Sicherheit

SPF Eintrag

Ein SPF (**Sender Policy Framework**) bezeichnet ein Verfahren, mit welchem verhindert werden soll, dass e-mails mit falscher e-mailadresse versenden können.
Beispiel: Ist SPF nicht aktiv kann eine e-mailnachricht mit Ihrer e-mailadresse versendet werden. Ist SPF aktiv, wird eine solche e-mailnachricht automatisch als Spam deklariert oder komplett abgelehnt.

Wie kann ich den SPF Eintrag setzen?

Ein SPF Eintrag ist ein einfacher TXT Eintrag welcher auf Ihrem DNS Server in der entsprechenden Zone gesetzt wird.

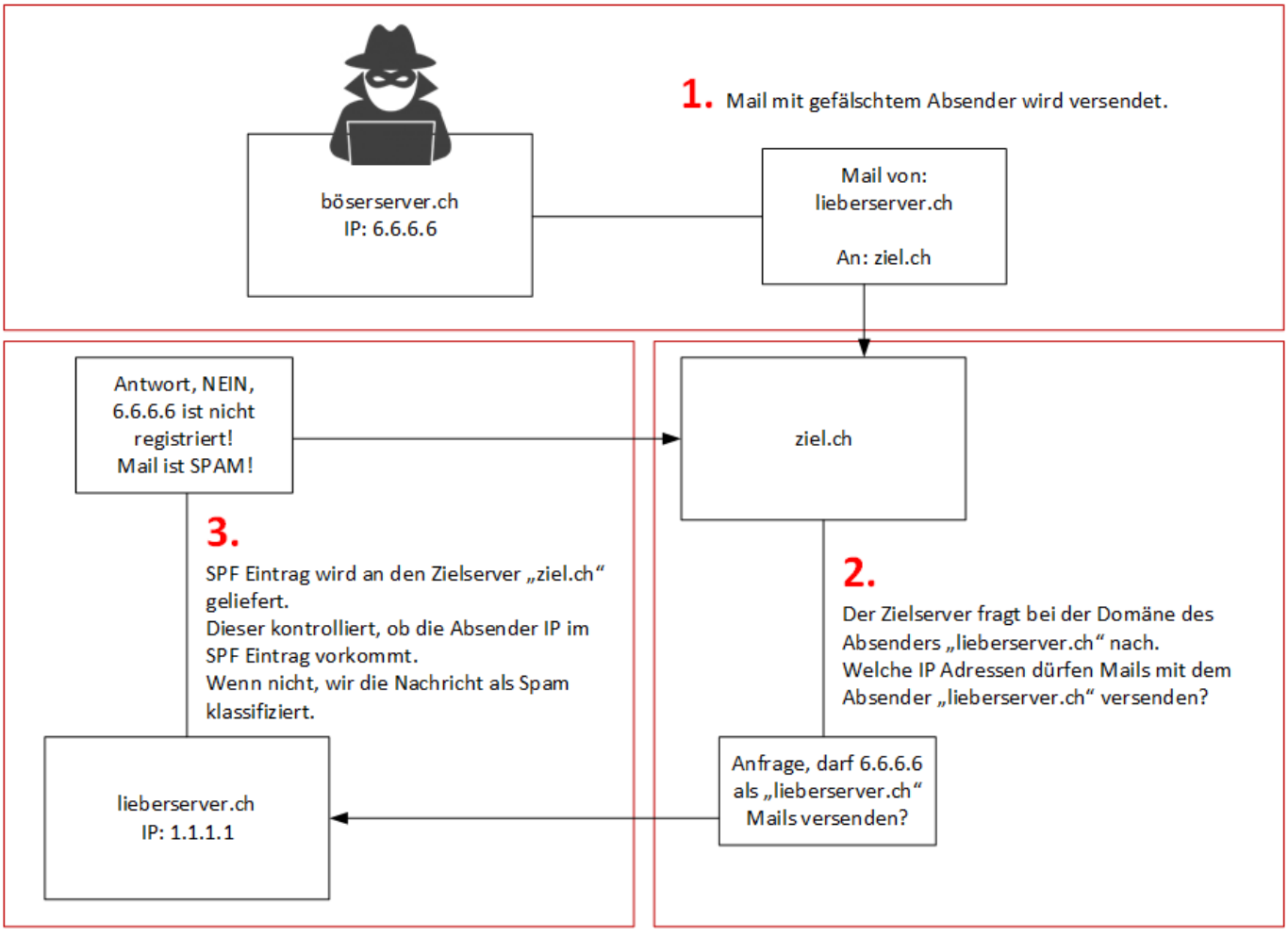
Der Eintrag sieht wie folgt aus:

ihredomain.com. IN TXT "v=spf1 a mx -all"

Der obige Eintrag erlaubt es von allen IP Adressen, welche in Ihrer DNS-Zone einen A oder einen MX Eintrag haben, e-mails zu versenden.

