Network Policy

E-Mail ist ein unverzichtbares Kommunikationsmedium für unsere Kunden. Leider wird es durch die grosse Anzahl an Spam-Mails inzwischen stark behindert; weniger als 5% der an unsere Server geschickten Mails sind tatsächlich für unsere Kunden bestimmte Nutzmails.

Damit die Killer-Applikation E-Mail nicht Ihr Unternehmen killt, braucht es klare „Spielregeln". Das anyHost Datacenter schränkt den Datenverkehr auf den Mailservern und verbundenen Internet Services im Kampf gegen unerwünschte und verseuchte E-Mails ein. Um die Verbreitung dieser Daten zu verhindern bzw. mindestens wesentlich einzuschränken, prüfen standardisierte Verfahren recht agressiv, ob Benutzer und Mailserver die Spielregeln des Mailbetriebes einhalten.

Vorliegende Netzwerkrichtlinien beschreiben die grundlegenden Verfahrensweisen für die korrekte E-Mail-Kommunikation mit den anyMails Plattformen und stehen im Einklang mit den weltweit gültigen Best Practices sowie den Schweizer Gesetzen.

Gültigkeit

Das anyHost Datacenter verarbeitet auf den Mailservern für unsere und aller verbundenen Internet Services nur E-Mails und Nachrichten, die unserer Network Policy und den damit zugrundeliegenden Richtlinien entsprechen. Kunden mit einer anyMails Collaboration Suite sind in der Parametrisierung der wichtigsten Einstellungen frei, für Kunden mit anyMails Groupware-Konten gelten die nachfolgend beschriebenen Parameter.

1. Grundsatz

anyMails nimmt grundsätzlich alle Nachrichten von legitimen Mailservern an, es werden keine E-Mails gelöscht. Dennoch kann es im Einzelfall dazu kommen, dass legitime E-Mails zurückgewiesen werden. Weitere Informationen dazu unter Punkt 4, 5, 6, 7, 8, 9 und 10.

2. Ports

Im Gegensatz zu vielen Internet- und Service-anbietern blockiert anyMails keine Standardports und kann daher weltweit providerunabhängig d.h. über den Internetzubringer Ihrer Wahl eingesetzt werden. Es gelten folgende Porteinstellungen:

Desktop/Web-Client	Port 80
Desktop/Web-Client SSL	Port 443
IMAP	Port 143
IMAP SSL	Port 993
IMAP Proxy	Port 7143
IMAP Proxy SSL	Port 7993
POP3	Port 110
POP3 SSL	Port 995
SMTP	Port 25 oder 587

3. Nur authentifizierte Zugriffe

Die Abfrage und Synchronisierung von Daten sowie der Versand über externe Clients, Programme oder Server setzt eine Benutzerauthentifizierung voraus. anyMails gestattet keine autonyme Anmeldung. Erfolgt über einen längeren Zeitraum keine Transaktion, wird die Verbindung automatisch getrennt (Timeout).

4. Mehrfacher Virenschutz

Alle eingehenden E-Mails und Anhänge werden auf schädliche oder virenverseuchte Inhalte überprüft. Infizierte E-Mails welche Viren, Würmer, Trojaner oder Phising-Inhalte enthalten, werden abgelehnt. Der Empfänger erhält in diesem Fall eine Systemnachricht mit folgenden Informationen:

- verwendete Empfängeradresse
- vermeintlicher Sender mit Name und E-Mailadresse
- sendender Mailserver mit eindeutiger IP-Adresse
- identifizierter Inhalt (Virus, Trojaner etc.) mit verwendetem Dateiname

Bitte beachten Sie, dass Verweise auf fremde Seiten nicht überprüft werden können. Hier gilt generell: wenn Sie den Absender nicht kennen sollten Sie weder E-Mails, Anhänge noch Links öffnen!

5. Zentrale Blocklists

anyMails nutzt zentral geführte Sperrlisten (DNSBL) welche in Echtzeit Netzwerkadressen abfragen um E-Mails zweifelhafter Herkunft als Spam zu klassifizieren. In den meisten Listen werden IP-Adressen von Rechnern gelistet, die in der Vergangenheit durch häufigen Versand unerwünschter Spamnachrichten aufgefallen sind.

Eingehende E-Mails können aufgrund von Listen-Einträgen abgewiesen werden. Der Sender erhält in diesem Fall eine Systemnachricht unter Angabe der referenzierten Sperrliste sowie der genutzten IP-Adresse.

anyHost Datacenter
Brunnackerstrasse 2
2563 Ipsach

by Troppus GmbH
T 032 512 14 90

Datacenter West
3186 Düdingen

Alle Daten liegen in der Schweiz, sicher und mit höchstem Datenschutz.
www.anyhost.ch

Erhält Ihr Korrespondenzpartner eine entsprechende Systemnachricht, sollte er sich an seinen Internet-anbieter wenden. Der Eigentümer der IP-Adresse müsste dafür besorgt sein, dass der Eintrag wieder gelöscht- und die verwendete Adresse freigegeben wird. Solange die Adresse gelistet ist, können von diesem Anschluss keine E-Mails empfangen werden.

