

Comp-Sys Informatik AG
Glutz-Blotzheim-Strasse 1
4500 Solothurn
032 653 70 77

ASG Anti Spam Gateway & Webquarantaene

Diese Kurzanleitung soll als moegliche Loesung dienen. Es kann sein, dass sich individuell auf den jeweiligen Einsatzbereich zugeschnittene Ansaezte besser eignen.

Die Angaben in dieser Kurzanleitung verstehen sich ohne Gewaehr der Comp-Sys Informatik AG und der Einsatz dieses Dokuments geschieht auf eigene Verantwortung.

Inhalt

Begriffsdefinitionen	3
Filterung und Regeln	4
DNS Blacklist.....	4
Sprachfilter	4
Länderfilter.....	4
Spamfilter.....	4
Virenfilter	4
SPF Prüfung	5
Geblockte Dateitypen	5
Anleitung Web Quarantäne	6
Spam-Mails verwalten.....	6
Zusätzliche Optionen.....	7
Einstellungen	8
Filterungseinstellungen.....	8
Quarantäne-Bericht Einstellungen	9

Begriffsdefinitionen

<i>DNS Blacklist</i>	Die DNS Blacklist ist eine Liste mit Einträgen von unerwünschten IP Adressen. In die Liste eingetragene IP-Adressen werden blockiert.
<i>Blacklist</i>	Die Blacklist beinhaltet vom Nutzer blockierte E-Mail-Adressen. Einkommende Nachrichten von diesen Adressen werden ausgefiltert und abgefangen.
<i>Whitelist</i>	In der Whitelist eingetragene Adressen sind als vertrauenswürdig gekennzeichnet. Sie sind vom Benutzer festgelegt, wobei darauf geachtet werden muss, keine falschen Adressen anzugeben.
<i>Greylisting</i>	Beim Greylisting werden Mails von unbekanntem Absendern beim ersten Empfangen aussortiert. Wird erneut eine Mail von derselben unbekanntem Adresse gesendet, wird dieses nichtmehr aussortiert und angenommen.
<i>Länderfilter</i>	E-Mails werden auch nach Herkunft (Gruppiert nach Ländern) gefiltert. Kommt eine Mail mit einer kritischen Top-Level-Domain als Endung, wird dieses abgefangen und ausgefiltert.
<i>Sprachfilter</i>	Mails welche in bestimmten Sprachen verfasst sind, werden abgefangen und aussortiert.
<i>SPAM Filter</i>	Nach Server und Inhalt geprüfte Nachrichten, bei welchen Werbung vermutet wird, werden aussortiert.
<i>SPF Prüfung</i>	Die SPF Prüfung kontrolliert die Absender-Adresse. Somit kann kein SPAM über falsche Namen gesendet werden. Eine sich auf der Blacklist befindende Adresse könnte mit einem anderen Namen weiterhin Mails senden. Dies wird jedoch durch die SPF Prüfung verhindert.

Filterung und Regeln

Einstellungen können wir für Sie individuell anpassen. Haben Sie Wünsche für Anpassungen, so melden Sie sich beim Comp-Sys Informatik Support Team.

Auf Wunsch können wir die Anti Spam Regeln für Sie verschärfen oder lockern.

DNS Blacklist

Mails welche von einer Adresse versendet werden, die auf der globalen Blacklist steht, werden nicht zugestellt und in der Mail Quarantäne abgelegt.

Die von uns verwendete Blacklist stammt von <https://www.spamhaus.org>

Sprachfilter

Mails, welche in einer der folgenden Sprachen verfasst wurden, werden standardmässig von Sprachfilter blockiert und in der Quarantäne abgelegt.

- Chinesisch
- Russisch
- Ukrainisch

Länderfilter

Es besteht die Möglichkeit Mails mit Absenderadressen aus bestimmten Ländern zu blockieren. Diese Funktion ist standardmässig nicht aktiv, da dies Probleme bei Firmen mit internationaler Kommunikation verursachen könnten.

Wünschen Sie Anpassungen an diesem Filter, melden Sie sich beim Comp-Sys Support.

