Unterwegs im öffentlichen WLAN – aber gut geschützt

Öffentliche WLANs sind eine praktische Sache, besonders, wenn sie wie bei Freifunk (http://freifunk.net/worum-geht-es/technik-der-community-netzwerke/) von einem Anbieter unabhängig sind und die Nutzung nichts kostet. Unterwegs, im Café, beim Warten am Bahnhof oder Flughafen oder gar während des Bummels in der Stadt Zugriff aufs Netz, ohne das Mobilfunkbudget zu belasten: Das freut viele Anwender. Allerdings sind sich Viele aber auch nicht klar darüber, dass mit öffentlichen WLANs und dem Zugang zum Netz über öffentliche Hotspots auch Gefahren verbunden sind. Wer sich des Risikos jedoch bewusst ist, kann einschätzen, was geht und was nicht - und auch Gegenmaßnahmen ergreifen, die das Online-Leben über ein öffentliches WLAN praktisch so sicher machen wie übers heimische Netz.

Vertrauenssache

Grundsätzlich gilt: In einem öffentlichen WLAN können Sie niemanden vertrauen und müssen davon ausgehen, dass eingehende sowie ausgehende Daten von anderen Nutzern des Netzwerks mitgelesen werden können. Wer Zugriff auf denselben Hotspot hat wie Sie selbst, kann prinzipiell auch die gesamte Kommunikation mitlesen, die über ihn läuft. Und um den Notebook-User im Café zu belauschen, der gerade in Facebook unterwegs ist oder sein Bankkonto checkt, muss man kein Netzwerk-Spezialist mehr sein. Ein einfaches Smartphone mit der passenden App genügt.

Diese Apps machen auch komplizierte Netzwerktechnik für jeden verfügbar: Der nette Junge mit dem Smartphone am Nebentisch fährt eine Man-in-the-Middle-Attacke via ARP-Spoofing – selbst wenn er keinen blassen Schimmer davon hat, was es mit dem Address Resolution Protocol (ARP) auf sich hat. Dann geht es auch nicht mehr um einfaches Mitlesen, sondern um die Extraktion und Nutzung von sicherheitsrelevanten Daten – so wird dann möglicherweise der Facebook-Account gekapert oder die Banking-Anwendung übernommen (http://www.heise.de/ct/artikel/Die-Hotspot-Falle-1394646.html).

Erschreckt? Man muss sich von solchen Szenarien nicht ins Bockshorn jagen lassen. Wer bislang im Internet offen kommuniziert hat, etwa seine E-Mails unverschlüsselt verschickte, kann das natürlich auch über ein öffentliches WLAN tun. Man muss sich nur

Hinweis zur Verwendung: Meinung des unabhängigen Gutachters Jürgen Kuri, stellv. Chefredakteur c't - magazin für computertechnik / heise online im Auftrag der Staatskanzlei NRW. Dieser Text ist zum Vervielfältigen und Verbreiten freigegeben unter der Creative-Commons-Lizenz Namensnennung-Keine Bearbeitung 3.0 Deutschland (CC BY-ND 3.0 DE. Details siehe https://creativecommons.org/licenses/by-nd/3.0/de/ Bei der Nutzung sind anzugeben: Autor, Auftraggeber und Lizenz (Bezeichnung und URL).

immer bewusst sein, dass verschickte Daten im Zweifelsfall mitgelesen werden – und kann sich möglicherweise darauf einstellen und nur solche Daten übertragen, die man auch auf eine Postkarte schreiben würde. Sobald es aber an sensible Daten geht, etwa Passwörter oder vertrauliche Informationen, muss man sich vorsehen: Es gibt Vorsichts- und Gegenmaßnahmen, mit denen man auch in einem öffentlichen WLAN weitgehend sicher unterwegs ist.

