

E-Mail-Verlässlichkeit: Auswertung der Umfrage Ende 2004

Christian Dietrich · Prof. Dr. Norbert Pohlmann



Institut für Internet-Sicherheit
Fachhochschule Gelsenkirchen
Fachbereich Informatik

Neidenburger Str. 43, D 45877 Gelsenkirchen

christian.dietrich@informatik.fh-gelsenkirchen.de

norbert.pohlmann@informatik.fh-gelsenkirchen.de

Zusammenfassung

Der E-Mail Dienst ist einer der am weitesten verbreiteten und meist genutzten Dienste des Internets. Obwohl E-Mail zunächst nicht als verlässlicher Dienst konzipiert wurde, wird es heutzutage häufig als Mittel zur einfachen, nachrichtenbasierten und zuverlässigen Kommunikation im Internet eingesetzt. Der E-Mail Dienst ist für die Informationstechnologie inzwischen eine nicht mehr wegzudenkende Anwendung.

Seit einigen Jahren jedoch beeinträchtigen insbesondere Spam und Viren, aber auch andere Bedrohungen (z.B. fehlende Geheimhaltung) das Medium E-Mail derart, dass fraglich ist, ob E-Mail in der Zukunft noch genauso einfach, unkonventionell und produktiv eingesetzt werden kann.

Um letztlich das Gefahrenpotential für die E-Mail Nutzung konkret einschätzen zu können, hat das Institut für Internet-Sicherheit der FH Gelsenkirchen eine Umfrage bei diversen Organisationen durchgeführt, die sowohl die aktuelle Bedrohungslage durch Spam und Viren als auch Maßnahmen zur Gefahrenabwehr erhebt. Mit Hilfe einer Fragebogenaktion wurde zunächst geklärt, welche Art von Informationen – mit welcher Bedeutung für die Kommunikationspartner – per E-Mail im Internet ausgetauscht werden. Des Weiteren wurde in Erfahrung gebracht, ob und inwieweit E-Mail-Kommunikation möglicherweise bereits eingeschränkt ist und welche Mechanismen sich in der Praxis bisher als wirkungsvoll und zuverlässig erwiesen haben.

Diese Umfrage des Instituts für Internet-Sicherheit der FH Gelsenkirchen – unterstützt durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) – bildet daher die Basis für eine Evaluierung von Mechanismen zur Etablierung von E-Mail-Verlässlichkeit, insbesondere von Anti-Spam-Maßnahmen. Hierbei gilt es, u.a. die zahlreichen und zumeist komplizierten Möglichkeiten der Spam-Abwehr auf ihre Praxistauglichkeit hin zu überprüfen.

Die Umfrage wird demnächst mehrfach wiederholt, um mögliche Trends und Veränderungen zu erkennen. Der nächste Umfrage-Lauf ist für den Frühsommer 2005 geplant.

1 Idee und Umsetzung

Das Medium E-Mail als Teilkomponente des Internet, das wiederum als offenes Kommunikationssystem realisiert ist, ermöglicht einen einfachen unkomplizierten Nachrichtenaustausch, da in der technischen Konzeption grundsätzlich keinerlei Beschränkungen der Möglichkeit der E-Mail-Kommunikation zwischen beliebigen E-Mail-Teilnehmern weltweit existiert. Dies bedeutet, jeder Teilnehmer kann jedem anderen Teilnehmer im Netz E-Mail Nachrichten senden, sofern die E-Mail-Adresse des Empfängers bekannt ist. Diese technisch mögliche „grenzenlose“ Freiheit nutzen allerdings auch Spammer, um in überaus großen Mengen E-Mails – überwiegend zu Werbezwecken – an beliebige Empfänger zu übersenden. Aktuelle Zahlen von Antispam-Dienstleistern (vgl. [Clea04] sowie [Mess04]) belegen, dass unerwünschte Spam-Nachrichten zwischen 60% und 90% des gesamten weltweiten E-Mail-Verkehrs ausmachen können. Dies führt beim Empfänger zu einem erheblichen Arbeitsaufwand, um aus der Fülle der übersandten E-Mails diejenigen Nachrichten zu extrahieren, die für ihn gleichwohl relevant sind. Ohne weitere technische Hilfsmittel kann man sich als Empfänger dieser unerwünschten Nachrichten grundsätzlich nicht erwehren.

Im Laufe der Zeit wurden diverse Alternativen zur Abwehr der Spam-Flut mit unterschiedlichen Ansatzpunkten entwickelt. Im Rahmen der Auswertung der Umfrageergebnisse werden die zurzeit verfügbaren, unterschiedlichen Mechanismen auf ihre Validität und Effektivität hin bewertet.

Aber nicht nur für den Empfänger, sondern auch für die Service Provider bedeutet die Verhinderung von Spam eine enorme Kosteneinsparung. So muss insbesondere von den Anbietern ein erheblicher Teil ihrer Ressourcen darauf verwendet werden, unerwünschte Nachrichten, die der Empfänger als wert-, nutz- und sinnlos erachtet, in Massen zu transportieren. Die Umfrageergebnisse zeigen, dass dies durch den gezielten Einsatz einzelner Maßnahmen zwar nicht ganz unterbunden, allerdings deutlich reduziert werden kann.

Neben der Spam-Problematik ergeben sich darüber hinaus insbesondere dadurch Probleme, dass der E-Mail-Dienst gängige Forderungen der IT-Sicherheit im Regelfall nicht erfüllt. E-Mail basiert auf den Protokollen SMTP und POP3 sowie IMAP. Diese Protokolle bieten von sich aus keinerlei bzw. nur unzureichende Sicherheitsmechanismen, mit Hilfe derer Vertraulichkeit und Integrität der Nachrichtenübermittlung realisierbar sind. Doch genau diese Aspekte sind grundlegend für eine verlässliche, sichere Anwendung des E-Mail-Dienstes. Ohne einen sicheren E-Mail-Dienst ist der Einsatz von E-Mail z.B. in elektronischen Geschäftsprozessen nahezu unmöglich, da beispielsweise im Falle von Vertragsabschlüssen per E-Mail zum Schutz aller Parteien ein vertraulicher und integrier Kommunikationskanal unabdingbare Voraussetzung ist.

Auch hierfür existieren mit E-Mail-Verschlüsselung und PKI mittlerweile Möglichkeiten, die vorgenannten Anforderungen zu etablieren. Im Rahmen der Ergebnisse der Untersuchung sollte beleuchtet werden, in wie weit diese zusätzlichen potentiellen Sicherheitsmechanismen heute bereits in der Praxis eingesetzt werden und welche Wirkung sie in der Realität zeigen.

2 Definition: Spam

Unter dem Begriff Spam wird im Folgenden das Phänomen verstanden, dass ein Urheber (sog. Spammer) in großen Mengen unerwünschte und unverlangte E-Mails an eine Vielzahl beliebiger Empfänger – meist zu Werbezwecken – versendet. Darüber hinaus bezeichnet man auch die Menge aller Spam-Nachrichten als Spam. Die Bezeichnung Spam-Nachricht beschreibt eine unerwünschte E-Mail-Nachricht im Massenversand. „Unerwünscht“ bedeutet in diesem Zusammenhang, dass der Empfänger keine Zustimmung zum Empfang einer solchen Nachricht erteilt hat. Für die Definition des Begriffes Spam im Rahmen dieser Untersuchung ist es unerheblich, ob die E-Mail legal oder unter Verstoß gegen geltendes Recht übersendet wurde.

Die Bezeichnung „unerwünscht“ ist dabei individuell abhängig vom Empfänger. Eine spezielle Spam-Nachricht kann für Empfänger A unerwünscht sein, für Empfänger B jedoch eventuell eine „wünschenswerte“ Information darstellen. Dieser Umstand macht es zusätzlich schwierig, Spam durch einen Automatismus zu bekämpfen. Eine weitergehende Unterteilung von Spam – wie im amerikanischen Raum üblich – in Unsolicited Bulk Email (UBE) oder Unsolicited Commercial Email (UCE) findet in diesem Rahmen nicht statt.

Es gilt darüber hinaus zu beachten, dass das Phänomen Spam in gewissen Szenarien nicht exakt abgrenzbar ist. Dies zeigt sich insbesondere dann, wenn Spam-Nachrichten einen oder mehrere Viren enthalten. In diesem Fall hängt die Zuordnung meist von der Anordnung der E-Mail-Sicherheitsmechanismen ab. Befindet sich beispielsweise der Virens Scanner vor dem Spam-Filter, so wird eine virenbehaftete E-Mail bereits im Virens Scanner als Virus-Nachricht erkannt und von den anschließenden Spam-Überprüfungen ausgeschlossen.

3 Ergebnisse der Umfrage

Im ersten Lauf der Umfrage vom 17.11.2004 bis zum 07.01.2005 haben 148 Organisationen teilgenommen. Hiervon haben 116 Organisationen den Fragebogen überwiegend beantwortet. Lediglich 32 teilnehmende Organisationen registrierten sich zwar, füllten jedoch den Fragebogen nicht aus. Die am häufigsten genannten Gründe hierfür waren eine Verletzung ihrer IT-Security-Policy oder die Tatsache, dass die Ermittlung der Antworten nicht möglich war – beispielsweise aufgrund von Outsourcing.

