

Spam auf dem Rückmarsch?

Auswertung der 2. Umfrage zur E-Mail-Verlässlichkeit, Sommer 2005

Stand: September 2005

Autoren **Christian Dietrich**
dietrich@internet-sicherheit.de

Prof. Dr. Norbert Pohlmann
norbert.pohlmann@informatik.fh-gelsenkirchen.de

Institut für Internet-Sicherheit
Fachhochschule Gelsenkirchen
Fachbereich Informatik
Neidenburgerstr. 43
45877 Gelsenkirchen



Web www.internet-sicherheit.de

1. Einleitung

Der E-Mail Dienst ist einer der am weitesten verbreiteten und meist genutzten Dienste des Internets und wird heutzutage als Mittel zur einfachen, nachrichtenbasierten und zuverlässigen Kommunikation im Internet eingesetzt. Er ist inzwischen für unsere vernetzte Wissens- und Informationsgesellschaft eine nicht mehr wegzudenkende Anwendung.

Seit einigen Jahren jedoch beeinträchtigt insbesondere Spam das Medium E-Mail derart stark, dass die Frage zu stellen ist, ob E-Mail auch in Zukunft noch genauso einfach, unkonventionell, produktiv und vielfältig eingesetzt werden kann.

Um letztlich das Gefahrenpotential für die E-Mail Nutzung detaillierter einschätzen zu können, hat das Institut für Internet-Sicherheit der Fachhochschule Gelsenkirchen unterstützt durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) eine Erhebung bei diversen Firmen, Organisationen sowie bei großen europäischen Internet Service Providern durchgeführt, die sowohl die aktuelle Bedrohungslage durch Spam und Viren als auch Maßnahmen zu deren Gefahrenabwehr analysiert (vgl. [DiPo05]).

2. Die Erhebungen

Die erste Untersuchung Ende des Jahres 2004 ist repräsentativ für über 40 Mio. E-Mail-Accounts und ein durchschnittliches monatliches E-Mail-Volumen von mehr als 2,3 Mrd. E-Mails.

Um Trends und Entwicklungen erkennen zu können, wurde die Erhebung zwischen Juni und August 2005 mit einigen ausgewählten Teilnehmern unter Verwendung von aktuellen Zahlen wiederholt. Im Rahmen dieser zweiten Erhebung wurde ein E-Mail-Volumen von 1 Mrd. E-Mails pro Monat und 18,5 Mio. E-Mail-Accounts berücksichtigt.

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-Nutzer hingegen sind die Verhältnisse von erwünschter E-Mail zu Spam und Viren von Bedeutung (siehe Abbildung 2). Aus diesem Grund werden im Folgenden diese beiden Sichtweisen unterschieden.

Generalisierte Sichtweise – Vergleich → Ergebnisse: System, Eingang

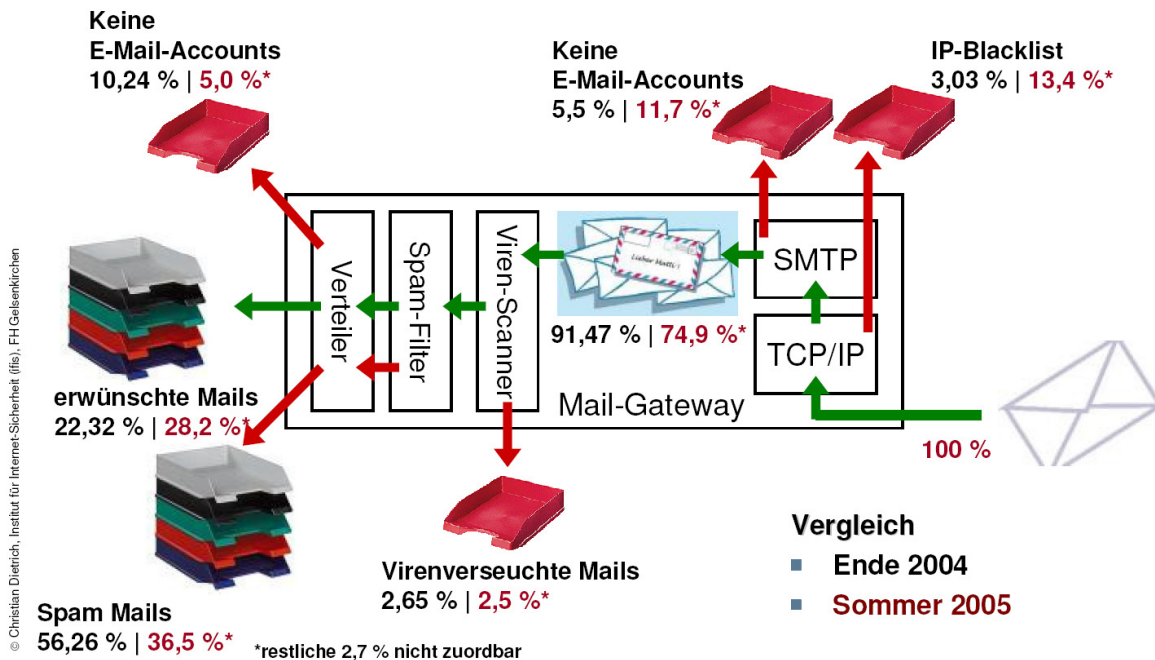


Abbildung 1: Anteilsverteilung des E-Mail-Volumens aus Perspektive des E-Mail-Systems, sog. Systemsicht

