Aktuelles zur Entwicklung von SPAM- und Viren-Mails am Behördennetzübergang

Wolfgang Rosenwirth

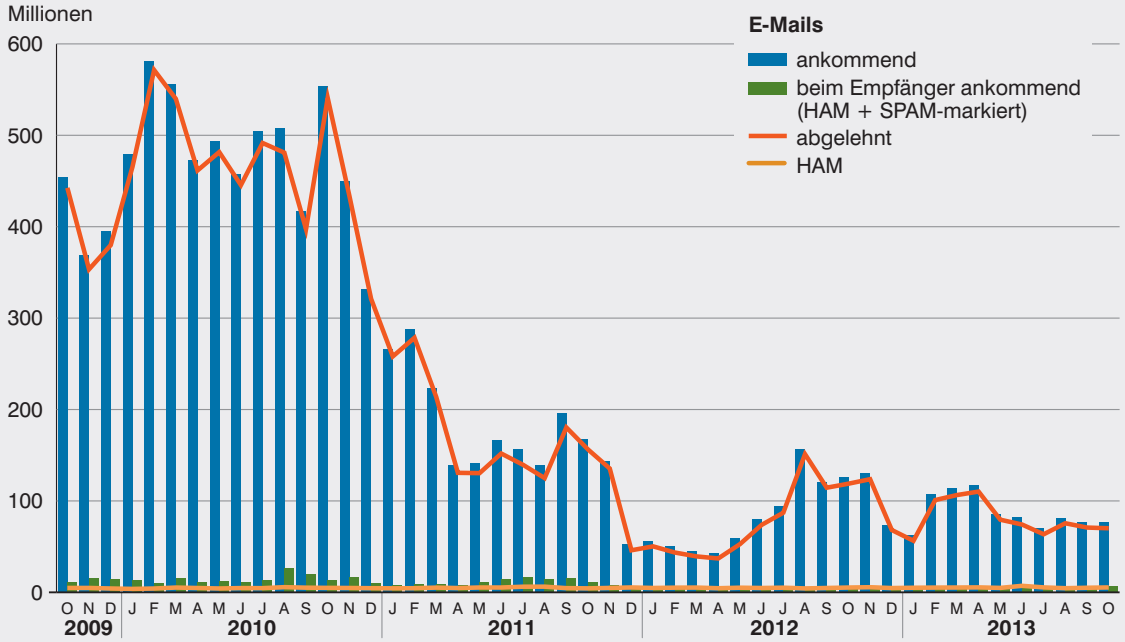
Weltweit liegt die Zahl der unerwünscht zugesandten Werbe-Nachrichten, sogenannte SPAM-Mails, seit Jahren weit über der Zahl der tatsächlich erwünschten, nutzbringenden elektronischen Nachrichten. Nur durch ausgeklügelte technische Gegenmaßnahmen gelingt es, dieser Flut an SPAMs „Herr“ zu werden. Der jahrelange Anstieg der SPAM-Nachrichten ist seit einiger Zeit gebrochen, eine Stabilisierung auf sehr hohem Niveau ist eingetreten.
Das Phänomen der seit 2012 immer wieder stark ansteigende Zahl von Mails mit Schadsoftware im Anhang („Viren-Mails“) kann auch 2013 festgestellt werden. Phasen mit relativer Ruhe wechseln sich mit Wellen vermehrten Auftretens von Viren-Mails ab.

Trotz leicht steigender Tendenz anhaltend „geringes“ SPAM-Aufkommen

Der Anteil des SPAM-Aufkommens liegt im Oktober 2012 bei 93,0 % und somit deutlich über dem Jahrestief des März 2012, wo „nur“ 88,5 % der eingehenden E-Mails als SPAM zu werten waren. Im Jahr 2013 schwankte die Quote zwischen 91,3 % im Juni und 95,4 % im März und April. Damit pendelte die SPAM-Belastung im Berichtszeitraum zwischen rund 57 Millionen und 111 Millionen E-Mails (vgl. Abbildung 1).

