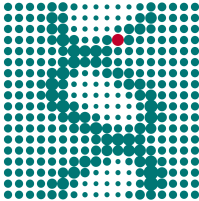


# Sicherheit im Netz von SMTP- und HTTP-Servern

Paul Menzel (Max-Planck-Institut für molekulare Genetik)

9. November 2017

## Wer bin ich?



- ▶ Systemarchitekt beim Max-Planck-Institut für molekulare Genetik
- ▶ Diplom-Wirtschaftsmathematiker an TU Berlin
- ▶ FLOSS-Befürworter

# Problemstellung

## Ziel

- ▶ Sichere Übertragung von Daten
- ▶ Geheim und authentifiziert

## Angriffsmodell

- ▶ Annahme: Keine Übernahme der Server durch Angreifer
- ▶ Mittelsmannangriff

## Realistisch?

- ▶ DFN-Netz separat vom „Internet“
- ▶ Netzwerkgeräte meist im Ausland produziert und enthält BLOBs
- ▶ Snowden-Veröffentlichungen zeigen, dass realistisch.

## Lösungen (TLS)

# Angriffe

Poodle, DROWN, ...

Verschiedene Angriffe.

1. Downgrade-Attacke (STARTTLS)
2. Poodle, DROWN
3. Unsichere Chiffren

## Sichere Konfiguration

<postmaster@...mpg.de> nach RFC 822 Pflicht!

1. BetterCrypto.org
2. Mozilla Wiki: Security/Server Side TLS
3. Cipherli.st

## Ideal für SMTP

Mehrere Komponenten: DNS, Zertifikate

## Zeitraum

- ▶ 8. November 2017

# Inkorrekte MX-Einträge

## Beispiel GV

```
$ host mpg.de  
[...]  
$ host mx1.mpg.de  
[...]
```

Keine Antwort von postmaster@mpg.de auf Nachricht.

## Problem Verwaltungsadressen

```
$ host vw.molgen.mpg.de  
[...]
```

Bitte überprüfen!

# HTTP

## Problem

1. Viele alte Dienste ohne HTTPS-Zertifikat, ohne ACME oder Wildcard-Zertifikate schwer zu handhaben
2. Never-touch-a-running System

## Lösung

1. SSL-Terminierung (HAProxy)
2. Wechsel zu Let's Encrypt und Skript, dass Zertifikate in Echtzeit erstellt

## Sicherheit der Serverprogramme

- ▶ Problem: Dienste von überall erreichbar
- ▶ Beliebige Eingabe (Analyseprogramme (Spam, Virenschutz),  
Formulare)
- ▶ Untersuchung der Sicherheit der Server
  - ▶ SMTP: Postfix, Exim, ...
  - ▶ HTTP: Apache HTTP Server, Nginx, ...



# Fazit

1. MPG-Netz auch Vorbildwirkung
2. Mehr Gewissenhaftigkeit
3. Mehr Bewusstsein (DNSSEC, DFN)
4. Ohne DANE keine automatische Konfiguration möglich, manuelle Konfiguration erforderlich

# Fragen