KANTON LUZERN

Datenschutzbeauftragter
des Kantons Luzern
Bahnhofstrasse 15
6002 Luzern
Telefon 041 228 66 06
dsb@lu.ch
www.datenschutz.lu.ch

Merkblatt “Sicherer Betrieb eines Wireless-LAN“

1. Zweck des Merkblattes

Der Einsatz von Funknetzen hat in den letzten Jahren ständig an Bedeutung gewonnen. Die Vorteile der kabellosen Verbindung sind unbestritten: Endlich ist der langersehnte mobile Arbeitsplatz mit Internetzugang Wirklichkeit geworden.

Erschreckend ist aber noch immer das Sicherheits-Niveau: Obwohl sich viele Betreiber von Funknetzen in der Zwischenzeit der Gefahr bewusst zu sein scheinen, sind noch immer viele Funknetze offen und können problemlos gehackt werden.

Dieses Merkblatt soll aufzeigen, dass der Betrieb eines ungesicherten Funknetzes grosse Risiken mit sich bringt und wie Sie ein W-LAN mit der grösstmöglichen Sicherheit konfigurieren.

2. Gefahrenquelle W-LAN

Funknetze sind häufig so eingestellt, dass sie weit über das eigentlich nötige Einsatzgebiet hinaus senden („signal bleeding“). Das erlaubt es sogenannten „Wardrivern“, mit einem Notebook und laufender Sniffer-Software[1] durch die Quartiere zu ziehen - auf der Suche nach W-LANs. Die meisten dieser „Wardriver“ sind harmlos und amüsieren sich lediglich über die Unprofessionalität der Betreiber.

Diese Tatsache darf aber keine Rechtfertigung für das Betreiben eines unsicheren Funknetzes sein. Denn Daten sind nach wie vor das Kapital vieler Unternehmen und ein erfolgreicher Angriff könnte verheerende Folgen haben. Man denke dabei nur an was zu erwarten wäre, wenn Patientendaten eines Arztes veröffentlicht oder wichtige Forschungsergebnisse eines Labors in falsche Hände gelangen würden. Jeder Inhaber von Datensammlungen ist für die Sicherheit der Daten gegenüber Kunden, Lieferanten und Mitarbeitern verantwortlich.

3. Sichere Konfiguration eines W-LANs

Nachfolgend finden Sie einige wichtige Punkte für eine möglichst sichere Konfiguration eines Funknetzes aufgelistet. Es gilt dabei aber zu beachten, dass die Technik einem schnellen Wandel unterzogen ist und als sicher geltende Technologien in kurzer Zeit unsicher werden können. Die Betreiber von Funknetzwerken sind für die Sicherheit ihres W-LANs

[1] Sniffer sind Programme, um den Datenaustausch in Netzwerken abzuhören.

verantwortlich. Es empfiehlt sich, regelmässig die neusten Berichte zu lesen und die Hard- und Software auf den neusten Stand der Technik zu bringen.

- *Reichweite der Signale beschränken*
  Die einfachste und wahrscheinlich effektivste Massnahme ist die Beschränkung der Reichweite der Signale auf das benötigte Zielgebiet. Je kleiner die Reichweite, umso geringer ist die Gefahr, dass unerwünschte Besucher ihr Netzwerk überhaupt orten und hacken können. Müssen zusätzliche Antennen benützt werden, so empfiehlt es sich, ein Modell zu kaufen, welches die Signale punktgenau an einen anderen Ort sendet und diese nicht in alle Himmelsrichtungen streut. Ebenso wichtig ist die Position des Access-Points. Wird er direkt am Fenster positioniert, so reichen seine Signale bis auf die Strasse hinaus und können von Hackern problemlos abgefangen werden. Vom Gesichtspunkt der Abhörsicherheit her gesehen, sollte ein Access-Point möglichst im Zentrum des Einsatzgebietes, z.B. der Wohnung aufgestellt werden. Ausserdem können bei den meisten Access-Points die Antennen so ausgerichtet werden, dass das Signal in eine Richtung (zum Beispiel zur Strasse hin) schwächer wird. Bei einigen Access-Points ist es sogar möglich, einzelne von mehreren Antennen ganz auszuschalten.

- *Netzwerknamen ändern*
  Die SSID (Service Set Identifier) bezeichnet den Namen des Funknetzes. Wer sich in ein Netz einwählen möchte, muss diesen Namen kennen. Ändern Sie den Namen des Netzwerkes und wählen Sie eine nicht zu erratende SSID. Die vorgegebenen Namen der Hersteller dürfen keinesfalls verwendet werden. Zudem ist es empfehlenswert, den Namen des Netzwerkes in regelmässigen Abständen zu ändern und wenn immer möglich das SSID Broadcasting auszuschalten.

- *Router- und Access-Point- Zugang schützen*
  Wenn Sie ein W-LAN in Betrieb nehmen, müssen Sie den Access-Point und den Router für ihr Netzwerk konfigurieren. Diese Konfiguration können Sie nur vornehmen, wenn Sie das richtige Passwort für den Zugang zu Router resp. Access Point kennen. Bei neugekauften Geräten steht das Anfangs-Passwort in der Bedienungsanleitung. Weil auch Hacker diese Handbücher und damit die Initial-Passwörter kennen, sollten Sie schon bei der ersten Konfiguration ein eigenes, nicht zu erratendes, möglichst zufälliges Passwort setzen. Wenn Sie das nicht tun, kann ein Hacker alle Sicherheitsmechanismen wie Verschlüsselung und Einschränkung der MAC-Adressen beim Router resp. Access-Point ausschalten.

