CB Übersetzung 315-15STK Orig.FR

Se déplacer dans le WiFi public – mais en toute sécurité

Les WiFi publics sont très pratiques en particulier s'ils ne dépendent pas d'un fournisseur comme chez Freifunk (http://freifunk.net/worum-geht-es/technik-der-community-netzwerke/) et que l'utilisation est gratuite. Avoir accès au réseau en déplacement, au café, pendant l'attente à la gare ou à l´aéroport et même en flânant en ville sans débiter le compte de téléphonie mobile: Cela réjouit beaucoup d'utilisateurs. Cependant beaucoup ne se rendent pas compte qu'il y a des dangers liés aux WiFi publics et à la connexion au réseau par le biais de bornes publiques. Mais celui qui est conscient du risque peut estimer ce qui va et ce qui ne va pas et prendre aussi des mesures conséquentes qui rendent la vie online via un WiFi public pratiquement aussi sûre que chez soi.

Question de confiance

En principe vous ne pouvez-vous fier à personne dans le WiFi public et devez partir du principe que d'autres utilisateurs du réseau peuvent lire aussi bien vos données entrantes que sortantes. Quiconque a accès à la même borne que vous-même peut en principe intercepter toute la communication qui se déroule grâce à cette borne. Et pour épier l'utilisateur d'un notebook dans un café qui surfe sur Facebook ou vérifie son compte en banque on n'a plus besoin d'être un spécialiste. Un simple Smartphone avec l'application adaptée suffit.

Ces applications rendent même une technique de réseau compliquée accessible à tous: Le garçon sympa avec son Smartphone à la table d'à côté est en train de mener une Man-in-the-Middle-attaque via ARP-Spoofing, même s'il n'a pas la moindre idée de ce qu'il en est au juste avec la Adress Resolution Protocol (ARP). Là il ne s'agit plus d'une simple lecture mais de l'extraction et l'utilisation de données de sécurité importantes- ainsi il est possible de pirater le compte Facebook et d'intercepter l'application bancaire. (http://www.heise.de/ct/artikel/Die-Hotspot-Falle-1394646.html)

Cela vous fait peur? Il ne faut pas se laisser intimider par de tels scénarios. Quiconque a jusqu'à présent communiqué ouvertement sur Internet, comme par exemple envoyé ses mails non cryptés peut bien entendu continuer à le faire également dans le WiFi public, cependant il faut toujours bien garder à l'esprit que les données envoyées peuvent être lues- on peut donc s'y préparer en conséquence et ne transmettre que des données que l'on écrirait soi-même sur une carte postale. Mais dès qu'il s'agit de données sensibles, par exemple des mots de passe et des informations confidentielles, alors là il faut se méfier: Il existe des mesures de précaution et des contre-

mesures grâce auxquelles on peut se déplacer à peu près en sécurité dans un espace WiFi public.

En parlant de e-mails, le mot clé est tombé: cryptage (cryptographie). Si les données transmises dans le WiFi public sont cryptées, alors un tiers mal intentionné ne peut rien faire, il ne voit que des données inutiles qui sont parfaitement cryptées et qu'il ne peut pas décoder. On peut réaliser un cryptage dans le WiFi public à plusieurs niveaux- cela signifie pour vous en tant qu'utilisateur que la complexité et les efforts varient.

Chemins à suivre

La méthode la plus simple est appelée le cryptage du transport. Enfin c'est simple au moins pour vous en tant qu'utilisateur. Il faut simplement que vous preniez soin de choisir le chemin de communication sûr passant par https quand vous êtes en communication avec un site web ou un service en ligne. Si vous êtes en communication avec votre banque en ligne, vous devriez toujours veiller à accéder à la page au moyen de https, de toute manière la plupart des banques n'autorisent plus d'autres moyens pour le e-banking. Les navigateurs modernes montrent que le transport crypté est activé non seulement par l'adresse Web https://... mais aussi par le symbole d'un cadenas s'affichant dans la barre d'adresse.

