Information für Wireless Anwender: 10 Punkte zum Sichern Ihrer Verbindung

i

In diesem Beiblatt finden Sie wichtige Informationen, damit **Sie** als Käufer von Wireless Produkten möglichst einfach zu einer bestmöglich sicheren Wireless Netzwerkumgebung finden. Hersteller informieren teilweise ungenügend, somit ist nicht immer verständlich, wie man sich vor Einbrüchen in ein Wireless Netzwerk schützen kann. Alle wichtigen Punkte sind in diesem Papier aufgelistet und mit Hilfe des Produkthandbuches kann man sich relativ einfach vor Einbrüchen Dritter schützen. Nicht alle Geräte unterstützen die hier aufgelisteten Sicherheitsmassnahmen. Vergessen Sie nicht: **Sie sichern nicht nur Ihr Wireless Netzwerk, sondern auch sich und Ihre Daten mit solchen Massnahmen.**

- ● Erforderliche Massnahme
- ○ Optionale Massnahme
- [i] Information
- [S] Supportmöglichkeit
- [§] Gesetzliches
- [!] Wichtiges

1

WEP Verschlüsselung einschalten (Achtung, dies muss auf dem Access Point wie auch auf den Adaptern erfolgen). Die Verschlüsselung muss auf mindestens 128-BIT konfiguriert sein. Als Schlüssel soll keine einfache Folge von Zeichen (AAAA) eingesetzt werden sondern eine Komplexe Zeichenfolge wie z.B. A9FE10. **Den WEP Schlüssel sollten Sie zu Ihrer eigenen Sicherheit in regelmässigen Abständen wechseln**. **Zugriffsschutz vor Dritten. Achtung WEP bietet nur einen Grundschutz, kann aber mit entsprechendem Aufwand durchbrochen werden!**

2

Auf dem Access Point die Zugriffsliste auf MAC Ebene einschalten und die vorhandenen Wireless Adapter darin eintragen die Sie benutzen wollen. **Zugriffsschutz vor Dritten.**

3

SSID/ESSID so benennen, dass kein Zusammenhang mit dem Namen einer Firma oder einer Privatperson hergestellt werden kann. **Betreiber eines Access Points kann nicht anhand des Namens des Netzwerkes identifiziert werden.**

4

SSID/ESSID verstecken. (NO SSID Broadcasting) **Netzwerk ist nicht öffentlich sichtbar. Achtung man kann sich so auch vom Access Point aussperren.**

5

Zugriffsdaten (Benutzername und Passwort) für den Access Point in regelmässigen Abständen ändern. Passwort mit komplexen Zeichenfolgen (Zahlen, Klein- und Grossbuchstaben gemischt, Sonderzeichen) wählen.

6

Bei längerem Nichtbenutzen des Wireless Netzwerkes den Access Point ausschalten. **Kein Einbruch möglich während dieser Zeit.**

7

Schliessen Sie den Access Point nicht an Ihr Firmennetzwerk, wenn Sie sich nicht sicher sind, dass es genügend geschützt ist gegen Zugriff von aussen. Netzwerklaufwerke mit Passwort schützen. **Erhöhter Zugriffsschutz auf Computer und Server. Achtung: Verlust (Datenklau) von Firmendaten kann auch rechtliche Schritte zur Folge haben.**

8

Computer und Server mindestens mit einer Softwarefirewall schützen. **Zugriffsschutz auf den Systemen**

9

Passwörter nirgendwo aufschreiben und kein Passwort zweimal benutzen. Nicht über Mail versenden oder auf einem Datenträger speichern. **Einbruchswahrscheinlichkeit ist kleiner.**

10

Kontrolle von Logdateien des Access Points oder Wireless Routers auf Angriffsversuche.

S

Support zu den verschiedensten Problemen erhalten Sie auch auf der unabhängigen Wireless Diskussionsplatform

www.wireless-forum.ch

Wireless-Forum

§

Vorsicht bei ungeschützten Wireless Netzwerken. Sie können für Taten Dritter haftbar gemacht werden!

!

Gemäss einer Statistik von www.wireless-bern.ch sind ca. **60%** der Access Points **NICHT** verschlüsselt
Achtung: Alle hier genannten Sicherheitsfunktionen sind beim Neukauf eines Produktes **ausgeschaltet**!