

## Mit Highspeed sicher ins Internet – Keine Chance für War Driver!

Lernpartnerschaft



Frank Schneider

Diplom Volkswirt  
Mitarbeiter Systemintegration

Brühl, 15.09.2005

## Überblick

1. Abgrenzung des Themas
2. Faktoren einer sicheren Internetnutzung
3. Gemeinsam ins Internet – Vernetzung auch ohne Kabel

## 1. Abgrenzung des Themas

- Einstieg in die Thematik
- Aufzeigen des Gefährdungspotentials
- Wirksame Abhilfe
- Sinnvolle Aufwand- Nutzen- Relation

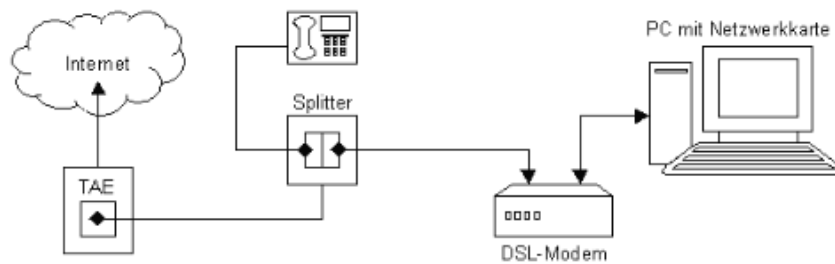
## 2. Faktoren einer sicheren Internetnutzung

- Verwendung eines Routers
- Virenschutz
- Aktualität des Betriebssystems -  
Update/Patches
- Konfiguration des Betriebssystems
- Problematik des WLAN

## 2.1 Verwendung eines Routers I

Anschlussmöglichkeiten an DSL:

- Direkter Anschluss des DSL-Modems an die Netzwerkkarte (bzw. USB-Schnittstelle)



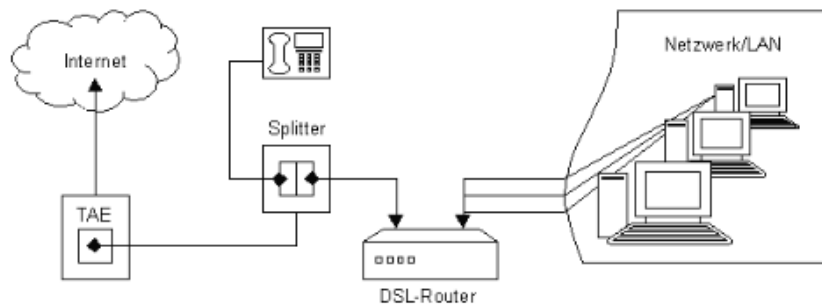
© 2005

STREITZ CONSULT  
GmbH

## 2.1 Verwendung eines Routers II

Anschlussmöglichkeiten an DSL:

- Anschluss über einen Router



© 2005

STREITZ CONSULT  
GmbH

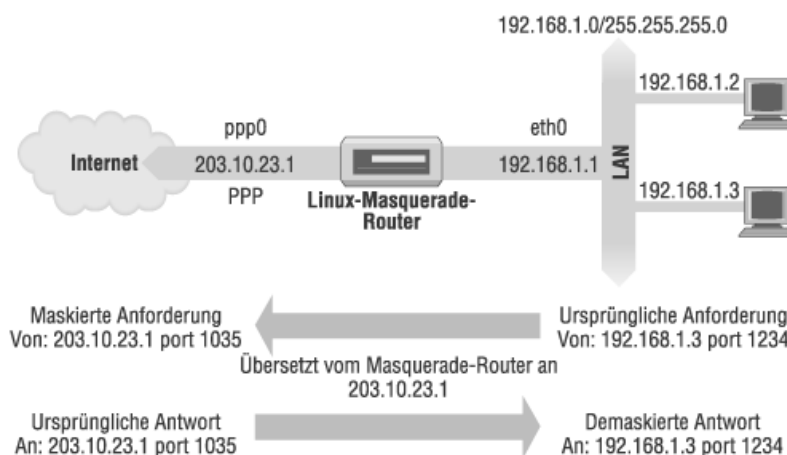
## 2.1.1 Router- grundsätzliche Funktionen

Vermittlungstechnisches Gerät zur Verbindung technisch unterschiedlicher lokaler Netze.

