Freifunk - TK-Anbieter - Starterpaket

History

Version	Datum / Bearbeiter	Beschreibung
0.1beta	30.5.2014, RM	Erstversion
0.2beta	23.6.2014, RM	Hinweis/Korrektur bei Meldepflicht, Reihenfolge geändert, Nummerierung bei Splash-Page korrigiert
0.3beta	14.8.2014, RM	Kleine Ergänzungen im Disclaimer; Ergänzung Meldepflicht (Absicht der Kostendeckung); Ergänzung Person und Anforderungen des Sicherheitsbeauftragten; Ergänzung/Korrektur bzgl. Pflicht zur Vorlage des Sicherheitskonzepts; Kreuz im BNetzA-Formular bei TK-Netzen

Lizenz

Von der Lizenz nicht umfasst ist der Vorschlag für die Splash-Page mit Impressum. An diesem werden keine Rechte geltend gemacht.
Anmerkungen und Vorschläge werden gerne unter Twitter (@offenenetze) oder per Mail gesehen.

Disclaimer / Einleitung

Das folgende „Starterpaket“ soll eine Hilfestellung für Freifunk-WLAN-Knoten bieten und enthält lediglich Vorschläge. Es erhebt keinen Anspruch auf Vollständigkeit und Richtigkeit. Das Starterpaket ist für andere WLANs als Freifunk-Knoten nicht gedacht und ggf. auch nicht geeignet.[1]

Wer einen Freifunk-Knoten aufbaut, sollte die unten dargestellten Punkte durchgehen, die entsprechenden Formulare ausfüllen und ggf. die Meldung an die Bundesnetzagentur absenden. Damit sollten alle regulatorischen Pflichten für den Betrieb eines Freifunk-Knoten erfüllt sein.

Grundlage für das Starterpaket ist:

- Ein „kleiner“ WLAN-Knoten im Freifunk-Netzwerk,
- der eine Splash-Page auf dem WLAN-Router bei Verbindung mit dem Knoten zeigt,
- in dem Daten über die Nutzer (Bestandsdaten) und die Nutzung (Verkehrsdaten) **nicht** erhoben und/oder gespeichert werden, und
- der den Datenverkehr über einen zentralen VPN routet, der ihn ins Internet leitet.

[1] Für weitere Informationen, zu Pflichten etc. bei WLANs s. *Sassenberg/Mantz*, WLAN und Recht – Aufbau und Betrieb von WLAN-Hotspots, Berlin 2014, http://www.wlan-recht.de.

Inhalt

1. Beispiel Splash-Page mit Impressum und Informationen

Wenn eine Splash-Page vorgehalten wird, muss diese ein Impressum mit den Pflichtangaben des § 5 Telemediengesetz (TMG) enthalten. Außerdem sollte die Splash-Page Informationen „zum Dienst“ vorsehen. Dazu gehört insbesondere, ggf. auf Einschränkungen des Dienstes (z.B. Portsperren, ZAPP-Skript) hinzuweisen. Eine Belehrung der Nutzer, rechtswidrige Handlungen zu unterlassen, ist empfehlenswert.
Der folgende Text ist an die tatsächlichen Gegebenheiten anzupassen.[2] Der Abschnitt über Beschränkungen kann bspw. bei Bedarf gestrichen werden. Das Impressum kann alternativ über einen Link mit der Bezeichnung „Impressum“ auf eine allgemein im Internet verfügbare Webseite mit den entsprechenden Angaben zur Verfügung gestellt werden.

Willkommen ,

Du bist mit dem WLAN-Netzwerk .freifunk.net verbunden. Bei Freifunk handelt es sich um (s. auch http://freifunk.net).

Ein Zugang ins Internet ist über dieses Netz möglich, da einige Freifunker/Freifunkerinnen ihren Breitband-Zugang zur Verfügung stellen. Du teilst das WLAN und die Breitband-Zugänge mit anderen Nutzern. Das bedeutet auch, dass über die Verfügbarkeit des WLANs und des Zugangs zum Internet keine Zusage getroffen werden kann.

Bitte sei Dir dieser Umstände bewusst und verhalte Dich entsprechend.

Insbesondere darfst Du das WLAN nicht verwenden, um rechtswidrige Handlungen zu begehen, z.B. Verletzungen des Urheberrechts durch Filesharing von geschützten Werken.

