

TLS härten

Mailcow deaktiviert mittlerweile unsichere Protokolle wie TLS 1.0 und 1.1 - jedoch sind noch einige 1.2 Cipher unsicher, diese können dann in der Datei /opt/data/conf/postfix/main.cf angepasst werden, fügt die Zeilen in der Mitte bei der TLS Konfiguration ein:

```
smtp_tls_protocols = !SSLv2, !SSLv3,!TLSv1,!TLSv1.1
smtp_tls_mandatory_protocols = !SSLv2, !SSLv3,!TLSv1,!TLSv1.1
smtpd_tls_protocols = !SSLv2, !SSLv3,!TLSv1,!TLSv1.1
smtpd_tls_mandatory_protocols = !SSLv2, !SSLv3,!TLSv1,!TLSv1.1
lmtp_tls_protocols = !SSLv2, !SSLv3,!TLSv1,!TLSv1.1
lmtp_tls_mandatory_protocols = !SSLv2, !SSLv3,!TLSv1,!TLSv1.1
# SSL/TLS supported ciphers
smtp_tls_ciphers = high
smtp_tls_mandatory_ciphers = high
smtpd_tls_ciphers = high
smtpd_tls_mandatory_ciphers = high
tls_high_cipherlist = tls_high_cipherlist = ECDHE-ECDSA-AES256-GCM-
SHA384:TLS_AES_256_GCM_SHA384:ECDHE-ECDSA-CHACHA20-
POLY1305:TLS_CHACHA20_POLY1305_SHA256:ECDHE-ECDSA-AES128-GCM-
SHA256:TLS_AES_128_GCM_SHA256:ECDHE-RSA-AES256-GCM-SHA384:TLS_AES_256_GCM_SHA384:ECDHE-RSA-
CHACHA20-POLY1305:TLS_CHACHA20_POLY1305_SHA256:ECDHE-RSA-AES128-GCM-
SHA256:TLS_AES_128_GCM_SHA256
smtpd_tls_eecdh_grade = ultra
```

Startet danach den Postfix Container neu und prüft anschließend mit internet.nl Mailservercheck, ob nun die Konfiguration übernommen wurde.

Weitere Informationen: <https://schroederdennis.de/tipps-tricks/mailcow-smtp-smtpd-tls-1-0-tls1-1-deaktivieren/>

Revision #4

Created 2024-08-25 08:25:23 UTC by Peter Leibling

Updated 2024-08-25 09:02:35 UTC by Peter Leibling