Umfrage zur E-Mail-Verlässlichkeit

Knackpunkt Spam

Christian Dietrich, Norbert Pohlmann

E-Mail ist einer der meistgenutzten Internet-Dienste und dient der einfachen, nachrichtenbasierten und zuverlässigen Kommunikation. Eine in den vergangenen Jahren mehrmals durchgeführte Umfrage zeigt erschreckende Entwicklungen auf, gibt aber auch Anlass zur Hoffnung.

Eine vernetzte Wissens- und Informationsgesellschaft benötigt E-Mail als Basis. Seit einigen Jahren jedoch beeinträchtigt insbesondere Spam das Medium so stark, dass sich die Frage stellt, ob sich E-Mail auch in Zukunft noch genauso einfach, produktiv und vielfältig einsetzen lässt.

Um die Aussichten für die E-Mail-Nutzung detailliert einschätzen zu können, hat das Institut für Internet-Sicherheit der Fachhochschule Gelsenkirchen – unterstützt vom Bundesamt für Sicherheit in der Informationstechnik (BSI) – mehrere Erhebungen bei diversen Firmen, Organisationen sowie großen europäischen Internet-Providern durchgeführt (www.internet-sicherheit.de). Sie zeigen sowohl die aktuelle Bedrohungslage durch Spam und Viren als auch Maßnahmen zu deren Abwehr auf.

Die Untersuchung fand zu drei Zeitpunkten statt, zuerst Ende 2004. Die zweite Erhebung folgte im Sommer 2005 und die letzte Ende 2006. Die Auswertung und damit einhergehend die Interpretation der Erhebung erfolgt aus mehreren Perspektiven. Insbesondere bei der Betrachtung der Anteilsverteilung von E-Mail ist die Sichtweise entscheidend für das Verständnis der Zahlen. Aus der Perspektive eines E-Mail-System-Betreibers spielt beispielsweise der Anteil, der bereits im SMTP-Dialog abgewiesen wird, eine große Rolle (siehe Abbildung 1). Für den E-Mail-Anwender hingegen sind die Verhältnisse von erwünschter E-Mail zu Spam und Viren von Bedeutung. Daher werden im Folgenden diese beiden Sichtweisen unterschieden.

Abbild mehrerer Jahre

Die Systemsicht stellt die Anteilsverteilung des E-Mail-Volumens nach Anzahl an E-Mails im Gesamtüberblick dar und ist in der Regel für die Dienstanbieter interessant, da sie zeigt, welcher Anteil an E-Mails die Kunden erreicht und welche Anteile die E-Mail-Systeme im Rahmen der Verarbeitung eliminieren. Außerdem verdeutlicht sie, welche Anteile die einzelnen Stufen der E-Mail-Sicherheitsmechanismen erfassen.

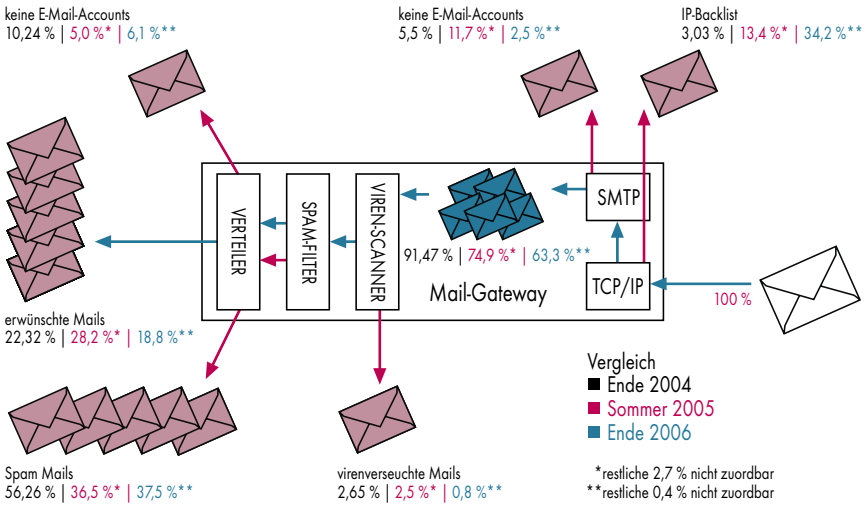
Demgegenüber hilft die Nutzersicht, die Perspektive der Anwender zu verdeutlichen. Hier tritt die Anteilsverteilung der zugestellten E-Mails in den Vordergrund.

Im Vergleich zur ersten Erhebung fällt negativ auf, dass derzeit ein geringerer Anteil an erwünschten E-Mails versandt und empfangen wird (siehe Abbildungen 1 und 2). Der Anteil erwünschter E-Mails betrug Ende 2006 aus Systemsicht nur noch rund 19 %, nachdem das Jahr 2005 vorübergehend Entspannung gebracht hatte.