Wir bitten Dich außerdem

1. alle Filesharing-Programme abzuschalten,
2. keine unnötigen Downloads oder Streams zu starten.

Das WLAN dieses Freifunk-Knotens ist unverschlüsselt. Du solltest daher bei sensitiven Informationen (insb. Passwörtern, z.B. beim Mailabruf) selbst für Verschlüsselung sorgen.

Der Zugang ins Internet über diesen Freifunk-Knoten ist zusätzlich eingeschränkt, nämlich

- ☐ sind die Ports gesperrt,
- ☐ ist das sog. ZAPP-Skript aktiv, d.h. es sollte nach kurzer Zeit erkannt werden, wenn Du trotz unserer Bitte Filesharing nutzt; Du wirst dann zeitweise über einen Proxy ins Internet geleitet, der Filesharing unterbindet,
- ☐ ...

[2] Der Text der Splash-Page basiert auf der Splash-Seite von Freifunk Leipzig, http://wiki.leipzig.freifunk.net/DHCP_Splash.

Impressum
Name des Betreibers mit Vorname
Bei Unternehmen ggf. Rechtsform, Vertretungsberechtiger, Registernummer, Umsatzsteueridentifikationsnummer, Aufsichtsbehörde
Anschrift
E-Mail-Adresse
Telefonnummer

Aufsichtsbehörde: Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen, Tulpenfeld 4, 53113 Bonn, Telefon: 02 28/14-0, Fax 02 28/14-88 72, www.bundesnetzagentur.de

2. Sicherheitskonzept / Sicherheitsmaßnahmen (und Beispiel)

Der Betreiber eines Freifunk-Knotens muss gewisse technische Schutzmaßnahmen ergreifen und ein Sicherheitskonzept erstellen, § 109 Abs. 1, 4 Telekommunikationsgesetz (TKG). Das Sicherheitskonzept muss der Bundesnetzagentur vorgelegt werden, unabhängig von der Anmeldung nach § 6 TKG. Wenn eine Anmeldung erforderlich ist, dann ist es mit der Anmeldung vorzulegen. „In der Schublade“ zum Vorzeigen auf Verlangen der Bundesnetzagentur reicht vermutlich nicht (anders als noch in v0.2 des Starterpakets ausgeführt! Die Frage ist bisher nicht geklärt, nach dem Gesetzeswortlaut aber wohl eher eine Pflicht zur Vorlage, s. auch *Mantz*, Rechtsfragen offener Netze, S. 63 ff.).

⇨ Siehe Anlage 1

Die Anlage ist als Beispiel zu betrachten und sollte an die konkrete Anlage angepasst werden. Bei Bedarf kann die Netzstruktur auch von Hand aufgemalt und dem Sicherheitskonzept beigelegt werden.

3. Benennung Sicherheitsbeauftragter

Der Betreiber eines Freifunk-Knotens muss einen Sicherheitsbeauftragten benennen, § 109 Abs. 4 TKG. An den Sicherheitsbeauftragten werden keine allzu hohen Anforderungen gestellt. Er sollte ein „Mindestmaß an technischem Verständnis“ mitbringen und die Anlage kennen und erklären können. Der Betreiber kann gleichzeitig der Sicherheitsbeauftragte sein.
Der Sicherheitsbeauftragte ist nicht verantwortlich für Meldung, Sicherheitskonzept etc. Pflichten, die mit dem Aufbau eines Freifunk-Knotens einhergehen, treffen allein den Betreiber, nicht den Sicherheitsbeauftragten. Der Sicherheitsbeauftragte ist z.B. gegenüber der Bundesnetzagentur keinen Weisungen oder Risiken ausgesetzt.

⇨ Siehe Anlage 2

4. Anmeldung Bundesnetzagentur (nur bei „gewerblichem WLAN“)

Anbieter gewerblicher TK-Dienste, wozu auch Anbieter von gewerblich betriebenen WLANs gehören, sind verpflichtet, dies bei der Bundesnetzagentur zu melden (§ 6 TKG). Dies gilt allerdings **nicht** für Freifunk-Knoten, die aus rein altruistischen Motiven zur Verfügung gestellt werden (zur Motivation bei Freifunk-Netzen *Mantz*, Rechtsfragen offener Netze, S. 16). Daher ist eine Anmeldung **nicht** erforderlich bei reinen Freifunk-Knoten (dazu *Sassenberg/Mantz*, WLAN und Recht, Rn. 30).