Natürlich gibt es heute für das Erstellen eines SPF Eintrages auch gute Helfer.
https://www.spf-record.com/generator
Falls Sie nicht genau wissen wie Sie Ihre DNS-Zone anpassen können, kontaktieren Sie Ihren IT Partner.

Wie funktioniert SPF?



Sicherheit

Was wenn ich kein SPF aktiviert habe?

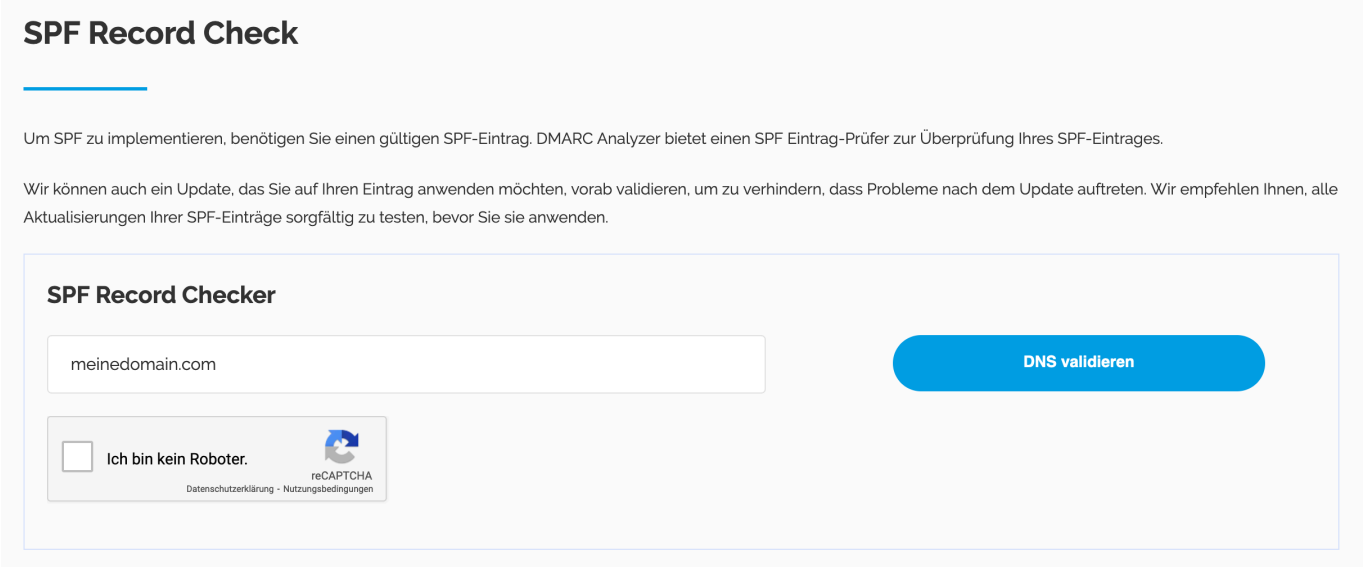
Falls Sie auf Ihrem DNS Server keinen SPF Eintrag gesetzt haben können Mailnachrichten mit Ihrem Absender versendet werden. Sofern ein SPF Eintrag nicht kontrolliert werden kann, könnte Ihr Mailprovider die gefälschte Nachricht als Legitim anschauen.

Betrüger nutzen diese Methode oft, um einfache Betrugsmails zu senden und so das Opfer dazu zu bewegen, Bitcoins an eine Adresse zu senden. Einige Beispiele dazu finden Sie nachstehend.

Wie prüfe ich meinen SPF Eintrag?

Ob Ihr Mailserver einen gültigen SPF Eintrag aufweist kann ganz einfach überprüft werden.
Öffnen Sie die Seite: https://www.dmarcanalyzer.com/de/spf-de/checker/

Geben Sie im Feld "Domain" den Domainnamen Ihrer e-mailadresse ein, das ist alles was nach dem @-Zeichen kommt.
Zum Beispiel: meineadresse@meinedomain.com => "meinedomain.com".
Klicken Sie auf DNS validieren und schauen Sie sich das Ergebnis an.



