Öffentliches WLAN

https://www.beobachter.ch/konsum/multimedia/offentliches-wlan-der-spion-im-starbucks

Er schaut nach links, er schaut nach rechts. Dann öffnet Andriu Isenring seine Ledertasche. Zwischen Kabelgewirr und Geldbeutel steckt ein handgrosses Gerät: schwarz, quadratisch, mit stumpfen Antennen auf beiden Seiten. Er drückt einen Knopf, ein Lämpchen blinkt. «Es geht los», sagt er und reibt die Hände.

An diesem Mittwochnachmittag sitzen mehrere Dutzend Leute im «Starbucks» beim Zürcher Hauptbahnhof. Einige arbeiten an ihrem Laptop, andere surfen mit dem Smartphone über das im Café angebotene kostenlose Netzwerk im Internet. Keiner ahnt, was Isenring mit ihren Geräten anstellen wird. Und – noch wichtiger – keiner wird es merken.

Isenrings schwarze Box beginnt, heimlich die Signale der Laptops und Smartphones abzufangen. Die Gäste können weiterhin normal das Internet nutzen – das Gerät lenkt den Datenfluss aber zuerst über Isenrings Computer. Innerhalb von 30 Sekunden haben sich rund 20 Besucher unwissentlich mit dem gefälschten Netzwerk verbunden. Wie ein riesiger Datenkrake greift das Gerät immer weiter um sich – iPads kommen hinzu, ein Hewlett-Packard-Computer, ein Dutzend Smartphones.

Sie surfen über ein gefälschtes WLAN

«Das Gerät gibt vor, ein WLAN zu sein, das man bereits einmal benutzt hat», erklärt Sicherheitsexperte Isenring. Damit nutzt es die Eigenschaft von Computern, Smartphones und Tablets aus, sich automatisch mit ihnen bekannten Netzwerken zu verbinden. Einem User wird vorgegaukelt, er befinde sich im WLAN «public inselspital». Andere wähnen sich im WLAN des Europa-Parks, des Hotels Theresa oder der Universität Zürich. Die Mehrheit der Geräte verbindet sich aber mit dem gefälschten WLAN «Starbucks».

Für Isenring wäre es jetzt ein Leichtes, diesen Leuten das Leben schwerzumachen. Er könnte die Passwörter stehlen, die E-Mail-Adressen, möglicherweise die Bankangaben. Auf diese Daten hat es der Inhaber der Zürcher Sicherheitsfirma Zerberos aber gar nicht abgesehen. Zu Beginn zeigt er lediglich auf, auf welchen Webseiten die Leute surfen. Jemand klickt sich durch «20 Minuten online», ein anderer interessiert sich für Finanzen auf Yahoo. Ein Dritter ist auf der Seite von Dropbox. «Schauen Sie hier», sagt Isenring und zeigt auf den HTML-Code, der auf seinem Bildschirm erscheint. Ein User besucht www.bittorrent.com – eine Website, die auch für das Herunterladen von illegalen Film- oder Musikkopien benutzt wird.

«Bis jetzt konnten wir nur unverschlüsselte Daten sehen», sagt Andriu Isenring. Die Kommunikation auf Webshop-Seiten, E-Mail-Portalen oder beim E-Banking ist jedoch fast immer verschlüsselt. Mit einem Klick auf ein Programm kann Isenring die verschlüsselten Inhalte zwar teilweise in unverschlüsselte umwandeln. «Das Programm ist aber nicht allmächtig – gewisse Webseiten wie Gmail oder Facebook sind dafür zu sichen», sagt er.

Das Passwort abgefangen

Wir testen es auf meinem Laptop. Ich gehe auf mein E-Mail-Portal, tippe meinen Namen und mein Passwort ein und logge mich ein. Wenige Sekunden vergehen, da lächelt Isenring. «Ist das Passwort ‹Katze42›?», fragt er. Ich schlucke. Isenring konnte nicht nur mein Passwort, sondern auch meine Cookies abfangen – Daten, die auf meinem Computer gespeichert sind, um mich für Webseiten zu identifizieren. «Wenn ich diese übernähme, könnte ich vorgeben, mit Ihrem Konto auf einer Webseite eingeloggt zu sein», erklärt er. Und etwa sehen, was beim Onlineshop Zalando in meinem Einkaufskorb liegt.

Obwohl Isenring es sichtlich geniesst, mir die Schwachstellen meines Computers aufzuzeigen, würde er die Daten niemals missbrauchen. Er zählt sich zu den so-genannten Ethical Hackers – IT-Experten, die im Auftrag von Firmen die Verwundbarkeit ihrer Netzwerke und Webserver testen. «Viele Private und Firmen exponieren sich teilweise stark – die wenigsten sind sich aber der Gefahren bewusst.» Isenring erzählt von Onlineshops, deren sämtliche Kundenadressen und Kreditkartendaten er bei einem Test aufspüren konnte. «Bei einer Dating-Webseite habe ich die Namen und Adressen aller User in der Kundenkartei gefunden.» Wenn die Schwachstellen erst bekannt sind, können sie behoben werden. Allgemein empfiehlt Isenring eins: mehr Vorsicht im Umgang mit Netzwerken.

