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 oder notieren es an einen sicheren Ort, 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 einen 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. Wobei dies nur eine kleine Maßnahme ist mit einigen Punkten dafür und auch dagegen. Wichtiger ist dagegen den Namen der vor eingestellten SSID zu ändern, da bei einigen Routern werksseitig als Name das Router Model bzw. eine bekannte Kennung eingetragen ist. Anhand dessen könnte nun nach Schwachstellen des spezifischen Models recherchiert werden.

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. Jedoch ist dieses Verfahren veraltet und nicht mehr besonders sicher.
Für eine Aktivierung von WEP spricht nur noch, wenn entsprechend veraltete Hardware genutzt werden muss. Die Verschlüsselung ist aber besser als gar keine, da immer noch ein gewisser Zeitaufwand nötig ist um die Verschlüsselung zu knacken. Es sollten dann schon 128 Bit sein und wichtig ist auch dass Sie die Schlüssel manchmal ändern, am besten in unregelmäßigen Abständen.
Unterstützt ihr Router und die restliche Hardware das wesentlich sichere und aktuelle WPA/WPA2 (Wi-Fi Protected Access) 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 Controll 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.