Spamfilter

Mails, die Inhalte folgender Kategorien aufweisen, werden als SPAM markiert und in die Quarantäne verschoben:

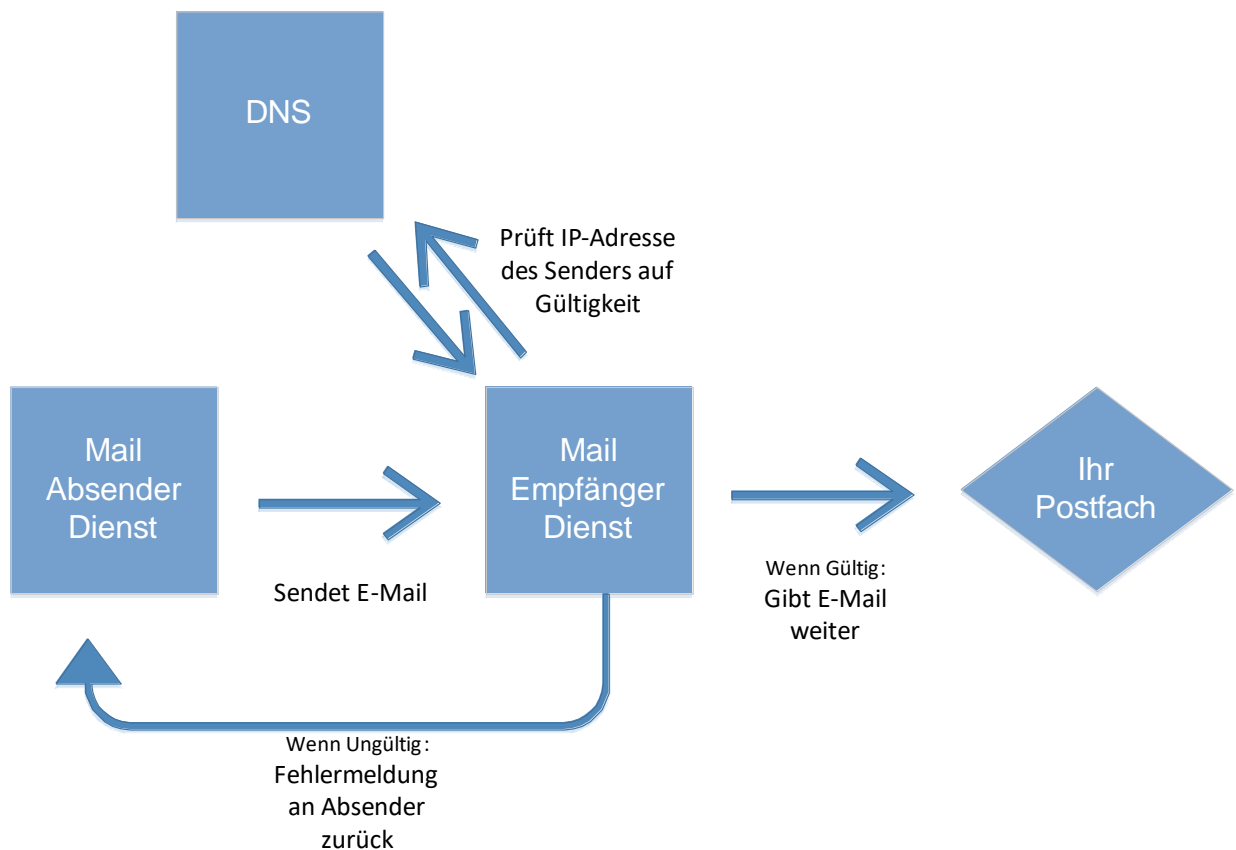
Kategorien	Erklärung zum Inhalt
Adult / Rotlicht	Pornografische oder erotische Inhalte
Money / Finanzen	Bsp.: Falsche Investitionsempfehlungen oder Darlehensangebote
Goods / Waren	Bsp.: Falsche Waren, Güter, Gewinne oder Gewinnspiele.
Health / Gesundheit	Bsp.: Werbe oder Falschhalte für Generikum oder Nahrungsergänzungsmittel.
Verschiedenes / Miscellaneous	Verschiedene andere Inhalte
Spam-Links	Mails mit unerwünschten, gefährlichen oder werbenden Links

Virenfilter

Werden in den Mails Viren oder potenzielle gefährliche Inhalte erkannt, werden diese sofort in die Quarantäne verschoben. Virenmails können mit normalen Benutzerrechten nicht freigegeben werden, da diese gefährlich sein könnten. Bei fälschlichem Virenverdacht in Quarantäne verschobenen Mails kann das Comp-Sys Team weiterhelfen und diese wieder freigeben.

SPF Prüfung

Der ASG prüft die Absenderadresse auf Ihre Gültigkeit. Dies geschieht durch einen sogenannten SPF Eintrag. Der SPF Eintrag zeigt, welche Domain über welche IP-Adresse Mails versenden darf. Stimmen IP-Adresse und Domain nicht überein, werden die Mails in der Quarantäne abgelegt.



Geblockte Dateitypen

Bestimmte Dateien könnten Schäden zufügen oder sind einfach nur unerwünscht. Die folgenden Dateitypen (Dateiendungen) werden aus Sicherheitsgründen blockiert. Mails welche einer dieser Dateitypen als Anhang oder Inhalt vorweisen werden in der Quarantäne abgelegt.

