Deutschlandfunk

Spam an der Wurzel gepackt

Neues Signatursystem soll E-Mail-Müll beseitigen helfen

Jeder kennt sie, die unerwünschten Mails, die täglich eingehen und zweifelhafte Werbung bescheren oder gar Viren und andere Schädlinge einschleppen. Ein Verfahren, das die Internet Engineering Taskforce jetzt standardisiert hat, soll hier Abhilfe schaffen.

Von Achim Killer

Sie gaben den Namen, Büchsenfleisch in einem australischen Supermarkt. (Stefan Lampe)

Domainkeys Identified Mails nennt sich das Verfahren, mit dem die IETF, die Internet Engineering Taskforce gegen Mails mit gefälschten Absendern vorgehen will.

"Wir sprechen es Dikim aus. Das sagt sich leichter. Es ist ein Mechanismus, der digitale Signaturen benutzt, um nachzuweisen, dass eine Mail tatsächlich von der angegebenen Absender-Domain aus verschickt worden ist."

So Barry Leiba von der IETF. Die Domains sind ja das Problem beim Spam. Die großen Mail-Dienstleister wie T-online und AOL achten darauf, dass

über Accounts bei ihnen keine Massenwerbung verschickt wird, so dass man einigermaßen sicher sein, dass eine Mail, die über AOL versandt worden ist, kein Spam ist. Aber man kann sich halt nicht sicher sein, dass eine Mail tatsächlich über AOL versandt worden ist. Und eben deshalb setzt DKIM bei den Betreibern von Mail-Servern an:

"Wenn ‚Joe At aol Dot com' eine Mail verschickt, dann wird sie von ‚Aol Dot com' signiert und nicht von Joe."

Also der Server, der die Mail verschickt, errechnet eine Prüfsumme, verschlüsselt die mit seinem privaten Schlüssel und hängt sie an. Der Server, der die Mail empfängt, entschlüsselt die Prüfsumme mit dem öffentlichen Schlüssel des Versenders und errechnet selbst eine. Stimmen beide überein, liefert er die Mail aus. Wenn nicht, wirft er sie weg oder er liefert sie doch aus, warnt den Empfänger aber, dass sie verdächtig ist. Ein derart aufwändiges Verfahren ist notwendig, weil die Absenderadresse einer Mail sehr einfach zu fälschen ist. Jim Fenton vom Router-Hersteller Cisco, der DKIM mitinitiiert hat:

"Das ‚Simple Mail Transfer Protocol', mit dem Mails im Internet transportiert werden, erlaubt es, jede beliebige Absenderadresse zu verwenden. Und das hat auch seinen Sinn. Wenn man beispielsweise von einer Webseite einer Internet-Zeitung aus einen Artikel an einen Freund verschicken will, dann versendet eigentlich die Internet-Publikation diesen Artikel. Sie verwendet aber die Adresse dessen, der das veranlasst hat. Zweck von DKIM ist es, so etwas weiterhin zu ermöglichen, böswillige Täuschungen aber zu verhindern."

Iniitiert worden ist DKIM von Yahoo und Cisco. Mittlerweile wird es auch von IBM, Google, AOL, der Kryptographie-Firma PGP und etlichen anderen unterstützt. Und auch die ersten Implementierungen existieren schon. Dave Crocker von der MIPA, der Organisation, zu der sich diese Unternehmen zusammengeschlossen haben:

"Ja, es gibt bereits Programme und Internetdienste, die DKIM verwenden, um Mails zu signieren. Und solche, die es verwenden, um Mails zu überprüfen. Da DKIM aber erst seit kurzem ein Standard ist, ist die Liste der Unterstützer nicht allzu lang. Aber sie wird länger. Und alles deutet darauf hin, dass im Laufe des Jahres alle wichtigen Hersteller und Dienstleister mitmachen werden."

Die Technologien, die DKIM verwendet, wie die asymmetrische Verschlüsselung, seien altbekannt und -bewährt, sagt Crocker.

"Es dreht jetzt sich nur noch darum, die Unternehmen dazu zu bewegen, Software mit DKIM-Funktionalität einzusetzen. Neue Software ist immer eine Herausforderung. Die IT-Abteilungen müssen schließlich dafür gerade stehen, dass alles reibungslos läuft. Das ist in dem Fall nicht schwierig. Aber es braucht seine Zeit."

Die IETF macht sich derweil schon Gedanken für die Zeit, wenn sich DKIM einmal etabliert haben wird. Es geht dabei vor allem um die Frage, wie mit Mails zu verfahren ist, die von Domains aus verschickt werden, die sich DKIM verweigern und nicht signieren. Die wird es auf jeden Fall auch geben. Spammer zumindest setzen darauf und registrieren derzeit Domains, die so ähnlich klingen wie jene etablierter Mail- und Finanzdienstleister. Der Wettlauf zwischen IT-Sicherheitsleuten und Spammern geht also weiter. Aber mit DKIM könnten die Sicherheitsleute zumindest mal einen gehörigen Vorsprung bekommen.

[t]