Aktuelle SPAM-Entwicklung am Behördennetz-Übergang

Dipl.-Ing. (FH) Wolfgang Rosenwirth

Für unerwünschte Werbemails hat sich das Kunstwort SPAM[1] eingebürgert. Es fand den Weg über einen Fernsehsketch der britischen Komiker-Truppe Monty Python über den EDV-Slang in den allgemeinen Sprachgebrauch. Dieser unerwünschte Mailverkehr überwiegt seit etlichen Jahren den erwünschten elektronischen Datenaustausch. Dabei war über lange Zeit ein Zuwachs an SPAM-Aufkommen zu verzeichnen, bis der Anteil an erwünschten Nachrichten fast verschwindend gering wurde. Technische Filtermaßnahmen in großen Firmen und Behörden sind daher zwingend erforderlich, um E-Mail als nutzbringenden Kommunikationsweg weiterhin verwenden zu können. Entsprechende Maßnahmen werden auch für die Bayerischen Behörden getroffen. Dieser Beitrag informiert über die aktuelle Situation und Wirksamkeit der Maßnahmen. Neben diesen technischen Lösungen werden weltweit von Behörden und Softwarehäusern gemeinsam weitergehende Maßnahmen ergriffen, um der SPAM-Flut an der Quelle Einhalt zu gebieten. Besonders hier konnten in der jüngsten Vergangenheit Erfolge verzeichnet werden.

Probleme durch SPAM und Abhilfemöglichkeiten

Durch SPAM entsteht weltweit ein beträchtlicher wirtschaftlicher Schaden. Allein die Zeit zum Löschen von unerwünschten Werbemails summiert sich schnell auf mehrere 100 000 Euro für einen Betrieb. Neben der Arbeitszeit kann durch SPAM die Netzinfrastruktur einer Firma oder eines Internet-Providers bedroht werden.

Durch den generell sehr hohen Anteil an SPAM-Mails – am Übergang zum Behördennetz pendelt der SPAM-Anteil seit Juni 2009 zwischen 97 % und 99 % bei konstant etwa 5 Millionen erwünschter E-Mails – ist die Nutzung von E-Mail ohne geeignete Schutzmaßnahmen mindestens stark beeinträchtigt. Für diese Flut an Mailnachrichten sind höhere (und damit teuerere) Bandbreiten sowie leistungsfähigere Hardware notwendig. Auch dies führt zu wirtschaftlichen Schäden durch SPAM.

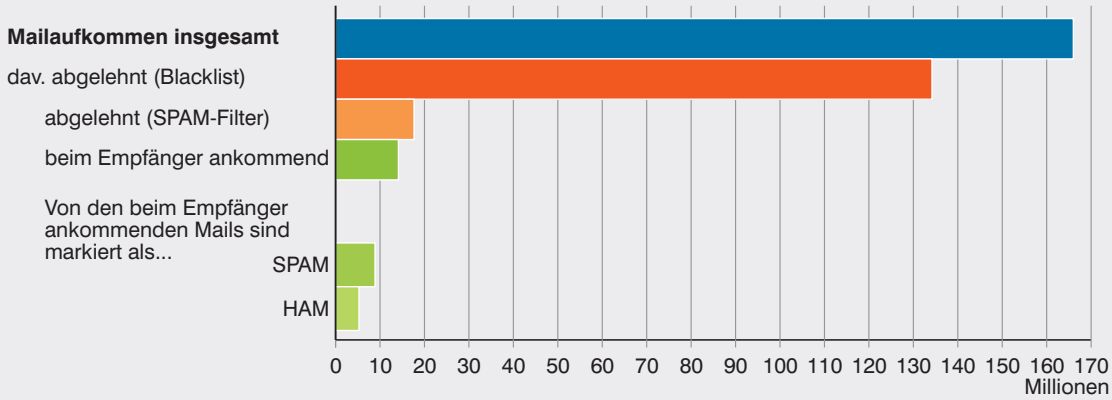
Verschiedene technische Abwehrmaßnahmen für SPAM stehen grundsätzlich bereit. Diese beginnen mit Blacklists, also Sperr-Listen für bestimmte IP-Adressen. Diese nur schwer manipulierbaren Absenderangaben können so bereits einen beträchtlichen Anteil an Werbemails abwehren, denn die sichtbaren Absenderangaben (z.B. Max.Mustermann@provider.de) können leicht gefälscht werden. Mailheader und Mailtext können nach bestimmten Schlüsselwörtern (z.B. Viagra), möglicherweise verdächtige Techniken (z.B. Javascript) und weitere Auffälligkeiten untersucht werden. Diese einzeln betrachtet mehr oder weniger zuverlässigen Untersuchungsergebnisse führen in Summe zu einer bestimmten SPAM-Wahrscheinlichkeit für jede Nachricht. Ab einer festgelegten Höhe der SPAM-Wahrscheinlichkeit werden solche Nachrichten markiert an den Empfänger ausgeliefert oder vollständig abgewiesen. Ein Bündel von Analysemethoden wird am Behördennetz-Übergang angewendet, also am zentralen E-Mail-Eingang für alle bayerischen Behörden.