Beim Stichwort E-Mail fiel bereits das entscheidende Schlagwort: Verschlüsselung (Kryptographie). Sind die im WLAN übertragenen Daten verschlüsselt, ist jeder Mitlauscher machtlos, er sieht nur Datenmüll und kann ihn bei starker Kryptographie auch nicht entschlüsseln. Verschlüsselung in einem öffentlichen WLAN kann man auf verschiedenen Ebenen realisieren – mit unterschiedlicher Komplexität und unterschiedlichem Aufwand für Sie als Anwender.

Wege zum Ziel

Die einfachste Methode nennt sich Transport-Verschlüsselung. Einfach zumindest für Sie als Anwender: Sie müssen nur darauf achten, dass bei der Kommunikation mit einer Website oder einem Online-Dienst der sichere Kommunikationsweg per https gewählt wird. Wenn Sie mit Ihrer Bank per Netz kommunizieren, sollten Sie sowieso immer darauf achten, die per https erreichbare Seite aufzurufen, die meisten Institute lassen für das Online-Banking schon gar keinen anderen Weg mehr zu. Die modernen Browser zeigen die Aktivierung des verschlüsselten Transportwegs auch nicht nur durch die Webadresse https://… an, sondern blenden ein Schlüsselsymbol in die Adresszeile ein.

Auch viele E-Mail-Provider bieten Transportverschlüsselung an. Nutzen Sie einen Webmailer im Browser, wählen Sie ebenfalls den Zugang per https. Setzen Sie ein Mail-Programm ein, sind für einen verschlüsselten Transport gesonderte Einstellungen notwendig: In der Konfiguration der Software muss man den Mailtransfer per SSL beziehungsweise TLS auswählen sowie die zugehörige Authentifizierungsmethode (meist per Passwort). Die notwendigen Informationen stellen die Provider bereit – viele unterstützen Transportverschlüsselung allerdings nur in den kostenpflichtigen Versionen der Mail-Zugänge.

Viele andere Online-Dienste, etwa Facebook, bieten ebenfalls den gesicherten Zugang im Webbrowser per https. Wann immer möglich, sollte man diese Methode auswählen. Das gilt nicht nur beim Zugang über ein öffentliches WLAN. Auch wenn Sie im heimischen WLAN auf Dienste im Internet zugreifen, sichert Transport-Verschlüsselung ihre Kommunikation. Denn auch wenn ihr WLAN daheim geschlossenen und verschlüsselt ist, laufen auf den weiteren Transport-Etappen im Internet die Daten unverschlüsselt, sofern Sie nicht selbst dafür sorgen.

App as App can

Sind Sie mit dem Smartphone oder Tablet unterwegs, können Sie solche Möglichkeiten

für Online-Dienste und E-Mails natürlich prinzipiell auch nutzen. Schwieriger wird es mit den Apps, etwa fürs Instant Messaging oder Chatten. Bei diesen sind Sie darauf angewiesen, dass Verschlüsselung von den Apps selbst vorgenommen wird – was oft nicht der Fall ist. Dann müssen Sie sich selbst entscheiden, ob Ihnen die Vertraulichkeit der Kommunikation so wichtig ist, dass Sie lieber nicht über ein öffentliches WLAN kommunizieren.

WhatsApp zum Beispiel unterstützte lange Zeit gar keine Verschlüsselung der Kommunikation. Derzeit (September 2015) bietet WhatsApp Verschlüsselung der Nachrichten nur in der Version für Smartphones mit Googles System Android, wie es beispielsweise Samsung-, HTC- oder Sony-Smartphones einsetzen. Da Sie aber in WhatsApp nicht erkennen können, welche Systemversion Ihr Gesprächspartner einsetzt, sind Sie über die verschlüsselte Kommunikation in WhatsApp nie wirklich sicher.

Anders ist es mit Chat- und Messaging-Clients, die von Haus aus verschlüsseln. Der bekannteste Vertreter dieser Gattung ist Threema, die wichtigsten Vertreter aus dem Open-Source-Lager sind Telegram und TextSecure. Auch iMessage bietet die Verschlüsselung der Nachrichten, die zwischen den Kommunikationspartnern ausgetauscht werden – allerdings gibt’s das nur für Apple-Systeme. Die Alternativen zu WhatsApp haben alle einen entscheidenden Nachteil: Meist sind Ihre Gesprächspartner per WhatsApp problemlos zu erreichen, da sie es eh nutzen. Von alternativen Messengern müssen Sie Ihre Kontakte in der Regel erst einmal überzeugen und zur Installation überreden.

