Stefan Jäger

Wardriving – die unterschätzte Gefahr

Wardriving ist normalweise nur denjenigen ein Begriff, die sich mit WLAN oder generell Funknetzen beschäftigen. Doch ist oft nicht genau bekannt, um was es sich hierbei handelt. Ist es legal oder illegal, kann es von jedermann oder nur von Fachleuten durchgeführt werden, usw.? Zudem stellt sich die Frage nach dem Zweck dieser Tätigkeit und den daraus resultierenden Einsatzgebieten. Auch ist die Aktualität des Themas zu klären. Gemessen an der Anzahl an Beiträgen in den analogen und digitalen Medien, ist es um das Wardriving seit 2008 sehr ruhig geworden. Generell wird das Thema WLAN-Sicherheit seit der faktischen Umsetzung des WPA2-Standards, etwa im Jahre 2006, kaum noch in der Breite und Tiefe behandelt. Aber ist mit Einführung des WPA2-Standards die Notwendigkeit tatsächlich entfallen, sich mit WLAN-Sicherheitsmechanismen auseinanderzusetzen?

Aber zunächst: was ist eigentlich Wardriving? Nachfolgend zwei unterschiedliche Definitionen:

1. „**Wardriving** ist das systematische Suchen nach *Wireless Local Area Networks* mit Hilfe eines Fahrzeugs. Der Begriff leitet sich von *Wardialing* ab, einer Methode, mittels Durchprobieren vieler Telefonnummern offene *Modem*-Zugänge zu finden. Einige Wardriver sehen die drei Anfangsbuchstaben dabei als *Backronym* für ‚Wireless Access Revolution'."[1]

2. „**War-Driving** Bezeichnet das unbefugte Eindringen in fremde WLANs, das oft vom Auto aus mit dem Laptop durchgeführt wird (daher ‚driving')."[2]

Zwei Definitionen, welche jede für sich einen anderen Schwerpunkt auf die Thematik legen. Die offizielle Definition des *Bundesamtes für Sicherheit in der Informationstechnik* (BSI) ist formal gesehen sogar falsch, da das Wardriving nur das Auffinden von offenen oder schlecht geschützten Funknetzen verfolgt. Das BSI unterstellt dieser Tätigkeit, möglicherweise allein schon wegen der Begriffskomponente *War,* von vornherein eine kriminelle Absicht. Dabei hängt es (wie bei fast jeder Tätigkeit) vom Einzelnen ab, ob Wardriving für gute oder schlechte Zwecke eingesetzt wird.

Der Begriff *Wardialing,* von dem die Bezeichnung Wardriving abgeleitet ist, wurde durch den Film *WarGames* geprägt. Dort wurde mithilfe eines Modems jede Telefonnummer in einem bestimmten Nummernbereich angerufen. Ziel war es, hierdurch einen Computer zu finden, in welchen man anschließend eindringen konnte.

Abbildung 1: Wardriving damals …
Foto: Rudolf Mittelmann

Wardriving in seiner heute üblichen Form wurde erstmals im Vortrag[3] von Peter Shipley auf der Konferenz *DefCon* im Jahre 2001 vorgestellt. Shipley hatte zuvor über einen Zeitraum von 18 Monaten nach Funknetzwerken in Berkeley gesucht.

Ausrüstung

Mittlerweile hat sich weltweit eine große (in einzelne länderbezogene Gruppen aufgeteilte) Wardriving-Community gebildet. Dieses Interesse rührt nicht zuletzt von den folgenden drei Gegebenheiten her:

- Wardriving befriedigt den natürlichen Sammlertrieb des Menschen.
- Wardriving kommt dem Entdeckerdrang des Menschen entgegen.
- Man braucht heutzutage zum Wardriving kaum noch spezielle Hardware.

Benötigte man in der Anfangszeit des Wardriving noch einen Laptop, einen GPS-Empfänger und eine externe WLAN-Antenne (Abbildung 1), kann dies heutzutage alles durch ein normales Smartphone ersetzt werden.

Neben diesen technischen Voraussetzungen bringen Smartphones durch große *App Stores* auch alle notwendigen Applikationen mit. Umfangreiche Softwaresammlungen sind also nicht mehr zwingend notwendig. Für jedes gängige Betriebssystem lassen sich die Tools bzw. Apps leicht aus dem Internet herunterladen (illegal sind sie nicht). Durch die Verwendung nutzerfreundlicher Apps wird auch keinerlei Vorwissen oder tiefgrei-

… und heute
Frame aus WiFi Tracker

fendes technisches Verständnis mehr benötigt. Der Anwender muss lediglich eine Applikation starten und bekommt dann unmittelbar die gefundenen Netzwerke auf einer Karte angezeigt. Hinzu kommt, dass eine nutzerbezogene Entscheidung, welche Netzwerke tendenziell unsicher sind, bereits durch die App gefällt und entsprechend eingefärbt auf der Karte dargestellt wird (Abbildung 2).

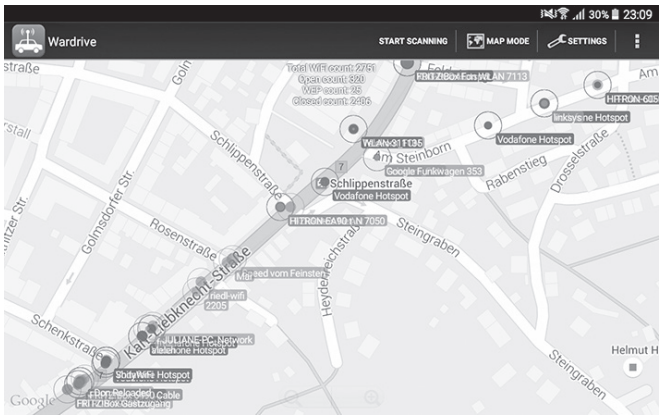


Abbildung 2: Streetmap
eigene Aufnahme vom 21.11.2015

In der Datenbank der Community *wardriving-forum.de* befinden sich fast 18 Millionen *Access Points*[4] (Abbildung 3, Stand 21.11.2015). Auf der Kartendarstellung sind deutlich die Umrisse Deutschlands zu erkennen.

