

## **Reputationsfilter zur Spam-Abwehr und Spam-Reduzierung (Möglichkeit einer Anti-Spam-Lösung)**

Version 1.0 © Holger Steinacker, Internet: <http://www.datahelp.de>  
Nur für Zwecke der Aus- und Fortbildung.

Reputationsfilter gelten heute zu den effektivsten Lösungen gegen Spam. Diese Filtertechnologie enthält einen Mix aus präventiven und reaktiven Schutzmaßnahmen. Der mehrstufige Aufbau ist einer Prozess- und Verarbeitungskette einer E-Mail-Kommunikation gleich zu setzen. Die Funktionsweise umfasst die vorgelagerten Präventivfilter, Inhaltsanalyse und Contentschutz (Anti-Spam-Engine). Die Konsolidierung sollte direkt am Gateway erfolgen. Spam-E-Mails werden somit über 90% erkannt. Je früher unerwünschte Daten ausgefiltert werden, umso weniger werden die nachfolgenden Systeme belastet!

Was ist ein Reputationsfilter?

Das englische Wort „Reputation“ umschreibt Begriffe wie „Vertrauenswürdig“, „Ehrwürdig“ usw. und versucht, bestimmten Absendern eine sog. „Korrektheit“ beim Versand einer E-Mail zu verleihen.

Diese Technologie blockt unerwünschte E-Mails (RFC-konform) bereits **vor** der Annahme ab! Sie bildet die äußerste Schicht einer Anti-Spam-Lösung. Hierfür wird auf einen Datenbestand zurückgegriffen, analysiert und auf eigene Richtlinien (Policies) angewendet. Anhand dieser Daten lassen sich legitime Absender von Spamsendern sehr präzise und wirkungsvoll unterscheiden. Auf diese Weise wird ca. 80% des unerwünschten Nachrichtenverkehrs direkt am Gateway, durch die Reputation, abgewehrt. Dadurch werden Systemressourcen und Bandbreiten eingespart.

*[Experten gehen davon aus, dass sich aufgrund immer raffinierterer Tricks der Spam-Versender Verfahren wie die Reputationsanalyse durchsetzen werden. Den Analysten der Radicati Group zufolge wurden im Jahr 2007 bereits etwa 332 Millionen Mailboxen durch Reputationsdienste geschützt]* Quelle: Computerwoche 03.06.2008.

Wie entsteht der Datenbestand?

Unternehmen die sich auf die Analyse des weltweiten E-Mail-Verkehrs spezialisiert haben stellen diesen zur Verfügung. Die Klassifizierung erfolgt mittels umfangreicher statistischer Daten. Hier fließen z.B. die Seriosität einer IP-Adresse, DNS Einträge, Webseiten (URLs), Herkunftsland, Beschwerdestellen, Anzahl der gleichen E-Mail und weitere 150 Parameter in das System ein.

Wer liefert die Daten?

Teilnehmer am Netzwerk wie z.B. Provider, Universitäten, Unternehmen und (sog. „Operation-Center“ der Herstellerfirmen) usw.

weitere Informationen zum Thema unter:

<http://www.datahelpsolution.de/xnet/mail/emailstart.htm>