

Cloudmark Desktop

Das Ende von Spam-eMail ist gekommen

Das durchschnittliche eMail-Aufkommen gliedert sich in 5–10% virusverseuchte Elektropost, in 5–10% so genannte Phishing-eMails und bis zu 75–85% Spam-eMails. Würde all dies effektiv aussortiert, bliebe der Eingang des digitalen Briefkastens an so manchem Tage völlig leer.

Das Problem der virusverseuchten eMails ist mittlerweile einigermaßen lösbar – Virussoftware, die auch den Posteingang kontrolliert (z. B. Norton Antivirus und andere), entdeckt, deaktiviert und löscht die meisten böartigen eMails auf dem Einzelplatzcomputer. Der weiterhin anhaltende Versand im eMail-Zustellsystem des Internets ist damit jedoch nicht gelöst. Genauso wenig wie der enorm weiter zunehmende Versand von unverlangt zugesandter Werbe-eMails („Spam“), häufig mit pornographischen Inhalten. In der Regel werden diese eMails mit gefälschten Absender-Angaben über Rechner von Dritten verteilt. Insbesondere wechseln sowohl die Absende-, als auch die Betreff-Angaben häufig, damit sie nicht zu leicht als Spam erkannt werden können.

Grundgedanke: Anstatt Musik Spaminfos tauschen

Um Spam-eMails ebenso wie virenverseuchte ePost erkennen und aussondern zu können, wurde in den letzten Jahren viel Aufwand getrieben. Mit Methoden der künstlichen Intelligenz oder komplexesten mathematischen Algorithmen versuchte man der ständig steigenden Flut der Dreckpost zu begegnen. Unterstützung von der Industrie gab es dabei nur zögerlich, in erster Linie von den primär betroffenen Netzbetreibern und einigen Großunternehmen. Andere Unternehmen, auch aus dem Arzneimittelsektor, nutzen bis heute Spam, um zum Beispiel ihre fragwürdigen Potenzmittel weltweit, völlig risikolos und an den Verordnern vorbei auf dem grauen Pharma-Markt zu verteilen. Da auch die Spam-Versender immer intelli-

gentere Methoden entwickeln, um den immer neuen Fallen und Filtern zu entgehen, zeigte sich endlich: Nur die menschliche Einschätzung ist in der Lage, rasch und effizient Spam-eMail als solche zu erkennen. Und: Man muss nur genügend viele eMail-Nutzer in einem gegenseitigen Melde-Netzwerk zusammenbringen, um den eigenen täglichen Erkennungs-Aufwand so gering wie möglich zu halten.

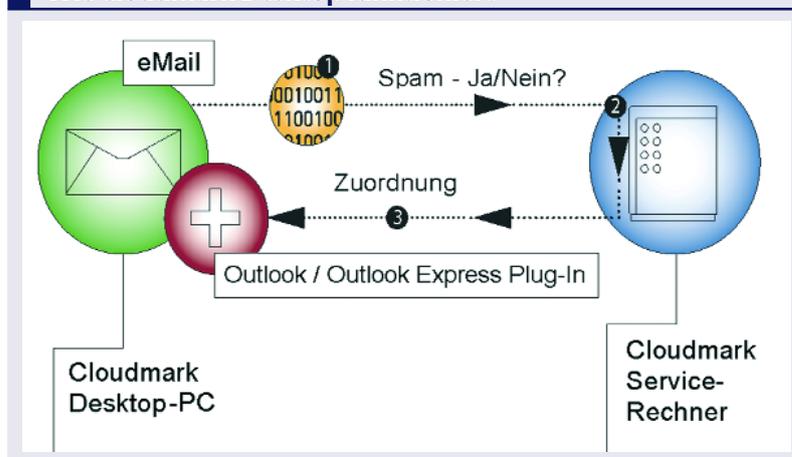
So entstand mit dem gleichen Grundgedanken der Musikaustauschbörse Napster vor rund fünf Jahren das Peer-to-Peer-Netzwerk Spam-Net, dessen Teilnehmer mit Hilfe passender Software jeder erkannten Spam-Mail eine eindeutige ID zuzuordnen und diese innerhalb des Netzes veröffentlichen konnten. Mittlerweile ist aus der ursprünglich

freien Software für Spam-Net seit 2003 ein kommerzielles, kostenpflichtiges Produkt geworden, nämlich Cloudmark Desktop.

