Anti-Spam und Anti-Virus: PureMessage

Vorwort: Handlungsempfehlung des DFN-Vereins

Die Grundlage für die Struktur der Systeme zur E-Mail-Filterung am Rechenzentrum der TU Clausthal ist die Handlungsempfehlung zur Abwehr von Spam und mit Viren behafteter E-Mails des DFN-Vereins. Sie ist im Web unter dieser Adresse zu finden:

- http://www.dfn.de/rechtimdfn/empfehlungen/handlungsempfehlungen/abwehrspam/

Content-Filtering mit Sophos PureMessage

Seit dem Jahre 2004 werden alle ein- und ausgehenden E-Mails mit der kommerziellen Software *Sophos PureMessage* auf Viren und Spam-Wahrscheinlichkeit überprüft. Sophos PureMessage steht dem Rechenzentrum durch eine Landeslizenz ausgewählter Sophos-Produkte zur Nutzung zur Verfügung.

Produkt-Informationen zu PureMessage findet man unter der folgenden Adresse:

- http://www.sophos.de/products/enterprise/email/security-and-control/

Behandlung von virenbehafteten E-Mails

Eingehende E-Mails, die Viren enthalten, werden von den E-Mail-Filtern des Rechenzentrums in Quarantäne gestellt. Der Empfänger der Viren-E-Mail wird im nächsten Quarantäne-Digest (täglich um 08:00 Uhr) über die in Quarantäne gestellten Viren-E-Mails informiert.

Bei Bedarf können die Viren-E-Mails aus der Quarantäne freigestellt und noch nachträglich in den Posteingang bzw. in den Ordner *Junk-E-Mail* des E-Mail-Kontos zugestellt werden.

Zusätzlich zum Verschieben in die Quarantäne von Sophos PureMessage werden die durch Viren verseuchten E-Mails mit dem folgenden Header-Eintrag versehen:

```
X-Virus-Status: YES, Virus EICAR-AV-Test
```

Des Weiteren erhalten alle E-Mails, die von den E-Mail-Filtern des Rechenzentrum auf Viren und Spam-Wahrscheinlichkeit überprüft wurden, den folgenden Header-Eintrag:

```
X-Virus-Scanned: by Sophos PureMessage 6.0.0.2142326, Antispam-Engine:
2.7.2.2107409, Antispam-Data: 2013.4.15.110017 at tu-clausthal.de
```

Ab dem 06.05.2013 werden mit Viren verseuchte E-Mails nicht mehr von unseren E-Mail-Systemen angenommen und damit auch nicht mehr in Quarantäne gestellt. Die Viren-E-Mails werden mit einer entsprechenden Fehlermeldung an den Absender zurück geschickt.

Behandlung von Spam-E-Mails

Die E-Mail-Filter des Rechenzentrums (Sophos PureMessage) versehen alle als Spam verdächtigten E-Mails mit den Header-Einträgen *X-Spam-Level* und *X-Spam-Flag*. Den Benutzern ist es mit Hilfe dieser Header-Einträge möglich Spam von gewollter Post zu trennen.

Hier ein Beispiel für die Header-Einträge:

```
X-Virus-Scanned: by Sophos PureMessage 6.0.0.2142326, Antispam-Engine:
2.7.2.2107409, Antispam-Data: 2013.4.15.50918 at tu-clausthal.de
X-Spam-Level: ************** (100%, 'DFN_X_SPAM_FLAG_YES+ 4.2, DFN_SCORE_20+
0, KNOWN_SPAM_CONTENT 8, FORGED_RCVD_UNKNOWN_HELO 6.5,
CANPHARM_URI 0.05, HTML_00_01 0.05, HTML_00_10 0.05,
BODYTEXTP_SIZE_3000_LESS 0, BODY_ENDS_IN_URL 0, BODY_SIZE_1000_LESS 0,
BODY_SIZE_100_199 0, BODY_SIZE_2000_LESS 0, BODY_SIZE_5000_LESS 0,
BODY_SIZE_7000_LESS 0, INVALID_MSGID_NO_FQDN 0, SMALL_BODY 0,
USER_AGENT_OE 0, __ANY_URI 0, __CP_URI_IN_BODY 0, __CT 0, __CTE 0,
__CT_TEXT_PLAIN 0, __HAS_FROM 0, __HAS_MSGID 0, __HAS_MSMAIL_PRI 0,
__HAS_X_MAILER 0, __HAS_X_PRIORITY 0, __INT_PROD_ONLINE 0, __MIME_TEXT_ONLY
0, __MIME_VERSION 0, __OUTLOOK_MSGID_1 0, __OUTLOOK_MUA 0,
__OUTLOOK_MUA_1 0, __SANE_MSGID 0, __TEXT_SIG_ANY 0, __TO_MALFORMED_2 0,
__TO_NO_NAME 0, __URI_CANPHARM_8CHAR_DOTCOM 0, __URI_NO_MAILTO 0,
__URI_NO_PATH 0, __URI_NO_WWW 0, __USER_AGENT_MS_GENERIC 0,
__ix.dnsbl.manitu.net_ERROR ')
X-Spam-Flag: YES
```