- Router als eine Art Übersetzer zwischen Netzwerken in denen unterschiedliche Sprachen gesprochen werden
- Die eigentliche Routing-Funktionalität bietet keine zusätzliche Sicherheit

## 2.1.2 Router – Sicherheitsmechanismen I

IP-Masquerade: Adressumsetzung nach Außen



## 2.1.2 Router – Sicherheitsmechanismen II

### Firewall: Filterregeln

Jede IP-Verbindungsanforderung wird auf Charakteristika an Hand einer Liste vordefinierter Regeln überprüft und die Verbindungsanforderung je nach Ergebnis zugelassen oder abgelehnt.

Beispiele Charakteristika:

IP-Adresse, IP-Port (Service), Applikation, Uhrzeit

## 2.1.2 Router – Sicherheitsmechanismen III

### Firewall-Zielkonflikt:

- Sichere Einstellungen führen zu eingeschränkter Funktionalität
- Volle Funktionalität ist meist unsicher
  
- Anpassungen an die individuelle Situation sind notwendig
- Hintergrundwissen ist erforderlich
- Standardvorgaben täuschen Sicherheit nur vor

## 2.2 Virenschutz

Ein Virenschutz ist zwingend notwendig wenn:

- Eine Verbindung mit dem Internet besteht
- Dateien über externe Datenträger in den PC gelangen

→ Eigentlich immer!

### 2.2.1 Virenschutz – geeignete Programme

Es gibt sehr viele Programme auf dem Markt.

Auswahlkriterien:

- Bedienung
- Schutz: kann nicht selber beurteilt werden
- Preis

## 2.2.2 Virenschutz – Aktualität

Die Virendefinition muss regelmäßig aktualisiert werden:

- Zeitgeplant (automatisch)
- Auf Anforderung (manuell)

Aber: häufig ist die Berechtigung zur Aktualisierung zeitlich beschränkt.

## 2.2.3 Virenschutz – unsere Empfehlung

- AntiVir PersonalEdition Classic  
(Freeware, nur für den privaten Einsatz)
- AntiVir PersonalEdition Premium (20 €)

Infos unter: [www.antivir.de](http://www.antivir.de)

## 2.3 Aktualität Betriebssystem

Jedes Betriebssystem enthält Schwachstellen, die für Angriffe genutzt werden können!

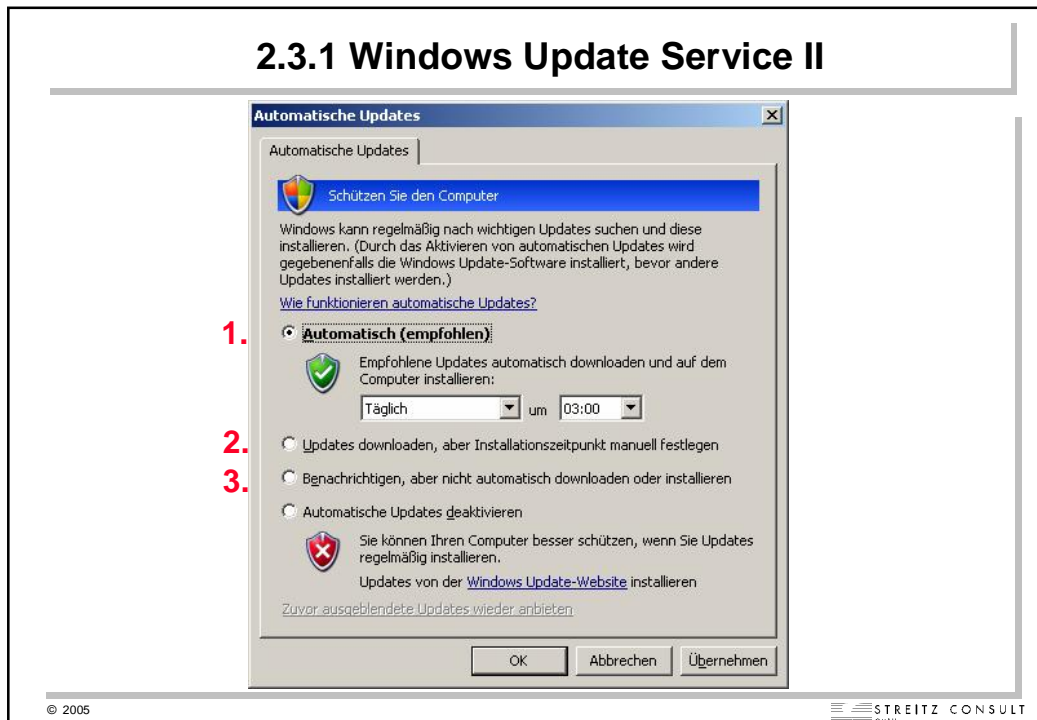
**Wichtig:**

Schließen erkannter Sicherheitslücken über Patches.