6. Individuelle White-/Blacklists

Kunden können pro Postfach eigene Richtlinien in Form von weissen und schwarzen Listen hinterlegen. Die Eintragung kann einzelne E-Mailadressen oder ganze Domainnamen umfassen welche explizit zugelassen- bzw. blockiert werden sollen. Voraussetzung in beiden Fällen ist, dass die E-Mails nicht gegen andere Richtlinien verstossen.

7. Greylisting

Zum Schutz der anyMails Plattformen setzen wir u.a. Greylisting ein, eine nach internationalen Normen definierte Form der Spam-Bekämpfung. Anders als bei anderen Verfahren wird hierbei nicht der Inhalt der E-Mail überprüft, sondern der Dialog des sendenden Mailservers.

Das Prinzip ist sehr einfach. Basierend auf der Annahme, dass sich ein Spammer nicht die Mühe eines zweiten Zustellversuchs macht, weisen unsere Server Anfragen von einem bisher unbekannten Mailserver mit einem temporären Fehler ab. Ein korrekt konfigurierter Mailserver wird die E-Mail nach kurzer Zeit erneut zustellen. Da die Kombination aus IP-Adresse, Empfänger- und Absenderadresse bei anyMails dann schon bekannt ist wird der Zustellversuch nun zugelassen und die IP-Adresse des Senders in einer automatisch generierten Whitelist eingetragen.

Ein Nachteil des Greylistings ist eine kurze Verzögerung von E-Mails, die je nach sendendem System zwischen 10-15 Minuten liegen kann. Diese Verzögerung beschränkt sich allerdings nur auf die erste E-Mail die von diesem System zugestellt wird. Sollte dieser Mailserver in der Zukunft weitere E-Mails zustellen wollen, werden diese Verbindungen sofort akzeptiert und müssen nicht mehr durch den Greylisting-Prozess. Da der E-Mail-Verkehr in den meisten Fällen immer zwischen den gleichen Empfängern ausgetauscht werden ist nach einer kurzen "Lernphase" des Filters von der Verzögerung nichts mehr zu spüren.

8. Spamfilter

Eingehende E-Mails welche legitim zugestellt werden, aus Sicht von anyMails aber in die Kategorie Spam gehören, werden im Betreff als „dedected Spam“ markiert und ohne Verzögerung an Ihr Postfach weitergeleitet.

Sie haben damit die volle Kontrolle, ob Sie das E-Mail bearbeiten - oder mittels Filter löschen bzw. in einen Spam-Ordner verschieben möchten. anyMails löscht keine E-Mails.

9. Individuelle Filter

Kunden können pro Postfach eigene Filter für eingehende oder ausgehende E-Mails hinterlegen. Es lassen sich Regeln nach beliebigen Kriterien wie bsp. nach Sender, Empfänger, Betreff oder Inhalte anlegen. Entsprechend dem Resultat lassen sich die E-Mails verwerfen, in beliebigen Ordnern speichern, markieren oder Weiterleiten.

10. Gesperrte Dateianhänge

Um Sie im täglichen Umgang mit E-Mails bestmöglich zu schützen, werden Dateianhänge mit ausführbarem Inhalt abgewiesen. Der Sender und Empfänger erhält in diesem Fall eine System-nachricht mit dem Hinweis, dass die Annahme der E-Mail abgelehnt wurde. Derzeit werden Inhalte mit folgenden Dateiendungen abgewiesen:

- .asd
- .bat
- .chm
- .cmd
- .com
- .dll
- .do
- .exe
- .hlp
- .hta
- .js
- .jse
- .lnk
- .ocx
- .pif
- .reg
- .scr
- .shb
- .shm
- .shs
- .vbe
- .vbs
- .vbx
- .vxd
- .wsf
- .wsh
- .xl

Bitte beachten Sie, dass auch in Office-Dateien wie beispielsweise .doc oder .xls ausführbare Makros versteckt sein können. Hier gilt generell: wenn Sie den Absender nicht kennen sollten Sie weder E-Mails, Anhänge noch Links öffnen!

Wir empfehlen grundsätzlich, Anhänge nur im PDF oder ZIP Format anzuhängen.