Falls nun steht "**Wir konnten keinen SPF Datensatz finden**", sollten Sie handeln und den Eintrag schnellstmöglich erstellen.

In allen anderen Fällen werden Sie über die Plausibilität oder allfällige Fehler im SPF-Eintrag hingewiesen.

Beispielnachrichten

Nachricht 1

Von: ihre@mailadresse.com
Datum: 20. November 2022 um 22:27:41 MEZ
An: ihre@mailadresse.com

Hallo
Wie Sie vielleicht bemerkt haben, habe ich Ihnen eine E-Mail von Ihrem E-Mail-Konto gesendet
Das bedeutet, dass ich vollen Zugriff auf Ihr Konto habe
Ich beobachte dich seit ein paar Monaten
Die Sache ist die, dass Sie sich über eine von Ihnen besuchte Website für Erwachsene mit einem Njrat infiziert haben
Wenn Sie das nicht wissen, lassen Sie es mich erklären
Der njrat gibt mir vollen Zugriff und Kontrolle über Ihr Gerät.

Das heißt, ich kann alles auf Ihrem Bildschirm sehen, die Kamera und das Mikrofon einschalten, aber Sie wissen es nicht
Ich habe auch Zugriff auf alle Ihre Kontakte und Ihre gesamte Korrespondenz.
Auf der linken Hälfte des Bildschirms habe ich ein Video gemacht, das zeigt, wie Sie sich zufriedengestellt haben, auf der rechten Hälfte sehen Sie das Video, das Sie sich angesehen haben.
Mit einem Mausklick kann ich dieses Video an alle Ihre E-Mails und Kontakte in sozialen Netzwerken senden
Ich kann auch den Zugriff auf alle Ihre Kommunikations- und Messaging-Programme sehen, die Sie verwenden.
Wenn Sie dies vermeiden möchten,
Überweisen Sie den Betrag von 1500 CHF an meine Bitcoin-Adresse ("schreiben Sie moonpay oder banxa oder gehen Sie zur Wechselstube, wenn Sie nicht wissen wie")

Meine Bitcoin-Adresse (BTC-Wallet): 1EiS5dgQFdRfwU9xSYP7GKMGq

Nach Zahlungseingang werde ich das Video löschen und Sie werden nichts mehr von mir hören
Ich gebe Ihnen 72 Stunden Zeit, um zu bezahlen
Vergiss nicht, dass ich dich sehen werde, wenn du die Nachricht öffnest, der Zähler startet
Wenn ich sehe, dass Sie diese Nachricht mit jemand anderem geteilt haben, wird das Video sofort gepostet

Nachricht 2

Hallo Sie!

Leider habe ich ein paar schlechte Nachrichten für Sie.
Vor einigen Monaten habe ich mir Zugang zu Ihren Computern verschafft, die Sie zum Surfen im Internet benutzen.
Daraufhin habe ich Ihre Internetaktivitäten zurückverfolgt.

Nachstehend finden Sie die Abfolge der vergangenen Ereignisse:
In der Vergangenheit habe ich mir von Hackern Zugang zu zahlreichen E-Mail-Konten verschafft (heutzutage ist das eine sehr einfache Aufgabe, die online erledigt werden kann).
Offensichtlich habe ich mich mühelos in Ihr E-Mail-Konto (ihre@mailadresse.com) eingeloggt.

Eine Woche später ist es mir gelungen, einen Trojaner auf den Betriebssystemen all Ihrer Geräte zu installieren, die für den E-Mail-Zugang verwendet werden.
Eigentlich war das ganz einfach (denn Sie haben auf die Links in den E-Mails im Posteingang geklickt).
Alle cleveren Dinge sind ganz einfach (^^)

Die Software von mir ermöglicht mir den Zugriff auf alle Bedienungselemente Ihrer Geräte, wie Videokamera, Mikrofon und Tastatur.
Ich habe es geschafft, alle Ihre persönlichen Daten sowie den Browserverlauf und Ihre Fotos auf meine Server herunterzuladen.
Ich kann auf alle Ihre Messenger sowie auf E-Mails, soziale Netzwerke, Kontaktlisten und sogar Chatverläufe zugreifen.
Mein Virus aktualisiert ständig seine Signaturen (da er treiberbasiert ist) und bleibt dadurch für Ihr Antivirusprogramm unsichtbar.

Jetzt sollten Sie bereits den Grund verstehen, warum ich bis zu diesem Moment unbemerkt blieb...