Die Umfrage ist repräsentativ für rund 40 Mio. E-Mail-Accounts und ein monatliches Gesamt-E-Mail-Volumen von 2,3 Mrd. E-Mails. Bei einer Annahme von 30 Mrd. E-Mails pro Tag entspricht dies ca. 1/400 des gesamten weltweiten E-Mail Aufkommens.

Die hohe Bedeutung von E-Mail für den Bereich des eCommerce schlägt sich in den Umfrageergebnissen deutlich darin nieder, dass über 46% aller teilnehmenden Organisationen E-Mail für elektronische Geschäftsprozesse verwenden. Betrachtet man die Antworten differenziert nach den Rechtsformen der Teilnehmer, fällt auf, dass Aktiengesellschaften mit 63% das relative Maximum nach Rechtsformen darstellen (vgl. Tabelle 1).

Tabelle 1: Einsatz von E-Mail in elektronischen Geschäftsprozessen, aufgeschlüsselt nach Rechtsformen¹

Rechtsform	ja
Aktiengesellschaften	63,6%
Behörden	28,1%
Gesellschaften mit beschränkter Haftung	61,5%
Service Provider	66,7%
diverse	53,8%

Durch diese Zahlen stehen zwei Dinge fest: E-Mail ist bereits heute eine wichtige – wenn nicht die wichtigste – Infrastruktur für den elektronischen Handel. Ein etwaiger Ausfall des E-Mail-Dienstes ist von den Teilnehmern im Mittel maximal zwischen 30 und 60 Minuten tolerierbar. Hierbei zeigen sich jedoch erhebliche Unterschiede. So geben Service Provider eine tolerable Ausfallzeit mit 0 an; umso mehr verwundert im Vergleich dazu, dass AGs (ohne ISPs) bei der Frage nach der Ausfallzeit gleichwohl eine höhere Toleranz zeigen als beispielsweise GmbHs. Die mittlere tolerable Ausfallzeit liegt für AGs bei 12 Stunden, für GmbHs bei 3-4 Stunden.

3.1 Viren-Rate

Anhand der von den Organisationen zur Verfügung gestellten Zahlen des monatlichen Viren-Volumens konnte eine durchschnittliche Viren-Rate von 2,9% ermittelt werden. Vergleichswerte von spezialisierten Anbietern, wie beispielsweise MessageLabs zeigen einen deutlich höheren Virenanteil der E-Mails (vgl. [Mess04]). Das Gefälle unter den Teilnehmern mit jeweils verschiedenen Rechtsformen ist groß. Einzelne Hochschulen, Behörden und GmbHs fallen durch relativ hohe Viren-Raten zwischen 6% und 10% auf, während Service Provider im Durchschnitt lediglich unter 2% virenbehaftete E-Mails feststellen.

Der Anteil virenbehafteter E-Mails im Internet unterliegt – wie in der Untersuchung festgestellt wurde – ständigen Schwankungen. So ließ sich beispielsweise für die Monate April und Mai 2004 ein überdurchschnittlich hohes Viren-Aufkommen feststellen. Dies deutet auf eine sehr unterschiedliche Verteilung der Bedrohung hin, die wir jedoch nicht mit den erfassten Daten aufschlüsseln konnten.

3.2 Spam-Rate

Die Spam-Rate, also der Anteil Spam-Nachrichten am Gesamtaufkommen beträgt im Durchschnitt 61,5% aller E-Mails. Auch hier lassen sich je nach Aufschlüsselung große Unterschiede feststellen (siehe Tabelle 2).

¹ Service Provider sind bei der Auswertung in eine eigene Kategorie ausgekoppelt, da sie meist auf den E-Mail-Dienst und in diesem Rahmen auch auf Spam- und Virenbekämpfung spezialisiert sind. Die Werte der einzelnen Kategorien lassen sich auf diese Art besser vergleichen.

Tabelle 2: Spam-Anteil, aufgeschlüsselt nach Rechtsformen

Rechtsform	Spam-Rate
Aktiengesellschaften	69,9%
Behörden	20,4%
Gesellschaften mit beschränkter Haftung	64,0%
Service Provider	46,9%
diverse	42,1%

Die beiden Extrema bilden zum einen die Aktiengesellschaften mit knapp 70% und zum anderen die Behörden mit lediglich 20,4% Spam-Nachrichtenanteil. Insbesondere Einzelunternehmen (in der Tabelle dargestellt unter „diverse“) sind einem hohen Spam-Aufkommen ausgesetzt. Eine mögliche Erklärung hierfür könnte darin begründet liegen, dass kleine Unternehmen zumeist viele E-Mail-Adressen auf ihren Webseiten abrufbar vorhalten, die gerade von Harvestern – also automatischen Sammelrobotern der Spammer – gesammelt und für den Spam-Versand genutzt werden. Große Unternehmen veröffentlichen oft nur eine Kontakt-Adresse der Art info@... oder contact@... . Diese bieten also weniger Angriffspunkte.

Eine wichtige Rolle für den Empfang von Spam spielt der Umgang mit E-Mail-Adressen. Generell gibt es neben Harvestern noch weitere Möglichkeiten, um an E-Mail-Adressen zu gelangen. Eine beliebte aktive Methode der Spammer, die als Directory Harvest Attack bezeichnet wird, nutzt die Tatsache, dass 62,2% der Befragten E-Mails mit nicht existierenden Empfänger-E-Mail-Adressen bereits im SMTP-Dialog ablehnen. Die Attacke besteht darin, Kombinationen von häufigen Vor- und Nachnamen zu bilden und diese als Empfänger-E-Mail-Adressen für Spam auszuprobieren. Schlägt die Zustellung einer E-Mail mit der Begründung, dass zu dieser Adresse kein Postfach existiert fehl, so kann der Spammer nicht existierende Adressen von existierenden abgrenzen. Gegen eine solche Attacke hilft oft nur eine Reglementierung der Zustellversuche, denn der Spammer muss eine große Anzahl von Zustellversuchen unternehmen, damit Directory Harvest Attacken für ihn lohnenswert sind.

Des Weiteren sollten E-Mail-Adressen nach Möglichkeit nur in Fällen, in denen es notwendig ist und selbst dann nur bei Online-Angeboten angegeben werden, die eine Geheimhaltung und Nutzung der E-Mail-Adresse im vereinbarten Rahmen – beispielsweise durch die AGBs – garantieren. Feldversuche zeigen, dass Spammer gerne und häufig von E-Mail-Adressen Gebrauch machen, die im Rahmen von Online-Angeboten ohne eine solche Zusicherung gewonnen wurden.

Eine sehr unscheinbare Möglichkeit an E-Mail-Adressen zu gelangen, besteht darin, auf einer Webseite ein Element einzubinden, welches nicht per HTTP sondern per Anonymous-FTP vom Browser geladen werden muss. Viele WWW-Browser unterstützen auch das Dateiübertragungsprotokoll FTP und laden das Element automatisch ohne Interaktion mit dem Benutzer. Allerdings hat es sich eingebürgert, dass in der Login-Prozedur beim anonymen FTP als Passwort die E-Mail-Adresse angegeben wird. Einige Browser geben hier – falls bekannt – die aktuelle E-Mail-Adresse des Benutzers preis. Für eine ausführliche Liste der Möglichkeiten, E-Mail-Adressen zu sammeln, sei auf [RazHVS] verwiesen.

Gruppiert man die Ergebnisse der Spam-Rate nach Branchen, so zeigt sich, dass gerade Finanzdienstleister unter sehr hohem Spam-Aufkommen (86,1%) leiden.

Tabelle 3: Spam-Anteil, aufgeschlüsselt nach Branchen

Spam-Rate (nach Branchen)	Spam-Rate
Bildungsinstitution	49,0%
Dienstleistungen	2,9%
Finanzdienstleistungen	86,1%
Industrie	46,0%
Informationstechnologie	68,0%
Öffentlicher Dienst	23,7%
Service Provider	61,1%
SUMME	61,5%

Bei der Betrachtung des relativen Spam-Anteils muss berücksichtigt werden, dass bei der Erfassung von Spam der Anteil, welcher bereits durch eine Blockierung auf TCP/IP-Ebene (z.B. Realtime Blackhole Lists) sowie im SMTP-Verbindungsaufbau (z.B. durch eine falsche HELO-Angabe) abgewehrt wird, nicht in die Spam-Rate einfließen kann. Generell gilt, dass auf IP-Ebene lediglich versuchte Verbindungsaufbauten aber keine Anzahl an Spam-Nachrichten gemessen werden können. Die o.g. durchschnittliche Spam-Rate von 61,5% bezieht sich daher ausschließlich auf die Bereiche, in denen E-Mails tatsächlich zahlenmäßig erfasst werden können. Dies wird nachfolgend in Abbildung 1 dargestellt.