Beaucoup de fournisseurs d'e-mail proposent le cryptage du transport. Utilisez un webmail depuis un navigateur et sélectionnez aussi l'accès par https. Si vous installez un programme mail, il faut mettre au point des paramètres spéciaux pour le cryptage du transport. Dans la configuration du logiciel il faut sélectionner le transfert Mail per SSL voire TLS ainsi que la méthode d'authentification

correspondante (le plus souvent par mot de passe). Les fournisseurs mettent les informations nécessaires à votre disposition – la plupart cependant encouragent le cryptage du transport seulement dans les versions payantes des accès aux mails.

Beaucoup de services en ligne, comme par exemple Facebook, proposent également l'accès sécurisé dans le navigateur par le biais de https. Il faut choisir cette méthode à chaque fois que c'est possible. Cela n'est pas seulement valable pour l'accès par le WiFi public. Même si vous accédez aux services Internet par votre WiFi personnel, le cryptage du transport rend votre communication sûre. Car même si votre WiFi chez vous est fermé et sécurisé, les données se promènent non sécurisées durant d'autres étapes du transport sur Internet, dans la mesure où vous ne vous en occupez pas vous-mêmes.

App as App can

Si vous vous déplacez avec votre Smartphone ou tablette, vous pouvez en principe utiliser également ces possibilités pour les services en ligne et e-mails. Mais c'est plus difficile avec les applications, comme Instant Messaging ou Chatten. Dans ces cas vous dépendez des applications qui doivent elle-même prendre en charge le cryptage, ce qui n'est pas souvent le cas. C'est alors à vous de décider si la confidentialité de votre communication est telle que vous préférez communiquer sans passer par un WiFi public.

Pendant longtemps WhatsApp par exemple n'a encouragé aucun cryptage de la communication. En ce moment (septembre 2015) WhatsApp propose un chiffrement des messages seulement dans la version pour Smartphones avec Googles System Android, comme l'utilisent par exemple les Smartphones Samsung, HTC et Sony. Mais comme vous ne pouvez pas reconnaitre chez WhatsAppp la version du système utilisé par vos interlocuteurs, vous n'êtes

jamais vraiment en sécurité en passant par la communication cryptée de WhatsApp.

La situation est différente avec Chat- et Messaging-clients qui cryptent d'eux-mêmes. Le représentant le plus connu de ces services est Threema, les partenaires principaux du camp «open source» (code source ouvert) sont Telegram et TextSecure. iMessage offre également le cryptage des messages qui sont échangés entre les interlocuteurs, mais seulement pour le système Apple. Les alternatives à WhatsApp ont un inconvénient majeur: La plupart du temps vos interlocuteurs sont facilement joignables sur WhatsApp car ils utilisent ce système de toute manière. Pour ce qui est des messageries alternatives, il vous faut d'abord en règle générale convaincre vos contacts et les persuader d'installer ces messageries.

Souvent les autres applications présentent des problèmes lors de l'utilisation dans les WiFi publics. Vous-même en tant qu'utilisateur ou utilisatrice pouvez difficilement juger si les des données sensibles par exemple dans des applications payantes sont vraiment transmises de manière sécurisée. A ce sujet certaines entreprises ont promis des améliorations comme par exemple Apple avec l'App Transport Security annoncée pour iOS9. Mais pour le moment ce n'est qu'une promesse. Indépendamment de cela, vous ne pouvez déjà pas juger si l'application est vraiment dénuée de défauts, et si des tiers mal intentionnés ne peuvent pas en abuser. Lors d'applications importantes qui exigent des informations sur votre compte en banque et des systèmes de paiement vous devez réfléchir et décider au cas par cas s'il est intelligent de les utiliser dans un WiFi public.

Principe de bout-à-bout

Le chiffrement des données à transmettre qui a lieu directement dans les applications est appelé chiffrement bout-

