TLS – Sicherheit im Internet durch Verschlüsselung

TLS steht für Transport Layer Security und ist ein Protokoll zur Verschlüsselung von Daten bei der Übertragung über Netzwerke – insbesondere im Internet. Es wird vor allem eingesetzt, um Verbindungen zwischen Clients (z. B. Webbrowsern oder E-Mail-Programmen) und Servern (z. B. Webseiten oder Mailservern) abzusichern. TLS sorgt dafür, dass Daten, die zwischen diesen Geräten übertragen werden, nicht von Dritten mitgelesen oder manipuliert werden können.

Wie funktioniert TLS?
Bei einer TLS-Verbindung wird zu Beginn ein sogenannter Handshake durchgeführt. Dabei tauschen Client und Server Informationen aus, um eine sichere Verbindung herzustellen. Der Server schickt dem Client ein digitales Zertifikat, das seine Identität bestätigt (z. B. für eine Webseite). Der Client prüft dieses Zertifikat und stimmt, falls alles passt, einer Verschlüsselung zu. Anschließend wird ein gemeinsamer Sitzungsschlüssel ausgehandelt, mit dem alle weiteren Daten verschlüsselt übertragen werden.

Wofür ist TLS gut?
TLS ist die Grundlage für Datensicherheit und Vertraulichkeit im Internet. Es schützt z. B. beim Onlinebanking, beim Einkauf in Webshops oder beim Versenden von E-Mails davor, dass sensible Informationen wie Passwörter, Kreditkartennummern oder persönliche Nachrichten abgefangen werden. Webseiten mit HTTPS (das "S" steht für Secure) nutzen ebenfalls TLS. Auch viele E-Mail-Dienste setzen TLS ein, um E-Mails während der Übertragung zwischen Mailservern oder von Nutzer zum Server zu verschlüsseln.

Für wen ist TLS verfügbar?
TLS ist nicht auf bestimmte E-Mail-Adressen oder Anbieter beschränkt. Jeder E-Mail-Anbieter oder -Nutzer kann TLS verwenden – vorausgesetzt, der entsprechende Dienst unterstützt es. Große Anbieter wie @t-online.de setzen längst standardmäßig TLS ein. Auch eigene E-Mail-Domains können TLS nutzen, wenn der Mailserver korrekt konfiguriert ist. Wichtig ist also nicht die Mail-Endung, sondern ob der Mailserver TLS unterstützt – und das ist heutzutage bei den meisten professionellen Anbietern der Fall.

Was muss der Anwender tun, um TLS nutzen zu können?

Damit ein Anwender TLS nutzen kann, ist in der Regel kein großer Aufwand nötig, denn die meisten modernen Geräte und Programme unterstützen TLS automatisch.

1. E-Mail-Programme richtig einrichten

Wenn man ein E-Mail-Programm wie Outlook, Thunderbird oder die Mail-App auf dem Smartphone nutzt sollte man sicherstellen, dass TLS bei der Verbindung zum Mailserver aktiviert ist:

- **Eingangsserver (IMAP/POP3)**: TLS/SSL-Verschlüsselung aktivieren
- **Ausgangsserver (SMTP)**: TLS/STARTTLS-Verschlüsselung aktivieren
- Oft gibt es beim Einrichten ein Häkchen oder Auswahlfeld wie „Sichere Verbindung (SSL/TLS) verwenden“ oder „STARTTLS verwenden“ – das sollte aktiviert sein.
- Die richtigen Ports verwenden:
    - IMAP mit TLS: Port 993
    - POP3 mit TLS: Port 995
    - SMTP mit TLS: Port 587 (mit STARTTLS) oder Port 465 (mit SSL/TLS)

2. Webmail-Nutzer (z. B. t-online.de)

Wer E-Mails über einen Webbrowser schreibt, nutzt automatisch TLS, wenn die Seite über HTTPS aufgerufen wird. In der Adresszeile des Browsers sollte dann ein Schloss-Symbol zu sehen sein – das zeigt eine gesicherte Verbindung an.

3. Eigene Domain / Mailserver

Wenn eine eigene E-Mail-Domain betrieben wird, muss man sicherstellen, dass der Mailserver TLS unterstützt:

- TLS-Zertifikat für den Mailserver einrichten
- Mailserver-Software korrekt konfigurieren
- STARTTLS und/oder SMTPS aktivieren

4. Nichts weiter bei modernen Geräten

Bei aktuellen Smartphones, Tablets und Computern ist TLS in den meisten Fällen standardmäßig aktiv, sofern der Mailanbieter es unterstützt. Der Anwender muss dann nur das richtige E-Mail-Konto einrichten – der Rest passiert automatisch.

Zusammenfassung:
Der Anwender hat darauf zu achten, dass sein Mailprogramm oder Webbrowser TLS aktiviert verwendet – bei seriösen Anbietern ist das bereits voreingestellt. Wird eine E-Mail-Einstellungen manuell vorgenommen, sollte sichergestellt sein, dass die Verschlüsselung für ein- und ausgehende Mails aktiviert ist.

Ein Support der TLS-Konfiguration auf der Partnerseite kann von der Waldenburger Versicherung AG **nicht** geleistet werden.

Eine TLS-Anbindung sollte nur Partnern ermöglicht werden, die im eigenen Haus über entsprechendes Know-How verfügen.

Mit der TLS Anbindung sparen Sie sich die jeweilige Eingabe der 12-stelligen TAN bei den von uns versendeten Dokumenten.

Die Verschlüsselung von personenbezogenen Daten ist datenschutzrechtlich vorgeschrieben und wurden bei Nichtbeachtung bereits durch Gerichtsurteile mit sehr hohen Bußgeldern belegt.

Entscheiden Sie – automatische Entschlüsselung per TLS oder manuelle einzeldokumentbezogene Entschlüsselung per TAN.