Wie funktioniert Cloudmark Desktop/Spam-Net?

Die Software steht als Plug-In für Outlook (Microsoft Outlook 2000/XP/2003 für Exchange, POP3, IMAP, Hotmail) und Outlook Express (Version 5 und 6 für POP3, IMAP, Hotmail) zur Verfügung. Nach der in wenigen Augenblicken erfolgten Installation gibt es einen neuen eMail-Ordner namens „Spam“. Beim eMail-Abwurf bildet die Software vom Inhalt jeder eMail eine Prüfsumme und gleicht diese mit bei der Firma hinterlegten Milliarden anderer Prüfsummen ab. Wird eine Spam-Mail erkannt, kommt sie in den entsprechenden Ordner. Falsch-positive eMails im Spam- und falsch-negative eMails im Eingangsordner können im Bedarfsfall durch einfachen Tastendruck („Block“, „Unblock“) umklassifiziert werden. Diese Information wird wiederum weitergemeldet. Deutlich über 98% aller Spam-eMail wird so erkannt und aussortiert. Die Software räumt deshalb einen internationalen Software-Preis nach dem anderen ab (wobei die Preise eigentlich den 1,6

Wie Cloudmark Desktop funktioniert



1. Sobald eine eMail eintrifft, bildet Cloudmark Desktop eine einmalige kurze Prüfsumme („digitaler Fingerabdruck“), die nicht dekodierbar ist.
2. Im Internet-Netzwerk installierte Cloudmark Desktop-Datenbanken werden dann auf diesen einmaligen Fingerabdruck hin abgefragt.
3. Dabei zeigt sich, ob Spam vorliegt oder nicht. Entsprechend wird die eMail auf dem PC entweder in den Spam-Ordner oder den Eingangsordner für zulässige eMail eingeordnet.

Millionen aktiven Nutzern in 160 Ländern der Welt zustehen...).

Bei so genannten Phishing-Attacken werden eMails versandt, die so aussehen, als stammten sie tatsächlich von einer etablierten Bank, einem Händler oder einer anderen Institution. In Wirklichkeit aber stammen sie von kriminellen Betrügern, die versuchen, die Empfänger der Phishing-eMails zur Weitergabe ihrer Kreditkarten-, Bank-

oder sonstigen wichtigen Daten auf gefälschten Websites zu bewegen. Auch solche Phishing-eMails werden von Cloudmark Desktop immer dann identifiziert, wenn sie von anderen Nutzern bereits klassifiziert worden sind.

Die durchschnittliche Reaktionszeit nach dem ersten Auftauchen einer neuen Spam- oder Phishing-eMail liegt zwischen 20 Sekunden und drei Minuten. Neben der Client-

Software für den einzelnen PC und ergänzender Security-Programme auch fürs Surfen liefert Cloudmark weitere Antispam-Lösungen für große Unternehmen, eMail-Provider oder eCommerce-Anbieter.

Wer den täglichen Aufwand des Aussortierens von Spam berücksichtigt, wird die jährlich anfallende Subskriptionsgebühr von US-\$ 39,95 (oder US-\$ 3,99/Monat) gerne befragen. Über eine 15-tägige Testphase können Sie die Software kostenlos testen (<http://www.cloudmark.com/desktop/>).

Hinweis

Cloudmark Desktop ist weder eine Lösung des globalen Spam-Problems, noch dient es der Vorbeugung. Es entlastet lediglich genervte eMail-Nutzer. Der völlig überflüssige und gigantische Ressourcenverbrauch durch Spam im Internet wird in keinsten Weise verringert.

Surftipp

„Spam-E-Mails - Häufig gestellte Fragen und die dazugehörigen Antworten“ beim Bundesamt für Sicherheit in der Informationstechnik:
<http://www.bsi.bund.de/faq/spam.htm>.

Anschrift des Verfassers

Rainer H. Bubenzer (DJV, KdM)
Medizin- und Wissenschaftsjournalist
multi MED vision/presseteam volksdorf -
hamburger medizinredaktion
Theodorstraße 41, Haus R1
22761 Hamburg
Tel: 040/41912873
Fax: 040/41912877
E-Mail: Rainer@Bubenzer.com