In der Datenbank der Community *wigle.net* befinden sich über 225 Millionen Access Points weltweit, welche von über 28.000 Mitgliedern erfasst wurden (Abbildung 4, Stand 30.11.2015).

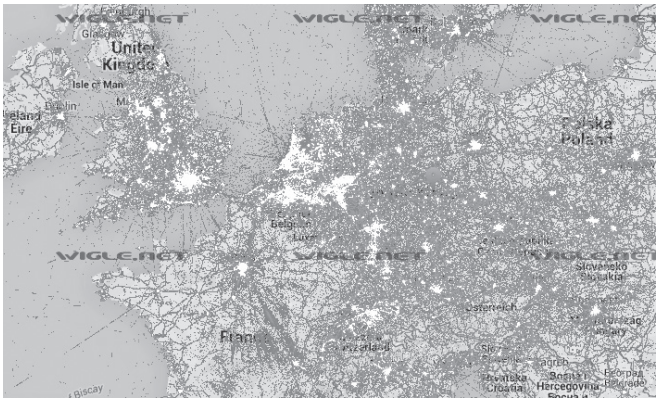


Abbildung 4: Screenshot von Access Points, Quelle: wigle.net
Die Bilddaten stammen von google, Map data ©2015 Google

Gefahren

Es stellt sich die Frage, warum Wardriving überhaupt diskutiert wird und ob von Wardriving eine Gefahr ausgeht. Diese Frage muss leider bejaht werden. Die Scansoftware wertet die erfassten Netzwerke in Echtzeit aus und zeigt offene sowie (z. B. wegen Einsatz von WEP[5]) potenziell schlecht gesicherte Netzwerke sofort an. Diese Netzwerke können von Angreifern missbraucht werden. Ein mehrminütiger Scan innerhalb einer Großstadt reicht (aus eigener Erfahrung) aus, um trotz evtl. vorhandener Sicherungsmechanismen hinreichend viele WLANs zu lokalisieren, auf die aussichtsreiche Angriffe gestartet werden könnten. Alternativ können über die bereits erwähnten Communities potenzielle Opfer auch bequem über die Karte ausgewählt werden. Anschließend kann man mit der benötigten Technik für den Angriff an den Zielort zurückkehren.

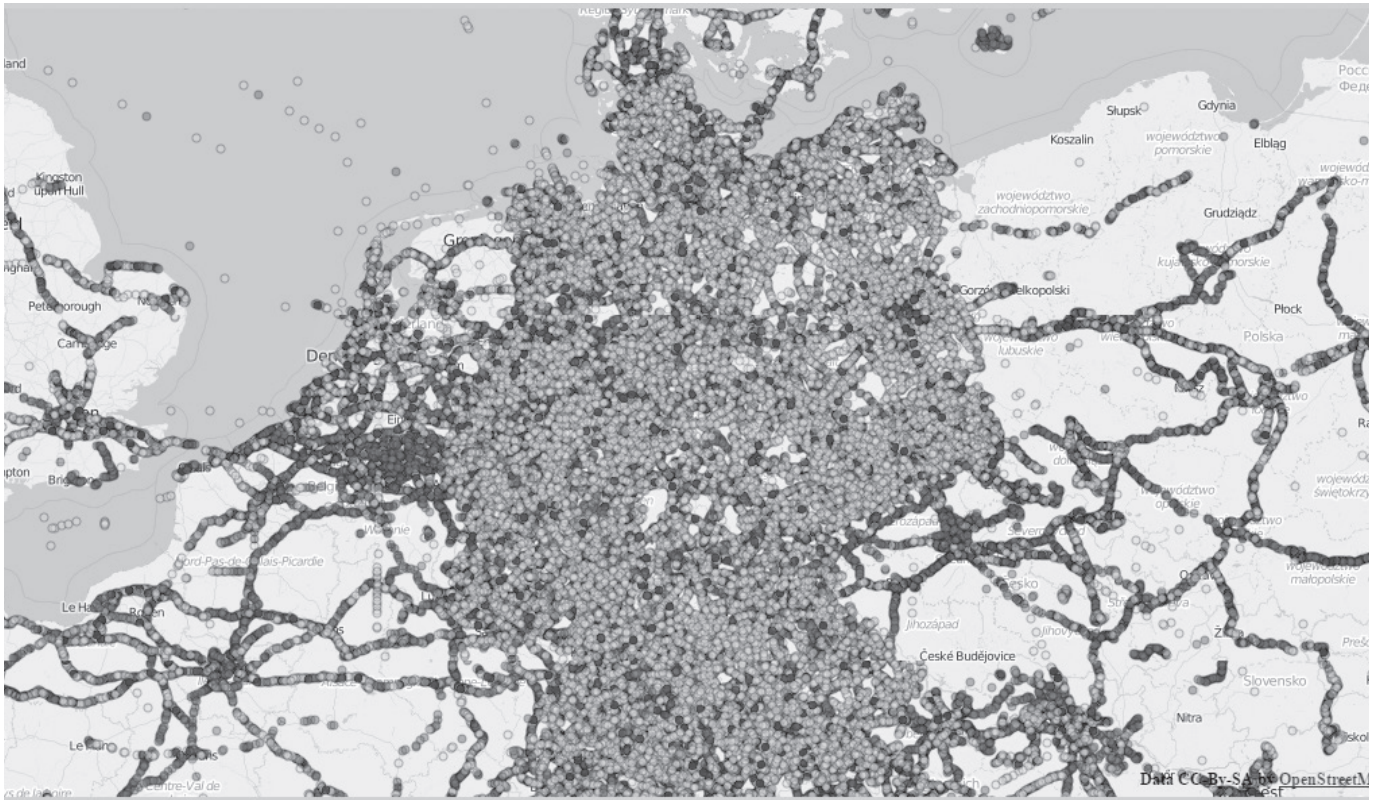


Abbildung 3: Screenshot von Access Points, Quelle: wardriving-forum.de
Diese Karte wird mit Hilfe von OpenLayers und OpenStreetMap erstellt, Stand: 21.11.2015

