Fraunhofer
SIT

Untersuchung von Spam-Eigenschaften kostenfreier Email-Dienste

Studie

Fraunhofer-Institut für Sichere Informationstechnologie (SIT)

25. März 2010

Fraunhofer-Institut für Sichere Informationstechnologie (SIT)
Rheinstraße 75
64295 Darmstadt

http://www.sit.fraunhofer.de

Ansprechperson:
Dr. Markus Schneider
markus.schneider(at)sit.fraunhofer.de

Autoren: Dr. Markus Schneider, Christian Winter, York Yannikos

Inhaltsverzeichnis

1 Zusammenfassung der Ergebnisse (Management Summary)

Spam ist eine sehr unangenehme Nebenerscheinung der Email-Kommunikation. Auch wenn man die Belästigung durch unerwünschte Werbemitteilungen schon sehr viel länger als Emails kennt, wie etwa durch Werbung und kostenlose Zeitungen im Briefkasten, so ist die Belästigung durch Email-Spam mittlerweile deutlich größer geworden, da Spammer ihre Mitteilungen praktisch zum Null-Tarif und schneller zum Adressaten bekommen. Vorliegenden Schätzungen zufolge beansprucht Spamming bereits 85%–95% des heutigen gesamten Email-Aufkommens. Von durchschnittlich 100 versendeten Emails werden 80 direkt als Spam herausgefiltert, bevor sie in irgendeiner Inbox oder Spambox erscheinen. Von den restlichen 20 zugestellten Emails besteht der überwiegende Teil dann wiederum aus Spam-Nachrichten. Spam, zwar oft nur als lästig empfunden, verursacht erhebliche Kosten für Benutzer und Unternehmen, die Emails als Kommunikationsmittel einsetzen, und für Anbieter von Kommunikationsdiensten und IT-Infrastrukturen.

Gegenstand der vorliegenden Arbeit ist die Untersuchung von Spam-Eigenschaften bestimmter kostenfreier Email-Dienste, welche fast ausschließlich von Endkunden für private Zwecke verwendet werden. Ziel dieser Untersuchung war es, festzustellen, wie stark Kunden bei verschiedenen Anbietern kostenfreier Email-Dienste von empfangenen Spam-Nachrichten betroffen sind. Bei der Untersuchung wurden die Dienstanbieter GMX, Google Mail, Hotmail, WEB.DE und Yahoo! berücksichtigt. Als Spam wurden hierbei nicht nur Emails von extern betrachtet, sondern auch Werbemitteilungen, die man als Kunde von dem eigenen Dienstanbieter erhält, sofern man dem Erhalt dieser Mitteilungen nicht ausdrücklich zugestimmt hat.

Um eine Aussage treffen zu können, wie sehr Kunden bei verschiedenen Dienstanbietern betroffen sind, wurden die von Testpersonen empfangenen Spam-Nachrichten in dem Beobachtungszeitraum gezählt. Insofern ging es bei der Untersuchung insbesondere um die Ermittlung von sogenannten False Negatives, also Spam-Nachrichten, die von den technischen Abwehrmaßnahmen nicht sicher als solche erkannt und herausgefiltert wurden. Bei den in der Untersuchung gezählten Spam-Nachrichten handelt es sich jedoch nicht ausschließlich um False Negatives: Ebenfalls von Interesse waren die Spam-Nachrichten, die in der Spam-Box zugestellt wurden, da sie einen gewissen Zeitaufwand für den Nutzer bedeuten. Dennoch ist es natürlich vorteilhaft, dass diese in der Spam-Box und nicht in der Inbox empfangen werden. Außerdem wurden Spam-Nachrichten berücksichtigt, welche vom Dienstanbieter selbst an seine Kunden versendet werden und schwerlich als False Negatives bezeichnet werden können.

Da bei der vorliegenden Studie ausschließlich die empfangenen Spam-Nachrichten betrachtet werden, handelt es sich nicht um eine umfassende Untersuchung von relevanten Spam-Eigenschaften. Bei einer solchen müssten weitere Spam-Eigenschaften von Diensten betrachtet werden, wie etwa die Anzahl von False Positives, also erwünschten Emails, welche von den Abwehrsystemen fälschlicherweise als Spam erkannt und herausgefiltert werden, so dass sie ihren Adressaten nicht erreichen.

Die vorliegende Untersuchung wurde von Fraunhofer SIT als passive Black-Box-Analyse durchgeführt. Das bedeutet, dass Fraunhofer SIT selbst keine Emails verschickt hat, die in die Messung eingegangen sind, und dass bei der Untersuchung nur das äußere Verhalten der technischen Systeme auf Dienstanbieterseite betrachtet wurde; Kenntnisse über die konkrete innere Struktur bei den Dienstanbietern lagen nicht vor und wurden folglich auch nicht verwendet. Die Untersuchung selbst ist für alle betrachteten Dienstanbieter unter gleichen Bedingungen, unparteiisch, fair, objektiv und für Dritte nachvollziehbar durchgeführt worden. Als Betrachtungszeitraum wurde für alle Dienstanbieter der Februar 2010 festgelegt.

Für eine Durchführung der Untersuchung unter gleichen Bedingungen wurden sehr viele verschiedene Aspekte berücksichtigt. So wurden bei allen Dienstanbietern die Standardeinstellungen der persönlichen Spam-Filter verwendet. Jede der insgesamt sechs Testpersonen hat sich bei jedem Dienstanbieter eine Email-Adresse einrichten lassen, wobei alle Email-Adressen einer Testperson bis auf den Domain-Namen exakt übereinstimmten. Jede Testperson hat ihre Email-Adressen bei den verschiedenen Dienstanbietern am selben Tag mit gewissem zeitlichen Abstand zum Beobachtungszeitraum eingerichtet. Alle bei der Untersuchung verwendeten Email-Adressen waren bei der Untersuchung noch relativ neu; keine war älter als drei Monate. Drei der sechs Testpersonen haben ihre Email-Adressen nicht publiziert, die restlichen drei Testpersonen mussten ihre Email-Adressen im Internet publizieren, damit diese relativ schnell in die Adresslisten der Spammer gelangen konnten. Wenn eine Testperson eine Email-Adresse an irgendeiner Stelle (z. B. Diskussionsforum) publiziert hat, dann musste sie alle ihre entsprechenden Email-Adressen, die sie bei den anderen Dienstbetreibern eingerichtet hatte, am selben Tag und an derselben Stelle (d. h. beispielsweise im selben Diskussionsforum, jedoch zu einem anderen Thema) publizieren. Somit waren die Voraussetzungen, um von Spammern gefunden zu werden, für die Email-Adressen einer Testperson bei verschiedenen Dienstanbietern gleich.

Bei der Durchführung der Untersuchung wurden während des Untersuchungszeitraums täglich für alle Testpersonen und für alle Dienstanbieter die neu empfangenen Spam-Nachrichten registriert und aufgezeichnet. Die somit erhaltenen Daten wurden in mehrerlei Hinsicht ausgewertet. Bei der Auswertung wurde festgestellt, dass bei allen Dienstanbietern in dem Betrachtungszeitraum nur eine niedrige Spam-Belastung vorlag. Die durchschnittliche Spam-Anzahl pro Tag und Person lag über die Testpersonen mit publizierten Email-Adressen gemittelt

bei allen Dienstanbietern unter einer Email pro Tag. Diese niedrigen Werte sind sicherlich auch dem Umstand geschuldet, dass sich die Email-Konten der Testpersonen alle noch in einer sehr jungen Lebensphase befanden. Im schlimmsten Fall hat eine Testperson über ihr Email-Konto bei GMX an einem Tag sechs Spam-Nachrichten empfangen. Auch wenn die durchschnittliche Spam-Anzahl pro Tag und Person über den Testpersonen mit publizierten Email-Adressen gemittelt niedrig ist, so erkennt man hier dennoch eine breite Streuung. Am oberen Ende (GMX) liegen die Werte in einer Größenordnung von durchschnittlich vier Spam-Nachrichten in fünf Tagen. Am unteren Ende (Yahoo!) empfängt eine Person durchschnittlich nur einmal in zehn Tagen eine Spam-Nachricht.

Um diese Streuung zu quantifizieren und Aussagen treffen zu können, wie gut Dienstanbieter relativ zu anderen Dienstanbietern abschneiden, war die Verwendung eines entsprechenden Instrumentariums notwendig. Hierzu wurden 10 verschiedene Metriken eingeführt, mittels derer verschiedene Aspekte über diesen Daten ausgewertet wurden. Die Metriken dienen in dieser Studie als Teilauswertungen und unterscheiden sich jeweils in dem gemessenen Gegenstand. Jede einzelne Metrik liefert eine Rangfolge der betrachteten Dienstanbieter, welche besagt, wie gut ein Dienstanbieter bzgl. des betrachteten Gegenstands relativ zu den anderen Dienstanbietern abgeschnitten hat. Ausgehend von den Teilauswertungen wurde eine Gesamtauswertung vorgenommen, bei welcher die Ergebnisse der Teilauswertungen gleichgewichtet eingegangen sind. Die Platzierung der Gesamtauswertung lautet:

1. Yahoo!
2. Hotmail
3. Google Mail
4. WEB.DE
5. GMX

Bei den Teilauswertungen hat sich bei drei der fünf Dienstanbieter ein sehr konstantes Bild ergeben. Bei allen Teilauswertungen hat Yahoo! den ersten, WEB.DE den vierten und GMX den letzten Platz belegt.

Tabelle 1.1: Gesamtanzahl Spam je Dienstanbieter für alle Testpersonen

	gmx	**googlemail**	**hotmail**	**web**	**yahoo**
Spam-Anzahl	116	18	13	57	8

Im Folgenden werden einige Teilauswertungen exemplarisch angeführt. Gemessen über allen Testpersonen wurden für den gesamten Zeitraum Februar 2010 die in Tabelle 1.1 gezeigten Anzahlen von Spam-Nachrichten ermittelt (Metrik M1). Die starke Streuung dieser Werte hängt sicherlich auch damit zusammen, dass sich die Email-Konten der Testpersonen in einer noch jungen Lebensphase befanden und somit der Spam-Umfang von extern noch ziemlich gering war, so dass die von den Dienstanbietern selbst verschickten Spam-Nachrichten (insbesondere beim GMX und WEB.DE) einen deutlichen Ausschlag erzeugt haben.

Für eine ausschließliche Betrachtung des externen Spams sei auf Metrik M10 weiter unten verwiesen. Die Platzierung nach M1 stimmt mit der Gesamtplatzierung überein.

Tabelle 1.2: Gesamtanzahl Spam für am stärksten betroffene Testperson je Dienstanbieter

	gmx	googlemail	hotmail	web	yahoo
Spam-Anzahl	26	8	6	20	4

In einer anderen Teilauswertung (Metrik M2) wurde je Dienstanbieter ermittelt, welche Testperson über dem Beobachtungszeitraum beim entsprechenden Dienstanbieter die meisten Spam-Nachrichten empfangen hat. Die Ergebnisse sind in Tabelle 1.2 dargestellt. Die Platzierung nach M2 stimmt mit der Gesamtplatzierung überein.

Tabelle 1.3: Anzahl von Tagen mit schlechtesten Tageswerten über allen Testpersonen je Dienstanbieter

	gmx	googlemail	hotmail	web	yahoo
Anzahl der Tage	18	3	3	9	1

In einer weiteren Teilauswertung (Metrik M5) wurde untersucht, an wie vielen Tagen des Beobachtungszeitraums ein Dienstanbieter über allen Testpersonen den für den jeweiligen Tag höchsten Wert an Spam-Nachrichten im Vergleich zu den anderen Dienstanbietern erreicht hat. Die Ergebnisse sind in Tabelle 1.3 dargestellt. Da das Tagesmaximum von mehr als einem Dienstanbieter erreicht werden kann, ergibt die Summe über den Werten in Tabelle 1.3 einen Wert größer als 28. Die Platzierung nach M5 stimmt nur in den Plätzen 1, 4 und 5 mit der Gesamtplatzierung überein. Nach M5 teilen sich Google Mail und Hotmail Platz 2.

Die Metrik M9 betrachtet, welcher Anteil von empfangenen Spam-Nachrichten in der Inbox ankommt. Bei den hier betrachteten Testpersonen haben sich für Google Mail und Yahoo! die Spitzenwerte von 0% ergeben, d. h. keine Spam-Nachricht ist in der Inbox empfangen worden. Bei Hotmail wurden immerhin 23% der empfangenen Spam-Nachrichten in die Inbox einsortiert, jedoch handelte es sich dabei ausschließlich um Emails, die von Hotmail selbst verschickt wurden. Bei WEB.DE waren es sogar 63% und bei GMX 78%. Die hohen Prozentwerte bei WEB.DE und GMX sind jedoch dadurch begründet, dass bei diesen der Anteil von solchen Spam-Nachrichten besonders hoch ist, die vom Dienstanbieter selbst verschickt werden. Solche selbst verschickten Spam-Nachrichten sortieren die Dienstanbieter stets in die Inbox. Nach M9 teilen sich Yahoo! und Google Mail den ersten Platz. Hotmail erreicht den dritten Platz, WEB.DE den vierten und GMX den fünften Platz.

Die Metrik M10 blendet die intern verschickten Spam-Nachrichten aus; hier werden nur solche Emails betrachtet, die nicht vom Dienstanbieter selbst verschickt werden. Also bietet die Metrik M10 eine Chance für diejenigen Dienstanbieter, die selbst viele Spam-Nachrichten an ihre Kunden verschicken, da diese hier nicht berücksichtigt werden. In dieser Teilauswertung wird je Dienstanbieter die Anzahl der von allen Testpersonen empfangenen Nachrichten, die nicht vom

Dienstanbieter stammen, über dem gesamten Beobachtungszeitraum ermittelt. Das Ergebnis dieser Teilauswertung zeigt jedoch, dass sich auch bei Nichtberücksichtigung der vom Dienstanbieter versendeten Spam-Nachrichten das gleiche Ergebnis einstellt wie bei Metrik M1 und wie in der Gesamtauswertung.

Die gezeigten Auswertungen (Gesamtauswertung und Teilauswertungen) geben lediglich die Ergebnisse der Messungen für die betrachteten Testpersonen im Beobachtungszeitraum Februar 2010 wieder. Verallgemeinerungen und Extrapolationen sind mit hoher Unsicherheit behaftet. Es wird in der Studie kein Anspruch erhoben, dass die behandelte Mengengröße die Voraussetzungen für eine repräsentative Abbildung aller Kunden erlaubt. Eine Übertragung der Untersuchungsergebnisse vom Februar 2010 auf andere Zeiträume ist problematisch, da die Dienstanbieter immer wieder die technischen Abwehrmaßnahmen gegen Spam verändern und Spammer immer wieder neue Angriffsvarianten entwickeln. Darüber hinaus ist davon auszugehen, dass sich die Spam-Belastung zu späteren Lebensphasen eines Email-Kontos verändert, da sich die Rahmenbedingungen für die Email-Konten der betrachteten Testpersonen ändern werden. Ebenso kann man die Bedingungen der betrachteten Email-Konten zum Zeitpunkt Februar 2010 nicht auf die Bedingungen anderer Email-Konten übertragen.

Es wird interessant sein zu sehen, ob bzw. wie sich die Spam-Eigenschaften der jeweiligen Dienstanbieter für spätere Lebensphasen der Email-Konten verändern.

2 Einleitung und Motivation

Spam-Nachrichten werden von vielen als unerwünschte Nebenerscheinung der Internet-Nutzung wahrgenommen, welcher man als einzelner Benutzer scheinbar nichts wirklich Effektives entgegensetzen kann. Spam-Nachrichten gehören heute zum Alltag wie Werbung (persönlich adressiert oder unpersönlich) und kostenlose Zeitungen im Briefkasten, jedoch mit dem Unterschied, dass man sich als Einzelner gegen die Werbung im Briefkasten besser zur Wehr setzen kann, wie etwa mittels Abmahnungen (siehe z. B. `http://gruppen.greenpeace.de/aachen/werbung.html`). Die Abwehr von Spam ist aus vielen Gründen schwieriger.

Seit der Öffnung des Internets für Jedermann und für kommerzielle Angebote hat die Anzahl von verschickten Emails und der Umfang von Spam rasant zugenommen. Auch wenn keine Angaben über den genauen Gesamtumfang von Spam-Nachrichten vorliegen, so kann man trotz der Entwicklung vieler technischer Abwehrmaßnahmen von erheblichen Spam-Mengen ausgehen. Die Messung des tatsächlichen Spam-Umfangs ist praktisch unmöglich, doch liegen Schätzungen vor. Im Jahr 2005 wurde geschätzt, dass die Anzahl der Spam-Nachrichten in 2006 bereits einen Anteil von 85% am Gesamt-Email-Aufkommen ausmachen [17]. Schon 2004 hat man angenommen, dass die Anzahl der Spam-Nachrichten im Jahr 2015 mehr als 95% des Gesamt-Email-Aufkommens ausmachen wird [18]. Nach aktuellen Meldungen scheint diese Zahl bereits jetzt erreicht zu sein [1, 11]. So werden nach einer Schätzung in [1] heute schon von 100 versendeten Emails 80 direkt von den Email-Dienstanbietern als offensichtlicher Spam gelöscht und unter den verbliebenen 20 Emails sind immer noch durchschnittlich 15 unerkannte Spam-Nachrichten enthalten.

Die Zielsetzungen der Spammer für die Versendung von Spam-Nachrichten können sehr stark variieren:

- Werbung: Eine Zielsetzung besteht in dem Bewerben von Produkten oder Dienstleistungen per Email. Auch wenn es sich bei diesen Emails für deren Empfänger offensichtlich um Spam handelt, so kann es immer einmal wieder gelingen, dass aus dem Empfänger ein Kunde wird. Nach Untersuchungen in [12] liegt diese Konversionsrate noch unterhalb von einem Tausendstel Prozent. Das bedeutet, dass man aus Sicht des Spammers Millionen von Emails versenden muss, um nur einige Kunden zu bekommen.

- IT-Angriffe: Spam wird auch aus dem Grund versendet, um darüber IT-Angriffe zu ermöglichen. So verwenden Spammer Emails zur Verteilung von sogenannter Malware, wie z. B. Viren oder Trojaner. Damit können

die Spammer eine breite Palette von Angriffszielen verfolgen. So werden Benutzer durch Malware beispielsweise ausspioniert, es werden Zugangsdaten wie Passwörter im System abgefangen und an die Angreifer geschickt, um damit Identitätsdiebstahl zu begehen. Als anderes Beispiel kann die Modifikation von Computersystemen genannt werden, durch welche man den Computer für das Opfer praktisch unbenutzbar macht und die Modifikation erst gegen Zahlung einer Gebühr wieder rückgängig macht.

- Betrug: Mit Spam sind auch bereits viele Betrugsdelikte initiiert worden (z. B. Nigeria Connection) und dies geschieht auch nach wie vor. Dabei werden Email-Empfängern größere Summen Geld versprochen, z. B. wenn sie dem Absender aus einer Notsituation helfen. Bei diesen Fällen gehen die Empfänger darauf ein, in Hoffnung auf größere Gewinne in finanzielle Vorleistung zu treten. Auf die Rückzahlung der Beträge oder eine Gegenleistung warten die Empfänger dann vergeblich.

- Manipulation von Aktienkursen: Durch die massenweise Versendung von Spam kann es gelingen, auf die Entwicklung von Aktienkursen einzuwirken. Spammer versenden hierzu etwa Emails mit Kurszielen von entsprechenden Aktien und fügen Ausschnitte aus Pressemitteilungen von den jeweiligen Unternehmen an [14]. Nach Untersuchungen in [4] kann es Spammern gelingen, Veränderungen von Wertpapierkursen im Bereich einiger Prozent zu erzielen.

Außer der bloßen Tatsache, dass Spam-Nachrichten für die Empfänger einfach lästig sind, gibt es weitere negative Konsequenzen von Spam. In diesem Zusammenhang sind die folgenden Punkte anzuführen:

- Spam-Nachrichten verursachen in Unternehmen eine geringere Produktivität der Mitarbeit. Die Arbeitszeit, welche Mitarbeiter damit verbringen, ihre Spam-Nachrichten zu kontrollieren und zu löschen, steht nicht für produktive Zwecke zur Verfügung.

- Für den Internet Service Provider (ISP) entstehen Kosten zur Übertragung. Schlussendlich werden diese Kosten jedoch auf die Kunden umgewälzt.

- Für die Anbieter von Email-Diensten entstehen Kosten für Übertragung und Speicherplatz. Auch diese Kosten werden schlussendlich auf die Kunden umgewälzt.

- Werden infizierte Computer dazu missbraucht, selbst Spam-Nachrichten zu versenden, dann entstehen auch an dieser Stelle Kosten für die Besitzer dieser Computer.

- Anbieter von Email-Diensten sind gezwungen, Abwehrmaßnahmen zu ergreifen. Hierfür können gemäß [1] bei Anbietern größerer Email-Dienste Kosten von jährlich knapp 1 Million Euro anfallen.

- Wird mittels Spam Malware verschickt, dann können die finanziellen Risiken für den Empfänger der Email sehr hoch sein. Hierbei kommt es darauf an, welche Angriffsziele der Spammer verfolgt und welchen Wert die angegriffenen Ressourcen für einen Empfänger haben. Im Kontext von angegriffenen Unternehmenscomputern kann der Schaden leicht in die Höhe von Millionen Euros gehen, wie z. B. durch das Einschleusen von Trojanern zur Wirtschaftsspionage.
- Arbeiten die Abwehrmaßnahmen nicht korrekt, dann kann dies dazu führen, dass erwünschte Emails als Spam klassifiziert und somit gelöscht werden, so dass sie nie bei dem gewünschten Empfänger ankommen. Dies kann sowohl für den Sender als auch für den Empfänger sehr ärgerlich sein. Darüber hinaus kann dies dazu beitragen, dass Email nicht als verlässliches Kommunikationsmedium wahrgenommen wird.
- Die Tatsache, dass permanent Abwehrmaßnahmen gegen Spam angewendet werden, bedeutet auch, dass technische Systeme die für die Benutzer bestimmten Emails mitlesen, verarbeiten und ggf. auch zensieren. Dies gilt insbesondere auch für die Emails, bei welchen es sich nicht um Spam handelt.

Grundsätzlich bestehen verschiedene Maßnahmen zur Bekämpfung und Vermeidung von Spam. Diese lassen sich nach technischen und rechtlichen Maßnahmen unterscheiden. Zusätzlich existieren aus Sicht eines Benutzers auch noch Empfehlungen, wie Benutzer durch ihr Verhalten dazu beitragen können, nicht zu sehr in das Visier der Spammer zu geraten.

Auf der Seite der technischen Maßnahmen gibt es eine Reihe von Ansätzen, wie man die Flut von Spam eindämmen kann. In der Tat findet hier zwischen Spammern und Bekämpfern von Spam seit langer Zeit ein regelrechter Wettstreit statt. Ist eine neue Variante für Spam-Filter entwickelt, dann überlegen Spammer sich wieder neue Wege, wie sie die verbesserten Spam-Filter überlisten können. Dies führt dazu, dass auf beiden Seiten eine permanente Weiterentwicklung stattfindet. Auf tiefer gehende Beschreibungen technischer Lösungen soll an dieser Stelle verzichtet werden, für weitere Informationen sei auf die Ausführungen in [10] und [5] verwiesen. Es sei hier lediglich erwähnt, dass einige Abwehrmaßnahmen aus Sicht des Benutzers völlig transparent durchgeführt werden, so dass diese von den Benutzern nicht wahrgenommen werden. Andere Abwehrmaßnahmen sind für den Benutzer dadurch sichtbar, dass Konfigurationsmöglichkeiten für diese existieren. So können z. B. diejenigen Adressen angegeben werden, von denen keine Emails mehr erhalten werden sollen. Diese Abwehrmaßnahme ist gegen Spammer jedoch nur eingeschränkt wirksam, da diese unter vielen verschiedenen und sich ständig ändernden Adressen ihre Nachrichten verschicken, z. B. über sogenannte Botnetze. Solche Botnetze als Verbünde gekaperter Computer werden heute von Spammern ferngesteuert und versenden unter falschem Namen täglich Unsummen von Spam-Nachrichten. So versendete das Waledac-Botnetz bis zu einem erfolgreichen Gegenschlag durch seine Bekämpfer ca. 1,5 Milliarden Spam-Nachrichten täglich

[16]. Allgemein stellen Botnetze hinsichtlich Spam eine große Bedrohung dar. Nach [15] sind die Botnetze seit 2004 jährlich um rund 400% gewachsen. Würde man heute auf die technischen Abwehrmaßnahmen gegen Spam verzichten, dann wäre Email als Kommunikationsmittel nicht mehr gebrauchstauglich.

Aus rechtlicher Sicht bestehen mit Gesetzen und Strafen weitere Instrumente, welche —zumindest theoretisch— zur Eindämmung von Spam dienen können. Der bzgl. Spam relevante Rechtsrahmen unterscheidet sich hier jedoch von Land zu Land. Werden Spam-Nachrichten aus Ländern mit weniger strengem Rechtsrahmen versendet, bestehen kaum Möglichkeiten, mit Gesetzen und Strafen geeignet repressiv auf die Spammer einzuwirken. Auch wenn es in einigen Ländern extrem hohe Strafen für das Versenden von Spam gibt, so genügt das nicht, Spammer wirksam abzuschrecken [6, 7], da diese trotz drohender Strafen, die in bis zu dreistelligen Millionenbereichen liegen können, ihre Emails verschicken. Dies mag jedoch auch damit zu tun haben, dass viele Spammer in der Praxis ungestraft bleiben. Das rechtliche Instrumentarium kann in Sonderfällen neben finanzieller Bestrafung auch dahingehend angewendet werden, dass ganze Botnetze abgeschaltet werden, wie dies im Februar 2010 mit dem Waledac-Botnetz geglückt ist [16]. Juristen stellen jedoch fest, dass die Gesetze zur wirksamen Bekämpfung von Spam in Deutschland noch nicht streng genug sind [8].

Für die Empfehlungen, wie sich Benutzer verhalten sollen, um nach Möglichkeit nicht in das Visier der Spammer zu geraten, ist es sinnvoll, sich zunächst zu vergegenwärtigen, wie Spammer an die Email-Adressen gelangen. Aus einigen dieser Möglichkeiten lassen sich Handlungsempfehlungen ableiten.

- Erraten von Email-Adressen: Spammer gelangen in der Praxis häufig an gültige Email-Adressen, indem sie diese erraten. Werden Email-Adressen nach einem zu einfachen und konventionellen Muster gebildet wie z. B. `vorname.nachname@emaildienst.de`, dann können diese von den Spammern effizient erraten werden. Hierzu kombinieren Spammer gängige Vornamen und Nachnamen oder andere Begriffe, die mit höherer Wahrscheinlichkeit verwendet werden, und probieren aus, ob die entsprechenden Email-Adressen existieren, indem sie an diese Spam-Nachrichten versenden. Um die Trefferwahrscheinlichkeit zu erhöhen, können Spammer für ihre Suche nach Email-Adressen ein Telefonbuch verwenden. Selbst wenn Dienstanbieter Email-Adressen auf Basis einer internen Bildungsregel vorgeben, wobei die Komponenten weder in einem Telefonbuch noch einem anderen Buch zu finden sind, dann können die Email-Adressen geraten werden, wenn die tatsächlich gültigen Adressen in der Menge aller der Bildungsregel entsprechenden Kombinationen zu dicht liegen [3].

- Suche nach Email-Adressen: Da viele Adressen im Internet publiziert werden (z. B. Web-2.0-Angebote, Web-Auftritte von Unternehmen), suchen Spammer mit entsprechenden Suchmaschinen die Seiten des World Wide Web ab, um so an die Email-Adressen anderer zu gelangen.

- Handel mit Email-Adressen: Spammer erhalten Email-Adressen auch durch den Handel ganzer Sammlungen von Email-Adressen als regelrechte Produkte. Hierbei werden die Adressen auch mit Zusatzinformationen angeboten, indem diese klassifiziert werden, z. B. nach Interessen, Alter, Geschlecht ihrer Besitzer. Während der Durchführung der dieser Studie zugrunde liegenden Untersuchung haben die Autoren dieser Studie eine Spam-Nachricht erhalten, über welche ihnen der Erwerb von mehreren Millionen Email-Adressen angeboten wurde. Diese Nachricht wird in Abbildung 2.1 gezeigt. Ob es sich bei dieser Spam-Nachricht um ein echtes Angebot oder um einen Versuch eines Vorkassen-Betrugs handelt, wurde nicht überprüft.

- Zugriff auf fremde Adressbücher: Mittels eingeschleuster Malware können Angreifer auf die Adressbücher der angegriffenen Computernutzer zugreifen. Die darin enthaltenen Email-Adressen können dann zur Versendung von Spam-Nachrichten verwendet werden. Dieses Prinzip wird auch bei Internet-Würmern angewendet.

- Sammlung von Adressen über Lockangebote: Spammer gelangen auch über Lockangebote an Email-Adressen. Hierzu werden beliebige Objekte, wie z. B. Dokumente, Benutzern nur dann zum Herunterladen angeboten, wenn diese sich zunächst bei dem Anbieter mit ihrer Email-Adresse registrieren. Andere Angebote zum Sammeln von Email-Adressen bieten Benutzern an, nach Eingabe der Email-Adressen von Freunden oder Bekannten an diese Emails zu versenden wie z. B. elektronische Grußkarten, Hinweise mit Informationen zu bestimmten Themen, für welche diese sich interessieren. Solche Angebote machen sich die Unwissenheit und die Bequemlichkeit von Benutzern zu Nutze, indem diese aus einer Web-Seite heraus durch einfache Eingabe einer Email-Adresse eine Email verschicken können. Der Sammler bekommt jedoch durch die Verknüpfung einer Email-Adresse mit einem Thema eine klassifizierte Email-Adresse.

