Stolperfallen beim E-Mail-Transport

Leicht gestört

Sven Krohlas

Mailserver sollen die ihnen anvertrauten E-Mails möglichst schnell weiterreichen und dabei möglichst wenig Spam durchlassen. Das setzen große Mailprovider manchmal anders um als kleinere Serverbetreiber – und die unterschiedlichen Maßnahmen können einander leider behindern.

Große Mailprovider vertrauen meist auf Systeme, die die Reputation der Absender bewerten – ein effizientes Verfahren, das umso zuverlässiger funktioniert, je mehr Kunden und damit E-Mail-Durchsatz ein Anbieter hat. Für jede Domain oder IP-Adresse zeigt sich im Laufe der Zeit, ob sie vor allem erwünschte E-Mails oder ausschließlich Spam versendet. Die Anwender können selbst zur Filtergenauigkeit beitragen, indem sie Unerwünschtes als Spam markieren.

Greylisting dagegen – das temporäre Abweisen eingehender E-Mails – ist bei großen Mailanbietern wegen der damit einhergehenden zusätzlichen Last ziemlich unbeliebt. Doch viele Betreiber kleinerer Mailserver nutzen es in der Hoffnung, dass Spamversender nur einen Zustellversuch unternehmen und der Spam somit nie ankommt. Ein legitimer Versender hingegen wird sicher erneut versuchen, die zurückgestellte E-Mail abzuliefern. Und falls Spammer doch weitere Zustellversuche unternehmen, befindet sich deren IP-Adresse dann vielleicht schon auf einer Blacklist oder die Inhaltsfilter erkennen den Spam mittlerweile. Der Nachrichtenmüll wird dann abgelehnt oder zumindest markiert.

Greylisting mit Bedacht

Wer auf seinem Mailserver Greylisting einsetzt, muss einkalkulieren, dass erneute Zustellversuche von anderen IP-Adressen der Gegenstelle aus stattfinden: Große Mailanbieter nutzen ganze Adressblöcke für den Versand, damit es beim Versenden der enormen Mengen an E-Mails keinen Engpass gibt. Ein Lösungsansatz für derartige Gegenstellen bestünde darin, große Mailprovider pauschal auf eine Whitelist zu setzen oder deren IP-Adressen mittels Abfrage des SPF-Eintrags der Absenderdomain zu ermitteln. Dazu darf die Verbindung jedoch nicht sofort temporär abgelehnt werden, der SMTP-Dialog muss bis zum MAIL FROM weiterlaufen.

Doch Vorsicht: Existiert für eine Domain ein zu laxer SPF-Eintrag, würden all diese IP-Adressen mit erfolgreichem Durchlaufen des Greylisting-Prozesses freigeschaltet werden. Im Extremfall würde eine Domain mit einem simplen „+all“ dem ganzen Internet die Maileinlieferung erlauben. Die konkreten Limits sind je nach Mailprovider sehr unterschiedlich. Gmail.com nutzt derzeit (neben IPv6 und diversen kleineren) drei /16er-Netze und kommt damit auf über 300 000 IPv4-Adressen, icloud.com erwähnt sogar vier /15er-Netze in seinem SPF-Eintrag und kommt auf über eine Million Adressen. Bei outlook.com sieht es ähnlich aus, vom /14er-Netz bis zur Einzeladresse ist hier vieles vertreten. Im Vergleich dazu wirken die wenigen Tausend Adressen bei gmx.de und web.de geradezu bescheiden, t-online.de bietet gar keine SPF-Informationen an. Auch wenn es nicht immer sinnvoll ist, dass manche Anbieter derart breit gestreute SPF-Einträge nutzen: Die Empfänger müssen darauf gefasst sein, dass ein Mailprovider die darin definierten IP-Adressen tatsächlich aktiviert.

Auch viele kleinere Mailanbieter verankern mehrere Mailserver in ihren MX-Einträgen. Dies kann sowohl den Durchsatz als auch die Zuverlässigkeit erhöhen, schließlich muss ein Server für Hard- und Softwarepflege gelegentlich heruntergefahren werden. Während solcher Auszeiten sollen andere Server einspringen können. Dieses Set-up kann jedoch dazu führen, dass der niedriger priorisierte Mailserver im Normalbetrieb nie angesprochen und somit nicht getestet wird. Im Ernstfall könnte es also sein, dass er seine Aufgabe nicht erfüllen kann.

Schlimmer noch: Es könnte passieren, dass große Mailanbieter zumindest phasenweise vor allem über den nachrangigen Server kommunizieren. Zwar sollen bei der Zustellung die Server geordnet nach fallender Priorität angesprochen werden, doch die entsprechenden Passagen im Internetstandard RFC 5321 bieten einen Implementierungsspielraum. Wer Millionen E-Mails am Tag versendet, will nicht immer wieder auf denselben Fehler stoßen. Es ist also naheliegend, den primären Server im Fehlerfall für ein paar Stunden nicht mehr anzusprechen und gleich den sekundären MX zur Zustellung zu nutzen. Die Nachrichten kommen dann weiterhin an, doch falls der Administrator aufseiten der Empfänger die höhere Last auf dem nachrangigen Server nicht bemerkt, erlebt es bei dessen nächster Wartung eventuell eine böse Überraschung und die Kunden sind dann möglicherweise nicht mehr erreichbar, obwohl der Hauptserver weiterhin läuft. Mit Testmailings und einer laufenden Systemüberwachung lassen sich solche Stolperfallen erkennen.

Wer sich in die Lage der Gegenstelle hineinversetzt, kann die hier beschriebenen Fehlerquellen generell vermeiden. Große Mailanbieter müssen teils andere Herausforderungen mit anderen Mitteln und Möglichkeiten meistern, als sie dem Administrator einer Maildomäne mit wenigen Tausenden Nutzern zur Verfügung stehen.

(un@ix.de)

Quellen

Weiterführendes zu SPF, Greylisting und SMTP findet sich unter ix.de/zkad.

Sven Krohlas

ist E-Mail-Spezialist und IT Security Consultant bei der BFK edv-consulting GmbH in Karlsruhe.