

Strict-Transport-Security (HSTS)

Sicherstellung verschlüsselter Kommunikation zwischen Bürgerinnen, Bürgern und OZG-Dienst





Stand: 26.01.2023, BETA

Management Summary

Unverschlüsselte und damit unsichere Kommunikation eines OZG-Dienstes ist nicht mehr zeitgemäß. HSTS lässt für einen angegebenen Zeitraum ausschließlich verschlüsselte und damit

sichere Verbindungen zwischen Bürgerinnen, Bürger und einem OZG-Dienst zu. Bestehende Weiterleitungen werden hierdurch ergänzt.

Ressourcenabschätzung

-  Gering (< 5 PT)
-  Ohne neue Hardware

Erläuterung für OZG-Dienstverantwortliche

Browser rufen den OZG-Dienst häufig zunächst unverschlüsselt und damit unsicher auf. Eingerichtete Weiterleitungen auf die jeweilige sicher verschlüsselte Seite reduzieren das Problem, aber es bleiben Restrisiken. HSTS stellt eine Lösung dieses Problems dar. Über einen Parameter wird der Browser der Bürgerinnen und Bürger angewiesen, den OZG-

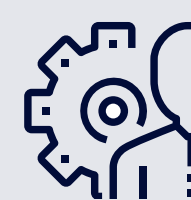
Dienst für eine vorgegebene Zeit ausschließlich verschlüsselt aufzurufen.

Referenz



BSI ISi-Webserver
4.2.2
RFC 6797

Umsetzung



RZ-Betrieb

Technischer Umsetzungsansatz

Ist HSTS konfiguriert, wird der aufrufende Webbrowser in der ersten Antwort des Dienstes dazu angewiesen, ausschließlich sichere HTTPS-Verbindungen mit TLS anstelle von HTTP-Verbindungen zu nutzen. Es ist daher zwingend erforderlich, solche sicheren Verbindungen auch anzubieten, um Nutzende nicht auszuschließen. Über den „Strict-Transport-Security“ HTTP Response Header wird die

Anweisung zu HSTS übergeben. Der Wert des Headers muss dazu eine Gültigkeitsdauer der Anweisung und optional die Direktive, den Zwang der sicheren Verbindung auf Subdomänen auszuweiten, enthalten. In der Regel kann HSTS durch Setzen des Headers gemäß RFC 6797 in Loadbalancer, WAF, Reverse-Proxy, Webserver oder externen CDN aktiviert werden.

```
# nginx.conf
server {

    [...]

    add_header
        Strict-Transport-Security
        "max-age=31536000;

}
```

Konfiguration Nginx-Reverse-Proxy