à-bout. Par rapport au cryptage du transport, il a l'avantage que seuls vous-même et votre interlocuteur ont vraiment accès aux données. Par contre, lors du cryptage de transport le service en ligne voire le fournisseur de messagerie peuvent bien entendu lire vos messages car ils s'occupent du déchiffrement des données avant la notification aux destinataires. C'est certes pratique pour vous, mais ce n'est pas sûr à 100%. En revanche lors du chiffrement bout-à-bout, le chiffrement des données est effectué dans le système émetteur et le déchiffrement ne se fait que dans le système récepteur. Aujourd'hui cela se fait grâce à un chiffrement dit asynchrone: Tout utilisateur a deux clés, une privée et une publique. Ce mail ne peut être déchiffré qu'avec votre clé privée – que seul vous-même devez connaître. Les clés sont des constructions logicielles compliquées que des systèmes tels PGP réalisent pour vous. Vous conservez la clé privée bien en sécurité chez vous et vous donnez la clé publique à vos amis et connaissances. Cela peut se faire aussi via des serveurs publics de clés de telle sorte que toute personne qui veut vous envoyer un mail crypté peut connaitre facilement votre clé publique.

Pour les systèmes Windows, Gpg4Win (http://www.gpg4win.de) est le système de choix pour réaliser le chiffrement des messages avec PGP. Il existe entre autres des Plug-Ins pour Outlook et le client de messagerie Thunderbird (https://www.enigmail.net/download/). Pour les utilisateurs de Mac il y a la suite GPG. (https://gpgtools.org), avec iOS vous pouvez utiliser iPGMail (https://ipgmail.com). Pour tablettes et Smartphones avec le système Android vous pouvez par exemple utiliser OpenKeychain (http://www.openkeychain.org.about) qui fonctionne avec le Programme Mail K9. Tous ces outils ont certes pour but de simplifier l'installation et l'utilisation mais ne sont pas

vraiment simples. En cas de doute vous devriez avoir recours à l'aide d'un ami spécialiste pour mettre au point le chiffrement de votre système e-mail.

Il est vrai que pour Webmailer il n'y a jusqu'à présent pas de moyen simple pour réaliser un chiffrement de bout-à-bout. Certains fournisseurs comme United Internet, GMX et web.de proposent maintenant des outils pour PGP également dans le Webmailer. Si cela n'est pas le cas chez votre fournisseur de messagerie, alors vous devriez envisager de passer à un client de messagerie classique comme Thunderbird, ou bien d'installer une application Mail dans votre Smartphone ou tablette, avec laquelle on peut réaliser une communication chiffrée.

Protection de base

Le cryptage des e-mails et une autre forme de protection directement dans les applications ne peuvent cependant pas dissimuler aux tiers mal intentionnés toutes les informations. Les véritables contenus d'un mail par exemple sont certes cryptés mais pas les informations du transport. On peut toujours voir avec qui et quand des e-mails ont été échangés, ainsi lors d'une communication confidentielle des informations peuvent être révélées que l'on n'a pas forcément envie de divulguer au public.

Mais on peut réaliser un chiffrement bout-à-bout pas qu'avec des applications. Avec une sorte de réseau crypté tout trafic de données qui quitte votre Smartphone, tablette ou notebook est déjà crypté avant d'être transmis au réseau et ne sera déchiffré que chez le récepteur. Le terme technique est le Réseau Privé Virtuel (VPN). En tant qu'utilisateur ou utilisatrice vous pouvez être sûr(e) que toute communication et toute donnée sont cryptées, mais vous avez beaucoup plus de travail de configuration et devez-vous accommoder du fait

qu'un VPN (http://heise.de/netze/artikel/Hotspot-aber-sicher-221475.html) exige une grande performance de la part de votre appareil.

Avec le VPN on peut, si besoin est, avoir accès sans danger à son propre réseau par le WiFi public et Internet, à condition bien sûr que l'on ait installé chez soi un serveur-VPN et un VPN-Client avec les données d'accès correspondantes sur le portable. De nombreux bureaux et entreprises permettent ainsi l'accès de leurs collaborateurs au réseau interne via internet. Si vous sentez capables de faire un peu de travail d'installation et de configuration, vous obtiendrez alors un accès sécurisé à votre propre réseau où que vous soyez dans le monde- et de-là vous pourrez avoir toujours accès à Internet sans que quelqu'un ne vous espionne depuis la table d'à côté. Le logiciel de choix devrait être pour cela OpenVPN (https://openvpn.net) avec Linux. Mais si vous utilisez chez vous une Fritz!Box pour accéder à Internet, vous pouvez alors simplement utiliser sa fonction VPN.