### 2.3.1 Windows Update Service I

- Verfügbar für  
Microsoft Betriebssysteme ab WINDOWS 2000
- Grundfunktionen:  
(Voll-)automatisierte Aktualisierung des  
Betriebssystems

## 2.3.1 Windows Update Service II



## 2.3.1 Windows Update Service III

Was geschieht bei welcher Option?

### 1. „Automatisch (empfohlen)“

- Updates werden automatisch herunter geladen und zur vorgegebenen Urzeit installiert
- Benutzer ohne Admin-Rechte werden zum Schließen ihrer Anwendungen aufgefordert, der Rechner wird **automatisch** neu gestartet

### 2.3.1 Windows Update Service IV

Was geschieht bei welcher Option ?

#### 2. „Updates downloaden, aber Installationszeitpunkt manuell festlegen“

- Updates werden automatisch herunter geladen
- Benutzer mit Admin-Rechte werden über ein Icon im System-Try informiert, dass die Updates nun installiert werden können
- Benutzer ohne Admin-Rechte merken nichts, Updates werden beim nächsten Herunterfahren automatisch installiert

### 2.3.1 Windows Update Service V

Was geschieht bei welcher Option?

#### 3. „Benachrichtigen, aber nicht automatisch downloaden oder installieren“

- Benutzer mit Admin-Rechte werden vor dem Download um Erlaubnis gebeten
- Benutzer ohne Admin-Rechte erfahren nichts

## 2.3.2 „alte“ Betriebssysteme

### **Gefährdungspotential:**

- + Neu erkannte Sicherheitslücken werden nicht mehr geschlossen
- Große Sicherheitslücken wurden bereits erkannt und geschlossen
- Dienen nur noch selten als Angriffsziele

## 2.4 Konfiguration des Betriebssystems

### **Ziel:**

Fläche für Angriffe aus dem Internet sollte möglichst gering gehalten werden.

## 2.4.1 Rechte/Benutzereinrichtung

Gründe für eine Einschränkung der Rechte des „normalen“ Benutzers:

- Viele Angriffe können nur mit den (hoffentlich) beschränkten Rechten des gerade angemeldeten Benutzers ausgeführt werden
- Schutz vor Fehlbedienung

## 2.5 Problematik des WLAN I

- Funkverbindungen enden nicht an der Wohnungs- bzw. Grundstücksgrenze
- Es ist sehr viel einfacher eine Funkverbindung herzustellen als eine (Kabel-) Leitung anzuzapfen

## 2.5 Problematik des WLAN II

Missbrauchspotential:

- Mitnutzung der Internetverbindung
  - Verursachung von Kosten
  - „verbotene“ Handlungen unter fremden Zugang
- Ausspionieren von Daten
- Sabotieren von Daten und Funktion

### 2.5.1 War Driving I



## 2.5.1 War Driving II

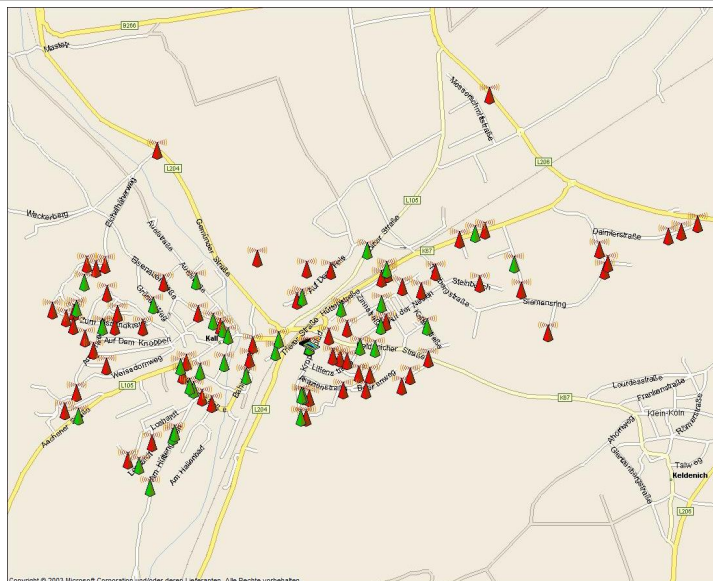
Systematisches Suchen und Erfassen von WLANs mit Hilfe eines Autos

