DMARC: wer in Ihrem Namen sendet (Pro)

> **Pro-Version.** Diese Funktion gehört zur Pro-Version von Mail Log. Was die Free-Version kann, steht unter *Free-Version und Pro-Version*.

Jeden Tag schicken die großen E-Mail-Anbieter Berichte darüber, wer in Ihrem Namen gesendet hat und ob diese Post sich als Ihre ausweisen konnte. Diese *DMARC-Berichte* kommen als gepacktes XML in einem Postfach an — und werden deshalb in der Praxis nie gelesen. Mail Log sammelt sie ein, packt sie aus und beantwortet daraus eine Frage: **Ist das noch unser Versand?**

Was ein Bericht beantwortet — und was nicht

Ein Bericht sagt: „Von dieser IP-Adresse kamen im Laufe des Tages 42 Nachrichten mit Ihrer Domain im Absender. 40 davon konnten sich ausweisen, 2 nicht.“ Er sagt *nicht*, ob die Post gelesen wurde, und er nennt keine Empfänger und keine Betreffs — ein Aggregatbericht enthält Zahlen, keine Nachrichten.

„Sich ausweisen“ heißt dabei: Die Nachricht trug eine gültige DKIM-Unterschrift Ihrer Domain *oder* kam von einem Server, den Ihr SPF-Eintrag erlaubt. Eines von beiden genügt. Deshalb ist eine weitergeleitete Nachricht kein Problem: Die Weiterleitung bricht SPF, die Unterschrift bleibt heil.

Einrichten: drei Schritte

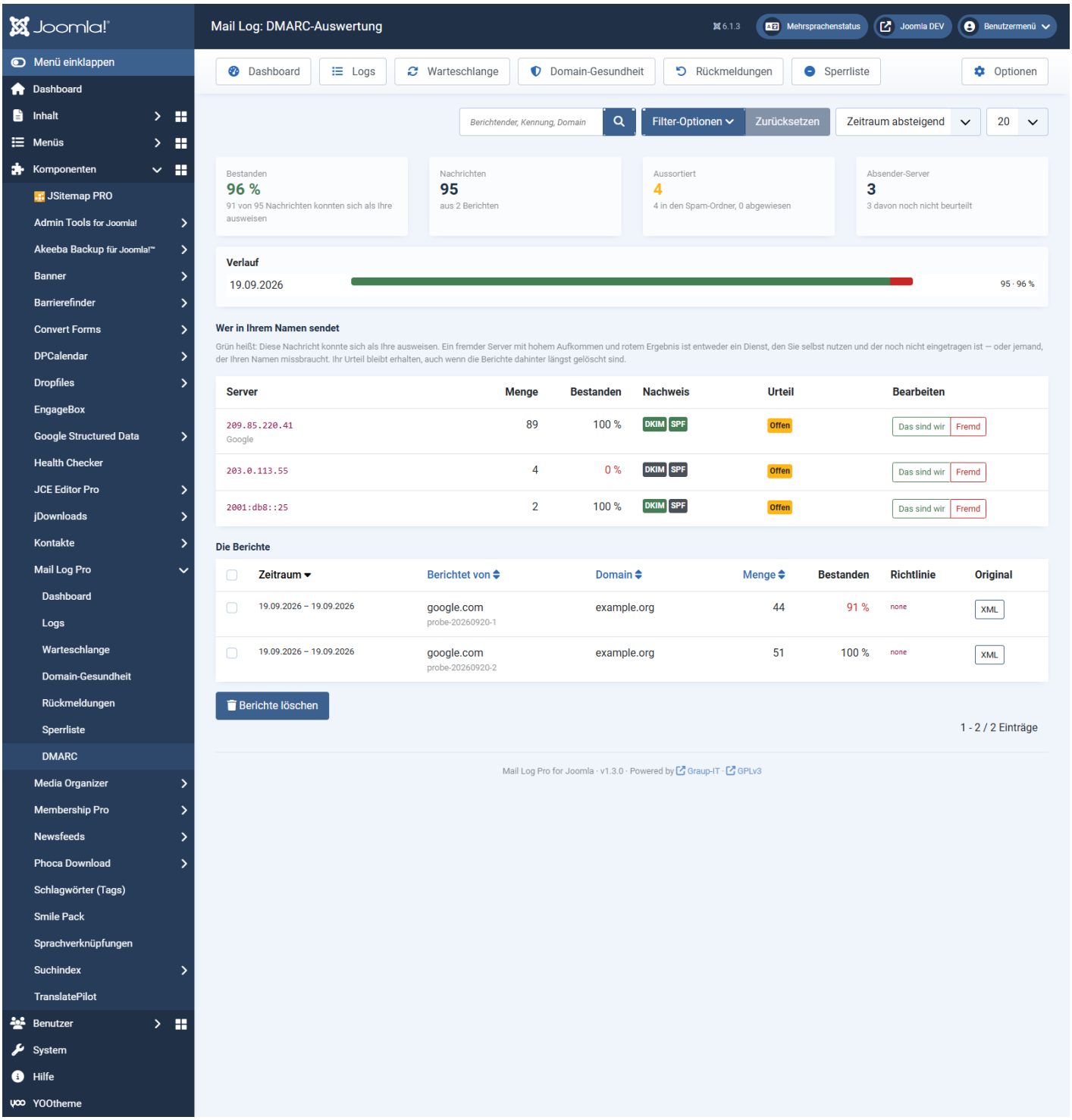
1. **Den Rückkanal einrichten.** Die Berichte kommen in *dasselbe* Postfach wie die Unzustellbarkeitsmeldungen. Wie Sie es hinterlegen, steht im Kapitel *Rückkanal*. Ohne den Postfachabruf kommt nichts an.
2. **Die Berichtsadresse im DNS eintragen.** In Ihrem DMARC-Eintrag gibt es dafür den Teil `rua=mailto:…`. Hier bestimmen *Sie*, wohin die Berichte gehen — anders als bei den Unzustellbarkeitsmeldungen, deren Adresse der Versand vorgibt. Tragen Sie die Adresse des Postfachs ein, das Mail Log abruft. Den fertigen Eintrag zeigt Ihnen die *Domain-*

