

Sensible Daten auf dem Präsentierteller

„Wardriving“ heißt der neue Volkssport unter Computerfreaks und Mächtgern-Hackern. Neugierige und „Sportbegeisterte“ mit ein wenig Software-Verstand nutzen dabei den Leichtsinns vieler Zeitgenossen, die Computernetze mit Funkstrecken betreiben und einfach „vergessen“, diese gegen Eindringlinge abzusichern. RADIO-SCANNER war mit einem „Wardriver“ in Hannover unterwegs.

Fazit: Kaum zu glauben, wie leicht es ist, auf fremden Festplatten zu spionieren. Die Anleitungen und die Software fürs „Wardriving“ gibt's übrigens frei im Internet.

Funknetze: Eintritt frei !

Von Robert Krauss

Mittwoch, 15.45 Uhr. Schichtende für Freizeit hacker Ingo B. Er steigt in sein Auto, greift hinter den Fahrersitz, holt sein Notebook heraus und schaltet es ein. Nachdem der Rechner hochgefahren ist, steckt er die über Funk arbeitende W(ireless)LAN-Karte ein. Die meldet mit einem leisen Piepton ihre Einsatzbereitschaft. Ingo B. entscheidet sich für einen Nachhauseweg, der ihn durch das ehrwürdige Philosophenviertel führt, wo Rechtsanwälte, Architekten, Werbeagenturen und Ärzte ihre Büros haben. Im Viertel angekommen, startet Ingo B. seine Spezialsoftware, die ihm hilft, Funknetze aufzuspüren. Schon nach wenigen Sekunden meldet sich die Software mit einem Klingeln. Das erste Funknetz ist gefunden. Jetzt wird es richtig spannend.

Automatisch „drin“

Deutlich zeigt die Software Feldstärke, Netzwerkadresse, Netzwerkname und -hersteller. An einem Symbol erkennt der Hacker, dass er ein verschlüsseltes Netz vor sich hat. Das hebt er sich für später auf. Er fährt weiter. Ein paar Querstraßen später meldet sich die Software erneut.

Diesmal steht das Netz weit offen, eine Verschlüsselung ist nicht eingeschaltet. Der Netzwerkname deutet darauf hin, dass es zu einem in der Nähe praktizierenden Arzt gehört. Da B. sein Notebook auf eine automatische

Verbindung hin programmiert hat, ist er sofort „drin“. Nun kann er in aller Seelenruhe auf Kosten des Netzbetreibers im Internet surfen und die im Netz sichtbaren Rechner auf interessante Inhalte absuchen. Die Gefahr, entdeckt zu werden, ist gering.

Die Software Network Stumbler [1] läuft hier unter Windows. Damit handelt man sich von Netz zu Netz – ohne weitere Hürden. Im Vor-



Rund 100 Euro kostet eine Funk-LAN-Karte für Laptops – wie diese von Orinoco.

Fotos: Dieter Hurcks

beifahren, aus dem Auto heraus. Nur die Netzwerke, bei denen im grauen Kreis ein Schloss zu sehen ist, sind verschlüsselt.

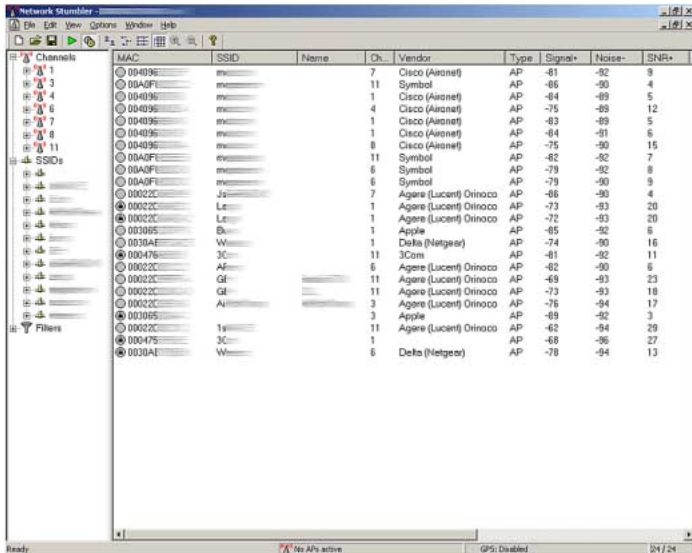
Volkssport Wardriving

Unter „Wardriving“ versteht man das Aufspüren von Funknetzwerken – Wireless Local Area Networks (WLANs) – durch geeignete Hard- und Software. Man benötigt nur ein Notebook oder einen Minicomputer (PDA) mit dem Betriebssystem Windows (oder Linux), eine WLAN-Karte und eine geeignete Software, die diese Karte auch unterstützt.

