SSL/TLS – Sichere Verschlüsselung für Internetkommunikation

Inhaltsverzeichnis

SSL (Secure Sockets Layer) und TLS (Transport Layer Security) sind Verschlüsselungsprotokolle, die die sichere Übertragung von Daten im Internet ermöglichen. TLS ist der offizielle Nachfolger von SSL und wurde eingeführt, da ältere SSL-Versionen unsicher sind. Die Begriffe werden oft synonym verwendet, obwohl nur TLS aktuell empfohlen wird. Es schützt Informationen vor unbefugtem Zugriff und Manipulation, insbesondere bei Webseiten (HTTPS), E-Mails und VPNs.

SSL (Secure Sockets Layer) und TLS (Transport Layer Security) sind Protokolle zur Verschlüsselung der Kommunikation im Internet. Sie sorgen dafür, dass Daten sicher zwischen Clients (z. B. Webbrowsern) und Servern übertragen werden und schützen vor Angriffen wie Man-in-the-Middle-Attacken.

1 Warum heißt es heute TLS statt SSL?

Viele Menschen sprechen noch von „SSL“, obwohl TLS der eigentliche Standard ist. Der Grund dafür liegt in der Weiterentwicklung des Protokolls:

- **SSL 2.0 (1995) und SSL 3.0 (1996)** wurden von Netscape entwickelt, sind aber unsicher und wurden offiziell als veraltet eingestuft.
- **TLS 1.0 (1999)** war die erste Version, die von der IETF (Internet Engineering Task Force) als Nachfolger von SSL standardisiert wurde.
- **TLS 1.1 (2006) und TLS 1.2 (2008)** brachten Verbesserungen in der Sicherheit und Performance.
- **TLS 1.3 (2018)** ist die aktuelle Version und bietet optimierte Verschlüsselungsalgorithmen sowie eine schnellere Verbindungsaushandlung.

Da SSL 2.0 und SSL 3.0 unsicher sind, sollte ausschließlich TLS verwendet werden. Dennoch wird der Begriff „SSL“ oft noch aus Gewohnheit benutzt, insbesondere bei der Bezeichnung von „SSL-Zertifikaten“, obwohl es technisch korrekter „TLS-Zertifikate“ heißen sollte.

2 Funktionsweise von SSL/TLS

SSL/TLS basiert auf einem hybriden Verschlüsselungsprinzip und nutzt sowohl **asymmetrische** als auch **symmetrische Kryptografie**:

1. **Handshake-Phase**: Der Client und der Server tauschen Zertifikate aus und vereinbaren einen gemeinsamen Schlüssel für die Verschlüsselung.
2. **Sitzungsverschlüsselung**: Nachdem ein sicherer Sitzungsschlüssel erstellt wurde, erfolgt die weitere Datenübertragung mit symmetrischer Verschlüsselung.
3. **Datenintegrität & Authentifizierung**: SSL/TLS stellt sicher, dass die übertragene Kommunikation nicht manipuliert wird und der Server authentisch ist.

3 Einsatzgebiete von SSL/TLS

- **Webseiten (HTTPS)**: SSL/TLS wird für verschlüsselte Webseitenverbindungen genutzt und schützt sensible Nutzerdaten.
- **E-Mail-Verschlüsselung**: POP3S, IMAPS und SMTPS sichern E-Mail-Kommunikation ab.
- **VPN & sichere Netzwerke**: TLS wird auch in VPN-Protokollen wie OpenVPN verwendet.
- **VoIP & Messaging**: Verschlüsselung von Internet-Telefonie und Chats.

4 Warum ist SSL/TLS wichtig?

- **Schutz sensibler Daten**: Kreditkarteninformationen, Passwörter und persönliche Daten bleiben geschützt.
- **Authentifizierung**: SSL-Zertifikate bestätigen die Identität einer Webseite oder eines Servers.
- **Vertrauen & SEO**: Suchmaschinen bevorzugen HTTPS-Webseiten, und Nutzer erwarten sichere Verbindungen.

5 Fazit

SSL/TLS ist essenziell für sichere Kommunikation im Internet. Webseitenbetreiber, E-Mail-Provider und andere Online-Dienste sollten immer moderne TLS-Versionen verwenden und regelmäßige Sicherheitsupdates durchführen.