Mit anderen Apps sieht es bei der Nutzung in öffentlichen WLANs oft problematisch aus. Sie selbst als Anwender oder Anwenderin können in den seltensten Fällen beurteilen, ob sensible Daten etwa bei Apps mit Online-Bezahlfunktion wirklich verschlüsselt übertragen werden. Einige Unternehmen versprechen hier Verbesserungen, etwa Apple mit dem für iOS 9 angekündigten App Transport Security. Aber das ist derzeit nur ein Versprechen. Unabhängig davon können Sie schon gar nicht beurteilen, ob die App wirklich so fehlerfrei ist, dass nicht etwa Kriminelle damit Schindluder treiben können. Bei wichtigen Anwendungen, die mit Account-Informationen und Bezahlsystemen verbunden sind, sollten Sie daher in jedem Einzelfall überlegen, ob es wirklich schlau ist, sie in einem öffentlichen WLAN einzusetzen.

Ende-zu-Ende

Die Verschlüsselung der zu übertragenden Daten direkt in den Anwendungen bezeichnet man oft als Ende-zu-Ende-Verschlüsselung. Sie hat gegenüber der Transportverschlüsselung den Vorteil, dass tatsächlich nur Sie und Ihr Kommunikationspartner an die Daten herankommen – bei der Transportverschlüsselung dagegen kann natürlich der Online-Dienst beziehungsweise Mail-Provider selbst mitlesen, da er für die Entschlüsselung der Daten vor der Zustellung an den Empfänger sorgt. Das ist für Sie bequem, aber eben nicht hundertprozentig sicher.

Bei Ende-zu-Ende-Verschlüsselung dagegen werden die Daten beim Sender verschlüsselt und erst vom Empfänger wieder entschlüsselt. Dies wird heutzutage über sogenannte asynchrone Verschlüsselung realisiert: Jeder Anwender hat zwei Schlüssel, einen privaten und einen öffentlichen. Will Ihnen jemand eine verschlüsselte Nachricht schicken, verschlüsselt er sie mit Ihrem öffentlichen Schlüssel. Entschlüsselt werden kann diese Mail nur mit Ihrem privaten Schlüssel – den auch nur Sie kennen sollten. Die Schlüssel sind komplizierte Software-Konstrukte, die Systeme wie PGP für Sie erstellen: Den privaten Schlüssel behalten Sie gut geschützt bei sich, den öffentlichen Schlüssel geben Sie an ihre Freunde und Bekannten weiter. Dies kann auch über öffentliche Schlüssel-Server geschehen, sodass jeder, der Ihnen eine verschlüsselte Mail schicken will, Ihren öffentlichen Schlüssel einfach erfahren kann.

Für Windows-Systeme ist Gpg4Win (http://www.gpg4win.de) das System der Wahl, um Mail-Verschlüsselung mittels PGP zu realisieren. Es gibt unter anderem Plug-Ins für Outlook und den sehr verbreiteten Mail-Client Thunderbird (https://www.enigmail.net/download/). Für Mac-Nutzer gibt es die GPG Suite (https://gpgtools.org), unter iOS können Sie iPGMail (https://ipgmail.com/) einsetzen. Für Tablets und Smartphones mit Android können Sie beispielsweise auf OpenKeychain (http://www.openkeychain.org/about) in Zusammenarbeit mit dem Mail-Programm K9 zurückgreifen. Alle diese Tools wollen die Einrichtung und Bedienung recht unkompliziert machen, sind aber nicht wirklich einfach. Im Zweifelsfall sollten Sie sich Hilfe bei einem netzaffinen Bekannten holen, um die Verschlüsselung für Ihr E-Mail-System einzurichten.