Besonders vor dem Hintergrund, dass der Anteil der angenommenen E-Mails von Jahr zu Jahr deutlich gesunken ist, handelt es sich um ein betrübliches Ergebnis. Im Jahr 2004 wurden 91 % aller E-Mails angenommen, im Jahr 2005 waren es 75 % und 2006 63 %. Dadurch gelangten Ende des Jahres 2004 durchschnittlich gut 56 % Spam zu den Anwendern. Dieser Anteil verringerte sich bereits bis Mitte 2005 auf lediglich 35 %. Das setzte sich jedoch leider nicht fort, sondern der Anteil angenommener Spam-E-Mails stieg bis Ende 2006 wieder geringfügig.

Betrachtet man diesen Sachverhalt aus der Perspektive der E-Mail-Emp-

fänger und lässt alle Anteile unberücksichtigt, die sie nicht zu Gesicht bekommen, zeigt sich im Jahr 2006 ein deutlich schlechteres Verhältnis von Spam zu erwünschten Nachrichten als noch im Jahr zuvor. Während 2005 aus Nutzerperspektive „nur“ 52 % der E-Mails im Postfach als Spam klassifiziert wurden, waren es im Jahr darauf 66 %. Damit erreichte der Spam-Anteil trotz mittlerweile verbesserter Filtermethoden fast wieder das Niveau von 2004 (69 %).



Anteilsverteilung des E-Mail-Volumens aus der Perspektive des E-Mail-Systems, der sogenannten Systemsicht (Abb. 1)

Virenverseuchte E-Mails rückläufig

Immerhin ist der Anteil virenverseuchter E-Mails deutlich zurückgegangen. Im Rahmen der ersten Befragung ergab sich aus der Systemsicht ein Virenanteil von 2,65 %, zum letzten Erfassungszeitpunkt lag er bei 0,8 % aller E-Mails, die die Mailserver erreichten. Hier kann es eine Rolle spielen, dass die Mailserver im Vergleich zur Erhebung 2004 deutlich weniger E-Mails überhaupt angenommen haben.

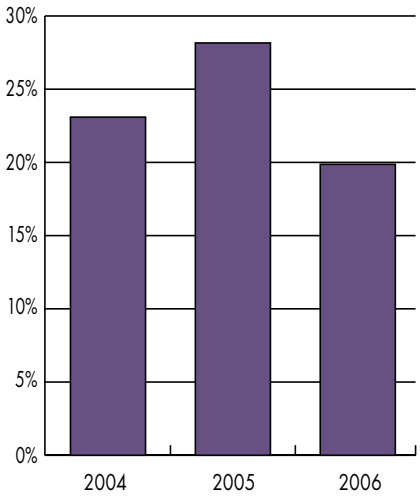
Wohl auch wegen des derzeitigen Trends zum Ablehnen von Mails schon am Server hat der Anteil von E-Mails mit nicht existierender Empfängeradresse laut neuester Zahlen auffallend deutlich abgenommen. Während er 2004 und 2005 bei 15,7 % respektive 16,7 % lag, beträgt er in der aktuellen Untersuchung nur noch 8,6 %.

Nicht nur basierend auf Mailadressen, sondern auch aufgrund von IP-Adressmerkmalen lässt sich Spam effizient abwehren. Diejenigen Befragten, die anhand von Merkmalen der IP-Schicht blockieren, lehnen auf diese Art bis zu über 90 % aller Zustellversuche ab. Lediglich rund 44 % der Befragten nutzen dazu IP-Blacklists. Im Vergleich zum Vorjahr hat sich dieser Anteil nicht wesentlich verändert. 2005 haben rund 45 % der Befragten IP-Blacklisting angewendet – immerhin deutlich mehr als der Verbreitungsgrad von 30 % im Jahr 2004. Damit hat sich der Anteil blockierter E-Mails aus der Systemsicht auf 34 % erhöht.

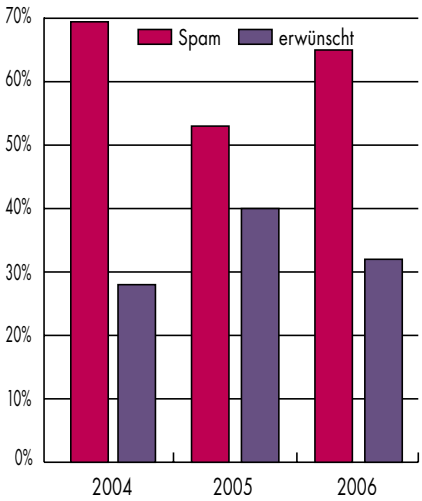
Darüber hinaus zeigt sich, dass sich der Spam-Schutz im Vergleich der Ergebnisse insgesamt deutlich vielfältigerer Mechanismen bedient. Greylisting etwa setzen schon 26 % der Befragten ein, im Jahr 2005 waren es lediglich 10 %. Am häufigsten kommen Zeichenketten-Analysen des E-Mail-Inhalts wie der Bayes-Filter zum Einsatz. Über 65 % der Befragten setzen derartige Verfahren in ihren Anti-Spam-Lösungen ein.

