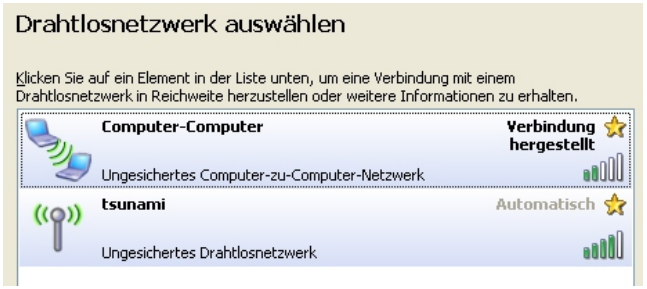
Was ist WLAN / WiFi

- Mit Wireless Local Area Networks (WLAN) können mit geringem Aufwand mobil lokale Netzwerke oder ein Zugang zum Internet aufgebaut werden. WLAN stellt mittlerweile eine Standardausstattung von Laptops dar.
- Gängige Standards zu WLAN sind IEEE 802.11b mit Übertragungskapazitäten bis zu 11 Mbit/s, neuere Modelle zunehmend auch mit 802.11g mit bis zu 54 Mbit/s.
- Die Hersteller-Vereinigung WiFi-Alliance dokumentiert die Kompatibilität zum Standard mit Vergabe des WiFi-Zertifikats.

WLAN Betriebsarten

WLANs können in zwei Modi betrieben werden:

- Über ein Computer-zu-Computer-Netzwerk (auch Ad-Hoc-Netzwerk) verbinden Sie Computer direkt miteinander, etwa um schnell Dateien auszutauschen.
- Im Infrastrukturmodus wird über einen Access Point eine Verbindung mit einem lokalen Netzwerk oder dem Internet hergestellt, etwa über Hot-Spots an Flughäfen oder in Cafés.



Meistens wird WLAN im Infrastrukturmodus verwendet, um mobil Internetzugang zu erhalten. Aktivieren Sie Ihr WLAN nur dann, wenn Sie es auch tatsächlich benötigen. Das Benutzerhandbuch Ihres mobilen Geräts gibt dazu Hinweise (Schalter, Tastenkombination, Konfigurationsprogramm, etc.)

Schalten Sie Ihr WLAN aus, wenn Sie es nicht benötigen!

Sicherheit der Funkstrecke

Durch die Funkübertragung sind WLANs exponierter als herkömmliche kabelgebundene Netzwerke. Die an der Funkstrecke übertragenen Daten können je nach Umgebung einfach über einige hundert Meter, mit Spezialantennen sogar darüber hinaus, abgehört werden.

- Verwenden Sie deshalb Verschlüsselung der Funkstrecke, wo immer es möglich ist.
- WEP (Wired Equivalent Protection) ist als kompromittiert anzusehen und sollte nicht mehr verwendet werden.

Verwenden Sie Verschlüsselung der Funkstrecke!

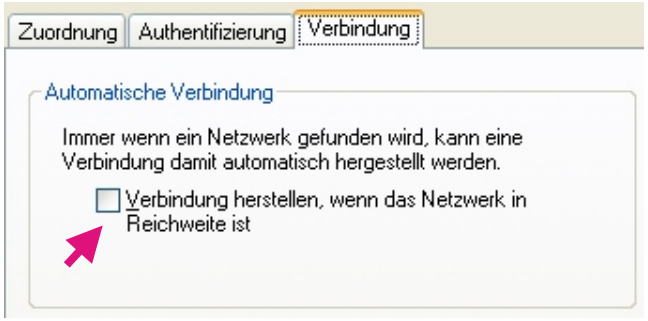
Verwenden Sie möglichst WPA (WiFi Protected Access).

Die Verschlüsselung der Funkstrecke sichert nur die Verbindung zwischen Ihrem mobilen Gerät und dem Access Point. Am lokalen Netzwerk dahinter stehen die Daten ungesichert klartextlich zur Verfügung.

