DNSSEC, DANE und MTA-STS

Informationen

Für eine erweiterte Emailsicherheit empfiehlt es sich auch noch DNSSEC, DANE und MTA-STS zu verwenden.

Für DANE ist jedoch zwingend DNSSEC benötigt und das bietet leider nicht jeder Anbieter, hier ein paar Möglichkeiten:

- DynDNS mit DNSSEC und IPV4/6 Unterstützung: https://desec.io/
- Günstiger DNS Anbieter mit DNSSEC Unterstützung: https://www.domaindiscount24.com/
- Anbieter, der nicht nur Domainanbieter ist (inkl. DNSSEC) - aber auch VServer anbieter: https://www.netcup.de/
- Dane und MTA-STS einrichten:https://github.com/internetstandards/toolbox-wiki/blob/main/DANE-for-SMTP-how-to.md

DANE Einträge erstellen (Mailcow auf Ubuntu)

> Der Anbieter muss natürlich DNSSEC und DANE unterstützen - z.B. NETCUP

- Exportieren Sie alle Zertifikate inkl. der Chain (z.B. URL im Browser aufrufen, Zertifikat anzeigen und dann das Zertifikate inkl. Intermediate und Root exportieren in Einzeldateien).
- Dann jedes Zertifikat den Hashwert ermitteln mit dem folgenden Befehl:

```
openssl x509 -in Zertifikatsname.crt -noout -pubkey | openssl pkey -pubin -outform DER |
openssl sha256
```

- Erstellen Sie einen DNS TXT Record für jeden Wert, denn sie haben wie folgt:
  Host: _25._tcp.servername Wert: 3 1 1 wert_vom_serverzertifikat
  Host: _25._tcp.servername Wert: 2 1 1 wert_vom_intermediatezertifikat
  Host: _25._tcp.servername Wert: 2 1 1 wert_vom_rootzertifikat

MTA-STS Eintrag erstellen (Mailcow auf Ubuntu)

- Erstellt eine Datei mta-sts.txt im Verzeichnis /opt/mailcow-dockerized/data/web/.well-known mit dem folgenden Inhalt:

```
version: STSv1
mode: enforce
max_age: 15552000
mx: mailserver.domain.de
```

- Fügt in der Datei /opt/mailcow-dockerized/mailcow.conf im Eintrag ADDITIOONAL_SERVER_NAMES den mta-sts.domain.com eintrag hinzu und startet die Mailcow neu (ggf. reicht auch nur ein Neustart des ACME Containers).
- Erstellt dann noch einen DNS Host-Eintrag für MTS-STS der auf eure Mailcow zeigt.

Weitere Infos: https://schroederdennis.de/tutorial-howto/mailcow-mta-sts-richtig-einrichten-security-mit-tls/

Revision #8
Created 2024-03-09 14:23:24 UTC by Peter Leibling
Updated 2024-08-27 11:05:53 UTC by Peter Leibling