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

ASG Anti Spam Gateway

Diese Kurzanleitung soll als mögliche Lösung dienen. Es kann sein, dass individuell auf den jeweiligen Einsatzbereich zugeschnitten sich andere Ansätze besser eignen.

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

Inhalt

Begriffsdefinitionen

DNS Blacklist	Die DNS Blacklist ist eine Liste mit Einträgen von unerwünschten IP Adressen. In die Liste eingetragen werden IP Adressen blockiert.
Blacklist	Die Blacklist beinhaltet vom Nutzer blockierte E-Mail-Adressen. Nachrichten einkommend von diesen Adressen werden ausgefiltert und abgefangen.
Whitelist	In der Whitelist eingetragene Adressen sind als vertrauenswürdig gekennzeichnet. Sie sind vom Benutzer festgelegt, wobei darauf geachtet werden muss, keine falschen Adressen anzugeben.
Greylisting	Beim Greylisting werden Mails von unbekannten Absendern beim ersten Empfangen aussortiert. Wird erneut ein Mail von derselben unbekannten Adresse gesendet, wird dieses nichtmehr aussortiert und angenommen.
Länderfilter	E-Mails werden auch nach Herkunft (Gruppiert nach Ländern) gefiltert. Kommt ein Mail mit einer kritischen Top-Level-Domain als Endung wird dieses abgefangen und ausgefiltert.
Sprachfilter	Mails welche in bestimmten Sprachen verfasst sind, werden abgefangen und aussortiert.
SPAM Filter	Nach Server und Inhalt geprüft werden Nachrichten, bei welchen Werbung vermutet wird, aussortiert.
SPF Prüfung	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.

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 Antispam 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 blockiert und in der Quarantäne abgelegt.

- Chinesisch
- Russisch
- Ukrainisch

Länderfilter

Mails mit einer Absenderadresse aus folgenden Ländern, werden blockiert und in der Quarantäne abgelegt.
Der Länderfilter kann für jede Domain einzeln deklariert werden.
Wünschen Sie Anpassungen an diesem Filter, melden Sie sich beim Comp-Sys Support.

- Polen (pl)
- Russland (ru)
- China (cn)
- Ungarn (hu)

Spamfilter

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

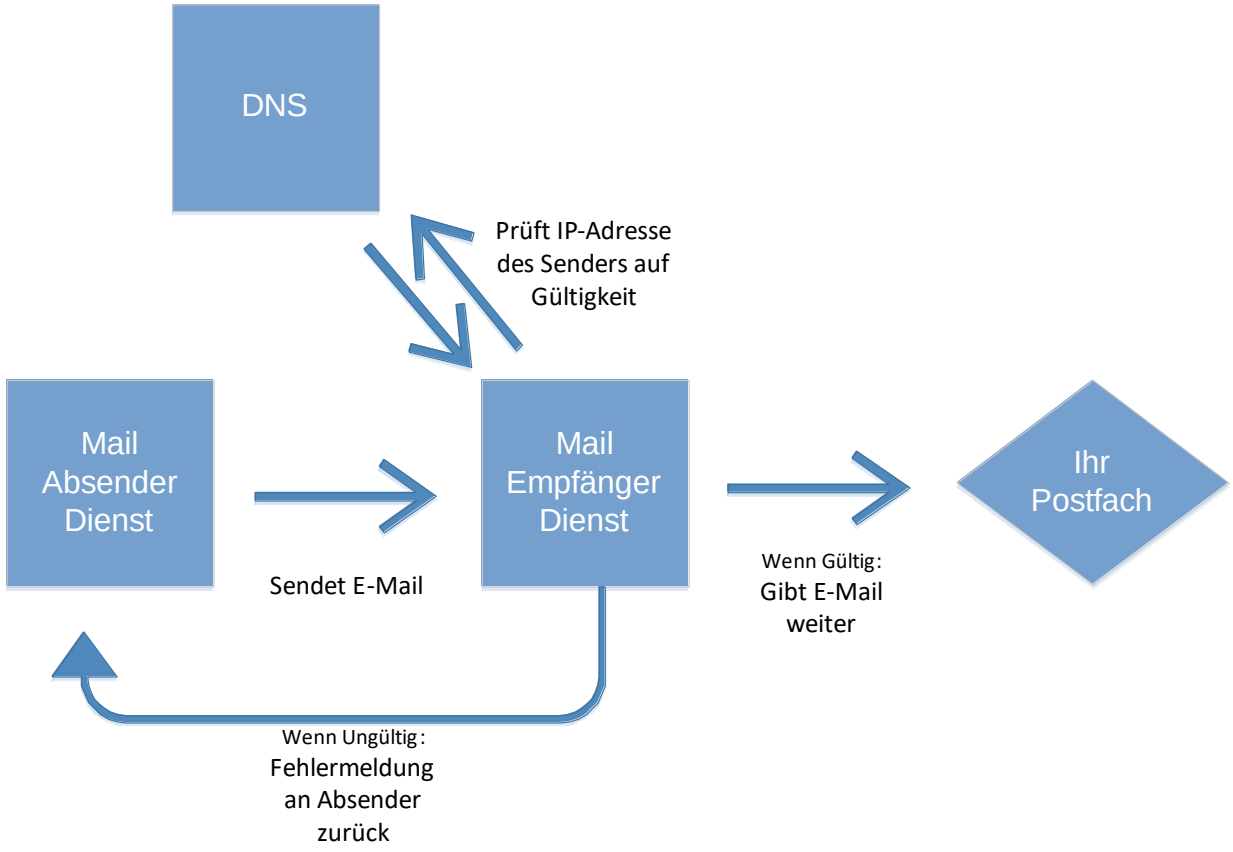
- Adult
- Money
- Goods
- Health
- Spam Links

Virenfilter

Werden in den Mails Viren erkannt, werden diese sofort in Quarantäne verschoben. Virenmails können mit normalen Benutzerrechten nicht freigegeben werden, da diese gefährlich sein könnten.

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.

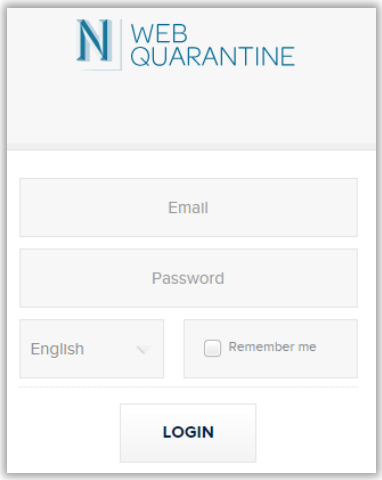


Geblockte Dateitypen

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

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 erreicht man ganz einfach über smail01.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 kann gleich bei der Anmeldung die Sprache gewählt werden.

Spam-Mails verwalten

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

Release Mail / Mail freigeben: Das Mail wird an den ursprünglichen Empfänger weitergeleitet als wäre es nie vom Antispam abgefangen worden. Dies eignet sich falls ein Mail fälschlicherweise gefiltert wurde und den Empfänger trotzdem noch erreichen soll.
Release & Trust / Freigeben & Vertrauen: Das Mail wird an den ursprünglichen Empfänger weitergeleitet als wäre es nie vom Antispam abgefangen worden. Ebenfalls wird der Sender zur Whitelist hinzugefügt. So werden künftige Mails nicht mehr blockiert. Dies eignet sich falls ein 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 werden und wird auf neue Mails geprüft.

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.