DMARC

Inhaltsverzeichnis

- 1 Policies
- 2 Alignment
- 3 Einführung
- 4 Fazit

DMARC baut auf SPF und DKIM auf und legt fest, wie empfangende Mailserver mit Nachrichten umgehen sollen, die Authentifizierungsprüfungen nicht bestehen.

Domain-based Message Authentication, Reporting and Conformance, kurz DMARC, verbindet SPF und DKIM mit einer veröffentlichten Policy im DNS. Domaininhaber können damit Regeln und Reporting für E-Mail-Authentifizierung definieren.

1 Policies

DMARC kennt verschiedene Richtlinien, die schrittweise eingeführt werden können.

- **none:** nur beobachten und Reports sammeln.
- **quarantine:** verdächtige Nachrichten in Spam oder Quarantäne verschieben.
- **reject:** fehlerhafte Nachrichten ablehnen.

2 Alignment

DMARC verlangt, dass die sichtbare Absenderdomain zu SPF oder DKIM passt. Dieses Alignment verhindert viele Spoofing-Szenarien.

- SPF-Alignment bezieht sich auf Envelope-Sender.
- DKIM-Alignment bezieht sich auf die signierende Domain.
- Mindestens eine Methode muss erfolgreich und aligned sein.

3 Einführung

DMARC sollte kontrolliert eingeführt werden, damit legitime Versandwege nicht blockiert werden.

- Mit p=none starten.
- Reports auswerten und Versandquellen bereinigen.
- Policy erst danach verschärfen.

4 Fazit

DMARC ist ein zentraler Schutz gegen Domain-Spoofing und sollte bei produktiven Domains sorgfältig geplant und überwacht werden.