Gesundheit.

3. **Die Auswertung einschalten.** *Optionen → Rückkanal → DMARC-Berichte → Berichte auswerten*.

> **Geduld beim ersten Mal.** Die Anbieter senden einmal täglich und beziehen sich auf den Vortag. Nach dem Veröffentlichen des DNS-Eintrags dauert es also bis zu zwei Tage, bis der erste Bericht eintrifft — und nur, wenn in dieser Zeit überhaupt Post von Ihrer Domain verschickt wurde.

Die Seite *DMARC*



Die Seite liest sich von oben nach unten als eine Antwort in drei Stufen.

Die Zahlen

Kennzahl	Was sie sagt
Bestanden	Der Anteil der Nachrichten, die sich ausweisen konnten. Das ist die eine Zahl, die man im Blick behält.

Kennzahl	Was sie sagt
Nachrichten	Wie viele Nachrichten die Berichte insgesamt beschreiben — nicht, wie viele Berichte eingegangen sind.
Aussortiert	Was der Empfänger in den Spam-Ordner gelegt oder abgewiesen hat. Steht hier eine Zahl über Null, hat Ihre Richtlinie bereits gewirkt.
Absender-Server	Wie viele verschiedene Server im Zeitraum in Ihrem Namen gesendet haben, und wie viele davon noch unbeurteilt sind.

Unter welchem Wert die Quote als auffällig gilt, stellen Sie in den Optionen ein (*Warnen unter … Prozent bestanden*, ab Werk 95). Hundert Prozent sind kein sinnvoller Wert: Eine einzige weitergeleitete Nachricht reißt sie.

