

LEITFADEN · TOMORIS TOOLBOX

E-Mail-Sicherheit: SPF, DKIM und DMARC in fünf Schritten

Einführungsplan von der Bestandsaufnahme bis p=reject, nach RFC 7208, RFC 6376 und dem DMARC-Standard RFC 9989

STAND

22.10.2026

UMFANG

PDF, 7 Seiten

ONLINE

tomoris.com/downloads/e-mail-sicherheit-spf-dkim-dmarc

AUF EINEN BLICK

5

Schritte von der Bestandsaufnahme bis p=reject

10

DNS-Abfragen höchstens für SPF (RFC 7208)

2048 Bit

DKIM-Schlüssel empfohlen (RFC 8301)

1 Monat

mindestens je DMARC-Stufe (RFC 9989)

FÜR WEN

- IT-Verantwortliche und Administratoren von Mailservern und Microsoft 365
- Unternehmen, deren Domain für Phishing missbraucht wird oder werden könnte
- Wer Newsletter, Rechnungen oder Tickets über externe Dienste versendet

WORUM ES GEHT

Mit SPF, DKIM und DMARC belegen Sie, dass E-Mails mit Ihrer Domain wirklich von Ihnen stammen, und sagen Empfängern, wie sie mit Fälschungen umgehen sollen. Dieser Plan führt in fünf Schritten von der Bestandsaufnahme bis zur Richtlinie `p=reject`, mit Beispiel-Einträgen für das DNS und den Stolpersteinen aus den Standards. Er berücksichtigt den im Mai 2026 veröffentlichten DMARC-Standard RFC 9989.

Die DNS-Einträge sind Beispiele mit reservierten Beispieldomains. Übernehmen Sie Werte erst nach der Bestandsaufnahme: Eine zu früh gesetzte Richtlinie `p=reject` kann dazu führen, dass legitime E-Mails abgewiesen werden.

INHALT

01	Wer was prüft	2
02	Schritt 1: Alle Absender erfassen	3
03	Schritt 2: SPF veröffentlichen	4
04	Schritt 3: DKIM für jeden Absender	4
05	Schritt 4: DMARC im Beobachtungsmodus	5
06	Schritt 5: Über quarantine zu reject	5
07	Auf einen Blick	6
08	Quellen	7

01 —

Wer was prüft

SPF, DKIM und DMARC in einer Tabelle: was geprüft wird, wo der Eintrag steht, welcher Standard gilt.

Die drei Verfahren im Überblick

VERFAHREN	WAS ES PRÜFT	DNS-EINTRAG	STANDARD
SPF	ob der sendende Server für die Domain im Envelope-Absender (MAIL FROM) bzw. im HELO senden darf, nicht die sichtbare Absenderadresse	TXT an der Domain, beginnt mit v=spf1	RFC 7208
DKIM	ob die Nachricht unverändert ist und von der signierenden Domain (d=) stammt	TXT unter <selector>._domainkey.<domain>	RFC 6376, aktualisiert durch RFC 8301
DMARC	ob die sichtbare Absenderdomain (From) zu einer per SPF oder DKIM bestätigten Domain passt (Alignment); dazu Richtlinie und Berichte	TXT unter _dmarc.<domain> , beginnt mit v=DMARC1	RFC 9989 (ersetzt RFC 7489), Berichte RFC 9990

SPF allein sagt nichts über die sichtbare Absenderadresse (RFC 7208, Abschnitt 11.2). Erst DMARC verknüpft sie: Eine Nachricht besteht DMARC, wenn mindestens eine per SPF oder DKIM bestätigte Domain zur Absenderdomain passt (RFC 9989, Abschnitt 5.3.5).

02 —

Schritt 1: Alle Absender erfassen

Jeder Dienst, der mit Ihrer Domain sendet, braucht passendes SPF oder DKIM, sonst scheitert er später an DMARC.

Erfassen Sie jeden Dienst, der E-Mails mit Ihrer Domain als Absender verschickt. Jeder legitime Absender braucht später ein beständenes SPF oder DKIM mit passender Domain; Lücken müssen geschlossen sein, bevor Sie eine strenge Richtlinie veröffentlichen (RFC 9989, Abschnitt 5.1.6).

- ☐ Eigener Mailserver oder Microsoft 365 bzw. Exchange Online
- ☐ Newsletter- und Marketingdienste
- ☐ CRM, Ticketsystem, Webshop und Buchhaltung (Rechnungsversand)
- ☐ Geräte und Anwendungen mit SMTP-Versand, etwa Scanner, Monitoring und Webformulare
- ☐ Dienstleister, die in Ihrem Namen senden
- ☐ Domains und Subdomains, die gar keine E-Mails versenden

03 —

Schritt 2: SPF veröffentlichen

Ein Eintrag pro Domain, höchstens zehn DNS-Abfragen, am Ende -all oder ~all.

