TLS 1.1 & 1.0 deaktivieren

Veraltete Verschlüsselung deaktivieren

OZG-Security-Challenge 2023

Stand: 26.01.2023 BETA

Management Summary

Das BSI stuft die veralteten IT-Sicherheitsmechanismen „TLS 1.0“ und „TLS 1.1“ zum Schutz der Datenübertragung zwischen Onlinedienst sowie Bürgerin und Bürger nicht mehr als angemessen sicher ein. Der Einsatz in Onlinediensten sollte daher deaktiviert sein.

Ressourcenabschätzung

- Gering (<5 PT)
- Ohne neue Hardware

Erläuterung für Onlinedienst-Verantwortliche

Die veralteten IT Sicherheitsstandards TLS 1.1 und TLS 1.0 erfüllen nicht mehr die BSI-Mindeststandards. Diese sollten daher, zum Schutz vor Risiken wie Abhören und Verfälschen von Kommunikation durch Dritte, in Onlinediensten deaktiviert werden. Der Anteil ausgeschlossener Nutzerinnen und 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 Verwendung des TLS-Protokolls in der Version 1.3 schon seit einigen Jahren. In der Regel kann TLS 1.3 durch eine Konfigurationsanpassung in Loadbalancer, WAF, Reverse-Proxy, Webserver oder externen CDN aktiviert werden. Bei Verwendung von Deep Paket Inspection sollte auf die Kompatibilität von Architektur und Produkt geachtet werden. Neben TLS 1.3 sollte zusätzlich derzeit noch TLS in der Version 1.2 zur Abwärtskompatibilität angeboten werden.

```
# nginx.conf
server {
[...]
ssl_protocols TLSv1.2 TLSv1.3;
}
```

Konfiguration Nginx-Reverse-Proxy

Bundesministerium des Innern und für Heimat
Bundesamt für Sicherheit in der Informationstechnik

OZG Onlinezugangsgesetz