Mithören von WLAN-Traffic

Völker, hört die Signale

Das WLAN erfreut sich immer größerer Beliebtheit. Damit geht aber auch einher, dass immer mehr Nutzer ihre Daten über unsichere Netze austauschen. Die gefunkten Daten mitlesen ist einfach – selbst wenn sie verschlüsselt sind. Wo liegen die rechtlichen Risiken für Lauscher und Betreiber? Olaf Koglin

Modern, ungebunden und dynamisch – dank dieser Trendattribute avanciert das WLAN vom Netzwerk zum Lifestyle. Öffentlich zugängliche WLANs gibt es an Hot Spots wie dem Münchner Englischen Garten, Flughäfen und neuen Cafés, in denen die Getränke „to go" in amerikanischen Schnabeltassen angeboten werden [1]. Wer dazu gehören will, erledigt hier seine Geschäfte oder schickt zumindest einer guten Freundin schnell eine E-Mail. Beim Gedanken an all die User mit Standardeinstellung und ohne Sicherheitsbewusstsein schlägt das Herz von Hackern und Crackern höher.

Bin ich schon drin?

Dank einheitlicher Standards und flexibler Nutzung von Computern ist das Abhören von Funknetzen recht einfach. Während es beim – technisch nicht weit entfernten – Mitschneiden der Signale von schnurlosen Telefonen noch spezieller teurer Technik bedarf, reichen für WLANs handelsübliche PC-Karten im Notebook. Zum Spaß am Gerät trägt ebenfalls bei, dass über Funknetze viele verschiedene Arten von Information ausgetauscht werden, die für die weitere Bearbeitung schon in vertrauten Formaten ankommen [2].

Der Wireless-Ethernet-Standard 802.11b beinhaltet eine optionale Verschlüsselung. Sie soll eine der kabelgebundenen Übertragung ebenbürtige Sicherheit leisten und heißt daher Wired Equivalent Privacy oder kurz WEP. Mehrere empirische Untersuchungen haben aber übereinstimmend ergeben, dass bei den von öffentlichem Grund aus erreichbaren Funknetzen nur rund 30 Prozent diese Verschlüsselung auch tatsächlich nutzen [3]. Ob es mit der kommenden, sichereren WPA-Verschlüsselung (ab 802.11i) besser wird, bleibt abzuwarten.

Abörverbot im TK-Recht

Die unverschlüsselten Daten mitzulesen ist einfach, sie dann auch auszuwerten verspricht zudem umfangreiche private und geschäftliche Information. Aber ist das auch legal? Laut Paragraf 86 Satz 1 Telekommunikationsgesetz (TKG) dürfen mit einer Funkanlage „Nachrichten, die für die Funkanlage nicht bestimmt sind, nicht abgehört werden". Ein Verstoß hiergegen wird nach Paragraf 95 TKG mit Freiheitsstrafe bis zu zwei Jahren bestraft.

Eine WLAN-Karte ist eine solche Funkanlage im Sinne des TKG. Jedoch sind innerhalb des WLANs technisch alle Funksignale für jeden Empfänger bestimmt. Ob sie auch inhaltlich an diesen Empfänger gerichtet sind, ist hier bedeutungslos [4]. Das „Mithören" des Datenverkehrs mit unmodifizierter Hardware ist danach kein strafbarer Eingriff.

Das Strafgesetzbuch (StGB) droht in Paragraf 202a bis zu drei Jahre Freiheitsstrafe für das „Ausspähen von Daten" an – allerdings nur für solche, die gegen unberechtigten Zugang besonders gesichert sind. Die Passwortabfrage eines Rechners vor dem Datenzugriff wird zum Beispiel als eine solche besondere Sicherung angesehen. Aber was ist mit den Daten, die gerade per Funk übertragen werden?

Besondere Sicherung

Um auch die Daten, die gerade übertragen werden, durch Paragraf 202a StGB zu schützen, erkennen die meisten Juristen eine Verschlüsselung als besondere Sicherung an – auch wenn dies rechtsdogmatisch strittig ist [5]. Unerheblich ist aber jedenfalls, wie wirksam die besondere Sicherung ist. Die bekannten Risiken der WEP disqualifizieren sie also nicht als besondere Sicherung.

Das heißt: Das Ausspähen von mit WEP (oder auf eine andere Weise) verschlüsselten Daten ist nach Paragraf 202a StGB

strafbar. Das Abhören und Speichern unverschlüsselter Daten verbietet Paragraf 202a StGB nicht.

Geschützte Geschäftsgeheimnisse

Es kann aber aus anderem Grund strafbar sein: Das Gesetz gegen den unlauteren Wettbewerb (UWG) verbietet es in Paragraf 17 Absatz 2, Geschäftsgeheimnisse unbefugt zu erlangen. Das sind alle nicht offenkundigen kaufmännischen oder technischen unternehmensinternen Informationen, die der Inhaber berechtigt geheimhalten will. Gemeint sind aber nicht private oder bekannte Informationen. Wer den Kollegen mailt, er surfe noch im Park, verrät kein Geschäftsgeheimnis. Eine interne Mail, die etwa ein konkretes Preisangebot enthält, ist aber von Paragraf 17 UWG geschützt. Bei Geschäftsgeheimnissen kommt es auch nicht darauf an, ob sie verschlüsselt sind oder nicht.

