Vorsicht vor kostenlos!

Öffentliche WLAN-Netze sind beliebt. Und öffnen Hackern Tür und Tor. Beim „Live Hacking“ erlebten das die Besucher hautnah

Städte, Hotels, Einkaufszentren, alle werben sie inzwischen mit einer ganz besonderen Attraktion – dem freien WLAN. Surfen für umme, das zieht. Groß die Verlockung, groß die Gefahr. Das demonstrierten die beiden IT-Sicherheitsexperten Kai Jendrian und Jörg Völker der Secorvo Security Consulting beim „Live Hacking“.

Zuerst zur Verlockung. „Ein kostenloser Internetzugang, dieser Verlockung können die wenigsten widerstehen“, so Jendrian. Selbst in einer Veranstaltung mit dem Titel „Live Hacking“. Zahlreiche Smartphones und Tablets der Besucher waren eingeloggt, ungeschützt. Und genau da liegt das Problem: „Wer in fremden WLAN-Netzen unterwegs ist, muss großes Vertrauen in den Betreiber dieser Access Points haben“, macht Völker deutlich. Denn das Netz kann durchaus zum Angriff blasen gegen den Nutzer. Und zwar ohne dass dieser das merkt. Hierfür das Bewusstsein zu schaffen, das hat sich die Karlsruher IT-Sicherheitsinitiative zum Ziel gesetzt, unter anderem mit solchen Informationsveranstaltungen.

Sich in fremden Hot Spots zu bewegen bedeutet, nicht mehr Herr oder Frau der eigenen Daten zu sein. Mitlesen, mitschauen, Bewegungsprofil erkennen, das sind dabei noch die harmlosesten Folgen. Brisanter die Möglichkeit, Internetseiten zu verändern. Mal schnell auf einer Börsenseite die Kurse in den Keller fallen lassen, kein Problem. Panikverkäufe beim getäuschten Leser inklusive. Hört sich bei diesem Beispiel noch halbwegs lustig an. Verliert jedoch jeden Spaßfaktor beim Ausmalen der vielfältigen Manipulationsmöglichkeiten und den entsprechenden Folgen.

Zumal auch verschlüsselte Seiten nur einen bedingten Schutz bieten. Gefahr droht dabei in erster Linie vom Nutzer selbst, wenn auch unfreiwillig. „Wir sind alle so konditioniert, beim Warnhinweis zu Zertifikatsproblemen auf weiter zu klicken“, berichtet Jendrian. Ein unvorsichtiger Klick, und schon sind die Daten nicht mehr verschlüsselt. Das Datenauslesen somit problemlos möglich. „Aber es geht noch perfider“, setzt Völker noch einen drauf. Der Besuch bereits im Vorfeld präparierter Seiten kann so zum Verhängnis werden. Vermeintlich unverfängliche und sichere Seiten werden so mitunter zum teuren Vergnügen. Beispielsweise lassen sich so Kontostände ändern oder Überweisungen ausführen. Und alles nur, weil im Hintergrund ein entsprechendes Java-Script mitläuft. Der totale Kontrollverlust also. „So lässt sich allerhand Schabernack auf dem Browser des Nutzers treiben“, fasst Jendrian das zusammen.

Aus der Theorie muss keine Praxis werden. Dafür gilt es jedoch zwei Dinge zu beherzigen. „Wenn schon freies WLAN, dann ausschließlich verschlüsselt surfen“, lautet der eine Tipp. Insbesondere die Warnhinweise zur Echtheit der Zertifikate gilt es ernst zu nehmen. Und der andere Ratschlag ist zwar „komplizierter, aber sicherer“. Das Zauberwort heißt VPN-Verbindung. Ein solches „virtuelles privates Netzwerk“ ist, wie der Name schon sagt, ein geschlossenes Netzwerk und somit gegen ungebetene Mitnutzer gefeit.

Michael Hölle

Kai Jendrian und Jörg Völker führten die Probleme mit kostenfreiem WLAN drastisch vor

Foto: Sandra Jacques