

## Der blaue Zahn verbindet – manchmal ungewollt

### Tipps der E-Plus Gruppe zum sicheren Umgang mit Bluetooth

Vor gut zehn Jahren befreite sich das Mobiltelefon vom Kabel. Seitdem verbinden sich die meisten Geräte per Bluetooth mit der angrenzenden Außenwelt. Tastaturen und Mäuse stellen drahtlos Kontakt zum Computer her, Handys verbinden sich mit Freisprecheinrichtungen und Fernbedienungen funken ihre Befehle wie von Geisterhand zum Fernseher. Bluetooth ist allgegenwärtig und fast jeder Handybesitzer nutzt es täglich. Viele sogar, ohne es zu wissen.

Ohne Frage eine bequeme Art des Telefonierens, vor allem unterwegs. So ganz ohne Kabel. Aber Bluetooth kann noch mehr. Wer Daten per Bluetooth verschickt, erzielt Übertragungsraten von mehr als 1 MBit/s, ältere Geräte erreichen noch etwa 700 kBit/s. Ideal ist die kurze Funkverbindung also für Notebooks, die ein Handy als Modem nutzen.

#### **Straßencafés eher ungeeignet**

Trotz aller Bequemlichkeit - ist Bluetooth in der eigenen Wohnung oder am Arbeitsplatz noch weitgehend sicher, so gilt dies nicht für öffentliche Bereiche. Wissenschaftler aus Israel demonstrierten im Jahr 2005, wie man fremde Bluetooth-Funkverbindungen für eigene Zwecke nutzt. Akademisches Know-How benötigt dazu niemand. Es reicht aus, die Jagd auf ahnungslose Handynutzer mit einem Notebook und darauf installierter, frei verfügbarer Software aus dem Internet zu starten. Angreifbar ist Bluetooth insbesondere bei älteren Mobiltelefonen. Die Länge der Bluetooth-Geheimzahl, mit der ein Nutzer den Zugriff von außen freigibt, ist bei diesen Geräten meist auf vier Zeichen für die Geheimzahl beschränkt. Und damit steigt das Risiko. Besitzer älterer Handys oder Notebook-Steckkarten sollten also genauer hinsehen und einige Grundregeln beachten.

#### **Zugriff auf den Blauzahn**

Mit dem sogenannten „Bluebugging“ erhalten Angreifer Zugriff auf ein fremdes Mobiltelefon, ohne Wissen des Benutzers. Auf diese Weise können Neugierige Textnachrichten senden und lesen, Kontakte im Adressbuch einsehen und Tele-

fongespräche mithören oder ins Internet gehen. Beim „Bluesnarfing“ dagegen haben Außenstehende nur Zugriff auf das Adressbuch, gespeicherte Bilder und den Kalender.

Eine besondere Form des Angriffs ist der „Car Whisperer“: Bei dieser Methode greifen Fremde auf die Freisprecheinrichtung im Fahrzeug zu. Sie belauschen unbemerkt die Gespräche der Insassen über das eingebaute Mikrofon im Fahrzeug. Allerdings funktioniert dies nur mit einer speziellen Ausrüstung und auf kurze Entfernung. Schwieriger ist das Abhören von Fahrzeugen im fließenden Verkehr, deutlich einfacher dagegen auf einem Parkplatz oder im Stau.

## **Geschädigte zahlen hohe Rechnungen**

Egal, auf welchem Wege: Greifen Außenstehende über Bluetooth auf das eigene Mobiltelefon zu, verursachen sie Kosten für Verbindungen ins Internet oder für Telefonate. Insbesondere im Ausland können gekaperte Verbindungen schnell teuer werden.

Hier einige Tipps der E-Plus Gruppe für Bluetooth Anwender:

- Stellen Sie die Bluetooth-Verbindung im Menü des Gerätes auf „Unsichtbar“ oder „nicht sichtbar“. So können Angreifer das Mobiltelefon kaum entdecken.
- Wählen Sie für die PIN deutlich mehr als vier Zeichen. Wirkungsvoll sind Geheimzahlen mit acht Zeichen und mehr.
- Nutzen Sie ein aktuelles Mobiltelefon oder eine Datenkarte mit dem Standard Bluetooth 2.0 oder besser. Ältere Geräte (bis 2004) arbeiten nach einem alten Standard und gelten daher als unsicher.
- Speichern Sie die PIN auf Ihrem Mobiltelefon. So vermeiden Sie es, bei jeder neuen Verbindung des Schlüssel eingeben zu müssen. Dieser wird sonst über die Funkverbindung übertragen.

- Einmal erkannte Gegenstellen sollte man dauerhaft in den Bluetooth-Einstellungen im Handy speichern.
- Eine unerwartete Abfrage der PIN trotz bereits bestehender Verbindung sollte stutzig machen und zur Vorsicht mahnen. Geben Sie Ihre PIN nur ein, wenn Ihnen das verbindende Gerät bekannt ist!
- Aktualisieren Sie die Software Ihres Gerätes. Dies ist meist sowohl per Internet als auch über Mobilfunk möglich.
- Verbinden Sie Ihre Geräte möglichst nur in privaten Umgebungen, also beispielsweise zu Hause.

Weitergehende Informationen zum Thema Bluetooth finden bietet die Internetseite der „Bluetooth Special Interest Group (SIG)“, einem gemeinnützigen Unternehmensverband: [www.bluetooth.com](http://www.bluetooth.com)

Über den Namen Bluetooth:

Der Name Bluetooth entstammt einer Ehrung des dänischen Wikingerkönigs Harald Blauzahn, der im 10. Jahrhundert lebte. Er galt als besonders kommunikationsfähig. Zu den Entwicklern des neuen Funkstandards gehörten Ende der neunziger Jahre auch die beiden skandinavischen Firmen Nokia und Ericsson, so wählte man auch deshalb den Namen des nordischen Wikingerkönigs.

Hannover, 17. März 2010

## **E-Plus Gruppe**

Unternehmenskommunikation / Themendienst Verbraucher

Jörg Borm

E-Mail: [presse-themendienst@eplus-gruppe.de](mailto:presse-themendienst@eplus-gruppe.de)

Tel. 0511 - 3832 - 220

Fax 0511 - 3832 - 219