3. Trends und Entwicklungen

Im Vergleich zur ersten Erhebung fällt sehr positiv auf, dass aktuell ein höherer Anteil an erwünschten E-Mails versandt und empfangen wird (siehe Abbildung 1). Statt 22,3% beträgt der Anteil an erwünschten E-Mails Mitte 2005 mehr als 28%. Dies ist im Wesentlichen auf 2 Entwicklungen zurückzuführen. Zum einen verdeutlicht die Statistik, dass der Anteil an angenommenen Spam-Nachrichten in jüngster Zeit abgenommen hat. Erhalten E-Mail-Nutzer Ende des Jahres 2004 durchschnittlich 69,3% Spam, so verringerte sich dieser Anteil bis Mitte 2005 auf lediglich 52,3% (vgl. Abbildung 2). Dieser Trend lässt sich auch durch andere Untersuchungen bestätigen. Das E-Mail-Sicherheitsunternehmen MessageLabs beispielsweise datiert den Zenith des Spam-Versands auf den Monat Juli 2004. Seit Anfang 2005 zeigt sich, dass das Verhältnis von Spam zu erwünschter elektronischer Post stetig abnimmt (vgl. [MeLI05]).

Zum anderen lässt sich ein leichter Rückgang des Virenvolumens verzeichnen. Im Rahmen der ersten Befragung konnte aus der Systemsicht ein Virenanteil von 2,65% ermittelt werden, zum aktuellen Zeitpunkt beträgt er nunmehr im Durchschnitt 2,5% aller E-Mails, die den E-Mail-Server erreichen. Aufgrund der Tatsache, dass im Vergleich zur Erhebung Ende 2004 durchschnittlich deutlich weniger E-Mails vom E-Mail-Server angenommen werden (91,47% bzw. 74,9%; vgl. Abbildung 1), wirkt sich dieser Rückgang jedoch nicht auf die Nutzerperspektive aus. Lediglich ein Anteil von nur noch dreiviertel aller E-Mails werden heutzutage von E-Mail-Servern entgegengenommen. Aus der Sicht eines E-Mail-Nutzers liegt das Virenvolumen dadurch derzeit mit 3,5% geringfügig über dem Wert der ersten Erhebung (3,3 %).

Generalisierte Sichtweise – Vergleich → Ergebnisse: Nutzerperspektive

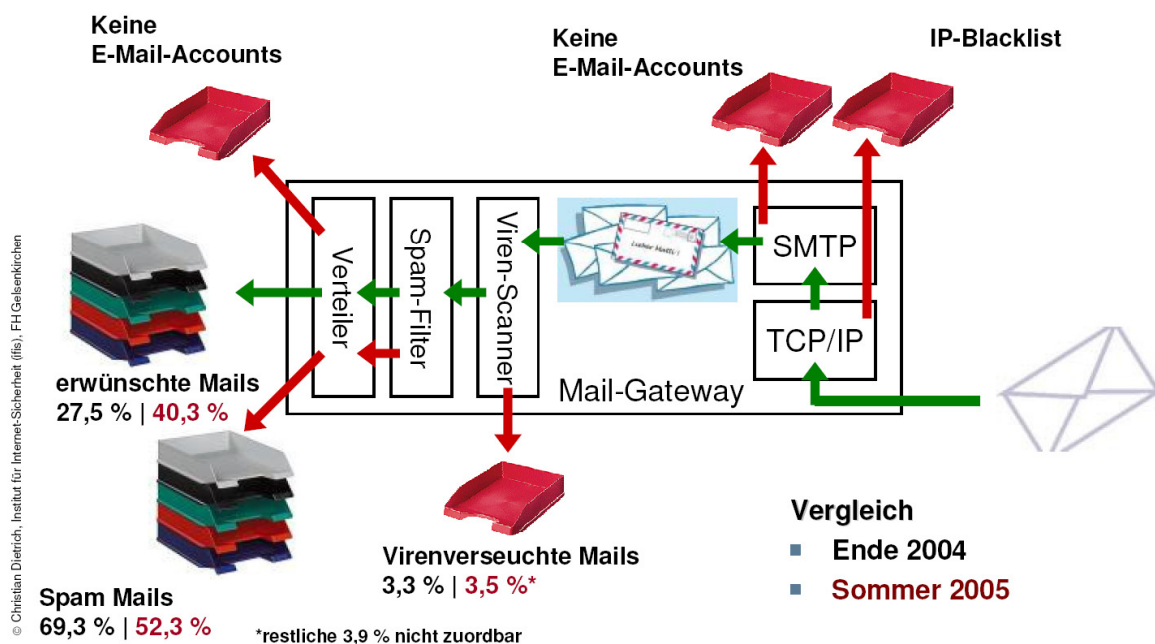


Abbildung 2: Anteilsverteilung des E-Mail-Volumens aus Perspektive des E-Mail-Benutzers

