

## **Spam-Abwehr und Spam-Reduzierung** (Mindestanforderungen einer Lösung)

Version 1.1 © Holger Steinacker, Internet: <http://www.datahelp.de>  
Nur für Zwecke der Aus- und Fortbildung.

Mit immer ausgefeilteren Methoden und durch die extreme Zunahme von unerwünschter E-Mails (Spam) versuchen Spammer, bestehende Schutzsysteme auszuhebeln und ihre „Botschaften“ an den Empfänger zu bringen.

Spam wirkt auf die Geschäftsprozesse (direkte Kosten) und bindet Mitarbeiter (indirekt Kosten) durch Diebstahl der Arbeitszeit, die benötigt wird, um unerwünschte E-Mails zu bearbeiten und zu löschen. Zudem können System-Ressourcen so beeinträchtigt werden, dass die Mailserver-Kommunikation erheblich beeinträchtigt und im Extremfall sogar lahm gelegt werden kann.

Einige Spam-E-Mails haben zudem erheblichen kriminellen Charakter. Sie können Inhalte aufweisen, die Systeme angreifen bzw. ausspähen!

Mit dem täglichen Aufräumen des Posteinganges bzw. Anwenden von Filterregeln auf dem „letzten System“ (meist Desktop-PC) ist es nicht mehr getan; Spam bedeutet längst eine gravierende ökonomische Belastung für die Unternehmen / KMUs!

Augenmerk soll auf den Abwehr und der Reduzierung von Spam liegen. Gleichzeitig muss eine Lösung gefunden werden, die Security-Prozesse sowie zukünftige leicht einzubindende Möglichkeiten bzw. Varianten zur Spamabwehr / Spamreduzierung beinhaltet.

### **Mindestanforderungen einer Lösung zur SPAM Abwehr, Reduzierung und Filterung**

#### **E-Mail-Sicherheit mit folgenden Kriterien:**

1. E-Mail-Firewall-Komponente
2. Anti-Spam-Komponente
3. Anti-Virus-Komponente
4. Quarantäne

#### **SPAM erfolgreich abwehren:**

Nur eine Kombination aus verschiedenen Möglichkeiten verspricht Erfolg!

Die unten beschriebenen Möglichkeiten müssen an die jeweiligen Bedingungen im Unternehmen angepasst werden. Auf Vor- und Nachteile einer Möglichkeit / Variante wird nicht eingegangen! Hier wird nur eine grobe Übersicht aufgelistet und wie immer keine Gewähr auf Vollständigkeit gegeben!

**Wenn möglich Spam-Abwehr-Massnahmen vor der Annahme bzw. im laufenden SMTP-Prozess einer E-Mail realisieren!**

**Möglichkeiten zur Spamabwehr und Spamreduzierung:**

- Prüfung auf dynamische IP-Adressen
- Namensauflösung der Mail-Server
- Greylisting
- Empfängerprüfung zur eingehenden E-Mail
- Heuristische Inhaltsprüfung
- Reputationsfiltersysteme
- Context Analyse
- DKIM (DomainKeys Identified Mail)
- SPF (Sender Policy Framework)
- Scanning von Attachments
- Spamfallen auf Webseite
- Rate Limiting
- White- und Black-Listen
- Tarpitting (Teergrube)
- ...

**Erweitere Möglichkeiten:**

- Einsatz von einem „E-Mail-Betriebssystem“
- Einsatz von Quarantäne-Lösungen
- Dynamisches Delivery Queue
- Auswertung des E-Mail-Verkehrs
- Auswertung von Logfiles
- ...

weitere Informationen zum Thema unter:

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