Der „reale“ Anteil an Spam im Internet ist daher noch deutlich höher anzusetzen.

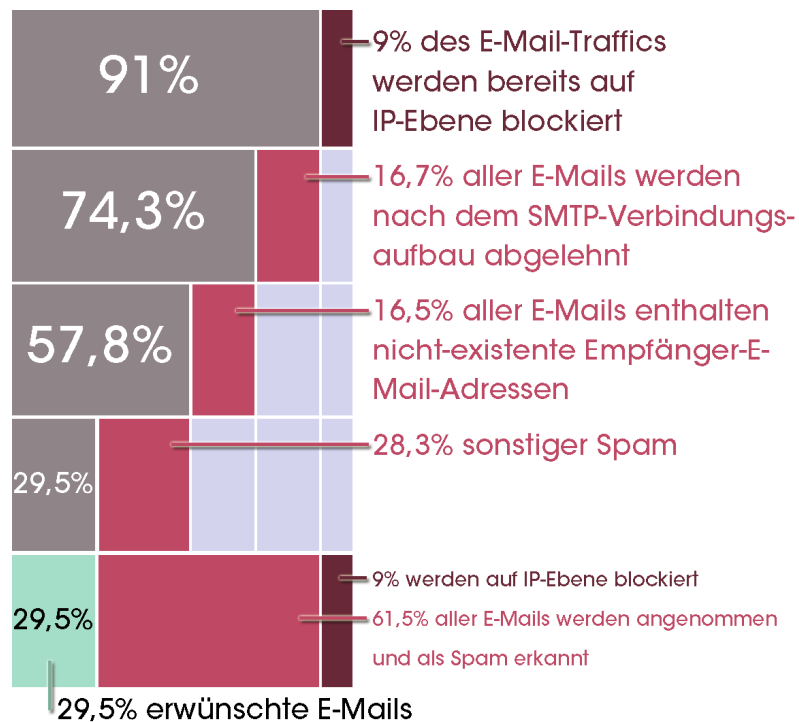


Abb. 1: Spam-Anteil am Gesamt-E-Mail-Volumen

Die Spanne der Spam-Raten der individuellen Organisationen deckt den Bereich von 0% bis 87% ab. Dies zeigt, dass die Bedrohung durch Spam für E-Mail-Nutzer sehr unterschiedlich ausfällt und es deutet insbesondere darauf hin, dass Spam kein uniformes Phänomen ist. Es lassen sich also keine einheitlichen Antworten und Ergebnisse treffen, sondern allenfalls Tendenzen erkennen. Unternehmen, die eCommerce unter Einsatz von E-Mail nutzen, haben tendenziell höhere Spam-Raten – im Durchschnitt 67,2% – gegenüber Non-eCommerce-Organisationen mit rund 45%.

Aus der Perspektive des E-Mail-Anwenders erreicht sein Postfach im Durchschnitt 28,3% des Gesamt-E-Mail-Volumens als Spam. Das Verhältnis zwischen Spam (28,3%) und Ham (29,5%) entspricht also an dieser Stelle in etwa 1:1 (siehe Abbildung 1). Intuitiv empfinden E-Mail-Nutzer den Spam-Anteil jedoch als deutlich gravierender.

Die Zahlen in Abbildung 1 sind die durch die Umfrage ermittelten Durchschnittswerte. Insbesondere die Grenzen zwischen Spam und Ham können allerdings in Folge von nicht zu vernachlässigenden False Positive und False Negative Raten von 2,4% respektive 8,9% zum Teil stark variieren.

Unabhängig davon gaben 14,5% der Befragten an, als Spam erkannte Nachrichten vom E-Mail-System vor Ablage im Postfach automatisch zu löschen.

4 Gegenmaßnahmen

Die Verbreitung von Antispam-Maßnahmen ist noch nicht flächendeckend, immer noch sind – trotz des hohen Spam-Aufkommens – mindestens 9% der Organisationen der Spam-Flut ungeschützt ausgesetzt. Über die Hälfte derer, die sich gegen Spam schützen, erreichen dies durch den Einsatz eines fertigen Produkts, das am Markt angeboten wird. Ein erwartungsgemäß geringer Prozentsatz von lediglich 5% hat seine Antispam-Lösung selbst entwickelt, diese Gruppe sind hauptsächlich ISPs oder IT-Dienstleister, die sich auf Spam-Schutz spezialisiert haben, da die Kostenersparnisse für optimale Gegenmaßnahmen den eigenen Mehraufwand sehr schnell rechtfertigen. Immerhin ergänzen 22,8% der Teilnehmer ein fertiges Produkt durch eigenentwickelte Mechanismen.

4.1 Das Ebenen-Modell

Um die Bedeutung der Antispam-Maßnahmen zu verdeutlichen, wird in Abbildung 2 ein schematischer Aufbau der Filtermechanismen auf den verschiedenen Ebenen eines empfangenden E-Mail-Servers aufgezeigt.

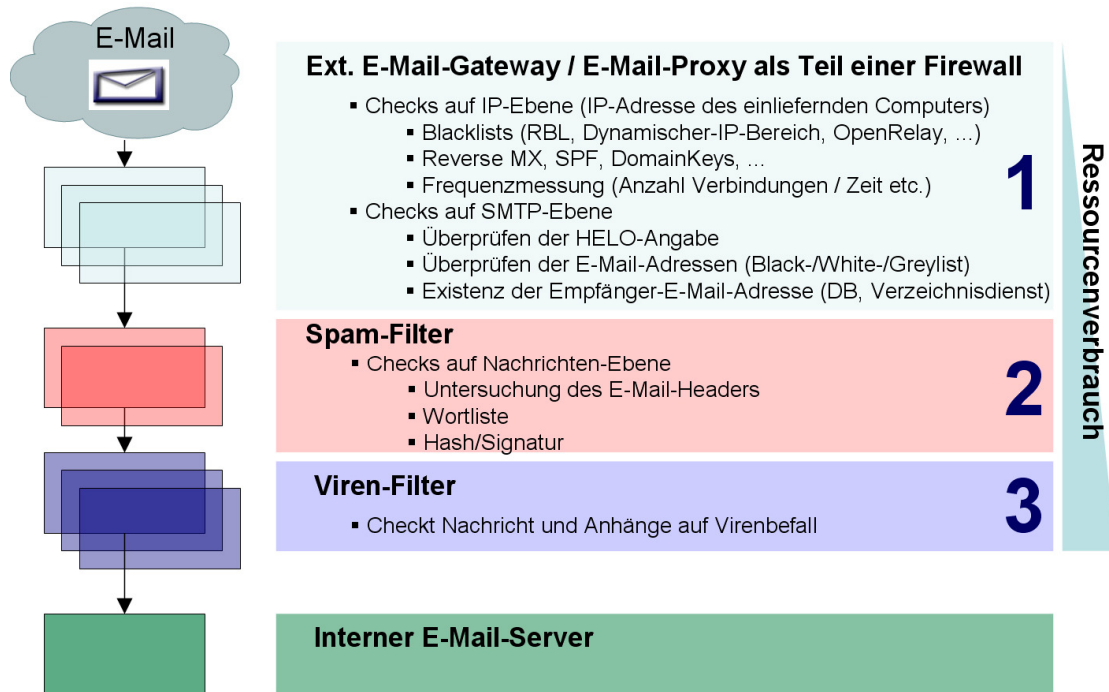


Abb. 2: Die verschiedenen Ebenen eines empfangenden E-Mail-Servers

4.2 Ebene 1

Die erste Ebene bilden die Überprüfungen der Merkmale der IP-Schicht (Netzwerk-Schicht) und der im SMTP-Verbindungsaufbau übermittelten Informationen. Der SMTP-Dialog ist in diesem Stadium noch nicht abgeschlossen. An dieser Stelle kann beispielsweise die IP-Adresse des einliefernden Computers in einer Realtime Blackhole List nachgeschlagen und dadurch in Erfahrung gebracht werden, ob diese IP-Adresse in der Vergangenheit bereits als Spam-Quelle auffällig geworden ist. Sollte dies der Fall sein, kann die Verbindung schon hier sofort abgebrochen werden.

Des Weiteren sollte ein empfangender E-Mail-Server bereits während des SMTP-Dialogs prüfen, ob er für die angegebene Empfänger-E-Mail-Adresse überhaupt ein korrespondierendes Postfach hat. Er sollte die E-Mail nur dann annehmen, wenn dies erfüllt ist. Immerhin enthalten 16,5% aller E-Mails nicht-existente Empfänger-Adressen. Dieser Mechanismus stellt insbesondere für große Unternehmen mit einer Vielzahl von E-Mail-Nutzern und mehreren, verteilten empfangenden E-Mail-Gateways ein Problem dar, denn oft existiert kein zentrales Verzeichnis des Unternehmens, in dem alle E-Mail-Postfächer aufgeführt werden. Allerdings lohnt der Aufwand, ein solches Verzeichnis anzulegen und zu pflegen, denn durch angenommene E-Mails, die dennoch nicht zustellbar sind, entstehen dem E-Mail-Betreiber erhebliche Kosten. Nicht nur die fälschlicherweise angenommene E-Mail verbraucht Bandbreite, sondern auch eine vom MTA erzeugte Non-Delivery Notification, also eine E-Mail zur Benachrichtigung des Absenders, dass seine ursprüngliche E-Mail nicht zugestellt werden konnte.