Aus dieser sicherlich nicht vollständigen Liste von Möglichkeiten, wie Spammer an Email-Adressen gelangen können, lassen sich Handlungsempfehlungen ableiten, was man beim Umgang mit seiner Email-Adresse bedenken und berücksichtigen sollte.

- Die Email-Adresse sollte nicht zu leicht erratbar sein. Insbesondere sollte sie nicht einem konventionellen Adressmuster folgen, auch auf die Gefahr hin, dass andere sich die Adresse weniger gut merken können.

- Man sollte seine Adressen nicht für Suchmaschinen lesbar im Internet publizieren.

- Man sollte gut überlegen, an wen man seine Adresse herausgibt. Insbesondere sollte man seine Email-Adresse nicht bei Lockangeboten preisgeben. Tritt man mit einem Anbieter nur einmal in Kontakt, dann ist die Verwendung von Wegwerfadressen sinnvoll, für welche es im Internet mittlerweile zahlreiche Angebote gibt.

Abbildung 2.1: Auszüge aus einer Spam-Nachricht zum Handel mit Email-Adressen

Datum: 14.02.2010 17:37
Betreff: Wir verkaufen rund 6,5 Millionen deutsche Email-Adressen interessiert?

Hallo,

Wir verkaufen rund 6,5 Millionen deutsche Email-Adressen aus Deutschland 100% alle gültig (keine Rückläufer) Die Email-Adressen setzen sich wie folgt zusammen

Rund 2,5 Millionen @t-online.de Emails
Rund 1,9 Millionen @web.de Emails
Rund 500000 @freenet.de Emails
Rund 400000 @gmx.de Emails
Rund 400000 @hotmail.com Emails

Dazu noch rund 700000 Emails von anderen deutschen Email-Providern

Die Emails sind in folgende Kategorien sortiert:

Kategorien

Auto
Handy
⋮

Interessen

Adult
Business & Investition
⋮

Alle Emails wurden im douple-opt-in Verfahren gesammelt nach den strengen Regeln des Datenschutzes. Die Empfänger haben der Zusendung von Emails durch dritte zugestimmt daher erwerben sie die Emails völlig legal. Sie erhalten zu jeder Email auch den Vornamen,Nachnamen,Adresse,Geschlecht und sie bekommen auch eine Lizenz im pdf Format geliefert das sie die Emails benutzen dürfen.

Der Preis beträgt 1000 Euro inkl. Mwst. Bezahlung ist nur mit Überweisung möglich. Die Emails bekommen sie auf einer DVD mit der Post geliefert nach dem sie bezahlt haben (Vorkasse). Die Emails sind eher für solche Leute oder Firmen gedacht die etwas verkaufen und neue deutsche Kunden gewinnen wollen. Wenn sie interessiert sind die Emails zu kaufen senden sie eine Email an folgende Email-Adresse:

info@optinmails.net

Bitte geben sie Ihre Rechnungs und Lieferadresse bekannt wohin wir die DVD verschicken solllen.

Mit freundlichen Grüssen

- Man sollte auch vertrauensvoll mit den Email-Adressen von Freunden und Bekannten umgehen. Insbesondere sollte man keine Angebote nutzen, bei welchen man deren Email-Adressen unbekannten Dritten bekanntmacht.
- Versendet man Emails an einen größeren Kreis von Adressaten, dann empfiehlt es sich, diese als BCC anzugeben.
- Man sollte auf keinen Fall auf eine Spam-Nachricht antworten. Dadurch bestätigt man dem Spammer, dass die Email-Adresse tatsächlich genutzt wird. Vor diesem Hintergrund sind auch die automatisch generierten Antworten (z. B. Out-of-Office Reply) als kritisch zu betrachten und man sollte im Einzelfall abwägen, ob und wann die Einrichtung einer automatisch generierten Antwort tatsächlich notwendig ist.

Grundsätzlich sollte einem Benutzer beim Umgang mit seiner Email-Adresse

klar sein, dass er bei den heutigen Rahmenbedingungen Informationen, die einmal freigegeben sind, nicht mehr zurückholen kann. Ist also eine Email-Adresse Spammern bekannt, dann ist davon auszugehen, dass das Spam-Aufkommen für diese Adresse in der Zukunft kontinuierlich zunehmen wird. Dies zeigt auch eine Untersuchung in [2] aus dem Jahr 2007. Dort wurde ermittelt, wie die Spam-Belastung für Email-Adressen über der Zeit zunimmt. Dies ist auch schon deshalb offensichtlich, da beim Handel mit Email-Adresslisten diese immer wieder an neue Abnehmer gegeben, von diesen mehrfach benutzt und ggf. auch von diesen an andere weitergegeben werden.

Nachdem sich viele Benutzer nun schon länger als ein Jahrzehnt über Spam per Email ärgern, sind mittlerweile neue Formen von Spam-Bedrohungen entstanden, die auf anderen Kommunikationsmedien aufsetzen, wie z. B. Blogs und anderen Web-2.0-Angeboten oder Instant Messaging. Beschreibungen dieser Bedrohungen sind z. B. in [9, 13] zu finden. Auch in diesem Bereich müssen geeignete technische Abwehrmaßnahmen entwickelt werden, wenn diese Kommunikationsmedien noch stärker in das Visier von Spammern geraten.

3 Gegenstand der Studie

3.1 Begriffsbestimmung und Abgrenzung

Gegenstand der Studie ist die Untersuchung des Spam-Aufkommens bei kostenfreien Email-Diensten verschiedener Anbieter. Der Begriff »Spam« umfasst hierbei alle Nachrichten, die einem Empfänger unverlangt zugestellt werden und häufig werbenden Inhalt haben. Hierzu können auch Nachrichten gehören, welche von dem Dienstanbieter selbst an die eigenen Kunden verschickt werden. Nun fallen jedoch nicht sämtliche Emails, welche von einem Dienstanbieter an die eigenen Kunden versendet werden, gleichermaßen in die Kategorie »Spam«. Vor diesem Hintergrund ist es wichtig, dass klar abgegrenzt wird, welche Nachrichten zur Kategorie »Spam« gehören und welche nicht.

Das Kriterium, dass eine empfangene Email »unverlangt« zugestellt wurde, ist zur Kategorisierung der Email als »Spam« von entscheidender Bedeutung. Es ist jedoch nicht in allen Fällen ganz einfach zu entscheiden, ob das Kriterium »unverlangt« erfüllt ist. Hierzu ist zu berücksichtigen, inwieweit ein Benutzer bei dem jeweiligen Dienst in der Lage ist, die eigenen Entscheidungen bzgl. »unverlangt« in den Optionen oder Einstellungen des Dienstangebots entsprechend zu konfigurieren. Dies kann sich sowohl auf die grundsätzliche und theoretische Konfigurationsmöglichkeit für Benutzer beziehen, einen bestimmten Typ von Nachrichten als »unverlangt« zu kategorisieren, als auch auf die eher praktisch orientierte Frage, inwieweit ein durchschnittlicher Benutzer dazu in der Lage ist oder den Aufwand aufbringen möchte, den Dienst entsprechend seiner persönlichen Wünsche zur Spam-Vermeidung zu konfigurieren, z. B. wenn bestimmte Optionen zur Konfiguration dessen, was unverlangt ist, nur sehr schwierig zu finden sind. Insofern ist nicht immer davon auszugehen, dass all das, was sich gemäß den Konfigurationsmöglichkeiten für einen Benutzer als »verlangt« darstellt, auch tatsächlich »verlangt« ist. Es ist also durchaus möglich, dass Emails zur Kategorie »unverlangt« gehören, auch wenn diese in der Praxis nicht als »unverlangt« konfiguriert wurden.

Sicherlich könnte man auch den entgegengesetzten Standpunkt vertreten, dass alle Emails, welche gemäß der Konfiguration des Benutzers nicht explizit als »unverlangt« klassifiziert sind, tatsächlich als »verlangt« zu bewerten sind. Als Konsequenz würde dies jedoch bedeuten, dass es bei einem Dienst, welcher für bestimmte Emails keine Konfigurationsmöglichkeit als »unverlangt« anbietet, keinen Spam geben kann, da sich der Benutzer durch die Entscheidung für einen Dienstanbieter auch für den Bezug von entsprechenden Emails entschieden hat. Würde man eine solche Argumentationsweise zur Abgrenzung von

Spam zugrunde legen, dann wäre dies sicher wenig sinnvoll, da es in strenger Konsequenz bedeuten würde, dass man zur Verbesserung der Spam-Eigenschaften eines Dienstes auf die Konfigurationsmöglichkeiten hinsichtlich »unverlangt« verzichten sollte.

Es ist jedoch gänzlich anders zu bewerten, wenn für einen Benutzer eine einfach wahrzunehmende Wahlfreiheit besteht und er aufgrund von expliziten wahlfreien Entscheidungen Emails mit werbendem Inhalt erhält. Willigt ein Benutzer also auf eine konkrete Anfrage seines Dienstanbieters explizit ein, dass er einen bestimmten Typ von Informationsmaterial erhalten möchte (z. B. Newsletter), dann handelt es sich bei den darauf folgenden Nachrichten nicht um Spam, da das Kriterium »unverlangt« hier keinesfalls zutrifft. Erfolgt die Einwilligung für die Zustellung eines bestimmten Typs von Informationsmaterial jedoch im Rahmen der Anerkennung der geltenden Allgemeinen Geschäftsbedingungen (AGB) des Dienstanbieters durch den Kunden ohne direkte Option für Opt-in oder Opt-out, dann kann man diese implizite Anerkennung in Abgrenzung dazu nicht dahingehend interpretieren, als wäre das Informationsmaterial erwünscht, so dass auch bei einer in solcher Form erhaltenen Einwilligung davon auszugehen ist, dass das Kriterium »unverlangt« zutrifft. Hier ist grundsätzlich davon auszugehen, dass ein Kunde den AGB notgedrungen zustimmt, da er in erster Linie den Email-Dienst nutzen möchte, und nicht, weil er sich entsprechende Informationsmaterialien wünscht.

3.2 Perspektive der Benutzer

Spam stellt für viele Benutzer ein lästiges Problem dar. Die Bearbeitung von Spam verursacht für die Benutzer einen unerwünschten Mehraufwand. Dies gilt in der Regel unabhängig davon, ob Spam in der Inbox als Postfach für erwünschte Nachrichten oder einer Spambox als Quarantäne-Postfach empfangen wird. Da nicht auszuschließen ist, dass erwünschte Nachrichten in die Spambox verschoben werden, kontrollieren Benutzer in bestimmten zeitlichen Abständen auch die Inhalte der Spambox, so dass die von der Technik vorgenommene Vorsortierung der empfangenen Nachrichten nach Inbox und Spambox kaum Aufwandsreduktion mit sich bringt, da ohnehin sämtliche Nachrichten überprüft werden. Ist der Speicherplatz zur Aufbewahrung empfangener Nachrichten stark beschränkt, dann kann gespeicherter Spam dazu führen, dass der zur Verfügung stehende Speicher aufgebraucht ist und keine weiteren Nachrichten entgegengenommen werden können, selbst wenn diese erwünscht sind.

Eine organisatorische, jedoch in der Praxis leider nur eingeschränkt wirksame Maßnahme zur Vermeidung von Spam besteht darin, die eigene Email-Adresse nur in sehr geringem Maße bekannt zu machen, d. h. die Adresse nur an wenige bzw. ausgewählte andere weiterzugeben. Dies kann jedoch nur bedingt erfolgreich sein, da Email-Adressen der Kommunikation dienen und somit zwangsläufig anderen zur Verfügung gestellt werden. Man wird heute bei der Nutzung sehr vieler Web-Angebote (z. B. Online-Shops, Registrierung in Online

Communities) aufgefordert, seine Email-Adresse anzugeben. Ohne Registrierung und Angabe der Email-Adresse bleibt man oftmals ganz oder teilweise von der Nutzbarkeit des Leistungsumfangs der Web-Angebote ausgeschlossen. Jedoch hat man nicht unter Kontrolle, wie andere mit der eigenen Email-Adresse umgehen. Es gibt im Internet viele Angebote, wie beispielsweise elektronische Grußkarten oder Seiten, auf denen man Empfehlungen an Interessierte versenden kann, und bei welchen Benutzer mit besten Absichten Email-Adressen von Bekannten und Freunden eingeben können. Leider lässt sich die Verwendung der so zur Verfügung gestellten Email-Adressen nicht mehr kontrollieren. So ist nicht auszuschließen, dass diese entweder direkt für Spam-Zwecke verwendet werden oder weitergegeben werden.

Selbst wenn Email-Adressen Spammern gar nicht zur Verfügung gestellt werden, so können Spammer diese durch einfaches Ausprobieren herausfinden. Dies wird durch typische Vorlieben von Benutzern erleichtert. Ein typischer Benutzer bevorzugt eine solche Email-Adresse, welche sich aus Begriffen einer natürlichen Sprache zusammensetzt (z. B. Vor- und Nachname) und nicht aus einer kryptischen Zeichenfolge besteht, welche durch wiederholte zufällige Auswahl von beliebigen Zeichen zustande gekommen ist. Genau dieser Umstand wird jedoch von Spammern ausgenutzt, indem unter Berücksichtigung von sogenannten Wörterbüchern und einigen weiteren Tricks wie Ersetzung und Variation von Buchstaben durch andere Zeichen entsprechende Zeichenketten generiert werden und durch Spam-Versand getestet wird, ob es sich dabei um existierende Email-Adressen handelt. Dadurch ist der Aufwand für Spammer zum Herausfinden von Email-Adressen sehr viel geringer als durch vollständige Suche, bei welcher alle kombinatorischen Möglichkeiten von Email-Adressen vorgegebener Längen getestet werden müssten.

Mit welcher Wahrscheinlichkeit Spam empfangen wird, hängt neben den technischen Vorkehrungen des Dienstanbieters und vom Nutzerverhalten auch von der Attraktivität des Dienstanbieters für Spammer ab. Es ist davon auszugehen, dass Dienstanbieter mit einer sehr großen Kundenbasis ein sehr viel interessanteres Ziel für Spammer darstellen als Dienstanbieter mit einer eher kleinen Anzahl von Kunden. Bei einem Dienstanbieter mit einer sehr großen Kundenbasis ist die Versendung von Spam an Email-Adressen, welche aus Wörterbüchern generiert wurden, mit einer sehr viel größeren Wahrscheinlichkeit erfolgreich als beim Austesten von Kombinationen für Email-Adressen bei weniger bedeutenden Anbietern mit einer geringeren Anzahl an Kunden.

Besteht zum Zeitpunkt der Spam-Versendung für den Spammer eine Unsicherheit, ob die verwendete Email-Adresse überhaupt existiert oder aktiv genutzt wird, dann sollte der Empfänger der Email unbedingt darauf achten, dass diese Unsicherheit für den Spammer bestehen bleibt. Wird die Existenz oder die aktive Verwendung einer Email-Adresse jedoch durch eine Rückantwort bestätigt, z. B. durch eine automatisch generierte Nachricht wie einen Out-Of-Office Reply, dann verschwindet die Unsicherheit aus Sicht des Spammers und dieser wird die Email-Adresse für zukünftige Spam-Aktionen berücksichtigen.

Als Benutzer hat man in der Praxis wenig rechtliche Möglichkeiten gegen Spammer vorzugehen. Spammer wählen sich zur Durchführung ihrer Aktionen oftmals Computer aus, welche sich im Hoheitsgebiet anderer Staaten befinden, so dass ein rechtliches Vorgehen gegen die Urheber schwierig oder praktisch unmöglich ist. Das Wissen darüber, dass keinerlei Repression zu befürchten ist, ermuntert Spammer dann zu weiteren Aktionen.

Ist die Email-Adresse eines Benutzers in den Adresslisten von Spammern enthalten, hat man als Benutzer in der Praxis wenig effektive Möglichkeiten, den Empfang von weiterem Spam zu vermeiden. Leider gibt es für den Benutzer keine Lösung, mittels derer die eigene Email-Adresse aus den Adresslisten von Spammern gelöscht werden kann. Die Möglichkeit, als Benutzer bestimmte Absenderadressen zu blockieren, ist dabei nur eingeschränkt zielführend, da Spammer ihre Nachrichten von unterschiedlichen Absenderadressen verbreiten. Als Benutzer ist man hier auf die technischen Systeme zur Spam-Abwehr von Dienstanbietern oder auch Mail-Clients angewiesen.

3.3 Prinzipielle Maßnahmen von Dienstanbietern zur Abwehr von Spam

Um eine entsprechende Dienstqualität anbieten zu können, müssen Anbieter technische Vorkehrungen zur Abwehr treffen. Grundsätzlich können Dienstanbieter verschiedene Abwehrmaßnahmen zur Bekämpfung von Spam bzw. auch Kombinationen dieser Abwehrmaßnahmen einsetzen. Die Abwehrmaßnahmen gegen Spam lassen sich grob in zwei Kategorien einteilen, wie auch in Abbildung 3.1 gezeigt wird:

- Allgemeiner Spam-Filter
- Persönlicher Spam-Filter

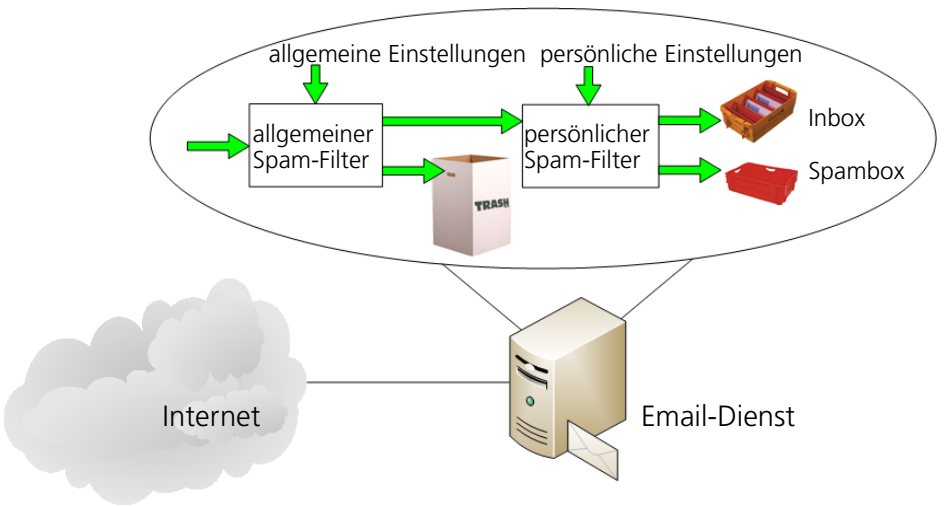


Abbildung 3.1: Kombination von Abwehrmaßnahmen gegen Spam bei Dienstanbietern

Im allgemeinen Spam-Filter wird unabhängig von Benutzereinstellungen ankommender Spam abgewehrt und gekennzeichnet. Zum Erreichen dieses Ziels können verschiedene Mechanismen zur Anwendung kommen, mittels derer ankommende Emails als Spam klassifiziert werden können. In diesem Zusammenhang können beispielsweise die IP-Adressen der Absender oder der Mail-Server auf das Vorkommen in allgemeinen Sperrlisten (Blacklists) überprüft werden. Eine andere Möglichkeit besteht in der maschinellen Überprüfung des Inhalts einer Email auf typische Signalwörter. Wird eine Email von einem allgemeinen Spam-Filter als Spam klassifiziert, wird sie bei hoher Entscheidungssicherheit direkt gelöscht oder bei geringerer Entscheidungssicherheit durchgelassen.

Hat eine Email den allgemeinen Spam-Filter durchlaufen ohne gelöscht zu werden, dann werden die Mechanismen des persönlichen Spam-Filters auf die Email angewendet. Prinzipiell werden hier ähnliche Überprüfungen wie bereits im allgemeinen Spam-Filter vorgenommen, jedoch sind diese vom Benutzer in einem vom Dienstanbieter abhängigen Umfang individuell für die empfangenen Emails einstellbar. Entsprechend der hier vorgenommenen Einstellungen oder bei Übernahme der Standardeinstellungen des Anbieters werden die empfangenen Emails klassifiziert. Entsprechend dieser Klassifikation werden die empfangenen Emails entweder in der Inbox oder in der Spambox abgelegt. Es gibt auch Anbieter, die mit einer zusätzlichen dritten Box arbeiten. In diese Box werden alle diejenigen Emails abgelegt, bei denen nicht klar entschieden werden kann, ob sie in der Inbox oder der Spambox abzulegen sind.

Die richtige Auswahl der persönlichen Einstellungen vorzunehmen ist für Benutzer nicht immer einfach. Hierzu muss zunächst einmal die richtige Stelle im Portal des Dienstanbieters gefunden werden, an welcher die persönlichen Einstellungen vorgenommen werden können. Darüber hinaus muss ein Benutzer zur Auswahl einer für ihn möglichst optimalen Einstellung die Auswirkung der ihm angebotenen Handlungsalternativen verstehen können. Das impliziert jedoch auch, dass das jeweilige subjektive Verständnis eines Benutzers bzgl. der Auswirkung von Handlungsalternativen dem Ergebnis der Anwendung entsprechender technischer Funktionen möglichst nahe kommt. Aus Sicht eines Dienstanbieters stellt dies ein schwieriges Problem dar, muss es ihm doch gelingen, die Konfiguration des persönlichen Spam-Filters für eine sehr heterogene Kundenbasis bzgl. technischem Hintergrundwissen intuitiv benutzbar zu machen. Bei unbedarften Benutzern kann es leicht geschehen, dass sie ohne konkreten Spam-Vorfall verunsichert sind, welche Einstellung sie wählen sollten, sofern sie die Stelle gefunden haben, an welcher sämtliche Eigenschaften des persönlichen Spam-Filters konfiguriert werden können. Es ist somit oftmals hilfreich, wenn Benutzer ausgehend von bestimmten empfangenen Spam-Nachrichten die Einstellungen des persönlichen Filters anpassen können, z. B. um eine als »Spam« klassifizierte Email zukünftig in der Inbox zu empfangen. Solche fallbezogenen Einstellungsmöglichkeiten des persönlichen Spam-Filters sind aus Sicht eines Benutzers unzweifelhaft wünschenswert, ob sie jedoch tatsächlich genutzt werden können, hängt davon ab, in welcher Form diese fallbezogenen Einstellungsmöglichkeiten angeboten werden und mit welchem Werkzeug der Benutzer seine Emails

liest. Werden die fallbezogenen Einstellungsmöglichkeiten ausschließlich außerhalb der Email z. B. auf der Web-Oberfläche des Dienstes angeboten und liest der Benutzer seine Emails mit einem Browser auf dieser Web-Oberfläche, dann kann er von den fallbezogenen Einstellungsmöglichkeiten bei Bedarf Gebrauch machen, da ihm diese offensichtlich dargestellt werden. Liest, schreibt und verwaltet der Benutzer seine Emails jedoch ausschließlich mit einem typischen Email-Programm (z. B. Mozilla Thunderbird, Microsoft Outlook), dann erlangt er ggf. keine Kenntnis über die vorhandenen fallbezogenen Einstellungsmöglichkeiten. Werden diese von dem Dienstanbieter in Form von anklickbaren Links an die entsprechenden Emails angehängt, dann kann unabhängig vom aktuell verwendeten Tool von den fallbezogenen Einstellungsmöglichkeiten für den persönlichen Spam-Filter Gebrauch gemacht werden.

Die Anwendung von Spam-Abwehrmaßnahmen auf empfangene Emails kann unterschiedliche Effekte haben. So können empfangene Emails korrekt oder auch falsch klassifiziert werden. Einen Überblick über die in diesem Zusammenhang möglichen Fälle bietet Tabelle 3.1.

Tabelle 3.1: Bewertung der Spam-Klassifikation

	empfangene Email ist Spam	**empfangene Email ist kein Spam**
als Spam erkannt	kein Fehler (Correct Positive)	Fehler (False Positive)
nicht als Spam erkannt	Fehler (False Negative)	kein Fehler (Correct Negative)

Handelt es sich bei einer empfangenen Email um Spam und wird diese als »Spam« klassifiziert, dann ist die vorgenommene Klassifikation korrekt (Correct Positive). Handelt es sich bei einer empfangenen Email nicht um Spam und wird diese auch nicht als »Spam« klassifiziert, dann ist die vorgenommene Klassifikation ebenfalls korrekt (Correct Negative). Diese beiden Fälle sind aus Sicht eines Benutzers erwünscht.

Wird jedoch eine Spam-Nachricht empfangen und wird diese nicht als »Spam« erkannt, dann landet sie in der Inbox, was aus Sicht des Benutzers unerwünscht ist. Diesen Fehler bezeichnet man als »False Negative«. Wird hingegen eine Nachricht empfangen, bei der es sich nicht um eine Spam-Nachricht handelt, welche jedoch fälschlicherweise als »Spam« klassifiziert wird, dann landet diese Email entweder in der Spambox oder sie erreicht den Benutzer überhaupt nicht. Diesen Fehler bezeichnet man als »False Positive«.

3.4 Spektrum von Ansätzen zur Untersuchung von Spam-Eigenschaften

Wenn man eine Studie zur Untersuchung von Spam-Eigenschaften durchführt, sind grundsätzlich mehrere Ansätze möglich. Zunächst kann die Durchführung

dahingehend unterschieden werden, in welcher Weise in die Abläufe eingegriffen werden darf. Hier werden die folgenden Kategorien unterschieden:

- »passiv«
- »aktiv«

Im Fall »passiv« betätigt sich der Untersuchende ausschließlich als Betrachter, der nicht in das System eingreift. Er betrachtet lediglich, wie das System auf die Eingaben anderer reagiert. Insbesondere versendet er im Rahmen der Untersuchung keine Emails an die zu Untersuchungszwecken eingerichteten Email-Adressen. Es wird also ausschließlich das Verhalten des Systems auf Emails anderer bewertet.

Im Fall »aktiv« ist es dem Untersuchenden erlaubt, selbsttätig Eingaben für das zu untersuchende System zu generieren, um zu betrachten, wie das System auf seine Eingaben reagiert. Insbesondere bedeutet dies, dass zur Durchführung Spam verschickt werden kann.

Bei einer Untersuchung kann man auch unterscheiden, auf welche Stellen bzw. Komponenten des untersuchten Systems der Untersuchende Zugriff hat und welche internen Systeminformationen ihm vorliegen. Hier kann man die folgenden Kategorien unterscheiden:

- White-Box-Ansatz
- Black-Box-Ansatz

Bei einem White-Box-Ansatz liegen dem Untersuchenden alle für die Untersuchung relevanten Informationen vor. Darüber hinaus kann er in dem zu untersuchenden System nach Wunsch und Notwendigkeit beliebig viele Messpunkte setzen und diese nutzen, um Aussagen über die Eigenschaften des Systems gewinnen zu können. Bei einem White-Box-Ansatz ist es beispielsweise möglich zu erkennen, dass eine empfangene Email aufgrund von allgemeinen Spam-Filtereinstellungen als »Spam« klassifiziert wird. Somit ist auch klar, dass ein White-Box-Ansatz im Spam-Zusammenhang eine enge Kooperation mit dem Dienstanbieter erfordert und natürlich auch dessen Bereitschaft, offen Auskünfte zu geben und beliebige systeminterne Messpunkte zu gestatten.

Im Black-Box-Ansatz hingegen liegen dem Untersuchenden keine internen Systeminformationen vor und es können auch keine beliebigen internen Messpunkte im System gesetzt werden. Das System kann lediglich durch Beobachtung des Systemausgangs untersucht werden. Bei einem Black-Box-Ansatz bleibt dem Untersuchenden beispielsweise die Tatsache verborgen, dass eine empfangene Email wegen der allgemeinen Spam-Filtereinstellungen als »Spam« klassifiziert wurde, sofern der Untersuchende keine Kenntnis von der Existenz der Email hat. Dies ist offensichtlich, da in diesem Ansatz der Untersuchende lediglich Zugriff auf die Inbox und die Spambox hat. Wie viele Emails bereits vorher herausgefiltert wurden, kann der Untersuchende nicht in Erfahrung bringen. Im Zusammenhang einer Spam-Untersuchung kann man einen Black-Box-

Ansatz auch ohne offene Kooperationsbereitschaft eines Dienstanbieters durchführen.

Darüber hinaus sind je nach Ziel und Gegenstand der Untersuchung unterschiedliche Betrachtungsobjekte relevant. Insofern können verschiedene Bewertungen zur Spam-Klassifikation im Vordergrund stehen, wie z. B.

- Anzahl der korrekten Entscheidungen bei der Spam-Klassifikation (Correct Negatives + Correct Positives),
- Anzahl der False Negatives zur Bewertung, wie viele Spam-Nachrichten nicht als solche erkannt wurden,
- Anzahl der False Positives zur Bewertung, wie viele Nicht-Spam-Emails dem Benutzer vorenthalten wurden,
- Anzahl der falschen Entscheidungen bei der Spam-Klassifikation (False Negatives + False Positives),
- viele weitere Kombinationen oder Verhältnisse dieser Anzahlen.