11. Gesperrte Netze

Die anyMails-Server werden durch Angrifferken-nungssysteme (Intrusion Detection) geschützt. Netzwerke aus denen Aktivitäten gegen die System- und Netzwerk-Sicherheit des anyHost Datacenter ausgehen, werden ggf. gesperrt und können in der Folge keine Verbindung zu den Mailserver mehr herstellen.

anyHost Datacenter
Brunnackerstrasse 2
2563 Ipsach

by Troppus GmbH
T 032 512 14 90

Datacenter West
3186 Düdingen

Alle Daten liegen in der Schweiz, sicher und mit höchstem Datenschutz.
www.anyhost.ch

Empfehlungen für eine korrekte Kommunikation

Prüfen Sie bitte, ob die Mail-Systeme Ihrer Korrespondenzpartner diesen Empfehlungen für eine korrekte und fehlerfreie Kommunikation entsprechen, bevor Sie unseren Support kontaktieren. Falls es zu Problemen bei der Kommunikation mit unseren Mailservern gekommen ist, prüfen Sie zunächst die Fehlermeldungen und geben Sie vorliegende Informationen an den Betreiber des anderen Mailservers weiter.

In 95% aller gemeldeten Fälle sind die Zustellversuche auf fehlerhafte, in jedem Fall aber unzureichend konfigurierte Mailserver und Programme zurückzuführen, die bei temporären Fehlern keinen späteren Zustellversuch unternehmen, sondern die E-Mail trotz nicht erfolgter Zustellung verwerfen. Dies gilt auch für den Versand über dynamische (wechselnde) IP-Adressen während dem Greylisting-Zeitfenster.

Die für alle beteiligten beste Lösung ist, auf Seite des Senders die Infrastrukturen dahingehend anzupassen, dass der Umgang mit anderen Parteien sicher und den Normen entsprechend stattfindet. Bitte haben Sie Verständnis, dass wir bei geteilten Infrastrukturen wie anyMails Groupware, welche durch mehrere Kunden genutzt werden, eine Sorgfaltspflicht gegenüber allen Anwender haben und Sicherheitsfunktionen nicht einfach ausschalten können. Kunden mit einer anyMails Collaboration Suite können die Sicherheitsfunktionen bei Bedarf individuell einstellen da Sie nur selber von den Auswirkungen betroffen sind.

Technische Voraussetzungen

- Alle E-Mails welche an die anyMails-Server und verbundenen Internet Services gesendet werden, müssen der anyMails Network Policy sowie den RFC-Richtlinien entsprechen. (Hinweise hierzu unter http://www.rfc-editor.org)
- Alle Mailserver, die sich mit unseren Systemen verbinden, müssen gegen den unerlaubten oder anonymen Missbrauch geschützt sein (kein Open Relay/keine Listung bei RBL).
- Alle Mailserver, die sich zu unseren Systemen verbinden, müssen einen gültigen Reverse DNS Record besitzen.

Hilfe bei der Fehlerbehebung

Falls Ihr Mailserver keine E-Mails an uns bzw. unsere Kunden zustellen kann, prüfen Sie bitte zunächst die erhaltene Fehlermeldung auf weitere Details. Jede Fehlermeldung beginnt mit einer dreistelligen Zahl, gemäss den Internet-Standards nach RFC-1893.

Fehlermeldungen die mit 4.x.x beginnen sind vorübergehender Natur d.h. Sie können diese im Normalfall ignorieren. Eine typische 4er-Fehlermeldung weist auf Verzögerungen in der E-Mail Zustellung hin.

Fehlermeldungen die mit 5.x.x beginnen sind von dauerhafter Art und sollten umgehend behoben werden. Sie finden ggf. im Logfile Ihres Mailservers weitere detaillierte Hinweise, warum eine E-Mail an unsere Server und Netze nicht zugestellt werden konnte. Weitere Informationen zu Fehlercodes aufgrund restriktiven Prüfungen finden Sie auch im Anhang.

Melden von abgewiesenen/fehlenden E-Mails

Falls Sie ein Betreiber von Maildiensten, ein verantwortlicher Postmaster oder ein System-Administrator sind und denken, dass wir irrtümlich E-Mails abweisen oder diese nicht mit unseren Plattformen kommunizieren können, nutzen Sie bitte unser Meldeformular für Kommunikationsprobleme:

- http://www.anyhost.ch/index.php/5ueberuns/50kontakt

anyHost Datacenter
Brunnackerstrasse 2
2563 Ipsach

by Troppus GmbH
T 032 512 14 90

Datacenter West
3186 Düdingen

Alle Daten liegen in der Schweiz, sicher und mit höchstem Datenschutz.
www.anyhost.ch

Anhang: Statuscode 4xx fehlgeschlagen

Dieser Artikel beschreibt die Ursachen für einen Verbindungsfehler mit unseren Netzen und Servern und deren Fehlerbeseitigung. Der Verbindungsfehler beruht auf einem Verstoss gegen unsere Network Policy.

Typische Fehlermeldung:

421 ip address 127.127.127.13 is blacklisted (pbl.spamhaus.org)

Ursache:

Ihr Mailserver (aus oberem Beispiel mit der IP-Adresse 127.127.127.13) ist auf einer oder mehreren Blocklists gelistet.

