ComNet eMail-Spam-Filterung

Benutzerhandbuch

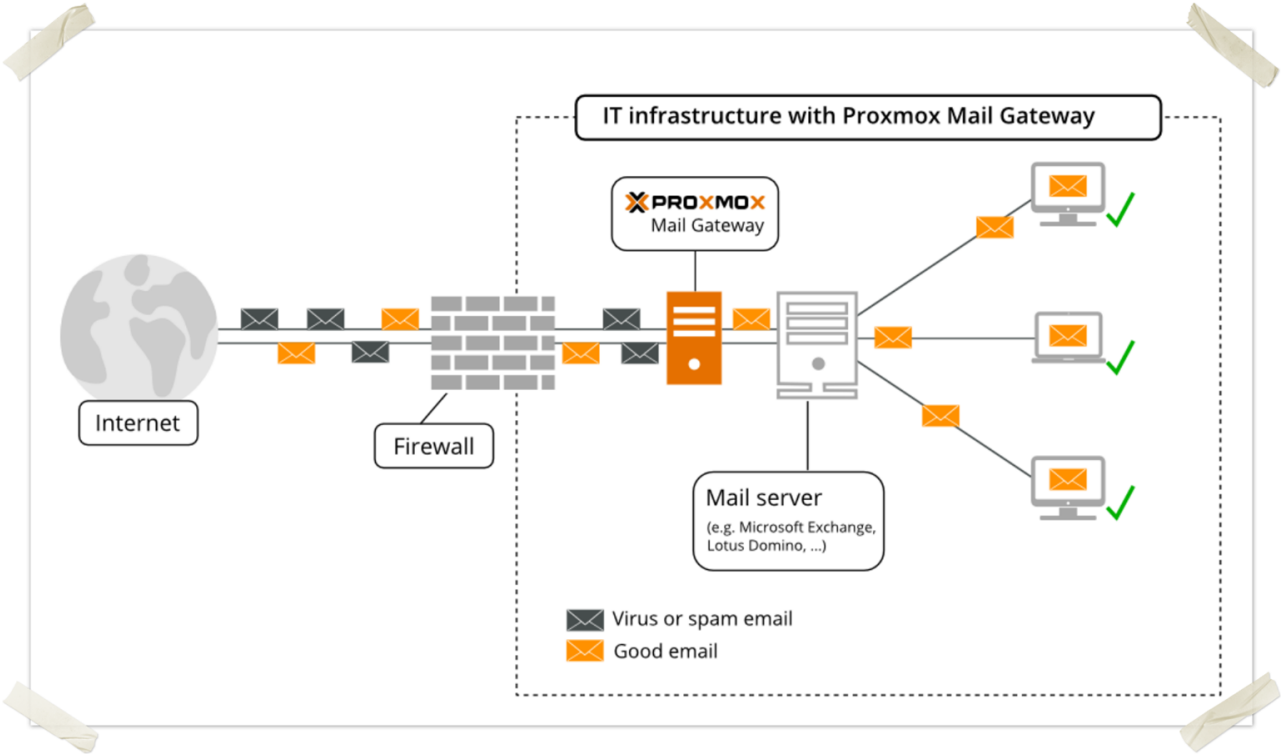
Stand 28.02.2020

Inhaltsverzeichnis

1. Technischer Hintergrund

Der ComNet Spamfilter basiert auf einer freien OpenSource Lösung und wird durch ComNet im Würselner Standort durch das ComNet NOC Team als zentraler Service für die Kunden betrieben.

1.2. Übersicht Maileingang / Filterung



2. ComNet Spamfilter

Der ComNet Spamfilter setzt bei der Erkennung von Spam und schädlichen Inhalten auf lokale und netzbasierte Tests um Spam eMail auszusortieren:

- **Empfängerverifizierung**
- **SPF Prüfung**
- **DNS basiertes Blacklisting**
- **Bayesian Filter – Training durch User (White / Blacklisting)**
- **Autolearning**
- **Spam Uri Realtime BlockList (SURBL)**
- **Greylisting**
- **SMTP Protokol Tests**

Die diversen Tests werden von jeder empfangenen eMail durchlaufen und entsprechend der Ergebnisse einsortiert. Erst nach Abschluss der Prüfung erfolgt eine Weiterleitung an Ihr Postfach. Falls die eMail aufgrund von den Ergebnissen der Tests nicht direkt zugestellt werden kann, erfolgt eine Einsortierung nach folgendem Muster.

