Wardriving scheint für immer mehr Freaks auf der ganzen Welt ein interessanter Sport zu sein. Ausgerüstet mit einem Laptop, spezieller Software, einer Antenne und einem GPS ziehen sie aus und durchkämmen Städte und ganze Landstriche mit dem Ziel, über einen Accespoint auf ein ungeschütztes Wireless-LAN zuzugreifen.

DOI 10.1007/s00287-003-0352-y

Wardriving zu RECHT?

Ursula Sury

Wardriver als Täter?

Gemäss eigenen Angaben der Wardriver besteht ihre Aktivität nur darin, mit Hilfe des spezifischen Equipments in nicht geschützte drahtlose Netzwerke zu gelangen. Falls ein einfacher Zugriff auf Computer oder Netzwerkkomponenten möglich ist, wird häufig ein Hinweis hinterlassen (z.B. über SNMP), damit dem zuständigen Netzwerkbetreiber bewusst wird, dass sein Netz ungeschützt ist (vgl. dazu beispielsweise unter www.wardriving.ch und Links). Um ins Netzwerk zu gelangen, ist kein spezieller Aufwand wie beispielsweise Hacken notwendig, da das Netzwerk völlig offen und ungeschützt ist. Die Software, die dafür verwendet wird, ist denn auch nicht mit einem Hackertool zu vergleichen. Es handelt sich um spezialisierte Netzwerkanalysatorsoftware, die für verschiedene Zwecke verwendet werden kann.

Im Folgenden wird der Frage nachgegangen, welche möglichen Rechtsprobleme sich daraus sowohl für die Wardriver als auch für die Neztwerkbetreiber ergeben könnten.

Bereicherungsabsicht und Vermögensverschiebung

Ob und gegebenenfalls welche Strafrechtstatbestände mit dem Wardriving erfüllt werden, kann korrekterweise nur für einen konkreten Fall abschliessend beurteilt werden, je nachdem, welche Aktivitäten der Wardriver auf dem von ihm aufgefundenen offenen Netz entfaltet. Wird das Datenverarbeitungssystem, in welches eingedrungen wird, nicht mittelbar zur Schädigung im Sinne einer Vermögensverschiebung missbraucht, so kommen Deliktstypen wie Computerbetrug (D StGB § 263 a), Fälschung technischer Aufzeichnungen (D StGB § 268), Fälschung beweiserheblicher Daten (D StGB § 269), Täuschung im Rechtsverkehr bei Datenverarbeitung (D StGB § 270) und mittelbare Falschbeurkundung (D StGB § 241) nicht in Betracht. Vergleichbare Straftatbestände gibt es auch in der Schweiz, wie der betrügerische Missbrauch einer Datenverarbeitungsanlage (CH StGB Art. 147) oder die Urkundenfälschung (CH StGB Art. 251) etc. Auch in Österreich sind dieselben Rechtsgüter mit ähnlichen oder gleichen Strafnormen geschützt.

Kein besonders gesichertes System

Gewisse Artikel im Bereich der Computerkriminalität der Schweiz und Deutschland, nämlich die unbefugte Datenbeschaffung (CH StGB Art. 143), das unbefugte Eindringen in ein Datenverarbeitungssystem (CH StGB Art. 143 bis) und das Ausspähen von Daten (D StGB § 202 a) wird ein Wardriver nicht erfüllen. Diese Artikel fordern nämlich, dass das Datenbearbeitungssystem *gegen unbefugten Zugriff besonders gesichert* sein müsse. Gerade dies wird ja kaum der Fall sein, da bei der oben beschriebenen Wardriving Freizeitbeschäftigung nach Netzwerken gesucht wird, die eben *nicht* gesichert sind.

Veränderung von Daten

Das Hinterlassen eines Hinweises auf dem System zuhanden der Administratoren ist eine Veränderung von Daten, welche in Deutschland als Datenveränderung (G StGB § 303 a), als Datenbeschädigung in der Schweiz (CH StGB Art. 144 bis) und in Österreich als Datenbeschädigung (StGB § 126 a) bestraft wird. Die Strafandrohung ist von Freiheitsstrafe bis zu zwei Jahren oder Geldstrafe

(D) über Freiheitsstrafe bis zu 6 Monaten und Geldstrafe (A) und Antrag auf Gefängnis bis zu 3 Jahren oder Busse (CH).

Eine eigentliche Veränderung der Daten wird aber erst dann bejaht, wenn die Manipulation dahingehend vorgenommen wird, dass der Informationsgehalt der Daten in einer für den Datenberechtigten unerwünschten Form verändert wird (vgl. dazu beispielsweise Schmid Niklaus, Computer- sowie Cheque- und Kreditkartenkriminalität, Zürich 1994, N. 26 zu Art. 144 bis StGB).