Lösung:

Überprüfen Sie die Konfiguration Ihres Mailservers und stellen Sie sicher, dass der Mailserver nicht für Spam missbraucht wird. Setzen Sie sich mit dem Betreiber der Blocklist in Verbindung (in oberem Beispiel via www.spamhaus.org/pbl) und folgen Sie den Anweisungen wie Sie Ihre IP-Adresse wieder von der Liste entfernen können. Falls die verwendete Adresse zwischenzeitlich von der Blocklist entfernt wurde oder nicht mehr gelistet wird, senden Sie die E-Mail erneut zu, da die Ablehnung auf Grund der Zwischenspeicherung der Liste erfolgte.

anyMails ist weder Betreiber von solchen Blocklists und nimmt auch keinen Einfluss auf eingetragene Adressen. Da die Listen zwischen Internet-Providern abgeglichen wird, ist die Wahrscheinlichkeit hoch, dass auch mit anderen seriösen Mailbetreibern keine Verbindung hergestellt werden kann.

Typische Fehlermeldung:

451 too many mails from ip address 127.127.127.13

Ursache:

Ihr Mailserver (aus oberem Beispiel mit der IP-Adresse 127.127.127.13) versucht, innerhalb einer definierten Zeitspanne zu viele E-Mails an unsere Mailserver zu senden und überschreitet hierbei ein definiertes Limit. Dies deutet auf die Zusendung von Spam-Mails, einem Missbrauch Ihres Mailservers oder einen Virus hin. Um die Systeme zu schützen wurde ein weiterer Empfang von E-Mails von dieser IP-Adresse abgelehnt.

Lösung:

Überprüfen Sie die Konfiguration Ihres Mailservers und stellen Sie sicher, dass der Mailserver nicht für Spam missbraucht wird. Reduzieren Sie ggf. die Anzahl der gleichzeitigen E-Mails welche Ihr Server versenden kann. Prüfen Sie, ob die E-Mails, die Sie an unsere Systeme senden, unseren Richtlinien entsprechen. Versuchen Sie zu einem späteren Zeitpunkt erneut, die E-Mails zuzustellen.

Weitere nützliche Hinweise und Tools zur Fehlerbehebung:

- http://www.dnsqueries.com
- http://www.dnsstuff.com
- http://www.dns-utils.com
- http://www.iptools.com
- http://www.fixyourip.com
- http://www.intodns.com
- http://www.dnsutils.com

anyHost Datacenter
Brunnackerstrasse 2
2563 Ipsach

by Troppus GmbH
T 032 512 14 90

Datacenter West
3186 Düdingen

Alle Daten liegen in der Schweiz, sicher und mit höchstem Datenschutz.
www.anyhost.ch

Anhang: Statuscode 5xx permanenter Fehler

Dieser Artikel beschreibt die Ursachen für einen Verbindungsfehler mit unseren Netzen und Servern und deren Fehlerbeseitigung. Der Verbindungsfehler beruht auf einem Verstoss gegen unsere Network Policy.

Typische Fehlermeldung:

51x

Ursache:

Beginnt die Fehlermeldung mit 51x, dann stimmt entweder etwas mit der Adresse des Empfängers oder mit der in Ihrem E-Mail-Programm als Absender hinterlegten Adresse nicht.

Lösung:

Prüfen Sie die Adresse des Empfängers. Gegebenenfalls rufen Sie den Empfänger an und überprüfen die Adresse gemeinsam mit ihm.

Typische Fehlermeldung:

550 Relay not permitted

Ursache:

Die Fehlermeldung 550 bedeutet darauf hin, dass sich Ihr E-Mail-Programm vor dem Versand über anyMails nicht korrekt angemeldet hat.

Lösung:

Prüfen Sie Ihre Zugangsdaten in Ihrem E-Mail-Programm. Am häufigsten tritt dieser Fehler bei einem frisch eingerichteten E-Mail-Konto in Microsoft Outlook auf. Denn Outlook meldet sich in der Grundeinstellung gar nicht am E-Mail-Server an, sondern beginnt direkt mit der Zustellung.

Öffnen Sie die Einstellungen des E-Mail-Kontos unter "Extras > Kontoeinstellungen". Rechts unten finden Sie einen Knopf "Weitere Einstellungen". Klicken Sie diesen an und wechseln Sie auf den Reiter "Postausgangsserver". Stellen Sie sicher, dass "der Postausgangsserver (SMTP) erfordert Authentifizierung" markiert ist.

anyHost Datacenter
Brunnackerstrasse 2
2563 Ipsach

by Troppus GmbH
T 032 512 14 90

Datacenter West
3186 Düdingen

Alle Daten liegen in der Schweiz, sicher und mit höchstem Datenschutz.
www.anyhost.ch