Sobald die WEP-Verschlüsselung überwunden wurde oder die Einwahl in ein offenes WLAN erfolgt ist, kann das Netzwerk für folgende Aktivitäten missbraucht werden:

- kostenfreies Surfen im Internet
- Auslesen von Dateien im Intranet
- Auslesen des Netzwerkverkehrs, z. B. Zugangsdaten, Kreditkartendaten, …
- Manipulation des Netzwerkverkehrs, z. B. beim Onlinebanking
- Einschleusen von Schadcode, z. B. Botnet-Client, Trojaner, …
- Angriff auf andere Rechner im Internet
- illegales Filesharing, Versand strafbarer Inhalte, Massenversand von E-Mail
- Übernahme von mit dem WLAN verbundenen Alltagsgeräten

Handelt es sich hierbei um eine konstruierte oder eine realistische Bedrohung? Wird dies nur von einigen wenigen Kriminellen oder Scriptkiddies ausgenutzt? Hierzu ein Beispiel aus den Medien: *Im Jahre 2011 konnte die Polizei in Seattle eine Bande festnehmen, welche über fünf Jahre hinweg in schlecht gesicherte Funknetze eingebrochen ist und so wertvolle Informationen stehlen konnte.*[6]

Für den WLAN-Betreiber ist es schwer bis unmöglich, einen solchen Angriff festzustellen. Das größte Problem ist allerdings das mangelnde Sicherheitsbewusstsein in der Bevölkerung. Zum einen wird davon ausgegangen, dass die erworbenen WLAN-Router bereits bei Inbetriebnahme ausreichend geschützt sind. Sowohl dieser Trugschluss als auch die Tatsache, dass von den Herstellern benutzte Standardeinstellungen inkl. Standardpasswort auch (vermeintlich) gut gesicherte WPA2-Netzwerke[7] angreifbar machen, sind sehr beunruhigend. Hinzu kommt ein unbegründetes Sicherheitsgefühl, da kaum jemand davon ausgeht, dass der eigene Internetanschluss für Straftaten missbraucht werden könnte.

Am Vorliegen mindestens eines der folgenden Punkte erkennt ein Angreifer sofort, ob es sich beim gescannten Netzwerk um ein potenzielles Ziel handelt:

- das Netzwerk ist offen
- das Netzwerk ist nur WEP-verschlüsselt
- der verwendete WLAN-Router stammt von einem Hersteller, dessen Geräte für Fehler und schlechte Programmierung bekannt sind
- bei dem sichtbaren Namen des WLAN handelt es sich um einen Standardnamen, welcher vor dem Verkauf automatisch vom Hersteller vergeben wird (hier ist die Chance sehr hoch, mit einem Standardpasswort eindringen zu können)

Um in ein WEP-geschütztes Netz einzubrechen, bedarf es weder starker Rechenleistung noch umfangreichen Vorwissens (vgl. dazu einschlägige YouTube-Videos im Netz). Neben einem Smartphone als Wardriving-Ausrüstung genügt z. B. ein *Raspberry Pi*[8] an einer Powerbank mit angeschlossenem WLAN-USB-Adapter (Abbildung 5), um WEP zu brechen. Über den WLAN-Adapter kommuniziert der *Raspberry Pi* mit dem Smartphone (oder z. B. einem Tablet), von wo aus er über eine SSH-App[9] gesteuert wird.

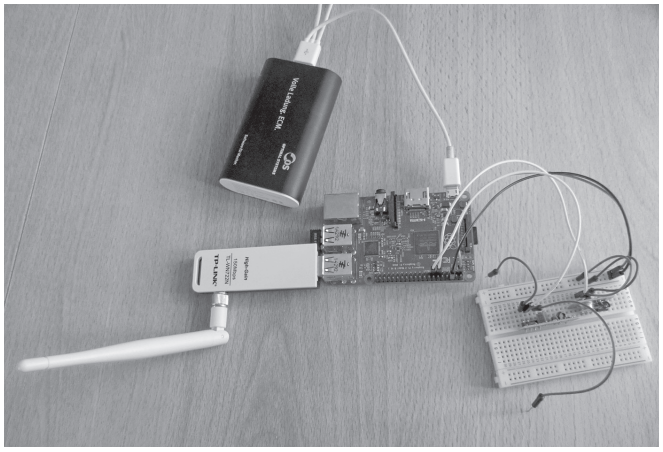


Abbildung 5: Raspberry Pi als modernes Hilfsmittel für Wardriving. Foto: eigene Aufnahme

Aber auch WPA2-geschützte Netzwerke sind mit einer solchen Ausrüstung erfolgreich angreifbar. Das WLAN-Passwort muss ja nicht unbedingt vor Ort entschlüsselt werden. Ist beispielsweise bekannt, dass an einem bestimmten Tag zu einer bestimmten Uhrzeit interessante Informationen über das WLAN übertragen werden sollen, so können alle zu diesem Zeitpunkt übertragenen Datenpakete empfangen und gespeichert werden. Wird im gleichen Zug ein Handshake[10] mit aufgezeichnet, kann zu einem beliebigen späteren Zeitpunkt versucht werden, das Passwort zu entschlüsseln (z. B. in einem leistungsstarken Rechnerverbund). Ist dies gelungen, können die aufgezeichneten Pakete nachträglich lesbar gemacht werden. Es ist zudem möglich, über das WLAN übertragene Druckaufträge zu rekonstruieren und in einer Datei abzuspeichern.

