E-MAIL-SICHERHEIT

SPF / DKIM / DMARC

Vollständige Checkliste & Schritt-für-Schritt-Anleitung

- Schritt-für-Schritt-Anleitung für alle drei Protokolle
- DNS-Record-Beispiele zum Copy-Pasten
- Häufige Fehler und wie du sie vermeidest
- Tools und Links für Tests
- 30-Tage-Projektplan

Warum SPF, DKIM und DMARC unverzichtbar sind

Jeden Tag werden Millionen gefälschter E-Mails verschickt – im Namen echter Unternehmen. Phishing, CEO-Fraud und Spam-Schleudern schaden Ruf und Umsatz. Die drei DNS-basierten Protokolle **SPF**, **DKIM** und **DMARC** bilden zusammen eine wasserdichte Authentifizierungsschicht für deinen E-Mail-Versand.

Protokoll	Was es tut	Ohne es riskierst du
SPF	Legt fest, welche Server deine Domain versenden dürfen	Jeder Server kann E-Mails in deinem Namen versenden
DKIM	Signiert jede E-Mail kryptografisch – verhindert Manipulation	E-Mails können unbemerkt verändert werden
DMARC	Verknüpft SPF/DKIM und gibt Empfängern Anweisungen bei Fail	Gefälschte E-Mails landen trotzdem im Posteingang

1. SPF – Sender Policy Framework

SPF ist ein TXT-Record in deinem DNS, der listet, welche IP-Adressen und Server berechtigt sind, E-Mails von deiner Domain zu senden. Empfänger-Server prüfen diesen Record beim Eingang jeder E-Mail.

Schritt-für-Schritt

1 **Alle E-Mail-Versender deiner Domain identifizieren** ☐
z. B. Google Workspace, Office 365, CRM, Newsletter-Tool

2 **SPF-Record erstellen** ☐
Kombiniere alle Versender zu einem einzigen TXT-Record

3	**Record im DNS deiner Domain eintragen** Beim Hoster / Registrar unter DNS-Verwaltung als TXT-Record	☐
4	**Record mit Tool validieren** mxtoolbox.com/spf.aspx oder kitterman.com/spf	☐
5	**Nach 24–48 h erneut prüfen** DNS-Propagation abwarten, dann Ergebnis bestätigen	☐

DNS-Record Beispiele

SPF TXT-Record (Typ: TXT | Host: @)

```
# Nur Google Workspace
v=spf1 include:_spf.google.com ~all

# Google + Office 365
v=spf1 include:_spf.google.com include:spf.protection.outlook.com ~all

# Google + Office 365 + eigener Mailserver (1.2.3.4)
v=spf1 ip4:1.2.3.4 include:_spf.google.com include:spf.protection.outlook.com -all
```

■■ Häufiger Fehler: Nie mehr als einen SPF-Record pro Domain anlegen! Mehrere TXT-Records mit *v=spf1* führen zu einem "PermError" – alle SPF-Prüfungen schlagen fehl. Mehrere Versender immer in einem einzigen Record kombinieren.

2. DKIM – DomainKeys Identified Mail

DKIM fügt jeder ausgehenden E-Mail eine kryptografische Signatur hinzu. Der öffentliche Schlüssel liegt im DNS; Empfänger-Server prüfen damit die Echtheit. Selbst wenn eine E-Mail auf dem Weg manipuliert wird, schlägt die Prüfung fehl.

Schritt-für-Schritt

1	**DKIM im E-Mail-Dienst aktivieren** Google Workspace: Admin-Konsole → Apps → Gmail → DKIM-Authentifizierung	☐
2	**Schlüsselpaar generieren lassen** Der Dienst generiert Public Key + Selector automatisch	☐
3	**TXT-Record im DNS eintragen** Format: ._domainkey. → Wert vom Dienst kopieren	☐
4	**DKIM-Versand aktivieren** Nach DNS-Propagation im Dienst auf 'Aktivieren' klicken	☐
5	**Verifizieren** E-Mail an mail-tester.com oder Check via MXToolbox	☐

DNS-Record Beispiele

DKIM TXT/CNAME-Record

```
# Format
<selector>._domainkey.<deine-domain.de>   TXT

# Beispiel Google Workspace (Selector: google)
google._domainkey.example.de   TXT
v=DKIM1; k=rsa; p=MIGfMA0GCSqGSIb3DQEBA...(langer Key vom Dienst)

# Beispiel Office 365 (zwei Records, beide eintragen!)
selector1._domainkey.example.de   CNAME   selector1-example-de._domainkey.example.onmicrosoft.com
selector2._domainkey.example.de   CNAME   selector2-example-de._domainkey.example.onmicrosoft.com
```

■■ Häufiger Fehler: DKIM-Schlüssel müssen mindestens 1024 Bit lang sein (empfohlen: 2048 Bit). Kürzere Schlüssel gelten als unsicher. Viele Dienste bieten 2048 Bit an – diese Option immer wählen. Schlüssel regelmäßig rotieren (alle 6–12 Monate).