Für Webmailer gibt es bislang allerdings keine einfache Möglichkeit, Ende-zu-Ende-Verschlüsselung zu realisieren. Einige Anbieter, darunter United Internet mit GMX und Web.de, bieten mittlerweile Tools für PGP auch im Webmailer an. Ist dies bei Ihrem Mail-Provider nicht der Fall, sollten Sie überlegen, auf einen klassischen Mail-Client wie Thunderbird zu wechseln beziehungsweise eine Mail-App im Smartphone oder Tablet einzurichten, mit der sich verschlüsselte Kommunikation realisieren lässt.

Grundschutz

Mail-Verschlüsselung und anderer Schutz direkt in den Anwendungen kann aber nicht alle Informationen vor Mitlauschern verstecken. Die eigentlichen Inhalte einer Mail beispielsweise sind dann zwar verschlüsselt, nicht aber die Transportinformationen. Wer mit wem wann E-Mails ausgetauscht hat, ist immer noch sichtbar und kann möglicherweise bei vertraulicher Kommunikation Informationen liefern, die man eben nicht in die Öffentlichkeit posaunen möchte.

Aber Ende-zu-Ende-Verschlüsselung kann man nicht nur mit den Anwendungen realisieren. Mittels einer Art verschlüsseltem Netz im Netz wird jedweder Datenverkehr, der Ihr Smartphone, ihr Tablet oder ihr Notebook verlässt, schon vor der Übergabe an das Netz verschlüsselt und erst beim Empfänger wieder entschlüsselt. Der Fachbegriff: Virtual Private Network (VPN). Als Anwender oder Anwenderin sind Sie sicher, dass jedwede Kommunikation, alle Daten verschlüsselt sind. Sie haben aber auch weit mehr

Konfigurationsaufwand und müssen damit leben, dass ein VPN (http://www.heise.de/netze/artikel/Hotspot-aber-sicher-221475.html) auch einiges an Rechenleistung von Ihrem Gerät verlangt.

Mittels VPN kann man bei Bedarf sogar gefahrlos auf das heimische Netz per öffentlichem WLAN und Internet zugreifen – Voraussetzung ist natürlich, dass man zu Hause einen VPN-Server installiert hat und einen VPN-Client mit den zugehörigen Zugangsdaten auf dem Mobilgerät. Viele Büros und Firmen realisieren so den Zugang von Mitarbeitern auf das interne Netzwerk über das Internet. Trauen Sie sich etwas Einrichtungs- und Konfigurationsarbeit zu, bekommen Sie so einen sicheren Zugang zum eigenen Netzwerk von überall auf der Welt – und können von dort aus dann wieder ins Internet, ohne dass Sie ein unliebsamer Zeitgenosse vom Nebentisch aus belauscht. Die Software der Wahl für solche Zwecke dürfte OpenVPN (https://openvpn.net/) unter Linux sein. Wer allerdings zu Hause eine Fritz!Box für den Internet-Zugang einsetzt, kann einfach deren VPN-Funktion nutzen.

Dass die Einrichtung eines eigenen VPNs nicht Jedermanns oder Jederfraus Sache ist, haben schnell auch Dienstleister gemerkt. Sie können auch VPN als Online-Dienst bekommen – mit einem VPN-Client auf Tablet, Smartphone oder Notebook verbinden Sie sich dann über das öffentliche WLAN mit dem VPN-Server des Dienstleisters. Dieser funktioniert als eine Art Gateway, mit dem Sie komplett verschlüsselt kommunizieren – und das dann die Daten an das eigentlich gewünschte Ziel weiterleitet. Im Unterschied zum selbst eingerichteten VPN muss man hier aber dem Anbieter vertrauen, dass er mit den Daten sicher umgeht und sich keine Schludrigkeiten leistet – was auch nach den Tests von c't nicht immer gewährleistet ist.

