# Mail Policy

**für die Mailserver der Dr. Bülow & Masiak GmbH | Stand 01.08.2018**

**In diesem Dokument wird der derzeitige Stand der Policy (Regelwerk zur Behandlung von E-Mails) des Mailsystems der Dr. Bülow & Masiak GmbH beschrieben. Generell haben unsere Kunden die Möglichkeit, ihre eigenen Mailserver als MX-er einzutragen/eintragen zu lassen oder den zentralen E-Mail-Dienst der Dr. Bülow & Masiak GmbH zu nutzen.**

## Allgemeine Maßnahmen

1. Die Absenderdomain muss existieren.
2. Wenn im HELO (EHLO) eine IP-Adresse (in dezimaler oder Oktett-Schreibweise) eingetragen ist, muss diese mit der IP der Gegenseite übereinstimmen.
3. Für die IP des versendenden Mailservers muss ein Reverse-DNS-Lookup möglich sein.
4. Die IP-Adresse der Gegenseite darf nicht als dynamische IP-Adresse gelistet sein (Basis der Überprüfung: pbl.spamhaus.org).
5. Die IP Adresse darf nicht bei NiX-Spam (ix.dnsbl.manitu.net), bei Barracuda oder SpamCop gelistet sein.
6. Die Empfängeradresse muss in einer gerouteten Domain und gültig sein.
7. Die Mailgröße (Header+Body) darf 20 MB nicht überschreiten.
8. Die Mailanzahl darf 1.000 Mails pro Stunde nicht überschreiten (Rate Limiting).
9. Bestimmte Dateiformate (z.B: exe) dürfen nur im ZIP-Format angehängt werden.
10. Es darf kein Sperrvermerk in der manuell gepflegten Sperrliste (Blacklist) vorliegen.
11. Der versendende Mailserver muss temporär abgelehnte Nachrichten nach einer kurzen Wartezeit erneut zustellen (Greylisting 3min).
12. Der Mailinhalt muss virenfrei sein.

## Greylisting

Beim Greylisting werden eingehende E-Mails temporär abgelehnt. Systeme, von denen Spam direkt verschickt wird, unternehmen dabei keinen weiteren Versuch diese E-Mail zuzustellen. Normale Mail-Server unternehmen i.d.R. nach 5-10 Minuten einen weiteren Versuch, die Mail zuzustellen. Ist eine E-Mail einmal angenommen und zugestellt worden, wird der Absender für 35 Tage auf eine dynamische Whitelist gesetzt, so dass weitere E-Mails direkt angenommen werden. Erfolgt ein permanenter Austausch von E-Mails, so wird der Whitelist-Eintrag immer wieder aktualisiert. Es können zudem Ausnahmen definiert werden (s.u.).

## Spam-Bewertung

Jede angenommene E-Mail mit einer Größe bis maximal 20 MB wird durch das Bewertungsprogramm auf Spam geprüft. Eine E-Mail, die als Spam klassifiziert wird, erhält eine eindeutige Kennzeichnung im Header der E-Mail (z. B. X-Spam-Level: ****) und wird zugestellt. Die Anzahl der Sterne gibt den Grad der Wahrscheinlichkeit für eine Spammail an. Diese Informationen können zur Formulierung von Filterregeln in den Mail-Clients herangezogen werden.

Eine E-Mail wird als Spam klassifiziert, wenn ein oder mehrere Filterkriterien zutreffen. Hier setzt die Dr. Bülow & Masiak GmbH auf die bekannten Methoden Bayes Filter und Realtime Blacklists (RBLs). Sollten einzelne E-Mail-Nachrichten falsch klassifiziert werden, kann dies dem u.g. Support mitgeteilt werden (Spam-Nachricht als Anhang via Mail). Die Systeme der Dr. Bülow & Masiak GmbH werden durch dieses Anlernen verbessert. Es können Nachrichten als Spam klassifiziert werden oder aber als reine E-Mail-Nachricht (Ham).

## Pflege der lokalen Black- und Whitelist

Die Dr. Bülow & Masiak GmbH kann die Mail-Annahme für Domains sehr granular bestimmen. Neben der Möglichkeit Ausnahmen für das Greylisting oder das Spamtagging zu erstellen, können auch einzelne Absenderadressen oder Server auf eine Blacklist gesetzt werden. Für Änderungen wenden Sie sich bitte an support@buelow-masiak.de.

