SICHERHEIT

WLAN FÜR ALLE – aber sicher?

Ein offenes Funknetz gibt vielen Menschen Zugang zum Internet, doch wie steht es um die Sicherheit? Die Risiken sind beherrschbar, wenn Nutzer und Betreiber übliche Vorsichtsmaßnahmen treffen.

Dass öffentliche Funknetze im Prinzip verwundbar sind, zeigte der amerikanische Entwickler Eric Butler im Jahr 2010. Er entwickelte das Programm „Firesheep", das automatisch den Datenstrom anderer Nutzer eines solchen Funknetzes abhören konnte. Hunderttausende luden das Programm herunter; auch um die Sicherheit bei sich selbst zu überprüfen. Mit dem Programm ließen sich die Benutzerkonten von Diensten wie Twitter, Facebook und Amazon übernehmen, die Webdienste mussten eilig nachbessern.

Verschlüsselung bei Webdiensten keine Ausnahme mehr

Die gute Nachricht: Im Zeitalter nach Edward Snowden sind viele Angriffe nicht mehr so einfach wie vor ein paar Jahren. Viele Anbieter haben Verschlüsselung in ihr Standard-Repertoire übernommen. Trotzdem müssen sowohl Betreiber als auch Nutzer eines offenen Netzes Vorsichtsmaßnahmen treffen, um ihre Sicherheit zu gewährleisten. Das fängt bei den üblichen Sicherheitsmaßnahmen an, die auch für jeden anderen Internetanschluss zu Hause gelten: Die neuesten Sicherheitsaktualisierungen sollten ständig installiert werden, besonders auf Windows-Computern empfiehlt sich der Einsatz von Antiviren-Programmen; man sollte Rechner und Benutzerkonten mit guten Passwörtern schützen.

In einem offenen Funknetz entfällt jedoch eine Vorsichtsmaßnahme, die jedem Nutzer zu Hause sonst empfohlen wird: Das Einschalten der WLAN-Verschlüsselung, die die Funkverbindung mit einem Passwort absichert und damit für Außenstehende unlesbar macht. Es liegt in der Idee eines offenen Netzes, dass die WLAN-Gastgeber auf ein solches Passwort verzichten.

Google, Amazon und sogar Wikipedia verschlüsseln heute ihren Datenverkehr komplett und schließen damit zufällige Daten-Schnüffler weitgehend aus. Andere Anbieter verschlüsseln lediglich kritische Daten wie Passwörter und Kreditkarteninformationen. Browser wie Chrome und Firefox zeigen mit einem kleinen Schloss-Symbol in der Adressleiste an, wenn eine Webseite verschlüsselt ist. Fehlt das Schloss, kann die Kommunikation im Prinzip mitgelesen werden, wenn keine anderen Vorsichtsmaßnahmen getroffen werden. Der Datenstrom enthält Informationen wie aufgerufene Webseiten, übertragene Bilder, gegebenenfalls auch ganze E-Mails.

VPN: Der Tunnel im Netz – auch für mehr Sicherheit

Auch verschlüsselte Webseiten geben mitunter Daten Preis. Hacker sind einfallsreich: Statt Usernamen und Passwort direkt abzugreifen, können sie zum Beispiel versuchen, die Cookies zu übernehmen, kleine Dateien, mit denen ein Browser sich gegenüber einem Anbieter automatisch ausweisen kann. Auch so kann ein Angreifer an einen fremden Account gelangen.

Ein Mittel, um solche Lauscher auszuschließen, ist der Aufbau einer weiteren Verschlüsselungs-Schicht. Sogenannte „Virtual Private Networks" – kurz: VPN – bauen einen verschlüsselten Tunnel auf, durch den der komplette Datenstrom fließt. Solche VPN-Tunnel sind in freien Funknetzen vielfältig einsetzbar. So können die Endnutzer eine verschlüsselte Verbindung nach Hause, in ihr Firmennetzwerk oder zu einem kommerziellen VPN-Anbieter aufbauen und sind so auch ohne WLAN-Verschlüsselung vor Mitlauschern geschützt.

Viele Freifunk-Netze benutzen intern ebenfalls solche VPN-Tunnel. So werden die Daten etwa im Köln-Bonner Netz über ein dezentrales VPN geleitet. Hier dient es dem Schutz des Betreibers der Zugangspunkte. Wenn ein Freifunk-Nutzer unzulässiges Filesharing betreibt, taucht auf einer etwaigen Abmahnung dann nicht die IP-Adresse des WLAN-Gastgebers auf, sondern die des zentralen Freifunk-Zugangs. Andere freie Funknetze leiten den kompletten Datenverkehr ins Ausland, um die Unsicherheit bei der Störerhaftung (siehe S. 33) auch für den Betreiber selbst zu umgehen. Nachteil der VPN-Verlängerungen: Alle Nutzer müssen sich die Bandbreite des Datentunnels teilen. Dies kann zu längeren Ladezeiten führen, zeitkritische Anwendungen wie Internettelefonie oder Livestreams sind mitunter nicht mehr möglich.

»

Die Gewährleistung eines Internetzugangs gehört zur Daseinsvorsorge. Mein langfristiges Ziel lautet: Wo öffentlicher Raum ist, soll auch ein öffentliches WLAN sein. Freifunk kann hierzu einen wichtigen Beitrag insbesondere dort leisten, wo erlösorientierte Modelle versagen.

Björn Böhning, Chef der Berliner Senatskanzlei

«