Aktuelle Spam- und Viren-Entwicklung am Behördennetzübergang

Dipl.-Ing (FH) Wolfgang Rosenwirth

Für unerwünschte Werbemails hat sich das Kunstwort Spam[1] eingebürgert. Es fand den Weg über einen Fernsehsketch der britischen Komikertruppe Monty Python in den EDV-Jargon und von da 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 Unternehmen und Behörden sind daher zwingend erforderlich, um E-Mails 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. Darüber hinaus werden neben den technischen Gegebenheiten neue Trends auf dem „Markt" unerwünschter E-Mails vorgestellt. So musste im ersten Halbjahr 2012 ein deutlicher Anstieg von E-Mails mit gefährlichen Anhängen („Viren-Mails") festgestellt werden.

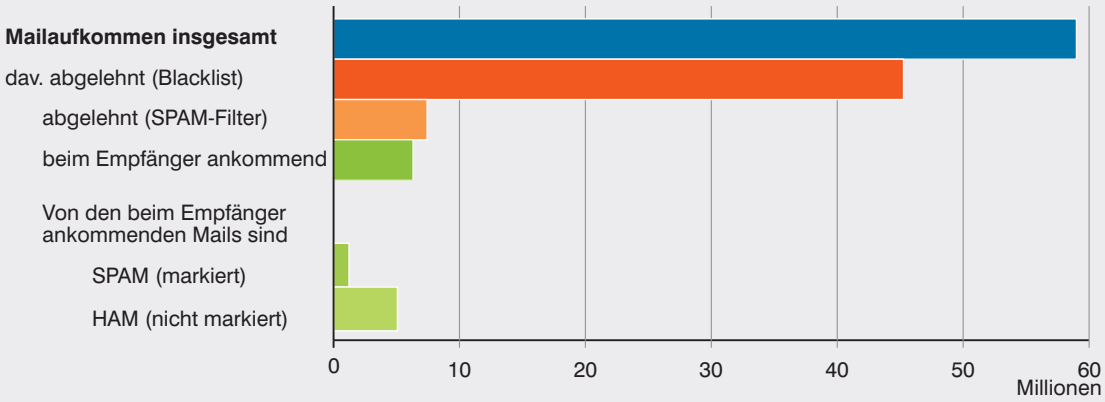
Das verhältnismäßig niedrige Spam-Aufkommen am Behördennetzübergang ist im ersten Halbjahr 2012 weiter gesunken

Im Mai 2012 wurden am zentralen Behördennetzübergang 59,0 Millionen eingehende Nachrichten gezählt. Davon wurden 52,7 Millionen Nachrichten abgewiesen und 1,2 Millionen als Spam markiert. Somit waren vom gesamten Nachrichtenaufkommen 8,6% sicher erwünschte Nachrichten und 91,4% Spam-Mails bzw. wahrscheinlich unerwünschte Nachrichten, die als Spam markiert zugestellt wurden, siehe Abb. 1.

Der seit Dezember 2010 feststellbare Trend eines deutlich gesunkenen Spam-Aufkommens hat sich im ersten Halbjahr 2012 nochmals verstärkt, wie Abb. 2 zeigt.

Seit dem bisherigen Maximalwert von 783 Millionen eingehender E-Mails im Juni 2008 ist dieser Wert auf etwa 50 Millionen E-Mails gesunken. Seit der Spitzenbelastung pendelte sich der Wert für etwa eineinhalb Jahre auf rund 500 Millionen E-Mails ein, bevor er kontinuierlich auf den aktuellen Wert von rund 50 Millionen eingehender Nachrichten gesunken ist.