DNS: SPF

```
; Microsoft 365 und ein eigener Server (192.0.2.25 ist eine Beispieladresse)
example.com.      IN TXT "v=spf1 ip4:192.0.2.25 include:spf.protection.outlook.com -all"

; Name, unter dem keine E-Mails versendet werden
www.example.com.  IN TXT "v=spf1 -all"
```

- Pro Domain genau ein SPF-Eintrag: Mehrere Einträge mit **v=spf1** ergeben einen permanenten Fehler (permerror, RFC 7208, Abschnitt 4.5).
- Höchstens 10 DNS-Abfragen durch **include**, **a**, **mx**, **ptr**, **exists** und **redirect** während der ganzen Prüfung, sonst permerror (Abschnitt 4.6.4). Die Einträge eingebundener Dienstleister zählen mit.
- **ptr** nicht verwenden (Abschnitt 5.5).
- **-all** (fail) erklärt nicht genannte Server ausdrücklich für unberechtigt, **~all** (softfail) ist nur eine schwache Aussage; allein wegen softfail sollen Empfänger nicht ablehnen (Abschnitte 2.6.4, 2.6.5 und 8.5).
- Namen ohne E-Mail-Versand veröffentlichen **v=spf1 -all** (Abschnitt 10.1.2).
- Ein TXT-String fasst höchstens 255 Zeichen. Längere Einträge werden auf mehrere Strings verteilt, die der Empfänger ohne Leerzeichen zusammensetzt (Abschnitt 3.3).

04 —

Schritt 3: DKIM für jeden Absender

Signieren mit rsa-sha256 und 2048-Bit-Schlüssel; der öffentliche Schlüssel steht im DNS unter dem Selektor.

Jeder Absender signiert mit einem eigenen Schlüssel. Den öffentlichen Schlüssel veröffentlichen Sie als TXT-Eintrag unter **<selector>._domainkey.<domain>**; Selektor (s=) und Domain (d=) stehen in der Signatur jeder Nachricht (RFC 6376, Abschnitte 3.5 und 3.6.2.1).

DNS: DKIM (Schlüssel gekürzt)

```
mail2026._domainkey.example.com.  IN TXT "v=DKIM1; k=rsa; p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA..."
```

- Signieren nur mit **rsa-sha256**; **rsa-sha1** darf weder zum Signieren noch zum Prüfen verwendet werden (RFC 8301, Abschnitt 3.1).
- Schlüssel mit mindestens 1024 Bit, empfohlen sind 2048 Bit (RFC 8301, Abschnitt 3.2).
- Microsoft 365: DKIM wird über zwei CNAME-Einträge **selector1._domainkey** und **selector2._domainkey** eingerichtet; die genauen Ziele zeigt **Get-DkimSigningConfig**. Beim Anlegen per PowerShell sind 1024 Bit voreingestellt; **Rotate-DkimSigningConfig -KeySize 2048** stellt auf 2048 Bit um.

- DKIM-Signaturen überstehen Weiterleitungen meist, SPF nicht. Wer `p=reject` veröffentlicht, darf sich deshalb nicht allein auf SPF verlassen und muss gültig mit DKIM signieren (RFC 9989, Abschnitt 7.4).

05

Schritt 4: DMARC im Beobachtungsmodus

`p=none` mit Berichtsadresse veröffentlichen, Berichte maschinell auswerten, Lücken schließen.

DNS: DMARC im Beobachtungsmodus

```
_dmarc.example.com. IN TXT "v=DMARC1; p=none; rua=mailto:dmarc-berichte@example.com"
```

- `p=none` äußert keine Präferenz für den Umgang mit Fehlschlägen (Monitoring Mode). Mit `rua` erhalten Sie aggregierte Berichte über alle Server, die mit Ihrer Domain senden (RFC 9989, Abschnitte 5.1.4 und 5.1.5).
- Die Berichte sind für die maschinelle Auswertung gedacht; nutzen Sie ein Auswertungswerkzeug oder einen Dienst (Abschnitt 5.1.5).
- Liegt das Berichtspostfach in einer fremden Domain, muss diese zustimmen, zum Beispiel mit einem TXT-Eintrag `example.com._report._dmarc.example.net` mit dem Inhalt `v=DMARC1` (RFC 9990).
- Fehlerberichte (`ruf`) enthalten Inhalte einzelner Nachrichten; die meisten Empfänger versenden sie aus Datenschutzgründen nicht (RFC 9989, Abschnitt 10.2). Aggregierte Berichte bleiben das empfohlene Mittel (RFC 9991).
- Jeder legitime Absender ohne passendes SPF oder DKIM wird nachgebessert, bevor eine strenge Richtlinie gilt (RFC 9989, Abschnitt 5.1.6).

06

Schritt 5: Über quarantine zu reject

Mindestens einen Monat `p=none`, ebenso lange `p=quarantine`, dann `p=reject`, mit Blick auf Mailinglisten.

Stufen bis `p=reject` (RFC 9989, Abschnitt 7.4)



p=none
Beobachten

`v=DMARC1; p=none; rua=mailto:...` –
Mindestens einen Monat.



p=quarantine
Quarantäne

`v=DMARC1; p=quarantine;`
`rua=mailto:...` – Ebenso lange;
Ergebnisse mit der Beobachtungsphase
vergleichen.



p=reject
Ablehnen

`v=DMARC1; p=reject; rua=mailto:...`
– Dauerhaft, wenn alle legitimen
Absender bestehen.