Spam-Abwehr verlagert sich nach vorne

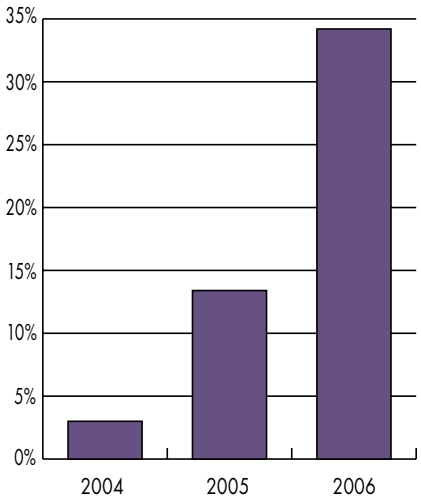
Auffallend deutlich zugenommen hat der Anteil der Befragten, die nicht zustellbare E-Mails während des SMTP-Dialogs ablehnen. Belief sich dieser Anteil im Jahr 2005 auf 29 %, so hat er sich im Laufe eines Jahres um rund 15 Prozentpunkte auf über 43 % erhöht. Demgegenüber unerwartet zeigt



Spammer halten Schritt: Anteil erwünschter E-Mails aus Systemsicht (Abb. 2)



Anteil erwünschter und Spam-Nachrichten aus der Nutzerperspektive (Abb. 3)



Anteil der E-Mails, die anhand der Client-IP-Adressen blockiert werden (Abb. 4)

sich jedoch, dass die Nicht-Annahme von E-Mails, die von Dialup-IP-Adressen eingeliefert werden, in der Verbreitung geringfügig abgenommen hat. Insbesondere zur Abwehr von Spam-Nachrichten, die über Bot-Netze ausgehen, hat sich das Blockieren von direkt zugestellten Mails von Hosts mit Dialup-IP-Adressen als recht wirksam herausgestellt.

Fazit

Zwischen der ersten Erhebung Ende 2004 und derjenigen im Sommer 2005 hatte sich die Lage vorübergehend deutlich entspannt, doch liegt der Spam-Anteil derzeit wieder auf einem ähnlich hohen Niveau wie zum Ausgangszeitpunkt. Ende 2006 bestanden aus Anwendersicht etwa zwei Drittel der E-Mails aus Spam. Unter Einbeziehung der E-Mails, die die Mailsysteme bereits während des Transports aussortieren, ergibt sich sogar ein Spam-Anteil von über 80 Prozent.

Positiv zu werten ist eine deutliche Verringerung des Anteils virenbehafteter E-Mails. Seit der ersten Untersuchung im Jahr 2004 reduzierte sich dieser Anteil konstant auf mittlerweile lediglich 1,3 % aus Sicht der E-Mail-Anwender, vorausgesetzt, sie bekommen erkannte Viren überhaupt (entsprechend markiert) zugestellt. Aus Sicht der Systembetreiber enthalten lediglich 0,8 % aller angenommenen E-Mails Viren.

Optimistisch stimmt ebenso die Tatsache, dass immer mehr E-Mails spätestens während des SMTP-Dialogs blockiert werden – in der aktuellen Untersuchung im Durchschnitt bereits mehr als ein Drittel. Einzelne Teilnehmer erreichen mit dieser Methode eine Filterung von mehr als 90 % aller E-Mails.

Der Anteil an aufgrund von nicht existierenden Empfänger-E-Mail-Adressen nicht zustellbaren E-Mails ist deutlich gesunken. Während bei den ersten beiden Untersuchungen rund 16 % nicht zustellbar waren, beträgt dieser Anteil in der aktuellen Erhebung lediglich 8,6 %.

Der gestiegene Spam-Anteil verdeutlicht jedoch auf alarmierende Weise, dass der Kampf gegen Spam bei Weitem nicht entschieden ist. Die Untersuchungen zeigen, dass Mechanismen existieren, mithilfe derer Spam reduziert werden kann. Dazu gehört in erster Linie IP-Blacklisting, unterstützt durch IP-Adress-basierte Reputationssysteme. (un)

CHRISTIAN DIETRICH

ist Mitarbeiter des Instituts für Internet-Sicherheit an der FH Gelsenkirchen und für den Forschungsbereich E-Mail-Sicherheit verantwortlich.

PROF. DR. NORBERT POHLMANN

ist Informatikprofessor für verteilte Systeme und Informationssicherheit sowie Leiter des Instituts für Internet-Sicherheit an der FH Gelsenkirchen.