

Die nachfolgend bereitgestellten Informationen dienen als Grundlage für ein fiktives Preismodell anhand des Beispiel-Einzelabrufs eines Penetrationstest des TI Gateway Zugangsmoduls. Dabei geht es grundsätzlich um die Überprüfung der Sicherheit und Ermittlung potenzieller Schwachstellen.

In der folgenden Skizze wird das TI-Gateway inkl. Scope dargestellt:

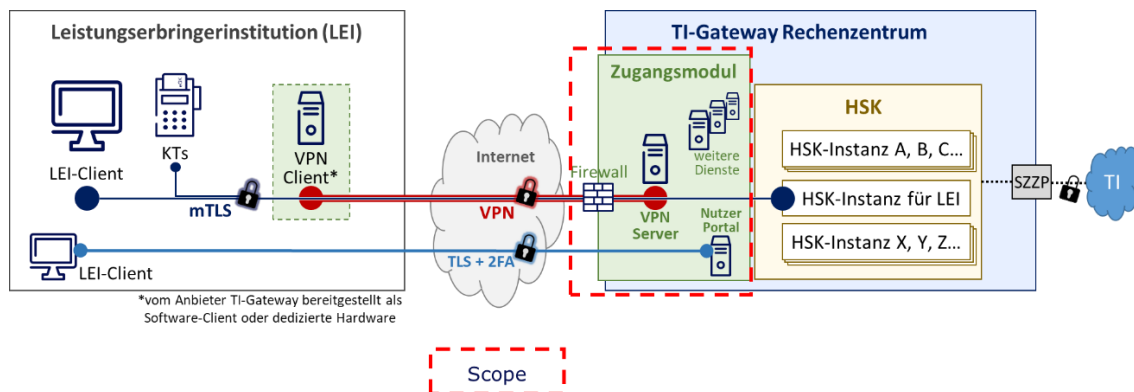


Abbildung 1 TI-Gateway-Skizze mit Sope-Eingrenzung

Informationsbasis:

- Black-Box Internetschnittstellen
- Grey-Box: Prüfung der Web-GUI und der VPN-Verbindung ohne und mit RU-Zugang + Client-Credentials, ggf. weitere alle erreichbaren Schnittstellen, Infrastruktur, Konfiguration (Installationsroutine)
- Frei zugängliche Informationsquellen über das gematik-Fachportal informativ/unterstützend nutzen

Prüfumgebung:

- Referenzumgebung (RU) des Anbieters/Herstellers

Rollen, aus denen heraus der Angriff erfolgen soll:

- Beliebige Person ohne Zugangsdaten
- Leistungsbringer-/Nutzer-Zugangsdaten für Web-GUI

Zu betrachtende Bedrohungsszenarien:

- Explorativ prüfen, wo sich Schwachstellen/Sicherheitsrisiken finden lassen, z. B. anhand veralteter Software oder Fehlkonfigurationen
- Angriff der Web-GUI und VPN-Verbindung und aller erreichbaren Schnittstellen
- Versuch, Daten unberechtigt anzulegen, zu ändern, zu löschen
- Gefährdung angrenzender Systeme durch Schwachstellen im Prüfsystem

Out of Scope:

- High-Speed-Konnektor
- Destruktive Tests, die zur persistenten Betriebsunfähigkeit führen, und Last-Tests

Bereitstellungen:

Wer	Was
Auftragnehmer	<ul style="list-style-type: none"> • E-Mail- und IP-Adressen, von denen aus geprüft wird
Anbieter/Hersteller TI-Gateway	<ul style="list-style-type: none"> • Referenzumgebung • Client-Credentials für VPN & Nutzerportal • Freischaltung der WAF/Firewall für Zugriff auf Backend • URLs

Durchführungsdauer des Pentests: Zwei Wochen