Spammer und Viren nutzen bisweilen selbst diese Non-Delivery Notifications, um in einer Art Spiegelverfahren Nachrichten zu versenden. Sie gehen dabei wie folgt vor: Eine E-Mail mit einer gefälschten Absender-Adresse und einer Empfänger-Adresse, zu der jedoch kein Postfach existiert, wird an den entsprechenden E-Mail-Server gesendet. Lehnt der E-Mail-Server diese Mail, obwohl kein Postfach existiert, nicht bereits im SMTP-Dialog ab – also auf der Ebene 1 –, muss der Server gemäß [Klen01] eine Non-Delivery Notification zurücksenden. Da jedoch als ursprünglicher Absender – vom Spammer absichtlich gefälscht – eine zwar tatsächlich existierende Adresse verwendet wird, die jedoch nie Urheber der ursprünglichen E-Mail war, hat der Spammer hierdurch verdeckt eine Werbenachrichtis zugestellt. Der Umstand, dass 37,8% der Befragten E-Mails mit Empfänger-Adressen, zu denen kein korrespondierendes Postfach existiert, nicht auf Ebene 1 ablehnen, zeigt, dass diese Strategie in der Praxis, obwohl das Verfahren seit Jahren bekannt, immer noch durchführbar ist. Eine vermeintliche Lösung, nämlich keine Non-Delivery Notifications mehr zu versenden, wird von 22,4% der Befragten angewendet. Dies hat jedoch in der Kombination mit der Annahme nicht-existierender Empfänger-E-Mail-Adressen – was bei 11,5% der Befragten der Fall ist – den erheblichen Nachteil, dass ein gutwilliger Absender, der versehentlich eine falsche Empfänger-E-Mail-Adresse angibt, nicht informiert wird, dass die E-Mail nicht zugestellt wird – aus Sicht des Absenders verschwindet die E-Mail quasi in einem schwarzen Loch.

Generell haben Mechanismen auf der Ebene 1 den entscheidenden Vorteil, dass die Kommunikation abgebrochen wird, bevor überhaupt große Datenmengen übertragen werden und dadurch Kosten entstehen. Der empfangende MTA kann den SMTP-Dialog nahezu an jeder Stelle des Verfahrens durch einen Fehlercode und evtl. mit einer entsprechenden Begründung abbrechen.

Darüber hinaus sind die meisten Mechanismen auf Ebene 1 wesentlich ressourcenschonender als solche auf den nachfolgenden Ebenen und können oft sogar in E-Mail-Proxies vor dem eigentlichen MTA implementiert werden, um damit den eigentlichen E-Mail-Server zu entlasten.

4.3 Ebene 2

Auf der Ebene 2 ist die E-Mail vom empfangenden MTA bereits angenommen und der SMTP-Dialog abgeschlossen. Die Abwehrmechanismen können an dieser Stelle auf die gesamte E-Mail zugreifen. Dies beinhaltet, dass nicht nur Empfänger- und Absender-Adressen überprüft werden, sondern dass der gesamte Inhalt der E-Mail zur Disposition steht.

Mittels Hash-Verfahren und einer zentralen Datenbank aller Hash-Werte eines Anbieters lässt sich beispielsweise ermitteln, ob exakt diese oder eine inhaltlich ähnliche E-Mail bereits anderen E-Mail-Servern begegnet ist. Hierdurch lassen sich Rückschlüsse dahingehend ziehen, ob eine E-Mail möglicherweise Teil eines Massenversands ist und demzufolge Spam sein könnte.

Ferner greifen auf Ebene 2 statistische Header- und Wortanalysen. Diese untersuchen die Kopfzeilen auf ihre Plausibilität hin sowie auf die Häufigkeit bestimmter Wörter im Nachrichtentext. Auch dies lässt Rückschlüsse auf Spam zu.

4.4 Ebene 3

Die Ebene 3 bildet der Viren-Filter. Auf dieser Ebene werden Nachricht und Anhänge auf Virenbefall untersucht und gegebenenfalls direkt gelöscht oder in Quarantäne verschoben und evtl. nach einem zuvor definierten Zeitraum gelöscht.

Virenbehaftete E-Mails werden von rund 33% der Befragten sofort gelöscht, während 50% der Befragten Viren-Mails zunächst in die Quarantäne verschieben und nach einem vorher definierten Zeitraum löschen.

Ein Vergleich der Mechanismen der unterschiedlichen Ebenen zeigt, dass der Ressourcenverbrauch – wie in Abbildung 2 dargestellt – mit jeder Ebene steigt. Während auf der Ebene 1 bei der Abfrage einer DNS-basierten Realtime Blackhole List lediglich eine DNS-Anfrage gestellt wird, muss ein Virens Scanner auf der Ebene 3 möglicherweise komprimierte Dateianhänge aufwendig dekomprimieren und anschließend rechenintensiv untersuchen.

4.5 Die Spam-Gegenmaßnahmen im Überblick

In der Rangliste der Verbreitung der Antispam-Mechanismen führen Wort- und Headeranalyse-Verfahren vor schwarzen sowie weißen Listen (siehe Tabelle 3).

Tabelle 4: Rangliste der Verbreitung der Mechanismen²

Mechanismus	Rel. Häufigkeit
Wortanalyse	58,2%
Header-Analyse	48,1%
Blacklist (insgesamt)	46,8%
Whitelist (insgesamt)	43,0%
Blacklist (als Scoring-Quelle ³)	33,8%
Heuristik	31,1%
Blacklist (im Verbindungsaufbau)	29,7%
Whitelist (im Verbindungsaufbau)	29,7%
Hash/Signatur-Verfahren	28,4%
Whitelist (als Scoring-Quelle)	21,6%
Blockieren dynamischer IP-Adressen (im Verbindungsaufbau)	20,3%

² Siehe Frage 9 des Fragebogens (im Anhang)

³ Der Begriff Scoring bezeichnet die Berechnung eines Wertes basierend auf mehreren Spam-Tests, sog. Scoring-Quellen.

Blockieren dynamischer IP-Adressen (als Scoring-Quelle)	16,2%
Greylisting	10,8%
Einsatz einer Teergrube	8,1%

Der dargestellten Tabelle kann entnommen werden, dass bisher die üblichen Spam-Filter – im Sinne von Analysen und Untersuchungen einer E-Mail – am meisten verbreitet sind.

4.5.1 Black- und Whitelists

Mit Hilfe einer sog. Blacklist lassen sich bekannte Spamquellen vom E-Mail-Empfang ausschließen, mit Hilfe einer sog. Whitelist lässt sich demgegenüber zuverlässige, gewünschte Kommunikation von der Überprüfung auf Spam ausnehmen. Die Häufigkeit des Einsatzes von schwarzen und weißen Listen liegt relativ nahe beieinander, da der Einsatz einer Blacklist immer individuelle Ausnahmen, die mit Hilfe einer Whitelist realisiert werden, erfordert. Nach selbstgepflegten schwarzen Listen ist die OpenRelay Database (ORDB) mit einer Häufigkeit von 37,8% derjenigen Teilnehmer, die überhaupt Blacklists nutzen, die am häufigsten eingesetzte frei verfügbare Blacklist.

Eine spezielle Art von Blacklist ist die sog. Realtime Blackhole List (RBL). Hierunter versteht man eine dynamische schwarze Liste, die meist per DNS abgefragt wird. Beim Einsatz von RBLs muss beachtet werden, dass nicht individuell über den Empfang einer konkreten Nachricht, sondern über alle E-Mails von einer bestimmten Quelle entschieden wird. Dies gestaltet sich insbesondere dann problematisch, wenn – wie in der Vergangenheit bereits aufgetreten – E-Mail-Server großer Service Provider auf eine schwarze Liste geraten und dadurch generell keine E-Mails, die über diesen Service Provider versendet werden, mehr empfangen werden. Die Entscheidung darüber, ob bzw. welche Blacklist eingesetzt wird, bedeutet also auch immer eine Vertrauensfrage, da die Kontrolle über den Empfang weitgehend an den RBL-Betreiber abgegeben wird.

Die Umfrageergebnisse zeigen jedoch, dass gewisse Befragte insbesondere durch aufwendig gepflegte Realtime Blackhole Lists einen Spam-Anteil von bis zu 50% bereits auf der Ebene 1 eliminieren können. Die Tatsache, dass der aktuelle Durchschnittswert des zu blockierenden Anteils lediglich 8,9% beträgt, zeigt, welches Potential in der Filterung auf IP-Schicht noch möglich ist.

Zurzeit wenden lediglich 27,6% der Teilnehmer Filtermechanismen auf IP-Schicht an, hauptsächlich RBLs. Durch eine höhere Verbreitung der Anwendung von Blacklists wird pro Organisation ein deutlich höherer Anteil an Spam als bisher auf Ebene 1 geblockt werden können.

