Wired Equvalent Privacy (WEP)

WEP ist das mittlerweile veraltete Standard-Verschlüsselungsprotokoll für WLAN. Die Aufgabe war den Zugang zum Netz sowie die Vertraulichkeit und Integrität der Daten sicherzustellen und zu regeln. Wegen verschiedenen Schwachstellen gilt das Verfahren als unsicher worauf wir später noch genauer eingehen werden. WEP benutzt die sogennante Open System Authentication. Dies ist eine Standard Authentifizierung, wo der Accesspoint zwei Zustände haben kann. Erstens es ist keine Verschlüsselung konfiguriert. Somit muss keine praktische Authentifizierung stattfinden und jeder Client kann sich mit dem WLAN verbinden. Es gibt noch eine Verschlüsselung. Hier gibt es wieder zwei verschiedene Arten: Einmal logisch und technisch. Bei der logischen Verschlüsselung ist der WEP-Schlüssel gleichzeitig die Authentifizierung, was wiederum heist, dass jeder Client mit korrektem WEP-Schlüssel Zugang zum Netz hat. Bei der technischen Verschlüsselung findet ein Autausch von Authentifizierungsnachrichten statt und der Client wird authentifiziert. Stimmen WEP-Key auf Accespoint und Client überein, ist die Kommunikation möglich. Stimmen diese nicht überein, ist der Client zwar authentifiziert aber, kann aber keine Daten mit den Netzwerk autauschen. Es gibt noch die Shared Key Authentication. Sie scheint sicherer zu sein als die anderen Authentications. Dies stimmt jedoch nicht. Genauers sagen wir Ihnen im nächsten Abschnitt. Die Authentifizierung erfolgt über die Challenge-Response Authentifizierung mit einem geheimen Schlüssel. Man muss sagen, dass die Challenge-Response Authentifizierung die selben Schwächen wie WEP aufweist. Durch den Einsatz der Shared-Key Authentication wird der geheime Schlüssel offengelegt. Deswegen ist es ratsam auf die Shared-Key Authentication zu verzichten und die Open Authentication zu benutzen. Es gilt Allerdings: Besser ist irgendeine Verschlüsselung als keine!