Sicherheit beim Freifunk-WLAN-Netzwerk

Immer wieder kommt die Frage auf: „Wie sicher ist Freifunk?“ In diesem Beitrag möchten die Autoren versuchen, diesen Aspekt näher zu beleuchten.

Für die **Nutzerinnen und Nutzer** lautet die Antwort: Freifunk ist so sicher oder unsicher wie jedes andere Netzwerk auch. Wie bei jeder Verbindung mit dem Internet sollten die Nutzerinnen und Nutzer nur verschlüsselte Verbindungen auf ihrem Endgerät nutzen, um sich und ihre Daten zu schützen. Beispielsweise sollte beim Browsen im WWW immer *https://* statt *http://* verwendet werden.

Für die **Betreiber** von Freifunk-Knoten wollen wir im Folgenden die technischen Hintergründe des Freifunk-Netzes erklären:

Ein Router, der zu einem bestehenden Freifunknetz dazu geschaltet werden soll, muss zunächst mit einer speziellen Freifunk-Software bespielt („geflashed“) werden. Das bedeutet, dass die herstellereigene Software auf dem Router durch eine Freifunk-spezifische Software auf Open-Source-Basis ersetzt wird. Dadurch wird ein handelsüblicher Router zum Freifunk-Knoten.
Bitte beachten Sie, dass nicht alle handelsüblichen Router-Modelle sich zum Freifunk-Knoten eignen.

Ist die Freifunk-Software installiert, erzeugt diese als erstes ein lokales Freifunk-WLAN und baut dann (über einen bestehenden Internet-Anschluss) eine Verbindung zum Internet auf. Diese steht anschließend allen Teilnehmern des Freifunk-WLANs zur Verfügung. So kann jedermann sich mit Freifunk verbinden, und darüber ohne weitere Authentifizierung auch das Internet benutzen.

Dazu muss der Freifunk-Router natürlich mit Ihrem bereits vorhandenen Internet-Router über ein Ethernet-Kabel verbunden werden. Daraus ergibt sich vielleicht die Befürchtung: kennt Freifunk nun meine Zugangsdaten des Providers?
Die Antwort ist einfach: Nein! Ein Freifunk-Router verhält sich wie jedes andere Netzwerk-Gerät, das Sie mit Ihrem Internet-Router verbinden, und nutzt lediglich die zur Verfügung gestellte Verbindung ins Internet.

Um die Datenpakete aus dem Freifunk-Netz nun ins Internet zu routen, sind im Freifunk-Knoten spezielle Routing-Tabellen eingetragen. Der Datenverkehr von Freifunknetz und privatem WLAN oder LAN werden hierdurch getrennt. Aufgrund der Routing-Tabellen kann von Endgeräten im Freifunk-Netz ***keine Verbindung ins private Netzwerk*** aufgebaut werden.

Für den Datenverkehr ins Internet nutzt die Freifunk-Software eigene Netzwerk-Server, sogenannte Freifunk-Gateways, die von der Freifunk-Community betrieben werden. Über diese wird der gesamte Freifunk-Verkehr Ihres Freifunkknotens geleitet, während Ihr privates

Netzwerk weiterhin direkt die Internetwege Ihres Providers (DSL/Kabel/etc.) nutzt. Die Verbindung zum Freifunk-Gateway erfolgt über ein sogenanntes Virtual Private Network (VPN) und ist verschlüsselt. Mit dem VPN haben Sie sozusagen zusätzlich zu Ihrem eigenen Internet-Anschluss eine zweite parallele Verbindung geschaffen, die sich lediglich der Bandbreite Ihres Internet-Anschlusses bedient.

Wird mein Anschluss dadurch langsamer?
Hier muss die Antwort lauten: es kommt darauf an. In der Regel merken Sie bei einem Anschluss mit großer Bandbreite nichts von einer meist kurzzeitigen Nutzung des Freifunk-WLAN-Access-Points.
Sollten Sie sich in Ihrer Arbeit behindert fühlen, so gibt es Einstellungen im Freifunk-Router, die eine Zeit- und/oder Bandbreiten-Beschränkung ermöglichen. Im Notfall schalten Sie den Freifunk-Router einfach aus! Auch können Sie eine Zeitschaltuhr an die Steckdose anschließen, über die der Freifunk-Router seinen Strom bezieht – alles legitime Möglichkeiten, Freifunk nur so viel von Ihren Ressourcen zu geben, wie Sie möchten.

