# WarDriving

**aus Wikipedia, der freien Enzyklopädie**

Unter **WarDriving** versteht man das systematische Suchen nach Wireless LANs mit Hilfe eines Autos. Der Begriff leitet sich von Wardialing ab, einer Methode durch durchprobieren vieler Telefonnummern offene Modem-Zugänge zu finden.

Wardriver-Ausrüstung: Laptop mit GPS-Empfänger

## Vorgehensweise

Ein klassischer Wardriver sitzt mit einem Notebook als Beifahrer in einem Auto und spürt drahtlose Netzwerke auf. Oft wird zusätzlich eine externe Antenne verwendet, um die Reichweite zu erhöhen. Zum Auffinden vorhandener WLANs wird meist ein WLAN-Sniffer benutzt, der die Daten gefundener Netzwerke automatisch protokolliert.

Ausgehend vom Fortbewegungsmittel gibt es weitere Bezeichnungen für die WLAN Suche:

- *WarTraming*: in Brandenburg entwickeltes Aufsuchen mit Hilfe der Straßenbahn. Es ist mit einigen interessanten Randbedingungen verbunden.
- *WarWalking*: Personen, die WLANs nutzen, welche zu Fuß zu erreichen sind.
- *WarBoating*: das Aufspüren mit Hilfe von Schiffen
- *WarBiking*: das Aufspüren mit Hilfe des Fahrrads

Auch für PDAs gibt es Software, um drahtlose Netzwerke aufzuspüren, womit jemand sogar unbemerkt auf einem Firmengelände schnüffeln kann.

## Motivation

Die Gründe Wardriving zu betreiben sind unterschiedlich. Es lassen sich grob drei Gruppen unterteilen:

Die einen wollen nur Netzwerke finden und mit Hilfe von GPS-Empfängern kartographieren. Diese Gruppe hat es sich zum Hobby gemacht, die Entwicklung der WLANs zu protokollieren und sich mit der Technik zu beschäftigen und stellen Wardriver im eigentlichen Sinne dar.

Die zweite Gruppe will nur auf Sicherheitslücken hinweisen, schnell mal ins Internet oder einfach etwas harmlosen Spaß haben. Von diesen Leuten wird auch das WarChalking betrieben.

Mitglieder der dritte Gruppe bezeichnen sich auch gern als WarDriver und versuchen, in Netze einzubrechen, um Daten zu stehlen oder nutzen das Netz als Sprungbrett für weitere Angriffe. Man sollte deshalb auch streng zwischen WarDrivern und Scriptkiddies unterscheiden.

# Sicherheit

## Schutzmaßnahmen

Das Auffinden und Eindringen in das gefundene Netz ist wegen fehlender Absicherung oft sehr einfach. Im Lieferzustand einiger Wireless Access Points sind sämtliche Sicherheitsmaßnahmen deaktiviert, um dem Nutzer die Installation zu erleichtern. Aufgrund technischer Unkenntnis aktivieren viele Heimanwender die Verschlüsselung nicht, so dass es immer noch eine große Zahl ungewollt offener WLANs gibt. In ein solches ungeschütztes Netzwerk kann sich jeder, auch versehentlich, ohne spezielle Hilfsmittel einbuchen.

Durch Abschalten des SSID-Broadcasts ist es möglich, die Existenz des WLANs teilweise zu verbergen. Dies schützt jedoch nur vor unabsichtlichem Einbuchen von in der Nähe befindlichen Rechnern. Mit einem passiven WLAN-Sniffer kann man die Kommunikation zwischen Clients und dem Access-Point belauschen und so die SSID erfahren. Dies ist somit keine wirksame Sicherheitsmaßnahme.

Das Verschlüsseln der Kommunikation mittels WEP bietet zumindest einen Schutz gegen unbeabsichtigtes Einbuchen, jedoch hat dieses Verfahren Schwachstellen und ist mit speziellen Programmen innerhalb von Minuten überwindbar. In sicherheitskritischen Bereichen sollte auf WLAN verzichtet werden, oder IPSec bzw. WPA zur Verschlüsselung des Datenverkehrs eingesetzt werden.

## Möglichkeiten nach dem Eindringen

Bei nichtvorhandener oder geknackter Verschlüsselung hat ein Angreifer die Möglichkeit, sämtliche Daten die zwischen Clients und Access-Point ausgetauscht werden abzuhören. Sofern die Rechner im internen Netz des WLAN-Betreibers nicht geschützt sind, kann der Angreifer sich mit ihnen verbinden und Daten stehlen, z.B. über Windows-Freigaben. Firewalls sind als Schutzmaßnahme oft unwirksam, da sie häufig nur zwischen internem Netz und dem Internet filtern.

# Weblinks

- Einführung in WLAN, Wardriving, Sicherheit usw. (http://it-academy.cc/content/article_browse.php?ID=593)
- http://www.wardriving.com/

## Weblinks zu WarDriving-Programmen

- Netstumbler - Aktiver WLAN-Sniffer für Windows
- MacStumbler (http://www.macstumbler.com/) - Aktiver WLAN-Sniffer für MacOS X
- Airopeek (http://www.wildpackets.com/products/airopeek) Protocol Analyzer
- Kismet (http://kismetwireless.net/) - Passiver WLAN-Sniffer für Linux, *BSD, MacOS X

- KisMAC (http://kismac.binaervarianz.de/) - Passiver WLAN-Sniffer für Mac OS X
- fakeAP (http://www.blackalchemy.to/project/fakeap/) - simuliert viele falsche WLANs (zum Ärgern von WarDrivern)
- WifiFoFum (http://www.wififofum.org/) - Aktiver WLAN-Sniffer für Pocket PC 2003 (Windows Mobile 2003)
- Wellenreiter (http://www.wellenreiter.net/) - eine weitere Sniffer-Software
- Pocketwarrior (http://pocketwarrior.sourceforge.net/) - Aktiver WLAN-Sniffer für Pocket PC
- Wireless Lan 802.11X (http://www.monolith81.de/) - Zusammenstellung diverser Publikationen über Wireless Lan in englischer und deutscher Sprache sowie umfangreiches Archiv an Software für Windows und Linux.

## Dokumente

- Warchalking Karte als PDF zum ausdrucken (http://www.hellfish-rm.de/down/warchalking0_9.pdf)
- Sammlung von Dokumentationen (http://www.wireless-nrw.de/?link=doku)