

Spam- und Virenmails

Um Sie vor gefährlichen Viren und Würmern zu schützen und von lästigem Spam zu befreien, befindet sich auf unseren Systemen ein Mailscanner im Einsatz. Der Mailscanner durchsucht alle ein- und ausgehenden Emails auf Viren und Spam.

Hier möchten wir Ihnen die Arbeitsweise des Mailscanners näher erläutern und Ihnen erklären, wie Ihr Email-Programm in Zusammenarbeit mit dem Mailscanner eine automatische Sortierung Ihrer Emails vornehmen kann.

Arbeitsweise des Mailscanners

Der Mailscanner untersucht alle ein- und ausgehenden Emails nacheinander auf Viren, Spam und sonstige Eigenschaften. Wird der Scanner fündig, geht er je nach Art des Fundes folgendermaßen vor.

Viren

Befindet sich ein Virus oder auch ein Wurm im Anhang der Email, dann wird die infizierte Datei gelöscht, damit keine Gefahr besteht, dass diese auf Ihren Computer gelangt. Als Kennzeichnung, dass die Email einen Virus enthielt, wird dem ursprünglichen Betreff "{Virus?}" vorangestellt.

Zusätzlich wird noch folgende Zeile in den Header der Email geschrieben:

X-MailScanner: Virus

Außerdem wird im Body der Email darauf hingewiesen, dass ein Virus entfernt wurde. Im Anhang finden Sie zusätzlich eine Textdatei mit weiteren Informationen zum gefundenen Virus und dem Grund der Löschung.

Der übrige Text der Email im Body bleibt übrigens erhalten und wird nicht entfernt. Sollten Sie daraus schließen können, dass die Löschung irrtümlich erfolgte bzw. die Datei vertrauenswürdig ist, dann wenden Sie sich bitte an uns. Eine Kopie der gelöschten Datei wird einige Tage in einem Quarantäne-Verzeichnis auf dem Server aufbewahrt und kann Ihnen bei Bedarf zur Verfügung gestellt werden.

Spam

Für jede Email wird durch den Mailscanner auf Grundlage verschiedener Untersuchungen auf typische Spam-Eigenschaften ein sogenannter SpamScore errechnet. Dieser Wert gibt an wie hoch die Wahrscheinlichkeit ist, dass es sich um eine Spammail handelt. Je höher der Wert, desto größer ist auch die Wahrscheinlichkeit.

Der SpamScore wird zusammen mit einer Auflistung der einzelnen gefundenen Spam-Eigenschaften vom Mailscanner in den Header der Email geschrieben.

Beispiel für eine eindeutige Spammail (Wert: 21,925):

X-MailScanner-SpamCheck: spam, SpamAssassin (Wertung=21.925, benoetigt 6, autolearn=disabled, BODY_ENHANCEMENT2 0.84, DNS_FROM_RFC_ABUSE 0.37, FORGED_YAHOO_RCVD 2.17, INFO_TLD 0.48, JOIN_MILLIONS 0.64, RCVD_IN_BL_SPAMCOP_NET 1.83, RCVD_IN_XBL 2.51, URIBL_AB_SURBL 2.01, URIBL_JP_SURBL 4.00, URIBL_OB_SURBL 2.00, URIBL_SBL 0.63, URIBL_SC_SURBL 3.90, URIBL_WS_SURBL 0.54)

Beispiel für eine Mail, die kein Spam ist (Wert: 0,178):

X-MailScanner-SpamCheck: not spam, SpamAssassin (Wertung=0.178, benoetigt 6, autolearn=disabled, NO_REAL_NAME 0.18)

Zusätzlich wird der SpamScore noch durch folgende Zeile visualisiert:

X-SpamScore: sssssssssssssssssss
(Beispiel für einen Wert von 21)

Folgende Angaben sollen Ihnen einen Anhaltspunkt geben, wie die möglichen Werte einzuordnen sind:

<i>Wert</i>	<i>Aussage</i>
bis 6	wahrscheinlich kein Spam
6-10	wahrscheinlich Spam
über 10	höchstwahrscheinlich Spam

Als Kennzeichnung, dass die Email höchstwahrscheinlich Spam ist, wird dem ursprünglichen Betreff ab einem SpamScore von 10 "{Spam?}" vorangestellt.

Sonstiges

Zusätzlich untersucht der Mailscanner die Emails noch auf einige weitere Eigenschaften.

Werden z.B. automatisch ausgeführte IFrames, Formulare oder Scripte in HTML-Mails gefunden, die meist dem Ziel dienen den erfolgreichen Empfang von Spam zurückzumelden und so die Empfängeradresse zu bestätigen, werden diese aus der Mail entfernt. Als Kennzeichnung, dass dies geschehen ist, wird dem ursprünglichen Betreff "{Disarmed}" vorangestellt.

Sind in einer Email Links vorhanden, die ein anderes Ziel haben als augenscheinlich zu erkennen ist, dann deutet dies auf eine Art von Phishing hin. Über diesen möglichen Täuschungsversuch werden Sie vom Mailscanner an der betroffenen Stelle in der Email hingewiesen.

Automatische Sortierung mit einem Email-Programm

Mittlerweile bieten ziemlich viele Email-Programme Filterregeln zur automatischen Sortierung eingehender Emails an. Je nach Umfang der von Ihrem Programm angebotenen Filter stehen Ihnen verschiedene Möglichkeiten zur Verfügung.

Wie die Einrichtung von Filterregeln funktioniert ist bei jedem Email-Programm verschieden. Weitere Informationen erhalten Sie in der Anleitung oder der Hilfe zu Ihrem Programm.

Suche nach einem Text im Betreff

Die einfachste Möglichkeit Viren- und Spammails auszusortieren besteht darin, die oben beschriebene Kennzeichnung im Betreff suchen zu lassen. Wenn Sie dazu eine Regel in Ihrem Email-Programm erstellen, dass alle Emails mit "{Virus?}" oder "{Spam?}" im Betreff automatisch verschoben werden sollen, dann haben Sie alle Virenmails und alle Emails, bei denen es sich höchstwahrscheinlich um Spam handelt, aussortiert.

Suche nach einem Text im Header

Wenn Sie zudem noch die Möglichkeit haben Regeln einzurichten, die nach einem Text im Header der Email suchen, dann können Sie für Spam ganz individuelle Einstellungen vornehmen.

Wenn Sie z.B. möchten, dass bereits alle Emails mit einem SpamScore ab 6 aussortiert werden, dann lassen Sie einfach nach dem Text "X-SpamScore: sssss" (oben genannte zusätzliche Visualisierung des SpamScore) im Header suchen. Da bei größeren Werten jeweils die entsprechende Anzahl "s" hinten angefügt wird, trifft dieser Beispieltext auf alle Werte ab 6 zu.

Auf diese Weise können Sie eine Filterung nach jedem beliebigen Wert vornehmen. Welcher SpamScore für Ihre Bedürfnisse am besten geeignet ist müssen Sie selbst herausfinden. Oben genannte Werte bilden allerdings einen gut geeigneten Anhaltspunkt.