



## Unser Spamfilter lässt unerwünschte E-Mails nicht durch, Ihre persönlichen schon. Und so wird's gemacht:

### Erkennung von Viren und Würmern

Die verbreitetsten und bekanntesten Viren und Würmer werden erkannt. E-Mails, die solche Viren oder Würmer enthalten, werden sofort gelöscht. Abwehrmechanismen vor neuen Viren oder Würmern werden dem Anwender im neuen update zur Verfügung gestellt.

### Abweisen / Umbenennen von (gefährlichen) Anhängen

Es kann konfiguriert werden, ob E-Mails, welche bestimmte Anhänge (z.B. .sys, exe,) enthalten, prinzipiell gelöscht werden, oder ob deren Anhänge in eine nicht ablauffähige Erweiterung umbenannt werden (hierzu wird der letzte Buchstabe der Erweiterung mit einem „\_“ ersetzt, z.B. .exe wird zu .ex\_). Die umbenannten Anhänge können beim Abspeichern auf den PC durch den Anwender manuell wieder in ihre Ausgangsform gebracht werden.

### Erkennen von Spam (-E-Mails)

#### 1. durch URL – Filterung

Kommerzielle Spam (-E-Mails) werden praktisch immer versendet, um dem Empfänger „irgend etwas“ zu verkaufen. Der Empfänger soll durch solche E-Mails motiviert werden, eine bestimmte Web-Seite zu besuchen, um dann ein entsprechendes Produkt zu kaufen. Deshalb enthalten Spam (-E-Mails) immer einen Link (URL) auf die Web-Seite, wo das beworbene Produkt gekauft werden soll. Diese URL's werden in der E-Mail erkannt (egal ob HTML oder nur Text) und auf die Domäne reduziert (Beispiel: wird „http://www.superprodukt.de/index/besterartikel/bestellung.html“ gefunden, so wird diese Zeichenkette auf „superprodukt.de“ reduziert). Die so gefundene Zeichenkette wird in der **URL-Whitelist** gesucht. Wird sie dort gefunden, ist die betreffende E-Mail kein Spam. Wird die Zeichenkette in der **URL-Whitelist** nicht gefunden, wird in der **URL-Blacklist** gesucht. Wird sie hier gefunden, handelt es sich bei der betreffenden E-Mail um Spam und wird als solcher behandelt. Weiterhin wird geprüft, ob sich die E-Mail Adresse des Absenders in der Adressen Whitelist befindet. Wird die Absenderadresse in der Adressen Whitelist gefunden, wird die betreffende E-Mail **nicht** als Spam betrachtet, auch wenn diese einen URL-Eintrag besitzt, welcher in der URL-Blacklist vorhanden ist.

#### 2. durch Einsatz der Adressen Blacklist und Adressen Whitelist

In die Adressen Blacklist werden die E-Mail Adressen eingetragen, von denen niemals eine E-Mail an genommen werden soll. E-Mails von E-Mail Adressen, welche in die Adressen Whitelist eingetragen worden sind, werden **immer** angenommen. Adressen Blacklist und Adressen Whitelist haben Vorrang vor URL-Blacklist und URL-Whitelist, die höchste Priorität hat die Adressen Whitelist. Das bedeutet:

- werden E-Mail Adressen in die Adressen Whitelist eingetragen, so werden E-Mails von diesen Absendern immer empfangen; unabhängig davon, ob sie in den Blacklists eingetragen wurden.

- Werden E-Mail Adressen in die Adressen Blacklist eingetragen, so werden E-Mails von diesen Absendern immer abgewiesen; außer, sie wurden in die Adressen Whitelist eingetragen.

- E-Mails, welche URL-Einträge besitzen, die in der URL-Blacklist vorhanden sind, werden als Spam behandelt; ausser, diese URL's befinden sich in der URL-Whitelist oder die betreffende E-Mail Adresse wurde in die Adressen Whitelist eingetragen.