4.5.2 Header- und Wortanalyse, (verteilte) Hash-Verfahren

Bei diesen Mechanismen werden Nachrichten-Header sowie Nachrichten-Body auf für Spam-Nachrichten charakteristische Eigenschaften hin untersucht. Hierbei hat sich in vielen Antispam-Lösungen im Laufe der Zeit ein beachtliches Regelwerk entwickelt, mit Hilfe dessen ein großer Anteil an Spam-E-Mails erkannt wird. Allerdings handelt es sich hier um ein Kopf

an Kopf Rennen mit den Spammern, denn auch sie verfeinern ihre Techniken und tarnen ihre Spam-Nachrichten immer besser, sodass es für die Filter scheinbar immer weniger Anhaltspunkte für eine Entscheidung gibt, ob es sich um Spam handelt. Die durch die Umfrage ermittelte und mit 8,9% doch sehr hohe Rate an False Negatives, also an Spam-Nachrichten, die nicht als solche erkannt wurden, spiegelt diesen Umstand deutlich wider.

Aber auch ein hoher Anteil an False Positives mit 2,4% und ein großer Wertebereich zwischen 0% und 20% zeigt, dass einige Befragte offensichtlich große Probleme mit Header- und Wortanalysen sowie mit Hash-Verfahren, also den Antispam-Mechanismen auf Ebene 2, haben. Hierdurch ergibt sich – insbesondere wenn Spam-Nachrichten automatisch gelöscht werden – ein Verlust wichtiger E-Mails. Immerhin geben rund 17% der Befragten an, bereits durch verloren gegangene, gleichwohl bedeutsame E-Mails tatsächliche Schäden erlitten zu haben.

4.5.3 Blockieren dynamischer ISP-Dial-Up-IP-Adressen

In der jüngeren Entwicklung im Internet hat sich gezeigt, dass die Phänomene Spam und Viren immer mehr miteinander verschmelzen. So gibt es Viren, deren einziges Ziel darin besteht, den Computer des Opfers als Versandstation von Spam-Nachrichten zu missbrauchen. Die meisten Opfer sind dabei Arbeitsplatzrechner, deren Nutzer den Befall vermutlich gar nicht bemerken. Dieser Umstand führt dazu, dass nicht mehr nur ein einzelner Quell-Computer des Spamversands existiert, sondern Spam von vielen unterschiedlichen Quellen in das Internet eingespeist wird.

Eine mögliche Gegenmaßnahme besteht darin, auf einem empfangenden E-Mail-System diejenigen IP-Adressen oder IP-Adressbereiche, die Internet Service Provider für Ihre Dial-Up-Kunden nutzen, per se zu blockieren.

Diese Möglichkeit ist vermutlich gerade deswegen so effektiv, weil lediglich 26,3% der Befragten eine Spam-Erkennung auf ausgehende E-Mails anwenden. Dabei bietet doch gerade die Überprüfung auf Spam für ausgehenden E-Mail-Verkehr Schutz vor Missbrauch der eigenen Infrastruktur bei geringem Aufwand.

Filtermechanismen zur Sperrung von ISP-Dial-Up-Adressen bereiten in der Praxis weitaus weniger Probleme als man zunächst vermuten würde. Es gibt einen zwar sehr geringen Anteil an E-Mail-Nutzern, die auf einem Computer mit dynamischer ISP-Dial-Up-IP-Adresse ihren eigenen MTA betreiben und durch diese Maßnahme in der direkten E-Mail-Zustellung eingeschränkt werden. Allerdings wird durch Berichte aus der Praxis klar, dass die entsprechenden Nutzer in vielen Fällen nach Darstellung der Situation aus der Sicht der Dienstleister Verständnis zeigen und meist eine unkomplizierte Einigung mit ihrem Service Provider – beispielsweise durch Verwendung eines SMTP-Smarthost ihres Providers – erzielen.

4.5.4 Greylisting

Bei Greylisting handelt es sich um ein Verzögerungsverfahren, welches darauf basiert, die Zustellung von E-Mails bei Vorliegen einer temporären Störung des empfangenden E-Mail-Servers nicht aufzugeben, sondern nach definierten Zeiträumen erneut zu versuchen. Viele Spammer können sich diesen Zeitaufwand allerdings nicht leisten und übergehen E-Mail-

Server, die Greylisting einsetzen. Dieses Überspringen von E-Mail-Servern mit Greylisting greift vermutlich zurzeit nur dadurch, dass lediglich 10,8% aller Teilnehmer überhaupt Greylisting einsetzen. Die geringe Verbreitung kommt dem Spammer entgegen, denn die Wahrscheinlichkeit, einen nicht greylistenden E-Mail-Server zu finden, ist relativ hoch.

Der Empfang von Spam wird beim Einsatz von Greylisting allerdings nicht vollständig verhindert, d.h. sollte ein erneuter Zustellversuch durch den Spammer in einem RFC-konformen Zeitraum erfolgen, so wird die Spam-Nachricht gleichwohl zugestellt.

Greylisting führt allerdings zu einem Verlust des Quality of Service, d.h. eine legitime Non-Spam-Nachricht benötigt eventuell für die Zustellung mehrere Versuche und dadurch länger, als dies technisch ohne Greylisting erforderlich ist. In den Umfrageergebnissen ist jedoch belegt, dass gerade diejenigen Unternehmen, die elektronische Geschäftsprozesse betreiben, keinen Verlust des Quality of Service hinnehmen können. Bei 14,3% der befragten AGs entstanden sogar Schäden infolge verminderter Quality of Service.

4.5.5 Frequenzmessungen des Kommunikationsverhaltens

Die Zustellversuche von Spammern können sich je nach Aggressivität des Spammers in der Häufigkeit und insbesondere in der Frequenz der Verbindungsaufbauten niederschlagen. Hieraus lässt sich als eine weitere Maßnahme zur Abwehr von Spam die Frequenzmessung des Kommunikationsverhaltens einliefernder MTAs ableiten. Ähnlich der Vorgehensweise von Intrusion Detection bzw. Intrusion Prevention Systemen kann durch die Analyse des Kommunikationsverhaltens eine Vermutung darüber geäußert werden, ob ein Angriff bzw. Missbrauch stattfindet oder ob in legitimem Umfang E-Mails zugestellt werden.

Die Frequenzmessung an sich kann allerdings nicht vor Spam schützen, sondern lediglich als Basis für andere Gegenmaßnahmen wie z.B. Teergrubing dienen. So können beispielsweise infolge der Frequenzmessung aufgefallene Kommunikationspartner anders bedient werden, indem ihre Verbindungen künstlich verzögert werden. Ein mutmaßlicher Spammer kann sich diesen – wenn auch nur geringen – Zeitverlust meist nicht leisten.

Die Methode der Frequenzmessung wird im Durchschnitt von 7,3% der Befragten eingesetzt. Durch die hohe Anzahl an E-Mails, die ISPs täglich empfangen, nutzen insbesondere Service Provider die Methode der Frequenzmessung, um sich optimal zu schützen.

5 Weitere Auswertungsergebnisse

5.1 Private Nutzung von E-Mail

Die private Nutzung von E-Mail erlauben 57,9% der befragten Organisationen und Einrichtungen, während 23,7% private Nachrichten über den organisationseigenen E-Mail-Dienst untersagen. Rund 54% der Befragten unterliegen einer Dienst- bzw. Betriebsvereinbarung über die private E-Mail-Nutzung.

Tabelle 5: Private Nutzung des Organisations-E-Mail-Dienstes⁴

Private Nutzung	Antwort			
	ja	nein	Keine Angabe	Gesamtergebnis
Aktiengesellschaft	87,5%	0,0%	12,5%	100%
Behörde	34,8%	47,8%	17,4%	100%
Gesellschaften mit beschränkter Haftung	72,2%	16,7%	11,1%	100%
Hochschule	50,0%	0,0%	50,0%	100%
Service Provider	66,7%	0,0%	33,3%	100%
diverse	60,0%	20,0%	20,0%	100%
Gesamtergebnis	57,9%	23,7%	18,4%	100%

Tabelle 6: Dienst-/Betriebsvereinbarung über private Nutzung der Organisations-E-Mail⁵

Dienst-/Betriebsvereinbarung	Antwort			
	ja	nein	keine Angabe	Gesamtergebnis
Aktiengesellschaften	50,0%	37,5%	12,5%	100,0%
Behörden	69,6%	17,4%	13,0%	100,0%
Gesellschaften mit beschränkter Haftung	33,3%	55,6%	11,1%	100,0%
Hochschulen	50,0%	25,0%	25,0%	100,0%
Service Provider	0,0%	0,0%	100,0%	100,0%
diverse	65,0%	25,0%	10,0%	100,0%
Gesamtergebnis	53,9%	30,3%	15,8%	100,0%

Kombiniert man die Ergebnisse der Fragen 18 und 19, so zeigt sich, dass 21,1% der Befragten die private E-Mail-Nutzung verbieten und dies auch in einer Dienst- bzw. Betriebsvereinbarung vereinbart wurde. Demgegenüber erlauben rund 30% der Befragten die private Nutzung des organisationseigenen E-Mail-Dienstes in Dienst- bzw. Betriebsvereinbarungen.

