CSBW
CYBER
SICHERHEITS
AGENTUR
BADEN-WÜRTTEMBERG

Öffentliche WLAN-Netzwerke & VPN

Die Nutzung öffentlicher WLAN-Netzwerke, beispielsweise in der Bahn oder in Hotels, birgt die Gefahr des Datendiebstahls und der Einschleusung von Schadsoftware. Um die Datenübertragung zu verschlüsseln und damit die Risiken zu minimieren, empfiehlt sich die Nutzung eines Virtual Private Networks (VPN).

Öffentliche WLAN-Netzwerke sind meist **unverschlüsselt**. Andere Nutzende desselben WLAN-Netzwerks können die zwischen Ihrem Endgerät und dem WLAN-Netzwerk übertragenen Daten **abfangen** und/oder **mitlesen**.

Außerdem besteht die Gefahr, dass Ihr Gerät bei Nutzung des unverschlüsselten öffentlichen WLAN-Netzwerks mit Schadsoftware infiziert wird.[1]

Handlungsempfehlungen zur Nutzung öffentlicher WLAN-Netzwerke:[1]

- Nutzen Sie ein Virtual Private Network (VPN).
- Nutzen Sie möglichst nur Webadressen, die mit „**https://**“ beginnen. Diese Seiten übertragen Daten verschlüsselt.
- Deaktivieren Sie die Datei-/Verzeichnisfreigabe bei der Verbindung mit einem WLAN-Netzwerk, so dass der unberechtigte Zugriff auf Daten unmöglich ist.
- Löschen Sie genutzte und gespeicherte öffentliche WLAN-Netzwerke aus Ihren Verbindungen, damit sich das Gerät bei Verfügbarkeit des Netzes nicht automatisch damit verbindet.
- Schalten Sie das WLAN unterwegs nur an, wenn Sie es tatsächlich benötigen.

Öffentliche WLAN-Netzwerke & VPN

Virtual Private Network bedeutet „virtuelles privates Netzwerk“

In einem virtuellen privaten Netzwerk baut das verwendete Endgerät eine Verbindung zu einem VPN-Server auf. Das Endgerät sendet Daten folglich nicht direkt zum Empfänger, sondern stattdessen zum VPN-Server. Dieser leitet die Daten an den Empfänger weiter. Der Datenaustausch zwischen dem Endgerät und dem VPN-Server wird mit einer **Verschlüsselung** geschützt. Diese ermöglicht, dass die Daten von Dritten nur schwer gelesen werden können.[2]

Die Verschlüsselung der Datenübertragung zwischen einem Endgerät, z.B. einem Laptop, und dem VPN-Server funktioniert umgangssprachlich wie eine Art abhörsicherer Tunnel, der durch das ungeschützte Internet führt. Daher wird auch von einem „VPN-Tunnel“ gesprochen. Hierbei werden am Tunneleingang (dem Laptop) alle zu übertragenden Informationen in verschlüsselte Datenpäckchen gepackt, durch den Tunnel sicher übertragen und am Tunnelausgang (VPN-Server) ausgepackt, also entschlüsselt.[2]

Ein weiterer Vorteil ist, dass der Empfänger und Dritte lediglich die **IP-Adresse** des VPN-Anbieters sehen und nicht die des verwendeten Endgerätes.

Eine IP-Adresse ist eine individuelle Zahlenfolge, die jedem mit dem Internet verbundenen Gerät zugewiesen wird und durch die sich das Gerät eindeutig identifizieren lässt.

Wie kann ein VPN-Netzwerk auf Smartphone, Tablet, Laptop & Co. eingerichtet werden?

- Installation einer entsprechenden App auf dem Endgerät. Diese gibt es für alle Betriebssysteme.
- Die App benötigt lediglich die IP-Adresse und die Zugangsdaten des zu nutzenden VPN-Servers.
- Anhand eines kleinen Schlüsselsymbols am Displayrand oder dem Schriftzug „VPN“ signalisiert die App die verschlüsselte Übertragung.

Quellen:
[1] Öffentliche WLAN-Netze sicher nutzen | Verbraucherzentrale.de
[2] BSI - Was ist ein virtuelles privates Netzwerk (VPN)? (bund.de)

CSBW
CYBER SICHERHEITS AGENTUR
BADEN-WÜRTTEMBERG

Weitere Factsheets und Informationen unter:
www.cybersicherheit-bw.de

CSBW Prävention
Kontakt: schulungen@cybersicherheit.bwl.de
Stand: 11.2023