Weltweite Entwicklung

Wie in der Fachpresse berichtet wurde, konnten im Frühjahr 2011 international im Kampf gegen die Flut von sogenannten SPAM-Mails einige Erfolge erzielt werden. So konnte durch Softwarefirmen und Behörden in den USA mit juristischen Mitteln das Abschalten bekannter „SPAM-Schleudern“ erzwungen wer-

1 SPAM ist eine Markenbezeichnung für „spiced ham“, eine Art Frühstücksfleisch. Im Sketch wird durch das Anpreisen von SPAM-Produkten jede Kommunikation in einem Pub unmöglich. In Anlehnung an diesen Begriff hat sich später HAM als Bezeichnung für nutzbringende E-Mails in den Sprachgebrauch eingebürgert.

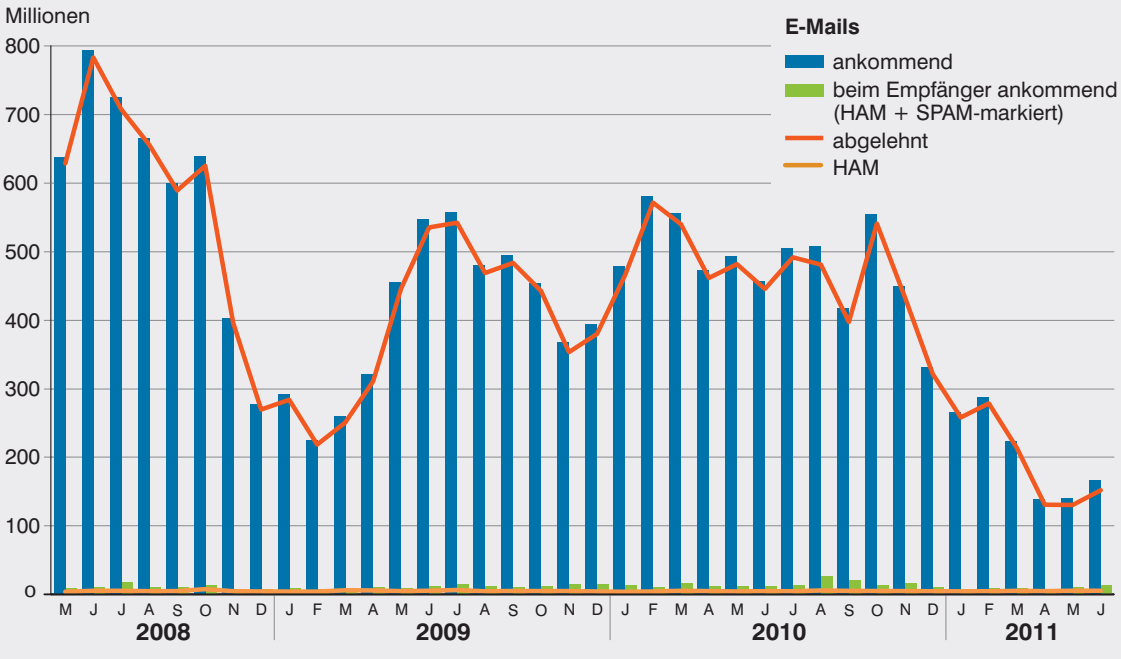
Monatsübersicht zum Mail-/SPAM-Aufkommen am bayerischen Behördennetzübergang für Juni 2011 Abb. 1
Stand: 30. Juni 2011