Les prestataires de service se sont vite rendu compte que l'installation d'un VPN personnel n'est pas l'affaire de tout le monde. Vous pouvez également obtenir VPN par service en ligne - et avec un VPN-client sur tablette, Smartphone ou Notebook vous vous connectez par le biais du WiFi public au serveur-VPN du prestataire de service. Celui-ci fonctionne comme une sorte de passerelle, avec laquelle vous communiquez de manière complètement cryptée et qui transmet ensuite les données au lieu choisi. A la différence du VPN que l'on installe soi-même, il faut donc avoir confiance en son fournisseur qui se doit de traiter les données de manière sûre et ne se permettre aucun écart, ce qui n'est pas toujours le cas comme le démontrent les tests de c't.

Une saine prudence et une utilisation sans soucis

Quel que soit l'angle sous lequel on analyse la situation: tout utilisateur est en mesure de bien sécuriser sa communication par WiFi public pour de nombreux cas d'application. Celui qui ne veut que surfer un peu pour se passer le temps et que cela ne dérange pas d'être espionné, peut donc bien le faire depuis une borne publique et n'a pas besoin de mesures de précaution particulières.

En ce qui concerne une communication que vous désirez traiter de manière confidentielle, vous devez absolument avoir recours à un cryptage – jusqu'à quel point et s'il faut aller jusqu'à un VPN, tout cela dépend de votre propre besoin de sécurité. En ce qui concerne des données personnalisées dont la transmission illégale vous ferait souffrir, vous devriez bien réfléchir si dans ce cas-là il ne serait pas préférable de vous rabattre sur un réseau mobile – en particulier quand il s'agit de données importantes comme l'accès à l'e-banking, vous ne devriez opérer hors de votre propre accès au réseau qu'en cas de force majeure, mais même dans votre propre réseau à la maison la sécurité de votre communication dépend de votre installation – cryptage, un logiciel toujours actualisé, une protection contre des logiciels malveillants sont également de bons remèdes chez soi.

Si vous observez ces mesures de précaution, rien ne viendra troubler une vie en ligne simple et confortable en déplacement via le WiFi public et les points d'accès Freifunk.

De plus amples informations:

-Freifunk: la technique des réseaux de la Community

http://freifunk.net/worum-geht-es/technik-der-community-netzwerke

- Des réseaux sans fil dans la pratique- Brochure avec introduction, arrière-plan et histoire du réseau sans fil de l'autorité des médias de Berlin-Brandebourg http://www.mabb.de/files/content/document/Publikationen/Freifunk-Broschuere/freifunk publication webversion.pdf

- Le piège de la borne: Dangers dans les réseaux publics http://www.heise.de/ct/artikel/Die-Hotspot-Falle-1394646.html

- Rester cool à la borne: Mesures pour une utilisation WiFi sûre http://www.heise.de/artikel-archiv/ct/2012/01/088 Cool-bleiben-am-Hotspot

- Le Bestiaire: attaques aux utilisateurs de bornes http://heise.de/artikel-archiv/ct/2012/01/082 Das-Bestiarium

- Une borne sûre: utiliser en déplacement des réseaux avec VPN sans risque d'être écouté http://www.heise.de/netze/artikel/Hotspot-aber-sicher-221475.html

- Chuchotements: Les applications Messenger réalisent des chiffrements au quotidien http://www.heise.de/ct/ausgabe/2015-13-Test-Verschlüsselnde-Messenger-Apps-im-Alltagseinsatz-2662824.html

- Bloquer la lecture par des tiers: Services alternatifs pour une communication e-mail confortable et sans interception http://www.heise.de/ct/ausgabe/2015-13-Test-Alternative-Dienste-fuer-komfortable-und-abhoersichere-Mail-

Kommunikation-2661636.html

- Vie privée virtuelle: une grande protection offerte par les services VPN
  http://www.heise.de/ct/ausgabe/2013-20-Test-So-viel-Schutz-bienten-VPN-Dienste-2314876.html

- Gpg4Win et GnuPGP-PGP pour Windows
  http://www.gpg4win.de/

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

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

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

- OpenKeyChain – PGP pour Android
  http://www.openkeychain.org/about

- OpenVPN – Open-Source-VPN pour tous
  https://openvpn.net