Dient der Freifunk-Knoten auch der Kundengewinnung bzw. –bindung, z.B. in einem Café, dann muss hingegen eine Anmeldung abgegeben werden. Die relevante Fragestellung hierfür ist, ob eine (ggf. teilweise) Kostendeckung durch Kundengewinnung oder –bindung beabsichtigt ist. **Werbung** mit einem freien WLAN („Hier kostenloses WLAN“, „Free WiFi“ etc.) im Café o.ä. kann ein Indiz für die Absicht der Kostendeckung sein.

Für die Meldung stellt die Bundesnetzagentur ein Formular zur Verfügung, das zwingend verwendet werden muss.[3]

- ⇨ Siehe Dokument „Meldeformular_Bundesnetzagentur_vorausgefüllt_v0.3.doc“. Es handelt sich um ein für Freifunk-Knoten vorausgefülltes Meldeformular der Bundesnetzagentur auf dem Stand vom 28.05.2014. Das Dokument ist mit den Angaben des Betreibers zu ergänzen.

[3] http://www.bundesnetzagentur.de/cln_1432/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Anbieterpflichten/Meldepflicht/meldepflicht-node.html

Anlage 1: Beispiel Sicherheitskonzept / Beschreibung der TK-Anlagen

Dokumentinformation
Historie:

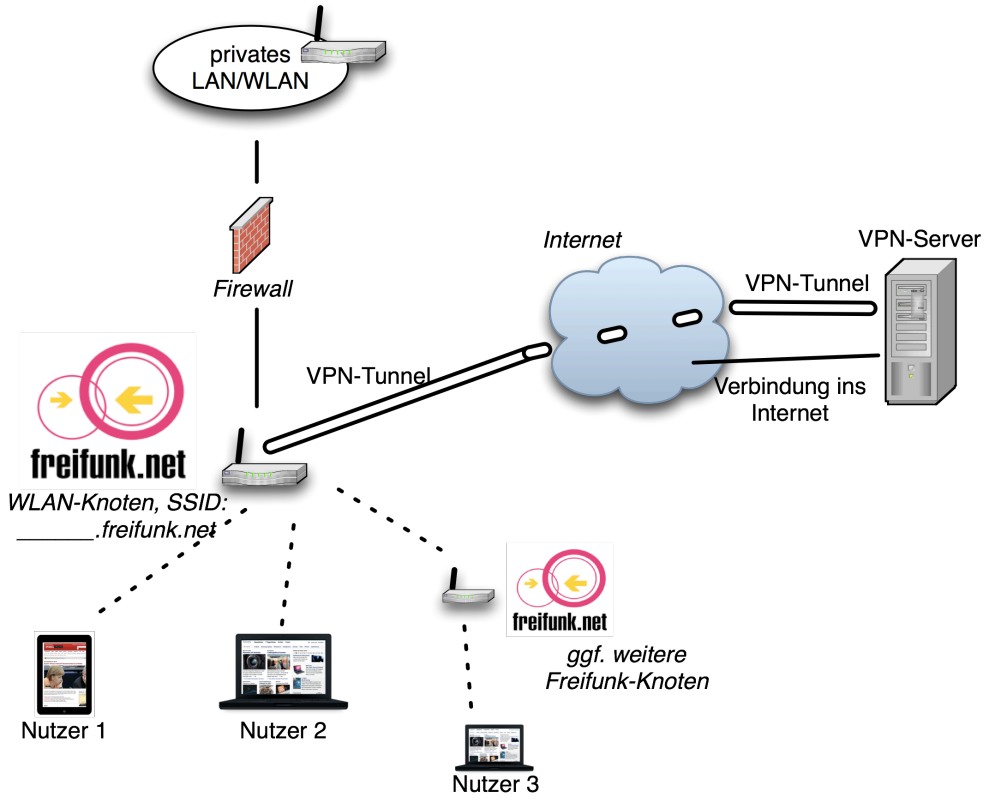
Version	Datum / Bearbeiter	Beschreibung
1.0	,	Erstversion
	,	

Ansprechpartner: *(z.B. Sicherheitsbeauftragter)*

Beschreibung der Anlage
Die Anlage dient der Gewährung von Internetzugang per WLAN für die Nutzer. Der WLAN-Router kann mit anderen Freifunk-Knoten vermesht sein. Zusätzlich besteht ein VPN-Tunnel zu , über den der aus- und eingehende Datenverkehr der Nutzer geleitet wird.