den (siehe http://www.heise.de/security/meldung/Rustock-Botnetz-ausser-Gefecht-1210310.html und http://www.heise.de/security/meldung/Freundliche-Uebernahme-FBI-steuert-Bot-PCs-1227965.html).

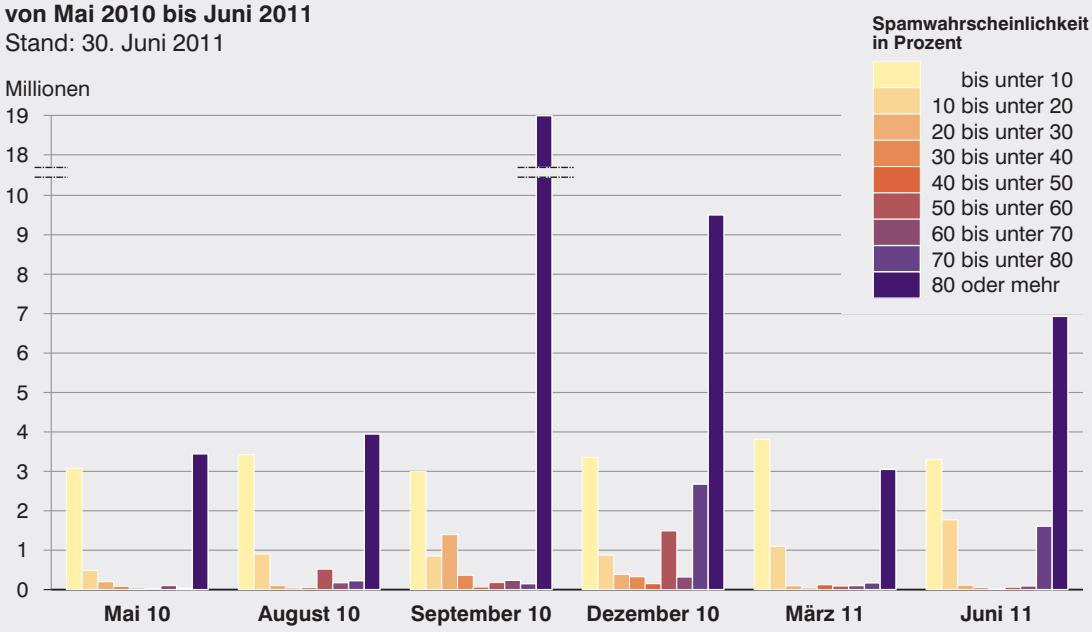
Als Ergebnis dieser und ähnlicher Maßnahmen sank das SPAM-Aufkommen ab und blieb bis in den Frühsommer 2011 auf einem erfreulich niedrigen Niveau. Allerdings ist zu berücksichtigen, dass bereits von einem „niedrigen Niveau“ gesprochen wird, wenn der Anteil der SPAM-Mails unter 99 % des gesamten Mailaufkommens liegt. Diese weltweite Entwicklung war auch am Übergang des Behörden-Netzes festzustellen.

Mail-/SPAM-Aufkommen am bayerischen Behördennetzübergang von Januar 2007 bis Juni 2011 Abb. 2
Stand: 30. Juni 2011



Aufteilung der E-Mails in SPAM-Wahrscheinlichkeitsklassen von Mai 2010 bis Juni 2011
Stand: 30. Juni 2011

Abb. 3



Das verhältnismäßig niedrige SPAM-Aufkommen am Behördennetz-Übergang bleibt weitgehend konstant