Eine Anleitung zur Erstellung einer Filterregel auf dem E-Mail-Server des Rechenzentrums, die alle Spam-E-Mails in einen Ordner sortiert (z.B. einen Ordner mit dem Namen SPAM), finden Sie hier.

Eine weitere Methode ist die Spam-E-Mails direkt in die Spam-Quarantäne von Sophos PureMessage verschieben zu lassen, bevor sie in den Posteingang des E-Mail-Kontos zugestellt wird. Den Benutzern ist es dann möglich, die Spam-Mails über das Web-Interface von PureMessage einzusehen und sich einen täglichen Bericht (Digest) über die in Quarantäne gestellten Spam-Mails zuschicken lassen (siehe unten).

Quarantäne-Digests (tägliche Übersichts-Mail)

Alle Benutzer, die Quarantäne-Nachrichten haben, bekommen täglich eine Übersichts-E-Mail (Quarantäne-Digest) zugeschickt, in der alle Quarantäne-E-Mails aufgelistet werden. **Der Digest wird täglich um 08:00 Uhr verschickt** und beinhaltet alle Quarantäne-E-Mails, die seit dem letzten Digest in Quarantäne gestellt wurden.

Die aufgelisteten E-Mails können sich die Benutzer dann über das Web-Interface oder per Reply auf die entsprechende Digest-E-Mail zuschicken lassen.

Es werden zwei verschiedene Quarantäne-Digests verschickt, nämlich:

- in Quarantäne gestellte Viren-E-Mails und
- in Quarantäne gestellte Spam-E-Mails.

Web-Interface

Das Web-Interface von Sophos PureMessage, über das Viren- und Spam-Mails, die in Quarantäne gestellt wurden, eingesehen und verwaltet werden können, ist unter der folgenden Adresse zu erreichen:

https://puremessage.tu-clausthal.de

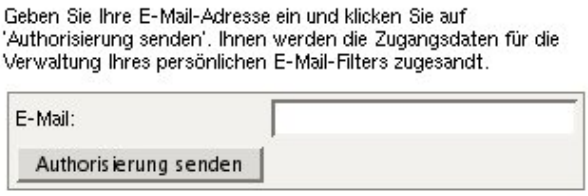
Achtung: Für den Zugriff auf das Web-Interface von Sophos PureMessage muss der Web-Browser Cookies akzeptieren!

Zugang zum Web-Interface der PureMessage Quarantäne

Wenn Sie bereits ein Passwort für Ihre E-Mail-Adresse angefordert haben, geben Sie Ihre E-Mail-Adresse und Ihr Passwort ein, um sich am Web-Interface von Sophos PureMessage anzumelden.

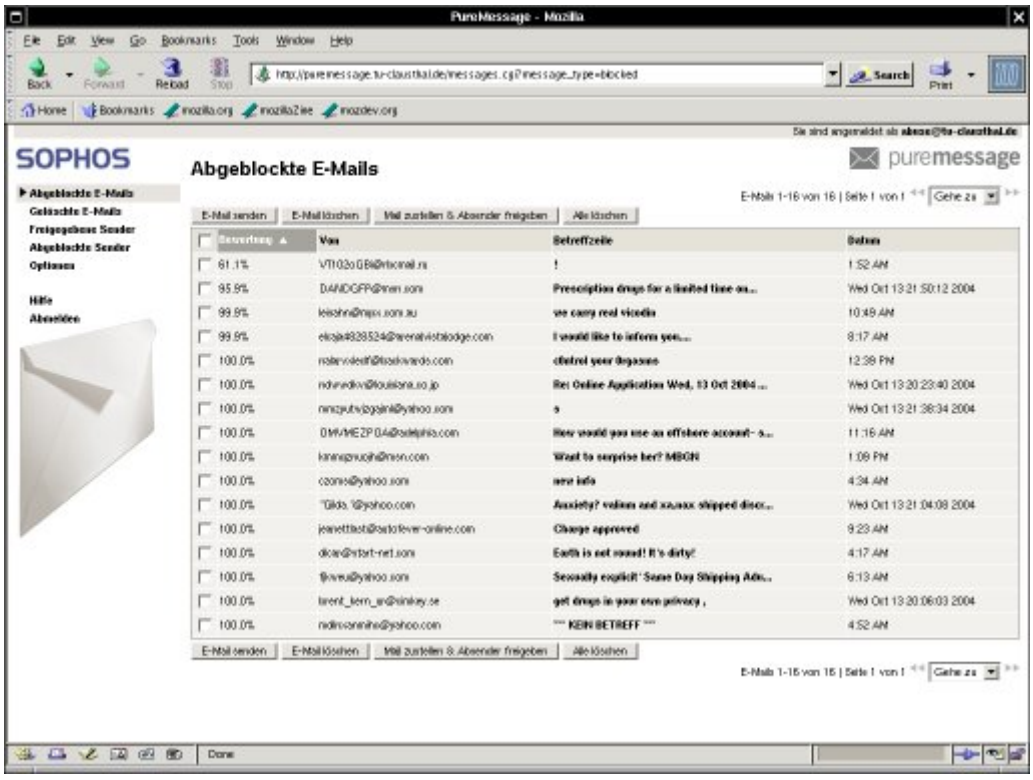
Wenn Sie noch kein Passwort haben, fordern Sie ein neues Passwort an, indem Sie auf hier klicken, Ihre E-Mail-Adressen in das Feld E-Mail eingeben und Sie dann auf Authorisierung senden klicken.