Mittels Wardriving lassen sich aber nicht nur Netzwerke in Gebäuden oder Plätzen erfassen. Auch mobile Hotspots von Notebooks oder mobilen Endgeräten können hierbei erfasst werden. Eine gänzlich neue Gefahr stellt WLAN in Fahrzeugen dar. Sollte das Fahrzeug gehackt und dadurch nicht mehr durch den Fahrer kontrolliert werden können, kann dies lebensbedrohlich enden.[11] Aufsehen erregten die Erfolge von Dr. Charlie Miller (ehemals NSA-Mitarbeiter) und Chris Valasek, welchen es gelang, aus großer Entfernung die Kontrolle über einen Jeep zu übernehmen.[12] Das vom Bund geförderte Sim^{TD}-Projekt soll in Zukunft Verkehrsdaten in Echtzeit erfassen und die vorhandenen Fahrerassistenzsysteme des Fahrzeugs erweitern.[13] Auch bei diesem – auf dem WLAN-Standard basierenden – System besteht die Gefahr der Übernahme durch einen Angreifer und des Verlusts der Fahrzeugkontrolle.

Neben der Vielzahl an Schwächen oder sogar Programmierfehlern in der Steuersoftware/Firmware von WLAN-Routern gibt es auch Schwächen in den Sicherheit suggerierenden werksseitig vergebenen Passwörtern der verkauften WLAN-Router. Auf

legalen wie illegalen Hackerseiten finden sich mittlerweile eine ganze Reihe entdeckter Probleme hinsichtlich der in WLAN-Routern verwendeten Standardpasswörter. In einigen Fällen konnte der Algorithmus zur Generierung der Standardpasswörter bestimmt werden. Auch letzteres ist sehr problematisch, da einige Hersteller von WLAN-Routern das Standardpasswort (oder zumindest Teile davon) mehr oder weniger direkt aus der MAC-Adresse und dem ebenfalls voreingestellten Netzwerknamen (SSID) der WLAN-Schnittstelle berechne(te)n[14] und diese Werte meist vom WLAN-Router bekanntgegeben werden[15].

Der WLAN-Router-Hersteller Arcadyan hat 2008 seinen Algorithmus zur Generierung des Standardpasswortes für seine Geräte in Deutschland sogar zum Patent angemeldet[16] und damit freiwillig öffentlich gemacht. Standardpasswörter für Geräte anderer Anbieter, die Arcadyan-Komponenten verwendeten, wurden gleichfalls nach diesem Algorithmus berechnet, dies betraf in Deutschland z. B. Arcor, EasyBox und Vodafone. Auf Basis der ausführlichen Patentbeschreibung wurden von privater Seite einige Passwortgeneratoren[17] erstellt und zum kostenlosen Download bereitgestellt. Durch Variation der Netzwerknamen blieben für jeden der drei genannten Anbieter nur noch 65536 mögliche Passwörter übrig, die selbst von einem älteren Notebook innerhalb weniger Sekunden getestet werden konnten. Sicherheitsvorkehrungen, wie beispielsweise eine Beschränkung der Anmeldeversuche pro Minute, sind hier wirkungslos, da die Passwörter an aufgezeichneten Datenpaketen getestet werden können. Zudem gibt es eine Vielzahl an Internetseiten, auf welchen gefundene Standardpasswörter und Algorithmen[18] aufgelistet sind; dort kann man auch gut nach bestimmten Gerätetypen und -modellen suchen. Diese Beispiele sollten zum Nachdenken darüber anregen, ob wir uns nicht sicherer fühlen als wir tatsächlich sind.

Neue Ansätze bringt die LINUX-basierte Open-Source-Software *Snoopy-NG* mit sich. Das Tool schneidet alle (über die unterschiedlichsten Funktechnologien) empfangenen Informationen des Gerätes mit, auf dem es (evtl. auch ohne Wissen des Gerätebetreibers) installiert ist, und wertet sie aus. Jedes mobile Gerät sendet bei der Suche nach gespeicherten Netzwerken ununterbrochen *Probe Requests*[19], aus denen sich die weltweit eindeutigen MAC-Adressen der Access Points dieser WLANs ermitteln lassen. Findet man diese MAC-Adressen anschließend in Wardriving-Datenbanken (wie *wigle.net* oder *wardriving-forum.de*), lassen sich in vorhandenen Bewegungsprofilen weitere Aufenthaltsorte ergänzen. Werden die von *Snoopy-NG* erfassten Daten ebenfalls in einer Datenbank abgelegt, könnten über obiges Vorgehen auch Beziehungen zwischen mobilen Geräten hergestellt werden, z. B. welche Geräte im selben WLAN angemeldet waren.[20]

Für Wardriving an sonst unzugänglichen Stellen (z. B. in hohen Gebäuden, abgesperrtem Gelände, Innenhöfen/-räumen) eignet sich der Einsatz von (immer günstiger werdenden) Drohnen, die mit einem Smartphone oder einem Mini-PC à la *Raspberry Pi* bestückt werden.[20] Die ausgespähten Informationen werden auf der Drohne gespeichert oder über Mobilfunk zu einem frei wählbaren Ziel verschickt.[21]

Neben dem Zugang zu geschützten Netzwerken gibt es auch eine Vielzahl an offenen Netzen. Die Zahl von frei zugänglichen Hotspots in Deutschland nimmt weiter zu. Diese könnten natürlich ebenfalls für illegale Tätigkeiten aller Art missbraucht werden.

