

TLS 1.1 & 1.0 deaktivieren

Veraltete Verschlüsselung deaktivieren



Stand: 21.01.2023, BETA

Management Summary

Das BSI stuft die veralteten IT-Sicherheitsmechanismen „TLS 1.0“ und „TLS 1.1“ zum Schutz der Datenübertragung zwischen OZG-Dienst und Bürgerin und Bürger nicht mehr als

angemessen sicher ein. Der Einsatz in OZG-Diensten sollte daher deaktiviert sein.

Ressourcenabschätzung

-  Gering (< 5 PT)
-  Ohne neue Hardware

Erläuterung für OZG-Dienstverantwortliche

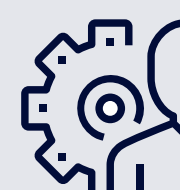
Die veralteten IT-Sicherheitsstandards TLS 1.1 und TLS 1.0 erfüllen nicht mehr die BSI Mindeststandards. Diese sollten daher, zum Schutz von Risiken wie Abhören und Verfälschen von Kommunikation durch Dritte, in OZG-Diensten deaktiviert werden. Der Anteil ausgeschlossener Nutzer mit veralteten, unsicheren Browsern ist vernachlässigbar.

Referenz



BSI TLS 2.0.01 b

Umsetzung



RZ-Betrieb

Technischer Umsetzungsansatz

Nahezu alle marktüblichen Webkomponenten unterstützen die Deaktivierung der veralteten und unsicheren TLS-Protokolle in den Versionen 1.0 und 1.1. In der Regel können TLS 1.1 und TLS 1.0 durch eine einfache Konfigurationsanpassung in Loadbalancer, WAF, Reverse-Proxy, Webserver oder externen CDN deaktiviert werden.

Neben dem aktuellen TLS 1.3 sollte zusätzlich derzeit noch TLS in der Version 1.2 zur Abwärtskompatibilität aktiviert sein.

```
# nginx.conf
server {

    [...]

    ssl_protocols TLSv1.2 TLSv1.3;

}
```

Konfiguration Nginx-Reverse-Proxy