Technische Aspekte der TR-03108 Version 2.0

Historie

- 1971: Erste Mail
- 1982: Erste Mail über SMTP
- 2023: > 340 Mrd. Mails (Quelle: Statista)
- Tendenz weiter steigend

Stand der Dinge

- TLS zwischen MTAs (STARTTLS) heute weit verbreitet
  - Unverschlüsselte Kommunikation aber nicht unüblich
  - Genutzte Kryptoverfahren teilweise veraltet
  - Zertifikate werden meist nicht authentifiziert:
    Kein Schutz gegen aktive Angriffe!
- TLS zwischen MTA und MUA teilweise nicht verfügbar

TR-03108 „Sicherer E-Mail-Transport“

- Wie sichert man die Kommunikation eines MTA?
- Fokus liegt auf technischen Anforderungen
- Wenige organisatorische Anforderungen (richten sich vor allem an Mail-Provider)
- Keine Authentifizierung von E-Mails (kommt mit TR-03182)

Grundsätze

- TLS zwischen MTAs sofern möglich (Best-Effort-Ansatz)
- TLS zwischen MTA und MUA (SMTPS/STARTTLS, IMAPS, POP3S)
- DANE (DNSSEC)
- MTA-STS (optional)
- TLSRPT

TLS zwischen MTA und MUA

- Kommunikation mit dem MUA muss verschlüsselt erfolgen können (SUBMISSIONS, IMAPS, POP3S, HTTPS)
- Eine automatische Konfiguration des MUA (DNS SRV / Autodiscover / Autoconfig) muss unterstützt werden

TLS zwischen MTAs

- Der MTA muss TLS mittels STARTTLS unterstützen
- Vorgaben für die Umsetzung von TLS macht TR-03116-4
- Aber: Wenn die Gegenstelle es nicht unterstützt, darf auch abweichend (unverschlüsselt) kommuniziert werden (Best-Effort-Ansatz)

DANE

- „Klassisches“ TLS zwischen MTAs schützt nur vor passiven Angriffen
- Schutz vor aktiven Angriffen:
  - Zertifikate müssen über DNS bezogen werden können und bereitgestellt werden (DANE)
  - DNSSEC muss unterstützt werden (eingehend wie ausgehend)

MTA-STS

- DNSSEC leider nicht flächendeckend
- MTA-STS ist leichtgewichtige Alternative
- Neu in Version 2.0 der TR
- Der Server signalisiert mittels DNS/HTTPS, dass sein Zertifikat einschl. Zertifikatskette (ähnlich wie bei HTTPS) zu prüfen ist
- Kann der sendende MTA (sofern er MTA-STS unterstützt) das Zertifikat nicht auf eine vertrauchenswürdige CA zurückführen, dann darf keine Kommunikation stattfinden
- TR macht MTA-STS (bislang) nur optional

TLSRPT

- Wie können Fehler erkannt und analysiert werden?
  - Hatte die Gegenstelle Probleme?
  - Warum hat die Gegenstelle nicht zugestellt?
- TLSRPT hilft, indem es anonymisierte Fehlerberichte an die Gegenseite sendet
- TLSRPT muss (eingehend wie ausgehend) unterstützt werden
- Neu in Version 2.0 der TR

Anwendungsbereich

- „Selbststudium“
  - Best-Practices für die Konfiguration des eigenen Mail-Servers
- IT-Sicherheitskennzeichen
  - Leichtgewichtige Möglichkeit die Einhaltung aufzuzeigen
  - Kennzeichen wird beim BSI beantragt
  - Eine Prüfung durch Dritte ist nicht erforderlich
  - Einige Mailprovider gehen diesen Weg:
    (freenet.de, mail.de, mailbox.org, …)
- Zertifizierung
  - Konformitätsbewertung durch vom BSI anerkannte Prüfstelle