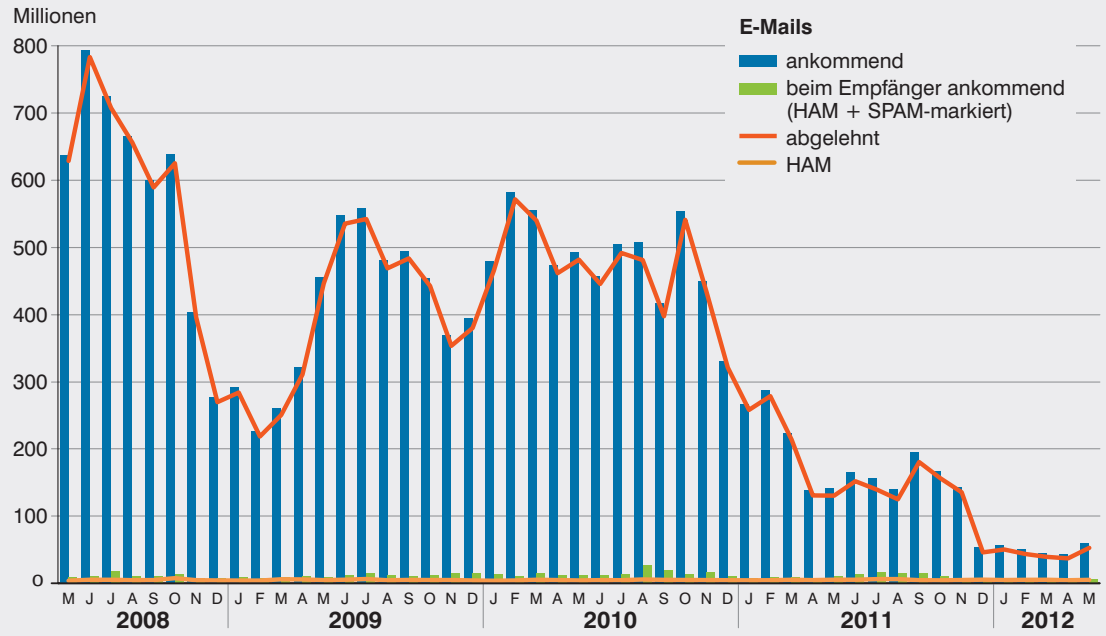
Monatsübersicht zum Mail-/SPAM-Aufkommen am bayerischen Behördennetzübergang für Mai 2012 Abb. 1



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.

Mail-/SPAM-Aufkommen am bayerischen Behördennetzübergang von Mai 2008 bis Mai 2012

Abb. 2



Damit ist die Spam-Quote in vier Jahren von über 99 % auf rund 90 % gesunken.

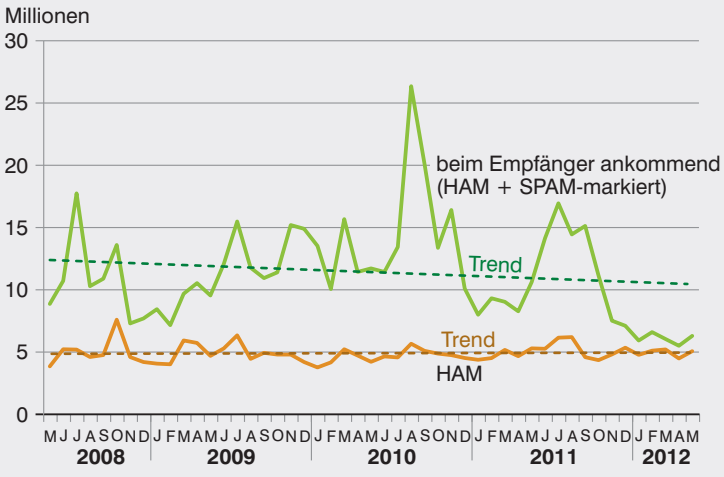
Wurde im März 2011 noch ein Spam-Aufkommen von knapp unter 98 % beobachtet, so ist dieses inzwischen auf fast 90 % gesunken. Allerdings ist nach einem Tiefpunkt im März 2012 mit einem Spam-Aufkommen von 88,5 % wieder ein leichter Anstieg zu beobachten, der jedoch nur ungefähr die Hälfte der Spam-Belastung vom März 2011 erreicht. Damit ist die Belastungssituation seit März 2011 unter der im Februar 2009, dem bisher tiefsten Wert seit Inbetriebnahme der aktuellen Spam-Abwehrmaßnahme am Behördennetzübergang.

Die Zahl der erwünschten Mails („Ham“) pendelt nach wie vor bei fünf Millionen, wie anhand der grünen Trendlinie in Abbildung 3 erkennbar ist. Der Anteil der als Spam markiert zugestellten E-Mails ist erstmals seit Beginn der aktuell angewendeten Spam-Abwehrmaßnahmen im Sommer 2008 über einen längeren Zeitraum gesunken, so dass sich die Trendlinie umgekehrt hat. Waren im Juni 2011 32,7 % der zugestellten E-Mails nicht als Spam markiert, ist diese Quote im März auf auf 86,2 % gestiegen und bewegt sich seither im Bereich von 80 %.