Firmware-Version des WLAN-Routers:
Firmware wird automatisch aktualisiert: ☐
Standort:

Netzstruktur (vereinfachte Darstellung)



Sicherheitsmaßnahmen

- WLAN-Router ist

☐ aufgrund seines Aufstellungsorts an/auf/bei
☐ durch eine wetterfeste Box
☐ durch (*Blitzschutzmaßnahmen etc.*)
☐

gegen Umwelteinflüsse geschützt.

- WLAN-Router ist gegen physischen Zugriff durch unbefugte Dritte durch

  - ☐ Aufstellung im abgeschlossenen Raum
  - ☐ Aufstellung an/auf/bei
  - ☐ durch ständige Sichtkontrolle
  - ☐ durch eine Installation in einer verschlossenen Box

  geschützt.
- Administrationsseite des WLAN-Routers ist nicht über das WLAN, sondern nur lokal über LAN zugänglich.
- Administrationsseite des WLAN-Routers ist durch ein selbst vergebenes, hinreichend langes Passwort geschützt. Dieses ist nur / dem Sicherheitsbeauftragten bekannt.
- Funktionsfähigkeit des WLAN-Routers wird durch / den Sicherheitsbeauftragten in regelmäßigen Abständen von Tagen / Wochen, z.B. durch Sichtkontrolle oder Test der Funktionalität, überprüft. Eventuelle Störungen werden unmittelbar behoben.
- / der Sicherheitsbeauftragte überprüft in regelmäßigen Abständen von Wochen / Monaten, ob eine neue Version der Router-Firmware vorliegt und installiert diese bei Bedarf; *alternativ*: Firmware wird automatisch aktualisiert.
- Nutzer werden durch eine Splash-Page auf die fehlende Verschlüsselung des WLANs und die Möglichkeit der Sicherung durch eigene Verschlüsselung hingewiesen.

Anlage 2: Ernennung zum Sicherheitsbeauftragten

Ernennung zum Sicherheitsbeauftragten (§ 109 Abs. 4 TKG)

Herr/Frau .....

wird für .....
(Name und Anschrift der Firma / des Betreibers)

zum Sicherheitsbeauftragten für den/die Freifunk-Knoten ..... ernannt.

Ort, Datum .....
(Unterschrift des Betreibers)

Ort .....
(Unterschrift des Sicherheitsbeauftragten)

§ 109 TKG: Technische Schutzmaßnahmen
(4) 1Wer ein öffentliches Telekommunikationsnetz betreibt oder öffentlich zugängliche Telekommunikationsdienste erbringt, hat einen Sicherheitsbeauftragten zu benennen und ein Sicherheitskonzept zu erstellen, aus dem hervorgeht,
1.welches öffentliche Telekommunikationsnetz betrieben und welche öffentlich zugänglichen Telekommunikationsdienste erbracht werden,
2.von welchen Gefährdungen auszugehen ist und
3.welche technischen Vorkehrungen oder sonstigen Schutzmaßnahmen zur Erfüllung der Verpflichtungen aus den Absätzen 1 und 2 getroffen oder geplant sind.
2Wer ein öffentliches Telekommunikationsnetz betreibt, hat der Bundesnetzagentur das Sicherheitskonzept unverzüglich nach der Aufnahme des Netzbetriebs vorzulegen. 3Wer öffentlich zugängliche Telekommunikationsdienste erbringt, kann nach der Bereitstellung des Telekommunikationsdienstes von der Bundesnetzagentur verpflichtet werden, das Sicherheitskonzept vorzulegen. 4Mit dem Sicherheitskonzept ist eine Erklärung vorzulegen, dass die darin aufgezeigten technischen Vorkehrungen und sonstigen Schutzmaßnahmen umgesetzt sind oder unverzüglich umgesetzt werden. 5Stellt die Bundesnetzagentur im Sicherheitskonzept oder bei dessen Umsetzung Sicherheitsmängel fest, so kann sie deren unverzügliche Beseitigung verlangen. 6Sofern sich die dem Sicherheitskonzept zugrunde liegenden Gegebenheiten ändern, hat der nach Satz 2 oder 3 Verpflichtete das Konzept anzupassen und der Bundesnetzagentur unter Hinweis auf die Änderungen erneut vorzulegen. 7Die Bundesnetzagentur kann die Umsetzung des Sicherheitskonzeptes überprüfen.