An dieser Stelle wird nun auch deutlich, dass man bei gegebener Zielsetzung der Untersuchung in der Auswahl seines Ansatzes nicht ganz frei ist. Geht es beispielsweise darum, die Eigenschaften eines Mail-Dienstes hinsichtlich False Positives zu bewerten, dann ist dies nicht im Rahmen einer Black-Box-Analyse möglich, bei der sich der Untersuchende rein passiv verhält und lediglich Zugriff auf die Ausgabe des zu untersuchenden Systems hat. Geht man von der Annahme aus, dass die Untersuchung im Rahmen einer Black-Box-Analyse durchgeführt werden soll und der Untersuchende sich rein passiv verhalten soll, was auch impliziert, dass er keine Aufträge an andere vergibt, aktiv einzugreifen, dann sind umfassende Untersuchungen der Spam-Filter hinsichtlich False Positives nicht möglich.

Die Möglichkeiten des Untersuchenden, welche sich aus den bestehenden Rahmenbedingungen ergeben, und der in Abhängigkeit davon gewählte Untersuchungsansatz bedingen somit das erreichbare Ziel der Untersuchung.

3.5 Rahmen, gewählter Ansatz und Ziel der Untersuchung

Für den Rahmen der Untersuchung ist festzuhalten, dass diese unter gleichen Bedingungen, unparteiisch, fair, objektiv, transparent und für Dritte nachvollziehbar durchgeführt wurde. Der Rahmen der vorliegenden Studie ist durch den beschränkten Ressourcenumfang von ca. einem Personenmonat gegeben, welcher zur Durchführung der Untersuchungen zur Verfügung steht. Innerhalb dieses Rahmens muss die Untersuchung geplant, initialisiert, Messwerte aufgenommen und ausgewertet und die vorliegende Beschreibung verfasst werden. Da die Durchführung der Untersuchung nicht auf Kooperationen mit den untersuchten Dienstanbietern basiert, stehen lediglich solche Informationen bereit, welche auch normalen Kunden dieser Dienstanbieter zur Verfügung stehen.

Ebenso kann bei der Untersuchung auch nur auf dieselben technischen Systeme und in gleicher Weise zugegriffen werden, wie das auch einem normalen Kunden möglich ist. Darüber hinaus wird ausgeschlossen, dass sich die Untersuchenden als Spammer betätigen. Ebenfalls wird ausgeschlossen, dass die Untersuchenden Spam-Aufträge an andere vergeben.

Aus diesem Rahmen ergibt sich, dass die Untersuchung als passiver Black-Box-Ansatz durchgeführt wird. Ausgehend davon besteht das Hauptziel der Untersuchung darin, festzustellen, in welchem Umfang man als Kunde welches Dienstanbieters durch den Empfang von Spam-Nachrichten beeinträchtigt wird. Hierbei werden sowohl Spam-Nachrichten berücksichtigt, die von unbekannten Absendern versendet werden, wie auch solche, die von dem Anbieter selbst stammen. Wenn Spam-Nachrichten empfangen werden, dann ist das Ziel, für die verschiedenen Dienstanbieter zu vergleichen, in welchem Umfang diese jeweils in der Spambox anstatt der Inbox empfangen werden.

Damit für eine faire Untersuchung die gleichen Rahmenbedingungen gelten, wurde bei der Auswahl der in der Untersuchung verwendeten Email-Adressen große Sorgfalt angewendet. Ebenfalls wurde bei den publizierten Email-Adressen darauf geachtet, dass durch die gewählten Publikationsstellen und -zeiten keiner der Anbieter gegenüber seinen Wettbewerbern benachteiligt wird. In diesem Zusammenhang war zu gewährleisten, dass die Voraussetzungen für Spammer, an die in der Untersuchung eingesetzten Email-Adressen zu gelangen, für alle bei den verschiedenen Dienstanbietern genutzten Email-Adressen gleich sind. Hierzu wurden die bei den verschiedenen Dienstanbietern genutzten Email-Adressen jeweils über dieselben Web-Portale publiziert. Um gleiche Voraussetzungen zu schaffen, konnten keine bestehenden Email-Adressen verwendet werden; diese wurden stattdessen vor der Untersuchung quasi zeitgleich angelegt. Zur Schaffung möglichst gleicher Rahmenbedingungen war es auch erforderlich, dass die angelegten Email-Adressen nicht an anderen Stellen publiziert wurden, womit sich in zufälliger Weise unterschiedliche Bedingungen hinsichtlich Verwendung der Email-Adressen für Spam-Zwecke hätten ergeben können.

Grundsätzlich ist eine niedrige Gesamtanzahl von Spam-Nachrichten wünschenswert, da somit der Kontrollaufwand bzgl. empfangener Emails für den Benutzer niedrig ist. Ergibt sich hier bei der Untersuchung eine niedrige Zahl für einen Anbieter, dann lässt sich dies dahingehend deuten, dass entweder die Spam-Filter des Anbieters während des Untersuchungszeitraums gut funktionierten oder dass der Anbieter während des Untersuchungszeitraums einem weniger starken Spam-Verkehr ausgesetzt war. Welche Argumentation hier die zutreffendere und für das gemessene Ergebnis relevanter ist, kann die Untersuchung nicht beantworten. Auf den Untersuchungszeitraum bezogen kommt es einem Benutzer in der Praxis jedoch weniger auf die Begründungen für das Spam-Aufkommen an als vielmehr auf eine niedrige Anzahl von Spam-Nachrichten.

3.6 Was wird betrachtet?

Bei der Durchführung der Untersuchung werden ausschließlich die empfangenen Spam-Nachrichten betrachtet. Für einen eindeutigen Sprachgebrauch und zur eindeutigen Klassifikation von Nachrichten ist es wichtig, darauf hinzuweisen, dass auf diese Spam-Nachrichten sowohl die Einstellungen des allgemeinen als auch des persönlichen Spam-Filters angewendet wurden. Für die Klassifikation dieser Nachrichten sind gemäß der zweiten Spalte in Tabelle 3.1 die folgenden Kategorien relevant:

- False Negatives
- Correct Positives

Die Betrachtung der False Negatives kann in einfacher Weise durchgeführt werden. Es handelt sich hierbei um Spam-Nachrichten, welche in der Inbox eines Email-Kontos empfangen werden. Insbesondere werden in dieser Studie intern verschickte Spam-Mails als False Negatives betrachtet.

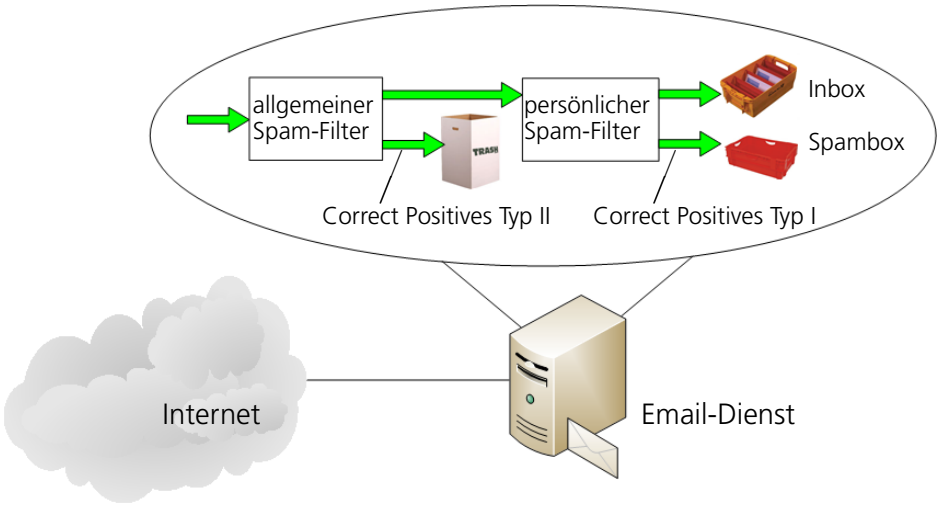
Bei der Untersuchung ist ebenfalls die Betrachtung der Correct Positives von Interesse. Im Rahmen der Untersuchung kann jedoch nur ein Anteil der Correct Positives betrachtet werden, nämlich diejenigen Spam-Nachrichten, die nach Filterung in der Spambox abgelegt werden. Diese werden hier »Correct Positives Typ I« genannt (siehe Abbildung 3.2). Spam-Nachrichten, die bereits von dem allgemeinen Spam-Filter als »Spam« erkannt und gelöscht werden, zählen ebenfalls zu den Correct Positives. Diese stellen jedoch einen Anteil von Correct Positives dar, welcher im Rahmen der hier durchgeführten passiven Black-Box-Analyse nicht betrachtet werden kann, da bei der Untersuchung keine Möglichkeiten zur Verfügung stehen, anhand derer man Informationen zum Umfang dieses Anteils abfragen kann. Dieser Anteil wird mit »Correct Positives Typ II« bezeichnet (siehe Abbildung 3.2).

Zur Interpretation des in der Betrachtung berücksichtigten Anteils von Correct Positives ist eine gewisse Vorsicht angebracht. Liegt eine hohe Anzahl von Correct Positives Typ I vor, dann ist nicht ohne weiteres klar, ob dies nun positiv oder negativ zu bewerten ist. Trifft der Spam-Filter eine Entscheidung, wodurch ein »Correct Positive Typ I«entsteht, anstatt einer Entscheidung, die einen »False Negative« nach sich ziehen würde, d. h. wächst die Anzahl der Correct Positives Typ I auf Kosten der Anzahl der False Negatives, dann ist dieses als positiv zu bewerten. Bei gleicher Anzahl von False Negatives in zwei vergleichbaren Fällen ist jedoch aus Nutzersicht eine geringere Anzahl von Correct Positives Typ I höher zu bewerten.

3.7 Was wird nicht betrachtet?

Wenngleich die Anzahl der Correct Negatives und der False Positives für die Bewertung von Spam-Eigenschaften eines Email-Dienstes ebenfalls von Interesse

Abbildung 3.2: Unterscheidung von Correct Positives



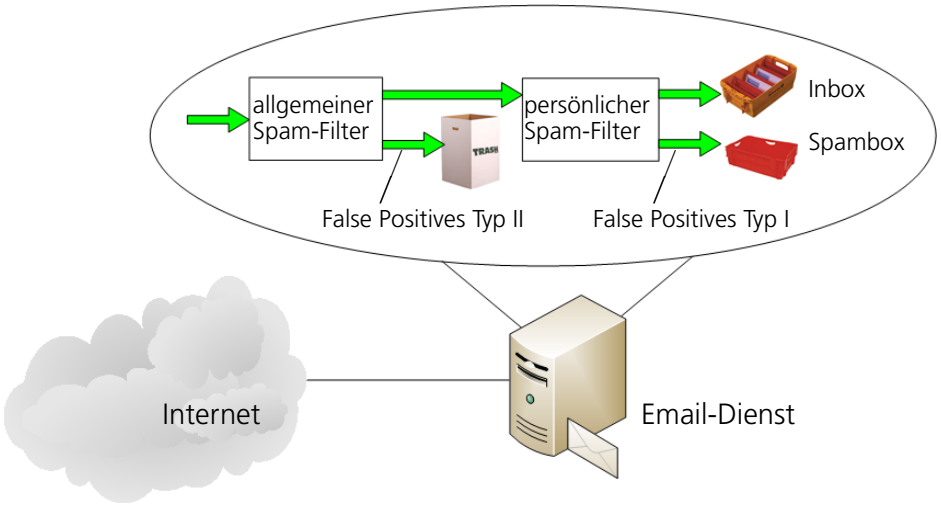
sind, wird hier ausdrücklich darauf hingewiesen, dass diese im Rahmen der Untersuchung nicht betrachtet werden.

Unter den Correct Negatives werden diejenigen Emails verstanden, die in der Inbox empfangen werden und bei denen es sich nicht Spam handelt. Die Anzahl der Correct Negatives wird im Rahmen der Untersuchung nicht betrachtet, da diese wegen unterschiedlicher Nutzungsintensität der Email-Konten verschiedener (Test)Personen wahrscheinlich wenig aussagekräftig ist. Darüber hinaus sollten auch von den Untersuchenden im Rahmen eines rein passiven Ansatzes keine Emails verschickt werden. Selbst wenn Fraunhofer SIT Emails verschickt hätte, welche als Correct Negatives empfangen worden wären, dann wäre die Aussage dieses Ergebnisses quasi wertlos, da die Anzahl der gemessenen Correct Negatives letztendlich die Anzahl der versendeten Emails wiedergegeben hätte. Eine Entscheidung, wie viele Emails zu diesem Zweck verschickt werden, kann nicht als Aussage über die Qualität der Spam-Eigenschaften eines Dienstes verwendet werden.

Bei den False Positives kann man streng genommen wieder zwischen zwei Typen unterscheiden: den False Positives Typ I und den False Positives Typ II. Bei den False Positives Typ I handelt es sich um erwünschte Nachrichten, die in der Spambox landen (siehe Abbildung 3.3). Bei den False Positives Typ II handelt es sich erwünschte Nachrichten, die bereits von dem allgemeinen Spam-Filter als Spam erkannt und direkt aussortiert werden (siehe Abbildung 3.3). False Positives werden im Rahmen der Untersuchung nicht betrachtet, da innerhalb eines rein passiven Ansatzes keine Emails an die Testkonten verschickt und diese nicht zur Abwicklung von erwünschter Email-Korrespondenz eingesetzt werden. Darüber hinaus besteht im Rahmen eines Black-Box-Ansatzes auch keine Möglichkeit, die Anzahl der False Positives Typ II in Erfahrung zu bringen.

Ebenfalls nicht betrachtet werden die Correct Positives Typ II, wie bereits in Kapitel 3.6 erwähnt wurde. Hierfür gilt die gleiche Begründung wie bei den False Positives Typ II.

Abbildung 3.3: Unterscheidung von False Positives



3.8 Welche Dienstangebote werden berücksichtigt?

In der vorliegenden Untersuchung werden ausschließlich kostenfreie Angebote kommerzieller Dienstanbieter betrachtet. Hierzu wurden die fünf Anbieter mit dem größten Marktanteil unter den Wettbewerbern mit kostenfreien Angeboten berücksichtigt. Diese sind in Tabelle 3.2 in alphabetischer Reihenfolge aufgelistet.

Aus technischen Gründen werden die zu betrachtenden Dienstangebote im Folgenden in Tabellen, Formeln und Diagrammen mit vereinfachten Schreibweisen referenziert: gmx, googlemail, hotmail, web und yahoo.

Tabelle 3.2: Betrachtete Anbieter von kostenfreien Email-Diensten

Nr.	Dienst	Domain	Kurzform
1	GMX	`gmx.de`	gmx
2	Google Mail	`googlemail.com`	googlemail
3	Hotmail	`hotmail.de`	hotmail
4	WEB.DE	`web.de`	web
5	Yahoo!	`yahoo.de`	yahoo

3.9 Was wird unter welchen Bedingungen gemessen?

Da die Untersuchung auf die Berücksichtigung der False Negatives und der Correct Positives Typ I beschränkt ist, wurde bei der Messung die pro Kalendertag empfangene Anzahl von Spam-Nachrichten in der Inbox und in der Spambox erfasst. Bei dieser Messung wurde zusätzlich noch dahingehend differenziert, welcher Anteil der Spam-Nachrichten von intern (d. h. von dem Dienstanbieter) und welcher Anteil der Spam-Nachrichten von extern (d. h. nicht von dem

Dienstanbieter) versendet wurde. Nachrichten von intern, welche keinen werbenden Inhalt haben und sich beispielsweise auf die Verwaltung des Email-Kontos beziehen, werden nicht als Spam-Nachrichten gezählt. Bei den Nachrichten von intern werden auch keine Emails berücksichtigt, in deren Empfang ein Benutzer explizit eingewilligt hat. Die in der Messung gezählten Spam-Nachrichten werden sowohl konto- als auch dienstanbieterbezogen gemessen.

Die somit ermittelten Messwerte sind in der Praxis für unterschiedliche Schlüsse von Relevanz. Die Anzahl der in der Inbox empfangenen Spam-Nachrichten sowie ihrer dienstanbieterbezogenen Aggregation und die Vergleichsmöglichkeit mit den Werten der anderen Dienstanbieter sind von Interesse, da diese wiedergeben, wie sehr man als Kunde in dem Betrachtungszeitraum durch Spam-Nachrichten betroffen bzw. beeinträchtigt war. Der Vergleich zwischen Kunden verschiedener Anbieter unter gleichen Ausgangsbedingungen erlaubt in gewissem Umfang auch ein Fazit, wie gut die Spam-Filterung der Anbieter im Betrachtungszeitraum funktioniert hat. Die Summe der Messwerte über Inbox und Spambox gibt den Aufwand für die von einem Benutzer zu kontrollierenden Spam-Nachrichten wieder. Da ein Benutzer die Sorge haben kann, dass eine erwünschte Email in der Spambox gelandet ist, wird er auch die Spambox auf erwünschte Emails hin überprüfen.

Die Messbedingungen sind für alle im Wettbewerb stehenden Anbieter gleich. Für alle Anbieter wurde unter gleichen Zeitbedingungen die gleiche Anzahl von Email-Adressen angelegt. Sowohl bei der Auswahl der Email-Adressen selbst als auch bei ihrer Publikation wurde berücksichtigt, dass gleiche Bedingungen gelten, damit die Email-Adressen in gleich leichter oder schwieriger Weise in die Hände von Spammern fallen und von diesen auch mit den gleichen Wörterbüchern durch Austesten gefunden werden können. Bei der Konfiguration von Email-Konten wurden dienstanbieterabhängig vergleichbare Ausgangsbedingungen geschaffen, indem die Standardeinstellungen übernommen wurden, sofern diese nicht über benutzerfreundliche Möglichkeiten für Opt-in oder Opt-out modifiziert werden konnten.

Die Messung wurde derart durchgeführt, dass sie für andere nachvollziehbar ist. Das bedeutet insbesondere, dass die Messung unabhängig davon sein muss, mit welchen Werkzeugen die Spam-Nachrichten abgefragt und die erforderlichen Werte gemessen werden. Sofern Interaktionen des Untersuchenden bei der Messung dazu führen können, auf Klassifikationen von zukünftigen Spam-Nachrichten einzuwirken, und diese Interaktionsmöglichkeiten abhängig von dem verwendeten Werkzeug sind, ist ein planvolles Vorgehen bei der Messung notwendig. Insbesondere sind damit auch die Untersuchenden angehalten, mit dem ausgewählten Werkzeug derart zu interagieren, dass sich Messwerte und Zustände des Email-Kontos mit allen Werkzeugen in gleicher Weise ergeben. Dies ist insbesondere in solchen Fällen relevant, in welchen Dienstanbieter ihren Kunden mit einer erhaltenen Email die Möglichkeit bieten, diese zu klassifizieren. Eine solche Option kann grundsätzlich sehr nützlich sein, da ein Benutzer somit den Email-Empfang von einem bestimmten, *a priori* unbekannten Spam-

mer durch sehr geringen Interaktionsaufwand ausschließen kann. Diese Möglichkeit zur Spam-Vermeidung ist jedoch in Abhängigkeit davon, auf welcher technischen Basis diese Interaktionsmöglichkeiten den Benutzern angeboten werden, nicht mit allen Werkzeugen in gleicher Weise nutzbar. Fügt ein Anbieter die alternativen Interaktionsmöglichkeiten durch das Einbetten von HTTP-Links in Emails ein, so kann ein Benutzer unabhängig davon, ob er seine Email mit einem Web-Browser oder einer Email-Software abruft, die ihm angebotenen Interaktionsmöglichkeiten nutzen, um die gewünschten Konfigurationsanpassungen vorzunehmen. Bietet ein Anbieter hingegen die alternativen Interaktionsmöglichkeiten ausschließlich als Bedienelemente auf der Web-Oberfläche an, dann kann ein Benutzer, welcher seine Emails mit einer Email-Software abruft, von diesen Möglichkeiten keinen Gebrauch machen.

Grundsätzlich sind fallbezogene Konfigurationsmöglichkeiten zur Bekämpfung von Spam als positiv zu bewerten. Wenn diese angeboten werden, dann sollte man sie jedoch mit sämtlichen relevanten Werkzeugen benutzen können. Vor diesem Hintergrund gilt für die Messung, dass nach einer empfangenen Spam-Nachricht eine Nachjustierung des persönlichen Spam-Filters erlaubt ist, wenn diese in gleicher Weise aus einem Web-Browser und einer Email-Software angestoßen werden kann und die Nachjustierung darüber hinaus keinen weiteren Interaktionsaufwand nach sich zieht. Eine sukzessive Anpassung der persönlichen Spam-Filtereinstellungen mit Zugang über die allgemeine Menüstruktur der Anbieterportale ist hingegen nicht zugelassen. Dies gilt für alle Email-Konten der Testpersonen und bei allen Dienstanbietern in gleicher Weise.

Die Testpersonen haben ihre Email-Konten für die Untersuchung eigens angelegt. Alle Testpersonen haben ihre Email-Adresse weder vor noch während der Untersuchungsdurchführung für anderweitige, die Untersuchung nicht betreffende Zwecke eingesetzt, so dass hinsichtlich der Verbreitungsmöglichkeiten für Email-Adressen für alle die gleichen Bedingungen bestanden haben. Um bzgl. der Verbreitung von Email-Adressen die gleichen Rahmenbedingungen für die Durchführung der Untersuchung zu haben, war es wichtig, dass die verwendeten Email-Konten ungefähr gleich alt sind. Miteinander korrespondierende Email-Adressen mussten zur Wahrung der gleichen Rahmenbedingungen am selben Tag angelegt werden. Bei der Untersuchung wurden nur solche Email-Adressen verwendet, die sich in einer noch jungen Lebensphase befanden und die bis zu ihrer Verwendung für die Untersuchung nur sehr kontrolliert eingesetzt wurden. Speziell bedeutet dies für die Untersuchung, dass keine der verwendeten Email-Adressen zu Beginn des Beobachtungszeitraums älter als drei Monate war. Dadurch sollte sichergestellt werden, dass die Email-Adressen gleich stark verbreitet sind. Es ist nicht auszuschließen, dass sich bei der Verwendung von Email-Adressen in einer älteren Lebensphase andere Untersuchungsresultate ergeben.

3.10 Aussage und Deutung der Ergebnisse

Die Zielsetzung der Untersuchung bestand ausschließlich in der Behandlung der im Vorangegangenen genannten Spam-Eigenschaften. Zur Bewertung von Dienstangeboten allgemein stellen diese lediglich ein relevantes Kriterium dar. Um eine Gesamtaussage über die Qualität eines Dienstes treffen zu können, müssen viele weitere Kriterien herangezogen und untersucht werden, welche jedoch in dieser Untersuchung ausdrücklich nicht berücksichtigt wurden. Hierzu zählen:

- Bedienbarkeit und Benutzungsfreundlichkeit
- Speichervolumen der Mailbox
- Umfang und Qualität angebotener Zusatzfunktionen (z. B. Suche, Adressbuch, Email-Sammeldienst)
- Sicherheitsaspekte (z. B. Verschlüsselung, Virenschutz, schwache Zugangskontrolle durch leicht von Dritten zu beantwortende Sicherheitsfragen)
- Qualität und Kundenfreundlichkeit der Allgemeinen Geschäftsbedingungen (AGB)
- Datenschutzaspekte
- Verfügbarkeit des Dienstes
- Begrenzung des Datenvolumens von Email-Anhängen
- Registrierung
- Kündigung
- Verständlichkeit für Kunden
- Zensur durch Dienstanbieter
- Begrenzung der Anzahl von Email-Abrufen
- Umfang weiterer technischer Zugangsmöglichkeiten (z. B. IMAP, POP3)

Die vorliegende Untersuchung basiert auf einer Bestandsaufnahme für die genannten Dienstanbieter während des Monats Februar im Jahr 2010. Auch wenn die Messungen in fairer Weise, objektiv, nachvollziehbar und transparent als Black-Box-Analyse durchgeführt wurden, sind die Ergebnisse nicht hinreichend für die Bewertung der Qualität der jeweils von den Dienstanbietern eingesetzten Technologie. Es ist durchaus möglich, dass ein Anbieter, für den sich das Studienergebnis schlechter darstellt als für einen anderen Wettbewerber, eine bessere technische Lösung einsetzt. Das Studienergebnis kann sich dennoch in anderer Weise darstellen, wenn beispielsweise ein Anbieter sehr viel stärker Spam-Angriffen ausgesetzt ist als sein Wettbewerber, so dass auch nach Anwendung deutlich besserer Abwehrmaßnahmen immer noch eine höhere

Anzahl von Spam-Nachrichten empfangen wird als von Kunden des Wettbewerbers.

Auch wenn somit das Ergebnis der Studie die Qualität der Diensterbringung nicht notwendigerweise berücksichtigen bzw. wiedergeben mag, so ist dies unproblematisch für die den Nutzer primär interessierenden Eigenschaften des Dienstes. Aus Perspektive des Kunden ist die Qualität der eingesetzten Technologie weniger relevant als die Anzahl der tatsächlich empfangenen Spam-Nachrichten. Bei dieser Studie wurde die exakte Anzahl tatsächlich empfangener Spam-Nachrichten für mehrere Kunden je Dienstanbieter berücksichtigt.

Dennoch ist darauf hinzuweisen, dass die Ergebnisse der Studie lediglich auf der Anzahl der empfangenen Spam-Nachrichten im Februar 2010 basieren. Diese Ergebnisse geben lediglich die betrachteten Diensteigenschaften im genannten Zeitraum wieder. Grundsätzlich besteht keine Rechtfertigung, auf Basis dieser Ergebnisse Aussagen für andere Betrachtungszeiträume abzuleiten.

In einigen Diskussionen wird die Spam-Problematik zusammen mit Fragestellungen des Energieverbrauchs behandelt. Es ist natürlich grundsätzlich interessant zu erkennen, wie viel Energie durch das Spam-Aufkommen verbraucht wird, und es wäre wünschenswert, wenn man diese Energiemenge einsparen könnte. Jedoch ist hinsichtlich schneller Rückschlüsse bzgl. der Auswirkungen potenzieller Abwehrmaßnahmen von Dienstanbietern Vorsicht geraten. Grundsätzlich können Spam-Filter als Abwehrmaßnahmen den Energieaufwand, welcher für das Versenden und Übertragen von Emails aufgebracht wird, nicht reduzieren. Darüber hinaus ist für eine faire Betrachtung auch der Energieaufwand für die Abwehrmaßnahmen zu berücksichtigen.

4 Durchführung der Messung

4.1 Rahmen der Messung

Für die Messung wurde das Spam-Aufkommen bei sechs Testpersonen betrachtet. Für diese Testpersonen wurden insgesamt 30 Email-Konten eingerichtet. Der Betrachtungszeitraum für die Messung lag zwischen dem 1. und dem 28. Februar 2010, jeweils einschließlich. Vor der Messung musste die Messumgebung für diese Testpersonen entsprechend initialisiert werden. Die Initialisierung war 36 Stunden vor Beginn des Messzeitraums vollständig abgeschlossen.

4.2 Initialisierung

Vor der Durchführung der Untersuchung und der hierfür erforderlichen Messungen mussten eine Reihe von Vorbereitungen getroffen werden. Hierbei ging es insbesondere darum, die Gegenstände der Messungen in planvoller Weise zu initialisieren, so dass für alle Dienstanbieter die gleichen Voraussetzungen bestanden, um einen fairen Vergleich durchführen zu können.

4.2.1 Einrichtung von Email-Adressen

Für jede der an der Untersuchung teilnehmenden Testpersonen wurde vor der Messphase bei jedem Dienstanbieter je ein Email-Konto angelegt. Für alle diese Email-Konten galt die Bedingung, dass die in den registrierten Email-Adressen ausgewählten IDs je Testperson bei allen Dienstanbietern identisch sind, d. h. es galt das in Tabelle 4.1 gezeigte Schema, so dass sich die Email-Adressen einer Testperson ausschließlich durch die Domainbezeichnung des Dienstanbieters voneinander unterschieden.

Tabelle 4.1: Schema der eingerichteten Email-Adressen

Person	gmx	googlemail	hotmail	web	yahoo
Person 1	id1@gmx	id1@googlemail	id1@hotmail	id1@web	id1@yahoo
Person 2	id2@gmx	id2@googlemail	id2@hotmail	id2@web	id2@yahoo
Person 3	id3@gmx	id3@googlemail	id3@hotmail	id3@web	id3@yahoo
Person 4	id4@gmx	id4@googlemail	id4@hotmail	id4@web	id4@yahoo
Person 5	id5@gmx	id5@googlemail	id5@hotmail	id5@web	id5@yahoo
Person 6	id6@gmx	id6@googlemail	id6@hotmail	id6@web	id6@yahoo

Die in Tabelle 4.1 gezeigten IDs der insgesamt 30 angelegten Email-Adressen sind lediglich als Platzhalter zu verstehen und dienen der Darstellung der regelmäßigen Struktur bei der Auswahl der Email-Adressen. Statt den Bezeichnungen id1,. . . ,id6 haben die Testpersonen realistisch erscheinende IDs ausgewählt. Die tatsächlich gewählten Email-Adressen werden in dieser Studie nicht bekanntgegeben.