Mail-/SPAM-Aufkommen am bayerischen Behördennetzübergang von Oktober 2008 bis Oktober 2013*

Abb. 1



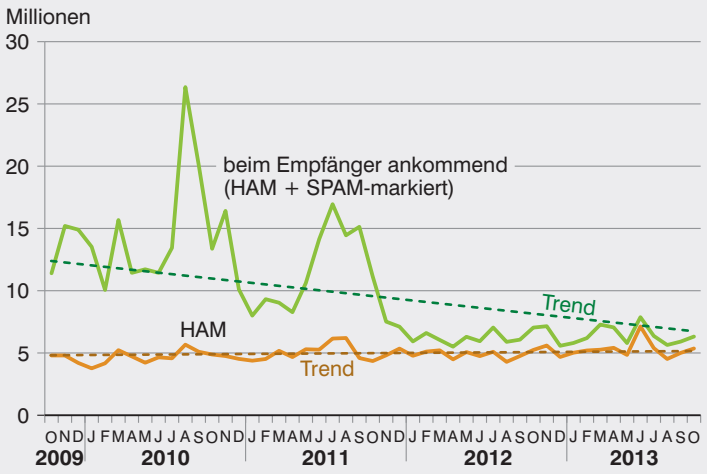
* Aus technischen Gründen ohne virenbelastete E-Mails.

Dies ist im Vergleich mit dem durchschnittlichen SPAM-Aufkommen in den Jahren 2009 und 2010 mit knapp 440 Millionen SPAM-Mails erfreulich gering. Der festgestellte Anstieg an SPAM-Mails seit dem langjährigen Minimum im April 2012 ist seit April 2013 gebremst. Mit einem leichten Abfall der SPAM-Zahlen hat sich in den letzten Monaten die Anzahl der SPAM-Mails auf rund 70 Millionen E-Mails stabilisiert.

Da in der Abbildung 1 aufgrund der großen Zahl an SPAM-Mails keine Tendenzen bei den zum Anwender zugestellten E-Mails erkennbar sind, wird in Abbildung 2 näher darauf eingegangen. Hier zeigt sich, dass sich nicht nur die Gesamtzahl der SPAM-Mails verringert hat, sondern auch die Zahl der möglicherweise unerwünschten E-Mails, die mit einer entsprechenden Markierung zugestellt wurden. Diese lagen im Berichtszeitraum dauerhaft unter der Anzahl der nicht markierten, also sehr wahrscheinlich erwünschten, sog. HAM-Mails. Aufgrund dieser erfreulichen Situation ergab sich sogar eine Trendumkehr. Die Anzahl der nicht markierten, also erwünschten Nachrichten, ist im gesamten Beobachtungszeitraum nahezu unverändert und schwankt um 5 Millionen E-Mails.

Zeitlicher Verlauf der beim Empfänger ankommenden E-Mails von Oktober 2009 bis Oktober 2013

Abb. 2



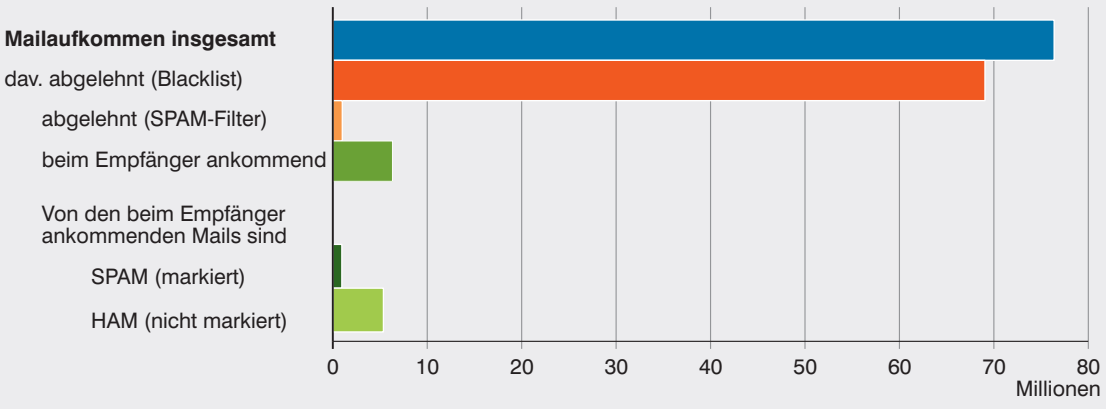
Das aktuelle SPAM-Aufkommen im Oktober 2013

Wie sich anhand der Abbildung 3 erkennen lässt, überwiegt der Anteil der abgewiesenen SPAM-Mails trotz allen erfreulichen Trends immer noch erheblich über den erwünschten Nutz-Mails. So wurden am Behördennetz-Übergang im Oktober insgesamt 76,4 Millionen eingehende Nachrichten gezählt. Von diesen wurden 69,1 Millionen sofort abgewiesen und weitere 1,0 Millionen nach einer eingehenden Inhaltsprüfung abgelehnt.