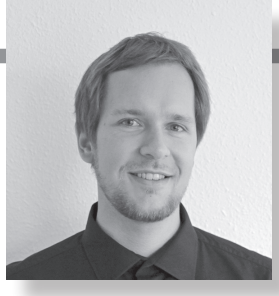
Schutzmaßnahmen

Gegen Wardriving selbst kann man sich nicht direkt schützen. Bedeutend wichtiger ist der Schutz des Zugangs zum eigenen WLAN. Da Wardriving normalerweise nur von außerhalb der Räume der Ausgespähten durchgeführt wird, muss darauf geachtet werden, dass das eigene WLAN-Signal sich nur in erwünschte Bereiche ausbreitet. Erreicht werden kann dies beispielsweise durch Ausrichten der Antennen des WLAN-Routers oder das Anbringen von reflektierender Alufolie.[22]

Für Angreifer wird Wardriving uninteressant, sobald mit angemessenem Zeitaufwand keine offenen oder schlecht gesicherten Funknetze mehr auffindbar sind. Somit besteht ein sinnvoller Schutz darin, das WLAN mit den besten zur Verfügung stehenden Mitteln abzusichern und einen Einbruch in das Netz in akzeptabler Zeit unter Einsatz von angemessenen Mitteln unwahrscheinlich zu machen. Doch kann das notwendige Wissen oder Interesse der Nutzer nicht vorausgesetzt werden. An dieser Stelle ist die Unterstützung der Politik, der Medien und der Industrie gefragt. Nachfolgend zwei positive Beispiele:

- Die indische *Mumbai Police* ist seit 2009 auf Streife, um ungesicherte Funknetzwerke in Mumbai aufzuspüren.[23] Auslöser waren Attentate im Jahre 2008. Dort wurden vermutlich Funknetzwerke für die Koordinierung der Angriffe genutzt.

- Seit März 2012 überprüft die australische Polizei regelmäßig die WLAN-Sicherheit von Brisbane.[24] Ziel ist es, die Straftat WLAN-Einbruch zu verhindern und die daraus resul-



Stefan Jäger

Stefan Jäger ist Diplom-Wirtschaftsmathematiker und arbeitet bei einem Unternehmen im Bereich des Dokumentenmanagements mit dem Schwerpunkt BOS (Behörden und Organisationen mit Sicherheitsaufgaben). Als zertifizierter IT-Sicherheitsbeauftragter in der öffentlichen Verwaltung beschäftigt er sich vor allem mit Funknetzwerken und der Sicherheit mobiler Endgeräte.

tierenden Schäden zu vermeiden. Wird ein solches WLAN entdeckt, weist die *Hi Tech Crime Investigation Unit* den Besitzer mit Bitte um Verbesserung darauf hin.

Eine sinnvolle Ergänzung stellen *Intrusion Detection Systems* (IDS) dar. Diese registrieren jeden Zugangsversuch zum WLAN. Je nach Konfiguration des IDS können so berechtigte von unberechtigten Zugriffen unterschieden werden. Bei einem unberechtigten Zugriff kann anschließend eine Warnmeldung an den Netzwerkbetreiber versandt und/oder das zugreifende Gerät abgewiesen werden.

Rechtliche Lage

In Bezug auf das Gesetz muss deutlich zwischen dem eigentlich Wardriving und dem Eindringen in ein fremdes WLAN unterschieden werden. Für Wardriving im ursprünglichen Sinne ist nur § 30 StVO (Umweltschutz, Sonn- und Feiertagsfahrverbot) einschlägig, in dem unter anderem geregelt ist: „Unnützes Hin- und Herfahren ist innerhalb geschlossener Ortschaften verboten, wenn Andere dadurch belästigt werden." Da es sich beim Begriff „unnütz" um eine Auslegungssache handelt, ist eine Verurteilung relativ unwahrscheinlich.

Folgende Gesetze sind zum Thema WLAN relevant[25]:

- § 202a StGB Ausspähen von Daten
- § 202b StGB Abfangen von Daten
- § 206 StGB Verletzung des Post- oder Fernmeldegeheimnisses
- § 263a StGB Computerbetrug
- § 265a StGB Erschleichen von Leistungen
- § 303a StGB Datenveränderung
- § 303b StGB Computersabotage
- § 89 TKG Abhörverbot, Geheimhaltungspflicht der Betreiber von Empfangsanlagen
- § 148 TKG Strafvorschriften
- § 17 UWG Verrat von Geschäfts- und Betriebsgeheimnissen

Ist das Netzwerk ungesichert, kommen nur Straftaten im Sinne von Diebstahl, Manipulation und Sabotage in Betracht. Sollte das Netzwerk geschützt sein, kommt noch Einbruch hinzu. Handelt es sich dabei lediglich um die Umgehung einer Sicherheitsvorkehrung, spricht man von Hausfriedensbruch, dies kann nach den §§ 123 und 124 StGB verurteilt werden. Dient der Einbruch der Ermöglichung eines Diebstahls, kommen die §§ 243 und 244 StGB in Betracht. Bei einigen der aufgeführten Gesetze liegt das Strafmaß bei 2 bis 5 Jahren Freiheitsstrafe oder Geldstrafe. Sollten aus den oben genannten Straftaten noch Personenschäden resultieren, so steigt das Strafmaß erheblich. Im Netz gibt es gute Literaturzusammenstellungen[25] bzw. Zusammenfassungen[26] zur Thematik.

Frei zugängliche *Hotspots* in deutschen Städten kommen nur langsam voran, da zwar nur wenige gesetzliche Einschränkungen existieren, aber dennoch mehr als in anderen Nationen. So müssen die Betreiber von Hotspots aufgrund der *Störerhaftung* zumindest teilweise für die Handlungen der Nutzer haften, da der WLAN-Betreiber sein Netzwerk für deren (u.U. auch illegale) Handlungen bereitstellt. Zudem unterliegt der Betreiber Prüfungs- und Belehrungspflichten gegenüber allen Netzwerknutzern. Der Bundesgerichtshof hat mit der Entscheidung vom 12. Mai 2010 festgelegt, dass der unbeteiligte Betreiber nur zu max. 100 € Abmahnkosten verurteilt werden kann, falls sein Netzwerk für Urheberrechtsverletzungen im Internet genutzt wurde.[27]

