



## **Methoden zum Schutz vor unerwünschten E-Mails.**

In letzter Zeit ist das Aufkommen unerwünschter E-Mail Nachrichten, meist unverlangte Werbung für zweifelhafte Produkte, oft weit jenseits des guten Geschmacks, stark angestiegen. Verschiedene Untersuchungen gehen von davon aus, dass diese „SPAM“ genannten Nachrichten mittlerweile zwischen 30% und 50% des Gesamten E-Mail-Verkehrs ausmachen.

Nicht nur die Menge derartiger Nachrichten, sondern auch die Zahl derjenigen, deren Postfächer damit überfüllt werden, steigt immer weiter an, da die Methoden, mit denen die als „Spammer“ bezeichneten Versender versuchen, an gültige Adressen zu kommen, immer perfider aber auch effizienter werden. Es reicht heutzutage, im Mail-Adressbuch eines Rechners vorzukommen, der mit sich mit Viren infiziert, die dieses auslesen, was um so wahrscheinlicher wird, je mehr Computer mit Internetzugang zu Allgemeingut werden, wodurch die Zahl unbedarfter Benutzer und/oder nicht ausreichend geschützter Benutzer steigt.

Um sich vor diesem Ärger zu schützen, gibt es Filterprogramme, die ähnlich einem Antivirenprogramm auf dem Mailserver installiert oder diesem vorgeschaltet werden, um alle einkommenden Nachrichten einer Überprüfung zu unterziehen. Dabei gibt es im Allgemeinen drei Methoden, die einzeln oder kombiniert angewandt werden können, wobei gute Spamfilter immer die Möglichkeit bieten, eine sog. „Whitelist“ zu definieren, die Absenderadressen definiert, die auf jeden Fall oder aber bei bestimmten der folgenden Überprüfungsmethoden zugelassen werden.

## 1. Überprüfung durch „Reverse DNS-Lookup“

---

Ausgehend von dem Umstand, dass Spammer meist mit gefälschten Absenderadressen oder nicht im DNS angemeldeten Rechnern über Einwählverbindungen operieren, wird überprüft, ob der Mailserver, von dem eine Nachricht verschickt wurde, mit dem DNS-Eintrag für den Server, der für die angegebene Absenderadresse zuständig ist, übereinstimmt. Ist dies nicht der Fall, wird die Nachricht als Spam eingestuft.

Hierzu muss der zu schützende Server aber die Nachrichten direkt aus dem Internet empfangen, auf einem Server, der Nachrichten von einem Provider herunterlädt, wäre ein derartiger Schutz nicht möglich, da sämtliche Nachrichten blockiert würden. Außerdem können so nicht mehr Mails empfangen werden, die über sog. „Relays“ versendet werden, was allerdings immer seltener von legitimen Absendern gemacht wird.

Szenario: Spammer nutzt Rechner mit DSL-Flatrate und dynamischer IP-Adresse, um im Namen von [hans.meyer@aol.com](mailto:hans.meyer@aol.com) zu senden. Es wird festgestellt, dass die Mail nicht von einem zuständigen Server für die Domäne „aol.com“ verschickt wurde und die Nachricht wird abgewiesen.

## 2. Überprüfung des Absenders („Blacklist“)

---

Anhand von Listen, die zum Teil von Enthusiasten gepflegt und kostenfrei zur Verfügung gestellt werden, zum Teil auch von kommerziellen Anbietern offeriert und aktualisiert werden, aber auch selbst erstellt werden können, wird festgestellt, ob der Versender dies mit einer Absenderadresse oder von einem Mailserver aus macht, der als Spam-Versender eingestuft wird.