5.2 Verschlüsselung und digitale Signatur

Der durchschnittliche Anteil verschlüsselter E-Mails beträgt lediglich 4,3%, der Anteil signierter E-Mails liegt geringfügig höher bei 6%.

Insgesamt liegt die der höhere Anteil signierter E-Mails vermutlich darin begründet, dass hierbei der Empfänger entscheiden kann, ob er die Verifikation durchführt oder nicht. Wenn

⁴ Siehe Frage 18 des Fragebogens (im Anhang)

⁵ Siehe Frage 19 des Fragebogens (im Anhang)

verschlüsselt wurde, muss der Empfänger die Technologie und den Schlüssel zur Entschlüsselung verfügbar haben bzw. im Falle von Public Key, seinen öffentlichen Schlüssel auf einen Schlüsselservers geuploadet haben. Letztendlich muss auf Empfängerseite auch die Entschlüsselung durchgeführt werden, um an den Inhalt der E-Mail im Klartext zu gelangen.

Tabelle 7: Durchschnittlicher Anteil verschlüsselter E-Mails

Branche	Ergebnis
Bildungsinstitution	0,1%
Finanzdienstleistungen	13,6%
Informationstechnologie	4,1%
Öffentlicher Dienst	4,2%
Industrie	0,7%
Dienstleistungen	0,5%
ISP	0,5%
Gesamtergebnis	4,3%

Tabelle 8: Durchschnittlicher Anteil digital signierter E-Mails

Branche	Ergebnis
Bildungsinstitution	0,0%
Finanzdienstleistungen	21,2%
Informationstechnologie	8,2%
Öffentlicher Dienst	0,8%
Industrie	0,3%
Dienstleistungen	0,5%
ISP	1,5%
Gesamtergebnis	6,0%

Spitzenreiter beim Einsatz von Verschlüsselung und digitaler Signatur für E-Mails sind Finanzdienstleister.

Insgesamt setzen 51,3% der Befragten Signatur- oder Verschlüsselungsstandards ein. Die folgende Tabelle zeigt die Verteilung der Verfahren.

Tabelle 9: Verteilung der Signatur-/Verschlüsselungsverfahren⁶

Verfahren	Häufigkeit
PGP/OpenPGP/GnuPG	38,2%
S/MIME	23,7%
Passphrase-gestützt	3,9%
Einsatz einer PKI	22,3%

5.3 Virtuelle Poststelle

Clientbasierte End-to-End Lösungen für E-Mail Sicherheit haben sich – obwohl seit langem verfügbar – in der Praxis kaum durchgesetzt. Neben hohen Kosten und aufwendiger Administration kranken diese Konzepte an vier charakteristischen Problemfeldern, für die es innerhalb dieser Konzepte bis heute keine überzeugenden Lösungen gibt. Neben der immer noch mangelhaften Interoperabilität der Lösungen, die sich immer dann als besonderes Handicap erweist, wenn der eigentlich sensible externe E-Mail-Verkehr geschützt werden soll, sind dies die Message-Recovery-Problematik, die Schwierigkeit der Abbildung interner Vertreter-Policies und die Viren-Problematik.

An dieser Stelle setzt das Konzept des Secure-E-Mail-Gateways an. Die Aufstellung an zentraler Stelle im E-Mail-Verkehr erlaubt die Anwendung einer zentralen Unternehmens-Policy hinsichtlich der Verteilung von E-Mails sowie der Anwendung von kryptographischen Operationen. Dies wird unterstützt durch die Möglichkeit, kryptographische Schlüssel innerhalb des Secure-E-Mail-Gateways gesichert speichern zu können. Hierzu kann zusätzlich ein Hardware-Sicherheitsmodul integriert werden, welches ein Höchstmaß an Sicherheit für die (kryptographischen) Schlüssel garantiert. Für weitere Informationen siehe [Pohl03].

19,7% der Befragten planen, eine Virtuelle Poststelle einzusetzen.

5.4 Schäden

Die Tatsache, dass 15,8% der Befragten Schäden durch verloren gegangene E-Mails erlitten haben, bestätigt, dass der Verlust von E-Mails unter anderem durch False Positives nicht hinnehmbar ist.

⁶ Siehe Frage 22 des Fragebogens (im Anhang). Die relative Häufigkeit bezieht sich auf die Gesamtzahl derjenigen, die diese Frage überhaupt beantwortet haben. Mehrfach-Antworten sind zugelassen.

Tabelle 10: Schäden durch verloren gegangene E-Mails⁷

Rechtsform	ja	nein	keine Angabe	Gesamtergebnis
Aktiengesellschaft	0,0%	37,5%	62,5%	100,0%
andere	40,0%	45,0%	15,0%	100,0%
Behörde	4,3%	69,6%	26,1%	100,0%
Gesellschaft mit beschränkter Haftung	11,1%	61,1%	27,8%	100,0%
Hochschule	0,0%	75,0%	25,0%	100,0%
ISP	33,3%	33,3%	33,3%	100,0%
Gesamtergebnis	15,8%	56,6%	27,6%	100,0%

Es wurden sowohl Imageschäden als auch erhebliche Störungen der Verfügbarkeit festgestellt. Finanzielle Schäden durch verloren gegangene E-Mails sind in der Regel kaum zu beziffern. 4% der Befragten mussten Schäden verzeichnen, die auf den Verlust des Quality of Service aufgrund ergriffener Anti-Spam-Maßnahmen zurückzuführen sind.

5.5 Einschätzung der Bedrohungslage

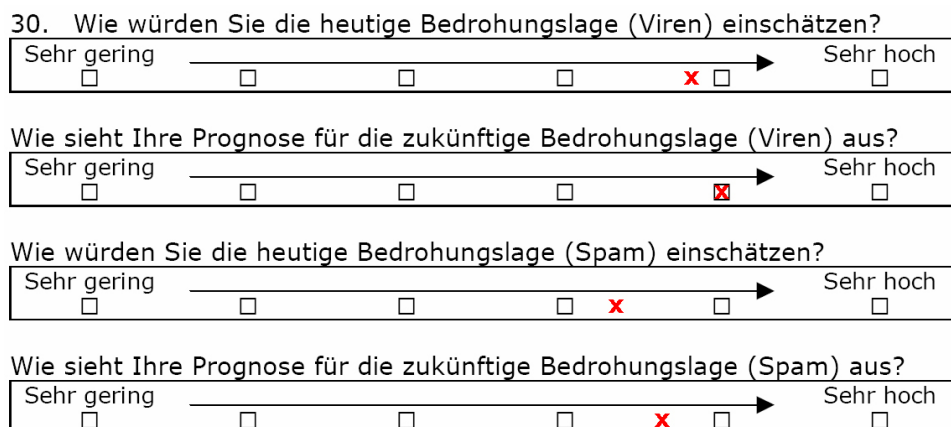


Abb. 3: Durchschnitt der Einschätzung der Bedrohungslage bzgl. Viren und Spam⁸

Die höher eingeschätzte Bedrohung durch Viren lässt sich dadurch begründen, dass Viren – wie z.B. Sobig oder Klez – in der Vergangenheit gezeigt haben, welcher horrende Schaden aus Virenbefall resultieren kann. Schätzungen zufolge hat allein Sobig zwischen 500 Mio. und 1 Mrd. US \$ an Schaden allein durch das Lahmlegen von Netzwerken verursacht, ohne dabei

⁷ Siehe Frage 28 des Fragebogens (im Anhang)

⁸ Die Kreuze stellen den Durchschnittswert aller Befragten zur Einschätzung der Bedrohungslage dar. Siehe Frage 30 des Fragebogens (im Anhang)

explizit Datenvernichtung programmiert zu haben. Dabei ist es lediglich ein kleiner weiterer Schritt in der Entwicklung der Viren, wenn zukünftig Viren nebenbei auch noch programmiert Daten löschen.

Demgegenüber zeigt sich Spam bisher zwar als lästiges Phänomen, hierdurch kommt es allerdings nur in seltenen Fällen auch zu direkten Schäden.

Die Ergebnisse der Einschätzung der Bedrohungslage zeigen, dass die Befragten generell eine Zunahme der Bedrohung für den E-Mail Dienst erkennen. Es ist also höchste Zeit zu handeln.

6 Fazit und Ausblick

Um die Struktur der Bedrohung des E-Mail-Dienstes zu untersuchen, hat das Institut für Internet-Sicherheit der FH Gelsenkirchen eine Fragebogenaktion zur E-Mail-Verlässlichkeit in Deutschland durchgeführt. Die Umfrageergebnisse, insbesondere bezogen auf Spam, dienen als empirische Grundlage für die Forschung im Bereich E-Mail-Verlässlichkeit.

