Ich habe für die Linksfraktion im Rat der Stadt am 31.08.2014 zusammen mit Reiner Gutowski von der PiPa-Gruppe eine Pressemitteilung zu der Möglichkeit von freiem und kostenlosen WLAN in Mönchengladbach raus gegeben. Der Antrag dazu ist gemeinsam von den Fraktionen DIE LINKE, Bündnis90/Grüne und der Gruppe Piraten-PARTEI gestellt. Zu unser Verwunderung kamen in kurzer Zeit ein paar Nachfragen zur Sicherheit im freien WLAN.

Genau diesen Punkt hatten wir nach längerer Diskussion aus der PM raus gelassen, da wir diesen Punkt nicht nur in einem kleinen Absatz hätten darstellen können. Um es auch nur Ansatzweise richtig zu Formulieren müssen da mehrere Aspekte im Detail erklärt werden. Außerdem hatten erwartet, dass dies Thema zu sehr ins technische geht und viele LeserInnen überfordert oder gar langweilt. Wie die Nachfragen zeigen war diese Einschätzung falsch. Deswegen hier ein paar Worte von mir dazu. Weiter könnt ihr auch einen taz Artikel lesen in dem Reiner Gutowski etwas dazu gesagt hat (Absatz "Steigende Zentralisierung"). Nun aber erstmal die wohl wichtigsten Aspekte zur Sicherheit:

**- Für den "User", also den, der sich ins freie WLAN einloggt:**
Grundsätzlich müssen die Datenpakete die durchs Internet geschickt werden als "Postkarten" angesehen werden. Es gibt zich Stellen, an denen sie Mitgelesen werden können. Wer das nicht will muss eine Verschlüsselung zwischen "Sender" und "Empfänger" nutzen. Für Webseiten wäre das zum Beispiel das HTTPS Protokoll (noch normal ist nur HTTP). Dies muss der Betreiber der Webseite anbieten, dann ist das kein Problem. Bei Emails gibt es die Verschlüsselung der Email (z.B. PGP etc). Diese erfordert ein ganz wenig Aufwand und muss zwischen jedem einzelnen Sender und Empfänger angewendet werden. Für Verbindungen wie FTP oder die Verbindungen zu ihrem Emailprovider (SMTP / POP3 /IMAP) gibt es auch entsprechend verschlüsselte Protokolle. Werden diese vom Anbieter angeboten ist deren Nutzung kein Problem, jedoch garantieren sichere SMTP / POP3 /IMAP Verbindungen nicht zwangsläufig, dass die Email an sich nicht gelesen werden kann. Dafür MUSS die zuvor genannte Email verschlüsselung angewandt werden.
**FAZIT zu diesem Punkt:** Das freie WLAN ist genauso unsicher wie das ganze Internet.

**- noch mal für den "User", also den, der sich ins freie WLAN einloggt:**
Freifunk setzt ab dem Punkt des WLAN, wo sich der User Einloggt bis zu dem Punkt, wo die Daten dem "normalen" Internet übergeben werden eigene Tunnel und Verschlüsselungen ein. Also ist die Gefahr von staatlicher Seite oder von einem Provider oder gar von dem Betreiber des jeweiligen Freifunkrouter abgehört zu werden deutlich geringer als bei einem herkömmlichen Zugang. Diese Gefahr besteht eben erst ab dem Punkt wo die Daten ins "normale" Internet gehen und an dieser Stelle ist eine Zuordnung der Daten zum User deutlich erschwert.
**FAZIT:** An diesem Punkt ist Freifunk sicherer, aber 100% Sicher gibt es nicht.

**- Für den Betreiber eines Freifunk-Router:**
Das Netz des Freifunk-Router wird trotz gemeinsamer Leitung ins Internet getrennt. Somit ist es nach derzeitigem Stand ausgeschlossen, dass das heimische WLAN oder heimische LAN durch Freifunk angegriffen wird. Da ist es wahrscheinlicher, dass direkt das eigene WLAN gehackt wird. Aber auch hier gilt: 100% Sicherheit gibt es nicht.
**FAZIT:** Jeder Internetanschluss kann entweder aus dem Internet oder über das heimische WLAN angegriffen werden. Der zusätzliche Freifunkrouter erhöht diese Gefahr nicht, ist aber rein theoretisch ein dritter Angriffspunkt. Aber dieser dritte Punkt ist besser gesichert, als die üblichen heimischen Anschlüsse.

Diese drei Punkte sollten den Sicherheitsaspekt von den wichtigsten Stellen her erläutern. Aber es gibt ja auch noch die "rechtliche Sicherheit" für die Betreiber, dabei geht es um die sogenannte Störerhaftung. Im Antrag steht dazu etwas, aber auch in meiner ersten PM "Freies WLAN ist mehr als nur öffentlich"
.