

## Wireless Lan -Sicherheit

### Router Passwort

Sie sollten unbedingt das Passwort für die Router bzw. Access Point Konfiguration ändern. Hier gelten natürlich auch die Regeln für sichere Passwörter, also ein möglichst langes Gewirr aus Sonderzeichen, Zahlen und Buchstaben. Merken Sie sich das Passwort aber gut, denn wenn der Router bzw. Access Point einmal richtig konfiguriert ist, benötigt man es nur noch selten und ist schnell vergessen.

### ESSID -Netzwerkname

Auf Messe Gelände und sonstigen Veranstaltungen mit Funknetzen kann jeder der sich dort mit einem Laptop und W-LAN Karte bewegt die Funknetze leicht aufspüren. Ermöglicht wird dies durch die Scan Funktion die die meisten Karten beherrschen. Die Access-Points pusten Ihre ESSID (Extended Service Set Identifier) also den Namen des Netzes einfach in die Gegend und jeder, der sich in Reichweite befindet, kann das Netz auf diese Weise entdecken.

Als Sicherheitsmaßnahme für ein privates W-LAN empfiehlt es sich, den Broadcast der ESSID abzuschalten. Man sollte auch nicht die vor eingestellte SSID belassen. So weiß nur derjenige von dem Netz dem der Netzname explizit mitgeteilt wurde.

### Router-Fernwartung

Sicherlich ist bei den Access-Points die Fernwartung über das Internet komfortabel aber auch etwas unsicher. Schalten Sie den Remote-Zugriff ab und konfigurieren Sie das W-LAN lokal, auch Schnickschnack wie Remote-Firmware-Update sollten Sie deaktivieren.

### WEP/WPA Verschlüsselung

Wired Equivalent Privacy ist ein Verfahren zur Datenverschlüsselung und Authentifizierung in W-LANs. Leider ist dieses Verfahren nicht besonders sicher. Jedoch spricht nichts gegen eine Aktivierung von WEP, da man mit den richtigen Tools und erst einigen Stunden Zeitaufwand die Verschlüsselung knacken kann.

Bei aktuellen Geräten sollten es schon 128 Bit sein. Wichtig ist auch, dass Sie die Schlüssel manchmal ändern, am besten in unregelmäßigen Abständen. Unterstützt ihr Router das wesentlich sichere WPA Verschlüsselungsverfahren sollten Sie dieses natürlich WEP vorziehen.

### MAC Adresse

(nur die gespeicherten MAC-Adressen dürfen sich mit dem Router/AP verbinden)

Sichern Sie Ihr W-LAN über so genannte Access Control Lists (ACL) ab, indem Sie nur bestimmten MAC-Adressen Zugang zu Ihrem Funknetz geben. Es ist eben viel schwerer eine Hardware Kennung zu fälschen als bei einer Passwort Abfrage dieses mit Glück zu erraten.

Windows gibt nach Eingabe des Befehls „ipconfig /all“ die MAC-Adressen in Ihrem Rechner Preis. Diese finden sie hinter dem Eintrag "Physikalische Adresse". Sie müssen nur noch die gültigen MAC-Adressen in die Konfiguration der Basisstation eintragen, was erst bei größeren Netzen viel Arbeit machen wird.