WEP- und WPA - Verschlüsselung

***Einstellung am Gerät, am Beispiel eines Routers, W500 oder W700 und einem Hama USB Stick (auf Seite 3 ganz unten*)**

Für die Sendetechnik eines WLAN gibt es einen umfassenden Standard mit dem Kürzel 802.11. Dieser Grundstandard umfasst mehrere Erweiterungen, die die Übertragungsgeschwindigkeit von 11 auf 54 MBit/s und mehr anheben. Diese Erweiterungen werden durch nachgestellte Buchstaben unterschieden – zum Beispiel definiert 802.11a die Übertragung mit 54 MBit/s.

Ein Kernpunkt des Standards 802.11 ist das Verschlüsselungsverfahren WEP (Wired Equivalent Privacy). Es gibt aber auch z.B. die Schlüssel WPA oder WP2. Es verschlüsselt die gesamte Kommunikation mit Hilfe eines Schlüssels von 64 oder 128 Bit Länge (5 bis 64 Zeichen in Ascii oder Hex). Da die kurzen 64-Bit-Schlüssel leicht zu knacken sind, sollte mindestens der 128-Bit-Schlüssel eingesetzt werden. Einige Geräte nutzen bereits 256-Bit-Schlüssel. Falls Ihr Gerät in der Lage sein sollte, 265-Bit-Schlüssel zu verwenden, setzen Sie diesen unbedingt ein. Falls Ihre Geräte außerdem die Eingabe mehrerer Schlüssel anbieten, sollten Sie die aktiven Schlüssel regelmäßig wechseln.

128-Bit-Verschlüsselung mit Hexadezimalzahlen

Der Schlüssel wird in jedes WLAN-Endgerät eingegeben. Bei 64-Bit-Verschlüsselungen ist der Schlüssel 10 Zeichen lang, bei 128 Bit sind es bereits 26 Zeichen. Der Schlüssel sollte niemandem bekannt gegeben werden und auch nicht zu erraten sein. Der Schlüssel wird in hexadezimalen Zahlen wie A0, F6 oder DF angeben oder in Ascii als - ABc12 -.
Dies ist vom Gerät (also Sender {meisten ein Router} und Empfänger {z.B. ein USB Stick} abhängig)

WEP macht ein Funknetzwerk abhörsicher und stellt dafür Funktionen für die Paketverschlüsselung und zur Authentifizierung der Geräte zu Verfügung. Verfahren mit besserer Verschlüsselung wie WEP-Plus oder WPA (Wi-Fi Protected Access) werden leider noch nicht von allen Geräten unterstützt. Wichtig ist vor allem, dass alle Geräte die gleiche Schlüssellänge unterstützen müssen. Wenn Sie also eine bessere Verschlüsselung einsetzen möchten, müssen Sie oft alle WLAN-Geräte austauschen. ***Daher empfiehlt es sich, bei einem Kauf auf die WPA-Fähigkeit eines Gerätes zu achten***.

WPA – die sichere Alternative

Wie WEP ist auch WPA ein Standard für die Verschlüsselung und Authentifizierung. Entwickelt wurde WPA, um die grundlegenden Schwächen der WEP-Verschlüsselung zu beheben. WPA kann also als der sichere Nachfolger von WEP angesehen werden.
Bietet Ihr Access-Point (z.B. ein Router) eine WPA-Verschlüsselung, sollten Sie dieser vor WEP auf jeden Fall den Vorzug geben. Ältere Geräte lassen sich über ein Software-Update oft auf den neuesten Sicherheitsstandard bringen. WPA verwendet für die Verschlüsselung das "Temporal Key Integrity Protocol" (TKIP). Das Protokoll muss in die Einstellungen für Ihre Netzwerkverbindung eingegeben werden.

Weitere Schlüssel

Leider ist ein WLAN-Funknetz trotz unterdrücktem SSID-Broadcast, MAC-Filterung und WEP-Verschlüsselung mit 128 Bit oder WPA-Verschlüsselung nicht hundertprozentig abgesichert. Sie können allerdings davon ausgehen, dass ein lokales Netzwerk durch die beschriebenen Methoden so weit abgesichert ist, dass ein Angreifer nur mit erheblichem Aufwand in das System kommt.

Es gibt eine Reihe von Ergänzungen der geschilderten Absicherungen und einige zusätzliche Maßnahmen, die Sie für einen verbesserten Schutz des WLAN ergreifen sollten:

 Kontrollieren Sie den Sendebereich der Basisstation mit einem WLAN-fähigen Notebook. Durch das Ändern der Geräteposition und der Antennenausrichtung haben Sie einen nicht geringen Einfluss auf die Senderichtung.

 Falls Ihre Basisstation eine Reduzierung der Sendeleistung erlaubt, sollten Sie diese Funktion nutzen. Probieren Sie aus, welche Sendeleistung ausreichend ist.