Bei der Auswahl der Email-Adressen gab es für die Testpersonen unterschiedliche Vorgaben. Drei Testpersonen hatten die Vorgabe, ihre ID nach dem Muster *Vorname.Nachname* auszuwählen. Bei dieser ID sollte es sich um tatsächlich im deutschen Sprachraum existierende Vornamen und Nachnamen handeln. Somit sollte eine realistische Situation nachgestellt werden, damit diese Email-Adressen von Spammern, die nach dem Wörterbuchprinzip vorgehen, gefunden werden können. Die Email-Adressen dieser Testpersonen wurden streng geheim gehalten. Somit bestanden für die 15 Email-Adressen dieser Kategorie jeweils die gleichen Voraussetzungen, um von einem Spammer gefunden zu werden.

Die drei anderen Testpersonen hatten hingegen die Vorgabe, als ID ein Pseudonym oder eine Abkürzung ihres Namens zu wählen. Die Komposition des Pseudonyms oder der Namensabkürzung mit einer Zahl war hierbei erlaubt. Bei diesen insgesamt 15 Adressen sollte es weniger wahrscheinlich sein, dass sie von Spammern, die nach dem Wörterbuchprinzip vorgehen, gefunden werden können. Die Email-Adressen dieser Testpersonen wurden jedoch im Internet publiziert (zur Beschreibung, unter welchen Bedingungen diese Email-Adressen für andere publiziert wurden, siehe Abschnitt 4.2.3).

Je Testperson galt für die Erstellung der Email-Konten die Verpflichtung, ihre Email-Adressen bei den verschiedenen Dienstanbietern am selben Tag zu registrieren. Darüber hinaus wurde von keinem der insgesamt 30 angelegten Email-Konten vor und während der Versuchsdurchführung eine Email verschickt, so dass kategoriebezogen die gleichen Ausgangsbedingungen für die Dienstanbieter gewahrt wurden.

4.2.2 Konfiguration der Email-Konten und dienstanbieterspezifische Besonderheiten

Nach der Einrichtung von Email-Konten konnten die Einstellungen der persönlichen Spam-Filter konfiguriert werden. Um von fairen und gleichen Ausgangsbedingungen für die Dienstanbieter auszugehen und um eine nachvollziehbare Basis hinsichtlich Vergleichbarkeit der Messwerte zu haben, wurden bei allen Dienstanbietern die Standardeinstellungen für die persönlichen Spam-Filter übernommen. Insofern blieben die vorhandenen Optionen im Menü zur Einstellung der persönlichen Spam-Filter ungenutzt.

Bietet ein Dienstanbieter seinen Kunden bei der Registrierung eine Möglichkeit, per einfachem Opt-out den Empfang bestimmter Emails (z. B. Newsletter) als unerwünscht zu erklären, dann wurde bei der Initialisierung von einem solchen Angebot Gebrauch gemacht. Verlangt ein Opt-out jedoch einen gesteigerten

Aufwand (z. B. Kündigung per Brief oder Telefonanruf), dann wurde von der Opt-out-Möglichkeit kein Gebrauch gemacht. Grundsätzlich ist das Angebot einer Opt-in-Funktion positiver zu bewerten als ein Opt-out. Da jedoch Anbieter existieren, die ihren Kunden überhaupt keine Möglichkeit zur Verfügung stellen, um solche intern versendeten Spam-Nachrichten abzubestellen, ist das Angebot einer Opt-out-Funktion auch positiv zu bewerten. Würde man im Rahmen der Untersuchung bei der Registrierung keinen Gebrauch der Opt-out-Funktion machen, so würde dieses Angebot gegenüber der Alternative, in welcher interne Emails grundsätzlich nicht abbestellt werden können, nicht ausreichend gewürdigt werden. Vor diesem Hintergrund ist es auch vertretbar, im Rahmen der Untersuchung ein benutzerfreundliches Opt-out einem kundenfreundlichen Opt-in gleichzusetzen.

Im Folgenden werden die während der Registrierungsphase untersuchungsrelevanten Besonderheiten für jeden Dienstanbieter kurz dargestellt.

GMX

GMX bietet seinen Kunden zwar die Möglichkeit eines Opt-outs an, jedoch ist dieses eher als kundenunfreundlich zu bewerten, da man als Kunde durch viele Untermenüs klicken muss oder eine eigene Nachricht zu verfassen hat, in der man erklären muss, keine entsprechenden Mitteilungen erhalten zu wollen. Über die Existenz dieser Möglichkeit wird man als Kunde ausschließlich in den Datenschutzhinweisen von GMX hingewiesen, in welchen man als Kunde diese Information in ca. 2,5 DIN-A4-Seiten Fließtext entdecken muss — neben ca. 10 DIN-A4-Seiten AGB, die man bei der Registrierung zu lesen hat. Der entsprechende Ausschnitt aus den Datenschutzhinweisen ist in Abbildung 4.1 gezeigt. Bei der Registrierung zur Durchführung der Untersuchung wurde von dieser Opt-out-Möglichkeit kein Gebrauch gemacht, da diese als zu benutzerunfreundlich eingestuft wurde und nicht in einfacher Weise durchführbar ist, wie z. B. mittels einer Klick-Option bei der Registrierung.

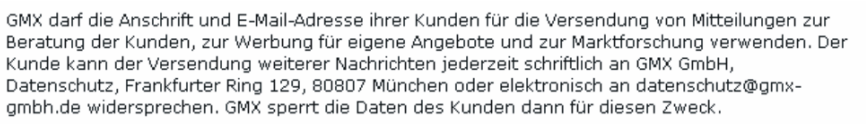


Abbildung 4.1: Auszug aus den Datenschutzhinweisen von GMX

Google Mail

Bei der Registrierung bietet Google Mail keine Möglichkeiten für Opt-in oder Opt-out an. In den Google Mail-Datenschutzhinweisen (aktuelle Version vom 12. September 2008) wird der Kunde jedoch darüber in Kenntnis gesetzt, dass man sich vorbehält, eventuell Informationen im Zusammenhang mit diesem und anderen Google-Diensten an den Kunden zu senden (siehe Abbildung 4.2).

Darüber hinaus wird keine Möglichkeit angeboten, den Erhalt von diesen Nachrichten als »unerwünscht« zu erklären. Aus Mangel an Alternativen werden hier die (nicht veränderbaren) Standardeinstellungen verwendet.

Abbildung 4.2: Auszug aus den Datenschutzhinweisen von Google Mail

> Google wird Ihnen eventuell Informationen im Zusammenhang mit Ihrem Google Mail-Konto oder anderen Google-Diensten senden.

Hotmail

Bei Hotmail ist der Bezug von bestimmten eigenen Werbemitteilungen als Email standardmäßig ausgeschaltet. Die Kunden haben bei der Registrierung eine Opt-in-Möglichkeit, um diese Nachrichten zu erhalten (siehe Abbildung 4.3). Diese Form zur Abfrage des Kundenwillens stellt hinsichtlich der Vermeidung von Spam eine wünschenswerte Alternative dar, sofern sich ein Dienstanbieter in seiner späteren Praxis an diesem Kundenwillen orientiert. Bei der Initialisierung wurde die Standardeinstellung übernommen.

Abbildung 4.3: Opt-in von Hotmail für Werbung vom Dienstanbieter

Auch wenn die Opt-in-Möglichkeit als positiv zu bewerten ist, bleibt für den Kunden, der sich registriert, aufgrund der Tatsache, dass in den Onlinedatenschutzbestimmungen von Microsoft (aktuell gültige Version vom Mai 2008) darauf hingewiesen wird, dass Kunden *möglicherweise* Newsletter oder auch Werbe-Emails erhalten können (siehe Abbildung 4.4), eine gewisse Restunsicherheit bzgl. des zukünftigen Bezugs von internen Spam-Nachrichten.

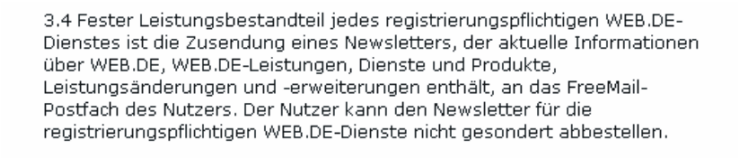
Abbildung 4.4: Auszug aus den Onlinedatenschutzbestimmungen von Microsoft (Hotmail)

> Microsoft verwenden Ihre persönlichen Daten möglicherweise auch, um mit Ihnen zu kommunizieren. Sie erhalten möglicherweise notwendige Servicenachrichten, wie Begrüßungsanschreiben, Zahlungserinnerungen, Informationen zu technischen Servicefragen sowie Sicherheitsmeldungen. Einige Dienste von Microsoft, z. B. Windows Live Hotmail, senden möglicherweise regelmäßig Newsletter an die Mitglieder, die als Teil der Dienstleistung betrachtet werden. Es werden möglicherweise auch gelegentlich Produktumfragen oder Werbe-E-Mails versendet, um Sie über andere verfügbare Produkte oder Dienste von Microsoft oder seinen Partnern zu informieren.

WEB.DE

WEB.DE bietet seinen Kunden während der Registrierung keine Möglichkeit an, interne Spam-Nachrichten als »unerwünscht« zu erklären. WEB.DE geht sogar so weit, dass der eigene als Email versendete Newsletter gemäß Punkt 3.4 der AGB nicht abbestellt werden kann (siehe Abbildung 4.5). Grundsätzlich stellt diese Rahmenbedingung für Kunden hinsichtlich der Vermeidung von Spam die schlechteste Alternative dar.

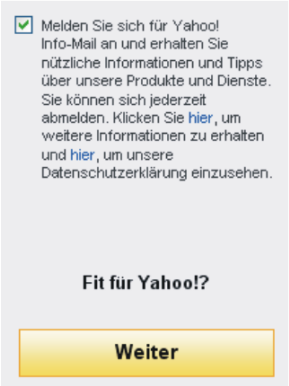
Abbildung 4.5:
Auszug aus den
AGB von WEB.DE



Yahoo!

Yahoo! bietet seinen Kunden während der Registrierung an, den Bezug von internen Spam-Nachrichten als »unerwünscht« zu erklären. Hierzu wird eine bereits im Voraus ausgewählte Opt-in-Möglichkeit angezeigt, so dass man als Kunde an dieser Stelle einfach die Option abwählen kann (siehe Abbildung 4.6). Vom Prinzip entspricht diese Vorgehensweise dann einem Opt-out. Bei der Initialisierung für die Untersuchung wurde die Option jeweils abgewählt.

Abbildung 4.6:
Opt-out bei Yahoo!



4.2.3 Bekanntmachung von Email-Adressen

Vor der Untersuchung wurden die Testpersonen wie in Abschnitt 4.2.1 beschrieben in zwei Gruppen aufgeteilt: eine Gruppe von Testpersonen, welche ihre Email-Adressen streng geheim zu halten hatte, und eine Gruppe von Testpersonen, welche ihre Email-Adressen gegenüber anderen bekannt zu machen hatte. Für die Gruppe von Testpersonen, die ihre Email-Adressen zu publizieren hatten, galten weitere strenge Regeln, damit die gleichen Voraussetzungen für alle Anbieter gewahrt blieben.

Die Bekanntmachung von Email-Adressen geschah für alle Dienstanbieter in gleicher Weise. Als Mittel zur Publikation von Email-Adressen waren ausschließlich Webportale (z. B. Web-2.0-Angebote) und Newsgroups vorgesehen, wo sie von Spammern gefunden werden sollten. Für jede Testperson galt hierbei die Verpflichtung, die bei den verschiedenen Dienstanbietern registrierten Email-Adressen unter den gleichen Bedingungen für andere im Internet verfügbar zu machen, wie in Abbildung 4.7 gezeigt wird. Konkret bedeutete dies, dass jede Testperson auf jedem von ihr ausgewählten Portal alle ihre Email-Adressen publizieren musste, wie z. B. durch Beteiligung an Diskussionen in einem Forum. Jede Testperson hatte hierbei darauf zu achten, dass alle ihre Email-Adressen

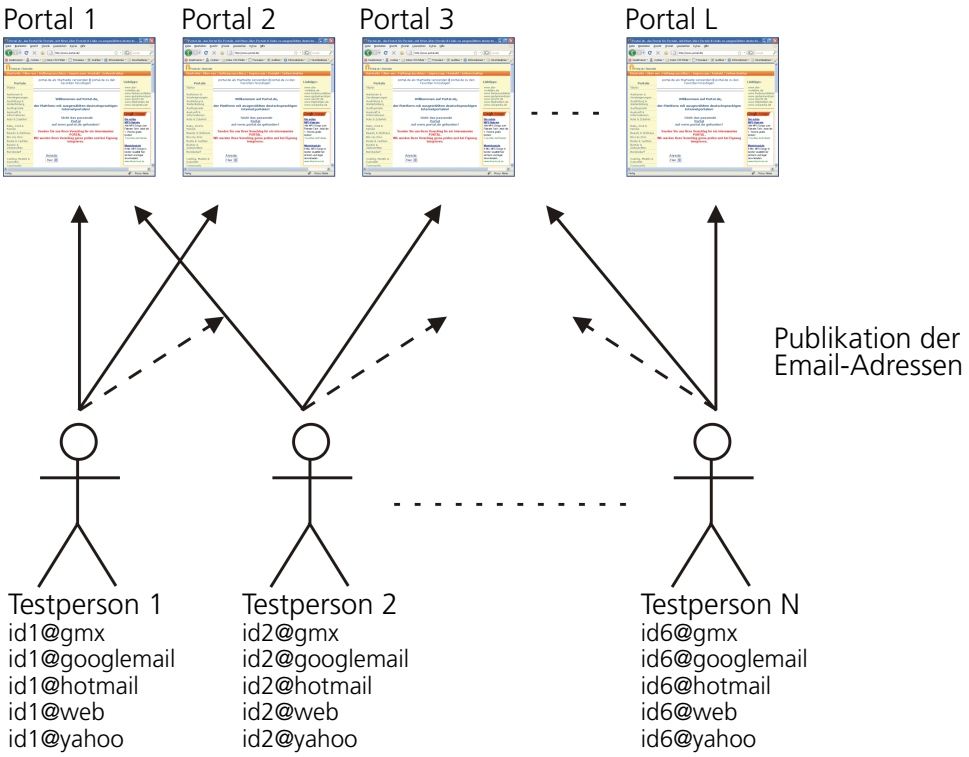


Abbildung 4.7: Bekanntmachung der Email-Adressen über Web-Portale

innerhalb eines kurzen Zeitfensters auf einem Portal publiziert werden. Die Menge der Portale war vorgegeben. Jede Testperson hatte außerdem alle eigenen Email-Adressen bei der gleichen Anzahl von Portalen zu publizieren. So bestanden für jeden Dienstanbieter die gleichen Bedingungen, dass die über ihn zur Verfügung gestellten Email-Adressen von Adresssammlern bzw. Spammern gefunden werden konnten. Die Portale, in welchen die Testpersonen ihre Email-Adressen publiziert haben, werden in dieser Studie nicht genannt.

5 Metriken zur Qualitätsbewertung

Das Ziel dieses Kapitels besteht in der Erklärung, wie die täglich aufgenommenen Messwerte verarbeitet und ausgewertet werden und wie aus diesen eine Gesamtaussage hinsichtlich der Spam-Eigenschaften einzelner Dienstanbieter abgeleitet wird. Hierzu werden im Hinblick auf eine klare Beschreibbarkeit zunächst einige Bezeichnungen eingeführt und notwendige Basisoperationen vorgestellt. Danach werden die Metriken eingeführt, anhand welcher relevante Aspekte quantifizierbar und somit vergleichbar gemacht werden. Abschließend wird erklärt, wie die einzelnen Metriken zu einer Gesamtaussage kombiniert werden.

5.1 Definitionen

5.1.1 Bezeichnungen

Im Folgenden werden einige Bezeichnungen eingeführt, welche für das Verständnis der weiteren Ausführungen relevant sind.

Testperson

Eine Testperson wird mit der Variablen t bezeichnet. Die im Rahmen der Untersuchung in Frage kommenden Werte, die t annehmen kann, sind id1, id2, id3, id4, id5 und id6.

Dienstanbieter

Ein Dienstanbieter wird mit der Variablen d bezeichnet. Die im Rahmen der Untersuchung in Frage kommenden Werte, die d annehmen kann, sind gmx, googlemail, hotmail, web und yahoo.

Zeit

Die tagesgenaue Zeit wird mit der Variablen z bezeichnet. Die im Rahmen der Untersuchung in Frage kommenden Werte, die z annehmen kann, sind $1, \ldots, 28$. Darunter sind die Kalendertage im Monat Februar zu verstehen.

Spam-Anzahl Inbox

Unter $I(t; d; z)$ soll die Anzahl der von Testperson t bei Dienstanbieter d zur Zeit z in der Inbox empfangenen Spam-Nachrichten verstanden werden. Hierbei ist es denkbar, für t einen einzelnen Wert oder auch eine Liste von Werten anzugeben. Wird mit einer Liste von Werten für t gearbeitet, dann werden die Spam-Anzahlen für die Inbox für die in der Liste enthaltenen Testpersonen addiert. Ebenfalls ist es möglich, für z einen einzelnen Wert oder auch eine Liste von Werten anzugeben. Wird hier eine Liste von Werten für z verwendet, dann werden die Spam-Anzahlen für die Inbox für die in der Liste enthaltenen Tage addiert.

Beispiel: $I(t = \text{id1}; d = \text{gmx}; z = 20) = 5$ besagt, dass Testperson id1 am 20. Februar in ihrer Inbox bei gmx insgesamt 5 Spam-Nachrichten empfangen hat. $I(t = \text{id2}; d = \text{gmx}; z = 20) = 3$ besagt, dass Testperson id2 am 20. Februar in ihrer Inbox bei gmx insgesamt 3 Spam-Nachrichten empfangen hat. Diese beiden Aussagen können zusammengefasst werden zu $I(t = \text{id1, id2}; d = \text{gmx}; z = 20) = 8$. Nimmt man mit $I(t = \text{id1}; d = \text{gmx}; z = 21) = 4$ nun zusätzlich noch an, dass Testperson id1 am 21. Februar in ihrer Inbox bei gmx insgesamt 4 Spam-Nachrichten empfangen hat, dann kann man die Werte vom 20. und 21. Februar auch über der Zeit zusammenfassen zu $I(t = \text{id1}; d = \text{gmx}; z = 20{,}21) = 9$.

Spam-Anzahl Spambox

$S(t; d; z)$ bezeichnet die Anzahl der von Testperson t bei Dienstanbieter d zur Zeit z in der Spambox empfangenen Spam-Nachrichten. Analog zu oben können für t und z Listen von Werten übergeben werden. In diesen Fällen werden die entsprechenden Spam-Anzahlen aufaddiert.

Spam-Anzahl Inbox & Spambox

Unter $E(t; d; z)$ soll die Anzahl der von Testperson t bei Dienstanbieter d zur Zeit z zusammen in Inbox und Spambox empfangenen Spam-Nachrichten verstanden werden. Es gilt offensichtlich $E(t; d; z) = I(t; d; z) + S(t; d; z)$. Hierbei ist es wiederum möglich, einen einzelnen Wert für t oder z oder auch eine Liste von Werten für t oder z anzugeben, was dann eine Addition der entsprechenden Anzahlen beschreibt.

Spam-Anzahl Inbox & Spambox von intern

$E_{\text{int}}(t; d; z)$ bezeichnet die Anzahl der insgesamt von Testperson t bei Dienstanbieter d zur Zeit z empfangenen Spam-Nachrichten, die von d versendet wurden. Auch hierbei ist es wiederum möglich, einen einzelnen Wert für t oder z

oder auch eine Liste von Werten für t oder z anzugeben, was dann eine Addition der entsprechenden Anzahlen beschreibt.

Spam-Anzahl Inbox & Spambox von extern

$E_{\text{ext}}(t; d; z)$ bezeichnet die Anzahl der insgesamt von Testperson t bei Dienstanbieter d zur Zeit z empfangenen Spam-Nachrichten, die nicht von d versendet wurden. Auch hierbei ist es wiederum möglich, einen einzelnen Wert für t oder z oder auch eine Liste von Werten für t oder z anzugeben, was dann eine Addition der entsprechenden Anzahlen beschreibt.

5.1.2 Operationen

Im Folgenden werden einige einfache Operationen eingeführt, welche für die spätere Erklärung der verwendeten Metriken hilfreich sind. Die Einführung geschieht lediglich in einer semi-formalen Weise, soweit dies für eine klare Beschreibbarkeit der Metriken erforderlich erscheint.

rang$(\cdot)$

Übergibt man dem Operator rang$(\cdot)$ eine Liste von reellen Werten, dann liefert rang$(\cdot)$ eine Rangfolge für diese Werte, wobei dem kleinsten Wert der niedrigste Positionswert beginnend bei 1 zugewiesen wird. Größeren Werten in der Liste sind jeweils höhere Positionswerte zugeordnet. Der nächste zu vergebende Positionswert entspricht der natürlichen Zahl, welche auf die Anzahl der bis dahin bereits verarbeiteten Listenwerte folgt. Enthält die Liste gleiche Werte, dann wird diesen Werten der gleiche Positionswert zugewiesen.

Beispiel: Man nehme an, für eine Liste von Dienstanbietern gelten die folgenden Werte.

Anbieter1 $\rightarrow$ 4,36
Anbieter2 $\rightarrow$ 3,25
Anbieter3 $\rightarrow$ 1,09
Anbieter4 $\rightarrow$ 3,25
Anbieter5 $\rightarrow$ 2,13

Wendet man auf diese Werte den Operator rang$(4{,}36; 3{,}25; 1{,}09; 3{,}25; 2{,}13)$ an, dann erhält man die Rangpositionen

$1{,}09 \rightarrow 1$
$2{,}13 \rightarrow 2$
$3{,}25 \rightarrow 3$
$3{,}25 \rightarrow 3$
$4{,}36 \rightarrow 5$

Dies impliziert für die Dienstanbieter die Rangfolge

Anbieter3 $\rightarrow 1$
Anbieter5 $\rightarrow 2$
Anbieter2 $\rightarrow 3$
Anbieter4 $\rightarrow 3$
Anbieter1 $\rightarrow 5$

max$(\cdot)$

Der Operator max$(\cdot)$ liefert für eine Liste von reellen Werten den höchsten Wert, der in der Liste enthalten ist.

Beispiel: Man nehme an, für eine Liste von Dienstanbietern gelten die folgenden Werte.

Anbieter1 $\rightarrow 10$
Anbieter2 $\rightarrow 3$
Anbieter3 $\rightarrow 12$
Anbieter4 $\rightarrow 6$
Anbieter5 $\rightarrow 12$

Wendet man den Operator max$(\cdot)$ auf die gegebenen Werte an, dann erhält man $\max(10; 3; 12; 6; 12) = 12$, d. h. Anbieter3 und Anbieter5 ist der höchste Wert zugeordnet.

mpos$(\cdot)$

Wendet man auf eine Liste von Rangfolgen und ein gegebenes Auswahlelement bzw. eine Liste von Auswahlelementen den Operator mpos$(\cdot)$ an, dann liefert mpos$(\cdot)$ die sich über den Rangfolgen ergebende mittlere Position des Auswahlelementes bzw. der Auswahlelemente. Es ist zu beachten, dass die hierbei verwendeten Rangfolgen jeweils über der gleichen Menge von Auswahlelementen gebildet wurden.

Beispiel: Es seien vier Rangfolgen gegeben.

Rangfolge1	Rangfolge2
Anbieter3 $\rightarrow$ 1	Anbieter5 $\rightarrow$ 1
Anbieter5 $\rightarrow$ 2	Anbieter4 $\rightarrow$ 1
Anbieter2 $\rightarrow$ 3	Anbieter2 $\rightarrow$ 3
Anbieter4 $\rightarrow$ 3	Anbieter3 $\rightarrow$ 4
Anbieter1 $\rightarrow$ 5	Anbieter1 $\rightarrow$ 5

Rangfolge3	Rangfolge4
Anbieter3 $\rightarrow$ 1	Anbieter5 $\rightarrow$ 1
Anbieter4 $\rightarrow$ 2	Anbieter2 $\rightarrow$ 2
Anbieter1 $\rightarrow$ 3	Anbieter4 $\rightarrow$ 3
Anbieter5 $\rightarrow$ 4	Anbieter1 $\rightarrow$ 4
Anbieter2 $\rightarrow$ 5	Anbieter3 $\rightarrow$ 5

Dann liefert $\text{mpos}(\text{Rangfolge1}, \text{Rangfolge2}, \text{Rangfolge3}, \text{Rangfolge4}; \text{Anbieter1}) = 4{,}25$ als mittlere Position für Anbieter1, da $(5 + 5 + 3 + 4) \cdot 0{,}25 = 4{,}25$. Analog erhält man $\text{mpos}(\text{Rangfolge1}, \text{Rangfolge2}, \text{Rangfolge3}, \text{Rangfolge4}; \text{Anbieter2}) = 3{,}25$, da $(3 + 3 + 2 + 5) \cdot 0{,}25 = 3{,}25$. Somit liefert $\text{mpos}(\text{Rangfolge1}, \text{Rangfolge2}, \text{Rangfolge3}, \text{Rangfolge4}; \text{Anbieter1}, \text{Anbieter2}) = 0{,}5 \cdot (4{,}25 + 3{,}25) = 3{,}75$.

anzahl$(\cdot)$

Wendet man auf eine Liste von Werten und ein gegebenes Auswahlelement den Operator anzahl$(\cdot)$ an, dann liefert anzahl$(\cdot)$ die Häufigkeit, mit welcher das gegebene Auswahlelement in der Liste von Werten auftritt.

Beispiel: $\text{anzahl}(\text{Anbieter3}, \text{Anbieter2}, \text{Anbieter3}, \text{Anbieter1}, \text{Anbieter4}, \text{Anbieter4}; \text{Anbieter3}) = 2$, da Anbieter3 zweimal in der gegebenen Liste enthalten ist.

5.2 Metriken

5.2.1 Zielsetzung und Klassifikation

Unter einer Metrik verstehen wir ein Konstrukt, mittels welchem sich bestimmte Eigenschaften von Untersuchungsgegenständen als Zahlenwert darstellen lassen. Das Ziel solcher Metriken besteht darin, klare Bewertungs- und Vergleichsmöglichkeiten zu schaffen. Grundsätzlich lassen sich komplexe Metriken auf Basis oder durch Kombination von einfacheren Metriken definieren.

Die bei der Untersuchung im Rahmen der Messwertermittlung betrachteten Messgrößen kann man als einfache Metriken bezeichnen. Diese Messgrößen geben bestimmte Eigenschaften der Untersuchungsgegenstände wieder, z. B. wie viele Spam-Nachrichten Testperson id1 am 20. Februar über den Anbieter Hotmail empfangen hat. Ausgehend von einer solchen Messgröße lassen sich weitere für die Bewertung des Untersuchungsgegenstandes interessante Eigenschaften ableiten und in Form von Metriken quantifizierbar machen, wie z. B. an wie vielen Tagen über Hotmail im Vergleich zu anderen Anbietern in der Summe über alle Testpersonen die meisten Spam-Nachrichten je Tag empfangen wurden. Wie an diesem Beispiel gezeigt wird, lassen sich dann auf Basis einfacher Metriken komplexere Metriken bilden.

Grundsätzlich können Metriken unterschiedlichen Zielen dienen. Die wiederholte Anwendung von Metriken über die Zeit kann bezogen auf einen Untersuchungsgegenstand dazu dienen, Veränderungen des Untersuchungsgegenstands und Trends zu erkennen, um ggf. bei unerwünschten Entwicklungen rechtzeitig gegensteuern zu können. Ein anderes Ziel besteht darin, verschiedene Untersuchungsgegenstände über einem einheitlichen Zeitrahmen (d.h Zeitpunkt oder Zeitintervall) vergleichen zu können. Sollen verschiedene Untersuchungsgegenstände verglichen werden, dann ist bei der Auswahl der Metrik darauf zu achten, dass diese auch der Vergleichbarkeit der Untersuchungsgegenstände dient.

Metriken können hinsichtlich verschiedener Aspekte klassifiziert werden. So kann eine Metrik entweder auf einer absoluten oder relativen Quantifizierung basieren. Im Rahmen der Untersuchung von Spam-Eigenschaften lassen sich die Metriken noch hinsichtlich anderer Kriterien unterscheiden:

- Metriken für gemitteltes Verhalten: Hierbei geht es darum, das durchschnittliche Verhalten eines Dienstanbieters zu quantifizieren.
- Metriken für punktuelles Verhalten: Hierbei geht es darum, Ausreißer im Verhalten eines Dienstanbieters zu quantifizieren.

Diese unterschiedlichen Betrachtungen haben bei der Bewertung der Spam-Eigenschaften verschiedener Dienste ihre Berechtigung. Würde man beispielsweise nur die über einem längeren Zeitraum gebildete Gesamtanzahl von Spam-Nachrichten bei einem Dienstanbieter betrachten, dann würde man beispielsweise die Tatsache, dass ein Dienstanbieter an einem Tag seinen allgemeinen Spam-Filter zu spät aktualisiert hat, wodurch seine Kunden mit einer außerordentlich hohen Anzahl von Spam-Nachrichten belästigt wurden, während die Gesamtanzahl der Spam-Nachrichten über einem längeren Zeitraum größenordnungsmäßig im Bereich der Wettbewerber gelegen hat, unter den Tisch fallen lassen.

Die im Rahmen dieser Studie verwendeten Metriken haben die Eigenschaft, dass sie als Ergebnis eine Rangfolge liefern. D.h. hinsichtlich jeder betrachteten Eigenschaft liefert die Metrik eine Reihenfolge der Dienstanbieter, aus welcher hervorgeht, wie gut ein Dienstanbieter bei der Untersuchung im Vergleich zu

seinen Wettbewerbern bzgl. der betrachteten Eigenschaft abgeschnitten hat. Diese einzelnen Reihenfolgen werden danach für eine Gesamtaussage entsprechend kombiniert.