Den Schärfegrad der Filterung kann per Webquarantäne angepasst werden.

Normal	*.BAT, *.COM, *.CMD, *.EXE, *.HTA, *.LNK, *.PIF, *.SCR, *.SHS, *.VB*, *.*
Strong	NORMAL , *.386, *.ACM, *.ADE, *.ADP, *.ASX, *.AVB, *.CD*, *.CHM, *.CLA*, *.CPL, *.CNV, *.CS, *.CRT, *.DLL, *.DOCM, *.DRV, *.DVB, *.GMS, *.HLP, *.HTT, *.INS, *.ISP, *.JAR, *.JS*, *.JTD, *.MSC, *.MSP, *.MST, *.MPD, *.NWS*, *.OBD, *.OCX, *.OFT, *.OV*, *.REG, *.PPTM, *.PS1, *.SCT, *.SHB, *.SHW, *.SMM, *.SYS, *.TLB, *.TSP, *.VSS, *.VST, *.WBT, *.WIZ, *.WSH, *.VXD, *.WBK, *.WSC, *.WSF, *.XLSM, *.INF
Extreme	NORMAL, STRONG , *.BAS, *.CPT, *.MD*, *.MHT*, *.MPP, *.MSI, *.PCD, *.PL, *.PLX, *.POT, *.QPW, *.RTF, *.WPD, *.VS*, *.WMF, *.WMV, *.MP3, *.MPG, *.INI

Anleitung Web Quarantäne

Die Web Quarantäne ist über folgende Adresse aufzurufen:
smail03.comp-sys.net

Es folgt eine Anmeldeseite, bei welcher die E-Mail-Adresse und das zugehörige Passwort angegeben wird.
Das Passwort entspricht dem E-Mail-Passwort.

Ebenfalls wird bei der Anmeldung die Sprache der Webquarantäne ausgewählt.

Spam-Mails verwalten

Sobald der Benutzer angemeldet ist werden die herausgefilterten Mails angezeigt.
An den gelisteten Mails können fünf Operationen vorgenommen werden.



Release Mail / Mail freigeben:

Die Mail wird an den ursprünglichen Empfänger weitergeleitet als wäre sie nie vom Anti Spam abgefangen worden.

Dies eignet sich falls eine Mail fälschlicherweise gefiltert wurde und den Empfänger trotzdem noch erreichen soll.

Release & Trust / Freigeben & Vertrauen:

Die Mail wird an den ursprünglichen Empfänger weitergeleitet als wäre sie nie vom Anti Spam abgefangen worden. Ebenfalls wird der Sender zur Whitelist hinzugefügt. So werden künftige Mails nicht mehr blockiert.

Dies eignet sich, falls eine Mail fälschlicherweise gefiltert wurde und den Empfänger trotzdem noch erreichen soll und Mails dieses Absenders in Zukunft nicht mehr gesperrt werden sollen.

Delete & Block / Löschen & Blockieren:

Markierte Mails werden gelöscht und die Absender dieser Mails zur Blacklist hinzugefügt. Mit dem hinzufügen zur Blacklist werden zukünftige Mails desselben Absenders blockiert.

Dies eignet sich, wenn Spammails endgültig gelöscht werden sollen und keine Mails von diesem Absender mehr durchkommen sollen.

Delete Mail / Mail löschen:

Markierte Mails werden gelöscht und aus der Web Quarantäne entfernt.

Dies eignet sich, wenn Mails endgültig entfernt werden sollen.

Clear All / Alle löschen:

Es werden alle in der Quarantäne abgelegten Mails gelöscht.

Dies eignet sich, wenn sich keine benötigten Mails in der Quarantäne befinden und Platz gemacht werden soll.

Zusätzliche Optionen



Über diesen Button kann die Quarantäne aufgefrischt und auf neue Mails geprüft werden.



Über diesen Button können Mailadressen blockiert werden, indem sie auf die Blacklist gesetzt werden und anschliessend definiert wird, was mit diesen Mails geschehen soll.



Über diesen Button können Mailadressen auf die Whitelist gesetzt werden, sodass Mails von der angegebenen Mailadresse zukünftig nicht mehr blockiert werden.

Einstellungen

Mit einem Klick auf die oben rechts angezeigte eigene Mail-Adresse oder das direkt daneben liegende Dreieck Symbol, wird ein Menü geöffnet. Über dieses Menü sind verschiedene Einstellungen zu erreichen.

Filterungseinstellungen

Im Abschnitt «Bevorzugte Einstellungen» besteht die Möglichkeit Schärfegrad und Aktion der Mail-Filterung anzupassen.