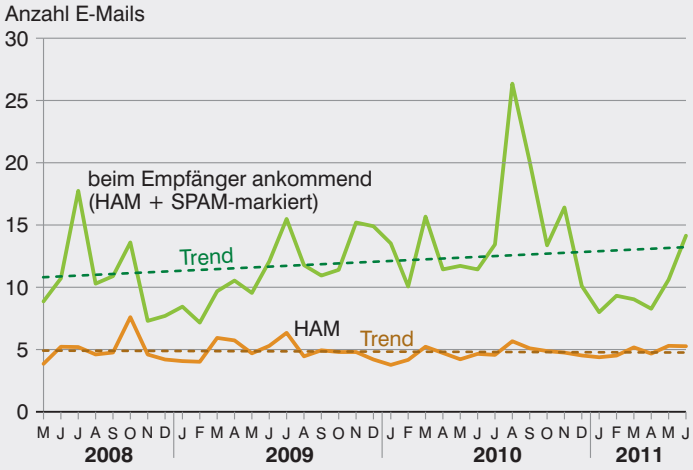
Im Juni 2011 wurden am zentralen Behördennetzübergang 166,0 Millionen eingehende Nachrichten gezählt. Davon wurden 151,8 Millionen Nachrichten abgewiesen und 8,9 Millionen als SPAM markiert. Somit waren vom gesamten Nachrichtenaufkommen 3,2 % sicher erwünschte Nachrichten und etwas weniger als 97 % SPAM-Mails bzw. wahrscheinlich unerwünschte Nachrichten, die als SPAM markiert zugestellt wurden.

Der seit Dezember 2010 feststellbare Trend eines massiv gesunkenen SPAM-Aufkommens hat sich im Berichtszeitraum leicht umgekehrt. Wurde im März 2011 noch ein SPAM-Aufkommen unter 98 % beobachtet, so ist dies zwar auf knapp unter 97 % weiter gesunken. Allerdings ist nach einem Tiefpunkt im April 2011 wieder ein leichter Anstieg auf den aktuellen Wert zu beobachten, der jedoch noch nicht die Märzwerte erreicht hat. Damit ist die aktuelle Belastungssituation sogar noch etwas geringer als im Februar 2009, dem bisher tiefsten Wert seit Inbetriebnahme der aktuellen SPAM-Abwehrmaßnahme.

Die Anzahl erwünschter (HAM-)Mails pendelt um ca. 5 Millionen Der Anteil der als SPAM markiert zugestellten E-Mails ist seit dem letzten Bericht wieder angestiegen. Waren im März 2011 57,3 % der zugestellten E-Mails nicht als SPAM markiert, ist diese Quote im Juni auf 37,2 % gesunken.

Zeitlicher Verlauf der beim Empfänger ankommenden E-Mails von Mai 2008 bis Juni 2011
Stand: 30. Juni 2011

Abb. 4



Dies zeigt sich bei der detaillierten Betrachtung der SPAM-Wahrscheinlichkeit in 10%-Schritten. Diese Zahl (Spamscore) ist ein Maß für die Wahrscheinlichkeit, dass es sich um ein SPAM-Mail handelt. Dabei werden grundsätzlich alle E-Mails mit einer Wahrscheinlichkeit über 50% markiert und mit einer Wahrscheinlichkeit über 90% gelöscht. Wie in der Abb. 3 erkennbar ist, blieb der Anteil der Mails mit einer SPAM-Wahrscheinlichkeit unter 50% näherungsweise konstant. Besonders die Anzahl der Mails mit einer SPAM-Wahrscheinlichkeit über 70% ist seit Beginn der aktuellen SPAM-Abwehrstrategie bis zum September 2010 stark angestiegen. Im Dezember 2010 ist wieder eine Beruhigung eingetreten, die im 1. Quartal 2011 anhielt, sich bis Juni 2011 jedoch wieder erhöht hat.

Auch wenn der aktuelle SPAM-Anstieg sehr moderat ist, zeigt sich, dass eine SPAM-Abnahme meist nur kurzfristig ist und sich rasch Änderungen ergeben können. Darüber hinaus belegt allein die Tatsache, dass nur 3,2% der E-Mails erwünscht sind, wie wichtig geeignete Abwehrmaßnahmen sind.