→ Ziel: Kartographieren der WLANs

Benötigte Werkzeuge:

- Notebook mit WLAN-Karte
- Leistungsfähige Antenne
- (unterstützende Programme; frei verfügbar im Internet)
- (GPS-Empfänger)

## 2.5.1 War Driving – Bsp. Kall (Eifel) IV



## 2.5.1 War Driving III

Zugang zum Netzwerkmedium ist bei Funknetzen extrem einfach.

→ daher sind weitere Schutzmechanismen erforderlich

## 2.5.2 Verschlüsselungsvarianten

**WEP** (Wired Equivalent Privacy, alter Standard):

- Kann in sehr kurzer Zeit „geknackt“ werden
- Dadurch eigentlich zu unsicher; aber besser als gar nicht verschlüsselt

**WPA** (Wi-Fi Protected Access)

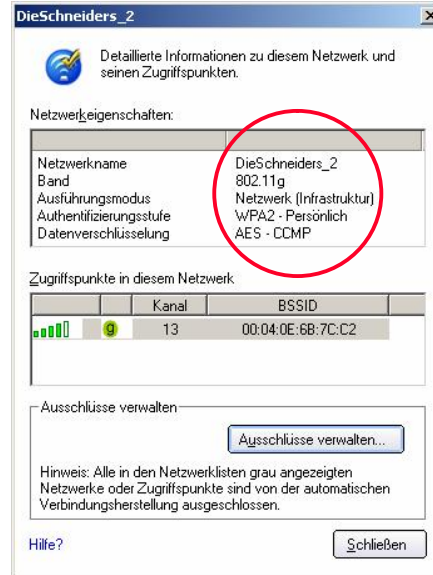
- Relativ sicher
- Wird noch nicht von allen Geräten unterstützt

**VPN** (Virtual Private Network)

## 2.5.2 Verschlüsselung I

### Beispiel:

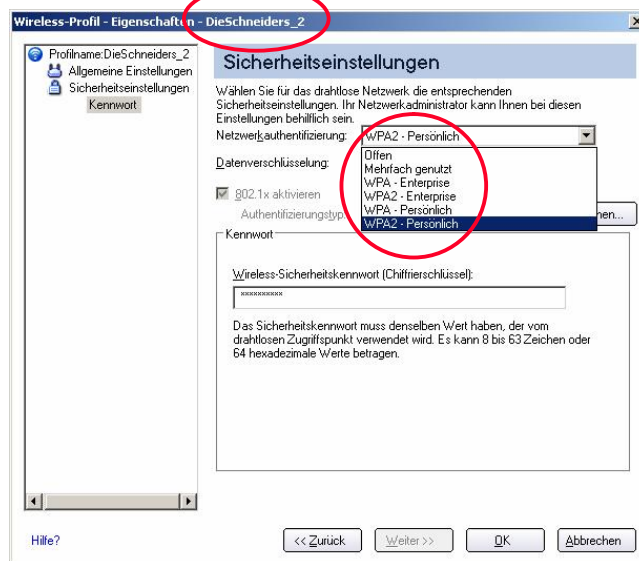
Einstellungen zu einer **WPA**-  
Verbindung mit Hilfe einer  
Intel 2200 bg – Netzwerkkarte  
(Notebook mit Intel-Centrino)



