von Rechtsanwalt **Arndt Joachim Nagel**

Strafrechtliche Aspekte beim Zugriff auf fremde WLAN-Netzwerke

Immer häufiger wird die IT-Recht-Kanzlei mit Fällen konfrontiert, in denen drahtlose Computernetzwerke von Unbekannten missbraucht werden, um fremde Daten auszuspähen. Nicht selten bemerken die Betroffenen erst, dass ihre persönlichen Daten ausgespäht wurden, wenn sie unverhofft eine Ware geliefert bekommen, die sie überhaupt nicht bestellt hatten oder (wie bereits von der IT-Recht-Kanzlei berichtet) wenn ihnen ein anwaltliches Schreiben ins Haus flattert, in dem ihnen ein urheberrechtlicher Verstoß vorgeworfen wird.

Die IT-Recht-Kanzlei hat dies zum Anlass genommen, sich einmal mit den strafrechtlichen Aspekten der unbefugten Nutzung eines fremden WLAN-Netzwerks zu befassen. Dabei wird im Folgenden auf einige Fragen von Betroffenen eingegangen.

Frage: Macht sich jemand strafbar, der unbefugt auf ein drahtloses Netzwerk zugreift um dieses als Internetzugang zu benutzen?

Antwort: Ein solches Verhalten kann unter bestimmten Voraussetzungen strafbar sein.

Frage: Welche Straftatbestände sind überhaupt denkbar?

Antwort: Als mögliche Straftatbestände kommen das Ausspähen von Daten gem. § 202a StGB, der Computerbetrug gem. § 263a StGB sowie das Erschleichen von Leistungen gem. § 265a StGB aber auch das Abhören von Nachrichten gem. §§ 89, 148 Abs. 1 Nr. 1 TKG in Betracht.

Frage: Macht es für die Strafbarkeit einen Unterschied, ob es sich um ein gesichertes oder ungesichertes Netzwerk handelt?

Antwort: Diese Frage ist für die Strafbarkeit von entscheidender Bedeutung. Ist das Netzwerk beispielsweise durch eine WEP-Verschlüsselung geschützt und knackt ein Unbefugter diesen Schutz durch eine Software, um an die persönlichen Daten des Netzwerkinhabers zu gelangen, so ist sein Verhalten aus strafrechtlicher Sicht anders zu würdigen, als wenn er „nur" auf ein ungesichertes Netzwerk zugreift.

Frage: Wie ist die Strafbarkeit zu beurteilen, wenn ein gesichertes Netzwerk von außen geknackt wird?

Antwort: In diesem Fall kommt eine Strafbarkeit nach § 202a StGB in Betracht. Danach macht sich strafbar, wer unbefugt Daten, die nicht für ihn bestimmt und die gegen unberechtigten Zugang besonders gesichert sind, sich oder einem anderen verschafft. Unter Daten sind dabei alle Informationen zu verstehen, die elektronisch, magnetisch oder sonst nicht unmittelbar wahrnehmbar gespeichert sind, sich also in EDV-spezifischer Form darstellen lassen. Dazu zählt zum einen das bei WEP verwendete Passwort, zum anderen aber auch die im Rahmen des Verbindungsaufbaus vom Router zugeteilte IP-Adresse. Für das Tatbestandsmerkmal „Verschaffen" reicht schon aus, wenn der Täter Kenntnis von den gesicherten Daten erlangt. Auf die tatsächliche Nutzung des WLAN-Netzwerks, beispielsweise als Internetzugang kommt es dabei nicht an. Das heißt, der Tatbestand des § 202a StGB ist bereits dann erfüllt, wenn der Täter vorsätzlich ein verschlüsseltes WLAN-Netzwerk knackt und hierdurch von den geschützten Daten Kenntnis nimmt.

Frage: Ist es strafbar, von außen unbefugt auf ein ungesichertes Netzwerk zuzugreifen um so „schwarz" zu surfen?

Antwort: Bei ungesicherten WLAN-Netzwerken liegt die Sache etwas anders:

- Eine Strafbarkeit nach § 202a StGB scheidet in diesem Fall aus, da es an einer besonderen Datensicherung fehlt.
- Eine Strafbarkeit wegen Computerbetrugs nach § 263a StGB kommt ebenfalls nicht in Betracht. Insoweit muss man schon danach differenzieren, ob der Netzwerkinhaber mit seinem Provider einen Flatrate-Tarif oder eine Bezahlung nach der jeweils heruntergeladenen Datenmenge vereinbart hat. Denn für den Fall, dass der Netzwerkinhaber einen Flatrate-Tarif vereinbart hat, erleidet er durch das unbefugte Mitsurfen eines Dritten schon keinen Vermögensschaden. Für den Fall, dass eine Bezahlung nach Datenmenge vereinbart wurde, tritt beim Netzwerkinhaber zwar ein Vermögensschaden in Höhe der über seine eigene Nutzung hinausgehenden und von ihm zu bezahlenden Datenmenge ein. Dem Vorteil des Nutzers steht in diesem Fall jedoch kein Schaden des Betreibers, dem möglichen Schaden des Betreibers kein vom Nutzer angestrebter Vorteil gegenüber. Es fehlt somit an der für § 263a StGB erforderlichen Stoffgleichheit.
- Eine Strafbarkeit wegen Erschleichens von Leistungen nach § 265a StGB kommt schon deshalb nicht in Betracht, weil dessen Schutzbereich sich nur auf öffentlichen Zwecken dienende Telekommunikationsnetze erstreckt. WLAN-Netzwerke, die nur geschlossenen Benutzergruppen zur Verfügung stehen, dienen jedoch nicht öffentlichen Zwecken.
- Bleibt eine mögliche Strafbarkeit wegen Abhörens von Nachrichten gem. §§ 89, 148 Abs. 1 Nr. 1 TKG. Diese scheitert jedoch daran, dass es sich beim Datenverkehr im Rahmen der IP-Zuweisung nicht um Nachrichten im Sinne des § 89 TKG handelt.

Fazit

Wird von außen unbefugt auf ein fremdes Funkdatennetz zugegriffen, welches durch eine Verschlüsselung besonders gegen Zugriff gesichert ist, so ist dies gem. § 202a StGB strafbar. Wird dagegen ein fremdes Datennetz als Internetzugang genutzt, ohne dass hierbei eine Verschlüsselung geknackt wird, so ist dies nicht strafbar.

Autor:
RA Arndt Joachim Nagel
Rechtsanwalt und Fachanwalt für Informationstechnologierecht