Große Datensammler

Nicht nur Wardriver, sondern auch Institute und Unternehmen sammeln die WLAN-Daten. So überrascht es nicht, dass der größte Datensammler der Welt, *Google,* auch mit dabei ist. 2010 wurde bekannt, dass Google während der Fotoaufnahmen für das Projekt *StreetView* auch WLAN-Daten aufzeichnet. Als Reaktion veröffentlichte Google ein Schreiben[28], aus welchem hervorgehen sollte, dass das Unternehmen nichts Illegales getan hätte. Es würden lediglich WLAN-Name (SSID), MAC-Adresse und Geopositon aufgezeichnet. Ziel sei es, die Lokalisierungs- und Navigationsdienste zu verbessern. Rechtfertigung suchte Google beim Verweis auf analoges Vorgehen bei *Skyhook* und dem *Fraunhofer-Institut*. Die öffentlichen Bedenken, Google würde personenbezogene Daten aufzeichnen wollen, wies das Unternehmen zurück. Der damalige Bundesdatenschutzbeauftragte Peter Schaar sagte zur Namensgebung der Netzwerke: „Bei letzterer verwenden Privatpersonen nicht selten ihre Klarnamen oder andere auf sie hinweisende Informationen. Sowohl mit Blick auf die Benutzung des eigenen Namens als auch auf die Möglichkeit, die WLAN-Netze aufgrund ihrer örtlichen Lage Bewohnern von Häusern zuzuordnen, handelt es sich um die Erfassung und Speicherung personenbezogener Daten und deren Übertragung in die USA."[29]

Neben dem Problem, dass mit den WLAN-Daten auch die StreetView-Bilder der Wohnungen und Häuser verknüpft sind, wurde publik, dass Google auch den Datenverkehr von offenen Funknetzen mitgeschnitten hatte. Nach der Stellungnahme von Google hatte der hamburgische Datenschutzbeauftragte Caspar um Prüfung der Inhalte der durch Google aufgezeichneten Daten gebeten. Bei der internen Überprüfung durch Google wurde festgestellt, dass ohne Absicht der Funkverkehr mitgeschnitten worden war. Dies ist einem der größten und innovativsten Softwareunternehmen der Welt schwer zu glauben. Google ordnete die Löschung dieser Daten und das Stoppen der WLAN-Datensammlung an. Anschließend musste Google an mehrere Einrichtungen Strafen bezahlen, so z. B. an die hamburgische (145.000 €) und an die französische Datenschutzbehörde CNIL (100.000 €).

2011 wurde bekannt, dass das Google-Betriebssystem Android den Netzwerknamen, die MAC-Adresse und die Geoposition aller WLAN-Netze, mit denen das Gerät verbunden ist, an Google überträgt. Hinzu kommen die MAC-Adressen aller Geräte, welche mit dem mobilen Gerät verbunden sind, sobald dieses als Hotspot fungiert. Der Entwickler Samy Kamkar stellte gegen den Willen von Google eine Website zur Verfügung, auf welcher man sich bei Eingabe der MAC-Adresse den zuletzt übermittelten Standort anzeigen lassen konnte.[30] Solch eine Funktion bietet auch die Website *wardriving-forum* an. Während aber die Mitglieder des Forums eher zufällig zu ihren Informationen kommen, werden Scans durch Google automatisch und in regel-

mäßigen Abständen durchgeführt. Dies könnte zur Ortsbestimmung eines bestimmten Mobilfunkgerätes oder einer Person, die dieses mit sich führt, und zur Erstellung von Bewegungsprofilen missbraucht werden.

Fazit

Wardriving ist nicht grundsätzlich kriminell: es kann (und sollte) auch zur präventiven Erkennung schlecht gesicherter Netze eingesetzt werden. Dass Wardriving von Kriminellen im Rahmen von Cyberattacken eingesetzt wird, dürfte sich auch zukünftig nicht prinzipiell verhindern lassen. Versuchen der Industrie (sowie der Behörden und Geheimdienste), mittels Wardriving die Perfektionierung des *gläsernen Bürgers* weiter voranzutreiben, kann und muss jedoch entschieden widersprochen werden.

Aus den aufgeführten Punkten ergibt sich ein größerer Handlungsbedarf für die Politik, die Industrie und vor allem die Medien. Dem Beispiel Indiens und Australiens folgend, sollte ein Team aus entsprechend geschulten Polizisten präventiv die WLAN-Sicherheit der Bevölkerung überprüfen. Die Router-Hersteller sehen derzeit nur Druck aus Wettbewerbssicht. Gesetzlich sind sie lediglich zum Anbieten einer zeitgemäßen Verschlüsselung verpflichtet. Ein Muss sollte es sein, jeden ausgelieferten Router mit voreingestelltem WPA2 und einem zufällig erzeugten langen und sicheren Passwort zu versehen.

Darüber hinaus sollten kundige Anwender ihre WLAN-Router aber auch selbst konfigurieren. Sind Netzwerke gut geschützt und für Unbefugte unsichtbar, und besitzen sie nicht auf die Betreiber zurückführende Namen, werden sie für Angreifer und für den kommerziellen Missbrauch schnell uninteressant. Allerdings führt die Fülle möglicher (und auch noch stark vom konkreten Routermodell abhängiger) Einstellungen schnell zu Überforderung. Für Laien ist es vergleichsweise schwierig, hierzu an brauchbare Informationen zu gelangen. An dieser Stelle soll zumindest auf grundsätzliche Ausführungen für jedermann[31] bzw. detaillierte, auf Unternehmen[32] zugeschnitte Handlungsanleitungen hingewiesen werden.

Für Anwender ist Wissen der beste Schutz. So muss es Aufgabe der Politik sein, Aufklärungskampagnen auf den Weg zu bringen, um vor allem auch über die Medien diese Inhalte aufbereitet an die Allgemeinheit zu bringen. Die deutschen Gesetze decken die Thematik prinzipiell ausreichend ab. Das Problem stellt die Ermittlung der Täter dar. Gehen diese professionell vor und verwischen ihre Spuren, ist es mit angemessenem Aufwand kaum möglich, diese später zu ermitteln.