## AntiVir-Filter

Alle E-Mails, die über die Mail-Relays der Dr. Bülow & Masiak GmbH empfangen oder versendet werden, werden durch ein Virenscanning überprüft. Schadhafte E-Mails werden geblockt und der Absender benachrichtigt.

# Mail Policy

**für die Mailserver der Dr. Bülow & Masiak GmbH | Stand 01.08.2018**

## Mailablehnung

Es gibt verschiedene Möglichkeiten, warum die Mailhubs der Dr. Bülow & Masiak GmbH eine E-Mail nicht entgegen nehmen, bzw. die Zustellung ablehnen:

1. Virenbefall
   Bei positivem Virenscanning wird die eingehende E-Mail von den Mailhubs abgelehnt (rejected).
2. Dynamische IP, offenes Mailrelay
   Bevor die Mail angenommen wird, findet eine Überprüfung der IP Adresse mit diversen Blacklistens statt. Es gibt eine allgemeine Vereinbarung unter Providern, dass E-Mail-Systemen mit dynamischen IPs keine direkte Mailzustellung gewährt wird, sondern dass zwingend immer das entsprechende Provider Mailrelay genutzt werden muss. Darüber hinaus sind in dieser Liste bekannte offene Mailrelays eingetragen, die von Spammern bevorzugt für den Spamversand genutzt werden.
3. Keine lokale Domain
   Die Mail wurde von einer nicht für das Relaying freigeschalteten IP an eine fremde Domain verschickt.
4. Reverse-DNS-Lookup nicht möglich
   Für die IP des Absenders existiert kein Reverse-DNS-Eintrag oder der Reverse-DNS-Eintrag stimmt nicht mit dem Forward-DSN-Eintrag überein.
5. IP auf Blacklist
   Die IP des Absenders ist entweder auf der pbl.spamhaus.org-, auf der NiX-Spam- , IX- ZEN- oder der lokalen Blacklist gelistet.
6. Mail-Größe
   Die Mail ist größer als 20 MB.
7. Mail-Anzahl
   Die erlaubte Mailanzahl liegt bei 1.000 Mails pro Stunde. Ausnahmen für z.B. Newsletter sind auf Anfrage möglich (Rate Limiting).
8. Verdächtige Anhänge
   Folgende Formate werden geblockt und können nur im ZIP-Format zugestellt werden: exe, vbs, pif, scr, bat, cmd, com, cpl, dll
9. Greylisting
   Die Mail wird bei aktiviertem Greylisting mit einem temporären Fehler abgelehnt und erst 3 Minuten nach dem ersten Zustellversuch angenommen. Der versendende Mailserver sollte die Zustellung normalerweise nach einer kurzen Wartezeit erneut versuchen. Weitere Mails aus diesem Netz mit den gleichen Absender- und Empfänger-Adressen werden für 35 Tage seit der letzten durchgestellten Mail ohne Verzögerung angenommen.

   Natürlich gibt es für das Greylisting Ausnahmelisten. Unterschieden wird hier zwischen der Absender- und der Empfänger-Domain. Wenn nicht gewünscht ist, dass für eine Domain Greylisting angewendet wird, kann sie auf die Ausnahmeliste gesetzt werden. Damit werden E-Mails ohne Verzögerung zugestellt. Sollen nur einzelne E-Mails ohne Verzögerung zugestellt werden, können die Mail-Server dieser Absender auf unsere Ausnahmeliste gesetzt werden.

## Infrastruktur

Aktuell werden von der Dr. Bülow & Masiak GmbH drei Mail-Relays betrieben:

1. Mail In (Standort Marl)
   System: mx01.dbmg.de|mx03.dbmg.de|mx04.dbmg.de
   => 80.241.192.48
2. Mail Out (Standort Marl)
   System: mx02.dbmg.de|mx05.dbmg.de|mx06.dbmg.de
   => 80.241.192.23 und 80.241.192.51

Wir empfehlen allen unseren Kunden als Smarthost bzw. Mailrelay für den eigenen Mailserver den mx02.dbmg.de zu verwenden.

## Firewall-Konfiguration bei direkter Mailzustellung

Folgende IP Adressen müssen für die Zulieferung von E-Mails über Port 25 in den Kunden-Firewalls frei geschaltet sein:

1. mx01.dbmg.de => 80.241.192.48
2. mx02.dbmg.de => 80.241.192.51
3. mx06.dbmg.de => 80.241.192.23

Die E-Mail Zustellung und Annahme erfolgt ausschließlich von diesen IP Adressen.