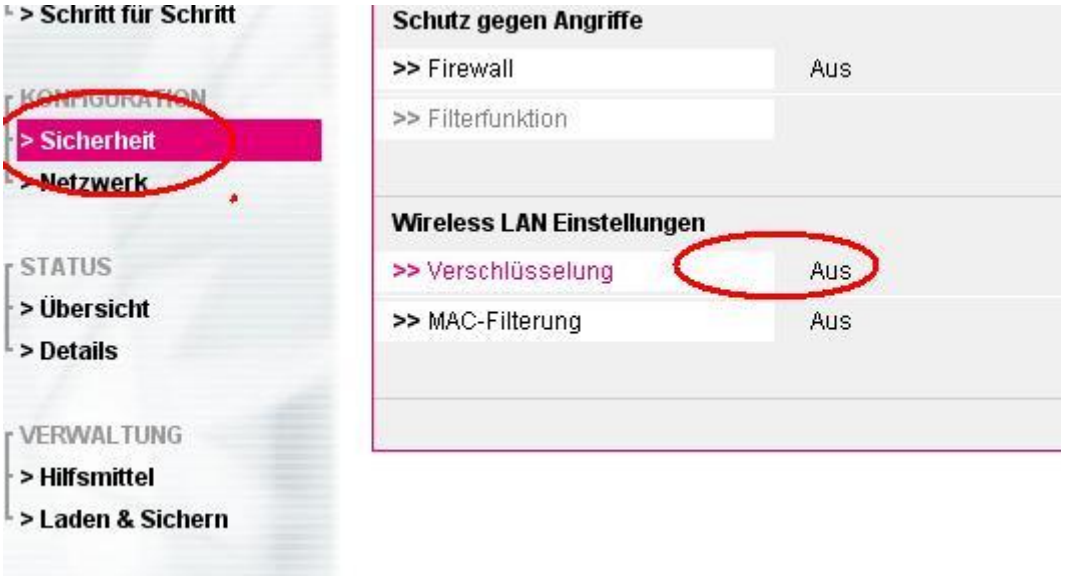
 Schalten Sie die Basisstation nur dann ein, wenn sie tatsächlich benötigt wird. Schließen Sie das Gerät am besten über eine Steckdosenleiste mit Schalter an das Stromnetz an.

 Falls die Basisstation mit einem integrierten DHCP-Server (Dynamic Host Configuration Protocol) ausgerüstet ist, sollten Sie diesen auf jeden Fall ausschalten. DHCP sorgt dafür, dass auch ein illegal angemeldeter Rechner sofort eine IP-Adresse bekommt. ***Vergeben Sie in Ihrem Heimnetzwerk stattdessen feste IP-Adressen.***

Verändern Sie das Standard Passwort im Router! Sonst kann Jeder, der per Wlan Zugang findet ihre Zugangsdaten nutzen und ändern.

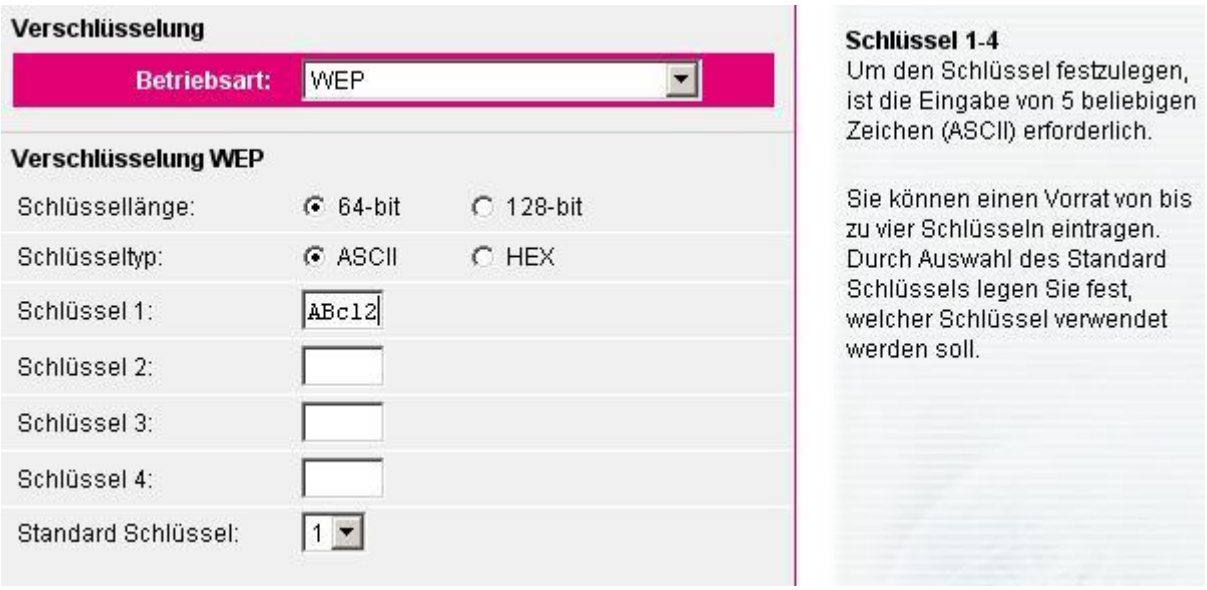
Einstellung am Gerät, am Beispiel eines Routers, W500 oder W700

Öffnen sie das Menü im Router, starten sie die Option Sicherheit und wählen sie eine Verschlüsselung aus z.B. Web



Schalten sie eine Verschlüssellung ein,
wählen eine Schlüssel Betriesart **die ihr Empfänger kennt** (z.B. Web).