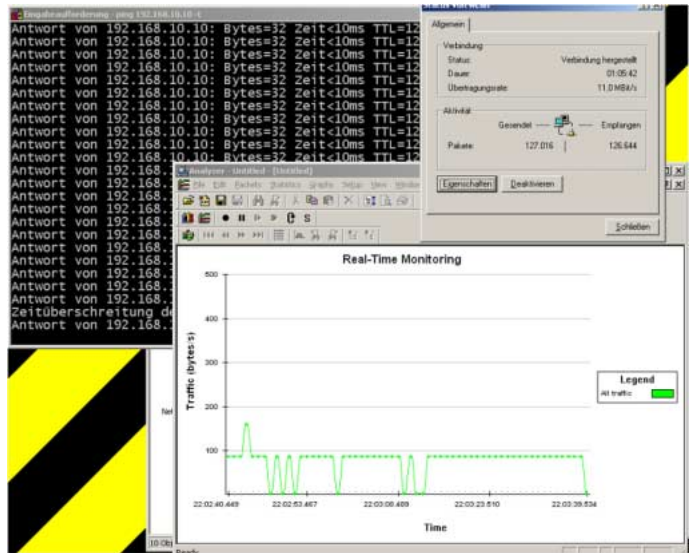
Entsprechende Programme findet man im Internet in großer Auswahl und meist kostenlos für Linux [2] und Windows [1].

Einige Lösungen bieten zusätzlich einen GPS-Anschluss. Damit kann per Satellitennavigation der Standort eines entdeckten Netzes automatisch an entsprechende Internet-Server weitergeleitet werden. Spezielle Landkarten mit Funknetz-Standorten erstellt der Server automatisch. Sehr zur Freude anderer Surfer, die sich somit nicht einmal mehr selbst auf die Suche machen müssen.

Meist durch einfaches Herumfahren oder -laufen werden Funknetze entdeckt und können, wenn sie ungesichert sind oder unfachmännisch eingerichtet wurden, sofort benutzt werden.



Die Software Network Stumbler [1] läuft hier unter Windows. Damit hängt sich der Wardriver von Netz zu Netz – ohne weitere Hürden. Einfach so im Vorbeifahren, aus dem Auto heraus. Nur die Netzwerke, bei denen im grauen Kreis ein Schloss zu sehen ist, sind verschlüsselt.



Mit Hilfe einiger im Internet frei verfügbarer Lösungen [7] lassen sich Funknetze leicht einrichten und dadurch stabilisieren. Hier werden z. B. mit Hilfe eines Dauer-Ping und einer Echtzeitdatenanalyse zwei WLAN-Karten optimal aufeinander ausgerichtet.

Software im Internet

Die zum Wardriving notwendigen Werkzeuge in Form von Software und detaillierten Anleitungen sind in hoher Qualität, kostenlos und legal aus dem Internet ladbar. Den Rest steuern die Funknetzbetreiber selbst bei: keine Änderung der vom Hersteller vorgegebenen Parameter, keine Verschlüsselung oder Aktivierung anderer Zugangsbeschränkungen.

Auspacken, einschalten, geht – warum also soll sich der Installateur noch mit dem Handbuchstudium abgeben – alles reine Zeitverschwendung. Ein gefährlicher Fehlschluss!

Ob diese Art von Freizeitaktivitäten strafbar ist, ist darüber hinaus unter Rechtsexperten durchaus umstritten. Im Strafgesetzbuch (StGB) steht unter „Ausspähung von Daten“ (§ 202a StGB) geschrieben: „Wer unbefugt Daten, die nicht für ihn bestimmt und die gegen unberechtigten Zugang besonders gesichert sind, sich oder einem anderen verschafft, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft...“ [3]. Von „besonders gesichert“ kann bei vielen Funknetzen aber, wie gesehen, keine Rede sein.