Wer auf das WLAN-Symbol in Kaffeehäusern oder anderen öffentlichen Einrichtungen stösst, sollte mit sensiblen Daten vorsichtig umgehen.

Quelle: Daniel Pilar/Laif

Das Zebra, das über den Bildschirm hüpft

Mittlerweile «gehören» fast 40 Geräte im Café ihm. Sogar die Signale einiger Smartphones und Laptops im benachbarten «McDonald's» sind in seine Reichweite geraten. Langsam gerät das Programm aber an seine technischen Grenzen: Die Internetverbindung stockt, die Webseiten laden nicht mehr. «Vermutlich sind alle genervt, dass das Internet lahmt», sagt Isenring.

Er packt seine Sachen, es geht weiter ins «Starbucks» beim Central. Hier will mir Isenring zeigen, was er jemandem antun könnte, wollte er ihm wirklich schaden. Als Erstes lässt er mich auf meinem Notebook eine beliebige Webseite öffnen. Anstelle meiner Facebook-Seite, die ich eigentlich öffnen wollte, wird im Browserfenster aber ein kleines Video geladen: ein tanzendes Zebra vor grellviolettem Hintergrund. Egal, auf welche Seite ich zugreifen will, das Zebra hüpft auf meinem Bildschirm immer weiter vor sich hin. Isenring schickt weitere Bilder auf meinen Bildschirm – einen lachenden Mann, einen Popstar. Ich bin machtlos. Beängstigend, wie einfach es für jemanden wie Isenring wäre, illegale Bilder auf meinen Laptop zu laden.

«Die Gefahr sind kleine Cyberkriminelle»

«Ich könnte auch eine Log-in-Seite nachbauen und dazwischenschalten», sagt Isenring. Etwa die von Facebook, Gmail oder GMX. «Das Logo, das Formular, die Farbe – alles wäre identisch.» Über diese gefälschte Webseite könnte Isenring alle Daten abfangen, die ich eintippe – zum Beispiel Benutzername und Passwort. Gehörten die Daten erst ihm, hätte er Kontrolle über einen grossen Teil meiner Onlineidentität. Er könnte die Daten weiterverkaufen oder sogar einen Trojaner, ein feindliches Programm, auf meinen Computer schmuggeln.

Doch wie gross ist die Gefahr, dass sich tatsächlich jemand böswillig in einem WLAN tummelt? Andriu Isenring zuckt die Schultern: «Es genügt, dass die Möglichkeit besteht.» Cyberspione versuchten solche Tricks vor allem beim internen Netzwerk einer Firma oder bei staatlichen Stellen. «In öffentlichen WLANs sind kleine Cyberkriminelle die Gefahr. Es gibt sicher einige, die gern rumpröbeln, auch Jugendliche auf der Suche nach einem Erfolgserlebnis.»

Isenrings kleines Gerät kostet rund 200 Franken und ist online mit wenigen Klicks bestellbar. Erwerb und Betrieb sind laut Rechtsexperten legal, solange keine Daten verändert werden. «Wer ein wenig IT-Kenntnisse hat, wird mit dem Programm auch nicht sonderlich Mühe haben», sagt Isenring. «Auch wenn er vielleicht den technischen Hintergrund nicht wirklich versteht.»

Die Melde- und Analysestelle Informationssicherung (Melani) des Bundes weiss nicht, wie viele Nutzer von öffentlichen Netzwerken bereits Betrügern zum Opfer gefallen sind. «Ich empfehle aber, nie sensible Daten in einem öffentlichen WLAN zu übermitteln oder vertrauliche Mails zu schreiben», sagt Max Klaus von Melani.

Zum Schluss schaut Isenring nochmals nach, wie viele Geräte mit ihm verbunden sind. Mittlerweile sind es fast 50.

Alle Daten, die bei diesem Experiment abgefangen wurden, wurden umgehend gelöscht.

So schützen Sie sich vor Hackern

- Schalten Sie Ihren WLAN-Empfang auf Computer und Smartphone aus, wenn Sie die Geräte nicht benutzen.
- Lassen Sie Ihr Gerät nicht automatisch mit bekannten Netzwerken verbinden.
- Geben Sie im öffentlichen WLAN nie sensible Daten preis.
- Um die Sicherheit stark zu erhöhen, können Sie beim Surfen in öffentlichen Netzwerken einen VPN-Client benutzen (VPN = Virtual Private Network). Dieser verschlüsselt sämtliche Kommunikation und schützt so vor Spionen.