Vergeben Sie einen Schlüsselnamen (Passwort) für Schlüssel 1. Bei 64 bit und Ascii 5 Zeichen (z.B. Abc12). Zum Wechseln können 4 Schlüssel vergeben werden die man wahlweise nutzen kann.



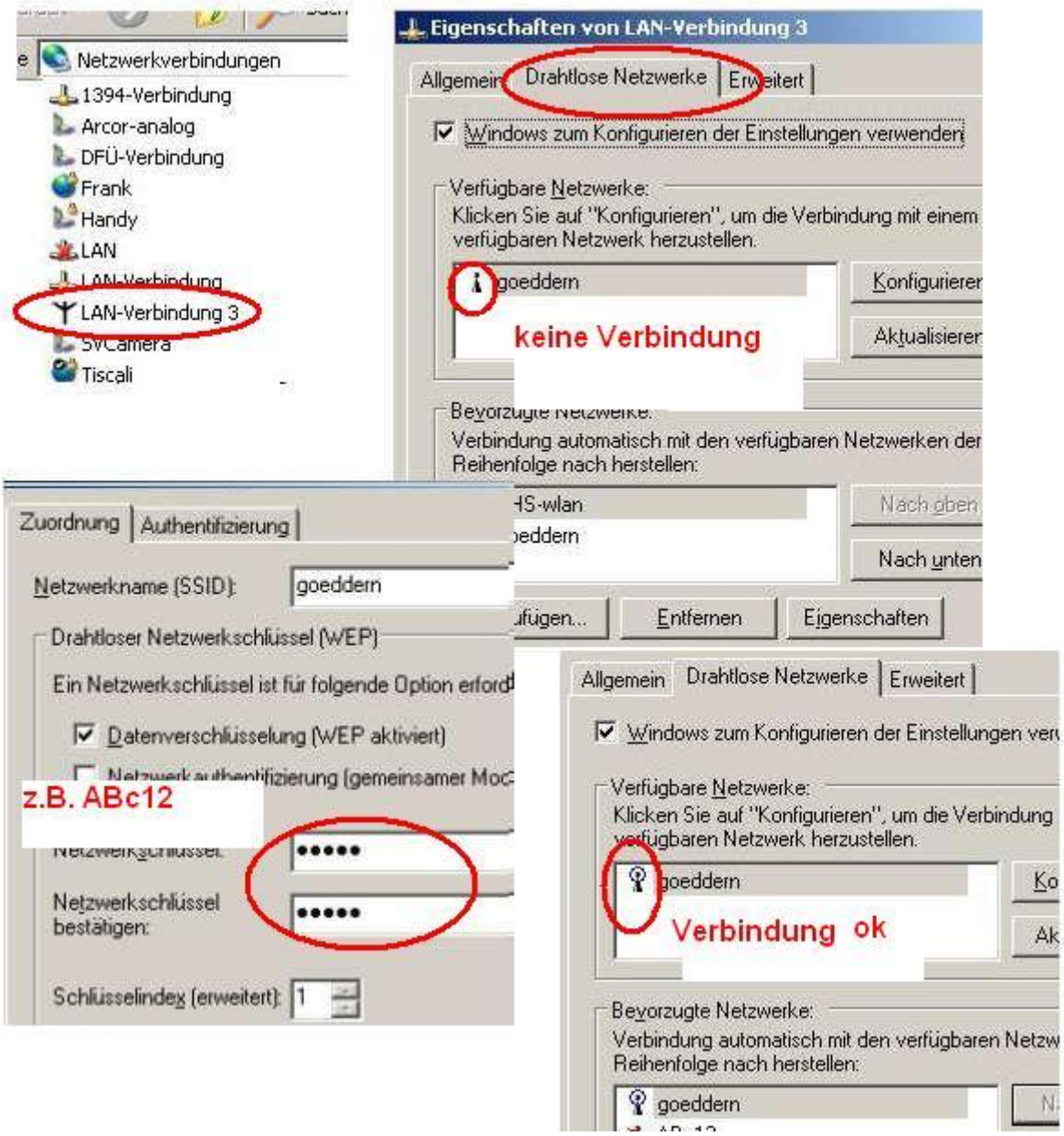
Installieren sie den gleichen Schlüsselnamen (Passwort) bei Ihrem Empfänger.
(Z.B. bei ihrem USB Stick)

Achtung:

nach dem Speichern im Router ist die Verbindung zum Empfänger unterbrochen, da noch kein Schlüssel beim Empfänger installiert wurde!

Einstellungen über :

Netzwerkumgebung/Eigenschaften / Drahtlose Lanverbindung / Drahtlose Netzwerke
(alles auf mittlerer Karteikarte) .



Sollten sie keine Verbindung bekommen, starten sie den Rechner neu oder melden sie sich neu an. USB Sticks können entfernt und wieder eingesteckt werden.