Wer in Ihrem Namen sendet

Die zweite Liste ist die eigentliche Arbeit. Sie zeigt jeden Server, der Post mit Ihrer Domain verschickt hat, mit Menge, bestandenem Anteil und — soweit auflösbar — seinem Namen. Bekannte Versanddienste erkennt Mail Log und beschriftet sie.

Jede Zeile bekommt von Ihnen ein Urteil:

- **Das sind wir** — ein Server, der in Ihrem Auftrag sendet: Ihr Hoster, Ihr Newsletter-Dienst, Ihr Ticketsystem.
- **Fremd** — jemand, der Ihren Namen benutzt, ohne dazu berechtigt zu sein.
- **Zurücknehmen** — wieder offen, wenn Sie sich geirrt haben.

Das Urteil gehört Ihnen und bleibt erhalten, auch wenn die Berichte, aus denen die Adresse stammt, längst der Aufbewahrung zum Opfer gefallen sind.

> **Ein eigener Dienst mit roter Quote ist der häufigste Fund.** Er bedeutet fast nie einen Angriff, sondern einen fehlenden Eintrag: Der Newsletter-Dienst steht nicht in Ihrem SPF-Eintrag, oder sein DKIM-Schlüssel ist nicht veröffentlicht. Beides zeigt Ihnen die *Domain-Gesundheit* mit dem fertigen Eintrag zum Kopieren.

Die Berichte

Zuletzt die Liste der eingegangenen Berichte: Zeitraum, Berichtender, Domain, Menge, Quote und die veröffentlichte Richtlinie. Über *XML* laden Sie das Originaldokument herunter — für den Fall, dass eine Zahl seltsam aussieht und jemand nachsehen will, was der Anbieter wirklich geschrieben hat.

Was Mail Log mit den Berichten sonst noch tut

- **Selektoren übernehmen.** Ein Bericht nennt, mit welchem DKIM-Selektor Ihr Versand unterschreibt. Mail Log merkt sich die nachweislich funktionierenden und prüft sie in der Domain-Gesundheit von selbst mit — Sie müssen sie nicht eintragen.
- **Im regelmäßigen Bericht.** Quote und die Zahl der unbeurteilten Quellen stehen im Wochen- beziehungsweise Monatsbericht, wenn Sie ihn eingeschaltet haben.
- **Im Dashboard.** Ein Streifen mit Quote und offenen Quellen.

Aufbewahrung

Zwei Fristen, weil es zwei verschiedene Dinge sind: Die ausgewerteten *Zahlen* bleiben ab Werk ein Jahr — so lässt sich die Frage „war das im letzten Sommer schon so?“ beantworten. Das *Originaldokument* bleibt drei Monate; es wird selten gebraucht und nur kurz. Danach bleibt der Bericht in der Liste stehen, nur ohne Anhang. Aufgeräumt wird von der Wartungsroutine *Alte Log-Einträge aufräumen*, die ohnehin läuft.

Wenn nichts ankommt

Die Seite sagt Ihnen, woran es liegt — sie unterscheidet vier Fälle: die Auswertung ist aus, der Postfachabruf ist aus, es gibt keine geplante Aufgabe, oder der Aufgabenplaner der Website läuft überhaupt nicht. Steht dort kein Hinweis und die Seite ist trotzdem leer, dann prüfen Sie den `rua=`-Teil Ihres DMARC-Eintrags: Zeigt er wirklich auf das Postfach, das Mail Log abruft?

> **Berichte fremder Domains.** Mail Log legt jeden Bericht ab, den es findet, und nennt in der Liste die Domain, um die es geht. Wenn dort eine Domain auftaucht, die Ihnen nicht gehört, hat jemand Ihre Adresse als Berichtsadresse eingetragen — ärgerlich, aber harmlos. Der Domain-Filter blendet sie aus.

English version

Revision #3
Created 2026-09-24 15:31:09 UTC by Norbert Graup
Updated 2026-09-24 17:01:15 UTC by Norbert Graup