

Email: Email Weiterleitungen (Forwarding) werden wegen SPF abgelehnt.

Nach der automatischen, direkten Weiterleitung einer Email über einen Forwarder wird die Email mit folgender Fehlermeldung abgelehnt, welche an den Absender zurück gesendet wird:

^

^

This is the mail system at host server.forwarder.de.
I'm sorry to have to inform you that your message could not be delivered to one or more recipients. It's attached below.
For further assistance, please send mail to postmaster.
If you do so, please include this problem report. You can delete your own text from the attached returned message.
^ ^ ^ ^ ^ ^ ^ ^ ^ ^ ^ The mail system
: host mail.receiver.de[1.2.3.4] said: 550 5.7.1
^ ^ : Recipient address rejected: Please see

<http://www.openspf.net/Why?s=mfrom;id=sender%40sender@sender.de;ip=4.3.2.1;r=mail.receiver.de>
^ ^ (in reply to RCPT TO command)

*This is the mail system at host server.forwarder.de.
I'm sorry to have to inform you that your message could not be delivered to one or more recipients. It's attached below.
For further assistance, please send mail to postmaster.
If you do so, please include this problem report. You can delete your own text from the attached returned message.
^ ^ ^ ^ ^ ^ ^ ^ ^ ^ ^ The mail system
: host mail.receiver.de[1.2.3.4] said: 550 5.7.1 ^ ^ : Recipient address rejected: Please see
<http://www.openspf.net/Why?s=mfrom;id=sender%40sender@sender.de;ip=4.3.2.1;r=mail.receiver.de>
de
^ ^ ^ ^ (in reply to RCPT TO command)*

In diesem Beispiel wurde folgende Email versendet:

Absender: sender@sender.de

Email: Email Weiterleitungen (Forwarding) werden wegen SPF abgelehnt.

Empfänger: recipient@forwarder.de

Beim Anbieter von **forwarder.de** wurde eine Email-Weiterleitung an **recipient@receiver.de** eingerichtet.

Allgemeine Info zu SPF:

SPF steht für **Sender Policy Framework** und ist ein Standard zur Vermeidung von Spam- oder Virenmails mit gefälschtem Absender.

Das Framework ist im rfc4408 seit April 2006 definiert.

Viele sendende Emailprovider (hier: **sender.de**) haben einen strikten SPF Eintrag gesetzt der den Versand der eigenen Absenderadressen (**@sender.de**) nur von den eigenen Emailservern zulässt.

Der finale Emailserver (**@receiver.de**) lehnt die Email jedoch ab, da die Email nun vom unerlaubten Emailserver **forwarder.de** versucht wird, zu versenden.

Wer ist verantwortlich?:

Weiterleitungen werden grundsätzlich auf dem Empfangenden Emailsystem (**forwarder.de**) konfiguriert, welches für die korrekte Zustellung der Email verantwortlich ist.

Das sendende Emailsystem (**sender.de**), welches SPF einsetzt, kann eine Weiterleitung auf dem Zielsystem nicht berücksichtigen.

Lösung:

Damit der finale Emailserver (**receiver.de**) die Email trotz aktivem SPF-Record des Senders annehmen kann, muss **der weiterleitende Emailserver (forwarder.de) einen für sich gültigen Absender** (genauer: Envelope Sender) setzen.

Der Envelope Sender ist dabei nur für den Emailtransport relevant und wird dem Email-Empfänger nicht als Absender angezeigt (nur im Emailheader).

Diese Implementierung wird als **SRS (Sender Rewriting Scheme)** bezeichnet.

Wie ist SPF und SRS bei fastdirekt.de implementiert?

Wir haben auf unseren Emailservern SRS aktiviert, d.h. bei konfigurierten Email-Weiterleitungen auf unseren Systemen wird der "Envelope Sender" umgeschrieben, wodurch beim finalen Empfänger nicht zur Ablehnung der weitergeleiteten Email kommt.

SPF-Records werden bei uns zur Einstufung von Spam berücksichtigt; unsere Emailserver lehnen jedoch keine Email ab.

Somit können unsere Kunden auch Email problemlos empfangen, die zuvor von einem anderen Anbieter weitergeleitet wurden, der noch kein SRS implementiert hat.

*Email: Email Weiterleitungen (Forwarding) werden wegen SPF
abgelehnt.*

Quellen:

SPF Forwarding:Â http://www.openspf.org/Best_Practices/Forwarding

SRS:Â <http://www.openspf.org/SRS>

Eindeutige ID: #1020

Autor: FastDirekt.de

Letzte Änderung des Artikels: 2017-03-30 18:30