Technische Grundlagen

Der Standard IEEE802.11b [4] für Wireless LANs, der die drahtlose Kommunikation mit Datentransferraten bis zu 11 MBit pro Sekunde definiert, verwendet das weltweit lizenzfreie Frequenzband bei 2,4 GHz. 14 Übertragungskanäle sind verfügbar. Auch in Mikrowellengeräten oder für das kurzreichweitige Protokoll Bluetooth, das aber eher z.B. für den Anschluss einer Funkmaus an einen Rechner gedacht ist, wird dieses Frequenzband verwendet.

Der alte Standard 802.11 war zunächst auf 2 MBit definiert. Dort waren auch noch zwei verschiedene Sendeverfahren vorgesehen: das „Direct Sequence Spread Spectrum“ (DSSS, 2 MBit als Standard und Fallback auf 1

MBit bei schlechter Netzverbindung) und das „Frequency Hopping Spread Spectrum“ (FHSS, standardmäßig mit 1 MBit und optionaler Erhöhung auf 2 MBit in Situationen mit sehr guter Feldstärke).

Bei der Variante 802.11b, die mit bis zu 11 Mbit/s Bandbreite arbeiten kann, ist heute nur noch das Sendeverfahren DSSS gebräuchlich. Das Protokoll 802.11 ist sehr robust und funktionsreich. Es beinhaltet unter anderem auch eine Sequenzkontrolle und Felder für Wiederholungsversuche. Das ermöglicht unter anderem einen auf den MAC-Adressen der beteiligten Geräte basierenden Handshakebetrieb, der Störungen untereinander minimiert und so die nutzbare Bandbreite maximiert.

Bis 300 Meter Reichweite

Die Reichweite eines WLANs kann in Abhängigkeit der Umgebung von 20 m im Gebäude

Internet-Links

- [1] Network Stumbler, <http://www.netstumbler.com>
 - [2] AirSnort, <http://sourceforge.net/projects/airsnort/>
 - [3] Strafgesetzbuch § 220a, <http://dejure.org/gesetze/StGB/202a.html>
 - [4] IEEE-Norm 802.11, <http://grouper.ieee.org/groups/802/11/>
 - [5] Pringles-Dose als Antenne, <http://www.oreilynet.com/cs/weblog/view/wlg/448>
 - [6] Reg TP, <http://www.regtp.de/aktuelles/pm/02599/index.html>
 - [7] Net-Analyzer, <http://netgroup-serv.polito.it/analyzer>
 - [8] Languard Network Security Scanner, <http://www.gfi.com/lannetscan/>
 - http://www.freenet.de/mobil/drahtlose/Netze_Hacker_Software_Landkarten...
 - <http://www.tgnet.de/v2/connectivity/wireless/sicherheit/>
- zur Sicherheit von Kabel- und Funknetzen
Test-Netzwerkkarte von www.orinocowireless.com

bis zu 300 m auf freiem Feld betragen. Mit speziellen Richtantennen, deren Selbstbau auch mit Hilfe von Kartoffelchipverpackungen [5] möglich ist, lassen sich Entfernungen bis zu einigen Kilometern überbrücken. Anleitungen dafür sind ebenfalls im Internet problemlos auffindbar.

Sicherheit

Unter der Bezeichnung „Wireless Equivalent Privacy“ (WEP) ist optional eine Verschlüsselung mit bis zu 128 Bit zuschaltbar. Auf Grund von Designschwächen von WEP ist es allerdings relativ problemlos möglich, den Schlüssel zu knacken. WEP verwendet als Grundlage den RC4-Algorithmus von RSA; dieser generiert aber, vereinfacht gesagt, zu viele ähnliche Schlüssel.

Das macht das Protokoll angreifbar. Dazu ist es jedoch notwendig, dass genügend verschlüsselte Datenpakete aufgefangen werden können. Ein vielbenutztes Netz ist daher schneller geknackt als eines, auf das nur zeitweise zugegriffen wird.

Sind WLANs schädlich?

Es gibt auch in diesem Bereich keine Studien oder endgültige Aussagen. Allerdings sind die verwendeten Leistungen mit maximal 100 mW so niedrig, dass das WLAN weniger gefährlich als ein Mikrowellengerät, ein Handy oder ein DECT-Schnurlostelefon sein dürfte.

