Wireless LAN's sichern !

Leider werden die meisten Access Point's (AP's) durch mangelnde Kenntnisse, Unwissenheit oder Zeitmangel falsch oder gar nicht konfiguriert.
Hier werden die wichtigsten Punkte aufgelistet, um einen Wireless Access Point so sicher zu machen, dass es nur mit erheblichem Aufwand möglich ist, sich in das Netzwerk einzuklinken, eine Session zu sniffen oder das WLAN zu missbrauchen.

1. Wenn es möglich ist, die Verbindung mit Kabel erstellen.
2. WEP Verschlüsselung einschalten (48 Bit oder wenn möglich 128 Bit), auch wenn die WEP Verschlüsselung nicht sicher ist, hält sie aber Skriptkiddies schon mal ab. Und der zeitliche und materielle Aufwand und das Wissen den Schlüssel zu knacken, ist doch schon erheblich. Der WEP Schlüssel sollte regelmässig erneuert werden.
3. Wenn möglich ist eine MAC-Adressen Zugriffsliste zu führen. Nur die eingetragenen MAC-Adressen werden am AP zugelassen. Leider unterstützen nicht alle AP's diese Funktion.
4. Die SSID nicht propagieren (SSID Broadcasting) und neutral benennen. Auf keinen Fall z.B. „Kassen-Netz" oder „FIRMA-XY". Auch diese Funktion ist nicht in allen AP's realisiert.
5. Den AP selber schützen, durch neue, regelmässig geänderte Usernamen/Passwörter, aktualisierung der Firmeware und durch geeignete, zugriffssichere Standortwahl.
6. Die AP's bei Nichtgebrauch abschalten, man spart Strom und liefert gar keine Angriffsmöglichkeit.
7. Alle AP's sind wie öffentliche Netze zu behandeln. Sie müssen daher gegenüber dem Firmennetz durch eine Firewall abgeschottet werden. Mittels einer Authentifizierung über eine sichere, verschlüsselte Verbindung SSH/HTTPS/SSL muss sich der User am Firewall oder Radius Server anmelden, kommt dann an das Firmennetz. Alle Daten die via WLAN übertragen werden, müssen verschlüsselt übertragen werden.
8. Die mobilen Stationen, die auf das Wireless zugreifen, müssen selber auch geschützt werden, z.B. durch eine Personal Firewall, aktuelle Sicherheitspatch's oder andere geeignete Massnahmen.
9. Ein weiteres Problem liegt beim User selber. Private Passwörter werden zum Allgemeingut aller User. Die SSID's oder WEP Schlüssel werden z.B. am Firmen-Infoboard bekannt gegeben. Benutzer müssen informiert, bzw. richtig geschult werden und auf die Gefahren aufmerksam gemacht werden.
10. Weiter ist eine regelmässige Auswertung der Logfiles von Firewall, AP's, IDS und anderen Sicherheits Systemen notwendig. Ein Security-Check durch eine Externe Drittfirma mit Wireless Erfahrung ist die Lösung, wenn kritische Daten oder Anlagen betrieben werden.

Die Punkte 2 bis 6 machen das Netzwerk nicht wirklich sicher, denn für diese Schutzmechanismen gibt es geeignete Mittel und Möglichkeiten sie zu umgehen oder knacken. Sie sind aber schnell zu installieren und halten den einfach vorbeifahrenden „Skriptkiddie" schon mal ab. Denn er kann es am nächsten AP einfacher haben. Die restlichen Punkte sind aufwändig, teuer und sehr administrations- und arbeitsintensiv, stellen aber ein beinahe sicheres WLAN zur Verfügung.

Dieses Dokument wurde von www.wardriving.ch zusammengestellt. Dort finden Sie auch die aktuellste Version dieses Dokumentes.

wardriver@wardriving.ch