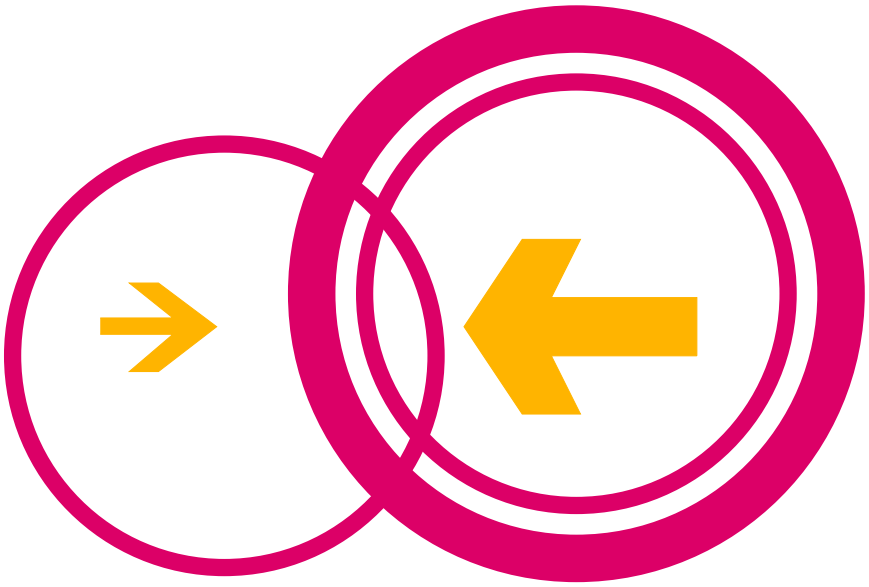

fulda.freifunk.net

Sicherheit in öffentlichen Netzen

Inhaltsverzeichnis

1 Sicherheit in öffentlichen Netzen

1.1 Die kleine Übersicht

1.1.1 Dinge in offenen/fremden Netzwerken beachten sollte

- Netzwerk als "öffentliches Netzwerk" in den Windows-Firewall Einstellungen markieren
- Freigaben von Daten ins Netzwerk abschalten
- HTTPS für Webseiten, an denen man sich anmeldet
- SSL/TLS in E-Mail Programmen aktivieren
- Sicherheitswarnungen im Browser beherzigen
- (optional) Verwenden von VPN
- Das Betriebssystem aktuell halten.
  D.h. Sicherheitsupdates regelmäßig installieren

1.1.2 Dinge die man in offenen/fremden Netzwerken vermeiden sollte

- Filesharing
- Öffnen von Ports
- "Firmen-/Heimnetzwerk"-Einstellungen
  in den Windows-Firewall Einstellungen nutzen

1.2 WLAN Sicherheit

1.2.1 Was bedeutet das überhaupt?

Bei der "WLAN-Sicherheit" bzw. richtiger der WLAN-Verschlüsselung handelt es sich ausschließlich um die Verschlüsselung, der durch die Luft übertragenen Daten, zwischen dem Client (Smartphone, Tablet, Laptop, etc.) und dem Accesspoint ("WLAN-Router", Freifunkknoten, etc.). Hierfür stehen verschiedene Mechanismen zur Verfügung, die hier im Anschluss grob erklärt werden sollen.

1.2.2 WPA/PSK und WPA2/PSK

Bei WPA/PSK und WPA2/PSK handelt es sich um die gängigsten Verschlüsselungsmethoden in Deutschland. Sie sind inzwischen als Nachfolger von WEP die Hauptverschlüsselungsmechanismen für private WLANs. WPA beschreibt hierbei, wie die Nachrichten verschlüsselt werden, aber der weit wichtigere Teil ist das Anhängsel PSK. PSK steht für Pre Shared Key. Der Schlüssel muss also sowohl dem Accesspoint als auch dem Benutzer bekannt sein. Das Problem hierbei ist, dass **jeder** Benutzer des Netzwerks **diesen für alle gleichen** Schlüssel kennen muss, wodurch auch jeder, der den Schlüssel besitzt den gesamten WLAN Verkehr mitlesen kann.