Beim Sammeln Ihrer Informationen habe ich herausgefunden, dass Sie auch ein großer Fan von Webseiten für Erwachsene sind.
Sie schauen sich gerne Pornoseiten an und sehen sich versaute Videos an und haben dabei jede Menge versauten Spaß.
Ich habe mehrere perverse Szenen von Ihnen aufgenommen und einige Videos montiert, in denen Sie beim leidenschaftlichen Masturbieren zum Orgasmus kommen.

Sicherheit

Wenn Sie immer noch an meinen ernsthaften Absichten zweifeln, ist es nur ein paar Mausklicks entfernt, Ihre Videos mit Ihren Freunden, Verwandten und sogar Kollegen zu teilen.
Es ist auch kein Problem für mich, diese Videos auch für die Öffentlichkeit zugänglich zu machen.
Ich denke, dass Sie das nicht wollen, denn Sie wissen, wie besonders die von Ihnen geschauten Videos sind (Sie sind sich dessen bewusst), und all das kann für Sie zu einer echten Katastrophe führen.

Lassen Sie uns das folgendermaßen lösen:
Alles, was Sie brauchen, ist eine Überweisung von 1800€ auf mein Konto (in Bitcoin, je nach dessen Wechselkurs während der Überweisung),
und nachdem die Transaktion erfolgreich war, werde ich das ganze perverse Zeug ohne Verzögerung löschen.
Danach können wir so tun, als ob wir uns nie zuvor getroffen hätten. Außerdem versichere ich Ihnen, dass die gesamte Schadsoftware von allen Ihren Geräten gelöscht wird. Seien Sie sicher, ich halte meine Versprechen.

Das ist ein ziemlich fairer Deal mit einem niedrigen Preis, bedenkt man, dass ich mir viel Mühe gegeben habe, Ihr Profil und Ihren Datenverkehr über einen langen Zeitraum hinweg zu überprüfen.
Wenn Sie nicht wissen, wie man Bitcoins kauft und verschickt - lässt sich leicht beheben, indem Sie alle entsprechenden Informationen online suchen.

Unten ist meine Bitcoin-Wallet: 1M4wy5VoXHxVE8cKy-------yhptPEEHP5

Sie haben nicht mehr als 48 Stunden Zeit, nachdem Sie diese E-Mail geöffnet haben (2 Tage, um genau zu sein).

Im Folgenden finden Sie eine Liste von Aktionen, die Sie nicht durchführen sollten:
*Versuchen Sie nicht, auf meine E-Mail zu antworten (die E-Mail in Ihrem Posteingang wurde von mir zusammen mit der Absenderadresse erstellt).
*Versuchen Sie nicht, die Polizei oder einen anderen Sicherheitsdienst anzurufen. Und denken Sie nicht einmal daran, dies Ihren Freunden mitzuteilen.
Sobald ich das herausfinde (Ich kann das ohne Zweifel mühelos tun, wenn man bedenkt, dass ich die volle Kontrolle über alle Ihre Systeme habe), wird das Video von Ihnen sofort öffentlich zugänglich sein.
*Versuchen Sie nicht, nach mir zu suchen - das ist völlig sinnlos. Alle Kryptowährungstransaktionen bleiben zu jeder Zeit anonym.
*Versuchen Sie nicht, das Betriebssystem auf Ihren Geräten neu zu installieren oder sie loszuwerden. Es ist auch sinnlos, weil alle Ihre Videos bereits auf entfernten Servern verfügbar sind.

Im Folgenden finden Sie eine Liste von Dingen, über die Sie sich keine Gedanken machen müssen:
*Dass ich das von Ihnen überwiesene Geld nicht erhalten werde.
- Keine Sorge, ich kann es auch nach erfolgreicher Transaktion noch zurückverfolgen, denn ich überwache weiterhin alle Ihre Aktivitäten (mein Trojanervirus enthält eine Fernsteuerungsoption, genau wie TeamViewer).
*Dass ich Ihre Videos auch nach Abschluss des Geldtransfers noch öffentlich zugänglich machen werde.
- Glauben Sie mir, es ist sinnlos, wenn ich Ihnen das Leben weiterhin schwer mache. Wenn ich das wirklich wollte, wäre es schon längst geschehen!

Alles wird auf der Grundlage der Fairness durchgeführt!

Bevor ich es vergesse...versuchen Sie in Zukunft, sich nicht mehr auf solche Situationen einzulassen!
Ein Rat von mir - ändern Sie regelmäßig alle Passwörter zu Ihren Konten.

Eindeutige ID: #1002

Sicherheit

Verfasser: Urs Kälin
Letzte Änderung: 2022-11-26 17:42