Die in diesem Frequenzbereich festgelegten Grenzwerte werden so weit unterschritten, dass WLAN-Karten sogar teilweise für den Einsatz im Medizinbereich zertifiziert sind. Die Access Points, die Basisstationen des WLANs, senden nicht permanent, sondern nur, wenn tatsächlich Datenübertragungen stattfinden. Der Access Point ist daher, anders als bei Mobilfunk-Basisstationen, funktentechnisch nicht aktiver als der Client-Rechner.

So arbeitet ein Funknetz

Ein WLAN besteht aus verschiedenen, modular aufgebauten Komponenten. Die wichtigsten sind der Access Point, die WLAN-Netzwerkarte für PCs/Laptops (PCMCIA), die PCI-Steckkarte oder der USB-WLAN-Adapter.

Der Access Point ermöglicht gemeinsame Kommunikation, indem er sich als Hub (eine Art Datenverteiler „an alle“) für WLAN-Karten darstellt. Zum drahtgebundenen Netz hin verhält sich der Access Point wie eine Bridge (verbindet verschiedene Netzwerke).

Mehrere Access Points können darüber hinaus größere Funkzellen bilden. Mit Hilfe von geeigneten Antennen sind im Richtfunkbetrieb bei einer Sichtverbindung der Endstellen bis zu 15 Kilometer zu überbrücken.

Einige Geräte bieten auch einen sog. „Infrastructure-Mode“. Damit lassen sich Funkzellen ähnlich der GSM-Technik erzeugen. Dadurch könnten gerade in Ballungsgebieten die im Aufbau befindlichen UMTS-Netze eine empfindliche Schlappe erleiden.

Die WLAN-Technik ist erprobt und vergleichsweise sehr kostengünstig. Und mit Datenübertragungsraten bis zu 54 MBit/s steht der im 5,2 GHz-Bereich betriebene 802.11a-Standard bereits in den Startlöchern.

Erst im Juli 2002 hat die RegTP [6] den Frequenzbereich freigegeben. Die 11 MBit/s, die mit dem 802.11b-Standard möglich sind, werden dabei um fast das Fünffache übertroffen. Diese Leistung reicht aus, um auch bandbreitenaggressive Anwendungen wie Video- und

Internetradiodienste sowie die Übertragung großer Dateien gleichzeitig zu nutzen.

Die WLAN-Netzwerkarten werden als Clients in PCs oder Notebooks eingesetzt.

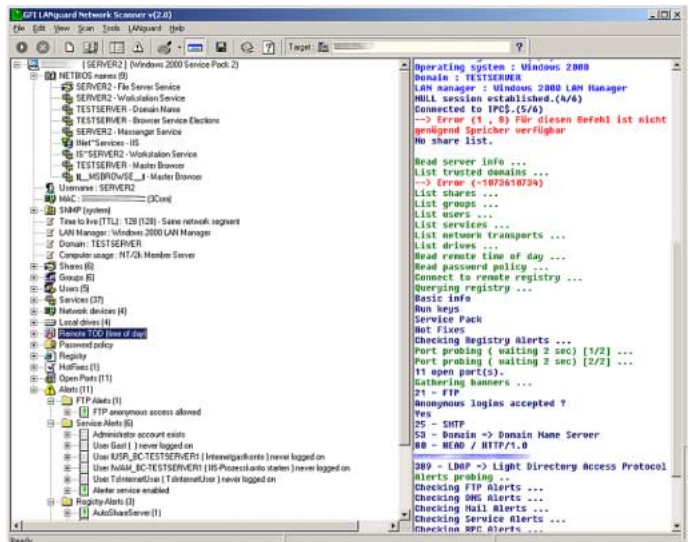
Bei einigen Herstellern werden sie auch im Innenleben von Access Points verwendet.

WLAN-Karten untereinander können sich zu Ad-Hoc-Netzen zusammenschließen und so ein komplikationsloses Peer2Peer-Netzwerk aufbauen. In diesem Modus sind allerdings in der Regel die Reichweiten geringer.

Sicherheitsvorkehrungen

Auch wenn die WEP-Verschlüsselung prinzipiell angreifbar ist, sollte der User nicht auf sie verzichten. Denn für die meisten Eindringlinge reicht diese Hürde aus.

Gerade in Netzen die nicht so häufig benutzt werden, wenn z. B. nur der Chef eine WLAN-Karte in seinem Notebook hat, dauert es sehr lange, bis die Hack-Software das Kennwort entschlüsselt hat – durchaus auch mehrere



Scan [8] eines Windows-2000-Servers. Er dauert nur Sekunden und ist für normale User und Administratoren nicht zu entdecken. Mit den hier erschnüffelten Informationen wird der Dateneinbruch zum Kinderspiel.