1.2.3 WPA/EAP und WPA2/EAP

Hierbei handelt es sich um einen Standard, wie er in Firmen häufig verwendet wird. Die Verschlüsselungsmethode ist die Gleiche, wie bei privaten WLANs auch. Den Unterschied macht hier das EAP, welches für "Extensible Authentication Protocol" steht und verschiedene Mechanismen bietet die Verschlüsselung zu nutzen. Gängig ist hier die Anmeldung an einem WLAN, wie man es auch sonst gewohnt ist, über einen Usernamen und ein Passwort, aber auch ein Zugriff über ein Zertifikat ist möglich und hängt von der Konfiguration ab.

1.2.4 Keine (offen/unverschlüsselt)

Nun ja, wie der Name schon sagt, findet hier einfach keine Verschlüsselung statt, der Zugriff ist also für jeden möglich und der Datenverkehr sichtbar.

1.2.5 Wozu brauchen wir eigentlich eine WLAN-Verschlüsselung?

Die WLAN-Verschlüsselung soll unsere Daten und unsere Privatssphäre schützen. Hierbei geht es aber weniger um die Daten, die wir direkt über das WLAN übertragen, denn dafür sind andere Mechanismen zuständig, als viel mehr um die Daten, die wir bereit stellen.
Zum Beispiel ist es inzwischen normal geworden, dass sich in privaten Haushalten sogenannte NAS-Systeme befinden auf denen private Daten, wie zum Beispiel Urlaubsbilder und ähnliches gespeichert sind. Hier will man nicht unbedingt, dass diese für jeden einsehbar sind und somit soll der Zugriff darauf geschützt werden.
Auch geschützt werden soll der Missbrauch unseres Internetanschlusses, sodass es eben nicht zu dem Problem der Störerhaftung kommt. Hierfür verwendet Freifunk allerdings VPN, welches den Datenverkehr nicht direkt über den Anschluss des Freifunkknotenbetreibers ins Internet entlässt, sondern an die Freifunkserver übermittelt. So wird das Freifunknetzwerk und das Privatenetzwerk vollständig getrennt und das offene WLAN stellt kein Sicherheitsrisiko mehr dar.

1.3 Übertragungssicherheit

1.3.1 Was bedeutet Übertragungssicherheit?

Bei Übertragungssicherheit geht es darum, dass die Kommunikation zwischen dem Sender und dem Empfanger vor Manipulation und Auslesen geschützt wird. Hierfür wird eine Ende-zu-Ende-Verschlüsselung verwendet. Der meist verwendete Standard nennt sich SSL/TLS.

1.3.2 Wie funktioniert SSL/TLS grundlegend?

SSL (Secure Sockets Layer) ist die ältere Bezeichnung für das heute aktuelle TLS (Transport Layer Security). Hierbei geht es darum, eine verschlüsselte Verbindung zwischen dem Client und dem Server/Dienst aufzubauen. Hierfür wird zunächst ausgehandelt welche Verschlüsselungen beide Seite beherrschen und welche für alles nachfolgende verwendet werden soll. Außerdem wird sichergestellt, dass die Gegenstelle auch wirklich die ist, die man erreichen möchte. Sobald diese Verbindung besteht werden alle Daten vollständig verschlüsselt zwischen den beiden Endpunkten übertragen.

1.3.3 HTTPS - SSL/TLS fürs Web

Mit dieser Technologie ist vermutlich jeder schon eimal in Berührung gekommen. Hierbei handelt es sich um die durch SSL/TLS gesicherte Variante des HTTP Protokolls, welches die gängige Variante ist eine Webseite aufzurufen.
Man erkennt solche verschlüsselten Verbindungen in erster Linie an dem Schlosssymbol im Browser und daran, dass eine Adresse mit https:// beginnt.
Sollte zum Beispiel von einem Browser festgestellt werden, dass eine Webseite nicht die ist, die sie vorgibt zu sein, was durch SSL/TLS überprüft wird, so wird eine große, gut sichtbare Warnung angezeigt.

1.3.4 Wozu brauchen wir SSL/TLS?

SSL/TLS verhindert die Erfassung und Manipulation von Daten, die wir über Netzwerkabschnitte übertragen, die abgehört werden können oder denen wir nicht vertrauen - sei es ein offenes WLAN oder das Internet selbst. Dadurch, dass die Strecke bis zur Anwendung auf beiden Seiten verschlüsselt ist, wird so sichergestellt, dass keine Passwörter oder sensible Daten abgehört oder manipuliert werden können.