MTA-STS

Inhaltsverzeichnis

MTA-STS erlaubt Empfängerdomains, per Policy TLS für die Zustellung zu verlangen. Unterstützende Absender-MTAs laden die Policy und stellen dann nur noch verschlüsselt an die genannten MX-Hosts zu.

1 Funktionsweise

Die Empfängerdomain veröffentlicht eine Policy (Web + DNS-Hinweis). Sendende MTAs laden sie und stellen nur noch per gültigem TLS zu den genannten MX-Hosts zu.

- **Policy-Datei:** Modus, MX-Liste, Max-Age
- **DNS-Record:** Auffindbarkeit der Policy
- **Reporting:** oft ergänzt durch TLS-RPT

2 Typische Einsatzbereiche

- Absicherung von Geschäfts- und Kundendomains
- Schutz vor Downgrade auf Klartext-SMTP
- Härtung neben SPF/DKIM/DMARC

3 Wichtige Hinweise

- Falsche MX-/Zertifikatskonfiguration blockiert Zustellung im enforce-Modus.
- Einführung schrittweise über Testing-Modus.
- Zertifikats- und MX-Änderungen an Policy koppeln.

4 Fazit

MTA-STS macht SMTP-Transportverschlüsselung policy-fähig – ein wichtiger Baustein gegen aktive Downgrade-Angriffe auf E-Mail.