Mit einem Siegel gegen Spam

Das neue Verfahren „Domain-Key Identified Mail" schützt vor unerwünschten Sendungen im elektronischen Postkörbchen

Ein neues Absendersiegel, „Domain-Key Identified Mail" oder kurz DKIM, soll uns bald einmal vor Spam-Mail schützen. Je nach Empfänger und vorgeschalteten Filtern handelt es sich heute bei bis zu 90 Prozent aller E-Mails um unerwünschte Reklame oder, noch schlimmer, um Phishing-Mails, die vorgeben, von einer Bank oder sonst einer geldbringenden Stelle zu kommen. Spams sind ärgerlich, Phishing kann viel Geld kosten, wenn man darauf hereinfällt. Grund genug, über Mechanismen nachzudenken, dergleichen sicher zu erkennen und zu unterbinden.

Wie arbeitet Spam, wie werden diese Spam-Massen heutzutage erzeugt? Seriöse Mail-Dienste fragen genau ab, wer ihnen da Mail zum Versand vorlegt. Sie lassen außerdem nur eine begrenzte Zahl von Kopien zu – was Laien bei Weihnachtsrundscheiben auffällt. Die sogenannten SMTP-Server (SMTP ist das übliche Simple Mail Transfer Protocol) verlangen Name und Passwort, bevor sie ihre Briefklappe öffnen. Leider gibt es noch genügend unseriöse Dienste, Mail-Absender lassen sich fälschen, und gelegentlich kann man sich selbst bei guten Diensten mit falschem Namen anmelden.

Massen-Spam entsteht jedoch inzwischen ganz anders, viel verdeckter: In einem ersten Schritt wird eine Anzahl von Rechnern „gekapert", die viel am Internet hängen und sich offen zeigen für heimliche Einbrüche („Sicherheitslücke"), dann werden dort rudimentäre Mail-Sendeprogramme installiert, die im entscheidenden Moment von außen mit frischen Spam-Nachrichten versehen werden und sie massenhaft aussenden, direkt, ohne weiteren Mail-Dienst. Ein Infektionsprozess. Von diesen „Bot-Netzen" (Bot assoziiert Roboter) werden somit für Spam gar nicht die herkömmlichen Mail-Versender wie GMX, T-Online oder AOL genutzt, höchstens vorgetäuscht. Die Folge: An der Quelle – ahnungslosen PCs – lassen sich solche Spams nicht schnappen.

Theoretisch könnte man jedem Internetbenutzer eine kryptographische Identität geben, eine „Signatur", dann hätte jeder einzelne Absender einen privaten und einen öffentlichen Schlüssel, mit dem der Empfänger prüfen könnte, ob eine Mail wirklich von ihm kommt. Bei besonders verschlüsselten Mails wird das gemacht. Generell wäre dafür der Aufwand groß. Jeder Einzelne müsste aktiv mitmachen. Das neue Verfahren kommt ohne Benutzerumtriebe aus. Es sichert eine Ebene höher. Bei DKIM – Domain-Key Identified Mail – wird nur die Absenderdomäne nachweisbar, nicht der einzelne Absender. In einer Adresse wie „Hugo@Maildienst.De" ist „Hugo" der Name des Einzelnen, der Person, und „Maildienst" die „Domäne", aus der er sendet. Machte man den Domänennameninhaber dafür verantwortlich, seine „Hugos" zur Ordnung zu zwingen, und hernach selbst die Mail zu signieren, so könnte man am empfangenden Ende bereits den Löwenanteil unerwünschter, gefälschter Nachrichten aussortieren. Oder: Mails von seriösen Mail-Diensten wären endlich sicher als solche erkennbar.

> Man müsste den Domänennameninhaber dafür verantwortlich machen können, seine Absender zur Ordnung zu zwingen.

Die Mechanik ist einfach: Der Mailserver des Absenders versieht die E-Mail mit einer digitalen Signatur. Der empfangende Server prüft anhand des öffentlichen Schlüssels, der im Domain Name System (DNS) der Domäne verfügbar ist, die Echtheit der Nachricht. Wo nicht, kann der empfangende Mail-Transfer-Agent (MTA) oder das empfangende Mail-Programm, ja sogar jeder Mailserver am Weg dazwischen, die E-Mail verweigern oder verwerfen. Das Verfahren stammt ursprünglich von Yahoo und ist inzwischen unter RFC 4871 standardisiert. Ein früheres, proprietäres Verfahren von Microsoft („Sender ID") nach dem Prinzip der individuellen Absenderidentifikation (Sender Policy Framework, SKF) hat sich nicht durchgesetzt. Es wurde erst 2006 – nach seinem Scheitern 2004 – vom Patentinhaber Microsoft freigegeben.

Vorreiter und Musterknabe bei DKIM sind wieder einmal Googles Gmail, das sogar SKF und DKIM aussendet, Yahoo und noch wenige andere. Man kann die DKIM-Eintragung in den Briefköpfen von Gmail-versandten Nachrichten sehen („Optionen" in Outlook), wenn die automatische Prüfung auch noch auf sich warten lässt. GMX ist sehr an DKIM interessiert, auch AOL, meist wird erst einmal abgewartet. Zu wünschen ist, dass sich bald auch die hiesigen Mail-Dienste die Mühe machen, Nachrichten per DKIM zu signieren.

Der Nachteil von DKIM ist neben einem gewissen rechentechnischen Aufwand – wie bei allen neu aufgesetzten Identifikationsverfahren –, dass der empfangende Mail-Dienst die Sache prüfen muss und (nach einer Anlaufzeit der Methode) dann auch streng mit nichtsignierten Nachrichten verfahren sollte. Spam-Versender müssten sich zum Signieren die Mühe machen, immer wieder andere Domänen zu erwerben, was schnell sichtbar würde. Der Vorteil wäre, dass Spam-Filter nicht mehr mühsam – und letztlich vergebens – den Inhalt von Mails inspizieren müssen. Denn als Bilder verkleidete Inhalte erweisen sich maschinell praktisch nicht prüfbar und bilden bereits einen Großteil von Spam. Viele Unternehmen dürfen selbst zur Spam-Prüfung Mails nicht ansehen. Wenn im Hause private Mail erlaubt ist, verbietet es der Datenschutz, sie zu öffnen. Mit DKIM wäre das gar nicht nötig. Mail ohne geprüfte DKIM-Signatur wird dann ungesehen verworfen.

FRITZ JÖRN