Link: https://www.tecchannel.de/a/workshop-so-spueren-sie-illegale-wlan-zugangspunkte-auf,432648

Workshop: So spüren Sie illegale WLAN-Zugangspunkte auf

Datum: 19.10.2005

Eigenmächtig aufgestellte WLAN Access Points sind Administratoren ein Gräuel. Meist nur schlecht gesichert, öffnen sie Angreifern Tür und Tor in das Firmennetz. Mit WLAN-Sniffern kommen Sie diesen Gefahrenherden auf die Spur.

Im WLAN lässt es sich bequem arbeiten. Egal in welchem Raum man sich aufhält, sobald der Laptop eine Verbindung hat, kann man bequem im Netzwerk arbeiten. Die notwendige Infrastruktur wie Access Points sind billig und in den Standardeinstellungen schnell eingerichtet.

Probleme tun sich dann auf, wenn Angestellte eigenmächtig versuchen, ein WLAN-Netz aufzuziehen und sich nicht mit dem Administrator absprechen. Schnell kommt dann gefährliches Halbwissen zum Einsatz. Da wird beispielsweise der Datenverkehr nicht oder nur unzureichend verschlüsselt oder Passwörter werden auf den Standardeinstellungen belassen.

Diese „wilden“ Zugangspunkte hängen oft ebenfalls am Firmen-LAN und erlauben neben einem Zugriff auf das Internet auch Einsicht in freigegebene Daten. Das Problem ist, dass sich Funknetzwerke nicht an die Grenzen der Firma halten. Aktuelle WLAN-Produkte schaffen locker eine Reichweite bis zu 100 Metern. Genug Reichweite also, um Wardrivern ein ausreichend starkes Signal zu liefern.

Schützen können Sie Ihr Netz, indem Sie die Zugangspunkte entweder deaktivieren oder in die Sicherheitsstruktur des Netzwerks einbinden. Doch zuvor müssen die Access Points erst einmal gefunden werden. Hier helfen Ihnen teilweise die gleichen Tools, die auch Wardriver einsetzen. Der für alle Leser frei zugängliche tecCHANNEL-Artikel “**Illegale WLAN-Zugangspunkte aufspüren**[1]“ zeigt Ihnen, wie es geht. (mec)

Links im Artikel:

[1] **https://www.tecchannel.de/link.cfm?type=article&pk=431414**