Missbrauch von Computerprogrammen

Wer Computerprogramme einführt, einsetzt, zur Verfügung stellt etc., welche dazu verwendet werden, widerrechtlichen Zugriff auf ein Computersystem oder Datenbeschädigung oder Störung der Funktionsfähigkeit eines Computersystems und Ähnliches bezwecken, macht sich selber strafbar (vgl. dazu A StGB § 126 c, CH StGB Art. 144 bis). Bei der von den Wardrivern verwendeten Software handelt es sich nicht um eine spezifische Hacksoftware, sondern wie oben schon ausgeführt, um in verschiedenen Bereichen eingesetzte Netzwerkanalysatorensoftware. Diese wird auch in ähnlicher Form selbst für private Wireless-LAN-Benutzer abgegeben und auf Laptops installiert. Die Software als solche wurde also nicht eigens zur Erreichung widerrechtlicher Zwecke erstellt.

Die Software kann aber selbstverständlich zu widerrechtlichen Zwecken eingesetzt werden, genauso wie ein Küchenmesser auch für einen Mord verwendet werden kann. Die einschlägigen Wardriver-Organisationen weisen aber ausdrücklich darauf hin, dass ihre Informationen und Aktivitäten rein zu Forschungszwecken erfolgen um insbesondere die Sicherheit der virtuellen Netzwerke zu erhöhen. Damit wird der subjektive Tatbestand, nämlich dass sie ein Programm einführen, verwenden, empfehlen etc., von dem sie wissen, oder wissen sollten, dass es unrechtmässig verwendet wird, nicht erfüllt.

Datenschutz

Tritt der Wardriver in Systeme ein, welche personenbezogene Daten enthalten, führt dies zu Verletzungen der Datenschutzgesetzgebung. Dies gilt nämlich als unberechtigte Datenbearbeitung, sowohl nach Schweizer Recht (Art. DSG Art. 13) als auch gemäss der Datenschutzrichtlinie der EU (insbesondere Art. 7 a).

Urheberrecht

Die Wardriver werden bei ihrem Spaziergang durch fremde Netzwerke automatisch auch dort eingesetzte Software mitbenutzen, auch wenn es sich bloss um das Betriebssystem handelt. Die Nutzung von Software bedarf aber der Einwilligung des Urhebers, welche man sich in der Regel über eine Lizenz einholt. Diese Einwilligung wird nur dann vorliegen, wenn der Urheber klar deklariert hat, dass er damit einverstanden ist, dass auch Dritte die Software mitbenutzen dürfen.

Die unberechtigte Benutzung von Software verletzt das Urheberrecht und wird zum Teil auch mit Strafe bedroht. Zur Regelung betreffend Urheberrecht vgl. Richtlinie des europäischen Parlamentes und des Rates 2001 / 29 / EG vom 22. Mai 2002 zur Harmonisierung bestimmter Aspekte des Urheberrechts und der verwandten Schutzrechte in der Informationsgesellschaft, insbesondere Art. 2 ff.; A Urheberrecht § 42; D UrhG § 69 c; CH UrG Art. 10, 11, 67.

Rechtsprobleme der Netzbetreiber

Den Netzbetreiber treffen, je nachdem, welche Daten über Netz gut zugänglich sind, unterschiedliche, gesetzliche oder vertragliche Sicherheitspflichten.

Die Datenschutzgesetzgebung verpflichtet den Inhaber einer Datensammlung, diese sicher aufzubewahren. Mit dem ungesicherten Betreiben eines Wireless-LAN wird dieser gesetzlichen Pflicht nicht nachgelebt und diese somit verletzt.

Die Software, welche eine Unternehmung in Lizenz zum Gebrauch erwirbt, darf sie in der Regel weder direkt noch indirekt Dritten zum Gebrauch zur Verfügung stellen. Dieser Schutzpflicht vor dem Zugriff Dritter kommt die Unternehmung mit einem ungeschützten Wireless-LAN-System nicht nach, weshalb sie möglicherweise auch ihren Lizenzvertrag gegenüber dem jeweiligen Softwareanbieter (Urheber) verletzt.

Ergänzend können den Netzwerkbetreiber gesetzliche oder vertragliche Geheimhaltungsverpflichtungen treffen, wie die Schweigepflicht der Ärzte, das Bankgeheimnis, oder Amtsgeheimnisse. Auch diese Pflichten verletzt er, wenn er das Netz nicht angemessen sichert, was empfindliche Haftpflichtansprüche nach sich ziehen kann.

Das Schlimmste, was einem Netzwerkbetreiber blühen kann, ist, dass ein Hacker mit wirklich rechtswidrigen Absichten von diesem Netzwerk aus strafrechtlich und/oder haftpflichtrechtlich relevante Aktivitäten unternimmt und diese dann dem Netzwerkbetreiber statt dem Täter zugeordnet werden.

Sobald Netzwerke nicht mehr nur rein privat betrieben werden, ist die Sicherungspflicht eine minimale unternehmerische Sorgfaltspflicht. Die Verletzung dieser Pflicht und dar-

aus fliessender Schaden muss der Unternehmung und den für die Führung verantwortlichen Personen angelastet werden.

Wardriver, die guten Täter?!

