Transport Layer Security (TLS) 1.3

Aktuelle Verschlüsselung der Kommunikation zwischen Bürgerinnen, Bürgern und Onlinedienst

OZG-Security Challenge 2023

Stand: 26.01.2023 BETA

Management Summary

Beim Datenaustausch zwischen Onlinedienst, Bürgerinnen und Bürgern muss ein zeitgemäßer Schutz gegen Mitlesen und Veränderung gewährleistet werden. TLS 1.3 ist der aktuelle Standard für die leistungsfähige, moderne und hochsichere Verschlüsselung der Daten während der Übertragung.

Ressourcenabschätzung

- Gering
- Ohne neue Hardware

Erläuterung für Onlinedienst-Verantwortliche

IT-Sicherheit lebt von aktuellen Verschlüsselungsstandards wie TLS 1.3 (Transport Layer Security 1.3). Auch das BSI fordert diesen in seinem Mindeststandard. Trotz technischer Verfügbarkeit in den Produkten ist TLS 1.3 bisher nicht flächendeckend aktiviert. Durch den Einsatz von diesem hochsicheren Verschlüsselungsverfahren wird der Gefahr des Abhörens und Verfälschens von Kommunikation durch Dritte bestmöglich begegnet. Die Verwendung von TLS 1.3 ist bei großen Internetangeboten gängige Praxis. Auch die Online-Kommunikation der Bürgerinnen und Bürger mit Onlinediensten ist entsprechend abzusichern.

Referenz

BSI TLS 2.0.01 a & c

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