Hierzu muss der eigene Mailserver nicht unbedingt der direkte Empfänger der Nachrichten sein, wenn auch in einem solchen Falle lediglich die Absenderadresse abgeglichen werden könnte, nicht der versendende Server. Allerdings muss hierbei beachtet werden, dass solche Listen naturgemäß den realen Verhältnissen stets hinterherhinken, da sie ja immer nur nachträglich aktualisiert werden. Ferner kann es sein, dass auch legitime Nachrichten blockiert werden, sei es, weil ein Mailserver-Betreiber für die Duldsamkeit seines Providers mit eventuellen Spammer-Kunden in Sippenhaft genommen wird, sei es, weil den

Listenverwaltern ein Irrtum unterläuft. Auch gibt es Listen, die den „Spam“-Begriff sehr weit auslegen und einen Server aufnehmen, weil er die technischen Voraussetzungen bietet, um von Spammern ausgenutzt zu werden, was ja vielleicht nur kurzzeitig der Fall war, weil der Rechner beispielsweise neu installiert wurde und die „Open Relay“-Funktion, die von Spammern genutzt werden kann, erst abgeschaltet werden musste.

Szenario: Der Spammer betreibt den Mailserver spam.com bei einem Provider, der ihn gewähren lässt. Entweder wird der Spammer selbst nach einiger Zeit in die schwarze Liste aufgenommen und sämtliche Nachrichten bei denen die Absenderadresse auf „spam.com“ lautet, werden nicht angenommen. Oder es wird jede Mail, die von diesem Server oder eben auch von jedem bei dem betreffenden Provider betriebenen Server kommt, blockiert.

### **3. Überprüfung einer Nachricht auf bestimmte Merkmale**

Anhand von Listen mit Schlüsselwörtern und darauf beruhenden Algorithmen, die bei guten Filterprogrammen anpassbar sind und gewissermaßen „trainiert“ werden können, wird jede Nachricht darauf überprüft, ob der Inhalt auf Spam schließen lässt. Hierzu wird der Nachricht meist ein numerischer Wert zugeteilt, der sich an der Anzahl der vorgefundenen möglichen Spam-Merkmale orientiert. Bei Überschreiten eines festlegbaren Schwellenwertes wird die Nachricht als Spam eingestuft.

Bei diesen Filtern ist zunächst eine Testphase anzuraten, da deren Erkennungsrate zunächst entweder zu niedrig sein wird oder aber legitime Nachrichten blockiert, weil sie zu grob gerastert sind. Gute Mailfilter bieten die Möglichkeit, einzelne Kategorien zu bestimmen, die blockiert werden sollen.

Szenario: Ein Spammer wirbt für angebliche Medikamentensonderangebote. Der auf dem Mailserver einer Reederei installierte Spamfilter ist darauf eingestellt, derartige Nachrichten als Spam zu klassifizieren, der einer Apotheke nicht, um nicht tatsächliche Angebote von Großhändlern zu verlieren, wobei dies dadurch geschehen könnte, dass generell Medikamentenangebote durchgelassen werden. Empfehlenswert, wenn derartige Angebote nur von bestimmten Großhändlern erwartet werden, wäre auch die Aufnahme von deren Absenderadressen oder -domänen in die „Whitelist“ bei gleichzeitiger allgemeiner Blockierung.

## Fazit

---

Die jeweiligen Vor- und Nachteile der beschriebenen Methoden sowie die Notwendigkeit, die Schutzmaßnahmen genau abzustimmen und anzupassen, machen es unmöglich, wie beim Schutz vor Viren einfach ein Produkt auszuwählen und zu installieren, denn jeder Fall ist anders gelagert. Eine Feinabstimmung der gewählten Produkte über einen Probezeitraum ist unumgänglich.

Die Art der zu implementierenden Lösungen hängt nicht nur vom Schutzbedürfnis, und der Frage ab, welche Nachrichten erwünscht sind und welche auf keinen Fall, sondern auch von der technischen Infrastruktur. Die Frage, welche Methode sich an welchem Ansatzpunkt implementieren lässt, kann die folgende Tabelle aufzeigen, bei der Frage nach der Auswahl und der weiteren Konfiguration sollten auf jeden Fall kompetente EDV-Berater hinzugezogen werden.

**Tabelle: Ansatzpunkte für Spamschutz-Methoden**

	DNS-Lookup	Server- Blacklist	Absender- Blacklist	Inhaltsfilter
ISP	x	x	x	
Mail-Server mit MX-Record	x	x	x	x
Mailserver			x	x
Client- Programm			x	x