WLAN im Hafen und am Ankerplatz

Immer weniger Segler wollen heute auf das Internet verzichten. Sei es, um die neuesten Revierinformationen einzusehen, noch einmal einen letzten Blick auf die Wettervorhersage zu werfen oder einfach nur, um E-Mails zu schreiben oder zu lesen. Lässt es sich doch am Abend vortrefflich mit zu Hause scypen, vorausgesetzt …, ja vorausgesetzt, ein Internetanschluss steht an Bord zur Verfügung.

Ich erinnere mich noch gut an die Zeiten, wo ich beim Hafenmeister erst mal Kleingeld in der Landeswährung eingetauscht habe und mich dann auf die Suche nach einer intakten Telefonzelle gemacht habe, um die Lieben daheim über die geglückte Ostseeüberquerung zu informieren.

Schnee von gestern. Mit einem Laptop an Bord ist, noch bevor der Mitsegler die Persenning über das Großsegel zum Schutz gegen die Sonne angebracht hat, eine Verbindung mit dem Netz geschaffen. Erste E-Mails werden gelesen und wenige Minuten später wird vom Plotter der neueste Track per kmz-Datei ins Netz geladen und die Segler Kommunity verfolgt per Google die neuste Tagesstrecke nebst eingestellten Fotos.

Ich gebe es zu. Auch ich bin ein Verfechter von Internet an Bord, wenn auch nicht so exzessiv, aber immerhin. Missen möchte ich es nicht. Habe ich doch im letzten Jahr die Vorteile des Internets auf Langfahrt kennen und schätzen gelernt.

Doch wie kommt das Internet an Bord? Ich unterscheide da zwischen zwei grundsätzlichen Möglichkeiten, dem aktiven und dem passiven Zugang.

Der aktive Zugang ist die Verbindung zu einem Provider (Anbieter) per Stick via UTMS-Karte. Eine, zugegebener weise im Ausland manchmal kostentreibende Möglichkeit, die tagesaktuellen Änderungen unterworfen ist und hier aufgrund der schnelllebigen Angebote diverser Provider nicht weiter untersucht werden soll. Jeder Versuch einer Beschreibung heute wäre morgen nicht mehr aktuell.

Beim passiven Zugang wählt man sich in ein - in den Häfen angebotenes WLAN-Netz (**W**ireless **L**ocal **A**rea **N**etwork) - ein. Wenn dabei einige Besonderheiten beachtet werden, stehen dem Nutzer die Tür zum Internet in einer in der Regel passablen Geschwindigkeit zur Verfügung.

Fast alle heutigen Notebooks besitzen einen eingebauten WLAN-Adapter, der allerdings nur für die heimischen Verhältnisse in der Wohnung ausgelegt ist. Für eine sichere Verbindung bedarf es eines WLAN-Routers in fast unmittelbarer Umgebung. Bei größeren Entfernungen reicht oft die im Displayrahmen des Notebooks untergebrachte Antenne nicht aus.

Dieses ist meist in den Häfen und an den Ankerplätzen der Fall. Die niedrige Höhe der am Naviplatz installierten Notebooks trägt auch nicht gerade zu einer guten, stabilen Verbindung bei.

Eine Lösung schafft ein externer WLAN-Adapter, der sinnigerweise über einen USB-Anschluss angeschlossen wird und mit einer am Adapter angebrachten externen Antenne möglichst deutlich über der Wasseroberfläche angebracht werden soll.

Etwas Hintergrundwissen kann nie schaden. Keine Angst, es folgt jetzt keine wissenschaftliche Abhandlung, sondern nur ein wenig Theorie, die den Kauf eines WLAN-Adapters unterstützen soll.

Bei der Wahl der Antenne hat man 2 Möglichkeiten.

Die Rundstrahl-Antenne (omnidirektionale Antenne) überträgt Signale in und aus allen Richtungen. Sie ist unempfindlich gegen Drehungen am Ankerplatz und es entfällt das oft mühsame Ausrichten.

Die Richtfunkantenne bündelt die Sende- und Empfangsleistung in eine bestimmte Richtung. Mir ihr können gezielt einzelne Verbindungen auch über größere Entfernungen aufgebaut werden.

Der Einfachheit halber und zu Gunsten einer sicheren Verbindung beim Schwojen, bevorzuge ich die Rundstrahlantenne.

Die Funksignale von drahtlosen Netzwerken sind sehr empfindlich gegen Abschirmungen. Das hat einen physikalisch leicht nachvollziehbaren Grund: Das von WLAN, Bluetooth und anderen Funkstandards genutzte "unregulierte Frequenzband" um 2,4 Gigahertz ist sehr unbeliebt und wurde bei allen anderen funktechnischen Netzen nicht berücksichtigt, weil es sich eigentlich für Funkübertragungen nur sehr schlecht eignet. 2,4 Gigahertz ist nämlich die Resonanzfrequenz von Wasser.

Grundsätzlich gilt für eine stabile Funkverbindung eine “quasi optische Sichtverbindung“. Kann man den Sender theoretisch sehen, hat man auch eine Verbindung. Jeder Baum, jedes Haus oder jedes andere Hindernis schwächt das Signal.