© 2005

STREITZ CONSULT

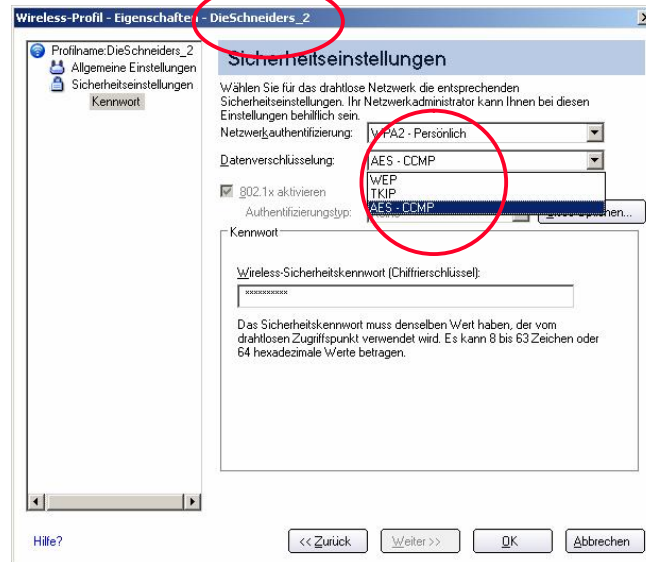
## 2.5.2 Verschlüsselung – Bsp. WPA II



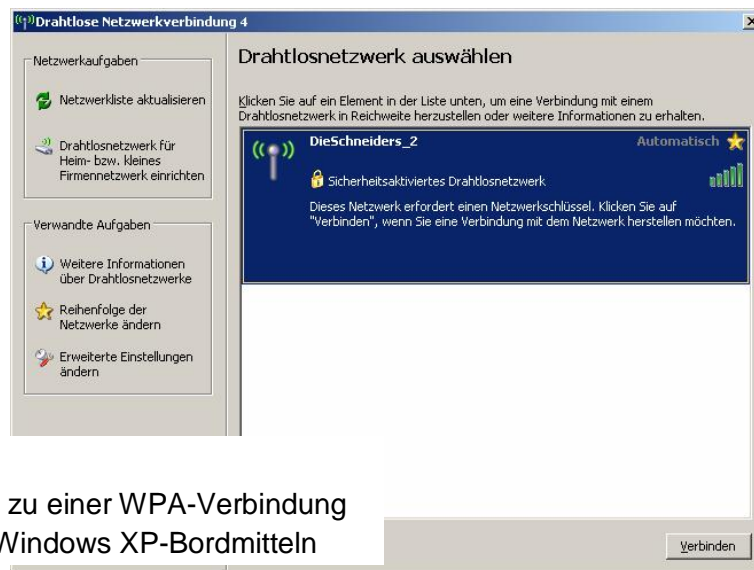
© 2005

STREITZ CONSULT

## 2.5.2 Verschlüsselung – Bsp. WPA III

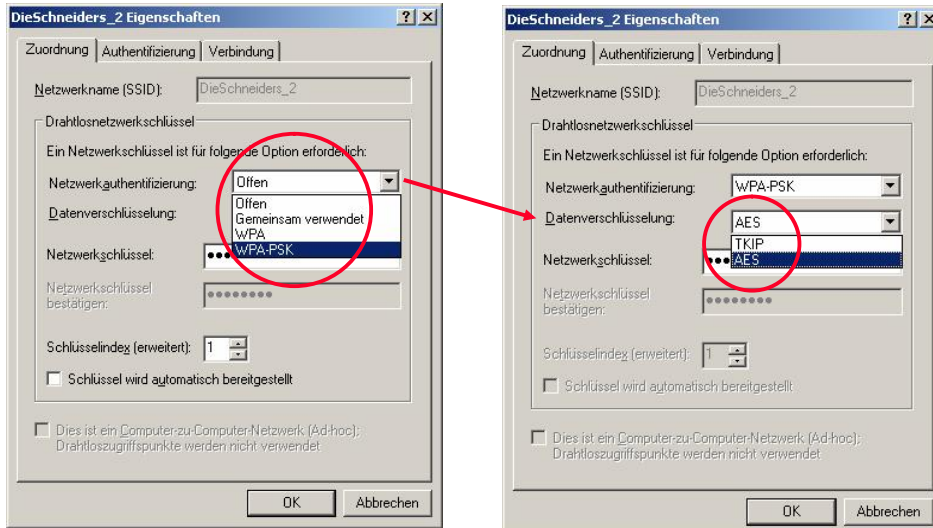


## 2.5.2 Verschlüsselung – Bsp. WPA IV



**Beispiel:**  
Einstellungen zu einer WPA-Verbindung  
mit Hilfe von Windows XP-Bordmitteln

## 2.5.2 Verschlüsselung – Bsp. WPA



## 2.5.3 sonstige Maßnahmen

- **Access Point mit individuellem Passwort sichern**
- Mac-Filter
- Kennung (SSID) verbergen
- Kontrolle von Onlinezeiten bzw. Übertragungsvolumen
- Nutzung zeitlich einschränken