Tage, in denen das Netz ununterbrochen belauscht werden muss. Das ist aber nur die einfachste Form der Sicherung.

Viele Access Points verfügen darüber hinaus über weitere Sicherheitsfunktionen. So ist es z. B. in der Regel möglich, die Nutzung auf bestimmte MAC-Adressen, das ist die eindeutige Seriennummer der Netzwerkarte, zu beschränken. Zwar sind auch MAC-Adressen leicht zu fälschen, aber herauszufinden, welche überhaupt benutzt werden dürfen, ist

bogerfunk Der Scanner Spezialist

Katalog mit Preisliste anfordern: 6.--€ (Briefm./Scheck)

 <p>AOR® AR-8200MKII</p> <p>100kHz - 2040MHz Allmode, 37 Steps / Sek. 3001 Speicher Schnittstelle Option-Steckkarten</p>	 <p>AOR® AR-7030</p> <p>0 - 32MHz Kurzwellenempfänger mit Schnittstelle, Fernbedienung, uvm.</p>	 <p>AOR® AR-5000</p> <p>5kHz - 2,6GHz verschiedene Modelle und Einbaumöglichkeiten *Sprachinverter *zusätzliche Filter *uvm.</p>	 <p>AOR® SDU-5500</p> <p>Spektrum-Display-Unit für AR-3000A/AR-5000 ICOM R7000, R8500 und andere(*) mit 10,7MHz ZF Ausgang (*) ohne Steuermöglichkeit</p>	 <p>AOR® AR-3000A</p> <p>100kHz .. 2036MHz All Mode 50Hz .. 9,9995MHz Step 50 Steps/Sek. 400 Speicher 14 Bandpässe RS-232 Schnittstelle</p>
---	--	--	--	---

Aktuelle Angebote von folgenden Herstellern

ICOM YAESU SONY YUPITERU ALAN KENWOOD

 <p>AOR® SA-7000</p> <p>Breitband-Passivantenne 30kHz - 2GHz</p>	 <p>AOR® DA-3000</p> <p>Diskontantenne 30MHz - 2GHz</p>	 <p>AOR® HS-1/BOA-3500</p> <p>Log-Per Antenne 700 - 3500MHz inkl. Holzstativ</p>
 <p>AOR® HE-011</p> <p>50kHz - 200MHz</p> <p>Die beste HE-011 die es je gab</p>		<p>ROHDE & SCHWARZ</p>

Grundesch 15, 88326 Aulendorf/Steinbach Tel. (0 75 25) 4 51, Fax (0 75 25) 23 82, eMail: bogerfunk@t-online.de
 Öffnungszeiten: Mo - Do 7.00 - 17.30 / Fr 7.00 - 16.00 täglich Versand ONLINE-SHOP www.boger.de
 BOGERFUNK SCHWEIZ Großhandel: Bahnhofstraße 4 CH-8590 Romanshorn Tel. + Fax (071) 4611057

schon eine Schwierigkeit für sich. Für die Mehrzahl der Freizeithacker dürfte spätestens an dieser Stelle der Spaß vorbei sein. Auch der meist per Voreinstellung (Default) aktivierte DHCP-Server sollte abgeschaltet werden. Wer jetzt noch an seine WLAN Karte feste IP-Adressen vergibt und nur diesen die Nutzung des Access Points gestattet, schiebt den blinden Passagieren im eigenen Netz einen weiteren Riegel vor. Wer sein WLAN besonders sichern möchte, kommt nicht umhin, seinen Datenverkehr zusätzlich noch mit einem VPN (Virtuelles Privates Netz) auf der Basis von starker Verschlüsselung zu sichern. Auch hier sind freie Lösungen für alle Betriebssysteme im Web zu finden.

Die Kosten sind minimal. Eine WLAN-Karte ist schon ab 75 € zu haben, für einen Access Point muss man etwa 250 € locker machen. Wer auch mit gebrauchten Geräten auf die „Jagd“ gehen will, findet bei den einschlägigen Auktions-Anbietern oft noch wesentlich günstigere Angebote.