Ein weiteres vom Gesetzgeber vorgegebenes Hindernis ist die Beschaffenheit der Geräte.

Die Empfangsverstärkung ist unlimitiert, Sendeleistung nicht!

Die Reichweite von Wireless LAN ist u.a. bedingt durch die niedrige max. erlaubte EIRP-Leistung von 100mW (20dBm). Diese sollte aber auf jeden Fall voll ausgenutzt werden, denn eine Erhöhung der Sendeleistung um 6 dB verdoppelt die Reichweite.

Ein Gerät, das 20dBm Sendeleistung (gesetzlich vorgegebene Höchstleistung) aufweist, kommt auf die doppelte Reichweite wie eines mit nur 14dBm (6dB Unterschied verdoppelt die Reichweite).

Nicht reglementiert ist die Empfangsempfindlichkeit. Gute Geräte haben eine Empfangsempfindlichkeit um -97dBm.

Ein Gerät, das -97dBm Empfangsempfindlichkeit hat, kommt im Gegensatz zu einem mit nur -85dBm auf die vierfache Reichweite. Also, Augen auf beim Kauf, denn zu einer guten Verbindung gehören ein guter Empfang ebenso dazu, wie eine ausreichende Sendeleistung. Das schwächste Glied bestimmt die Reichweite.

Ein wesentliches Kaufkriterium sollten deshalb die vom Betreiber aufgezeigten Technischen Daten eines Gerätes sein. Es gibt keinen Grund, Geräte ohne Spezifikationen zu kaufen, auch nicht, wenn sie besonders preiswert erscheinen.

Mit den Routern, die den **W-LAN Standard 802.11n** unterstützen, sind maximal bis zu 300 Mbit/sec. möglich, ein Wert, der in der Praxis aber in der Regel nicht erreicht wird.

Nun ein paar Gedanken an die **Sicherheit in öffentlichen WLAN-Netzen**.

Im Unterschied zum eigenen WLAN daheim, tummeln sich bei öffentlichen WLAN-Hotspots mehrere unbekannte Nutzer im selben Funknetz.

Oft verzichten die Betreiber auf die Verschlüsselung des Datenverkehrs, um den Internetzugang für ihre Kunden möglichst einfach zu gestalten. Dann aber kann die Funkverbindung abgehört werden. Außerdem besteht die Gefahr, dass fremde Nutzer des WLAN-Hotspots unbefugt auf Ihr Gerät zugreifen. So kann es Übeltätern gelingen, an Ihre vertraulichen Daten, z.B. Zugangs- oder Kreditkartendaten, zu kommen.

Wie immer im Internet gilt also daher,

Vorsicht beim Umgang mit vertraulichen Daten.

Wer mit vertraulichen Daten arbeitet, oder gar das immer beliebter werdende Banking nutzen möchte, sollte sich hinreichend über sichere Verbindungen informieren. Die Verschlüsselung einzelner Verbindungen zu bestimmten Diensten wie Online-Banking, E-Mail, etc., erfolgt mit Hilfe einer TLS/SSL-Verbindung. Diese Möglichkeit wird bereits von vielen Anbietern bereitgestellt und ist im Browser am Kürzel „https://“ in der Adresszeile zu erkennen. Alle Daten außerhalb von TLS/SSL-Verbindungen (d.h. wenn das Kürzel „https://“ nicht angezeigt wird) bleiben allerdings ungeschützt

Unter Seglern sehr beliebt ist der externe WLAN-Adapter ALFA Networks AWU…., den es in verschiedenen Ausführungen gibt. Achtung: Hier handelt es sich um eine “Non EU-Version“, da die Sendeleistung bis zu 2000mW betragen kann. Neuere Geräte sind schon auf 500mW begrenzt, erfüllen aber ebenso nicht die technischen Voraussetzungen wie die älteren Geräte mit 2000mW.

Oft wird damit argumentiert, dass die Sendeleistung per Software reguliert werden kann und dass man natürlich niemals mit mehr als 200 mW sendet.

Es macht Sinn, den Adapter mit einer aktiven 5m langen USB-Verlängerung anzuschließen. Die beinhaltet bereits eine eingebaute Verstärkung. Gegen Regen und Feuchtigkeit kann man den Adapter gut schützen, wenn man ihn von unten in eine Wasserflasche schiebt, von der man den Boden ausgeschnitten hat. Mit dem Großfall kann man die Flasche mit dem Adapter hochziehen und den Adapter so deutlich oberhalb der Wasseroberfläche installieren.

Interessant ist, dass ich im letzten Jahr auf meiner Schwedenreise fast nur Segler traf, die mit diesem WLAN-Adapter ausgerüstet waren.

Übrigens, nutzt man so einen Adapter, werden in der Regel mehrere – auch private – Netze angezeigt. Sind die Netze nicht zugangsgesichert, ist es völlig legal, in diesen Netzen zu surfen. Nur Kosten darf man für den Netzinhaber nicht verursachen.

Strafbar macht man sich hingegen, wenn man eine Sicherung überwindet, um in das Netz zu gelangen. Ist das Netz nicht gesichert, geht der Gesetzgeber davon aus, dass der Netzbetreiber mit einer Nutzung einverstanden ist. So ist es zumindest in Deutschland.