Die Einträge in beide Listen erfolgen manuell.

### 3. durch Erkennung so genannter „Dictionary attempts“

Der Spammer versendet hier E-Mails an eine (sehr grosse) Liste von Empfängern einer Zieldomäne, wobei häufig vorkommende Vor- und Nachnamen verwendet werden (z.B. [hans.maier@domäne.de](mailto:hans.maier@domäne.de)). Dies geschieht in der Hoffnung, zufällig eine richtige E-Mail Adresse zu treffen. Sollte eine E-Mail an mehr als drei lokale Empfänger adressiert sein, wird die Trefferquote analysiert. Existieren 75% der Empfänger nicht, wird die betreffende E-Mail automatisch als Spam markiert.

### 4. durch Verwendung der NCT URL-Blacklist Datenbank (updatefähig!)

Wird diese Funktion konfiguriert, wird die NCT URL-Blacklistdatenbank vom NCT Web-Server automatisch herunter geladen. Zu diesem Zweck wird alle vier Stunden geprüft, ob eine neue Version der NCT URL-Blacklistdatenbank zur Verfügung steht. Durch diesen Vorgang wird die lokale URL-Blacklist um die fehlenden Einträge der NCT URL-Blacklist ergänzt. URL's der NCT URL-Blacklist Datenbank, die sich in der URL White-List des Anwenders befinden, werden nicht in die lokale URL-Blacklist des Anwenders übernommen!

### 5. durch Verwendung der Option „Spamblock Konto“

Wird ein Benutzerkonto mit der Option „Spamblock Konto“ versehen, so werden alle E-Mails, welche an diesen Benutzer gesendet werden als Spam behandelt. Diese Funktion kann wie folgt genutzt werden:

a) Wird eine erhaltene E-Mail vom Benutzer als Spam eingestuft, kann diese an ein Spamblock Konto weitergeleitet werden. Damit wird diese E-Mail in der weiteren Abarbeitung als Spam behandelt, d.h. die sich in dieser E-Mail befindlichen URL's werden automatisch in die lokale URL-Blacklist eingetragen.

### b) Die „honeypot-Methode“

Ein Benutzerkonto mit der Option „Spamblock Konto“ wird verwendet, um sich bei erkannten Spammern „abzumelden“. Da die bei vielen Spammern vorhandene Möglichkeit zur „Abmeldung vom E-Mail Verkehr“ (z.B.: „Wollen Sie weiterhin E-Mails erhalten Ja / Nein“) in der Regel nur dazu missbraucht wird, um festzustellen, ob eine E-Mail Adresse aktiv ist, zieht man nach der „Abmeldung“ von solchen Spammern geradezu Spam an. Diese Tatsache macht sich die „honeypot-Methode“ zu Nutze. Durch „Abmelden“ eines Benutzerkontos mit der Option „Spamblock Konto“ bei einem Spammer versendet dieser gerade Spams an dieses Spamblock Konto. Die so „angezogenen“ E-Mails werden sofort als Spam erkannt und die sich in dieser E-Mail befindlichen URL's automatisch in die URL-Blacklist eingetragen. Damit ist abgesichert, dass alle anderen Benutzer diese Spam garantiert nicht bekommen. (Eine weitere Möglichkeit, Spam auf den „honeypot“ zu lenken ist, die „Spamblock Konto“ E-Mail Adresse ab und zu im Newsnet zu verwenden!)

### 6. durch Festlegung: „Simplified Chinese“ gleich Spam (konfigurierbar)

Es kann konfiguriert werden, ob eine E-Mail, welche aus den Zeichensätzen „Simplified Chinese“, „BIG5“ oder CSBIG5 besteht, prinzipiell als Spam betrachtet werden soll. Oft werden dadurch bis zu 10% der möglichen Spam-E-Mails erkannt und entsprechend behandelt.

## NCT TECHNOLOGY