4. Spam-Abwehr

Der Anteil an E-Mails mit nicht-existierender Empfänger-Email-Adresse hat sich insgesamt nicht auffällig verändert. Er liegt derzeit bei 16,7% (5% + 11,7%). Im Rahmen der ersten Erhebung betrug dieser Anteil 15,7% (10,2 % + 5,5%). Die Überprüfung der Zustellbarkeit einer E-Mail kann zu zwei verschiedenen Zeitpunkten während der Verarbeitung durch einen empfangenden E-Mail-Server erfolgen (siehe Abbildung 1). Zum einen kann ein MTA eine E-Mail vollständig akzeptieren und daraufhin überprüfen, ob ein entsprechendes Postfach zu der angegebenen Empfänger-Adresse existiert. Ist dies nicht der Fall, so generiert der E-Mail-Server eine Informationsnachricht über die fehlgeschlagene Zustellung, eine sog. Non Delivery Notification. Dieses Verfahren war historisch bedingt durch den sog. Store-and-forward-Mechanismus bei E-Mail sehr weit verbreitet. Zum anderen kann bereits während des SMTP-Dialogs die Zustellung abgebrochen werden, falls kein Ziel-Postfach zugeordnet werden kann. Die letztere Methode ist ressourcenschonender als die erstere, da in diesem Fall die E-Mail gar nicht erst übertragen wird und somit Kosten für Bandbreite, Speicherplatz etc. eingespart werden.

Es zeigt sich, dass heutzutage den E-Mails mit nicht-existierender Empfänger-Adresse in höherem Maße bereits im SMTP-Dialog die Annahme verweigert wird. Ca. 35% aller E-Mails mit nicht-existierender Empfänger-E-Mail-Adresse wurden zum ersten Erhebungszeitpunkt bereits im SMTP-Dialog abgewiesen. Mittlerweile hat sich der Anteil auf 70% erhöht.

Nicht nur basierend auf SMTP-Adressinformationen, sondern auch aufgrund von IP-Adressmerkmalen kann die Spam-Abwehr effizient ermöglicht werden. Unter einer Blacklist wird eine Liste negativ aufgefallener (IP-)Adressen in Bezug auf die E-Mail-Nutzung verstanden. Ebenso können in einer Blacklist Adressen von Rechnern, die nicht für die direkte E-Mail-Einlieferung vorgesehen sind – wie beispielsweise dynamische IP-Adressen – aufgeführt werden. Eine Blacklist entscheidet damit nicht zwangsläufig über Zulassung oder Ablehnung einer Verbindung. Die Entscheidung, ob eine Kommunikation aufgrund eines Eintrags einer entfernten Partei in einer Blacklist abgebrochen wird, liegt weiterhin beim Empfänger und muss durch eine eigene Policy auf der Empfängerseite bestimmt werden. Der Eintrag eines Adressdatums in einer Blacklist kann – wenn ein Missbrauch des eigenen E-Mail-Dienstes durch Spam verhindert werden soll – als Indiz gegen eine Verbindung gewertet werden.

Diejenigen Befragten, die anhand von Merkmalen der IP-Schicht blockieren, lehnen auf diese Art im Durchschnitt 28,5% der

gesamten Anzahl an monatlichen E-Mails ab. Jedoch wenden lediglich ca. 45% der Befragten IP-basierte Blacklists an. Dies ist immerhin deutlich mehr als der Verbreitungsgrad von 30% bei der vorhergehenden Befragung. Damit hat sich dieser Anteil aus der Systemsicht sehr positiv auf 13,4 % erhöht, was sich für den Nutzer durch einen sehr viel höheren Anteil von erwünschten Mails auswirkt.

5. Fazit

Seit der ersten Erhebung Ende 2004 hat sich der Anteil an erwünschten E-Mails vergrößert. Die beiden wichtigsten Gründe hierfür sind eine erhebliche Verminderung an angenommenen Spam-Mails sowie ein leichter Rückgang des Viren-Volumens.

Darüber hinaus werden mehr E-Mails bereits im Dialog durch IP-Blacklisting und Überprüfung nicht-existierender Empfänger-Adressen abgelehnt. Dieser Trend ist zu begrüßen und sollte fortgeführt werden.

6. Literatur

- [DiPo05] C. Dietrich, N. Pohlmann: E-Mail-Verlässlichkeit: Auswertung der Umfrage Ende 2004, 2005, <http://www.internet-sicherheit.de/center-berichte.html>
- [MeLI05] MessageLabs Intelligence: ‚MessageLabs Intelligence: July 2005‘, Juli 2005, <http://www.messagelabs.com>