Anmerkungen

1 *Wikipedia: Wardriving. 20.11.2015. https://de.wikipedia.org/wiki/Wardriving*

2 *Bürger-CERT: Glossar. 20.11.2015. https://www.buerger-cert.de/glossar?index=w*

3 *Peter Shipley: 802.11b War Driving and LAN Jacking. Vortrag auf der DefCon 9, 2001. http://bit.ly/1mFQ8eO*

4 *Die Bezeichnung Access Point wird meist als Synonym für WLAN-Router verwendet. Genau genommen handelt es sich dabei aber um eine Komponente im WLAN-Router, welche für den Datenaustausch zwischen dem WLAN-Router und dem angemeldeten WLAN-Client genutzt wird.*

5 *Bei WEP handelt es sich um das erste in der Praxis verbreitete Verschlüsselungsprotokoll für Datenpakete, welche in drahtlosen Netzwerken übertragen werden. Auf Grund der Schwächen in den Grundprinzipien des Protokolls wird dringend vom Einsatz abgeraten. Erfahrene Hacker können in ein solches Netzwerk in 5–20 Minuten (abhängig vom verwendeten Router und von der Anzahl angemeldeter Clients) eindringen.*

6 *Levi Pulkkinen: Police: Wireless network hacker targeted Seattle-area businesses. seattlepi.com, 19.04.2011. http://bit.ly/1ZcfL2L*

7 *Aufgrund der Schwächen von WEP wurde im Jahre 2003 ein neues Konzept zur verschlüsselten Übertragung von Datenpaketen in drahtlosen Netzwerken unter dem Namen WPA erstellt. Eine überarbeitete und sicherere Variante von WPA wurde 2004 als WPA2-Standard verabschiedet.*

8 *Der Raspberry Pi ist einer der bekanntesten und beliebtesten Minicomputer. Aufgrund seiner sehr geringen Größe und des vergleichsweise niedrigen Preises ist er sehr gut für Eigenbauten und Prozesse jeglicher Art geeignet. Der meist mit Linux betriebene Computer kann durch eine Reihe von Modulen und Adaptern erweitert werden, wodurch die Anzahl seiner Einsatzgebiete sich um ein Vielfaches erhöht.*

9 *SSH (Secure Shell) ist ein Netzwerkprotokoll, über welches Programme, die dieses Protokoll implementiert haben, eine gesicherte Verbindung zu anderen Geräten herstellen können.*

10 *Während des Anmeldeprozesses eines Gerätes am WLAN-Router werden spezielle Datenpakete ausgetauscht. War die Anmeldung erfolgreich, konnten diese als Handshake bezeichneten Datenpakete von einem Angreifer aufgezeichnet werden. Diese stellen die Grundlage fast aller Angriffstechniken gegen WPA2 dar.*

11 *Thomas Harloff: Der Fahrer ist machtlos. Süddeutsche Zeitung, 22.07.2015. http://bit.ly/1IiGS7m*

12 *Charlie Miller & Chris Valasek: Remote Exploitation of an Unaltered Passenger Vehicle. illmatics.com, 10.08.2015. http://bit.ly/1K4CNl4*

13 *sim[TD]: Technologie. 30.11.2015. http://bit.ly/1mKCtTF*

14 *Daniel Bachfeld: Vorkonfigurierte WPA-Schlüssel bei T-Online und Vodafone leicht erratbar. heise online, 20.08.2011. http://bit.ly/1JB3VNz*

15 *Ronald Eikenberg: Router-Schwachstelle für Telefonterror missbraucht. heise Security News, 21.08.2013. http://bit.ly/1ZTqlxQ*

16 *Patent Nr. 096117094. 20.11.2008. http://bit.ly/1OGeDTq*

17 *Google-Code-Project: android-thomson-key-solver. 30.11.2015. http://bit.ly/1cldX2c*

18 *wardriving-forum.de: Standardpasswörter. 30.11.2015. http://bit.ly/14zG4ud*

19 *Bei Probe Requests handelt es sich um spezielle Datenpakete, welche von WLAN-fähigen Geräten ausgesendet werden. Diese dienen dem Zweck, dem Gerät bekannte drahtlose Netzwerke aufzuspüren, um sich anschließend mit ihnen verbinden zu können. Das Gegenstück bilden die Datenpakete, welche als Beacons bezeichnet werden. Diese werden vom WLAN-Router ausgesendet, damit Geräte in Reichweite das dort erzeugte drahtlose Netzwerk finden können.*

20 *Uli Ries: Gratis-Software macht Drohnen zu WLAN-Schnüfflern. heise Security News, 09.08.2014. http://bit.ly/1OXfZoB*

21 *Philipp Schweizer: USB Surfstick am Raspberry Pi verwenden – Mobiles Internet. Raspberry.Tips, 29.04.2015. http://bit.ly/1PUZcYu*

22 *Marco Rinne & Beate Kipphardt: Genialer WLAN-Booster im Eigenbau. Chip, 07.07.2015. http://bit.ly/1Sa0T5J*

23 *Reiko Kaps: Indische Polizei als Wardriver. heise Netze, 19.01.2009. http://bit.ly/1OTxxYT*

24 *Kai Biermann: Polizei in Australien sucht nach offenen WLANs. Zeit Online, 27.03.2012. http://bit.ly/1UEEYRQ*

25 *Herbsttagung „Tatort Internet – eine globale Herausforderung für die Innere Sicherheit" des BKA, 22.11.2007: Strafrecht in der digitalen Welt. COD-Literatur-Reihe, Band 19. http://bit.ly/1Sa140R*

26 *Stefanie Hagemeier: Das Google WLAN-Scanning aus straf- und datenschutzrechlicher Sicht. HRRS, Heft 2/2011. http://bit.ly/1VT6Cfh*