2.1. Virus / Schadcode Erkennung

Erkennung eines Virus / Schädlings aufgrund von lokalen Signaturprüfungen
Sollte das System eine eMail oder deren Anhang als Virus / Schadcode erkennen, verschiebt das System diese eMail in eine gesicherte Quarantäne und der Empfänger der eMail wird über den Erhalt dieser eMail informiert, kann aber in keinem Fall darauf zugreifen

ComNet AixGate eMail Information zu blockiertem Virus in Dateianhang:

Der Absender toj@itls-concepts.org hat versucht eine Datei mit schadhaftem Inhalt an toj@aixbyte.de zu übermitteln, diese Nachricht wurde vorsorglich entfernt.

Weitere Details zur geblockten Nachricht:

Betreff der eMail: Virus Test

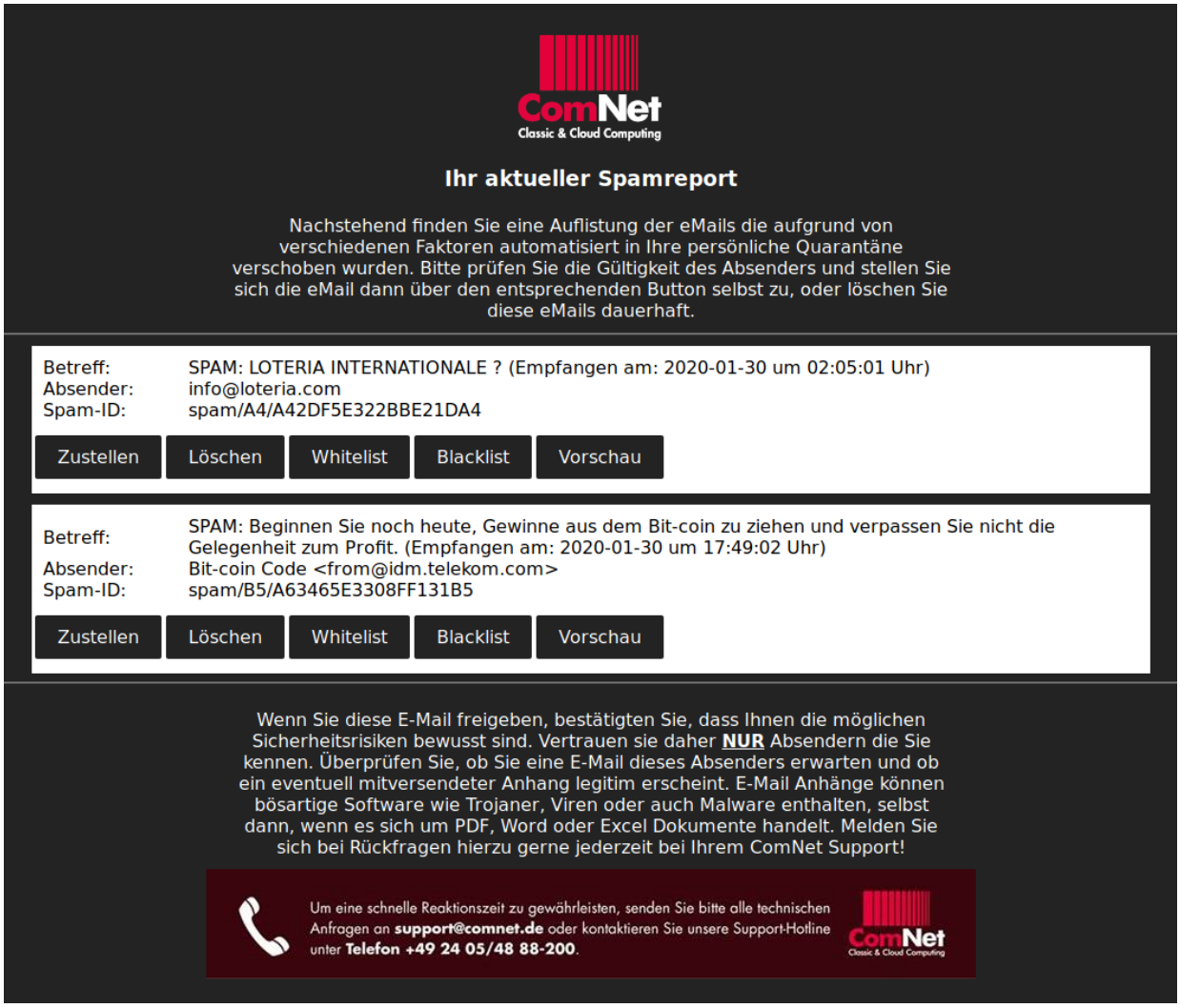
Absender der eMail: toj@itls-concepts.org
IP des Absenders: 80.67.31.32
Empfänger der eMail: toj@aixbyte.de
Ablehnungsursache: Virus in eMail gefunden
Virusdetails: Virus Info: EICAR Test-NOT virus!!! (avast)