3. DMARC – Domain-based Message Authentication

DMARC verbindet SPF und DKIM: Es legt fest, was mit E-Mails passiert, die beide Prüfungen nicht bestehen – und sendet dir Berichte über alle E-Mails, die im Namen deiner Domain verschickt werden.

Policy-Stufen (schrittweise verschärfen!)

Policy	Bedeutung	Empfehlung
p=none	Nur beobachten, keine Aktion	Startpunkt – immer zuerst!
p=quarantine	Verdächtige E-Mails in Spam verschieben	Nach 2–4 Wochen Beobachtung
p=reject	Verdächtige E-Mails komplett ablehnen	Ziel – nach vollständiger Verifikation

Schritt-für-Schritt

1. **Reporting-E-Mail-Adresse vorbereiten** ☐
   Eigene Adresse für DMARC-Berichte, z. B. dmarc-reports@example.de
2. **DMARC-Record mit p=none anlegen** ☐
   Zuerst nur beobachten – SPF/DKIM müssen fehlerfrei sein
3. **Berichte 2–4 Wochen analysieren** ☐
   Tool-Empfehlung: dmarcanalyzer.com, postmarkapp.com/dmarc

4	**Policy auf p=quarantine erhöhen** Wenn alle legitimen Sender korrekt konfiguriert sind	☐
5	**Policy auf p=reject setzen** Maximale Sicherheit – erst wenn alles sauber läuft	☐
6	**Laufend überwachen** DMARC-Berichte regelmäßig prüfen, neue Versender zeitnah einpflegen	☐

DNS-Record Beispiele

DMARC TXT-Record (Host: _dmarc.<deine-domain.de>)

```
# Typ: TXT | Host: _dmarc | Wert:

# Stufe 1: Nur beobachten (Startpunkt)
v=DMARC1; p=none; rua=mailto:dmarc-reports@example.de; ruf=mailto:dmarc-reports@example.de; fo=1

# Stufe 2: Quarantine (50% der Failures)
v=DMARC1; p=quarantine; pct=50; rua=mailto:dmarc-reports@example.de; fo=1

# Stufe 3: Reject (Vollschutz)
v=DMARC1; p=reject; rua=mailto:dmarc-reports@example.de; ruf=mailto:dmarc-reports@example.de; fo=1
```

Test-Tools & Ressourcen

MXToolbox	mxtoolbox.com	SPF, DKIM, DMARC, Blacklist – der Klassiker
Mail Tester	mail-tester.com	Kompletter E-Mail-Score mit Detailanalyse
DMARC Analyzer	dmarcanalyzer.com	DMARC-Reports lesen und verstehen
Google Admin Toolbox	toolbox.googleapps.com/apps/checkmx	MX/DNS-Analyse für Google Workspace
DMARC Record Check	dmarcian.com/dmarc-inspector	DMARC-Record inspizieren und validieren
SPF Wizard	spfwizard.net	SPF-Record interaktiv erstellen

30-Tage-Projektplan

Dieser Plan führt dich sicher von Null zu einem vollständig gesicherten E-Mail-Setup. Gehe nicht zu schnell vor – Beobachtungsphasen sind entscheidend.

Woche 1 (Tage 1–7)		
Tag 1–2	Inventur: Alle E-Mail-Versender identifizieren und dokumentieren	☐
Tag 3–4	SPF-Record erstellen, im DNS eintragen, verifizieren	☐
Tag 5–6	DKIM in allen Diensten aktivieren, DNS-Records eintragen	☐
Tag 7	Erstes vollständiges Testing (MXToolbox + mail-tester.com)	☐

Woche 2 (Tage 8–14)		
Tag 8	DMARC-Record mit p=none anlegen, Reporting-Adresse prüfen	☐
Tag 9–10	Ersten DMARC-Report empfangen und analysieren	☐
Tag 11–13	Unbekannte Versender identifizieren und SPF/DKIM ergänzen	☐
Tag 14	Zwischencheck: Alle Tests grün? Weiter zu Woche 3	☐

Woche 3 (Tage 15–21)		
Tag 15	DMARC auf p=quarantine pct=25 erhöhen	☐
Tag 16–20	Täglich Reports prüfen – Auffälligkeiten dokumentieren	☐
Tag 21	Erhöhung auf pct=50 falls keine Probleme aufgetreten	☐

Woche 4 (Tage 22–30)		
Tag 22–24	pct=100 mit p=quarantine – alle Reports prüfen	☐
Tag 25–28	Stabilisierungsphase – keine neuen Sender?	☐
Tag 29	DMARC auf p=reject setzen – maximale Sicherheit	☐
Tag 30	Abschlusscheck und Dokumentation für die IT-Akte	☐

■ **Profi-Tipp:** Richte dir einen Kalender-Erinnerung alle 6 Monate ein, um DKIM-Schlüssel zu rotieren und SPF-Records auf veraltete Sender zu prüfen. E-Mail-Sicherheit ist kein einmaliges Projekt, sondern laufende Pflege.

Professionelle Unterstützung benötigt?
Unser Team richtet SPF, DKIM und DMARC zuverlässig für dich ein – inkl. Überprüfung aller Dienste und laufendem Monitoring.

itsupport.online
+49 (0)30 7478 1308
info@itsupport.onl