Die positive Entwicklung zeigt sich auch bei der detaillierten Betrachtung der Spam-Wahrscheinlichkeit

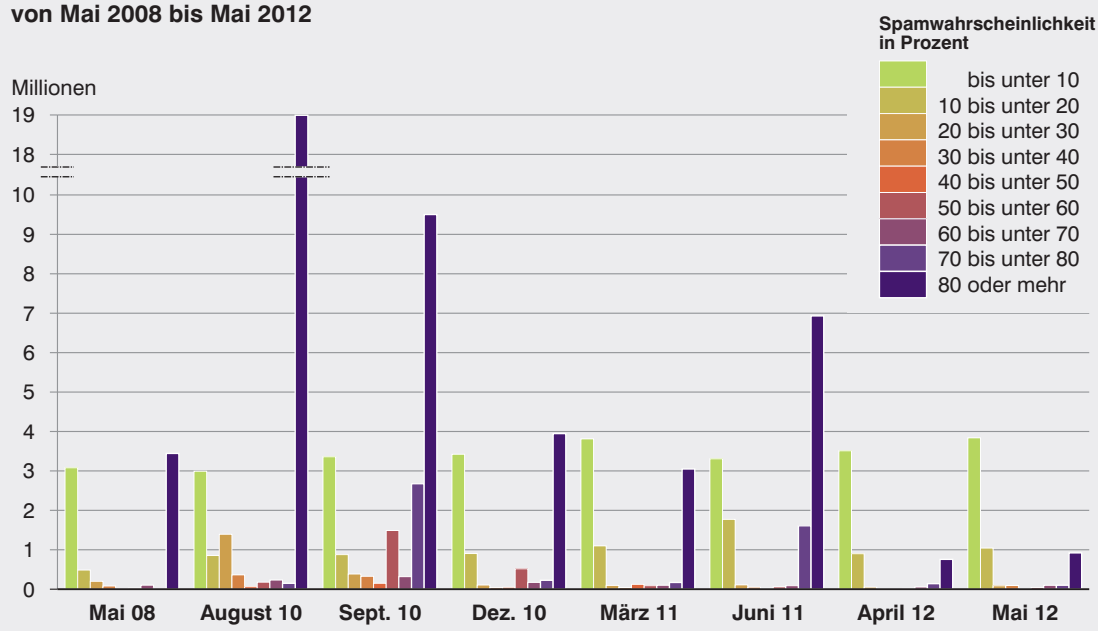
Zeitlicher Verlauf der beim Empfänger ankommenden E-Mails von Mai 2008 bis Mai 2012

Abb. 3



Aufteilung der E-Mails in SPAM-Wahrscheinlichkeitsklassen von Mai 2008 bis Mai 2012

Abb. 4



in zehn-Prozent-Schritten. Diese Zahl (sog. „Spam score“) bezeichnet die Wahrscheinlichkeit, ob eine Spam-Mail vorliegt oder nicht. Dabei werden grundsätzlich alle E-Mails mit einer Wahrscheinlichkeit über 50 % markiert und mit einer Wahrscheinlichkeit über 90 % gelöscht.

Wie Abb. 4 zeigt, blieb der Anteil der Mails mit einer Spam-Wahrscheinlichkeit unter 50 % ungefähr konstant. Die Anzahl der Mails mit einer Spam-Wahrscheinlichkeit über 70 % ist seit Beginn der aktuellen Spam-Abwehrstrategie bis zum September 2010 stark angestiegen. Zum Jahresende 2010 entspannte sich die Lage wieder; nach einem auch noch „ruhigen“ ersten Quartal gab es aber bis Juni 2011 jedoch wieder vermehrt solche Mails. Aktuell hat sich die Anzahl sehr verringert.

Mögliche Ursachen für den starken Rückgang des Spam-Aufkommens

Neben erfolgreichen Maßnahmen der internationalen Strafverfolgungsbehörden in Zusammenarbeit mit der Computerindustrie[2] wird in der Fachpresse als Ursache genannt, dass das Spamming, also das Versenden unerwünschter Massenwerbung via E-Mail, zunehmend auf anderen Wegen erfolgt. Im Fokus der Spammer stehen insbesondere Medien oder Plattformen wie Facebook.[3] Da der Behördennetzübergang hiervon nicht betroffen ist, erklärt dies zu einem guten Teil den massiven Rückgang.