Bei Rückfragen zu dieser ComNet Status-eMail kontaktieren Sie bitte das ComNet Support Team:

eMail: support@comnet.de
Telefon: +49 (0)2405 4888 0
Website: https://www.comnet.de

2.2. Spam Erkennung

Erkennung von Spam aufgrund von lokalen und netzseitgen Prüfungen
Die Spamerkennung erfolgt aufgrund von diversen Checks und bei dem Erreichen eines definierten Spamlevels, wird die eMail in die persönliche Quarantäne der User verschoben. Diese Quarantäne liegt hierbei auf dem Webservice des Mailfilters und muss mit dem Webbrowser durch den User besucht werden, um die eMail im Webserver zu prüfen, bevor eine Zustellung der eMail durch den User durchgeführt werden kann. Die Links auf diesen Webserver erhält jeder User kurz nach dem Erhalt einer solchen Nachricht und hat folgendes Format:



Hinweis: zur Nutzung der Links im ComNet Spamreport, empfehlen wir als Standardbrowser den Mozilla Firefox oder einen anderen aktuellen Browser.

2.2.1. SpamReport Funktionen

Der SpamReport bietet dem User die folgenden Optionen für jede in der Quarantäne befindlichen Nachricht an:

- Zustellen

  Zustellen bedeutet, dass die Mail ohne nähere Prüfung im Webportal an den Empfänger übermittelt wird

- Löschen

  Löschen bedeutet, dass die Mail direkt gelöscht wird

- Whitelist

  der Absender wird auf eine Liste mit Adressen gesetzt, die zukünftig nicht mehr als Spam eingestuft werden sollen, eine Virenübermittlung ist dann aber trotzdem nicht möglich

- Blacklist

  der Absender wird auf eine Liste mit Adressen gesetzt, so dass zukünftige eMails direkt geblockt werden

- Vorschau

  ein Direktlink auf das Webportal der persönlichen Quarantäne, in dem dann nähere Details zu der eMail und dem Spamscore einzusehen sind:

  - Beispiel eines Spamscorings

Toggle Raw | Toggle Spam Info | Download | Whitelist | Blacklist | Deliver | Delete

AWL	0.07	Adjusted score from AWL reputation of From: address
BAYES_00	-1.9	Bayes spam probability is 0 to 1%
DKIM_SIGNED	0.1	Message has a DKIM or DK signature, not necessarily valid
DKIM_VALID	-0.1	Message has at least one valid DKIM or DK signature
DKIM_VALID_AU	-0.1	Message has a valid DKIM or DK signature from author's domain
DKIM_VALID_EF	-0.1	Message has a valid DKIM or DK signature from envelope-from domain
HTML_MESSAGE	0.001	HTML included in message
KAM_GRABBAG3	3	Grab bag of spam that employs multiple tricks that indicate tracking of recipi…
KAM_HUGEIMGSRC	0.2	Message contains many image tags with huge http urls
KAM_REALLYHUGEIMGSRC	1.1	Spam with image tags with ridiculously huge http urls
KAM_SHORT	0.001	Use of a URL Shortener for very short URL
KAM_TRACKIMAGE	0.2	Message has a remote image explicitly meant for tracking
LONG_HEX_URI	2.187	Very long purely hexadecimal URI
RCVD_IN_DNSWL_NONE	-0.0001	Sender listed at https://www.dnswl.org/, no trust
RCVD_IN_MSPIKE_H2	-0.001	Average reputation (+2)
SPF_HELO_NONE	0.001	SPF: HELO does not publish an SPF Record
SPF_PASS	-0.001	SPF: sender matches SPF record
T_KAM_HTML_FONT_INVALID	0.01	Test for Invalidly Named or Formatted Colors in HTML
URIBL_GREY	0.424	Contains an URL listed in the URIBL greylist
Spamscore	**5.0919**	

  - eMail Header Informationen
  - Bodytext
  - im „Vorschaubereich" können Sie auch einen Datumsbereich zur Filterung wählen

2.3. Anhang / Dateifilter

Neben der Filterung auf Spam und schadhaften Inhalten, bietet ComNet auch die Möglichkeit gezielt nur einzelne Dateitypen an die eMail Empfänger Ihrer Organisation zuzustellen. Da immer häufiger Schwachstellen auf gezielt ausgesuchte Applikationen bekannt und ausgenutzt werden, bietet es sich an, die Möglichkeiten des unkontrollierten Dateiempfangs weitestgehend auf sichere Formate einzuschränken.

Auch für eMails die aufgrund von unerwünschten Dateianhängen in die Quarantäne verschoben werden, erfolgt eine Benachrichtigung an den Empfänger über den ComNet SpamReport, so dass der User auch bei solchen eMails die Möglichkeit hat, die Inhalte der eMail im Webportal zu betrachten um sich die eMail dann selbst zu zustellen.