Sie bekommen nach wenigen Minuten eine E-Mail mit Ihren Zugangsdaten für die Sophos PureMessage-Quarantäne zugeschickt.



Bitte beachten Sie, dass die E-Mail-Adressen (z.B. *mmust13@tu-clausthal.de* und *max.mustermann@tu-clausthal.de*), die zu einem E-Mail-Konto gehören, vom PureMessage-System als jeweils eigenständige E-Mail-Adressen betrachtet werden. Wenn Sie sich also ins PureMessage-System einloggen wollen, um auf E-Mails zuzugreifen, die unter der E-Mail-Adresse *max.mustermann@tu-clausthal.de* in Quarantäne gestellt wurden, nutzen Sie bitte auch diese Adresse für das Login (und nicht mmust13@tu-clausthal.de).

So sieht das Web-Interface von Sophos PureMessage aus, über das Sie Zugriff auf Ihre Quarantäne-E-Mails bekommen und über das Sie White- und Blacklisten verwalten können:



Aktivieren der Spam-Quarantäne für die eigene E-Mail-Adresse

Per Default-Einstellung ist die Spam-Quarantäne von Sophos PureMessage für alle bereits bestehenden E-Mail-Adressen erst einmal deaktiviert.

Wird die Spam-Quarantäne vom Benutzer gewünscht, so ist sie vom Benutzer selbst über das Web-Interface zu aktivieren.

Nach dem die Spam-Quarantäne aktiviert worden ist, werden alle E-Mails, die bisher nur mit den Header-Einträgen **X-Spam-Flag: Yes** und **X-Spam-Level** markiert worden sind, nicht mehr an den eigentlichen Empfänger weitergeleitet, sondern in der Quarantäne abgelegt und dort für den betreffenden Benutzer bereit gehalten.

- Die Default-Einstellung ist zunächst einmal, dass keine Spam-E-Mails in Quarantäne gestellt werden und dass Sie deswegen auch keinen täglichen Digest zugeschickt bekommen. (siehe Bild)
- Wenn Sie die zentrale **Spam-Quarantäne für Ihre E-Mail-Adresse aktivieren** wollen, **entfernen** Sie den oberen Haken neben dem Text *Für meine E-Mails alle Abblockfunktionen für Spam und beleidigende Inhalte deaktivieren*.
- Wenn Sie die Spam-Quarantäne für Ihre E-Mail-Adressen aktiviert haben und eine tägliche Übersicht über Ihre Quarantäne-E-Mails (Digest) wünschen, setzen Sie neben dem Text *Ich möchte regelmäßig über abgeblockte E-Mails benachrichtigt werden.* einen Haken.

Bei E-Mail-Konten, die durch das Rechenzentrum neu eingerichtet werden, wird die Spam-Quarantäne automatisch aktiviert.

