

Q-106.212 - Versendete eMails werden durch den Spamfilter als Spam-eMail erkannt

Q-106.212 - Versendete eMails werden durch den Spamfilter als Spam-eMail erkannt

aus Tobit KB importiert - vom 21.03.2007 - [Beitrag bei Tobit](#)

Problem

Eine versendete eMail wird beim Empfänger-eMailprovider als Spam-eMail gewertet. Was können die Ursachen dafür sein?

Antwort

Ein Spamfilter untersucht empfangene eMails anhand verschiedener Vorgaben. Prüfen Sie daher, ob einer der hier aufgeführten Punkte auf diesen Sachverhalt zutrifft:

- **Begrenzung der Empfängerzahl einer Nachricht**
Ein Spamfilter prüft mitunter die Zahl der Empfänger und ordnet die eMail je nach Ergebnis entsprechend zu. Befinden sich im Feld »To« und »CC« zu viele Adressen, kann die Nachricht abgewiesen werden.
- **Überprüfung der Absender-Domain mithilfe des Domain Name Systems (DNS)**
Stelle Sie sicher, dass die Absender-Domain auf Ihren David-Server verweist. Ist dies nicht der Fall, wird durch einen Spamfilter verhindert, dass Spammer, die für ihre eMail-Attacks willkürliche Absenderadressen einsetzen, den Empfänger wirklich erreichen. Dies bedeutet, dass an den Absender »info@ihrefirma.de« auch direkt, ohne zusätzlichen eMailprovider eine eMail gesendet werden kann.
- **Überprüfung der Reverse-DNS-Einträge für den David PostMan**
Unter Umständen benötigt der David PostMan eine öffentliche IP-Adresse oder eine öffentliche Domäne, da Anti-Spam-Programme einen Reverse-DNS-Lookup für IP-Adressen der Hosts im Übertragungspfad durchführen könnten. Wenn kein gültiger Eintrag vorhanden ist, wird dann die Herstellung der Verbindung verweigert.

Um diese Probleme zu beheben, tragen Sie im David-Administrator unterhalb von »PostMan -> System -> SMTP Host Name« die öffentliche IP Adresse oder die Domäne des Hosts ein. Zusätzlich ändern Sie folgenden Parameter in der POSTMAN.INI unterhalb von »DAVID\APPS\POSTMAN\CODE« von

```
;EHLOWITHDOMAIN = FALSE  
in  
EHLOWITHDOMAIN = TRUE
```

- **Realtime-Blacklists**
Bei dieser Methode überprüft ein eMail-Host, ob Ihr David PostMan, der versucht eine eMail zuzustellen, bereits als Spam-Versender aufgefallen ist. Entsprechende Informationen werden in schwarzen Listen (Blacklists) von unabhängigen Gruppen angeboten, die üblicherweise als Non-

Profit-Organisationen agieren.

Der am häufigsten genutzte Dienst dieser Art wird von der MAPs-Gruppe bereitgestellt (<http://www.mail-abuse.org>).

In den Listen sind so genannte offene Relays (falsch konfigurierte Relays, die für Missbrauch durch Weiterleitung unerwünschter eMails von Dritten offen stehen) oder bekannte Spammer dokumentiert, die dem Administrator einer Liste gemeldet werden. Der Administrator übernimmt diese Informationen in den DNS-Dateien. Ein Nutzer dieser Dienste startet eine DNS-Abfrage, um herauszufinden, ob der Host, von dem die Nachrichten empfangen werden sollen, in der schwarzen Liste (DNSBL oder DNS Black List) eingetragen ist. Weitere Informationen entnehmen Sie dem [KnowledgeBase Artikel Q-106.167](#).

- **Erkennung von Schlüsselwörtern**

Hier werden typische Sätze anhand einer "Spamfilterliste" aus Spam-eMails gefiltert.

Diese Liste enthält in der Regel häufig verwendete Wörter, Redewendungen oder Ausdrücke, die in den meisten Arten von Spam gefunden werden. Das bekannteste Beispiel hierfür ist, dass eMails häufig von einem Filter abgewiesen werden, die Wörter wie beispielsweise »WALLPAPER« enthalten.

Häufig werden von Spam-Filtern auch die Header-Informationen und die Kommunikation zwischen den eMail-Servern überwacht. Generell gilt allerdings, dass der David PostMan sich bei der Erstellung des eMail-Headers und bei der Kommunikation mit anderen eMail Systemen streng an die im RFC definierten Spezifikationen hält.