SPF-Record

Was bedeutet SPF?

SPF steht für „Sender Policy Framework“ und ist eine Technik zur Vermeidung von eingehenden Spam- oder Virenmails mit gefälschtem Absender.

Wie funktioniert SPF (einfach erklärt)?

Bei SPF wird die Zone einer Domain um einen speziellen TXT Eintrag erweitert. Mit Hilfe dieses TXT Eintrages, in dem erlaubte Versandmailserver definiert werden, wird verhindert, dass Unbefugte eine E-Mail-Manipulationen vornehmen können.

SPF-Record

v=spf1 mx include:spf1.x-mailer.de include:spf2.x-mailer.de -all

Sofern der empfangende Mailserver eine SPF Prüfung durchführt, wird in der DNS-Zone der absendenden Domain geprüft, ob der absendende Mailserver gem. Mailheader berechtigt ist, die Mail zu versenden. Fällt die Prüfung positiv aus, wird die Mail zugestellt. Fällt diese negativ aus, wird die Mail abgelehnt.

Populäre Freemailer (Google, T-Online, …) lehnen zunehmend eingehende Mails ohne SPF-Record ab. Weitere Informationen

SPF hilft Ihnen jedoch nicht, wenn Ihr Mailkonto gehackt und dann missbraucht wird. Hier hilft Ihnen nur ein sicheres Kennwort.

Was muss ich bei der Verwendung von externen Mailservern/Maildiensten beachten?

Erweitern Sie in diesem Fall den SPF-Record um die Domain oder IP. Bei Maildiensten (z.B. mailchimp.com/cleverreach.com/mailgun.com/…) findet man die entsprechenden Informationen in den FAQs. Außerdem wird i.d.R. bereits bei der Anmeldung des Dienstes auf die Einrichtung eines SPF-Records hingewiesen.

Was gibt es bei Weiterleitungen zu beachten?

Es ist wichtig zu beachten, dass es bei der Weiterleitung von E-Mails Probleme geben kann, wenn der Empfänger Mails auf SPF-Records prüft. Aus diesem Grund empfiehlt sich der Einsatz von SRS (Sender Rewriting Scheme), welches die E-Mail Adresse des Absenders so umschreibt, dass sie vom SPF-Record akzeptiert wird.

Seitens Plesk ist SRS von Haus aus aktiv, die Weiterleitung von E-Mails bei aktivem SPF-Record ist also möglich. Weitere Informationen finden Sie hier.

Auf unseren Systemen, welche das Server-Interface nutzen, ist die Nutzung von SRS leider nicht möglich. Sofern Sie dennoch SPF-Records auf diesen Systemen einsetzen möchten, sollten Sie beachten, dass die Weiterleitung von E-Mails gegebenenfalls Probleme verursacht, sofern der Empfänger die E-Mail auf SPF-Records prüft.

Wo kann ich den SPF einsehen und verändern?

Abhängig von dem von Ihnen genutzten System finden Sie unter den nachfolgenden genannten Menüpunkten die Möglichkeit, die DNS-Zone einzusehen und somit den SPF-Record anzupassen/anzulegen:

Server-Interface:
*/IHREDOMAIN/*server-interface/ oder IHRSERVER/server-interface/ -> Domainverwaltung -> DNS -> gewünschte Domains auswählen -> DNS Zone bearbeiten

Reseller-Interface:
https://ssl-entry.de/reseller/ -> Account editieren -> gewünschten Account suchen -> DNS

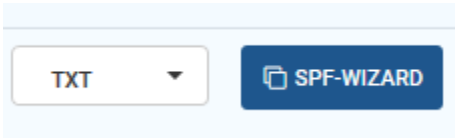
Plesk – Webhosting Tarif:
/IHRSERVER:8443 -> DNS -> Zone / Records bearbeiten

Plesk – Reseller Tarif:
/IHRSERVER:8443 -> Links im Menü „DNS“ -> Reiter „Domains“ -> Domain suchen -> Icon mit dem Bleistift anklicken -> DNS-Zone im NS-Entry bearbeiten -> Zone / Records bearbeiten

Plesk – Serverkunden:
IHRSERVER:8443 -> Links im Menü „DNS Admin“ -> Reiter „Domains“ -> Domain suchen -> Icon mit dem Bleistift anklicken -> DNS-Zone im NS-Entry bearbeiten -> Zone / Records bearbeiten
(Wichtig: Dieser Aufruf funktioniert nur, wenn unter „DNS Admin“ die API Daten von Ihrem Nameserver hinterlegt sind.)

Power-Nic (Domainrobot):
https://login.power-nic.de -> Zonenverwaltung -> Domain suchen -> Bearbeiten -> Zusätzliche Nameserver-Einträge

Bei TXT Records wird Ihnen der Button „SPF-WIZARD“ eingeblendet. Über den SPF-WIZARD können Sie vorhandene SPF-Records anpassen oder einfach neue SPF-Records erstellen.



SPF Wizard: [redacted]

Über das "Sender Policy Framework"-Protokoll (SPF) kann der Domaininhaber durch einen DNS-Eintrag definieren, über welche IP-Adressen E-Mails im Namen seiner Domain verschickt werden dürfen.

Bei vorhandenen SPF-Einträgen in der Zone einer Absender-Domain kann der Mailempfänger überprüfen ob eine Mail, die vorgibt von einer bestimmten Domain versandt worden zu sein, tatsächlich von dieser Domain stammt oder ob es sich ggf. um eine gefälschte Absender-Domain handelt.

A	Erfolgt der E-Mailversand ausschliesslich über die IP des Servers
✔ MX	Erfolgt der E-Mailversand auch über die IP des innerhalb des MX eingetragenen Servers
PTR	Möchten Sie jeden host zum Senden von Emails zulassen, der mit testcm-spf.gleich-testen.de endet?

A-Records

geben Sie hier weitere reguläre Hostnamen an, von denen aus testcm-spf.gleich-testen.de sendet.

MX-Records

geben Sie hier weitere Domainnamen für testcm-spf.gleich-testen.de an. Alle MX-Einträge dieser Domains werden zugelassen.

IPv4-Adressen

geben Sie hier weitere IP4-Adressen an, von denen aus testcm-spf.gleich-testen.de sendet.

Include

Wenn Sie Mails über einen Drittanbieter, z. B. web.de, im Namen von testcm-spf.gleich-testen.de versenden und dieser selbst einen SPF Eintrag verwendet, geben Sie die Domain (z.B. web.de) hier an.

spf1.x-mailer.de
spf2.x-mailer.de