**Going Wireless**

**IDK GmbH hat einen Auftrag bekommen ein kabelloses Netzwerk in einem Unternehmen aufzubauen. Dabei soll es ein privates Netzwerk, die nur für die Mitarbeiter zugreifbar sein soll, und ein öffentliches Netzwerk für die Kunden des Unternehmens.**

Kabellose & automatische Verbindung der Geräte wie Smartphones, Notebooks, Tablets und Fernseher mit dem Internet, WLAN, ist heutzutage zu einem Standard geworden. Bei der Einrichtung eines drahtlosen Netzwerkes muss man auf einige Punkte achten.

Benötigte Hardware

Die Provider, in der Regel, liefern die wichtigste Hardware wie

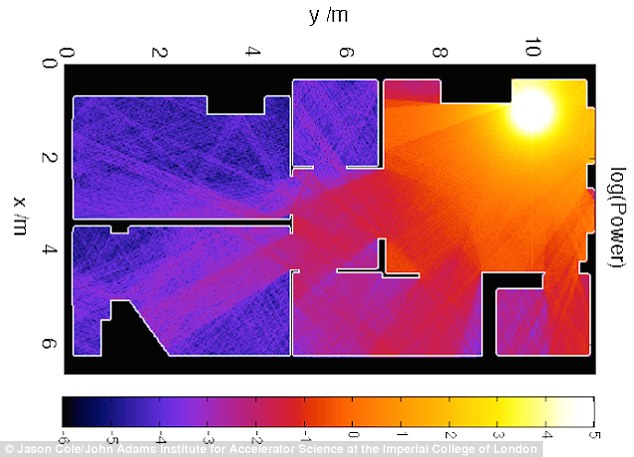
Splitter, DSL-Modem oder NTBA kostenlos. Dabei muss man beachten, dass, um WLAN benutzen zu können, braucht man unbedingt einen Router, für den dann zusätzliche Kosten anfallen könnten.

Zudem muss jedes Gerät das WLAN-Signal empfangen können mit Hilfe einer Netzwerkkarte. Auf mobilen Geräten ist so eine Netzwerkkarte schon standardmäßig vorhanden, aber für die Rechner müsste man eventuell eine PCI-Karte besorgen, um sich mit WLAN verbinden zu können. Bei den Notebooks und einigen Mini-PCs oder Barebones besteht die Möglichkeit eine PCMCIA-Karte einzubauen, wenn diese noch nicht vorhanden war.

In manchen Fällen ist es empfehlenswert einen USB-Adapter, da dieser universell einsetzbar ist. Es gilt allerdings zu beachten, dass der Rechner eine USB-2.0-Schnittstelle benötigt.

Standort

Auch wenn heutzutage Router mit gängigsten Reichweiten zwischen 30 und 100 Metern in meisten Fällen für gute Verbindung sorgen können, muss man auf die sonstigen Faktoren achten, die eventuell das Signal stören könnten, beispielsweise die Wanddicke oder allgemein die Struktur der Räume, die das Signal durchqueren muss.



Sicherheit

1. Sendeleistung des Access-Points, wenn möglich, soweit reduzieren, dass nur die Räume, bzw. Gebäude abgedeckt sind, welche WLAN-Zugang benötigen.
2. Broadcast SSID (Service Set Identifier, Netzwerkname) abschalten, sofern das Produkt dieses unterstützt. Damit ist ihr WLAN nicht für alle sofort sichtbar.
3. Wi-Fi Protected Access 2 (WPA2) oder WiFi Protected Access (WPA) Verschlüsselung aktivieren. Eine WEP Verschlüsselung reicht nicht aus, da der Schlüssel innerhalb einer Minute geknackt werden kann.
4. Anlegen einer Media-Access-Control-List (MAC-Filterung), sofern das Produkt dieses unterstützt. Dadurch erhalten nicht zugelassene Netzwerkkarten keinen Zugriff auf ihr WLAN. Da MAC-Adressen jedoch fälschbar sind bietet dies keinen 100%igen Schutz.
5. In der Regel haben DSL-WLAN Router eine eingebaute Firewall. Es ist empfehlenswert diese zu nutzen, um alle Rechner im Netzwerk zu schützen.

Einrichtung des Gastnetzwerks

Diese Funktion bieten inzwischen die meisten Router. Ein Gäste-WLAN bringt Besucher/Kunden über den Internetzugang des Unternehmens online. Allerdings ist das Gäste-WLAN ein eigenes Netzwerk, das logisch vom privaten Heimnetz getrennt ist. Es hat eine eigene Netzwerkkennung (SSID), ein eigenes WLAN-Passwort und einen eigenen IP-Adressbereich. Die Firewall im Router sorgt dann dafür, dass die IP-Pakete des Gäste-WLANs nicht ins Heimnetz gelangen.



Auftrag

In diesem Fall ist es von großer Bedeutung die richtige Hardware für das Netzwerk auszusuchen. Es ist notwendig für den Kunden, dass der Router „Gast-Netzwerk“ Funktion unterstützt und die Software des Routers auf dem neuesten Stand ist.

Außerdem müssen wir dafür sorgen, dass das Empfangssignal an allen Geräten stabil und stark bleibt. Das kann durch bessere Netzwerkkarten, bessere Netzwerk-Planung (Standort des Routers) oder sogar durch die Hintereinanderschaltung mehrere Router erreicht werden.

Zusätzlich müssen wir für die Sicherheit der Netzwerke (privat und gast) sorgen, in dem wir, wenn möglich, WPA2 Verschlüsselung verwenden und ein sicheres Password dem Netzwerk vergeben.