Risiken und Nebenwirkungen

Nach der alten Bauernweisheit, dass in 90 % aller Fälle das Problem vor dem Gerät sitzt, bleiben aber alle Hinweise ungenutzt und das Handbuch wird zur Kaffeetaschenunterlage degradiert. Da darf man sich dann nicht wundern, wenn die nächste Onlinerechnung höher als erwartet ausfällt oder wenn gar der Staatsanwalt vor der Tür steht. Wer sagt denn, ob nicht ein Mitarbeiter der Firma A vor der (WLAN)-Tür des Konkurrenten, der Firma B,



In nicht mal einer Stunde haben die Bastler aus einer Dose und ein paar weiteren Teilen eine Richtantenne mit 12 dB Gewinn gemacht. Gesamtkosten laut Internet-Seite (5): 6,45 Dollar. Unten: die Einzelteile.



steht, sich als Mitarbeiter der Firma B ausgibt und sich selbst, also A, beleidigt. In der späteren Beleidigungsklage weisen alle Indizien auf die Firma B als Urheber hin. Da wird es dann schwierig, das Gegenteil zu beweisen.

Natürlich gibt es auch Flatrate-User die das soziale Gewissen plagt und die deshalb ihren Mitmenschen oder Nachbarn freiwillig ein schnelles Tor zu Internet öffnen. Wenn dieses Phänomen um sich greift, werden einigen Mobilfunkbetreibern die Augen tränen. Wer wird dann noch freiwillig die horrenden Gebühren für GPRS oder UMTS zahlen wollen? Man darf gespannt sein.

Sichere Voreinstellungen nötig

Das Hacken von Funknetzen ist ein Kinderspiel – die Absicherung dagegen allerdings auch. Aber solange User und Administratoren die elementarsten Kenntnisse ihrer Zunft nicht beherrschen wollen, werden wohl weiter Tag für Tag gelangweilte oder neugierige Zeitgenossen in ihren Autos auf der Suche nach „Bandbreite“ das Wohngebiet umkreisen. Die Hemmschwelle ist ebenso gering wie die Gefahr, erwischt zu werden. Bleibt zu hoffen, dass die Hersteller von WLAN-Komponenten sich der User annehmen und ihre Geräte mit sinnvollen, sicheren Voreinstellungen ausliefern. Sonst werden wohl in Zukunft die Terroristen nur durch ihre Lachanfalle daran gehindert, anonym und unentdeckbar das Netz für ihre Zwecke zu missbrauchen.

Bericht über ein Funknetz: Seite 30/31.

Preise und Komponenten siehe Seite 35 !

FUNK-SHOP: Antennen

DX-500 *RF systems*

Breitband-Aktivantenne

30 kHz bis 550 MHz (durchgehend)

Die **DX-500** ist eine kompakte, universell einsetzbare Aktivantenne. Ihre Stromversorgung erfolgt per Fernspeisung über das vorhandene Koaxkabel, entweder mit 12 V Gleichspannung über das Steuergerät **DX-500/1** bei mobilem oder maritimem Betrieb oder über ein hochwertiges 230-V-Netzteil **DX-230/1** bei stationärem Betrieb.

Auch ein 24-V/12-V-DC-Konverter **DX-500-24/12** ist erhältlich.

Die **DX-500** wird durch die breite Palette von Zubehör zu einem leistungsfähigen Antennensystem, das maßgeschneiderte Lösungen für jeden Anwendungsfall bietet.

Prospekt unter www.funkempfang.de/dx500.pdf

DX-500 mit Marine-Mount

Highlights

- Breitband-Aktivantenne für den lückenlosen Empfang im Lang-, Mittel-, KW-, VHF- und UHF-Bereich
- Größere Verstärkung bei höheren Frequenzen = bessere Empfindlichkeit im UKW-Bereich, geringe Übersteuerung im Kurzwellen-Bereich
- Sehr hoher Intercept-Punkt für gutes Großsignal-Verhalten
- Sehr niedriges Eigenrauschen
- Rundumempfang mit vertikaler Polarisation
- Äußerst kompakte Abmessungen, nur 40 cm Länge, 35 mm Durchmesser
- Robuste Edelstahl-Konstruktion, dauerhaft wetterbeständig
- Unauffällige Montage, gefälliges Design
- Verschiedene Montageschellen lieferbar
- Vier unterschiedliche Steuergeräte verfügbar

Bezug über den FUNK-SHOP von RADIO-SCANNER