Die Entscheidung zur Anwendung von Rangfolgen bei der Auswertung basiert darauf, dass ein solches Vorgehen eine einfache Möglichkeit bietet, die verschiedenen Einzelergebnisse zur Gesamtauswertung miteinander zu kombinieren. Bei den Einzelergebnissen stehen unterschiedliche Messgrößen im Vordergrund (siehe Abschnitt 5.2.2), aus denen sich nicht direkt in sinnvoller Weise durch einfache arithmetische Verknüpfungen ein Gesamtergebnis berechnen lässt. Die Bestimmung von Rangfolgen aus den Einzelergebnissen bietet eine einfache Möglichkeit der Normierung. Darüber hinaus lassen sich die Einzelergebnisse mit Rangfolgen für den Leser schneller interpretieren, als wenn er für andere Messgrößen oder Kennziffern zunächst deuten müsste, ob nun ein größerer oder kleinerer Messwert bei einer gegebenen Eigenschaft von Vorteil ist. Bei einer Rangfolge sind entsprechende Aussagen und Vergleiche hingegen sehr einfach möglich. Dabei ist offensichtlich, welchen Wettbewerbern ein Dienstanbieter in welchen Kategorien überlegen bzw. unterlegen ist. Allerdings lässt sich aus den Rangpositionen nicht entnehmen, ob sich die Werte, auf welche sich die Rangfolgenbildung bezieht, nur sehr wenig unterscheiden oder deutlich auseinander liegen.

5.2.2 Verwendete Metriken

M1: Gesamtanzahl Spam je Dienstanbieter

Diese Metrik gibt an, wie stark die betrachteten Testpersonen je Dienstanbieter über dem kompletten Betrachtungszeitraum von Spam-Nachrichten betroffen waren. Über den Gesamtanzahlen von Spam-Nachrichten je Dienstanbieter wird dann eine dienstanbieterbezogene Rangfolge ermittelt.

$$\begin{aligned}\mathrm{M1} = \mathrm{rang}\big(&E(t = \mathrm{id1},\ldots,\mathrm{id6}; d = \mathrm{gmx}; z = 1,\ldots,28),\\ &E(t = \mathrm{id1},\ldots,\mathrm{id6}; d = \mathrm{googlemail}; z = 1,\ldots,28),\\ &E(t = \mathrm{id1},\ldots,\mathrm{id6}; d = \mathrm{hotmail}; z = 1,\ldots,28),\\ &E(t = \mathrm{id1},\ldots,\mathrm{id6}; d = \mathrm{web}; z = 1,\ldots,28),\\ &E(t = \mathrm{id1},\ldots,\mathrm{id6}; d = \mathrm{yahoo}; z = 1,\ldots,28)\big)\end{aligned}$$

Bei M1 handelt es sich um eine Metrik zur Beschreibung eines gemittelten Verhaltens von Diensten.

M2: Gesamtanzahl Spam für am stärksten betroffene Testperson je Dienstanbieter

Diese Metrik zielt darauf ab, für jeden Dienstanbieter den schlechtesten Gesamtwert für die Anzahl von empfangenen Spam-Nachrichten je Testperson

über dem kompletten Betrachtungszeitraum zu ermitteln. Diese diensteanbieterbezogenen Werte werden danach in eine Rangfolge gebracht. Bei M2 handelt es sich um eine Metrik zur Beschreibung eines punktuellen Verhaltens von Diensten.

$$\begin{aligned}\mathrm{M2} = \mathrm{rang}\Big(&\max\big(E(t=\mathrm{id1};d=\mathrm{gmx};z=1,\ldots,28),\ldots,\\ &\qquad E(t=\mathrm{id6};d=\mathrm{gmx};z=1,\ldots,28)\big),\\ &\max\big(E(t=\mathrm{id1};d=\mathrm{googlemail};z=1,\ldots,28),\ldots,\\ &\qquad E(t=\mathrm{id6};d=\mathrm{googlemail};z=1,\ldots,28)\big),\\ &\max\big(E(t=\mathrm{id1};d=\mathrm{hotmail};z=1,\ldots,28),\ldots,\\ &\qquad E(t=\mathrm{id6};d=\mathrm{hotmail};z=1,\ldots,28)\big),\\ &\max\big(E(t=\mathrm{id1};d=\mathrm{web};z=1,\ldots,28),\ldots,\\ &\qquad E(t=\mathrm{id6};d=\mathrm{web};z=1,\ldots,28)\big),\\ &\max\big(E(t=\mathrm{id1};d=\mathrm{yahoo};z=1,\ldots,28),\ldots,\\ &\qquad E(t=\mathrm{id6};d=\mathrm{yahoo};z=1,\ldots,28)\big)\Big)\end{aligned}$$

M3: Maximale Gesamtanzahl Spam pro Tag je Dienstanbieter

Bei M3 wird die maximale Gesamtanzahl von Spam-Nachrichten pro Tag je Dienstanbieter über dem kompletten Betrachtungszeitraum ermittelt. Anschließend ergibt sich über diesen Werten eine Rangfolge. Mit der Metrik M3 wird ein punktuelles Ausreißerverhalten der Dienstanbieter betrachtet.

$$\begin{aligned}\mathrm{M3} = \mathrm{rang}\Big(&\max\big(E(t=\mathrm{id1},\ldots,\mathrm{id6};d=\mathrm{gmx};z=1),\ldots,\\ &\qquad E(t=\mathrm{id1},\ldots,\mathrm{id6};d=\mathrm{gmx};z=28)\big),\\ &\max\big(E(t=\mathrm{id1},\ldots,\mathrm{id6};d=\mathrm{googlemail};z=1),\ldots,\\ &\qquad E(t=\mathrm{id1},\ldots,\mathrm{id6};d=\mathrm{googlemail};z=28)\big),\\ &\max\big(E(t=\mathrm{id1},\ldots,\mathrm{id6};d=\mathrm{hotmail};z=1),\ldots,\\ &\qquad E(t=\mathrm{id1},\ldots,\mathrm{id6};d=\mathrm{hotmail};z=28)\big),\\ &\max\big(E(t=\mathrm{id1},\ldots,\mathrm{id6};d=\mathrm{web};z=1),\ldots,\\ &\qquad E(t=\mathrm{id1},\ldots,\mathrm{id6};d=\mathrm{web};z=28)\big),\\ &\max\big(E(t=\mathrm{id1},\ldots,\mathrm{id6};d=\mathrm{yahoo};z=1),\ldots,\\ &\qquad E(t=\mathrm{id1},\ldots,\mathrm{id6};d=\mathrm{yahoo};z=28)\big)\Big)\end{aligned}$$

M4: Maximale Gesamtanzahl Spam pro Tag je Testperson gemittelt je Dienstanbieter

Bei der Metrik M4 werden für jede Testperson und für den kompletten Betrachtungszeitraum die maximalen Tageswerte von Spam-Nachrichten bei einem Dienstanbieter ermittelt. Über diesen Werten wird dann eine Rangfolge gebildet. Für jeden Dienstanbieter wird dann die mittlere Rangfolgenposition über

allen Testpersonen berechnet. Über den so erhaltenen mittleren Rangpositionen wird erneut eine Rangfolge ermittelt.

Zur einfacheren Beschreibbarkeit von M4 wird zunächst mit m4 eine Hilfsmetrik eingeführt.

$$
\begin{aligned}
\mathrm{m4} = \mathrm{rang}\Big(& \\
& \max\big(E(t=\mathrm{id1}; d=\mathrm{gmx}; z=1), \ldots, E(t=\mathrm{id1}; d=\mathrm{gmx}; z=28)\big), \\
& \vdots \\
& \max\big(E(t=\mathrm{id6}; d=\mathrm{gmx}; z=1), \ldots, E(t=\mathrm{id6}; d=\mathrm{gmx}; z=28)\big), \\
& \max\big(E(t=\mathrm{id1}; d=\mathrm{googlemail}; z=1), \ldots, \\
& \qquad E(t=\mathrm{id1}; d=\mathrm{googlemail}; z=28)\big), \\
& \vdots \\
& \max\big(E(t=\mathrm{id6}; d=\mathrm{googlemail}; z=1), \ldots, \\
& \qquad E(t=\mathrm{id6}; d=\mathrm{googlemail}; z=28)\big), \\
& \max\big(E(t=\mathrm{id1}; d=\mathrm{hotmail}; z=1), \ldots, \\
& \qquad E(t=\mathrm{id1}; d=\mathrm{hotmail}; z=28)\big), \\
& \vdots \\
& \max\big(E(t=\mathrm{id6}; d=\mathrm{hotmail}; z=1), \ldots, \\
& \qquad E(t=\mathrm{id6}; d=\mathrm{hotmail}; z=28)\big), \\
& \max\big(E(t=\mathrm{id1}; d=\mathrm{web}; z=1), \ldots, E(t=\mathrm{id1}; d=\mathrm{web}; z=28)\big), \\
& \vdots \\
& \max\big(E(t=\mathrm{id6}; d=\mathrm{web}; z=1), \ldots, E(t=\mathrm{id6}; d=\mathrm{web}; z=28)\big), \\
& \max\big(E(t=\mathrm{id1}; d=\mathrm{yahoo}; z=1), \ldots, \\
& \qquad E(t=\mathrm{id1}; d=\mathrm{yahoo}; z=28)\big), \\
& \vdots \\
& \max\big(E(t=\mathrm{id6}; d=\mathrm{yahoo}; z=1), \ldots, \\
& \qquad E(t=\mathrm{id6}; d=\mathrm{yahoo}; z=28)\big)\Big)
\end{aligned}
$$

Die Hilfsmetrik m4 liefert eine Rangfolge von 30 Werten (da 6 Testpersonen bei 5 Dienstanbietern). Damit kann nun M4 eingeführt werden. Mit den Operatoren $\mathrm{mpos}(\cdot)$ und $\mathrm{rang}(\cdot)$ wird aus einer 30-elementigen Rangfolge eine 5-elementige Rangfolge zur Bewertung der Dienstanbieter berechnet.

$$
\begin{aligned}
\mathrm{M4} = \mathrm{rang}\big(& \mathrm{mpos}(\mathrm{m4}, \mathrm{gmx}), \\
& \mathrm{mpos}(\mathrm{m4}, \mathrm{googlemail}), \\
& \mathrm{mpos}(\mathrm{m4}, \mathrm{hotmail}), \\
& \mathrm{mpos}(\mathrm{m4}, \mathrm{web}), \\
& \mathrm{mpos}(\mathrm{m4}, \mathrm{yahoo})\big)
\end{aligned}
$$

Bei M4 handelt es sich um eine Metrik, bei welcher ein gemitteltes Verhalten bewertet wird.

M5: Anzahl Tage mit schlechtesten Tageswerten für Dienstanbieter aggregiert

Bei dieser Metrik wird betrachtet, an wie vielen Tagen des Betrachtungszeitraums alle Testpersonen zusammengefasst je Dienstanbieter die höchste Anzahl von Spam-Nachrichten haben. Über der ermittelten Anzahl von Tagen je Dienstanbieter wird dann eine Rangfolge der Dienstanbieter aufgestellt. Zur Beschreibung von M5 werden die Hilfsgrößen $\mathrm{d1}, \ldots, \mathrm{d28}$ verwendet. Jede dieser Hilfsgrößen gibt den oder die Dienstanbieter wieder, die an dem entsprechenden Tag das höchste Spam-Aufkommen hatten. Hierbei steht d1 für den oder die Dienstanbieter des ersten Tages des Betrachtungszeitraums, d2 für den oder die Dienstanbieter des zweiten Tages des Betrachtungszeitraums, usw. Man beachte, dass es Tage geben kann, an denen das höchste Spam-Aufkommen von mehreren Dienstanbietern erreicht wird. In diesem Fall werden den Hilfsgrößen mehrere Dienstanbieter zugewiesen, für welche die Maximalwerte von Spam-Nachrichten an dem entsprechenden Tag erreicht werden.

$$
\begin{aligned}
\mathrm{d1} = \text{Liste der } d \text{ mit } & E(t = \mathrm{id1}, \ldots, \mathrm{id6}; d; z = 1) = \\
& \max\big(E(t = \mathrm{id1}, \ldots, \mathrm{id6}; d = \mathrm{gmx}; z = 1), \\
& \quad E(t = \mathrm{id1}, \ldots, \mathrm{id6}; d = \mathrm{googlemail}; z = 1), \\
& \quad E(t = \mathrm{id1}, \ldots, \mathrm{id6}; d = \mathrm{hotmail}; z = 1), \\
& \quad E(t = \mathrm{id1}, \ldots, \mathrm{id6}; d = \mathrm{web}; z = 1), \\
& \quad E(t = \mathrm{id1}, \ldots, \mathrm{id6}; d = \mathrm{yahoo}; z = 1)\big) > 0 \\
\vdots \quad \vdots & \\
\mathrm{d28} = \text{Liste der } d \text{ mit } & E(t = \mathrm{id1}, \ldots, \mathrm{id6}; d; z = 28) = \\
& \max\big(E(t = \mathrm{id1}, \ldots, \mathrm{id6}; d = \mathrm{gmx}; z = 28), \\
& \quad E(t = \mathrm{id1}, \ldots, \mathrm{id6}; d = \mathrm{googlemail}; z = 28), \\
& \quad E(t = \mathrm{id1}, \ldots, \mathrm{id6}; d = \mathrm{hotmail}; z = 28), \\
& \quad E(t = \mathrm{id1}, \ldots, \mathrm{id6}; d = \mathrm{web}; z = 28), \\
& \quad E(t = \mathrm{id1}, \ldots, \mathrm{id6}; d = \mathrm{yahoo}; z = 28)\big) > 0
\end{aligned}
$$

Da mit $\mathrm{d1}, \ldots, \mathrm{d28}$ nun die jeweils schlechtesten Tagesperformer vorliegen, kann über allen Tagen eine Rangfolge erstellt werden.

$$
\begin{aligned}
\mathrm{M5} = \mathrm{rang}\big(&\mathrm{anzahl}(\mathrm{d1}, \ldots, \mathrm{d28}; \mathrm{gmx}), \\
&\mathrm{anzahl}(\mathrm{d1}, \ldots, \mathrm{d28}; \mathrm{googlemail}), \\
&\mathrm{anzahl}(\mathrm{d1}, \ldots, \mathrm{d28}; \mathrm{hotmail}), \\
&\mathrm{anzahl}(\mathrm{d1}, \ldots, \mathrm{d28}; \mathrm{web}), \\
&\mathrm{anzahl}(\mathrm{d1}, \ldots, \mathrm{d28}; \mathrm{yahoo})\big)
\end{aligned}
$$

Die Metrik M5 stellt eine Mischform zwischen gemitteltem und punktuellem Verhalten dar.

M6: Anzahl Tage mit schlechtesten Tageswerten für Testpersonen

Die Metrik M6 ist verwandt mit der Metrik M5. Bei der Metrik M6 werden die schlechtesten Tageswerte jedoch nicht für Dienstanbieter aggregiert, sondern es wird die Anzahl von Spam-Nachrichten, welche von einer Testperson an einem Tag über einen Dienstanbieter empfangen werden, direkt betrachtet. Es wird bei M6 also für jeden Tag des Betrachtungszeitraums die Testperson oder die Testpersonen mit maximalem Spam-Aufkommen ermittelt. In diesem Zusammenhang werden erneut Hilfsgrößen $\mathrm{d1}, \ldots, \mathrm{d28}$ verwendet. Jede dieser Hilfsgrößen gibt den oder die Dienstanbieter wieder, für den/die mindestens ein Kunde an dem entsprechenden Tag das höchste Spam-Aufkommen hatte. Hierbei bezieht sich d1 auf den ersten Tag des Betrachtungszeitraums, d2 auf den zweiten Tag des Betrachtungszeitraums, usw.

$$
\begin{aligned}
\mathrm{d1} = &\text{Liste der } d\text{, für die ein } t \text{ existiert mit}\\
&E(t;d;z=1) = \max\big(E(t=\mathrm{id1};d=\mathrm{gmx};z=1),\ldots,\\
&\qquad E(t=\mathrm{id6};d=\mathrm{gmx};z=1),\\
&\qquad E(t=\mathrm{id1};d=\mathrm{googlemail};z=1),\ldots,\\
&\qquad E(t=\mathrm{id6};d=\mathrm{googlemail};z=1),\\
&\qquad E(t=\mathrm{id1};d=\mathrm{hotmail};z=1),\ldots,\\
&\qquad E(t=\mathrm{id6};d=\mathrm{hotmail};z=1),\\
&\qquad E(t=\mathrm{id1};d=\mathrm{web};z=1),\ldots,\\
&\qquad E(t=\mathrm{id1};d=\mathrm{web};z=1),\\
&\qquad E(t=\mathrm{id1};d=\mathrm{yahoo};z=1),\ldots,\\
&\qquad E(t=\mathrm{id6};d=\mathrm{yahoo};z=1)\big) > 0\\
&\vdots \quad \vdots\\
\mathrm{d28} = &\text{Liste der } d\text{, für die ein } t \text{ existiert mit}\\
&E(t;d;z=28) = \max\big(E(t=\mathrm{id1};d=\mathrm{gmx};z=28),\ldots,\\
&\qquad E(t=\mathrm{id6};d=\mathrm{gmx};z=28),\\
&\qquad E(t=\mathrm{id1};d=\mathrm{googlemail};z=28),\ldots,\\
&\qquad E(t=\mathrm{id6};d=\mathrm{googlemail};z=28),\\
&\qquad E(t=\mathrm{id1};d=\mathrm{hotmail};z=28),\ldots,\\
&\qquad E(t=\mathrm{id6};d=\mathrm{hotmail};z=28),\\
&\qquad E(t=\mathrm{id1};d=\mathrm{web};z=28),\ldots,\\
&\qquad E(t=\mathrm{id1};d=\mathrm{web};z=28),\\
&\qquad E(t=\mathrm{id1};d=\mathrm{yahoo};z=28),\ldots,\\
&\qquad E(t=\mathrm{id6};d=\mathrm{yahoo};z=28)\big) > 0
\end{aligned}
$$

Da mit $\mathrm{d1}, \ldots, \mathrm{d28}$ nun die jeweils schlechtesten Tagesperformer bezogen auf einzelne Email-Konten vorliegen, kann nun über allen Tagen eine Rangfolge

erstellt werden.

$$\begin{aligned}\mathrm{M6} = \mathrm{rang}\big(&\mathrm{anzahl}(\mathrm{d1},\ldots,\mathrm{d28};\mathrm{gmx}),\\ &\mathrm{anzahl}(\mathrm{d1},\ldots,\mathrm{d28};\mathrm{googlemail}),\\ &\mathrm{anzahl}(\mathrm{d1},\ldots,\mathrm{d28};\mathrm{hotmail}),\\ &\mathrm{anzahl}(\mathrm{d1},\ldots,\mathrm{d28};\mathrm{web}),\\ &\mathrm{anzahl}(\mathrm{d1},\ldots,\mathrm{d28};\mathrm{yahoo})\big)\end{aligned}$$

Die Metrik M6 stellt eine Mischform zwischen gemitteltem und punktuellem Verhalten dar.

M7: Mittlerer Tagesrang für Dienstanbieter aggregiert

Bei dieser Metrik wird für jeden Tag des Betrachtungszeitraums eine Rangfolge ermittelt, welche sich aus der Anzahl von Spam-Nachrichten ergibt, die je Dienstanbieter von allen Testpersonen empfangen werden. Aus den auf die jeweiligen Tage bezogenen Rangfolgen wird durch Berechnung der mittleren Positionen eine Rangfolge für die Dienstanbieter über dem gesamten Zeitraum berechnet. In diesem Zusammenhang werden Hilfsmetriken $\mathrm{r1},\ldots,\mathrm{r28}$ zur Beschreibung der Tagesrangfolgen verwendet.

$$\begin{aligned}\mathrm{r1} = \mathrm{rang}\big(&E(t=\mathrm{id1},\ldots,\mathrm{id6};d=\mathrm{gmx};z=1),\\ &E(t=\mathrm{id1},\ldots,\mathrm{id6};d=\mathrm{googlemail};z=1),\\ &E(t=\mathrm{id1},\ldots,\mathrm{id6};d=\mathrm{hotmail};z=1),\\ &E(t=\mathrm{id1},\ldots,\mathrm{id6};d=\mathrm{web};z=1),\\ &E(t=\mathrm{id1},\ldots,\mathrm{id6};d=\mathrm{yahoo};z=1)\big)\\ \vdots\quad&\vdots\\ \mathrm{r28} = \mathrm{rang}\big(&E(t=\mathrm{id1},\ldots,\mathrm{id6};d=\mathrm{gmx};z=28),\\ &E(t=\mathrm{id1},\ldots,\mathrm{id6};d=\mathrm{googlemail};z=28),\\ &E(t=\mathrm{id1},\ldots,\mathrm{id6};d=\mathrm{hotmail};z=28),\\ &E(t=\mathrm{id1},\ldots,\mathrm{id6};d=\mathrm{web};z=28),\\ &E(t=\mathrm{id1},\ldots,\mathrm{id6};d=\mathrm{yahoo};z=28)\big)\end{aligned}$$

Über diesen Werten kann dann die Rangfolge M7 für die Dienstanbieter berechnet werden.

$$\begin{aligned}\mathrm{M7} = \mathrm{rang}\big(&\mathrm{mpos}(\mathrm{r1},\ldots,\mathrm{r28};\mathrm{gmx}),\\ &\mathrm{mpos}(\mathrm{r1},\ldots,\mathrm{r28};\mathrm{googlemail}),\\ &\mathrm{mpos}(\mathrm{r1},\ldots,\mathrm{r28};\mathrm{hotmail}),\\ &\mathrm{mpos}(\mathrm{r1},\ldots,\mathrm{r28};\mathrm{web}),\\ &\mathrm{mpos}(\mathrm{r1},\ldots,\mathrm{r28};\mathrm{yahoo})\big)\end{aligned}$$

Bei M7 handelt es sich um eine Metrik, durch welche das gemittelte Verhalten von Diensten bewertet werden soll.

M8: Mittlerer Tagesrang über Testpersonen

Die Metrik M8 ist verwandt mit der Metrik M7. Im Gegensatz zu M7 werden bei M8 die Tagesrangfolgen jedoch nicht aggregiert für die Dienstanbieter betrachtet, sondern über den von den jeweiligen Testpersonen bei den jeweiligen Dienstanbietern empfangenen Spam-Nachrichten berechnet. Pro Tag wird also eine 30-elementige Rangfolge berechnet. Über diesen tagesbezogenen Rangfolgen werden dann für jeden Dienstanbieter gemittelt über die Zeit und die Testpersonen eine Rangfolgenposition berechnet. Ausgehend von dieser mittleren Rangfolgenposition wird dann die Rangfolge für die Dienstanbieter gebildet. In diesem Zusammenhang werden wiederum Hilfsmetriken $\mathrm{r1}, \ldots, \mathrm{r28}$ zur Beschreibung der Tagesrangfolgen verwendet, welche sich hier jedoch im Vergleich zu M7 etwas unterscheiden.

$$
\begin{aligned}
\mathrm{r1} = \mathrm{rang}\big(& E(t=\mathrm{id1}; d=\mathrm{gmx}; z=1), \ldots, \\
& E(t=\mathrm{id6}; d=\mathrm{gmx}; z=1), \\
& E(t=\mathrm{id1}; d=\mathrm{googlemail}; z=1), \ldots, \\
& E(t=\mathrm{id6}; d=\mathrm{googlemail}; z=1), \\
& E(t=\mathrm{id1}; d=\mathrm{hotmail}; z=1), \ldots, \\
& E(t=\mathrm{id6}; d=\mathrm{hotmail}; z=1), \\
& E(t=\mathrm{id1}; d=\mathrm{web}; z=1), \ldots, \\
& E(t=\mathrm{id6}; d=\mathrm{web}; z=1), \\
& E(t=\mathrm{id1}; d=\mathrm{yahoo}; z=1), \ldots, \\
& E(t=\mathrm{id6}; d=\mathrm{yahoo}; z=1)\big) \\
\vdots \quad \vdots & \\
\mathrm{r28} = \mathrm{rang}\big(& E(t=\mathrm{id1}; d=\mathrm{gmx}; z=28), \ldots, \\
& E(t=\mathrm{id6}; d=\mathrm{gmx}; z=28), \\
& E(t=\mathrm{id1}; d=\mathrm{googlemail}; z=28), \ldots, \\
& E(t=\mathrm{id6}; d=\mathrm{googlemail}; z=28), \\
& E(t=\mathrm{id1}; d=\mathrm{hotmail}; z=28), \ldots, \\
& E(t=\mathrm{id6}; d=\mathrm{hotmail}; z=28), \\
& E(t=\mathrm{id1}; d=\mathrm{web}; z=28), \ldots, \\
& E(t=\mathrm{id6}; d=\mathrm{web}; z=28), \\
& E(t=\mathrm{id1}; d=\mathrm{yahoo}; z=28), \ldots, \\
& E(t=\mathrm{id6}; d=\mathrm{yahoo}; z=28)\big)
\end{aligned}
$$

Über diesen Werten kann dann die Rangfolge M8 für die Dienstanbieter berechnet werden.

$$\begin{aligned}\mathrm{M8} = \mathrm{rang}\Big(&\mathrm{mpos}\big(\mathrm{r1},\ldots,\mathrm{r28};(\mathrm{id1},\mathrm{gmx}),\ldots,(\mathrm{id6},\mathrm{gmx})\big),\\ &\mathrm{mpos}\big(\mathrm{r1},\ldots,\mathrm{r28};(\mathrm{id1},\mathrm{googlemail}),\ldots,(\mathrm{id6},\mathrm{googlemail})\big),\\ &\mathrm{mpos}\big(\mathrm{r1},\ldots,\mathrm{r28};(\mathrm{id1},\mathrm{hotmail}),\ldots,(\mathrm{id6},\mathrm{hotmail})\big),\\ &\mathrm{mpos}\big(\mathrm{r1},\ldots,\mathrm{r28};(\mathrm{id1},\mathrm{web}),\ldots,(\mathrm{id6},\mathrm{web})\big),\\ &\mathrm{mpos}\big(\mathrm{r1},\ldots,\mathrm{r28};(\mathrm{id1},\mathrm{yahoo}),\ldots,(\mathrm{id6},\mathrm{yahoo})\big)\Big)\end{aligned}$$

Bei M8 handelt es sich um eine Metrik, durch welche das gemittelte Verhalten von Diensten bewertet werden soll.

M9: Verhältnis Spam in Inbox zu Gesamtanzahl Spam

Wenn Spam-Nachrichten empfangen werden, dann sollten diese als Spam-verdächtig gekennzeichnet werden, d. h. in der Spambox abgelegt werden. Zum Vergleich dieses Verhaltens ist es von Interesse, für einen Dienstanbieter die Anzahl der von allen Testpersonen in der Inbox empfangenen Spam-Nachrichten mit der entsprechenden Gesamtanzahl von empfangenen Spam-Nachrichten in Beziehung zu setzen. Metrik M9 vergleicht die Quotienten zwischen Spam-Nachrichten in der Spambox mit der Gesamtanzahl von Spam-Nachrichten in Spambox und Inbox und bildet über diesen eine Rangfolge. Je kleiner ein solcher Quotient ist, desto höher die Bewertung des Dienstanbieters.

$$\begin{aligned}\mathrm{M9} = \mathrm{rang}\Bigg(&\frac{I(t=\mathrm{id1},\ldots,\mathrm{id6};d=\mathrm{gmx};z=1,\ldots,28)}{E(t=\mathrm{id1},\ldots,\mathrm{id6};d=\mathrm{gmx};z=1,\ldots,28)},\\ &\frac{I(t=\mathrm{id1},\ldots,\mathrm{id6};d=\mathrm{googlemail};z=1,\ldots,28)}{E(t=\mathrm{id1},\ldots,\mathrm{id6};d=\mathrm{googlemail};z=1,\ldots,28)},\\ &\frac{I(t=\mathrm{id1},\ldots,\mathrm{id6};d=\mathrm{hotmail};z=1,\ldots,28)}{E(t=\mathrm{id1},\ldots,\mathrm{id6};d=\mathrm{hotmail};z=1,\ldots,28)},\\ &\frac{I(t=\mathrm{id1},\ldots,\mathrm{id6};d=\mathrm{web};z=1,\ldots,28)}{E(t=\mathrm{id1},\ldots,\mathrm{id6};d=\mathrm{web};z=1,\ldots,28)},\\ &\frac{I(t=\mathrm{id1},\ldots,\mathrm{id6};d=\mathrm{yahoo};z=1,\ldots,28)}{E(t=\mathrm{id1},\ldots,\mathrm{id6};d=\mathrm{yahoo};z=1,\ldots,28)}\Bigg)\end{aligned}$$

Bei M9 handelt es sich um eine Metrik, durch welche das gemittelte Verhalten betrachtet wird.

