Was tut sich an der WLAN-Front?

Was tut sich an der WLAN-Front?

Hotspot in einer Lounge am Flughafen. *Swisscom*

Die Nachrichten über WLAN sind in letzter Zeit etwas in den Hintergrund gerückt. In der schnelllebigen ICT-Welt sind Weiterentwicklungen von bestehenden Lösungen voll im Gang. Public Wireless (PWLAN) beispielsweise ermöglicht den öffentlichen Zugang zu WLAN.

WLAN ist längst etabliert, so genannte Hotspots schiessen wie Pilze aus dem Boden. Doch wie werden die Angebote genutzt? Und wie sieht die rechtliche Seite aus, wenn WLAN-Hacker ihr Unwesen treiben?

Euphorie beim Hotspot-Ausbau – Ernüchterung bei der Nutzung

Zum Ende des zweiten Quartals 2005 gab es weltweit 84 283 WLAN-Hotspots und noch vor Jahresende soll die Zahl der weltweiten WLAN-Hotspots die Grenze von 100 000 überspringen. Das berichtet eine neue Studie aus der Wireless-Broadband-Analyst-Serie des Marktforschungsunternehmens Informa Telecoms Media. Mit einem Anteil von 42% hält Westeuropa die weltweite Führung bei den WLAN-Hotspots. Der prozentuale Anteil Westeuropas wuchs im Vergleich zum Vorjahr jedoch nur um 2%. Stärker wuchs dagegen der Anteil Nordamerikas: von 21% im Vorjahr auf 26% im zweiten Quartal 2005. Der asiatisch-pazifische Raum dagegen gab im weltweiten Vergleich Prozente ab. Der Anteil sank von 39% im Vorjahr auf 32% in diesem Jahr.

Dass das Hightech-Land Südkorea als weltweit führende Breitbandnation auch den global grössten Betreiber öffentlicher WLAN-Hotspots stellt, wird keinen wundern. Die Korea Telecom betreibt 13 412 Hotspots, was einem Anteil von 49% am Hotspot-Aufkommen der Region und einem Anteil von 16% der weltweiten Hotspots entspricht. Wie stark die nun fast 100 000 WLAN-Hotspots genutzt werden, steht jedoch auf einem anderen Blatt. Bei den Geschäftsreisenden zumindest scheint die Arbeit im WLAN-Hotspot am Flughafen oder im Hotel nicht sonderlich beliebt zu sein. Eine Studie des Marktforschungsunternehmens Gartner hat herausgefunden, dass nur ein Viertel der Geschäftsreisenden öffentliche Hotspots überhaupt nutzen (www.wlanreport.de/index-4.html).

Rechtliche Handhabe gegen WLAN Hacker

Nach Recherchen von PC-Professionell ist das Eindringen in fremde Funknetze, so genanntes War-Driving, zwar strafbar, den Tätern droht in der Praxis jedoch selten eine Strafverfolgung. Denn der Blick auf fremde Festplatten oder das Surfen auf Kosten anderer ist kaum nachzuweisen.

Mit automatischer WLAN-Erkennung finden auch immer mehr «Nicht-Hacker» mit ihrem Notebook zufällig und ungewollt offene Funknetze. Doch das Hacken, Juristen sprechen auch vom «elektronischen Hausfriedensbruch», ist gemäss § 202a Strafgesetzbuch (StGB) verboten und kann mit bis zu drei Jahren Gefängnis oder einer Geldstrafe geahndet werden. Dabei zählt nur, dass die Daten vor dem Zugriff durch Dritte technisch geschützt sind. Wie effektiv dabei dieser Schutz ist, spielt keine Rolle. Auch Datenveränderungen im fremden WLAN sind mit bis zu zwei Jahren Gefängnis unter Strafe gestellt (§ 303a StGB).

Eine erfolgreiche Sabotage, welche die Verarbeitung wesentlicher Daten beispielsweise eines Betriebs, Unternehmens oder auch von Freischaffenden stört, kann den Hacker bis zu fünf Jahre hinter Gitter führen. Allerdings zeigt die Praxis, dass eine Strafverfolgung nur selten stattfindet. Das Opfer merkt meist nichts vom WLAN-Hacker, der auf ihre Kosten mitsurft. Zudem sind mobile Täter nur schwer auffindbar. Wird ein WLAN-Spion einmal erwischt, kann es durchaus sein, dass das Verfahren wegen Geringfügigkeit und mangelnden öffentlichen Interesses eingestellt wird (www.wlanreport.de/index-4.html). ■