- *WEP-Verschlüsselung*
  WEP (Wired Equivalent Privacy) ist ein Sicherheitsstandard im W-LAN, der sowohl für die Verschlüsselung der Datenübertragung als auch für die Benutzerauthentifizierung zuständig ist. Abhängig von der Hardware kann mit 40- oder 104-Bit verschlüsselt werden. Unglücklicherweise muss der kleinste gemeinsame Schlüssel verwendet werden, damit alle Geräte auf das Netzwerk zugreifen können. Aus diesem Grund muss bereits beim Kauf der W-LAN Hardware auf die Unterstützung von 104-Bit Verschlüsselung geachtet werden, denn auch hier gilt: je länger der Schlüssel, umso sicherer die Verschlüsselung. Auch die WEP-Verschlüsselung kann allerdings gehackt werden und gilt nicht als sehr sicher.

- *WPA-Verschlüsselung*
  Der Einsatz von WPA (Wi-Fi Protected Access) verstärkt die Verschlüsselung in einem W-LAN derart, dass ein Hacking kaum mehr möglich ist. Die erhöhte Sicherheit kann WPA allerdings nur gewährleisten, wenn lange, möglichst zufällige Passphrasen verwendet werden. Seit 2004 gibt es den weiter verbesserten Standard WPA2, der andere Algorithmen verwendet, aber prinzipiell gleich wie WPA funktioniert. Für beide Standards gilt, dass alle am W-LAN teilnehmenden Geräte die jeweilige Verschlüsselung unterstützen müssen. Achten Sie deshalb beim Kauf sowohl des Access-Points wie auch

der W-LAN-Adapter darauf, dass sie alle zumindest WPA unterstützen. Wenn Sie ein Notebook haben, dessen eingebauter W-LAN-Adapter lediglich WEP-kompatibel ist, so können Sie auch einen zweiten W-LAN-Adapter beispielsweise über die PCMCIA-Schnittstelle anschliessen.

- *Einschränkung der MAC-Adressen*
  Die meisten Router erlauben es, den Zugang zum Netzwerk auf vordefinierte MAC-Adressen zu beschränken. Dadurch wird ein potenzieller Eindringling mit einer unbekannten MAC-Adresse bereits „an der Eingangstür“ abgeblockt. Auch hier gilt es zu beachten, dass mit bestehenden Hacker-Tools gültige MAC-Adressen simuliert werden können.

- *Einsatz von VPN*
  Die sicherste Methode, ein W-LAN vor Hackern zu schützen, ist zur Zeit der Einsatz von VPN (Virtual Private Networks). Ein VPN kann aber nur bei Server-basierten Netzwerken eingesetzt werden und ist relativ aufwändig im Aufbau.
  Falls Sie aber schützenswerte Daten in ihrem Netzwerk bearbeiten, so ist der Einsatz von VPN zwingend notwendig.

- *Weitere wichtige Punkte für ein sicheres W-LAN*
  In jedem Fall ist immer eine Firewall einzusetzen, um die ein- und ausgehenden Verbindungen zu kontrollieren und diese falls nötig auf bestimmte IP-Adressen zu beschränken. Mit einer “Intrusion Detection“-Software können Attacken von Aussen erkannt und abgeblockt werden. Der Einsatz eines Virenschutz-Programms ist ebenfalls notwendig. Diese Massnahme kann zwar nicht das Eindringen von Hackern verhindern, aber die allfällig hinterlassenen Viren beseitigen. Zusätzlich können Sie die Dateien mit einer Kryptographie-Software (z.B. PGP, Pretty Good Privacy) verschlüsseln, was für Hacker eine weitere Hürde darstellt.

4. Vorsicht mit geheimen Daten

Grundsätzlich ist aber davon auszugehen, dass kein Funknetz zu 100% sicher ist, auch wenn es mit allen Sicherheitsmechanismen ausgestattet ist. Wenn sich ein professioneller Hacker daran macht in ihn Netzwerk einzudringen, wird er es bei entsprechendem Geschick früher oder später höchstwahrscheinlich knacken können. WEP-Verschlüsselung können mit frei verfügbaren Tools gehackt werden und MAC-Adressen können abgehört und manipuliert werden. Ein W-LAN sollte entsprechend nur mit einem hohen Sicherheitsstandard betrieben werden, um einen unbefugten Zugriff zu verhindern. Jeder Betreiber sollte sich regelmässig über den aktuellen Stand der Technologie- und Sicherheitsempfehlungen informieren und diese umsetzen.

Falls Sie mit geheimen Daten arbeiten, sollten diese ganz vom Funknetz getrennt bearbeitet werden.

5. Fragen und Informationen

Für Fragen und weitere Informationen über W-LAN stehen Ihnen die Datenschutzbeauftragten gerne zur Verfügung.

Postadresse:	Datenschutzbeauftragte des Kantons Luzern Bahnhofstrasse 15 6002 Luzern
Telefon:	+ 41 41 228 66 06
Fax:	+ 41 41 228 69 13
E-Mail:	dsb@lu.ch **WARNUNG**: Der E-Mail-Verkehr ist unsicher. Vertrauliches gehört deshalb nicht in E-Mails!
Internet:	http://www.datenschutz.lu.ch

Luzern, Oktober 2004
(aktualisiert Oktober 2005)