Wer sich im Internet über Wardriving kundig macht, ist sehr darüber erstaunt, wieviele ungeschützte virtuelle Netzwerke es gibt. Eigentlich dürften die Wardriver nicht einen Bruchteil so erfolgreich sein, wie das eben leider der Fall ist. Ein Wireless-LAN ist relativ einfach zu schützen, dies wird aber offensichtlich häufig nicht gemacht. Der Grund dafür liegt zum einen im fehlenden Sicherheitsbewusstsein/Awareness und zum anderen im fehlenden Know-how darüber, wie dieser Schutz zu bewerkstelligen ist.

Die Aktivitäten der Wardriver sind aus diesem Blickwinkel betrachtet ein wichtiger Beitrag zur Erhöhung der Informatiksicherheit. Manch ein Netzwerkbetreiber wird so dank dem Hinweis eines Wardrivers (falls er diesen ernst nimmt und entsprechend handelt) vor Problemen und Schäden bewahrt.

Zusammenfassung

Je nach den Aktivitäten, welche beim Wardriving konkret ausgeführt werden, kann es zu Rechtsverletzungen kommen. Ein Wardriver, der nur in ein fremdes Netzwerk einsteigt und dort einen kleinen Hinweis betreffend der Unsicherheit des Systems hinterlässt, ohne irgendwelche Daten zu beschädigen, zu ändern etc., wird höchstens unzulässigerweise ein Programm gebrauchen oder unzulässigerweise personenbezogenen Daten bearbeiten (jede Art von Umgang mit personenbezogenen Daten gilt als Bearbeiten!).

Wer ein Wireless-LAN ungesichert betreibt, gefährdet sich selbst, seine Daten aber auch Dritte, gegenüber denen er gesetzlich oder vertraglich in irgendeiner Form der Vertraulichkeit verpflichtet ist.

Ursula Sury ist selbständige Rechtsanwältin in Luzern (CH) und leitet den Fachhochschul-Lehrgang Wirtschaftsinformatik an der Hochschule für Wirtschaft HSW Luzern der Fachhochschule Zentralschweiz. Sie ist zudem Dozentin für Informatikrecht an verschiedenen Nachdiplomstudien, welche am Institut für Wirtschaftsinformatik der Hochschule durchgeführt werden. Die Autorin ist hauptsächlich im Bereich Informatikrecht und Datenschutz tätig. Informieren Sie sich unter www.hsw.fhz.ch

20 Jahre SI – Schweizer Informatik(er) Gesellschaft

Ein starker Knoten in einem weitgespannten Beziehungsnetz

1983 wurde die SI gegründet, heute feiert sie ihr Jubiläum, ein Anlass, die wichtige Rolle der SI in der Schweizer Informatik-Verbandslandschaft etwas auszuleuchten.

Die Schweiz stand und steht im Informatikbereich in verschiedenen Beziehungen weit vorne. So war Konrad Zuses Z4, als sie von 1950 – 1954 mietweise im Institut für Angewandte Mathematik von Eduard Stiefel an der ETH Zürich stand, der allererste Rechenautomat an einer kontinentaleuropäischen Hochschule. Und die Schweiz weist seit den 60-er Jahren weltweit nach den USA die grössten pro-Kopf-Investitionen in Computer auf. Selbstverständlich arbeiteten hier auch entsprechende Fachleute und pflegten Kontakt mit Gleichgesinnten. Dass eine SI erst im Jahre 1983 gegründet wurde, muss daher besondere Gründe haben.

Schweizer Mathematiker und Elektrotechniker hatten nach dem zweiten Weltkrieg rasch von den neuen Entwicklungen von Rechenautomaten Kenntnis genommen und auch die USA besucht; kein Wunder, dass Schweizer auch früh der *Association for Computing Machinery (ACM)* beitraten und zurück in der Schweiz ein "*Swiss Chapter of the ACM*" bildeten. Damals gab es aber i der Schweiz auch andere wissenschaftliche Gesellschaften, die auf die neuen Rechenautomaten aufmerksam geworden waren. Für die weitere Entwicklung wichtig war vor allem die *Schweizerische Gesellschaft für Automatik (SGA)*, die in dieser Frühzeit die Vertretung der Schweiz in der neugegründeten internationalen Dachgesellschaft der Informatik, der *International Federation for Information Processing (IFIP)* aufbaute und pflegte. Über die SGA wurde als erster Schweizer Ambros P. Speiser von 1965–68 IFIP-Präsident.

Innerhalb der Schweiz waren in den 60-er Jahren bereits mehrere Informatiker-Organisationen tätig und warben Mitglieder. Schon damals war zahlenmässig die *Datenverarbeitung* weit wichtiger als die *wissenschaftliche* Informatik. Von der Öffentlichkeit kaum bemerkt, war die Datenverarbeitung schon vor dem zweiten Weltkrieg in der Schweiz heimisch geworden; so hatte 1928 die Rentenanstalt für ihre Prämienrechnungen eine eigene Lochkarten-Abteilung eingerichtet. Mit der Zeit entstand eine Vereinigung der *Lochkarten-Fachleute im Schweiz. Kaufmännischen Verband (SKV)*, später umbenannt in *Datenverarbeitungsfachleute (VDF)*. Erst 1994 machten sich diese als *Wirtschaftsinformatik-Fachverband (WIF)* selbständig und fusionierten im Jahr