### 3. Gemeinsam ins Internet - Vernetzungsalternativen

Nutzen der Vernetzung

→ gemeinsame Nutzung von Ressourcen

- Internetzugang (Router)
- Daten
- Drucker

### 3.1 Gemeinsam ins Internet - Vernetzungsmedien

- **Kabel**  
**(klassisches Netzwerk)**
- **Funk**
- **Stromnetz**

### 3.1.1 Kabel (klassisches Netzwerk) I

Vernetzung über Kupferkabel:

→ für den „Hausgebrauch“ sind Twisted-Pair-Kabel der Kategorie 5e relevant

- 100 Mbit (ca. 8-9 MB/s)
- 100 m Kabellängen
- Sternförmige Verkabelung mit zentralem Verteiler (Switch)
- RJ 45 Anschlüsse

### 3.1.1 Kabel (klassisches Netzwerk) II

#### **Pro:**

- Bewährte Technik
- Wenig stör anfällig, „garantierte“ Qualität
- Preiswerte Komponenten
- Für handwerklich versierten Laien realisierbar

#### **Kontra:**

- Kabel müssen verlegt werden
- Ortsgebunden

### 3.1.2 WLAN (Funk) I

Vernetzung über Funk:

→ für den „Hausgebrauch“ ist der Standard IEEE 802.11g relevant

- 54 Mbit (ca. 2-3 MB/s real)
- (125 Mbit, 802.11g++)
- Reichweite bis 100 m
- Realisierung meist über zentralen Accesspoint

### 3.1.2 WLAN (Funk) II

**Pro:**

- **Keine Kabel notwendig**
- Nicht ortsgebunden
- Preiswerte Komponenten/Accesspoint im Router meist schon vorhanden

**Kontra:**

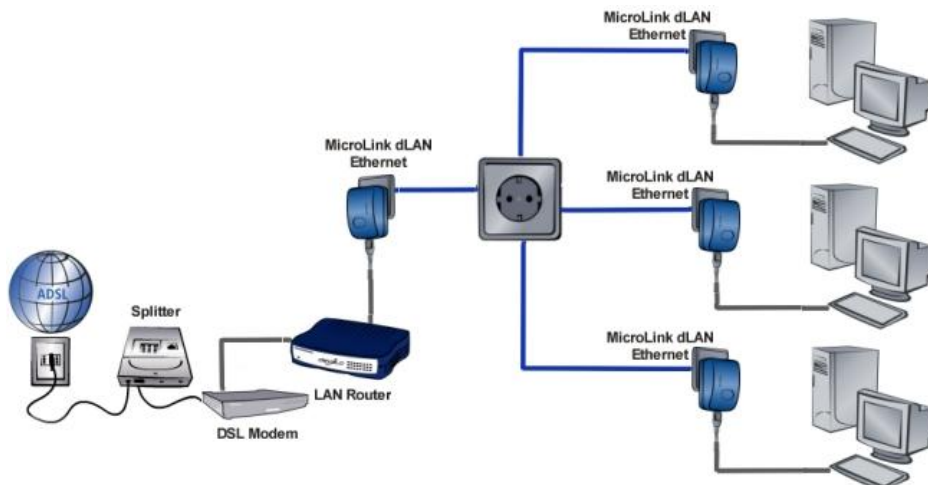
- störanfällig
- Reichweite je nach örtlichen Gegebenheiten völlig ungewiss
- relativ niedrige Geschwindigkeit
- relativ unsicher/Sicherheit muss konfiguriert werden
- Permanenter Stromverbrauch

### 3.1.3 Stromnetz I

Vernetzung über (vorhandene) Stromnetz:

- 14 Mbit/s (ca. 1 MB/s real)
- Auch 24 / 85 Mbit/s
- Reichweite bis 200 m
- Keine Konfiguration notwendig

### 3.1.3 Stromnetz II



### 3.1.3 Stromnetz III

**Pro:**

- **Keine Kabel notwendig**
- Meist sehr unkompliziert

**Kontra:**

- Funktion abhängig vom Zustand des Stromnetzes
- Reichweite je nach örtlichen Gegebenheiten völlig ungewiss
- niedrige Geschwindigkeit
- muss konfiguriert werden
- Adapter relativ teuer (ca. 50 €)

### Vielen Dank

**Ich  
danke  
für  
Ihre  
Aufmerksamkeit**

