Secuenza

Anleitung zur Zustellbarkeit: SPF, DKIM und DMARC

Ob Ihre E-Mails im Posteingang ankommen, hängt von zwei Dingen ab: dass die Anbieter prüfen können, dass Sie es wirklich sind, und dass Ihr Postfach einen guten Ruf hat. Diese Anleitung erklärt die drei Einträge, die das belegen, wie Sie sie bei den gängigsten Anbietern einrichten und welche Gewohnheiten Ihren Ruf schützen.

Warum das wichtig ist

Gmail, Yahoo und Outlook.com verlangen von allen, die regelmäßig versenden, **SPF, DKIM und DMARC** für ihre Domain, eine Abmeldung mit einem Klick in jeder E-Mail und dass kaum jemand sie als Spam meldet. Ohne diese Einträge landen Ihre E-Mails meist im Spam oder kommen gar nicht erst an.

Secuenza versendet aus Ihrem eigenen Postfach, also signiert Ihr E-Mail-Anbieter jede E-Mail (oder eben nicht). Ihre Aufgabe ist es, im DNS Ihrer Domain die Daten zu veröffentlichen, die das bestätigen.

Bevor Sie anfangen: Wo ist Ihr DNS?

Das DNS Ihrer Domain wird dort verwaltet, wo Sie sie gekauft oder hingeleitet haben (beim Registrar, Ihrem Hosting, Cloudflare …) – nicht immer dort, wo Ihr Postfach liegt. Melden Sie sich in diesem Bereich an und suchen Sie die DNS-Zone: Dort tragen Sie die Einträge aus dieser Anleitung ein.

Eine DNS-Änderung ist nach einigen Minuten bis einigen Stunden sichtbar. Gehen Sie danach in Secuenza wieder zu **Prüfungen**.

SPF: Wer für Ihre Domain versenden darf

SPF ist ein **TXT**-Eintrag in der Wurzel der Domain, der mit `v=spf1` beginnt, angibt, welche Server in ihrem Namen versenden dürfen, und mit `~all` (alle anderen sind verdächtig) oder `-all` (alle anderen werden abgelehnt) endet.

Anbieter	Was Ihr SPF enthalten muss
Microsoft 365	`include:spf.protection.outlook.com`
Google Workspace	`include:_spf.google.com`
IONOS	`include:_spf-eu.ionos.com`
OVHcloud	`include:mx.ovh.com`
Hostinger	`include:_spf.mail.hostinger.com`
Aruba	`include:_spf.aruba.it`
Zoho Mail (EU)	`include:zoho.eu`

Zum Beispiel mit Microsoft 365: `v=spf1 include:spf.protection.outlook.com ~all`.

Drei Regeln, die Sie kennen sollten:

- **Es darf nur einen SPF geben.** Wenn Sie schon einen haben (für Ihre Website, Ihr Rechnungsprogramm), fügen Sie keinen zweiten hinzu: Fassen Sie die `include` im selben Eintrag zusammen. Bei zwei Einträgen gilt keiner.
- **Höchstens 10 Abfragen.** Jedes `include` zählt, auch die darin enthaltenen. Wer darüber liegt, gilt bei den Servern als fehlerhaft.
- **Niemals** `+all`: Damit dürfte jeder in Ihrem Namen versenden.

Wenn Ihr Postfach eine Gmail- oder Outlook.com-Adresse ist (keine Ihrer Domain), müssen Sie nichts einrichten: SPF und Signatur kommen vom Anbieter. Diese Postfächer haben allerdings niedrige Limits, und Secuenza hält sie ein.

DKIM: die Signatur Ihrer E-Mails

Mit DKIM signiert Ihr Anbieter jede E-Mail mit einem privaten Schlüssel, und Sie veröffentlichen den öffentlichen Schlüssel im DNS, unter einem Namen wie `selektor._domainkey.ihredomain.de`. So weiß der Empfänger, dass die E-Mail unterwegs nicht verändert wurde und wirklich von Ihrer Domain stammt.

- **Microsoft 365:** Wählen Sie im Microsoft-Defender-Portal in den Einstellungen zur E-Mail-Authentifizierung (DKIM) Ihre Domain. Sie erhalten zwei **CNAME**-Einträge (`selector1` und `selector2`): Tragen Sie sie im DNS ein und aktivieren Sie die Signatur anschließend im Portal.

- **Google Workspace:** Erzeugen Sie in der Admin-Konsole unter Gmail → E-Mails authentifizieren einen Eintrag mit **2048 Bit**, tragen Sie ihn als **TXT** unter `google._domainkey` ein und klicken Sie auf „Authentifizierung starten“.
- **IONOS, OVHcloud, Hostinger, Aruba, Zoho und die meisten Hostings:** Suchen Sie im E-Mail-Bereich nach „DKIM“. Viele aktivieren es selbst, wenn auch das DNS bei ihnen liegt; sonst erhalten Sie den Eintrag zum Kopieren.

Secuenza sucht die Signatur unter den üblichen Namen jedes Anbieters. Hat Ihre einen anderen Namen, findet der **echte Versandtest** (Pro) sie. Verwenden Sie Schlüssel mit **2048 Bit**: Solche mit 1024 Bit gelten bereits als schwach.