Ein WLAN wird über einen Namen, die so genannte SSID (Service Set Identity) identifiziert. Bekannte SSIDs, wie etwa die Namen der Hot-Spots bekannter WLAN Anbieter, sind kein Garant dafür, dass es sich auch um einen solchen handelt. Jeder Laptop oder PDA in räumlicher Nähe kann sich als bekanntes WLAN ausgeben.

Deaktivieren Sie automatische Verbindungen mit ungesicherten WLANs.

Am Beispiel von Microsoft XP wäre die entsprechende Einstellung unter Eigenschaften der drahtlosen Netzwerkverbindung (Netzwerkverbindungen in Systemsteuerung):



Internet-Zugang über WLAN

Wenn Sie sich über WLAN mit einem öffentlichen Hot-Spot verbinden, kann Ihr mobiles Gerät - je nach Konfiguration des Betreibers - auch offen im Internet sichtbar sein. Zumindest im Empfangsbereich des WLAN bietet Ihnen der Hot-Spot-Betreiber keine erweiterten Sicherheitsfunktionen wie Firewalls, die Sie aus Ihrer Büro- oder Heimumgebung gewohnt sind.

Ähnliches gilt für Access Points, die Ihnen etwa in Meeting-Räumlichkeiten Ihrer Geschäftspartner zur Verfügung stehen. Selbst wenn dort Firewalls installiert sind, ist Ihr mobiles Gerät im WLAN-Empfangsbereich oder aus dem lokalen Netzwerk angreifbar.

Sie müssen Ihren Rechner deshalb vor Angriffen schützen.

Betreiben Sie Ihr mobiles Gerät in fremden Umgebungen nicht ohne Zusatzschutz wie Personal Firewalls.

Sicherer WLAN-Zugang zu Intranets

Wenn Sie über WLAN mobil an das Intranet Ihrer Organisation verbinden, soll das immer über Ende-zu-Ende-Verschlüsselung erfolgen. VPN-Lösungen (Virtual Private Networks) sind etwa auf Basis IPSEC (Internet Protokoll Security) oder SSL (Secure Socket Layer) verfügbar.

Für Remote-Zugang zu Intranet-Bereichen soll immer VPN mit Ende-zu-Ende-Authentifizierung und Verschlüsselung eingesetzt werden!

Beachten Sie, dass Ihr mobiles Gerät aus dem WLAN-Empfangsbereich oder aus dem lokalen Netzwerk des Access Points (der Broadcast-Domäne des Distribution Networks) meist trotz aktivem VPN angreifbar ist. Es soll deshalb zusätzlich zu VPN immer auch eine Personal Firewall verwendet werden.

Wenn Sie Ihr mobiles Gerät im stationären Netz betreiben, schalten Sie WLAN aus.

Betreiben Sie das mobile Gerät nie mit zwei gleichzeitig aktiven Netzzugängen.

Z.B. soll ein Gerät nicht gleichzeitig im Intranet und an einem WLAN betrieben werden.

Neben WLAN gilt Gleiches etwa für Modemeinwahl, etc.

Weitere Empfehlungen

Dieser Flyer behandelt die wesentlichsten Aspekte des sicheren Betriebs mobiler Geräte im WLAN.

Für den sicheren Betrieb eines WLAN-Angebots und weitere Informationen zur Sicherheit von WLANs bietet die IKT-Stabsstelle des Bundes Empfehlungen und Checklisten auf:

http://www.cio.gv.at/it-infrastructure/wlan/

Über WLAN hinausgehend sind mobile Geräte besonders exponiert. Über Dateiverschlüsselung (z.B. secure EFS, vgl. E-Government Flyer Nr. 207) werden sensible Daten auch gegen Verlust oder Remote Filezugriff geschützt.

Fragen

Senden Sie ein E-Mail an: technology@a-sit.at

Zentrum für sichere Informationstechnologie - Austria
A-SIT
Secure Information Technology Center - Austria

Sicherheit von Wireless-LAN

E-Government Flyer Nr.302

Hinweise zur sicheren Verwendung von WLAN und WiFi

- Was ist WLAN / WiFi
- WLAN Betriebsarten
- Sicherheit der Funkstrecke
- Internet-Zugang über WLAN
- Sicherer WLAN-Zugang zu Intranets

DIGITAL AUSTRIA