscatter-Spam auf die schwarze Liste gesetzt wird, müssen Sie sich vor Weiterleitungsszenarien in Acht nehmen. Behalten Sie schwarze Listen im Auge, um zu sehen, ob Ihr Server Probleme verursacht.

Blockieren Sie Nachrichten mit Fehlercodes, anstatt sie an den Absender zurückzusenden (Unzustellbarkeitsmeldungen). Konfigurieren Sie den Server mit einer strengen Zustellungsrichtlinie. Der beste Weg, Backscatter-Spam zu verhindern, besteht darin, Nachrichten zu blockieren, bevor sie in den Mailserver gelangen. Jetzt wissen Sie, wie das geht.