Navigation im Web-Interface von Sophos PureMessage

- Unter dem Menüpunkt *Abgeblockte E-Mails* finden Sie

alle E-Mails, die als Spam erkannt worden sind.
- Unter *Gelöschte E-Mails* werden alle E-Mails einsortiert, die zuvor unter *Abgeblockte E-Mails* zu finden waren und vom Benutzer gelöscht worden sind.
- Unter dem Menüpunkt *Freigegebene Sender* können benutzerspezifische Whitelisten gepflegt werden. E-Mails von E-Mail-Adressen in dieser Liste werden nicht in Quarantäne gestellt, auch wenn es sich um Spam handelt.
- Über den Menüpunkt *Abgeblockte Sender* ist es möglich, eine sogenannte Blackliste zu definieren. E-Mails, die von E-Mail-Adressen versendet worden sind, die in einer Blackliste stehen, werden in die Quarantäne verschoben, auch wenn es sich bei der betreffenden E-Mail nicht um Spam handelt.
- Unter *Optionen* können Sie die Spam-Quarantäne für Ihre E-Mail-Adresse und/oder den täglichen Digest deaktivieren. Des weiteren können Sie die Sprache, in der das Web-Interface geschrieben ist, auf die von Ihnen gewünschte Sprache umstellen. Mögliche Sprachen sind Deutsch, Englisch, Französisch, Italienisch und Spanisch.
- Unter *Hilfe* bekommen Sie Erklärungen über die Funktionen des Web-Interfaces von PureMessage.
- Mit dem Menüpunkt *Abmelden* melden Sie sich von der PureMessage-Quarantäne wieder ab.

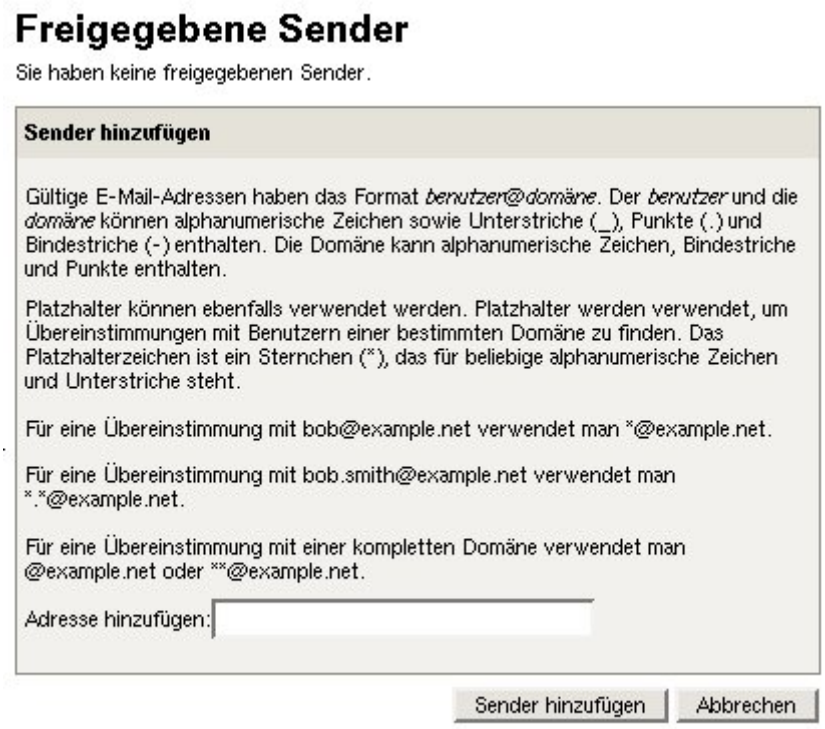
E-Mails aus Quarantäne freischalten oder löschen

- Klicken Sie auf *E-Mail senden*, um eine oder mehrere ausgewählte E-Mails aus der Quarantäne freizuschalten. Die ausgewählten E-Mails werden dann nach wenigen Minuten in Ihrem Posteingang oder im Ordner *Junk-E-Mail* erscheinen.
- Mit dem Button *E-Mail löschen* können Sie eine oder mehrere ausgewählte E-Mails aus der Quarantäne löschen. Die ausgewählten E-Mails werden dann zunächst in den Ordner *Gelöschte E-Mails* verschoben, bevor sie endgültig gelöscht werden.
- Klicken Sie auf *Mail zustellen & Absender freigeben*, um eine oder mehrere ausgewählte E-Mails

aus der Quarantäne freizuschalten und den oder die Absender auf die Whiteliste Ihrer E-Mail-Adresse zu setzen.
- Über den Button *Alle löschen* können Sie alle in der Quarantäne befindlichen E-Mails löschen.

In Quarantäne gestellte Spam-E-Mails bleiben 30 Tage in der Quarantäne und werden danach gelöscht.

Pflege von White- und Blacklisten



Es ist möglich, sowohl einzelne E-Mail-Adressen als auch ganze Domains in eine White- oder Blackliste aufzunehmen.

[mitarbeitende], [studierende]

Direkt-Link:
https://doku.tu-clausthal.de/doku.php?id=e-mail_und_kommunikation:puremessage:start

Letzte Aktualisierung: **11:12 25. January 2021**