Surfen im ICE ist sicherer als in vielen öffentlichen Netzen.

MICHAEL PETERSON, DB-Vorstand

VORSICHT bei der Nutzung öffentlicher W-LAN-Netze!

FOTOS: DEUTSCHE BAHN AG

Durch die Röhre

W-LAN – Ob am Flughafen, im ICE oder in der Innenstadt: Die Zahl der Gratis-Internetzugänge wächst. Gut für Geschäftsreisende. Doch zugleich steigt damit die Gefahr der Datenspionage.

TEXT: SILKE LIEBIG-BRAUNHOLZ

Eine unendliche Vielzahl an Daten auf ebenso unendlich vielen Verbindungen schwirrt in öffentlichen W-LAN-Netzen umher. Mit etwas Geschick sind diese Daten für jedermann greifbar – und manipulierbar. Und eine „Datenpolizei" gibt es genauso wenig wie Sicherheitskontrollen oder Grenzstationen. Die klare Warnung von IT-Experten lautet deshalb: möglichst verschlüsselte Verbindungen nutzen und bei sensiblen Firmendaten höchste Vorsicht walten lassen.

Mit der Änderung des Telemediengesetzes wurde eine erste Grundlage geschaffen, um für die Betreiber öffentlicher W-LAN-Netze mehr Rechtssicherheit zu schaffen. Soll heißen: Die Haftungsrisiken etwa für Hotels oder Cafés werden weiter gesenkt: Die Netzanbieter werden von sämtlichen Kosten für Gerichtsprozesse befreit, wenn Gäste über das W-LAN-Netz gegen geltendes Recht verstoßen. Das soll die Internetzugänge auch für Reisende noch einfacher machen.

Tatsache ist, Gratis-W-LAN-Hotspots sprießen derzeit aus dem Boden: vor allem in den Metropolregionen, in Hotels, Cafés, Einkaufszentren, im öffentlichen Nahverkehr, auf Bahnhöfen, in Zügen und Flughäfen. Für Geschäftsreisende ist das genauso verlockend wie für Kriminelle, die fremde Handys und Rechner mit sensiblen Firmendaten ausspionieren.

Zugänge locken Kriminelle

Statistiken zeigen: Menschen auf Reisen werden doppelt bis viermal so häufig Opfer von Cyber-Kriminalität wie andere. Aus Kontakten mit Antiviren-Herstellern ist dem Bundesamt für Sicherheit in der Informationstechnik bekannt, dass im Februar 2016 auf mindestens 80.000 Endgeräten in Deutschland Schadprogramme mit sogenannter Identitätsdiebstahlfunktion installiert waren – ohne das Wissen der Nutzer natürlich. Daneben nimmt die Vernetzung unter Geräten, Sensoren und Netzwerken täglich zu und bildet eine weitere Gefahrenstelle.

Mittlerweile spricht nicht nur die IT-Branche vom Internet der Dinge, wenn es um Begriffe wie „Smart City" oder „Smart Home" geht, mit denen Städte und Wohnungen technisch fortschrittlich gesteuert werden sollen. Doch die Risiken, dass Kriminelle hier dazwischenfunken, sind enorm. Daher gilt es, Wege zu finden, wie Datentüren möglichst verschlossen gehalten werden können.

Der Bundesverband Informationswirtschaft, Telekommunikation und neue Medien warnt generell vor der Installation von Viren und Schadprogrammen durch Dritte in öffentlichen Netzwerken. Vorbeugen lässt sich durch eingeschränkte Benutzerrechte wie Passwörter. Außerdem sollten Surfer die Verbindungsdauer stets so kurz wie möglich halten. „Je kürzer die Surf-Dauer in öffentlichen Hotspots, umso geringer die Chance eines Angriffs für Hacker", sagt Verbandsmanager Maurice Shahd.

Acht Surf-Tipps

1. Nutzen Sie nur vertrauenswürdige Hotspots.
2. Wählen Sie den Hotspot manuell aus.
3. Richten Sie die Bildschirmsperre ein.
4. Surfen Sie möglichst kurz.
5. Installieren Sie den neuesten Webbrowser.
6. Aktivieren Sie Ihren Virenscanner.
7. Verschlüsseln Sie Ihren Zugang durch einen VPN-Tunnel.
8. Bevorzugen Sie https-gesicherte Seiten.

Zudem sollte man den Hotspot immer manuell auswählen. „Eine automatische Verbindungsaufnahme durch das Betriebssystem ist nicht zu empfehlen", so Shahd. Und: „Nutzer sollten sich nur mit Hotspots verbinden, die sie für vertrauenswürdig halten und vor der Nutzung des öffentlichen Internetzugangs auf jeden Fall alle nicht benötigten Funkverbindungen wie Bluetooth deaktivieren."