Das Abhören mit dem WLAN-Rechner ist eine „Anwendung technischer Mittel". Allerdings muss der Täter subjektiv aus wirtschaftlichen Eigennutz oder den anderen in Paragraf 17 UWG genannten Motiven handeln. Daran fehlt es, wenn das Netz tatsächlich nur aus Neugier oder Langeweile abgehört wurde. Doch Vorsicht: Auch das Verwerten oder Weitergeben der zunächst uneigennützig gewonnenen Geschäftsgeheimnisse ist nach Paragraf 17 Absatz 2 UWG strafbar.

Schutz personenbezogener Daten

Daten von Privatpersonen abhören kann aber auch datenschutzrechtlich verboten sein. Wer zum Beispiel im Sommer im Park liegt und Daten mitschneidet, könnte dabei E-Mails speichern, deren Header die E-Mail-Adressen von Absender und Empfänger zeigen. Das sind „personenbezogene Daten" im Sinne des Bundesdatenschutzgesetzes (BDSG).

Das BDSG gilt unter anderem für jede nicht-behördliche Stelle, die personenbezogene Daten erhebt oder verarbeitet. Eine Ausnahme besteht nur dann, wenn die Datenverarbeitung ausschließlich zu persönlichen oder familiären Tätigkeiten erfolgt. Die Grenzen der persönlichen und familiären Tätigkeiten sind eng gezogen – um den Zweck des Datenschutzes nicht durch zu weite Ausnahmen zu gefährden.

Der Hacker als nicht-öffentliche DV-Stelle

Da der Täter datenschutzrechtlich weder zur Erhebung noch zur Verarbeitung der Daten berechtigt ist, verstößt er gegen das BDSG. Diese Ordnungswidrigkeit zieht gemäß Paragraf 43 Absätze 2 und 3 BDSG eine empfindliche Geldbuße bis zu 250000 Euro nach sich. Wer gegen Entgelt oder in der Absicht handelt, den Betroffenen zu schädigen, macht sich nach Paragraf 44 BDSG sogar strafbar. Aber auch unterhalb der Schwelle der Strafbarkeit drohen rechtliche Folgen. So ist das Abhören ein Eingriff in das allgemeine Persönlichkeitsrecht einer Privatperson oder in die Rechte eines Unternehmens [6]. Als Folge drohen wegen zivilrechtlicher Unterlassungsansprüche kostspielige Abmahnungen und Schadensersatzansprüche.

Die Seite des Opfers

Aber es geht nicht nur um den Angreifer. Unabhängig davon, ob er ermittelt und irgendwann bestraft wird, müssen Netzbetreiber und -teilnehmer präventiv tätig werden. Hierzu gehört eine angemessen sichere Technik. Sonst droht Haftung wegen Mitverschuldens, wenn Dritte die Geschäftsgeheimnisse allzu leicht mitlesen können. *(fan)*

Ausspähen von Daten

§ 202a Absatz 1 Strafgesetzbuch: Wer unbefugt Daten, die nicht für ihn bestimmt und die gegen unberechtigten Zugriff besonders gesichert sind, sich oder einem anderen verschafft, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.

Verschaffen von Geschäfts- oder Betriebsgeheimnissen

§ 17 Gesetz gegen Wettbewerbsbeschränkungen (Auszug): Mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe wird bestraft, wer zu Zwecken des Wettbewerbs, aus Eigennutz, zugunsten eines Dritten oder in der Absicht, dem Inhaber des Geschäftsbetriebs Schaden zuzufügen, sich ein Geschäfts- oder Betriebsgeheimnis durch Anwendung technischer Mittel unbefugt verschafft.

Personenbezogene Daten

§ 3 Absatz 1 Bundesdatenschutzgesetz: Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener).

Anwendungsbereich des Bundesdatenschutzgesetzes

§ 1 Absatz 2 Bundesdatenschutzgesetz: Dieses Gesetz gilt für die Erhebung, Verarbeitung und Nutzung personenbezogener Daten durch (...)

3: nicht öffentliche Stellen, soweit sie die Daten unter Einsatz von Datenverarbeitungsanlagen verarbeiten, nutzen oder dafür erheben oder die Daten in oder aus nicht automatisierten Dateien verarbeiten, nutzen oder dafür erheben, es sei denn, die Erhebung, Verarbeitung oder Nutzung der Daten erfolgt ausschließlich für persönliche oder familiäre Tätigkeiten.

Infos

[1] Ausbaufähige Übersichten gibt es unter: [http://www.sofanet.de/hotspots] und [http://www.stadtnet.org]

[2] Dornseif/Schumann/Klein, „Tatsächliche und rechtliche Risiken drahtloser Computernetzwerke": Datenschutz und Datensicherheit, Heft 4/02, S. 1ff. [http://md.hudora.de/publications/200204-dud-wlan/200204-dud-wlan.pdf]

[3] Dornseif/Klein-Studie (siehe [2]) und der International Wardriving Day: [http://www.integralis.de/press/pressemeldungen/pre_82.pdf].

[4] Beck'scher TKG-Kommentar zum Paragrafen 86

[5] Schmid: „Computerhacken und materielles Strafrecht" (2001)

[6] Palandt, Kommentar zum Bürgerlichen Gesetzbuch, Paragraf 823

Der Autor

Dipl.-jur. Olaf Koglin [ok@opensourcerecht.de] ist Rechtsanwalt in Berlin und arbeitet seit Jahren im IT-Recht. Unter anderem promoviert er über Open-Source-Software und ist Mitarbeiter im Institut für Rechtsfragen der freien und Open-Source-Software (ifrOSS) in München.