27 *Urteil des Bundesgerichtshofs vom 12.05.2010, 1 ZR 121/08 – Haftung für unzureichend gesicherten WLAN-Anschluss*

28 *Peter Fleischer: Data collected by Google cars. Google Europe Blog, 27.04.2010. http://bit.ly/1Oao0Jp*

29 *Johannes Caspar & Peter Schaar: Presseerklärung „Google-Street-View-Fahrten werden auch zum Scannen von WLAN-Netzen genutzt". datenschutz-hamburg.de, 22.04.2010. http://bit.ly/1OaogrY*

30 *Ernst Ahlers: WLAN-MAC-Adressen: Googles langes Gedächtnis. heise Netze, 16.06.2011. http://bit.ly/1K4DPgW*

31 *Marius Eichfelder: WLAN sichern: Fünf Tipps für mehr Sicherheit. Chip-Praxistipps, 06.08.2014. http://bit.ly/1JhjANY*

32 *Bundesamt für Sicherheit in der Informationstechnik: IT-Grundschutz-Kataloge. Baustein 4.6 WLAN. September 2011. http://bit.ly/1UEFM9v*

Dominik Brodowski und Felix Freiling

Transnationale Cyberkriminalität vs. nationale Strafverfolgung: Mögliche Auswege aus einem grundsätzlichen Dilemma

Cyberkriminalität wird nicht selten über Landesgrenzen hinweg begangen und stellt daher ein transnationales Phänomen dar. Die Strafverfolgung hingegen wird grundsätzlich von den Nationalstaaten betrieben und ist daher im Ausgangspunkt an nationalstaatliche Regelungen gebunden. Dieser Beitrag möchte durch einen skizzenhaften Problemaufriss zum Nachdenken über dieses grundsätzliche Dilemma anregen.

Das Problem

Das Internet stellt eine Kommunikationsinfrastruktur zur Verfügung, mit deren Hilfe sich Computer und Personen auf sehr einfache Art und Weise weltweit vernetzen können. Interaktive Webseiten wie Blogs und soziale Medien sowie ein transnational ausgerichteter E-Commerce erzeugen bei vielen Menschen den Eindruck eines Raumes gr
freiheit. Dass mit dem Internet
doch nicht verschwunden sind,
wenn man selbst Opfer von Cy
etwa durch betrügerische Nutzu
formationen oder dadurch, dass man seinen eigenen Rechner nach einer Infektion mit erpresserischer Ransomware freikaufen muss.

Die digitale Schattenwirtschaft agiert professionell, arbeitsteilig und seriösen Schätzungen zufolge (Anderson et al., 2013) mit großem ökonomischen Gewinn. Bei aller Notwendigkeit, die technischen Ursachen von Cyberkriminalität zu verstehen und diesen entgegenzuwirken (Brodowski & Freiling, 2011, S. 81 ff.), erfordert das soziale Problem von Cyberkriminalität auch eine (straf)rechtliche Antwort. Diese wird aber dadurch erschwert, dass Cyberkriminalität nicht vor den Grenzen der Nationalstaaten halt macht.

Auch wenn man das Internet aus technischer wie aus soziologischer Sicht als *virtuellen Cyberspace* verstehen kann, so nimmt jedes Verhalten im Internet seinen Ursprung in einem menschlichen Verhalten und lässt sich daher auf einen physischen Ort zurückführen. Neben diesem *Handlungsort* gibt es noch eine Fülle weiterer Anknüpfungspunkte dafür, dass das materielle Strafrecht eines bestimmten Nationalstaats anwendbar ist. Daher ist ein transnationales, kriminelles Verhalten im Regelfall nach dem Recht mehrerer Staaten strafbar. Das grundlegende Problem, das dieser Artikel beleuchten möchte, entsteht nun in der Vielzahl von Fällen, in denen die Strafverfolgungsbehörden in einem Staat A eine Straftat verfolgen wollen (und dürfen), dabei jedoch auf Ermittlungen in einem anderen Staat B angewiesen sind, um diese Straftat erfolgreich aufzuklären und um den oder die Straftäter wegen dieser Straftat zu verurteilen.

erschienen in der FIfF-Kommunikation, herausgegeben von FIfF e.V. - ISSN 0938-3476 www.fiff.de

nd die Strafverfolgungsbehörden
gspunkt dadurch eingeschränkt,
aber nicht im Staat B – tätig werden dürfen, ohne die Souveränität des anderen Staates zu verletzen und möglicherweise eine Straftat nach dem Strafrecht des Staates B zu begehen. Ein Beispiel hierzu aus der analogen Welt: Wenn ein Polizist aus dem Staat A ohne entsprechende Befugnis des Staates B auf dessen Staatsgebiet einen Verdächtigen festnimmt und auf verschlungenen Pfaden nach A verbringt, so wird dies zum einen zu erheblichen diplomatischen Verwicklungen führen. Da Entführungen in wohl allen Staaten strafbar sind, wird sich zum anderen der Polizist im Staat B wegen der nach dortigem Recht rechtswidrigen Entführung des Verdächtigen strafrechtlich verantworten müssen.

Es liegt somit eine Souveränitätskollision vor: Einerseits gehört es zu den Kernaufgaben eines souveränen Staates, seine Staatsgewalt in seinem eigenen Staatsgebiet auszuüben – und damit für den Staat A, sein materielles Strafrecht durchzusetzen und hierdurch auch die Restitution der durch die Straftat Geschädigten zu unterstützen. Andererseits aber bedeutet staatliche Souveränität auch, den Staat und die im Staatsgebiet ansässigen Personen vor einer Machtausübung anderer Staaten zu schützen – und damit für den Staat B, seine Bürger sowohl davor zu schützen, dass sie selbst in den Staat A verschleppt werden, als auch davor, dass ihre Daten in den Staat A transferiert werden.