Gesunde Skepsis, sorgenfreie Nutzung

Wie man es auch dreht und wendet: Jeder Nutzer kann seine Kommunikation über ein öffentliches WLAN für viele Anwendungsfälle gut absichern. Wer nur ein wenig Surfen will, um sich die Zeit zu vertreiben und sich nicht daran stört, wenn ihm dabei jemand über die Schulter schaut, kann das getrost auch am öffentlichen Hotspot tun und braucht nicht einmal besondere Vorsichtsmaßnahmen.

Bei Kommunikation, die Sie vielleicht lieber vertraulich halten wollen, sollten Sie auf jeden Fall zu Verschlüsselung greifen – wie weit man das treibt und ob man bis zu einem VPN geht, bleibt dem eigenen Sicherheitsbedürfnis vorbehalten. Bei personalisierten Daten, deren unerlaubte Weitergabe schmerzen würde, sollten Sie sehr genau darüber nachdenken, ob Sie für diesen Zweck nicht doch auf die Mobilfunkverbindung ausweichen – besonders, wenn es um so wichtige Daten wie den Zugang zum Online-Banking geht, sollten Sie nur im Notfall außerhalb ihres eigenen Netzzugangs operieren. Aber auch im heimischen Netzwerk ist Ihre Kommunikation nur so sicher, wie Sie sie gestalten – Verschlüsselung, fortwährend auf den neusten Stand aktualisierte Software, Schutz gegen Schadprogramme sind auch Zuhause gute Hilfsmittel dafür.

Wenn Sie diese Vorsichtsmaßnahmen beachten, steht einem einfachen und komfortablen Online-Leben unterwegs über öffentliche WLANs und über den Freifunk nichts im Wege.

Weitergehende Informationen:

- Freifunk: Die Technik der Community-Netzwerke
http://freifunk.net/worum-geht-es/technik-der-community-netzwerke/

- Freie Funknetze in der Praxis – Broschüre mit Einführung, Hintergrund und Geschichte zu Freifunk von der Medienanstalt Berlin-Brandenburg
http://www.mabb.de/files/content/document/Publikationen/Freifunk-Broschuere/freifunk_publikation_webversion.pdf

- Die Hotspot-Falle: Gefahren in öffentlichen Funknetzen
http://www.heise.de/ct/artikel/Die-Hotspot-Falle-1394646.html

- Cool bleiben am Hotspot: Maßnahmen zur sicheren WLAN-Nutzung
http://www.heise.de/artikel-archiv/ct/2012/01/088_Cool-bleiben-am-Hotspot

- Das Bestiarium: Angriffe auf Hotspot-Nutzer
http://www.heise.de/artikel-archiv/ct/2012/01/082_Das-Bestiarium

- Hotspot, aber sicher: Funknetze unterwegs mit VPN benutzen ohne Abhörgefahr
http://www.heise.de/netze/artikel/Hotspot-aber-sicher-221475.html

- Gespräche im Flüsterton: Verschlüsselnde Messenger-Apps im Alltagseinsatz
http://www.heise.de/ct/ausgabe/2015-13-Test-Verschluesselnde-Messenger-Apps-im-Alltagseinsatz-2662824.html

- Mitleser-Sperren: Alternative Dienste für komfortable und abhörsichere Mail-Kommunikation
http://www.heise.de/ct/ausgabe/2015-13-Test-Alternative-Dienste-fuer-komfortable-und-abhoersichere-Mail-Kommunikation-2661636.html

- Virtuelle Privatsphäre: So viel Schutz bieten VPN-Dienste
http://www.heise.de/ct/ausgabe/2013-20-Test-So-viel-Schutz-bieten-VPN-Dienste-2314876.html

- Gpg4Win und GnuPG – PGP für Windows
http://www.gpg4win.de/

- Enigmail – PGP-Plugin für Thunderbird
https://www.enigmail.net/download/

- iPGMail – PGP für iOS
https://ipgmail.com/

- GPG Suite – PGP für Mac OS X
https://gpgtools.org/

- OpenKeychain – PGP für Android
http://www.openkeychain.org/about/

- OpenVPN – Open-Source-VPN für Alle
https://openvpn.net/