Als aktuell wirksamer, gleichwohl noch nicht weit verbreiteter Mechanismus haben sich schwarze Listen, insbesondere Realtime Blackhole Lists erwiesen, die aufgrund der Ablehnung von Spam bereits im SMTP-Dialog eine deutliche Kosteneinsparung darstellen. Einzelne Beispiele zeigen, dass die Erkennungsrate von Spam bei diesem Verfahren von derzeit im Schnitt 8,9% auf bis zu über 40% gesteigert werden kann.

Ferner lässt sich durch das Blockieren dynamischer Dial-Up-IP-Adressen bereits ein Großteil an Spam reduzieren.

Darüber hinaus sollten insbesondere in großen Organisationen nur E-Mails angenommen werden, zu denen ein Postfach auch tatsächlich existiert.

Der E-Mail Dienst ist derzeit noch kein absolut verlässliches, integriertes Kommunikationsmedium. Die Auswirkungen durch Spam und Viren bekommen E-Mail-Nutzer tagtäglich zu spüren, hierdurch werden erhebliche Kosten verursacht. Die Verbreitung und Bewertung der verschiedenen Antispam-Mechanismen zeigt, dass jeder Mechanismus für sich genommen Vor- aber auch Nachteile hat und E-Mail nicht zu einem sicheren Dienst macht. Vielmehr ist eine Kombination mehrerer Mechanismen aller genannten Ebenen notwendig, um zurzeit und künftig mit einem vertretbaren Aufwand einen angemessenen Schutz vor Spam und Viren zu realisieren.

Literatur

- [Klen01] J. Klensin: Simple Mail Transfer Protocol, RFC 2821, 2001
- [Pohl03] N. Pohlmann: „Die virtuelle Poststelle“, in "IT-Sicherheit im verteilten Chaos", Hrsg.: Bundesamt für Sicherheit in der Informationstechnik, SecuMedia Verlag, 2003
- [RazHVS] U. Raz: How do spammers harvest email addresses?, <http://www.private.org.il/harvest.html>
- [Clea04] Clean MX: Spam Report Deutschland Dezember 2004. http://www.clean-mx.de/downloads/041208_clean_mx_-_spam_report_deutschland_dezember_2004.rtf, 2004
- [Mess04] MessageLabs Intelligence: Annual Email Security Report 2004. http://www.messagelabs.com/binaries/LAB480_endofyear_v2.pdf, 2004

Anhang – Fragebogen zur E-Mail-Verlässlichkeit

Dies ist die Version des Fragebogens zur E-Mail-Verlässlichkeit vom 17.11.2004.

Fragebogen zur E-Mail-Verlässlichkeit

Dieses Dokument enthält die Fragen des Online-Fragebogens und kann dazu genutzt werden, sich VOR dem eigentlichen Ausfüllen auf der Webseite einen Überblick über die Fragen zu verschaffen und gegebenenfalls Zahlen aus einer anderen Abteilung einzuholen oder eintragen zu lassen.

Bitte schicken Sie uns keine ausgefüllten oder ausgedruckten Fragebögen dieser PDF-Version zu, sondern nutzen Sie bitte lediglich die unter <http://www.forschung.informatik.fh-gelsenkirchen.de:8080/online-fragebogen/> verfügbare Online-Version dieses Fragebogens!

Grau hinterlegte Fragen erfordern zur Beantwortung eher technisches Know-how, diese Fragen sollten beispielsweise von E-Mail-Systemadministratoren beantwortet werden. Falls Ihr Unternehmen keine eigene E-Mail-Administration hat, können die grau hinterlegten Fragen am ehesten übersprungen werden.

Anonymität, Geheimhaltung:

Die Antworten werden von uns zusammengefasst und anonym ausgewertet. Eine Weitergabe an Dritte erfolgt nicht. Wir sichern Ihnen zu, dass die Informationen von uns vertraulich behandelt werden.

6.1 Komplex A – Allgemeine Fragen

1. Betreiben Sie kritische Geschäftsprozesse (z.B. Vertragsabschlüsse, Statusabfragen/-berichte per E-Mail) auf E-Mail-Basis?

ja

nein

keine Angabe

2. Wie lange wäre ein Ausfall des E-Mail Dienstes für Ihr Unternehmen tolerierbar?

- weniger als 1 Min.
 weniger als 30 Min.
 weniger als 1h
 weniger als 1 Tag
 weniger als 1 Woche
 mehr als 1 Woche
 keine Angabe

3. Wie viele E-Mail-Adressen werden in Ihrem Unternehmen verwaltet?

Anzahl: _____

6.2 Komplex B - Fragen bezüglich E-Mails, Viren und Spams

E-Mail-Volumen

Bemerkung

Im Folgenden wird eine E-Mail als „angenommen“ bezeichnet, wenn die SMTP-Datenübertragung (SMTP Kommando DATA) abgeschlossen ist.

Die folgenden Fragen können auf zwei Arten beantwortet werden. Alternative A bietet die Möglichkeit, lediglich die Zahl oder Schätzung für den letzten Monat einzutragen. Bitte füllen Sie, falls Sie genaue, monatliche Werte zu den entsprechenden Fragen für den Zeitraum der vergangenen 6 Monate haben, nach Alternative B aus.

4. Wie hoch war das gesamte E-Mail-Aufkommen an angenommenen E-Mails in Ihrem Unternehmen im letztem Monat / in den letzten Monaten?

Alternative A	Alternative B
Oktober 04 Angabe in Anzahl der E-Mails: _____	Mai 04 Angabe in Anzahl der E-Mails: _____
	Juni 04 Angabe in Anzahl der E-Mails: _____
	Juli 04 Angabe in Anzahl der E-Mails: _____
	August 04

	Angabe in Anzahl der E-Mails: _____ September 04 Angabe in Anzahl der E-Mails: _____ Oktober 04 Angabe in Anzahl der E-Mails: _____
--	---

5. Wie hoch ist von dem gesamten E-Mail-Aufkommen an angenommenen E-Mails die Anzahl der erkannten virenverseuchten E-Mails im letzten Monat?

Alternative A	Alternative B
Oktober 04 Angabe in Anzahl der E-Mails: _____	Mai 04 Angabe in Anzahl der E-Mails: _____ Juni 04 Angabe in Anzahl der E-Mails: _____ Juli 04 Angabe in Anzahl der E-Mails: _____ August 04 Angabe in Anzahl der E-Mails: _____ September 04 Angabe in Anzahl der E-Mails: _____ Oktober 04 Angabe in Anzahl der E-Mails: _____

6. Wie hoch ist von dem gesamten E-Mail-Aufkommen an angenommenen E-Mails die Anzahl der identifizierten Spams im letzten Monat?

Alternative A	Alternative B
Oktober 04 Angabe in Anzahl der E-Mails: _____	Mai 04 Angabe in Anzahl der E-Mails: _____ Juni 04 Angabe in Anzahl der E-Mails: _____ Juli 04 Angabe in Anzahl der E-Mails: _____ August 04 Angabe in Anzahl der E-Mails: _____ September 04 Angabe in Anzahl der E-Mails: _____

	Oktober 04 Angabe in Anzahl der E-Mails: _____
--	---

7. a) Wie hoch ist der Anteil an E-Mails, die Ihrem E-Mail-System zugestellt werden, aber ein/e auf Ihrem E-Mail-System nicht-existentes E-Mail-Postfach/nicht-existente Email-Empfänger-Adresse haben?

Angabe in %: _____

7. b) Weisen Sie solche E-Mails auf SMTP-Ebene vor Beginn der SMTP-Datenübertragung (SMTP Kommando DATA) ab?

ja

nein

keine Angabe

8. a) Wie hoch ist der Anteil an E-Mails, die Ihr E-Mail-System (MTA) aufgrund von Merkmalen auf IP-Ebene vor dem SMTP-Verbindungsaufbau (z.B. durch Abbruch des TCP-Handshakes) ablehnt?

Angabe in %: _____

8. b) Wie hoch ist der Anteil an E-Mails, die Ihr E-Mail-System (MTA) vor Übertragung des Inhalts der E-Mail abweist?

Angabe in %: _____

Gegenmaßnahmen

9. Welche Mechanismen setzen Sie gegen Spam ein?

Bitte beantworten Sie den grau hinterlegten Teil dieser Frage nur, wenn Sie die interne Funktionsweise Ihrer Anti-Spam-Lösung genau kennen. Wenn Sie sich nicht sicher sein sollten, lassen Sie diesen Teilaspekt bitte unbeantwortet.

Bitte kreuzen Sie die Anti-Spam-Maßnahmen an, die in Ihrem Unternehmen im Einsatz sind.