2.3.1. Gefilterte Dateitypen / Formate

Aktuell werden folgende Inhalte entsprechend gefiltert und zunächst in die Quarantäne verschoben:

Multimedia

Type	Value
Content Type Filter	content-type=audio/.*
Content Type Filter	content-type=video/.*

Office Dateien

Type	Value
Content Type Filter	content-type=application/msword
Content Type Filter	content-type=application/vnd\.ms-excel
Content Type Filter	content-type=application/vnd\.ms-powerpoint
Content Type Filter	content-type=application/vnd\.oasis\.opendocument\..*
Content Type Filter	content-type=application/vnd\.openxmlformats-officedocument\..*
Content Type Filter	content-type=application/vnd\.stardivision\..*
Content Type Filter	content-type=application/vnd\.sun\.xml\..*

Sonstiges

Type	Value
Content Type Filter	content-type=application/bat
Content Type Filter	content-type=application/javascript
Content Type Filter	content-type=application/postscript
Content Type Filter	content-type=application/vnd.oasis.opendocument.presentation
Content Type Filter	content-type=application/vnd.oasis.opendocument.text
Content Type Filter	content-type=application/vnd.openxmlformats-officedocument.spreadsheetml.sheet
Content Type Filter	content-type=application/vnd\.ms-powerpoint\.presentation\.macroEnabled\.12
Content Type Filter	content-type=application/vnd\.ms-word\.document\.macroEnabled\.12
Content Type Filter	content-type=application/x-bat
Content Type Filter	content-type=application/x-executable
Content Type Filter	content-type=application/x-java
Content Type Filter	content-type=application/x-java-archive
Content Type Filter	content-type=application/x-ms-dos-executable
Content Type Filter	content-type=application/x-perl
Content Type Filter	content-type=application/x-shellscript
Content Type Filter	content-type=application/x-shockwave-flash
Content Type Filter	content-type=text/x-ms-regedit
Match Filename	filename=.*\.(vbs|pif|lnk|shs|shb|bat|exe|dll|com|cpl|xls|xlsm|iso|doc|jar)
Match Filename	filename=.*\.\{.+\}

3. Häufig gestellte Fragen

„Ich erhalte immer wieder Spam von einem Absender obwohl ich erhaltene eMails in der Quarantäne nach dem Erhalt des ComNet Spamreports die eMails immer lösche."

➔ bevor man eine eMail dauerhaft entfernt empfehlen wir die Nutzung der „Blacklist" Funktionalität um das Filtersystem mit diesem „Training" weiter zu entwickeln, um dann zukünftig keine eMail von diesem Absender zu erhalten

„Wielange kann es maximal dauern, bis ich über den Eingang einer als Spam markierten eMail einen SpamReport erhalte?"

➔ die durchschnittliche Wartezeit beträgt 2:30 Minuten und kann maximal 5 Minuten betragen

Kann durch das irrtümliche Whitelisting eines Absenders, zukünftig irrtümlich auch ein Virus oder schadhafter Code an den Empfänger der eMail übermittelt werden, da Prüfungen nicht mehr stattfinden?

➔ Nein, ein Whitelisting betrifft lediglich die Übermittlung von eMails ohne Virus, oder schadhaftem Code, es ist nicht möglich, dass eine eMail mit als Virus erkanntem Inhalt an den Empfänger geht, außer der Absender nutzt dazu verschlüsselte Archive in die ein Virenscanner ohne das Passwort nicht „hineinschauen" kann, daher empfehlen wir den Austausch von geschützten Daten nicht auf Basis von eMailanhängen, sondern über eine entsprechende Cloudlösung

Bekommt der Absender eine Information über ein Black / Whitelisting durch die User?

➔ Nein, eine Benachrichtigung des Absenders über diesen Vorgang wird still unterdrückt

Unsere Organisation möchte gerne nur noch gezielte Dateiformate in der eMail Kommunikation erlauben, besteht die Möglichkeit einer individuellen Filterung nach unserer Vorgabe?

➔ Ja, eine Filterung nach Ihren Vorgaben ist möglich, kontaktieren Sie hierzu bitte den ComNet Support

Ist es möglich den jeweiligen Sicherheitsbeauftragten, einer Domain, anstelle der Enduser über eingehenden Spam oder bei geblockten Dateien zu informieren?

➔ Ja, es ist möglich, dass der Report über geblockte eMails an eine zentrale Stelle reported werden. Sprechen Sie dazu bitte auch den ComNet Support an.

Kann ich ein White / Blacklisting wieder rückgängig machen?

➔ Ja, es ist jederzeit möglich im Webportal die entsprechende Liste einzusehen und Einträge zu bearbeiten.