M10: Anzahl externer Spam aggregiert für Dienstanbieter

Die von extern erhaltenen Spam-Nachrichten landen in der Inbox oder der Spambox. Die von intern erhaltenen Spam-Nachrichten landen ausschließlich in der Inbox, könnten jedoch (zumindest theoretisch) sehr viel leichter eliminiert

werden als die von extern empfangenen Spam-Nachrichten, wenn der Dienstanbieter darauf verzichten würde, diese zu versenden und stattdessen seine Werbung im Web-Browser anzeigen würde. Auch wenn der Dienstanbieter vorzieht, seine Werbung per Email zu verschicken, so wird er eine bestimmte Anzahl von Spam-Nachrichten pro Zeitintervall nicht überschreiten. Von einer solchen Maximalanzahl kann man für Spam-Nachrichten, die von extern empfangen werden, nicht ausgehen. Wenn die Spam-Filter eines Dienstanbieters nicht genügend gut eingestellt sind, ist es also theoretisch möglich, dass bei größeren Spam-Wellen eine hohe Anzahl von Spam-Nachrichten empfangen wird. Vor diesem Hintergrund ist eine niedrige Anzahl von externem Spam wünschenswert.

Bei Metrik M10 geht es darum, eine Aussage über die je Dienstanbieter im gesamtem Betrachtungszeitraum über allen Testpersonen von extern erhaltenen Spam-Nachrichten zu treffen. Hierzu wird für M10 über den entsprechenden Anzahlen eine Rangfolge ermittelt.

$$\begin{aligned}\mathrm{M10} = \mathrm{rang}\big(&E_{\mathrm{ext}}(t = \mathrm{id1},\ldots,\mathrm{id6}; d = \mathrm{gmx}; z = 1,\ldots,28),\\ &E_{\mathrm{ext}}(t = \mathrm{id1},\ldots,\mathrm{id6}; d = \mathrm{googlemail}; z = 1,\ldots,28),\\ &E_{\mathrm{ext}}(t = \mathrm{id1},\ldots,\mathrm{id6}; d = \mathrm{hotmail}; z = 1,\ldots,28),\\ &E_{\mathrm{ext}}(t = \mathrm{id1},\ldots,\mathrm{id6}; d = \mathrm{web}; z = 1,\ldots,28),\\ &E_{\mathrm{ext}}(t = \mathrm{id1},\ldots,\mathrm{id6}; d = \mathrm{yahoo}; z = 1,\ldots,28)\big)\end{aligned}$$

Bei M10 handelt es sich um eine Metrik, durch welche das gemittelte Verhalten betrachtet wird.

5.2.3 Verwertung der Metriken für Gesamtergebnis

Mit den Metriken $\mathrm{M1},\ldots,\mathrm{M10}$ liegen nun 10 Ranglisten als Einzelergebnisse vor, in denen unterschiedliche Eigenschaften bewertet werden und anhand derer die jeweiligen Dienstangebote in den jeweiligen Kategorien verglichen werden können. Über den Einzelergebnissen sollte nun jedoch auch ein Gesamtergebnis berechnet werden. Hierzu wird eine Metrik M eingeführt, welche über den arithmetischen Mittelwerten der Dienstanbieterpositionen in den Rangfolgen $\mathrm{M1},\ldots,\mathrm{M10}$ berechnet wird. Diese ergibt sich gemäß

$$\begin{aligned}\mathrm{M} = \mathrm{rang}\big(&\mathrm{mpos}(\mathrm{M1},\ldots,\mathrm{M10}; \mathrm{gmx}),\\ &\mathrm{mpos}(\mathrm{M1},\ldots,\mathrm{M10}; \mathrm{googlemail}),\\ &\mathrm{mpos}(\mathrm{M1},\ldots,\mathrm{M10}; \mathrm{hotmail}),\\ &\mathrm{mpos}(\mathrm{M1},\ldots,\mathrm{M10}; \mathrm{web}),\\ &\mathrm{mpos}(\mathrm{M1},\ldots,\mathrm{M10}; \mathrm{yahoo})\big)\end{aligned}$$

6 Auswertung und Ergebnis

6.1 Allgemeine Beobachtungen

Allgemein ist festzustellen, dass die Anzahl der je Testperson bei einem Dienstanbieter empfangenen Spam-Nachrichten sehr niedrig ist. Dies ist wahrscheinlich darauf zurück zu führen, dass die für die Testpersonen angelegten Email-Konten allesamt noch ziemlich neu und somit noch nicht in vielen bei den Spam-Aktionen berücksichtigten Adresslisten enthalten waren. Die Anzahl der Spam-Nachrichten, die im Betrachtungszeitraum von den sechs Testpersonen bei den fünf Dienstanbietern empfangen wurden, streut zwischen den Extremwerten 0 (bei id4@googlemail, id5@googlemail, id6@googlemail, id4@hotmail, id5@hotmail, id4@yahoo, id5@yahoo, id6@yahoo) und 26 (bei id1@gmx). Das bedeutet, dass selbst im schlechtesten Fall durchschnittlich noch knapp weniger als eine Spam-Nachricht pro Tag empfangen wurde. Somit kann man festhalten, dass in dieser Phase mit noch nicht allzu lang existierenden Email-Konten die Anzahl der empfangenen Spam-Nachrichten für keine Testperson bei keinem Dienstanbieter unzumutbare Ausmaße erreicht hat. Selbst für diejenigen Email-Konten, bei denen die schlechtesten Werte gemessen wurden, befinden sich diese noch in einem erträglichen Rahmen.

Auch wenn in einer jungen Lebensphase eines Email-Kontos die Anzahl der in dem Betrachtungszeitraum empfangenen Spam-Nachrichten bei keinem Dienstanbieter besonders hohe Werte annimmt, sind doch einige interessante Aspekte zu erkennen und festzuhalten.

Tabelle 6.1: Gesamtanzahl Spam je Dienstanbieter von intern / extern / gesamt

Spam-Anzahl	**gmx**	**googlemail**	**hotmail**	**web**	**yahoo**
$E_{\text{int}}(t=\text{id1},\ldots,\text{id6};d;z=1,\ldots,28)$	90	0	3	36	0
$E_{\text{ext}}(t=\text{id1},\ldots,\text{id6};d;z=1,\ldots,28)$	26	18	10	21	8
$E(t=\text{id1},\ldots,\text{id6};d;z=1,\ldots,28)$	116	18	13	57	8

- Spammende Dienstanbieter und nicht spammende Dienstanbieter: Kunden von solchen Dienstanbietern, welche selbst Spam-Nachrichten verschicken, empfangen abgesehen von einer einzigen und später noch zu erwähnenden Ausnahme deutlich mehr Spam-Nachrichten als Kunden von Dienstanbietern, welche Ihre Kunden nicht mit Spam-Nachrichten belästigen. Dies wurde bei den Testpersonen in dem Betrachtungszeitraum so festgestellt. Der erkannte Zusammenhang gilt jedoch wahrscheinlich nur für eine frühe Lebensphase der Email-Konten. In Tabelle 6.1 ist deutlich zu erkennen, dass die Testpersonen insgesamt über GMX und

WEB.DE die meisten Spam-Nachrichten empfangen haben und auch der hohe Anteil der von intern empfangenen Spam-Nachrichten ist zu erkennen (bei GMX 90 von insgesamt 116, bei WEB.DE 36 von insgesamt 57). In Tabelle 6.1 ist außerdem zu erkennen, dass sowohl Google Mail als auch Yahoo! keine internen Spam-Nachrichten versenden (entsprechende Einträge in der Tabelle: 0). Bemerkenswert in Tabelle 6.1 ist, dass Hotmail eine Ausnahme vom oben beschriebenen Zusammenhang darstellt. Obwohl Hotmail wenige interne Spam-Nachrichten und Google Mail keine an seine Kunden verschickt hat, liegt Hotmail in der Gesamtanzahl der Spam-Nachrichten vor Google Mail (bei Hotmail 13 insgesamt, bei Google Mail 18 insgesamt).

- Gesamtanzahl Spam von extern sowie Spam von intern und extern: Betrachtet man die Gesamtanzahl der empfangenen Spam-Nachrichten von intern und extern und vergleicht die Werte für die Dienstanbieter miteinander, dann ergibt sich nach Tabelle 6.1 folgende Rangfolge:

  1. Yahoo! (8)
  2. Hotmail (13)
  3. Google Mail (18)
  4. WEB.DE (57)
  5. GMX (116)

  Zwischen dem besten Wert (8) und dem schlechtesten Wert (116) besteht ein sehr deutlicher Unterschied, der sicherlich auch dadurch begründet ist, dass GMX intern Spam-Nachrichten versendet und Yahoo! dies nicht tut. Betrachtet man jedoch die Werte, bei welchen ausschließlich der von extern erhaltene Spam berücksichtigt wird, dann erkennt man, dass diese Werte zur gleichen Rangfolge führen:

  1. Yahoo! (8)
  2. Hotmail (10)
  3. Google Mail (18)
  4. WEB.DE (21)
  5. GMX (36)

  Dies bedeutet, dass die Berücksichtigung bzw. Nichtberücksichtigung von internen Spam-Nachrichten auf die ermittelte Rangfolge der Dienstanbieter an dieser Stelle keinen Einfluss hat. Andererseits bleibt festzustellen, dass die Testpersonen gerade bei den Dienstanbietern, bei welchen die größte Anzahl von externem Spam-Nachrichten empfangen wird, auch noch durch zusätzliche interne Spam-Nachrichten belästigt werden.

- Durchschnittswerte empfangener Spam-Nachrichten: Auch wenn Durchschnittswerte im Vergleich zu aggregierten Werten vor dem Hintergrund einer Rangfolgenbildung eigentlich keine zusätzliche Information bringen, sollen sie hier dennoch betrachtet werden, da sie dem Betrachter einen Eindruck der Größenordnungen vermitteln, welche hier im Raum stehen. Tabelle 6.2 zeigt die über den Testpersonen mit publizierten Email-Adressen gebildeten Durchschnittswerte von Spam-Nachrichten, die pro Person täglich empfangen wurden. Die Durchschnittswerte sind getrennt nach externem Spam, internem Spam und gesamtem Spam aufgelistet. Dadurch wird für alle Dienstanbieter das bereits zu Beginn dieses Kapitels erwähnte Ergebnis unterstrichen, nach welchem die Gesamtanzahl von empfangenen Spam-Nachrichten bei allen Dienstanbietern sehr niedrig ist. Es ist jedoch anzunehmen, dass diese Durchschnittswerte zu späteren Lebensphasen von Email-Accounts hin deutlich ansteigen werden. Dennoch zeigt Tabelle 6.2 auch, dass die Durchschnittswerte dienstanbieterabhängig stark streuen. Die Werte bewegen sich am oberen Ende (GMX) in einer Größenordnung, bei welcher von einer Person in 5 Tagen durchschnittlich 4 Spam-Nachrichten empfangen werden. Am unteren Ende (Yahoo!) empfängt eine Person durchschnittlich nur 1 Spam-Nachricht in 10 Tagen.

- Publizierte Email-Adressen und nicht-publizierte Email-Adressen: Publizierte und nicht-publizierte Email-Adressen bieten prinzipiell unterschiedliche Rahmenbedingungen für den Empfang von Spam. Dies gilt insbesondere für den Anteil der Spam-Nachrichten, der von extern empfangen wird. Die Anzahl der Spam-Nachrichten von intern an publizierte Email-Adressen stimmt für alle Dienstanbieter ungefähr mit der Anzahl der Spam-Nachrichten von intern an nicht-publizierte Email-Adressen überein, wie in Tabelle 6.3 durch einen Vergleich der Werte in den Zeilen mit $E_{int}(t = \mathrm{id1}, \mathrm{id2}, \mathrm{id3}; d; z = 1, \ldots, 28)$ und $E_{int}(t = \mathrm{id4}, \mathrm{id5}, \mathrm{id6}; d; z = 1, \ldots, 28)$ zu erkennen ist. Bei der Anzahl der von extern empfangenen Spam-Nachrichten ist hingegen ein deutlicher Unterschied zwischen den publizierten und den nicht-publizierten Email-Adressen festzustellen. Dies geht aus den korrespondierenden Werten der Zeilen $E_{ext}(t = \mathrm{id1}, \mathrm{id2}, \mathrm{id3}; d; z = 1, \ldots, 28)$ und $E_{ext}(t = \mathrm{id4}, \mathrm{id5}, \mathrm{id6}; d; z = 1, \ldots, 28)$ in Tabelle 6.3 hervor. Man erkennt, dass die Email-Konten mit den nicht-publizierten Email-Adressen in dieser Lebensphase praktisch keine Spam-Nachrichten erhalten.

- Spamming per Brute Force oder Wörterbuch: Spam-Nachrichten an Email-Konten mit nicht-publizierten Email-Adressen können praktisch nur durch Austesten von Kombinationen auf Basis von Brute Force oder dem Einsatz von Wörterbüchern an die Empfänger gelangen. Dieser Aussage liegt die Annahme zugrunde, dass Dienstbetreiber die Email-Adressen ihrer Kunden nicht an andere Unternehmen zur Versendung von Werbung herausgeben. Sollte ein anderes Unternehmen ein Interesse haben, den Kunden eines Dienstanbieters Werbung zukommen zu lassen, dann geschieht

dies über den Dienstanbieter. Da in der Zeile $E_{ext}(t = \text{id4, id5, id6}; d; z = 1, \ldots, 28)$ von Tabelle 6.3 nicht alle Werte 0 sind, wird deutlich, dass es Spammern hier bereits in der frühen Lebensphase eines Email-Kontos geglückt ist, durch Austesten von Kombinationen eine bis dahin unbekannte Email-Adresse zu finden. Konkret war hier nur eine Testperson über ihr Email-Konto bei GMX betroffen. Bei den anderen Dienstanbietern haben die Testpersonen mit nicht-publizierten Email-Adressen keine Spam-Nachrichten erhalten. Ob dies daran liegt, dass entweder keine Spam-Nachrichten an die entsprechenden Testpersonen mit nicht-publizierten Email-Adressen verschickt wurden oder dass die Dienstbetreiber diese mit ihren Spam-Filtern erfolgreich und für die Testpersonen unbemerkt abgewehrt haben, kann nicht gesagt werden. Die bei GMX betroffene Testperson hat in dem Beobachtungszeitraum 3 Spam-Nachrichten von extern erhalten. Es ist an dieser Stelle jedoch zu bemerken, dass dieselbe Testperson bei den anderen Dienstanbietern keinen externen Spam erhalten hat, obwohl sie dort wegen Gleichheit der id abgesehen vom Domain-Namen die gleiche Email-Adresse besaß.

Tabelle 6.2: Durchschnittswerte Spam je Person und Tag für publizierte Email-Adressen

Spam-Anzahl	**gmx**	**googlemail**	**hotmail**	**web**	**yahoo**
$Ø_{int}$ je Person und Tag	0,52	0	0,02	0,21	0
$Ø_{ext}$ je Person und Tag	0,27	0,21	0,12	0,25	0,10
Ø je Person und Tag	0,80	0,21	0,14	0,46	0,10

Tabelle 6.3: Anzahl Spam je Dienstanbieter von intern / extern / gesamt für publizierte (id1,id2,id3) und nicht-publizierte (id4,id5,id6) Email-Adressen

Spam-Anzahl	**gmx**	**googlemail**	**hotmail**	**web**	**yahoo**
$E_{int}(t = \text{id1, id2, id3}; d; z = 1, \ldots, 28)$	44	0	2	18	0
$E_{ext}(t = \text{id1, id2, id3}; d; z = 1, \ldots, 28)$	23	18	10	21	8
$E(t = \text{id1, id2, id3}; d; z = 1, \ldots, 28)$	67	18	12	39	8
$E_{int}(t = \text{id4, id5, id6}; d; z = 1, \ldots, 28)$	46	0	1	18	0
$E_{ext}(t = \text{id4, id5, id6}; d; z = 1, \ldots, 28)$	3	0	0	0	0
$E(t = \text{id4, id5, id6}; d; z = 1, \ldots, 28)$	49	0	1	18	0

Damit sind nun einige Eigenschaften geklärt, die für einen Kunden eines kostenfreien Email-Angebots hinsichtlich Spam von Relevanz sind. Auch wenn für die frühe Lebensphase von Email-Konten bei allen betrachteten Dienstanbietern je Testperson nur Werte ermittelt wurden, die für einen typischen Nutzer wohl tolerierbar sind, ist aufgefallen, dass diese Werte dienstanbieterabhängig stark streuen. Die zuvor vorgenommene Differenzierung bei der Betrachtung hat möglicherweise beim Leser bereits dazu beigetragen, sich einen ersten Eindruck über die betrachteten Dienstanbieter bzgl. bestimmter Spam-Eigenschaften zu bilden.

Im Folgenden soll es nun darum gehen, die im vorangegangenen Kapitel vorgestellten Metriken auf die gewonnenen Messwerte anzuwenden und somit eine Basis für den Vergleich der Dienstanbieter zu schaffen.

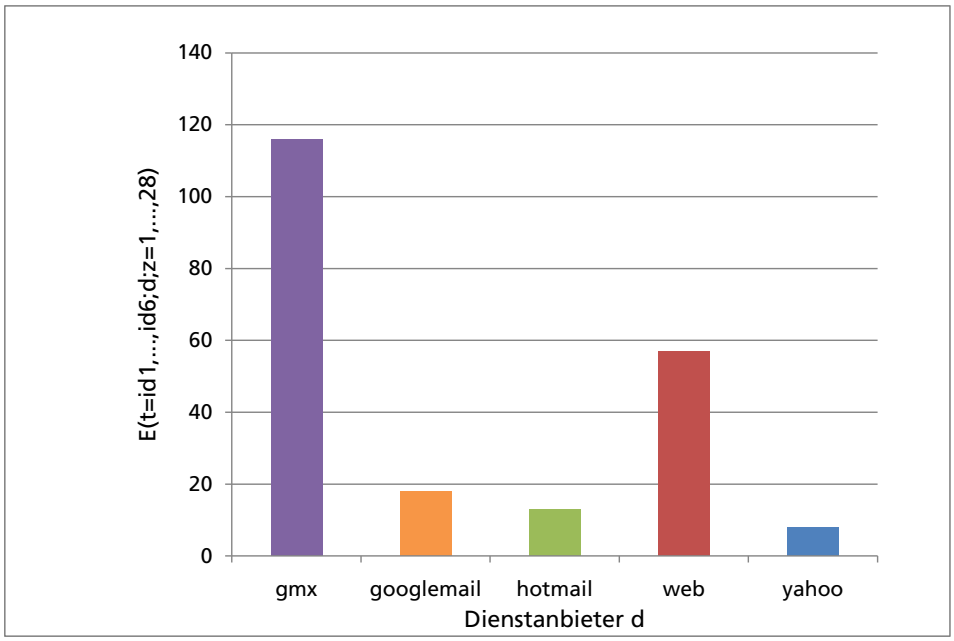
6.2 Auswertung der Metriken

Nachfolgend werden die in dem Beobachtungszeitraum gewonnen Messwerte verarbeitet und im Rahmen der Metriken M1 bis M10 ausgewertet. Da es sich hierbei stets um quantifizierbare Kenngrößen handelt, können diese nachvollziehbar für den Vergleich der Dienstanbieter verwendet werden. Abschließend wird aus den Metriken M1 bis M10 eine Gesamtmetrik M berechnet.

6.2.1 Metrik M1

Das dieser Metrik zugrunde liegende Kriterium für den Vergleich der Dienstanbieter bezieht sich auf die Gesamtanzahl von Spam-Nachrichten, die alle betrachteten Testpersonen über dem gesamten Betrachtungszeitraum bei den jeweiligen Dienstanbietern empfangen haben. Diese Gesamtanzahl umfasst sowohl Spam von extern als auch von intern.

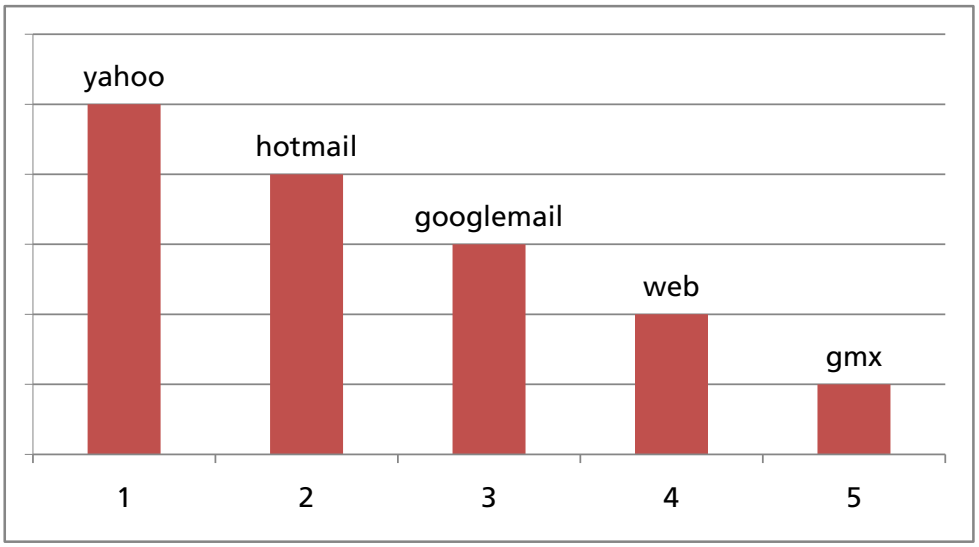
Abbildung 6.1: Gesamtanzahl Spam je Dienstanbieter



Man erkennt in Abbildung 6.1, dass die dienstanbieterabhängigen Gesamtanzahlen sehr stark auseinander liegen. Bei GMX und WEB.DE fällt um ein Vielfaches mehr Spam an als bei Google Mail, Hotmail und Yahoo!. Der Wert von GMX liegt selbst noch einmal ungefähr doppelt so hoch wie der Wert von WEB.DE.

Ausgehend von diesen Werten lässt sich eine Rangfolge erstellen, anhand derer die Dienstanbieter hinsichtlich der im Beobachtungszeitraum festgestellten Gesamtanzahl von Spam-Nachrichten verglichen werden können. Man beachte, dass die Rangfolge sich lediglich an der Größer- oder Kleiner-Relation der Messwerte orientiert und sie nicht berücksichtigt, ob die Messwerte nahe beieinander oder sehr weit voneinander entfernt liegen.

Abbildung 6.2: Rangfolge für M1



6.2.2 Metrik M2

Wurde bei M1 das Spam-Aufkommen bei den Testpersonen noch über den Dienstanbietern aggregiert betrachtet, so wird bei M2 nun die Spam-Anzahl für die Testpersonen betrachtet. Bei einer über den Dienstanbietern aggregierten Betrachtung verliert unter Umständen ein besonders umfangreiches Spam-Aufkommen an Bedeutung. Deshalb geht es bei M2 darum, für jeden Dienstanbieter diejenige Testperson zu ermitteln, die über dem gesamten Zeitraum die meisten Spam-Nachrichten bekommen hat. Dies umfasst sowohl Spam von extern als auch von intern. Diese Testpersonen werden in Tabelle 6.4 zusammen mit der jeweils bei dem entsprechenden Dienstanbieter erhaltenen Anzahl von Spam-Nachrichten dargestellt. Die schlechtesten (höchsten) Werte je Dienstanbieter sind in Tabelle 6.4 hervorgehoben.

Tabelle 6.4: Gesamtanzahl Spam für am stärksten betroffene Testpersonen je Dienstanbieter

Person	gmx	googlemail	hotmail	web	yahoo
id1	**26**	5	4	11	1
id2	19	5	**6**	**20**	**4**
id3	22	**8**	2	8	3
id4	16	0	0	0	0
id5	15	0	0	0	0
id6	18	0	1	1	0

Die in Tabelle 6.4 markierten Werte sind in Abbildung 6.3 dargestellt. Wie man dort erkennen kann, überragen die Werte bei GMX und WEB.DE die Werte bei Google Mail, Hotmail und Yahoo! deutlich. Bei GMX und WEB.DE erhielt die Testperson mit den schlechtesten Werten um ein Vielfaches mehr Spam-Nachrichten als bei den anderen Dienstanbietern.

Ausgehend von dieser Auswertung lässt sich die Rangfolge der Dienstanbieter nach M2 bilden, die in Abbildung 6.4 gezeigt wird. Auch wenn für M2 die

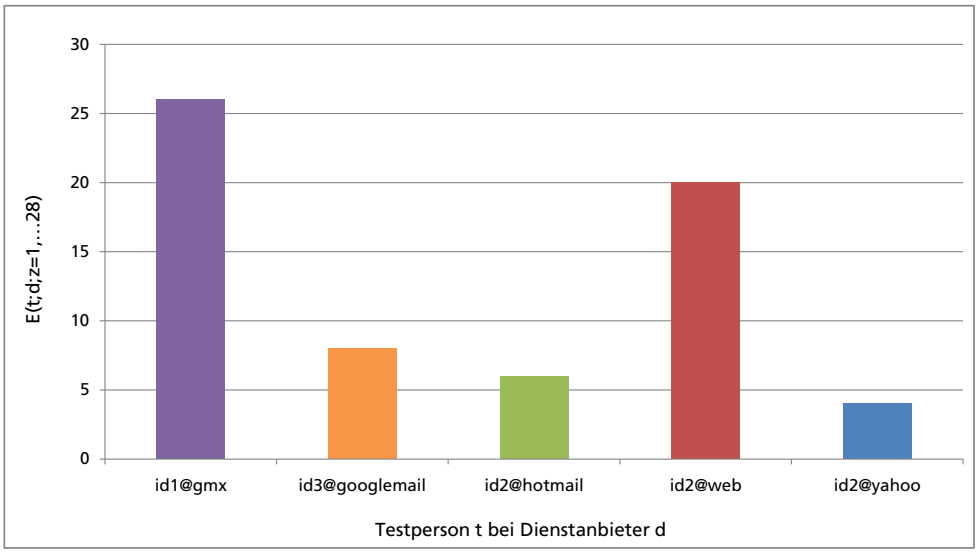


Abbildung 6.3: Gesamtanzahl Spam für am stärksten betroffene Testpersonen je Dienstanbieter

Messwerte in anderer Weise im Vergleich zu M1 ausgewertet wurden, stimmt die Rangfolge für M2 mit der für M1 überein.

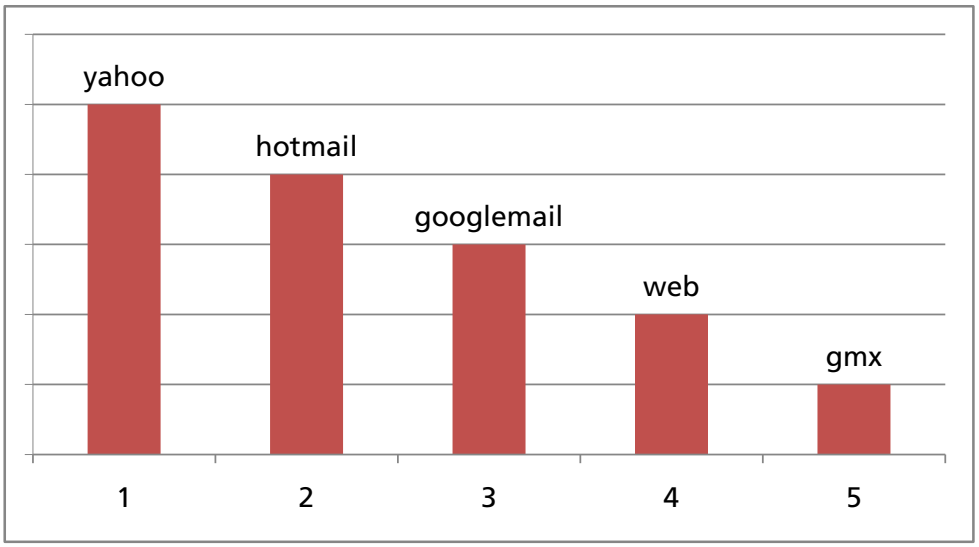


Abbildung 6.4: Rangfolge für M2

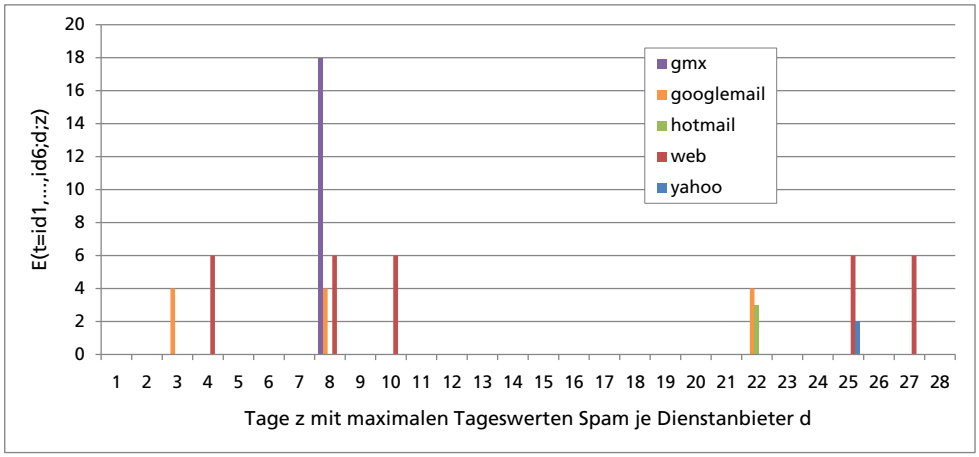
6.2.3 Metrik M3

Bei M3 wird das Spam-Aufkommen erneut über allen Testpersonen je Dienstanbieter aggregiert betrachtet. Es steht jedoch hierbei nicht die über der Zeit ermittelte Gesamtanzahl im Vordergrund, sondern es wird das Spam-Aufkommen je Tag betrachtet. Somit sollen etwaige Tage mit besonders hohem Spam-Aufkommen je Dienstanbieter berücksichtigt werden, die in einer zeitlich aggregierten Betrachtung nach M1 möglicherweise keine Berücksichtigung finden.