Was passiert, wenn jemand meinen Freifunk-Knoten für illegale Downloads, also Urheberrechtsverletzungen, oder sonstige kriminelle Aktivitäten nutzt?
Hier muss man Strafrecht und Zivilrecht unterscheiden: *strafrechtlich* haftet sowieso immer nur der Täter selbst. Es geht also ausschließlich um *zivilrechtliche* Ansprüche wie Urheberrechtsverletzungen.
Zivilrechtlich wurde früher von einer sogenannten „Störerhaftung“ des WLAN-Anbieters ausgegangen. In 2017 trat jedoch ein neues Telemediengesetz in Kraft, das (vereinfacht) besagt, dass ein Netzanbieter, sei es ein Provider oder der Inhaber eines WLAN-Zugangspunkts, nicht für die rechtswidrigen Handlungen eines Nutzers auf Unterlassung oder Schadensersatz verklagt werden kann. Sie sind also nicht verantwortlich für strafbare Handlungen, die über Ihren Freifunk-Knoten begangen werden. Natürlich sollten Sie die Empfehlungen der Freifunker beachten, wozu z.B. automatische Installation von Software-Updates gehört. Aber das gilt ja auch für Ihre anderen Geräte.
Aufgrund des oben skizzierten technischen Setups (Nutzung von Freifunk-Gateways) wird Ihre eigene IP-Adresse nach außen nicht sichtbar. Stattdessen findet die öffentliche Kommunikation über IP-Adressen von Freifunk statt. Eine Rückverfolgung auf Ihren Anschluss ist vom Netz her grundsätzlich nicht vorgesehen. Es findet keine Vorratsdatenspeicherung statt. Insofern ist es sowieso nahezu ausgeschlossen, dass Sie als Anschlussinhaber überhaupt in den Fokus von Strafverfolgungsbehörden oder zivilrechtlichen Ansprüchen geraten.

Muss jeder Freifunk-Knoten an den Internet-Anschluss angeschlossen werden?
Insbesondere in größeren Einrichtungen wie der Altenpflege oder in Hotels können auch mehrere Freifunk-Knoten zum Einsatz kommen. Nur der erste davon muss am vorhandenen Internet-Router angeschlossen werden. Die anderen können untereinander ein sogenanntes Mesh-Netzwerk aufbauen. Die Geräte müssen dazu lediglich in „WLAN-Sichtweite“ voneinander stehen.

Wenn also ein Freifunk-Access-Point in der Nähe ist, können sich weitere Access Points drahtlos zu einem Mesh-Netzwerk verbinden und so ein unabhängiges Drahtlosnetzwerk für einen WLAN-Zugang über Freifunk untereinander bilden.
Für alle diese Geräte gilt das bisher Gesagte: mit Ihrem Internet-Anschluss teilen sie sich nur die Bandbreite, bauen aber ihre ***eigene Verbindung*** über die bestehende Verbindung auf und bleiben weg von Ihrem hauseigenen Netzwerk!

Gerne können Sie mit uns Kontakt zum Thema aufnehmen:

Andreas Schmidt
Stiftung MedienKompetenz Forum Südwest
schmidta@medienanstalt-rlp.de
+49 6131 279675 (Di, Fr) | Homeoffice: +49 6130 918841 (Mo, Mi, Do)

Freifunk Mainz e.V.
kontakt@freifunk-mainz.de

Quellen:

- https://wiki.freifunk.net/Sicherheit#H.C3.A4ufige_Fragen_zur_Sicherheit_von_Freifunk-Router-Firmware (abgerufen am 27.11.2020)
- https://wiki.freifunk.net/Freifunk-Firmware (abgerufen am 27.11.2020)
- https://www.pcwelt.de/a/freifunk-offenes-wlan-ohne-risiko,3449868 (abgerufen am 27.11.2020)
- https://dejure.org/gesetze/TMG/8.html (abgerufen am 27.11.2020)
- https://www.heise.de/ct/artikel/Freifunk-Alle-Infos-zum-offenen-Netzwerk-zum-Betrieb-und-den-Haftungsrisiken-4607516.html (abgerufen am 27.11.2020)
- Freifunk Mainz e.V., namentlich Florian Altherr (1. Vorsitzender) und Frank Zimmermann, https://www.freifunk-mainz.de/