Johannes Rundfeldt

Handout zum Fachgespräch vertrauliche Kommunikation im Deutschen Bundestag am 03.09.2013

Session 4
Sicheres und anonymes Surfen

Dieses Handout soll Ihnen einige wenige wichtige Hinweise geben zur verschlüsselten Kommunikation im Internet. Haben Sie keine Angst, dieses Handout ist darauf ausgelegt, dass Sie keine Vorkenntnisse benötigen.

Einfache Verschlüsselung im Browser
Sie haben bestimmt schon mal in Ihrem Browser die Adresszeile angeschaut. Egal was dort steht, die ersten Buchstaben sind immer: **http://...**
Wenn Sie auf einer Website Informationen eintragen, z.B. Ihren Benutzernamen und Passwort, achten Sie darauf, dass in Ihrer Adresszeile dann immer: **https://...** steht. Dies heißt für Sie, dass die Daten zwischen Ihrem Browser und dem Webserver (der Ihnen die Website liefert) leicht verschlüsselt übertragen werden. Wollen Sie Daten in einer Website eintragen und diese operiert nicht per https, dann probieren Sie, ob Sie die Adresse (URL) dahingehend verändern können (das „s“ eintragen). Geht dies auch nicht, sehen Sie am besten von der Nutzung dieses Anbieters ab.

Gefahrensituationen
- öffentliche WLANs (Hotel, Coffeeshop, Messegelände..)
- Internetzugang im Ausland
- Kommunikation über Internetzugänge, deren Betreiber Sie nicht kennen oder kein Vertrauen zu dem Betreiber haben
- anonymer Zugriff auf zensierte oder regional beschränkte Websiten

Lösungen zur Verringerung der Gefahr dieser Szenarien
Öffentliche WLANs sind eine große Gefahr, da die Kommunikation an mehreren Stellen vollständig mitgeschnitten werden kann. Der einzige Weg ist, die Kommunikation zwischen Ihrem Rechner und dem Internet zu verschlüsseln. Dafür gibt es verschiedene Werkzeuge.

Tor (The Onion Router) https://www.torproject.org/
Tausende Privatpersonen bieten automatisiert an, Ihren Datenverkehr zu anonymisieren. Ihre Daten werden durch eine Kette von zufälligen Computern transportiert und innerhalb dieser Kette bis zum Endpunkt der Kette (dem sogenannten „Exit-Node“) verschlüsselt. Auf diese Weise kann Ihr Name nicht mehr Ihrer Internetadresse zugeordnet werden und Internetüberwachung ist nahezu unmöglich. Tor ist kostenlos, die verfügbaren Datenübertragungsgeschwindigkeiten variieren stark und können manchmal sehr langsam sein.

Mit der Tor-Software können Sie beliebige Daten beliebiger Programme sicher und anonym übertragen. Für den Hausgebrauch wird es meistens ausreichen, lediglich einen Internetbrowser durch Tor zu routen. Hierfür gibt es fertig vorbereitete Browserpakete, z.B. auf Basis des populären Browsers „Firefox“ https://www.torproject.org/projects/torbrowser.html.

VPN-Services http://www.deutscher-vpn.de/anbieter/
Ein VPN ist ein virtuelles privates Netzwerk. Dabei werden Ihre Daten durch einen hochverschlüsselten Tunnel zu dem VPN-Server übertragen und gelangen erst von dort in das offene Internet. Ein Zugriff auf den Datenverkehr innerhalb des Tunnels ist unmöglich. Das Tunnelende kann in einem beliebigen Land liegen, so können z. B.. regionale Beschränkungen (China, Gema-YouTube-Konflikt) temporär aufgehoben werden. Internetüberwacher können lediglich das Ende des Tunnels feststellen, nicht aber den Anfang. VPN-Services sind meistens kostenpflichtig, aber deutlich schneller, als z. B. Tor.