Es werden bei M3 für jeden Dienstanbieter aggregiert für alle Testpersonen diejenigen Tage ermittelt, an welchen das Spam-Aufkommen je Dienstanbieter seinen maximalen Wert erreicht hat. Abbildung 6.5 zeigt für alle Anbieter die Tage

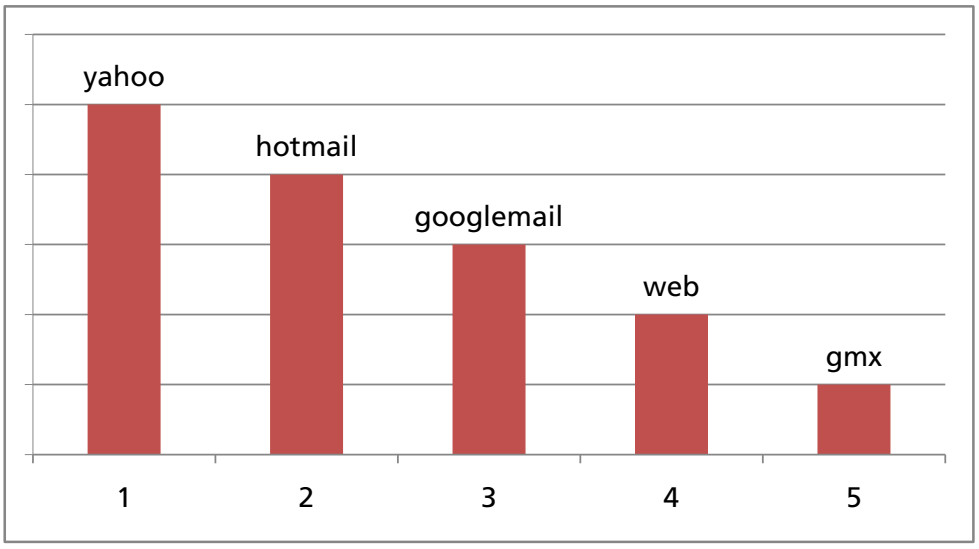
mit den schlechtesten (höchsten) Tageswerten. Man beachte, dass ein solcher auf einen Dienstanbieter bezogener schlechtester Tageswert an mehreren Tagen auftreten kann, wie dies in Abbildung 6.5 für Google Mail und WEB.DE der Fall ist. Wie man außerdem in Abbildung 6.5 leicht feststellen kann, überragt der schlechteste Tageswert für GMX die schlechtesten Tageswerte für die anderen Dienstanbieter um ein Vielfaches. Die schlechtesten Tageswerte von Yahoo!, Hotmail und Google Mail sind im Vergleich dazu sehr niedrig. Ursprüngliche Erwartungen, dass sich die schlechtesten Tageswerte rund um den Valentinstag einstellen werden, haben sich bei der Untersuchung nicht bewahrheitet.

Abbildung 6.5: Maximale Gesamtanzahl Spam pro Tag je Dienstanbieter



Diese schlechtesten (höchsten) Tageswerte für die Dienstanbieter können dann miteinander verglichen werden und man erhält die in Abbildung 6.6 gezeigte Rangfolge. Auch wenn hier ein anderes Kriterium im Fokus der Auswertung stand, stimmt die Rangfolge für M3 mit den Rangfolgen für M1 und M2 überein.

Abbildung 6.6: Rangfolge für M3



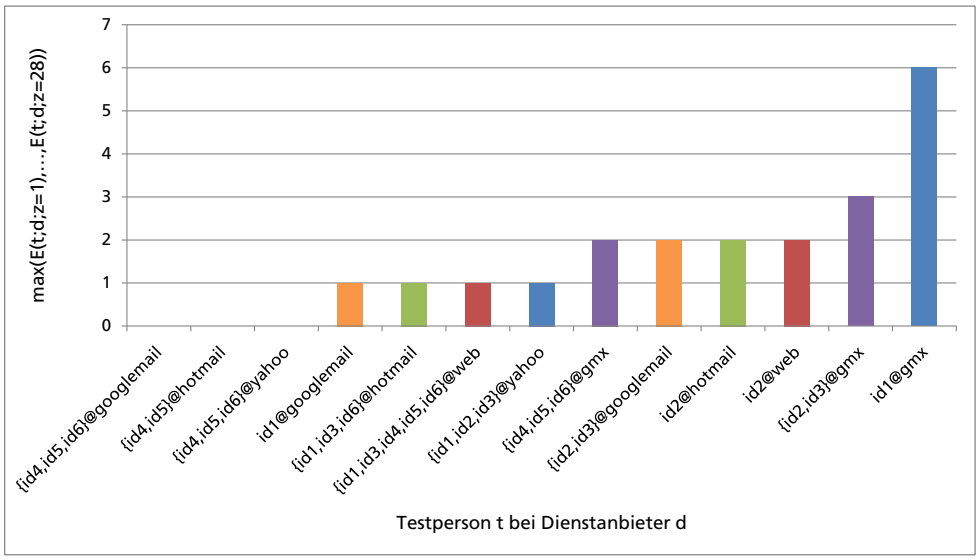
6.2.4 Metrik M4

Wurden bei den Metriken M2 und M3 die in M1 enthaltenen Aggregationen entweder nach Testpersonen oder nach Zeit durchgeführt, so werden in der Metrik M4 die Aggregationen nun sowohl nach Testpersonen als auch nach Zeit durchgeführt. Es wird für jede Kombination aus Testperson und Dienstanbieter über der Zeit der schlechteste (höchste) Tageswert von erhaltenen Spam-Nachrichten ermittelt. Diese Werte sind in Tabelle 6.5 und als Diagramm in Abbildung 6.7 für alle Kombinationen von Testpersonen und Dienstanbietern dargestellt.

Tabelle 6.5: Maximale Gesamtanzahl Spam pro Tag je Email-Account

Person	gmx	googlemail	hotmail	web	yahoo
id1	6	1	1	1	1
id2	3	2	2	2	1
id3	3	2	1	1	1
id4	2	0	0	1	0
id5	2	0	0	1	0
id6	2	0	1	1	0

Abbildung 6.7: Maximale Gesamtanzahl Spam pro Tag je Testperson und Dienstanbieter



In Tabelle 6.5 bzw. in Abbildung 6.7 ist zu erkennen, dass die schlechtesten Tageswerte für die Testpersonen allesamt im einstelligen Bereich liegen. Gehäuft treten dort die Werte 0, 1 und 2 auf. Lediglich bei Testperson id1 bei dem Dienstanbieter GMX liegt ein Ausreißer vor, der jedoch vom Absolutwert 6 her immer noch relativ niedrig ist (Interpretation: »id1@gmx hat maximal 6 Spam-Nachrichten pro Tag bekommen«). Weiterhin sind auch die Testpersonen erkennbar, die über den gesamten Beobachtungszeitraum hinweg keine Email bekommen haben, was zu einem Maximalwert 0 geführt hat.

Ausgehend von den 30 in Tabelle 6.5 bzw. in Abbildung 6.7 gezeigten Werten wird nun für die Kombinationen aus Testperson und Dienstanbieter eine 30er-

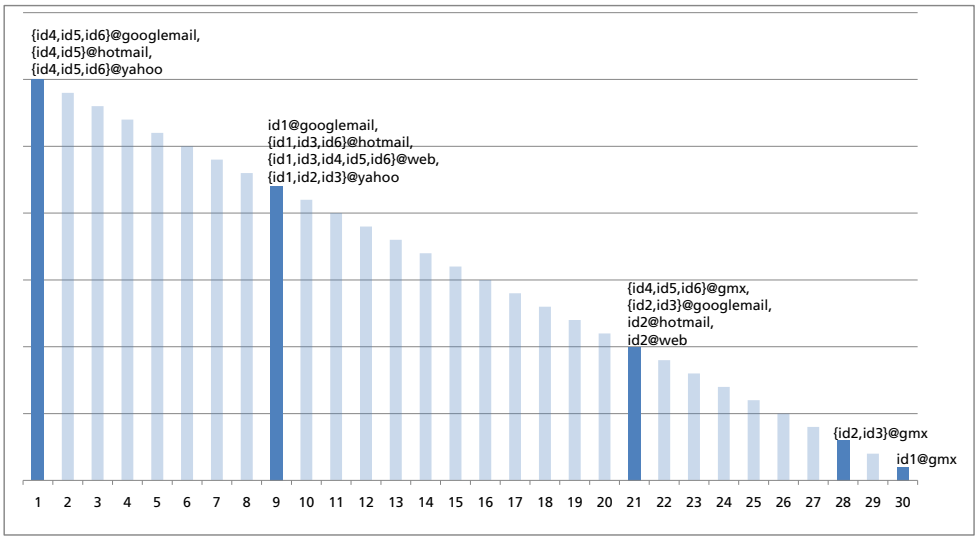


Abbildung 6.8: Rangfolge über maximale Gesamtanzahl Spam pro Tag je Testperson und Dienstanbieter

Rangfolge ermittelt. Diese wird in Abbildung 6.8 dargestellt. Die Häufung von Werten in Tabelle 6.5 bzw. in Abbildung 6.7 schlägt sich in Abbildung 6.8 dahingehend nieder, dass einige Rangfolgenpositionen in der 30er-Rangfolge sehr gehäuft vergeben werden, wodurch wiederum sehr viele Plätze in der Rangfolge nicht vergeben werden, z. B. die Plätze 2–8, 10–20.

Die gezeigte 30er-Rangfolge wird nun zur Vergleichbarkeit der Dienste noch zu einer 5er-Rangfolge aggregiert, indem die mittleren Rangfolgenpostionen für die jeweiligen Dienstanbieter berechnet werden. Das Ergebnis dieser Berechnung wird in Tabelle 6.6 gezeigt.

Tabelle 6.6: Mittlere Rangfolgenposition nach Abbildung 6.8

Dienstanbieter	**gmx**	**googlemail**	**hotmail**	**web**	**yahoo**
Mittelwerte	149/6 = 24,83	54/6 = 9	50/6 = 8,33	66/6 = 11	30/6 = 5

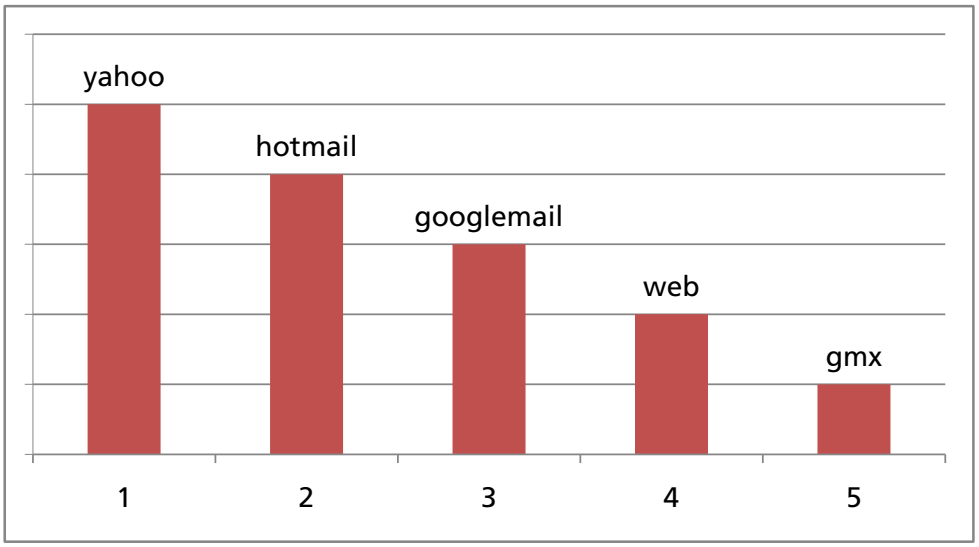
Aus den in Tabelle 6.6 gezeigten Werten wird dann die Rangfolge nach M4 aufgestellt (5er-Rangfolge), welche in Abbildung 6.9 dargestellt wird. Diese Rangfolge stimmt mit den Rangfolgen M1–M3 überein.

6.2.5 Metrik M5

Im Gegensatz bei den Metriken M1–M4, bei denen die Anzahlen von empfangenen Spam-Emails im Vordergrund standen, zielt die Metrik M5 auf die Anzahl der Tage ab, an welchen über einen Dienstanbieter aggregiert für alle Testpersonen die jeweils schlechtesten Tageswerte (Werte größer Null) gemessen wurden. Es wurden zur Auswertung also für jeden einzelnen Tag der (oder die) Dienstanbieter bestimmt, über welchen die Testpersonen zusammengenommen die meisten Emails empfangen haben.

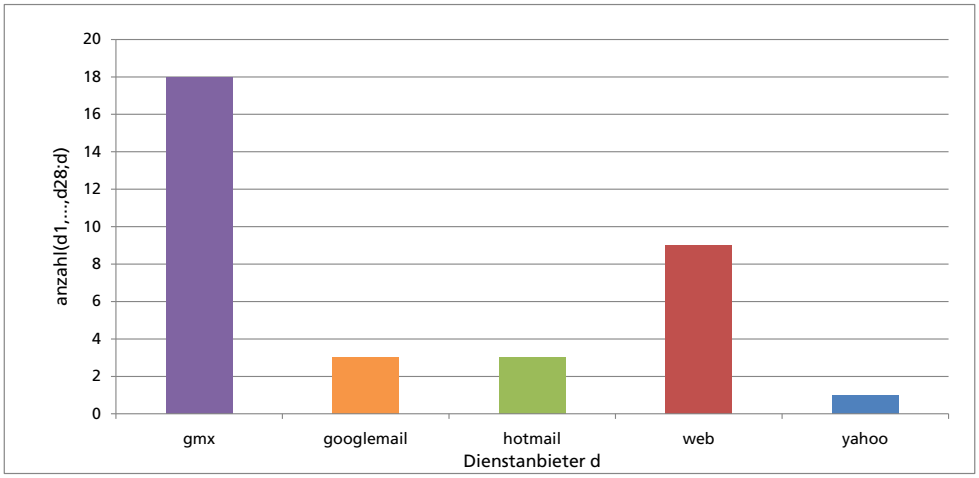
Danach wurde ermittelt, an wie vielen Tagen ein Dienstanbieter den schlechtesten Tageswert aggregiert über alle Testpersonen erreicht hat. Diese Anzahl ist

Abbildung 6.9: Rangfolge für M4



letztendlich das relevante Kriterium für die Metrik M5. Die ermittelten Werte werden in dem Diagramm von Abbildung 6.10 gezeigt. Auch hier ist zu erkennen, dass die Werte für GMX und WEB.DE die Werte für Google Mail, Hotmail und Yahoo! um ein Vielfaches übersteigen. Yahoo! hat im Betrachtungszeitraum einmal den schlechtesten Tageswert erzielt, Google Mail und Hotmail je dreimal.

Abbildung 6.10: Anzahl Tage mit schlechtesten Tageswerten für Dienstanbieter aggregiert

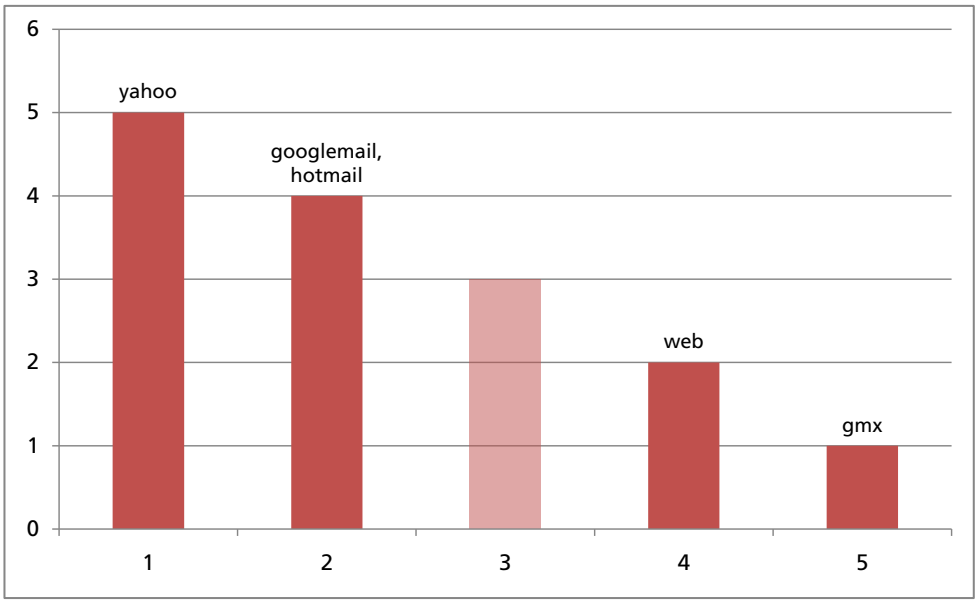


Aus den in Abbildung 6.10 gezeigten Werten ergibt sich die in Abbildung 6.11 gezeigte Rangfolge für die Dienstanbieter. In dieser Rangfolge belegen Google Mail und Hotmail den zweiten Platz. Der dritte Platz wurde deshalb nicht vergeben.

6.2.6 Metrik M6

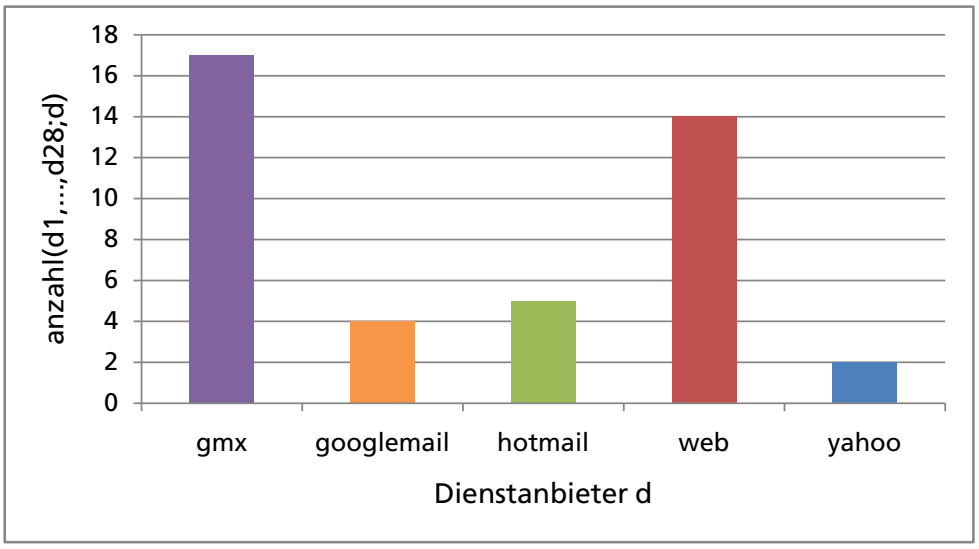
Wurden bei der Metrik M5 die Anzahl der Tage mit den schlechtesten Tageswerten aggregiert über allen Testpersonen gezählt, so wird bei der Metrik M6 nun die Anzahl der Tage mit den schlechtesten Tageswerten je Testperson betrachtet.

Abbildung 6.11: Rangfolge für M5



Auch hier werden nur schlechteste Tageswerte gezählt, wenn diese größer als Null sind. Bei der Auswertung wurden für jeden einzelnen Tag die Kombination aus Testperson(en) und Dienstanbieter(n) bestimmt, welche an dem entsprechenden Tag die meisten Emails empfangen haben. Hierbei war es durchaus möglich, dass an einem Tag der schlechteste Tageswert bei mehr als einer Kombination aus Testperson und Dienstanbieter erreicht wurde.

Abbildung 6.12: Anzahl Tage mit schlechtesten Tageswerten für Testpersonen



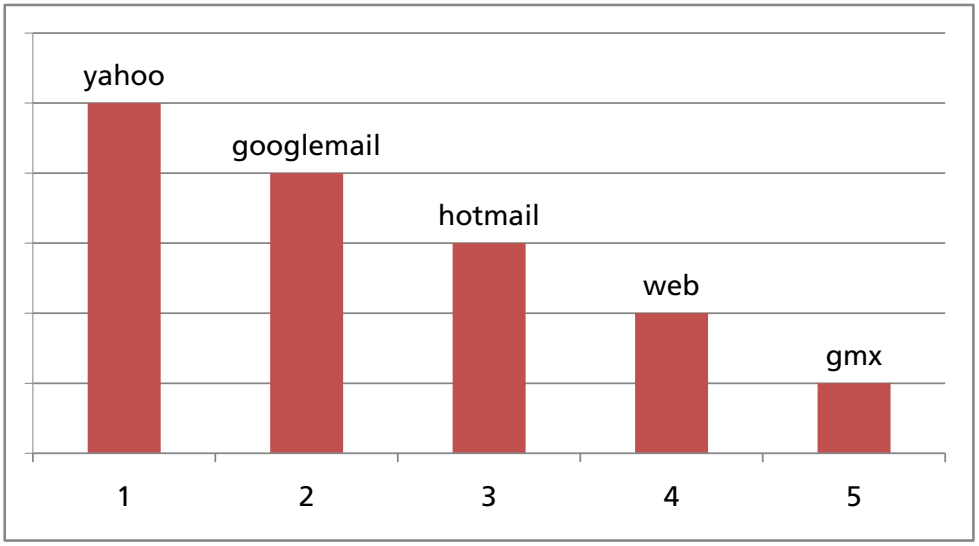
Anschließend wurde ermittelt, an wie vielen Tagen Kombinationen mit den jeweiligen Dienstanbietern den schlechtesten Tageswert erreicht haben. Diese Anzahl stellt das relevante Kriterium für Metrik M6 dar. Die so ermittelte Anzahl von schlechtesten Tageswerten wird dienstanbieterabhängig in Abbildung 6.12 gezeigt. In Abbildung 6.12 ist zu erkennen, dass die schlechtesten Tageswerte wieder am häufigsten (17 mal) bei denjenigen Testpersonen auftreten, die Kunden von GMX sind. Die schlechtesten Tageswerte werden am zweithäufigsten (14 mal) von WEB.DE-Kunden erreicht. Im Gegensatz dazu schneiden die

Yahoo!-Kunden mit nur 2 schlechtesten Tageswerten am besten ab.

Haben Google Mail und Hotmail in der aggregierten Betrachtung nach M5 noch gleichauf gelegen, so hat sich dies nun in der nicht-aggregierten Betrachtung gemäß M6 verändert. Hier liegt nun Google Mail mit 4 schlechtesten Tageswerten vor Hotmail mit 5 schlechtesten Tageswerten. Die gemessenen Werte führen zu der in Abbildung 6.13 gezeigten Rangfolge.

An dieser Stelle wird auch deutlich, dass leichte Änderungen bei der Auswertung zu Unterschieden in der Rangfolge führen können. Vor diesem Hintergrund ist es im Sinne einer fairen Auswertung wichtig, dass man verschiedene Methoden zur Auswertung berücksichtigt.

Abbildung 6.13: Rangfolge für M6



6.2.7 Metrik M7

Nachdem bei Metrik M3 mit den tagesbezogenen Maximalwerten über aggregierten Testpersonen je Dienstanbieter Ausreißer betrachtet wurden, werden nun bei Metrik M7 nicht nur die tagesbezogenen Maximalwerte, sondern alle gemessenen Tageswerte betrachtet. Damit steht die Metrik M7 auch in einer gewissen Verwandtschaft zu Metrik M1.

Hierzu wird für jeden einzelnen Tag eine Rangfolge über der Anzahl von allen Spam-Nachrichten berechnet, bei welcher die Testpersonen je Dienstanbieter aggregiert betrachtet werden. Dadurch erhält man eine 5er-Rangfolge der Dienstanbieter für jeden Tag des Betrachtungszeitraums, d. h. also insgesamt 28 verschiedene 5er-Rangfolgen. Ausgehend von diesen tagesbezogenen 5er-Rangfolgen wird dann das arithmetische Mittel der Rangpositionen der Dienstanbieter berechnet. Diese Mittelwerte werden in Abbildung 6.14 dargestellt. Man erkennt, dass die Mittelwerte von Yahoo! (1,46), Hotmail (1,61) und Google Mail (1,68) bei niedrigen Werten sehr nahe beieinander liegen, wohingegen die Mittelwerte von GMX (3,56) und WEB.DE (3,07) bei höheren Werten relativ nahe zusammen liegen.

Abbildung 6.14: Mittlerer Tagesrang für Dienstanbieter aggregiert

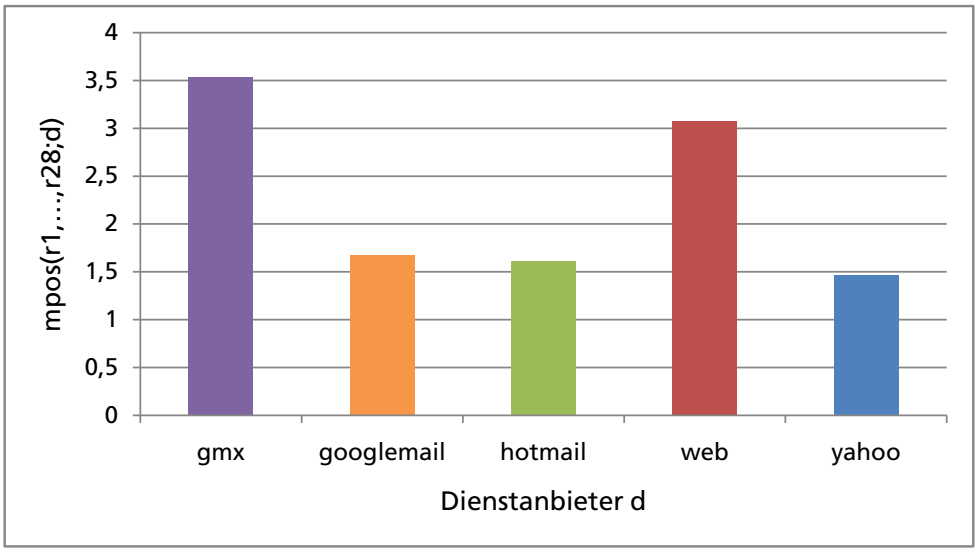
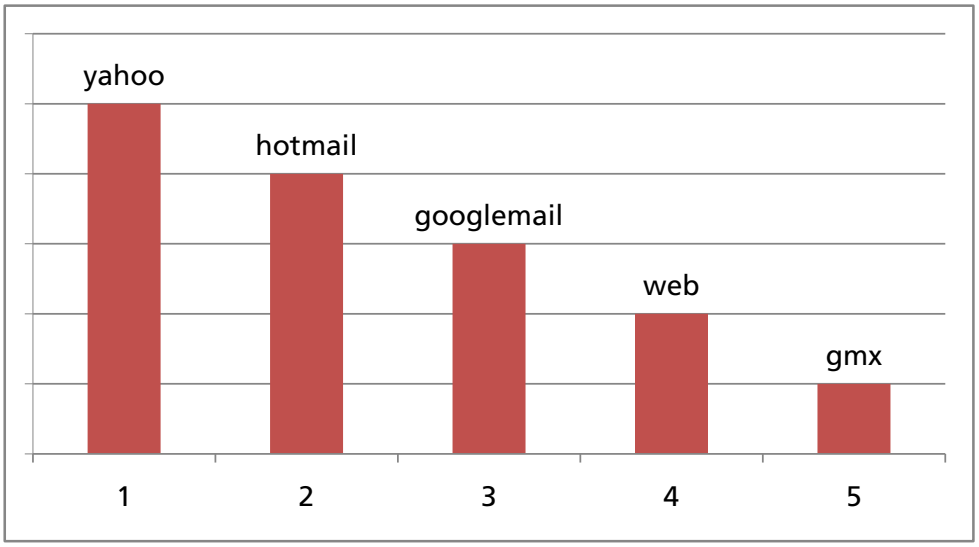


Abbildung 6.15: Rangfolge für M7



Ausgehend von dem arithmetischen Mittelwerten wird dann eine Rangfolge für die Dienstanbieter aufgestellt. Die so erhaltene Rangfolge stimmt mit den Rangfolgen M1–M4 überein.

6.2.8 Metrik M8

Bei Metrik M8 werden die Testpersonen nicht mehr wie in Metrik M7 aggregiert betrachtet. Hier werden nun tagesbezogene Rangfolgen (30er-Rangfolgen) über allen Kombinationen von Testpersonen und Dienstanbietern berechnet.

Nachdem für alle 28 Tage des Betrachtungszeitraums 30er-Rangfolgen ermittelt wurden, können nun für die 30 verschiedenen Kombinationen von Testpersonen und Dienstanbietern über Bildung der arithmetischen Mittelwerte die mittleren Rangfolgenpositionen berechnet werden (30 Mittelwerte). Diese werden in Abbildung 6.16 dargestellt.