DMARC: was mit dem geschieht, was nicht besteht

DMARC ist ein **TXT**-Eintrag unter `_dmarc.ihredomain.de`, der den Anbietern sagt, was sie mit einer E-Mail tun sollen, die angeblich von Ihrer Domain kommt, aber weder SPF noch DKIM besteht, und wohin sie Ihnen Berichte schicken sollen. Damit er greift, muss die Domain des Absenders mit der des SPF oder der DKIM-Signatur übereinstimmen (das „Alignment“).

Beginnen Sie mit Beobachten:

```
v=DMARC1; p=none; rua=mailto:dmarc@ihredomain.de
```

1. **Zwei bis vier Wochen mit `p=none`**: Es ändert sich nichts, aber Sie erhalten Berichte darüber, wer für Ihre Domain versendet. Prüfen Sie, dass alles Legitime signiert hinausgeht (Ihr Postfach, Ihre Website, Ihre Rechnungen).
2. **Wechseln Sie zu `p=quarantine`**: Was nicht besteht, landet im Spam.
3. **Und dann zu `p=reject`**: Was nicht besteht, wird abgelehnt. Das schützt Ihre Domain am besten vor allen, die sich als Sie ausgeben wollen.

Die Berichte kommen als XML. Es gibt kostenlose Dienste, die sie zusammenfassen; es genügt, ab und zu hineinzuschauen.

Mit Secuenza prüfen

In den Details jedes Postfachs kontrolliert **Prüfungen** SPF, DKIM und DMARC, außerdem den E-Mail-Empfang (MX), den Reverse-Namen des Servers, MTA-STS, BIMI und die Verschlüsselung. Jede Prüfung erscheint grün, gelb oder rot, mit dem, was wo einzutragen ist. Wenn Sie schon einen SPF haben, schlägt Secuenza den vollständigen Eintrag mit dem Fehlenden vor.

Mit **Pro** außerdem:

- **Echter Versandtest:** Secuenza schickt eine echte E-Mail aus Ihrem Postfach und sagt Ihnen, was der empfangende Server sieht: Signatur, SPF, DMARC-Alignment, Verschlüsselung und Spam-Prüfung.
- **Blocklisten:** Es prüft, ob Ihr Server oder Ihre Domain auf den Listen stehen, die Filter verwenden.

Und der Bereich **Sicherheit** bündelt, was die Bremse gestoppt hat, Ihre Zahlen der letzten 30 Tage im Vergleich zu ihren Grenzwerten und den Zustand jedes Postfachs: Versandsicherheit erklärt es.

Der Ruf: worauf Filter achten

Sind die Einträge gesetzt, entscheidet Ihr Verhalten:

- **Fangen Sie langsam an.** Ein neues Postfach oder eine neue Domain, die plötzlich Hunderte E-Mails verschickt, wirkt wie Spam. Die Aufwärmphase von Secuenza erhöht das Limit Tag für Tag.
- **Halten Sie die Limits ein.** Für jeden Anbieter verwendet Secuenza ein vorsichtiges Tages- und Stundenlimit unter dessen Maximum und verteilt den Versand auf Ihre Zeiten.
- **Machen Sie die Abmeldung leicht.** Jede E-Mail enthält den Abmeldelink und den Header, mit dem Gmail und Outlook ihre Schaltfläche „Abbestellen“ anzeigen. Abmeldungen gelten sofort.
- **Saubere Listen.** Kaufen Sie niemals Listen. Unzustellbare E-Mails und inaktive Kontakte werden aussortiert, und die Sicherheitsbremse pausiert eine Kampagne, wenn es zu viele unzustellbare E-Mails oder Abmeldungen gibt, und stoppt den Versand an einen Anbieter, bei dem niemand Ihre E-Mails öffnet.
- **Wenig Beschwerden.** Wenn mehr als 2 oder 3 von tausend Personen Ihre E-Mails als Spam melden, werden Sie von den Filtern abgestraft. Schreiben Sie nur denen, die Ihre E-Mails erwarten.
- **E-Mails wie von einem Menschen.** Klarer Text, wenige Links, keine Linkverkürzer, Bilder mit Text drumherum. Laden Sie Bilder im Editor hoch: Bilder aus Drive oder Dropbox oder direkt in die E-Mail eingefügte landen oft im Spam. Die Spam-Prüfung warnt Sie vor dem, was meist negativ zählt.
- **Sorgen Sie für Antworten.** Eine Antwort ist das beste Zeichen, dass Ihre E-Mail willkommen ist. Schreiben Sie so, dass man Ihnen antwortet.

Wenn Ihre E-Mails im Spam landen

1. Öffnen Sie **Prüfungen**: Sind die drei Einträge grün?

2. Machen Sie mit Pro den **echten Versandtest** und sehen Sie nach, was beim empfangenden Server scheitert.
3. Prüfen Sie die **Spam-Prüfung** der E-Mails der Kampagne.
4. Sehen Sie unter **Sicherheit** nach, ob die Bremse einen Anbieter gestoppt hat, und unter **Ergebnisse** nach Abmeldungen und unzustellbaren E-Mails: Wenn sie steigen, halten Sie an und bereinigen Sie die Liste.
5. Senken Sie das Limit für ein paar Tage und erhöhen Sie es dann langsam wieder.