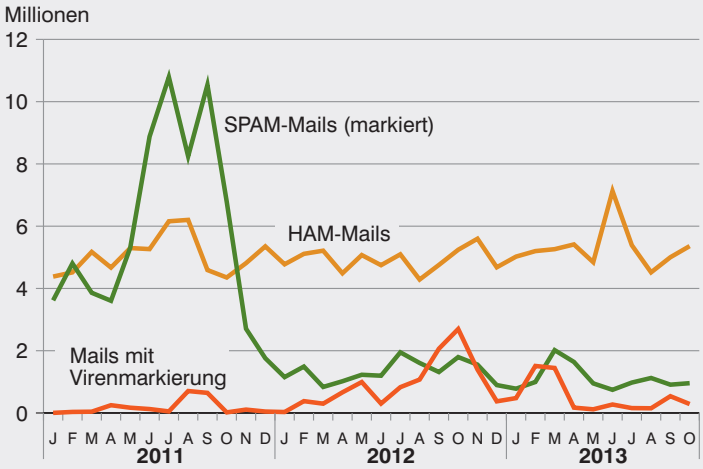
Von den 6,3 Millionen E-Mails, die den Nutzern im Behördennetz zugestellt wurden, waren 5,3 Millionen, dies entspricht 84,8 % aller zugestellten Nachrichten, nicht markiert und daher mit großer Wahrscheinlichkeit erwünschte Mitteilungen. Nur noch 957 Tausend Nachrichten wurden als SPAM markiert zugestellt. Bei diesen Nachrichten besteht eine gewisse Unsicherheit, ob es sich tatsächlich um SPAM handelt.

Monatsübersicht zum Mail-/SPAM-Aufkommen am bayerischen Behördennetzübergang für Oktober 2013

Abb. 3



Entwicklung der beim Empfänger ankommenden E-Mails seit Anfang 2011 Abb. 4



Ein 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), potentiell unerwünschte Nachrichten (als SPAM gekennzeichnet) und Nachrichten mit gefährlichen Anhängen (als Viren-Mail gekennzeichnet).

Seit Beginn der Aufzeichnungen schwankte der Eingang an Viren-Mails meist zwischen rund 50 Tausend und 100 Tausend Mails. Nur im Zeitraum von August bis September 2011 war bereits einmal ein deutlich erhöhtes Aufkommen entsprechender Nachrichten feststellbar. Im Vergleich zum SPAM-Aufkommen mit bis zu 780 Millionen Mails (Juni 2008) und einem Aufkommen als wahrscheinlicher SPAM markierter E-Mails in der Größenordnung der HAM-Mails oder darüber war dies bis Ende 2011 ein praktisch vernachlässigbarer Anteil.

Wie in der Abbildung 4 erkennbar ist, ist seit Februar 2012 dieser Wert jedoch stark angestiegen und hat im September erstmals das Aufkommen an SPAM-markierten E-Mails überschritten. Der bisher höchste Wert wurde im Oktober 2012 mit fast 2,7 Millionen Viren-Mails erreicht. Seitdem schwankt der Wert auffällig zwischen 117 Tausend Viren-Mails im Mai 2013 und 1,5 Millionen Viren-Mails im Februar 2013.

Bei den bemerkenswerten Viren-Mail-Wellen im September/Oktober 2012 und im Februar/März 2013 ist auch ein Blick auf die Verteilung unterschiedlicher Virenarten interessant. In der Viren-Welle im Herbst 2012 war vor allem ein einzelner Virus (Mal/BredoZp-B) mit einem Anteil von 74,6% des Gesamt-Aufkommens dominierend. Die breitere Viren-Mail-Welle im Frühjahr 2013 wies ein wesentlich breiteres Spektrum an verteilten Viren auf, der am häufigsten detektierte Virus (Troj/Eloigne-E) erreichte „nur“ eine Verbreitung von 45,7 % und insgesamt fünf Virentypen erreichten eine Verbreitung über 5%.