	Verbindungsaufbau	Inhaltliche Bewertung
kein Empfang von E-Mails, die von Rechnern mit dynamischen IP Adressen versendet wurden	<input type="checkbox"/>	<input type="checkbox"/>
die Existenz der Empfänger-E-Mail-Adresse / Empfänger-Postfaches wird überprüft	<input type="checkbox"/>	<input type="checkbox"/>
Blacklist	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> selbstgepflegt		
<input type="checkbox"/> abonniert		
<input type="checkbox"/> SpamCop.Net		
<input type="checkbox"/> ORDB, OpenRelay Database		
<input type="checkbox"/> Relay Stop Blacklist		
<input type="checkbox"/> SPAMHaus blacklist		
<input type="checkbox"/> SPEWS.org blacklist		
<input type="checkbox"/> njabl.org		
<input type="checkbox"/> RFC-Ignorant.org		
<input type="checkbox"/> andere: _____		
Whitelist	<input type="checkbox"/>	<input type="checkbox"/>
Greylist	<input type="checkbox"/>	<input type="checkbox"/>
Einsatz einer Teergrube	<input type="checkbox"/>	
Header-Analyse		<input type="checkbox"/>
Wörter/Zeichenketten-Basis in Nachrichten-Body und Betreff-Zeile		<input type="checkbox"/>
Hash/Signatur		<input type="checkbox"/>
Frequenzmessungen des Kommunikationsverhaltens	<input type="checkbox"/>	<input type="checkbox"/>
Heuristik		<input type="checkbox"/>
Weitere: _____	<input type="checkbox"/>	<input type="checkbox"/>

Bitte kreuzen Sie die für Sie zutreffende der folgenden Antwortoptionen an:

- a) Wir setzen zur Zeit keine Anti-Spam-Lösung ein.
b) Wir setzen ausschließlich ein Produkt/eine Dienstleistung ein.

- c) Wir setzen ausschließlich eine Eigenentwicklung ein.
d) Wir setzen ein Produkt/eine Dienstleistung ergänzt durch eine Eigenentwicklung ein.
e) keine Angabe

Falls b) oder d) angekreuzt wurde:

Bitte nennen Sie den Hersteller/Anbieter/Produktbezeichnung/OpenSource-Software Ihrer Anti-Spam-Lösung:

- Clearswift
 eleven
 SpamAssassin
 Brightmail GmbH
 GROUP Technologies AG
 Ironport Systems
 Kaspersky Labs
 Messagelabs
 Webwasher AG
 All About IT
 andere: _____

Bietet Ihre Anti-Spam-Lösung einen Lernmechanismus, der von den Anwendern aktiv genutzt wird (z.B. Verschieben von False Positives in einen bestimmten Lern-Ordner)?

- ja
 nein
 keine Angabe

10. Nutzen Sie Standards für die Überprüfung der (IP-)Adressen von Zulieferern an Ihre SMTP-Server?

serverseitig

- SPF (Sender Policy Framework)
 Sender-ID / Caller-ID
 Reverse MX
 DomainKeys
 Domain Name Accreditation (DNA)
 andere

Wenn andere, welche: _____

clientseitig

- Client SMTP Validation (CSV)
 Client SMTP Authorization (CSA)

- SMTP AUTH
- POP-before-SMTP
- andere

Wenn andere, welche: _____

11. Wie hoch schätzen Sie den Anteil an False Negatives (E-Mails, die nicht erkannt, gefiltert oder markiert werden, jedoch von Anwendern trotzdem als Spam deklariert werden) ein?

Angabe in %:

12. Wie hoch schätzen Sie den Anteil an False Positives (gefilterte oder markierte Spams, die keine Spams waren) ein?

Angabe in %:

13. Setzen Sie auch Sicherheitsmechanismen ein, die erkennen, ob Spam-Mails aus Ihrem Unternehmen herausgesendet werden (z.B. Spam-Filter für ausgehende Nachrichten)?

- ja
- nein

E-Mail-Nutzung

14. Welches E-Mail-System setzen Sie in Ihrem Unternehmen ein?

Name/Produktbezeichnung des Mail Transfer Agent

- Sendmail
- Postfix
- Qmail
- Exim
- Microsoft Exchange
- Stalker Software: CommuniGate
- IBM Lotus Notes Domino Mail Server
- Eudora Internet Mail Server
- anderer: _____

Name/Produktbezeichnung des (meist verwendeten) Mail User Agent

- Microsoft Outlook
- Microsoft Outlook Express
- Mozilla E-Mail-Client / Mozilla Thunderbird / Netscape Messenger
- Apple Mail
- Pegasus Mail
- Eudora
- KMail
- Lotus Notes
- anderer: _____

15. Wie wird im Rahmen Ihres Anti-Viren-Mechanismus eine als virenverseucht erkannte E-Mail behandelt?

- Wir setzen zur Zeit keinen Anti-Viren-Mechanismus ein
- Sie wird automatisch gelöscht
- Sie wird in ein Quarantäne-Verzeichnis verschoben und dort nach einem definierten Zeitraum gelöscht
- Sie wird in ein Quarantäne-Verzeichnis verschoben und bleibt dort auf unbegrenzte Zeit verfügbar
- keine Angabe

16. Wird eine als Spam erkannte E-Mail im Rahmen Ihres Anti-Spam-Mechanismus automatisch gelöscht?

- ja
- nein
- keine Angabe

17. Werden Non-Delivery-Notifications von Ihrem Unternehmen gesendet?

- ja
- nein
- keine Angabe

18. Dürfen Ihre Mitarbeiter auch die E-Mail-Anwendung für private Zwecke nutzen?

- ja
- nein
- keine Angabe

19. Ist mit den Mitarbeitern eine Dienstvereinbarung/Betriebsvereinbarung über die private und dienstliche E-Mail-Nutzung geschlossen worden?

- ja
- nein
- keine Angabe

20. Haben Sie schon rechtliche Maßnahmen (z.B. Unterlassungsklage) gegen Personen oder Organisationen einleiten lassen?

- ja
- nein
- keine Angabe

Wenn ja, erfolgreich?

- ja
- nein

21. Existieren in Ihrem Unternehmen ausgehende E-Mail-Server, die unter Ihrem Domain-Namen E-Mails versenden, jedoch im DNS nicht mit einem MX-Eintrag versehen sind?

- ja
- nein
- unbekannt
- keine Angabe

Wenn ja, Anzahl: _____

Komplex C - Digitale Signatur und Verschlüsselung von E-Mails

22. Setzen Sie in Ihrem Unternehmen Signatur-/Verschlüsselungsstandards ein?

ja

nein

keine Angabe

Wenn ja, welche

PGP/OpenPGP, GnuPG

S/MIME

passphrase-gestützte Verschlüsselung

andere: _____

Wenn ja, nutzen Sie Absendervalidierung?

ja, über eine PKI

nein

23. Planen Sie eine virtuelle Poststelle einzusetzen?

ja

nein

keine Angabe

24. Wie hoch liegt in Ihrem Unternehmen der prozentuale Anteil an E-Mails, die verschlüsselt werden?

Angabe in %:

25. Wie hoch liegt in Ihrem Unternehmen der prozentuale Anteil an E-Mails, die digital unterschrieben werden?

Angabe in %:

Missbrauch

26. Wurden E-Mail-Adressen Ihres Unternehmens von externen Spammern gezielt oder ungezielt missbraucht?

ja

nein

keine Angabe

Wenn ja und genaue Zahl bekannt, Anzahl der Fälle in den letzten 6 Monaten: _____

Wenn ja und genaue Zahl nicht bekannt, Schätzung der Anzahl an Fällen in den letzten 6 Monaten:

27. Haben Sie schon Denial of Service Attacken auf die E-Mail-Anwendung in ihrem Unternehmen feststellen können?

- ja
 nein
 keine Angabe

Schäden

28. Sind Schäden aufgetreten, die durch verloren gegangene E-Mails entstanden sind?

- ja
 nein
 keine Angabe

Wenn ja, welche Art von Schaden trat auf

- finanzieller Schaden
 geschätzter finanzieller Schaden insgesamt in €: _____
- Imageschaden
- erhebliche Störung der Verfügbarkeit
- Anzahl verlorener E-Mails: _____

29. Sind Schäden zu verzeichnen, die auf den Verlust des Quality of Service aufgrund ergriffener Anti-Spam-Maßnahmen (z.B. zeitliche Verzögerung der E-Mail-Zustellung) zurückzuführen sind?

- ja
 nein
 keine Angabe

Wenn ja, geschätzter Schaden in €: _____

Prognose der E-Mail-Bedrohungslage

30. Wie würden Sie die heutige Bedrohungslage (Viren) einschätzen?

Sehr gering	□	□	□	□	□	□	Sehr hoch
-------------	---	---	---	---	---	---	-----------

Wie sieht Ihre Prognose für die zukünftige Bedrohungslage (Viren) aus?

Sehr gering	_____→	Sehr hoch
<input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	<input type="checkbox"/>

Wie würden Sie die heutige Bedrohungslage (Spam) einschätzen?

Sehr gering	_____→	Sehr hoch
<input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	<input type="checkbox"/>

Wie sieht Ihre Prognose für die zukünftige Bedrohungslage (Spam) aus?

Sehr gering	_____→	Sehr hoch
<input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	<input type="checkbox"/>

31. Wie hoch schätzen Sie den Schaden für Ihr Unternehmen insgesamt, der zur Zeit durch Spam pro Jahr verursacht wird?

Angabe in Euro: _____