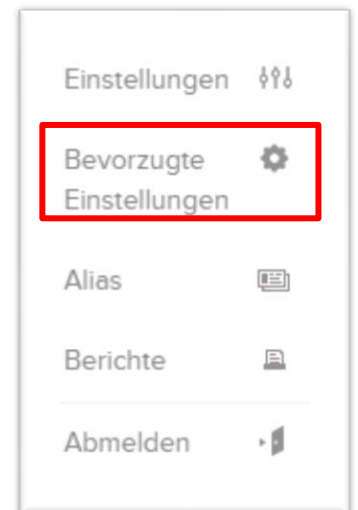
Sämtliche Regeln können verstärkt oder gelockert werden.

Es ist auch möglich die Sprachfilter oder Spam Kategorien anzupassen.

Bei Viren und verbotenen Anhängen kann zusätzlich die Mail Benachrichtigung von Sender und Empfänger aktiviert oder deaktiviert werden. Wird etwas runter gescrollt, sind auch die zu blockierenden Sprachen zu wählen.

Bevor die Filterungseinstellungen angepasst werden, gibt es deren Folgen zu bedenken. Bei falschen Einstellungen könnten beispielsweise vermehrt vom Empfänger gewünschte Mails in der Quarantäne blockiert werden.

Das Comp-Sys Team gibt Ihnen auf Anfrage gerne genauere Auskunft.



Bevorzugte Einstellungen

	Filterebene	Nachricht löschen	Nachricht in Quarantäne blockieren	Nachricht markieren und durchlassen (Spam)	Absender benachrichtigen	Empfänger benachrichtigen
Phishing	Extrem	<input type="radio"/>	<input checked="" type="radio"/>			
Virus	Normal	<input type="radio"/>	<input checked="" type="radio"/>		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Verbotene Anhänge	Stark	<input type="radio"/>	<input checked="" type="radio"/>		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Spamfilter	Normal	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>		
Sprachfilter		<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>		

SPAMKATEGORIEN

Spezielles <input checked="" type="checkbox"/>	Newsletter <input type="checkbox"/>	Waren <input checked="" type="checkbox"/>	Verschiedenes <input checked="" type="checkbox"/>
Rotlicht <input checked="" type="checkbox"/>	Finanzen <input checked="" type="checkbox"/>	Gesundheit <input checked="" type="checkbox"/>	Spam-Links <input checked="" type="checkbox"/>

ERLAUBTE/BLOCKIERTE SPRACHEN

Erlaubte Sprachen: _____
Blockierte Sprachen: _____

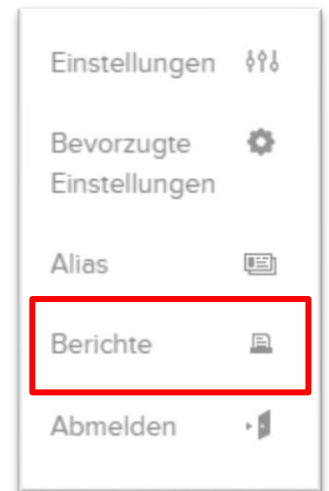
Quarantäne-Bericht Einstellungen

Damit der Überblick über die Quarantäne besser gehalten werden kann, sind automatische Quarantäne-Berichte definiert. Diese werden dem Benutzer für die jeweilig zugehörige Mail auch gleich per Mail zugestellt.

Per Webquarantäne können die Berichte angepasst werden.

Es ist möglich die Häufigkeit, den Inhalt, die Details und den gezeigten Inhalt zu definieren. Per Knopfdruck kann zusätzlich auch gleich ein manuell erzeugter Bericht erstellt werden.

ASG Kunden der Comp-Sys Informatik AG erhalten den Quarantäne Bericht standardmässig täglich um 16:00, insofern neu gefilterte Mails in der Quarantäne gelandet sind.



Berichte
Bericht jetzt erstellen

Berichtszeitplan einstellen:

Bericht niemals senden
 Senden alle:
 7
Tage
@
16:00

Bericht einstellen: CS

Berichtsinhalte auswählen:

Alle Objekte in Quarantäne
 Nur neue Objekte seit dem letzten Bericht

Wählen Sie die zu meldenden Objekte:

- Spam
- Viren
- Phishing (Betrug)
- Verbotene Anhänge

Spam-Wahrscheinlichkeitsstufen:

- Gering = Nachrichten, die ihre Aufmerksamkeit erfordern
- Mittel = ziemlich wahrscheinlich Spam
- Hoch = sehr wahrscheinlich Spam

Die Nachrichtendetails im Bericht anzeigen:

- Datum
- Größe
- Von
- Verfällt am