- `t=y` kennzeichnet eine Richtlinie im Test: Empfänger wenden eine Stufe weniger an, bei `p=reject` also nur quarantine (RFC 9989, Tag `t`). Den früheren Tag `pct` gibt es seit RFC 9989 nicht mehr; ältere Anleitungen, auch von Microsoft, nennen ihn noch.

- Subdomains: **sp** gilt für bestehende Subdomains, **np** für nicht existierende; fehlen beide, gilt **p** (RFC 9989, Tags **sp** und **np**).
- Mailinglisten: Domains, deren Nutzer an Mailinglisten im Internet schreiben, sollen laut RFC 9989 kein **p=reject** veröffentlichen; wer es trotzdem tut, soll die Nutzer darauf hinweisen, dass die Teilnahme an Mailinglisten beeinträchtigt sein kann (Abschnitt 7.4).

DNS: Domain ganz ohne E-Mail-Verkehr

```
parked.example.com.      IN TXT "v=spf1 -all"
_dmarc.parked.example.com. IN TXT "v=DMARC1; p=reject;"
parked.example.com.      IN MX 0 .
```

Der Null-MX-Eintrag **MX 0 .** sagt, dass die Domain keine E-Mails annimmt; daneben darf es keinen anderen MX-Eintrag geben, und Domains, die als Absender genutzt werden, sollen ihn nicht veröffentlichen (RFC 7505). Für ungenutzte Domains empfiehlt Microsoft DMARC-Einträge, nach denen nie E-Mails von ihnen kommen dürfen, und keine DKIM-Einträge.

07 —

Auf einen Blick

Die sieben Punkte zum Abhaken, vom Absenderverzeichnis bis zur abgesicherten Zweitdomain.

- ☐ Alle Absender sind erfasst, auch externe Dienste und Geräte.
- ☐ Genau ein SPF-Eintrag, höchstens 10 DNS-Abfragen, Abschluss mit **-all** oder **~all**.
- ☐ DKIM für jeden Absender mit **rsa-sha256** und 2048-Bit-Schlüssel.
- ☐ DMARC mit **p=none** und **rua**; die Berichte werden ausgewertet.
- ☐ Alle legitimen Absender bestehen DMARC mit passender Domain.
- ☐ **p=quarantine**, dann **p=reject**; Mailinglisten sind berücksichtigt.
- ☐ Domains ohne E-Mail-Verkehr sind mit SPF, DMARC und Null-MX abgesichert.

NÄCHSTER SCHRITT

Selbst prüfen oder gemeinsam umsetzen

KOSTENLOS PRÜFEN

E-Mail-Sicherheits-Check

tomoris.com/tools/email-security-check

DNS-Sicherheits-Check

tomoris.com/tools/dns-security-check

UMSETZUNG BESPRECHEN

Kontakt aufnehmen

tomoris.com/contact

contact@tomoris.com

08 —

Quellen

Alle Aussagen sind belegt. Gesetzestexte gelten in der jeweils geltenden Fassung.

- 1 **RFC 7208: Sender Policy Framework (SPF)**
Abschnitte 2.6, 3.3, 4.5, 4.6.4, 5.5, 8.5, 10.1.2, 11.2
www.rfc-editor.org/rfc/rfc7208
- 2 **RFC 6376: DomainKeys Identified Mail (DKIM) Signatures**
Abschnitte 3.5, 3.6.1, 3.6.2.1
www.rfc-editor.org/rfc/rfc6376
- 3 **RFC 8301: Cryptographic Algorithm and Key Usage Update to DKIM**
Abschnitte 3.1 und 3.2
www.rfc-editor.org/rfc/rfc8301
- 4 **RFC 9989: Domain-Based Message Authentication, Reporting, and Conformance (DMARC)**
Standards Track, Mai 2026, ersetzt RFC 7489
www.rfc-editor.org/rfc/rfc9989
- 5 **RFC 9990: DMARC Aggregate Reporting**
www.rfc-editor.org/rfc/rfc9990
- 6 **RFC 9991: DMARC Failure Reporting**
www.rfc-editor.org/rfc/rfc9991
- 7 **RFC 7489: DMARC (frühere Fassung, Informational, März 2015)**
www.rfc-editor.org/rfc/rfc7489
- 8 **RFC 7505: A "Null MX" No Service Resource Record**
www.rfc-editor.org/rfc/rfc7505
- 9 **Microsoft Learn: DKIM für Microsoft 365 einrichten**
[learn.microsoft.com/defender-office-365/email-authentication-dkim...](https://learn.microsoft.com/defender-office-365/email-authentication-dkim)
- 10 **Microsoft Learn: DMARC für Microsoft 365 einrichten**
learn.microsoft.com/defender-office-365/email-authentication-dm...
- 11 **Microsoft Learn: SPF für Microsoft 365 einrichten**
learn.microsoft.com/defender-office-365/email-authentication-sp...