Neuer Trend am Behördennetzübergang: Mails mit gefährlichen Anhängen

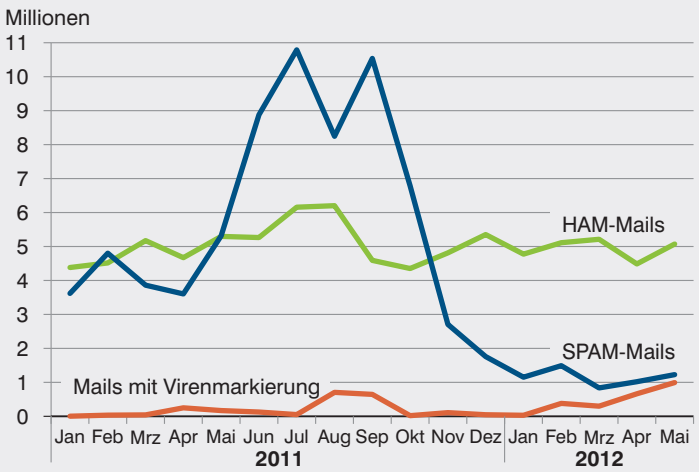
Die Sicherung am Behördennetzübergang erfolgt mehrstufig. Angenommene E-Mails werden zuerst auf potentiell riskante Anhänge überprüft. Diese E-Mails, im Folgenden Viren-Mails genannt, werden nach der Entfernung des gefährlichen Anhangs entsprechend markiert an den Empfänger zugestellt. Handelt es sich um keine Viren-Mail, findet die Spam-Überprüfung statt. Für den Empfänger gibt es somit drei Kategorien von E-Mails, die er erhalten kann: Erwünschte Nachrichten (Ham), unerwünschte Nachrichten (als Spam gekennzeichnet) und Nachrichten mit gefährlichen Anhängen (als Viren-Mail gekennzeichnet).

Die Anzahl der eingehenden Viren-Mails bewegt sich meist zwischen rund 50 000 und 100 000 Mails. Nur in den Monaten August und September 2011 war bereits einmal ein deutlich erhöhtes Aufkommen entsprechender Nachrichten feststellbar. Verglichen mit dem Spam-Aufkommen war dies bis Ende 2011 aber ein praktisch vernachlässigbarer Anteil.

2 Siehe auch: http://www.heise.de/security/meldung/Vier-Jahre-Haft-fuer-Botnetz-Betreiber-1584203.html, http://www.heise.de/security/meldung/Microsoft-fuehrt-Schlag-gegen-Zeus-Botnetze-an-1479665.html und http://www.heise.de/security/meldung/Provider-melden-Angriffe-einheitlich-1487193.html

3 Siehe auch http://www.heise.de/security/meldung/Indien-ueberholt-USA-als-Hauptspammer-1557970.html

Entwicklung der beim Empfänger ankommenden E-Mails seit Anfang 2011 Abb. 5



Wie Abb. 5 zeigt, ist dieser Wert seit Februar 2012 jedoch stark angestiegen und hat nun im Mai eine Größenordnung von fast einer Million erreicht: Fast jede siebte zugestellte E-Mail war eine bereinigte Viren-Mail und entsprechend gekennzeichnet.

Auswirkungen auf die Abwehrmaßnahmen am Behördennetzübergang

Auch wenn der aktuelle Spam-Anstieg moderat ist und seit einigen Monaten ein insgesamt verhältnismäßig niedriges Spam-Niveau festgestellt wurde, verdeutlicht allein die Tatsache, dass immer noch 90 % der am Behördennetzübergang ankommenden E-Mails Spam sind, dass eine Änderung der Abwehrstrategie nicht angebracht ist.

Da die Überprüfung der Anhänge auf mögliche Risiken enorme Ressourcen bindet, werden durch den festgestellten Anstieg der Viren-Mails die freiwerdenden Ressourcen zur Spam-Erkennung kompensiert. Ein Nachlassen der Abwehrbereitschaft ist daher nicht angebracht.