Abbildung 6.16: Mittlerer Tagesrang je Testperson

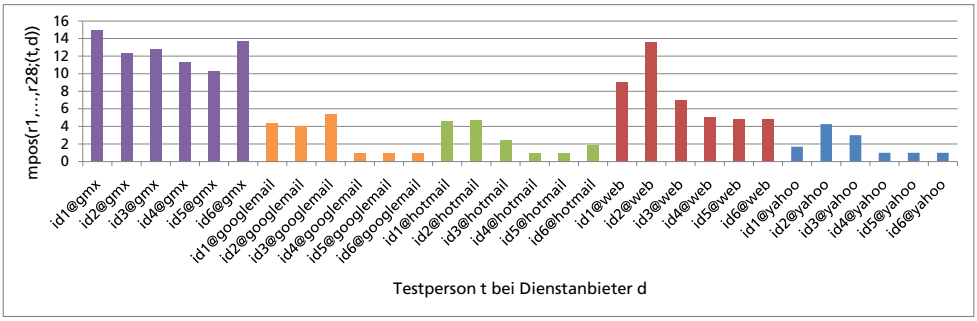
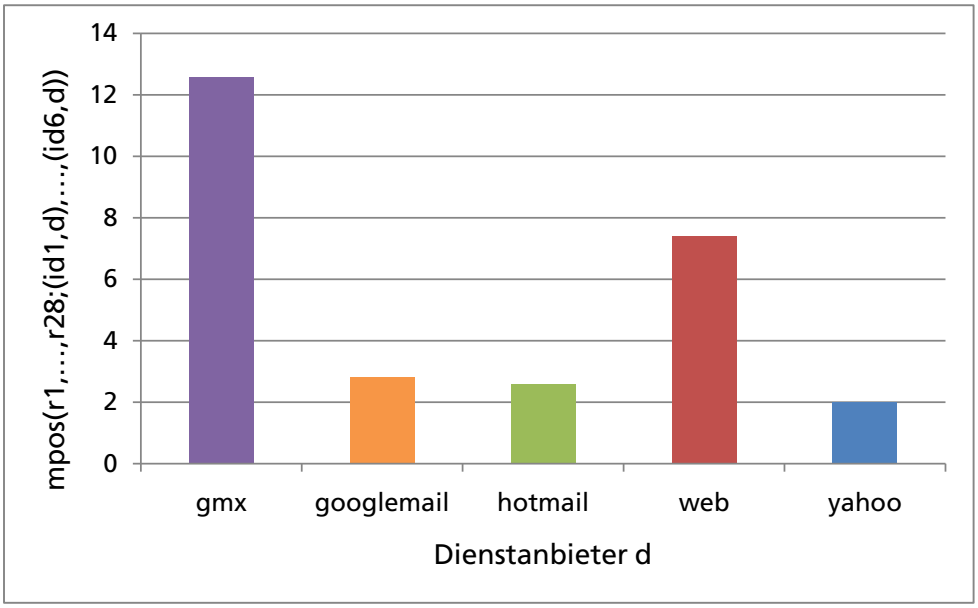


Abbildung 6.17: Mittlerer Tagesrang für Testpersonen über Dienstanbieter aggregiert



Um eine Vergleichbarkeit für die Dienstanbieter zu erzielen, wird aus den vorliegenden Mittelwerten je Dienstanbieter ein neuer Mittelwert berechnet. Diese dienstanbieterbezogenen Mittelwerte werden in Abbildung 6.17 gezeigt. Sie streuen sehr stark zwischen kleinen Werten für Google Mail, Hotmail und Yahoo! und deutlich höheren Werten für GMX und WEB.DE.

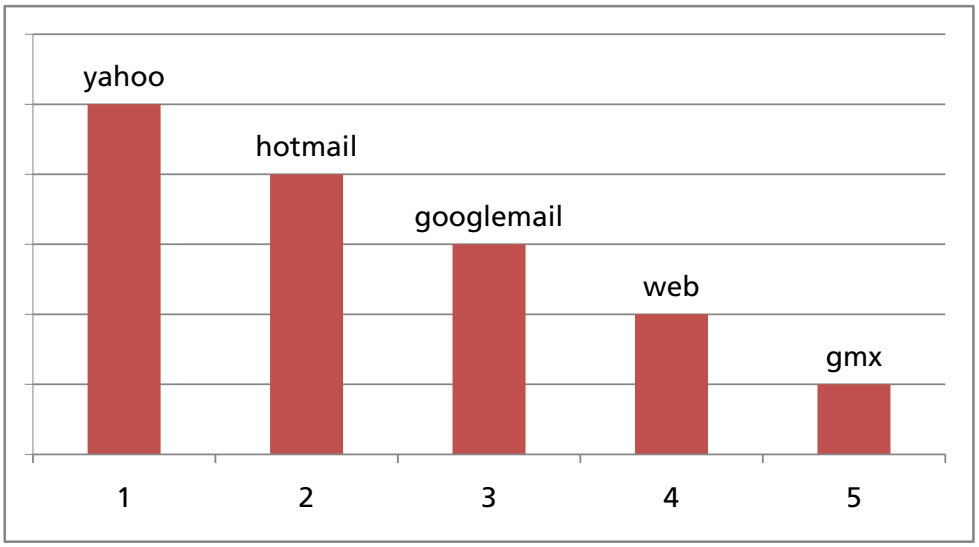
Auf Basis der dienstanbieterbezogenen Mittelwerte kann dann die Rangfolge für die Dienstanbieter aufgestellt werden. Die ermittelte Rangfolge entspricht den Rangfolgen M1–M4 und M7.

6.2.9 Metrik M9

Bei M9 wird das Verhältnis der Anzahl von Spam-Nachrichten, die in der Inbox von Testpersonen landen, zur Gesamtanzahl von Spam-Nachrichten betrachtet, die entweder in der Inbox oder in der Spambox empfangen werden. Die Anzahlen werden hierbei über allen Testpersonen und über dem gesamten Betrachtungszeitraum aggregiert.

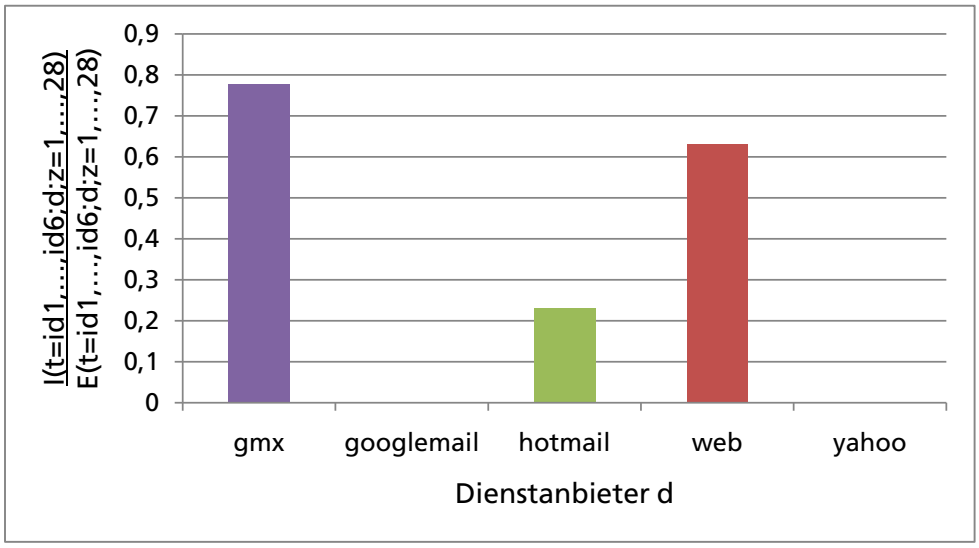
Wertet man die empfangenen Spam-Nachrichten aus, dann ergeben sich für Google Mail und Yahoo! der Bestwert 0, da bei beiden Anbietern keine Spam-

Abbildung 6.18: Rangfolge für M8



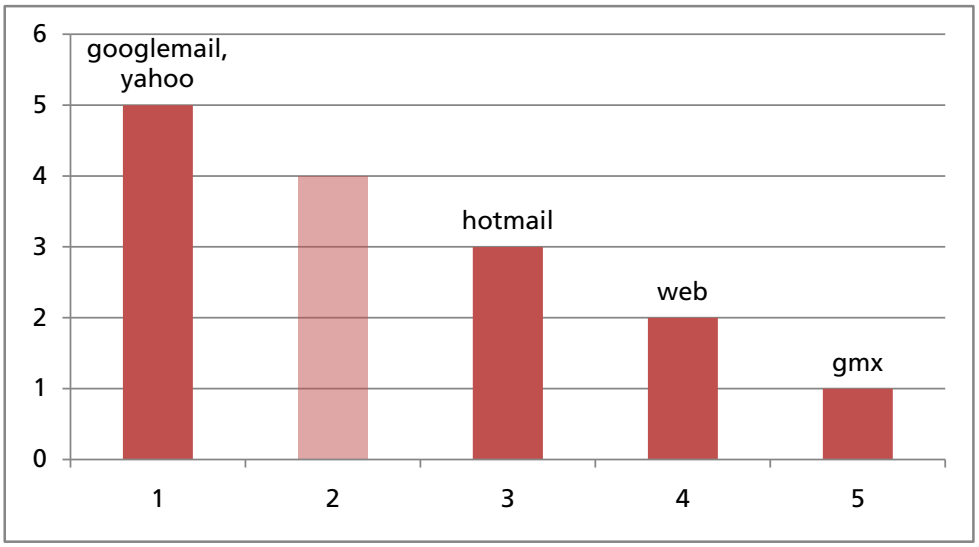
Nachrichten in der Inbox landeten. Für Hotmail ergibt sich ein Quotient von 0,23. Deutlich anders sieht es bei GMX (Quotient 0,78) und WEB.DE (Quotient 0,63) aus. Diese doch eher hohen Quotientenwerte ergeben sich dadurch, dass unter den empfangenen Spam-Nachrichten sehr viele von dem Dienstanbieter selbst stammen. Interne Spam-Nachrichten werden automatisch in der Inbox abgelegt. Die Quotienten für die jeweiligen Dienstanbieter sind in Abbildung 6.19 dargestellt. Es ist jedoch bemerkenswert, dass bei allen Dienstanbietern keine externe Spam-Nachricht in der Inbox gelandet ist. Dies zeugt von einer gewissen Qualität der eingesetzten Spam-Filter, wobei man aber aus dieser kleinen Stichprobe nicht auf eine 100%-ige Zuverlässigkeit der Filter schließen kann.

Abbildung 6.19: Verhältnis Spam in Inbox zu Spam insgesamt je Testperson



Aus diesen Werten ergibt sich die in Abbildung 6.20 gezeigte Rangfolge der Dienstanbieter, in welcher Google Mail zusammen mit Yahoo! auf dem ersten Platz liegen. Wegen der Doppelbelegung von Platz 1 wird Platz 2 nicht vergeben.

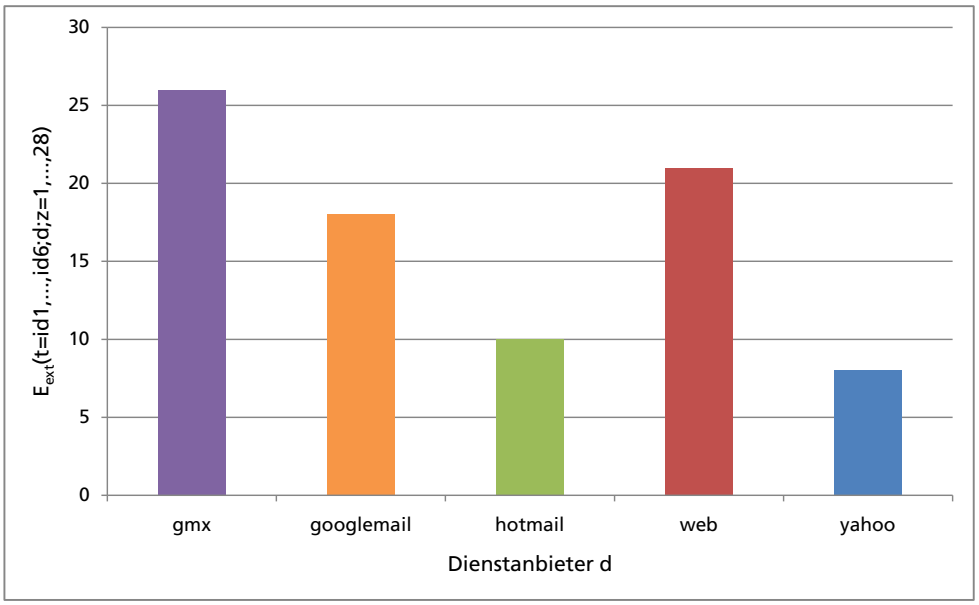
Abbildung 6.20: Rangfolge für M9



6.2.10 Metrik M10

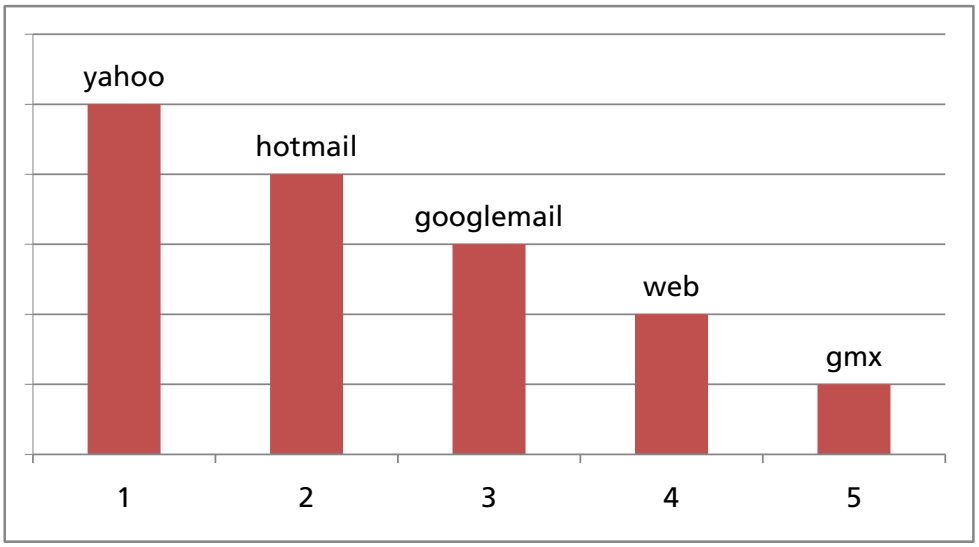
Bei Metrik M10 wird die Gesamtanzahl von Spam-Nachrichten betrachtet, welche von extern empfangen werden. Hierbei werden die Spam-Nachrichten je Dienstanbieter über allen Testpersonen und für den kompletten Betrachtungszeitraum aggregiert. Es werden hier die Spam-Nachrichten betrachtet, die sowohl in der Spambox als auch in der Inbox der Testpersonen landen.

Abbildung 6.21: Anzahl externer Spam aggregiert für Dienstanbieter



Die gemessenen Werte werden in Abbildung 6.21 dargestellt. Es fällt auf, dass die dienstanbieterabhängigen Anzahlen von Spam-Nachrichten nicht so stark streuen, wie die Werte einiger vorangegangener Metriken. Hier liegt Yahoo! knapp vor Hotmail. Danach folgen erst mit deutlichem Abstand Google Mail, dann WEB.DE und GMX.

Abbildung 6.22: Rangfolge für M10



Die gemessenen Werte werden als Rangfolge in Abbildung 6.22 dargestellt. Die Rangfolge entspricht den Rangfolgen von M1–M4, M7 und M8.

6.2.11 Metrik M

Die Metrik M dient letztendlich dazu, die Aussagen der Metriken M1–M10 zu einer einzigen Aussage zusammenzufassen. In Tabelle 6.7 werden hierzu der besseren Übersichtlichkeit wegen die Rangfolgenpositionen der Dienstanbieter in M1–M10 nochmals wiedergegeben. Zur Kombination der Ergebnisse von M1–M10 werden über den vorliegenden Rangfolgenpositionen der Dienstanbieter die arithmetischen Mittel berechnet. Das Ergebnis dieser Berechnung ist in der rechten Spalte von Tabelle 6.7 dargestellt.

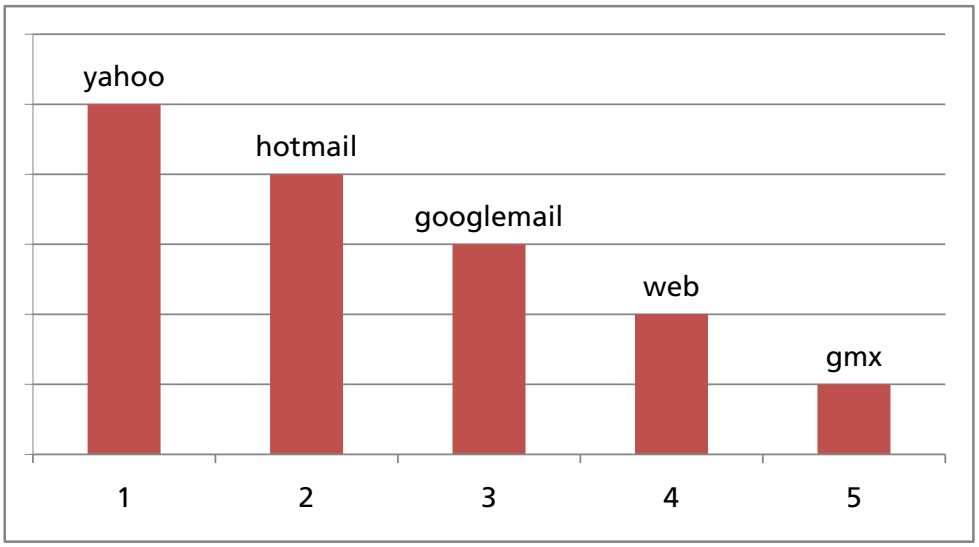
Tabelle 6.7: Gesamtergebnis Metrik M

Dienstanbieter	M1	M2	M3	M4	M5	M6	M7	M8	M9	M10	M
gmx	5	5	5	5	5	5	5	5	5	5	5
googlemail	3	3	3	3	2	2	3	3	1	3	2,6
hotmail	2	2	2	2	2	3	2	2	3	2	2,2
web	4	4	4	4	4	4	4	4	4	4	4
yahoo	1	1	1	1	1	1	1	1	1	1	1

Ausgehend von den Werten in der rechten Spalte von Tabelle 6.7 wird eine Rangfolge der Dienstanbieter erstellt, welche in Abbildung 6.23 gezeigt wird. In diese Rangfolge gehen alle bisher erstellten Rangfolgen für M1–M10 mit gleichem Gewicht ein. Die Rangfolge von M stellt das Gesamtergebnis der vorliegenden Untersuchung dar.

Bei dem Gesamtergebnis ist zu erwähnen, dass Yahoo! bei allen Teilauswertungen (M1–M10) jeweils den ersten Platz belegt hat. Ebenso ist das Ergebnis für WEB.DE (Platz 4 bei M1–M10) und GMX (Platz 5 bei M1–M10) sehr deutlich.

Abbildung 6.23: Rangfolge für M



Hotmail erreicht in 8 von 10 Teilauswertungen Platz 2. Google Mail landet hingegen in 7 von 10 Teilauswertungen auf Platz 3. In 7 Teilauswertungen liegt Hotmail somit besser als Google Mail und lediglich in 2 Teilauswertungen steht Google Mail vor Hotmail.

7 Zusammenfassung der Ergebnisse und Ausblick

Fasst man die Ergebnisse der Studie zusammen, so bleibt festzustellen, dass in dem Beobachtungszeitraum der Umfang von empfangenen Spam-Nachrichten bei keiner der Testpersonen ein Ausmaß erreicht hat, welches die Nutzung des entsprechenden Mail-Kontos für die Testperson unzumutbar machen würde. Dies ist wahrscheinlich hauptsächlich dadurch begründet, dass sich die Mail-Konten der Testpersonen noch in einer frühen Lebensphase befanden und die Email-Adressen somit in noch nicht allzu vielen Adresslisten von Spammern enthalten waren.

Bei genauerer Betrachtung der aus Perspektive eines Kunden noch akzeptablen Messergebnisse haben sich jedoch bereits deutliche Unterschiede gezeigt. Über sämtlichen Testpersonen betrachtet hat sich herausgestellt, dass selbst bei insgesamt niedrigen Durchschnittswerten von Spam-Nachrichten, die ein Kunde dieser Dienstanbieter im Mittel täglich erhält, die Ergebnisse dennoch deutlich streuen. So hat die Gesamtauswertung der Messergebnisse und die Kombination aller vorliegenden Teilauswertungen zu folgender Platzierung der betrachteten kostenfreien Email-Angebote geführt:

1. Yahoo!
2. Hotmail
3. Google Mail
4. WEB.DE
5. GMX

Diese abschließende Reihenfolge ist das Ergebnis der Kombination von 10 verschiedenen Teilauswertungen. Zur fairen und objektiven Auswertung der aufgenommenen Messwerte wurden 10 verschiedene Metriken als Teilauswertungen eingeführt, mit denen unterschiedliche Aspekte erfasst wurden, wie z. B. die Bewertung eines durchschnittlichen Verhaltens oder die Bewertung von punktuellem Verhalten. Darüber hinaus unterschieden sich die Teilauswertungen auch in der technischen Vorgehensweise.

Die Reihenfolge als Gesamtergebnis der Untersuchung gibt jedoch lediglich das beobachtete Spam-Aufkommen in Form von empfangenen Spam-Nachrichten (False Negatives) bei den betrachteten Testpersonen und Dienstanbietern in dem konkreten Untersuchungszeitraum wieder. Andere wichtige Spam-Eigenschaften wie z. B. die Anzahl der False Positives wurden bei der Untersuchung

aus Ressourcengründen nicht betrachtet. Es sei auch ausdrücklich darauf hingewiesen, dass die Übertragung der Ergebnisse dieser Untersuchung für andere Zwecke kritisch sein kann und nicht unbedingt gerechtfertigt ist.

Es seien hier einige Punkte genannt, die auf die Grenzen der Übertragbarkeit der Untersuchungsergebnisse hindeuten. So wurden wegen des beschränkten Ressourcenaufwands das Spam-Aufkommen von sechs Testpersonen je Dienstanbieter untersucht. Die Untersuchung gibt lediglich die Realität dieser sechs Testpersonen je Dienstanbieter wieder. Es besteht kein Anspruch, dass die behandelte Mengengröße die Voraussetzungen für eine repräsentative Abbildung von Kunden der einzelnen Dienstanbieter hat. Als Untersuchungszeitraum wurde der Februar 2010 gewählt. Die Ergebnisse geben lediglich die Realität der betrachteten Testpersonen im Februar 2010 wieder. Es besteht keine Anspruch, die Untersuchungsergebnisse vom Februar 2010 auf andere Zeiträume zu übertragen. Das kann allein schon deshalb nicht gelingen, da die Dienstanbieter immer wieder die technischen Abwehrmaßnahmen gegen Spam verändern und die Spammer immer wieder neue Angriffsvarianten entwickeln. Aus Gründen der Schaffung gleicher Ausgangsbedingungen hatten alle Testpersonen bei allen Dienstanbietern ungefähr gleich alte Email-Konten. Alle bei der Untersuchung verwendeten Email-Konten waren noch relativ neu. Es besteht auch kein Anspruch, die für die betrachteten Email-Konten gewonnenen Ergebnisse auf Email-Konten zu übertragen, die sich in einer anderen Lebensphase befinden.

Dies macht deutlich, dass eine Extrapolation der gemessenen Ergebnisse wahrscheinlich keinen guten Schätzwert für zukünftige Messwerte liefert. Der wahrscheinlich wichtigste Grund hierfür besteht in der jungen Lebensphase der betrachteten Email-Konten. Es besteht die Möglichkeit, dass die ermittelte Rangfolge der Dienstanbieter von den Lebensphasen der Email-Konten abhängig ist. Hierfür sind mehrere Gründe anzuführen. Zunächst lässt sich aus den gemessenen Werten grundsätzlich keine Aussage über zukünftiges Spam-Aufkommen ableiten. Darüber hinaus ist davon auszugehen, dass in verschiedenen Lebensphasen eines Email-Kontos verschiedene Einflüsse für die Anzahl von empfangenen Spam-Nachrichten von entscheidender Bedeutung sind. Es wurde festgestellt, dass in einer frühen Lebensphase eines Email-Kontos die von dem Dienstanbieter selbst verschickten Spam-Nachrichten (sofern solche überhaupt verschickt werden) einen wesentlichen Beitrag zur Gesamtanzahl der empfangenen Spam-Nachrichten liefern. Grundsätzlich ist jedoch davon auszugehen, dass die Anzahl der von einem Dienstanbieter selbst verschickten Spam-Nachrichten über der Zeit nicht signifikant zunehmen wird, da ein Dienstanbieter seine Kunden nicht übermäßig durch solche Nachrichten stören möchte. Bei dem Anteil der selbst verschickten Nachrichten wird man im Zeitmittel von einer konstanten Anzahl ausgehen können. Mit der Verbreitung von Email-Adressen in die von den Spammern berücksichtigten Adresslisten ist jedoch davon auszugehen, dass die Anzahl der von extern an diese Email-Konten versendeten Spam-Nachrichten zu späteren Lebensphasen der Email-Konten beträchtlich zunehmen wird. Es kann also angenommen werden, dass sich in einer späteren

Lebensphase eines Email-Kontos der Einfluss der Spam-Quelle selbst auf das Gesamtergebnis verschieben wird, d. h. der Anteil der von extern empfangenen Nachrichten weiter anwachsen wird und dann u. U. den größeren Beitrag zur Gesamtanzahl der empfangenen Spam-Nachrichten ausmachen wird. Zu Gunsten welches Dienstanbieters sich die Werte jedoch verschieben werden, kann aus heutiger Sicht nicht beantwortet werden.

Grundsätzlich ist die Frage sehr interessant, welchen Einfluss die Lebensphase der Email-Konten bei den verschiedenen Anbietern auf die Anzahl von empfangenen Spam-Nachrichten hat. Deshalb ist beabsichtigt, die Spam-Eigenschaften der betrachteten Dienstanbieter zu späteren Zeitpunkten nochmals anhand der vorhandenen Testpersonen zu untersuchen. Dann kann außerdem analysiert werden, wie sich die Lebensdauer eines Email-Kontos bei einem kostenfreien Email-Dienst auf die betrachteten Spam-Eigenschaften auswirkt.

Literaturverzeichnis

[1] BITKOM. 95 Prozent aller Mails sind Spam. http://www.bitkom.org/62462_62435.aspx, Feb. 2010.

[2] C. Dhinakaran, J. Lee, and D. Nagamalai. An Empirical Study of Spam and Spam Vulnerable email Accounts. In *Future Generation Communication and Networking (FGCN 2007), Proceedings*, 2007.

[3] T. Eggendorfer. 1 Billion Kombinationen. Linux Magazin, Nr. 6, 2009.

[4] L. Frieder and J. Zittrain. Spam Works: Evidence from Stock Touts and Corresponding Market Activity. Technical Report, Berkman Center for Internet & Society, Harvard University, http://cyber.law.harvard.edu/publications/2007/Spam_Works, 2007.

[5] J. Goodman, G. Cormack, and D. Heckerman. Spam and the ongoing battle for the inbox. *Communications of the ACM*, 50(2), Feb. 2007.

[6] heise online. 711-Millionen-Dollar Strafe für Facebook-Spam. http://www.heise.de/newsticker/meldung/711-Millionen-Dollar-Strafe-fuer-Facebook-Spam-846097.html, Oct. 2009.

[7] heise online. Massen-Spammer erneut verurteilt. http://www.heise.de/newsticker/meldung/Massen-Spammer-erneut-verurteilt-891960.html, Dec. 2009.

[8] heise online. Datenschützer fordert strengere Anti-Spam-Gesetze. http://www.heise.de/newsticker/meldung/Datenschuetzer-fordert-strengere-Anti-Spam-Gesetze-894440.html, Jan. 2010.

[9] P. Heymann, G. Koutrika, and H. Garcia-Molina. Fighting Spam on Social Websites: A Survey of Potential Approaches and Future Challenges. *IEEE Internet Computing*, 11(6):36–45, 2007.

[10] B. Hoanca. How Good Are Our Weapons in the Spam Wars? *IEEE Technology and Society Magazine*, 25(1), 2006.

[11] iX. Spam-Bekämpfung als Wettbewerbsvorteil. http://www.heise.de/ix/meldung/Spam-Bekaempfung-als-Wettbewerbsvorteil-910348.html, 2010.

[12] C. Kanich, C. Kreibich, K. Levchenko, B. Enright, G. Voelker, V. Paxson, and S. Savage. Spamalytics: An Empirical Analysis of Spam Marketing Conversion. *Communications of the ACM*, 52(9), Sept. 2009.

[13] B. Leiba. Unwanted Traffic: Finding and Defending against Denial of Service, Spam, and Other Internet Flotsam. *IEEE Internet Computing*, 13(6):10–13, November/December 2009.

[14] A. O´Donnell. The evolutionary microcosm of stock spam. *IEEE Security & Privacy*, 5(1), January/February 2007.

[15] Project Honey Pot. 1 Billion Spammers Served. http://www.projecthoneypot.org/1_billionth_spam_message_stats.php, Dec. 2009.

[16] U. Ries. Spam-Jäger knipsen riesiges Zombie-Netzwerk aus. Spiegel Online, http://www.spiegel.de/netzwelt/web/0,1518,680457,00.html, Feb. 2010.

[17] Steve Linford. Increasing Spam Threat from Proxy Hijackers. http://www.spamhaus.org/news.lasso?article=156, Feb. 2005.

[18] B. Whitworth and E. Whitworth. Spam and the Social-Technical Gap. *IEEE Computer*, 37(10):38–45, 2004.