Um Firmendaten zu schützen, sollten Unternehmen außerdem eigene Sicherheitsvorkehrungen schaffen. Dazu zählen die Verwendung des neuesten Webbrowsers und verschlüsselter Verbindungsprotokolle. „Auch sogenannte Virtual Private Networks, kurz VPN, bieten eine gute Möglichkeit, um Daten bei der Übertragung im Internet zu verschlüsseln", erläutert Shahd. „Viele Anbieter offerieren so genannte VPN-Tunnel in guter Qualität und zu günstigen Preisen." Doch Vorsicht: Nur wenige VPN-Apps sind sicher!

Dies empfiehlt auch Thorsten Bittner, Manager IT Network Product Solution beim Frankfurter Flughafen. „Wir raten allen Reisenden, die das öffentliche W-LAN nutzen, die Verbindung von ihrem Endgerät über einen VPN aufzubauen."

Stichwort VPN

Ein VPN (virtuelles privates Netzwerk) ist im klassischen Sinne ein in sich geschlossenes Kommunikationsnetz: Mitarbeiter greifen über ihren Computer aufs Firmennetz zu. Im erweiterten Sinne handelt es sich bei VPN um einen **VERSCHLÜSSELTEN FERNZUGRIFF AUF UNTERNEHMENSDATEN**. Sogenannte „Mobile IP VPN" ermöglichen dies auch bei Handys und Notebooks. Angeboten werden sie von den großen Telekommunikationsdienstleistern wie der Telekom. Sie schützen weitgehend vor **UNBERECHTIGTEM ZUGRIFF**; die Authentifizierung der Anwender geschieht über die Handy-Nummer oder per Benutzername und Passwort.

Anbieter wie die Telekom geben dazu umfangreiche Tipps. Allerdings warnt auch Bittner davor, dass unverschlüsselte Daten von Reisenden, die sich im öffentlichen W-LAN im Terminal 1 und 2 und in den Bussen auf dem Vorfeld einloggen, mitgelesen werden können. Diesem Sicherheitsrisiko kann auch der Flughafen nicht vorbeugen. Denn: „Zuhause muss sich ein mobiles Endgerät zunächst mit einem W-LAN-Zugangspunkt verbinden, bevor es im Internet surfen kann", erklärt Bittner. „Diese Verbindung kommt erst zustande, wenn in das Endgerät ein Passwort eingetragen wurde. Dann sind auch die Daten verschlüsselt. In einem öffentlichen Netz ist dieses Vorgehen nicht möglich." Denn dann müsste jeder Passagier das Passwort kennen, was es wiederum auch jedem ermöglichen würde, die Daten mitzulesen. „Daher wird das W-LAN nicht verschlüsselt, und wir empfehlen, die Verschlüsselung durch einen individuellen VPN umzusetzen", so der IT-Experte.

VPN auch in der Bahn

Die Deutsche Bahn hat mit der Aufrüstung der gesamten ICE-Flotte auf neueste W-LAN-Technik einige Sicherheitsvorkehrungen getroffen. „Wir haben zusammen mit unserem Zulieferer Icomera Merkmale eingebaut, die das Surfen im ICE deutlich sicherer machen als in Netzwerken, die in Cafés und öffentlichen Bereichen zu finden sind", sagt DB-Marketingvorstand Michael Peterson. Dazu gehöre die sogenannte IP Client Isolation, die ein unbemerktes Zugreifen von einem auf den anderen W-LAN-Nutzer verhindere.

Doch Zweifel bleiben. „Wir können nicht garantieren, dass die Verbindungen komplett sicher sind und Kommunikationsverbindungen nicht aufgefangen werden können", räumt die DB ein. „Fahrgäste sind allein verantwortlich für den Einsatz von Sicherheitsmaßnahmen." Auch die Bahn empfehle deswegen die Nutzung von VPN-Tunneln, das Aktivieren des Virenscanners und das Surfen auf https-gesicherten Seiten.

Noch allerdings haben sich VPN-Tunnel kaum durchgesetzt. So verweist Filip Chytry vom Sicherheits-Software-Produzenten Avast auf eine von ihm erstellte Umfrage. So nutzen nur 9 Prozent der Deutschen einen VPN-Tunnel – obwohl 71 Prozent in frei zugänglichen W-LAN-Netzen surfen, für die weder Registrierung noch Passwort nötig sind.

Auch Chytry warnt eindringlich, dass derartige öffentliche W-LAN-Netze eine der Hauptgefahren für die IT-Sicherheit darstellen. Eine Bedrohung, die von Nutzern – auch Geschäftsreisenden – in der Regel völlig unterschätzt wird.