orell füssli

Norbert Pohlmann / Markus Linnemann

Sicher im Internet

Tipps und Tricks für das digitale Leben

Sicher im Internet
Norbert Pohlmann
Markus Linnemann
orell füssli

Ein Projekt vom Institut für Internet-Sicherheit:

securityNews: Kostenlose App für mehr Sicherheit im Netz

- Kostenlose App vom Institut für Internet-Sicherheit
- Aktuelle Sicherheitshinweise für Smartphone, Tablet, PC und Mac
- Warnung vor Sicherheitslücken in Standardsoftware, dank BSI-Schwachstellenampel
- Konkrete Anweisungen für Privatanwender und Unternehmen

» www.it-sicherheit.de

Available on the App Store

ANDROID APP ON Google play

Mit freundlicher Unterstützung

Bundesamt für Sicherheit in der Informationstechnik

Norbert Pohlmann/Markus Linnemann

Sicher im Internet
Tipps und Tricks
für das digitale Leben

Teil 6: Antennen ausfahren –
Zugang zum Internet

orell füssli Verlag AG

Antennen ausfahren – Zugang zum Internet

«Es hat gefunkt» steht umgangssprachlich für den Anfang einer Verbindung zwischen zwei Menschen oder auch dafür, etwas begriffen zu haben. Um die Funktechnik zu erklären, wäre ein Ausflug in die Physik notwendig, der Ihnen hier aber erspart bleiben soll.

Funknetzwerke sind «die begonnene Zukunft». Kaum eine Technologie hat sich so rasant verbreitet wie Wireless LAN (WLAN), aber auch seine «Kollegen» GSM, UMTS, Bluetooth und Co. sind gewaltig auf dem Vormarsch. Denn sie bilden die Basis für das prognostizierte «Überall-Internet». Und die Möglichkeiten scheinen in der Tat grenzenlos: Während eines Stadtbummels durch eine historische Altstadt doziert das Handy im Vorbeigehen über ein Gebäude – die Daten dazu kommen direkt aus dem Internet. Im Café an der Ecke können Internetnutzer frühstücken und gleichzeitig mit dem Handy, dem Notebook oder einer WLAN-Uhr ihre E-Mails abfragen. Und auch zu Hause ist es vorbei mit dem Kabelchaos. Arbeiten mit dem Notebook auf der Couch wird zum entspannten Erlebnis.

Die Funktechnologie bietet eine Menge Vorteile – aber auch Gefahren, wenn sie nicht richtig eingesetzt wird. Denn sensible Daten, die über die Luft übertragen werden, können ganz einfach mitgelesen werden, wenn sie nicht ausreichend geschützt sind. Deshalb wird in diesem Kapitel der richtige

und vor allem sichere Umgang mit den unterschiedlichen Funktechnologien erläutert.

DSL und WLAN – sicher einrichten und sicher nutzen

Vor einigen Jahren stellte bereits ein Prominenter in einem Fernsehspot die Frage: «Bin ich schon drin?» Die damalige Werbung eines Internetanbieters sollte suggerieren, wie einfach es ist, mit seiner Zugangstechnologie ins Internet zu gelangen. Auch lag zu dieser Zeit noch jede Woche eine CD in deutschen Briefkästen, die 50 Stunden kostenloses Surfen versprach – ein Angebot, das heute, da die Flatrate die privaten Haushalte erobert hat, niemanden mehr hinter dem Ofen hervorlocken würde. Sie sehen, auch vor zehn Jahren versprach die Werbung schon den problemlosen Anschluss des Computers ans Internet. Aber damals wie heute gibt es immer wieder Probleme …

Dieses Kapitel soll Ihnen einen kurzen Überblick geben, wie ein Internetanschluss heutzutage eingerichtet wird. Ein besonderes Augenmerk liegt dabei auf dem DSL-Router mit WLAN-Funktion, der in der Regel vom Anschlussanbieter gleich mitgeliefert wird.

Was ist Wireless LAN (WLAN) genau?

Die Abkürzung WLAN steht für Wireless Local Area Network, die kabellose Datenübertragung in Verbindung mit Computern, Notebooks, Handys, Lautsprechern, Internetradios, Massenspeichern oder Inventurscannern in Kaufhäu-

sern. Es ist fraglos eine eindrucksvolle Technik, bei der die Daten in Funkwellen übertragen und wieder aufgefangen werden. Die Reichweite eines normalen WLAN-Routers beträgt 30 bis 100 Meter (mit einer entsprechenden Antenne bis 300 Meter), wobei der Empfang durch Hindernisse wie dicke Wände beeinträchtigt oder sogar komplett verhindert werden kann. Aber die Reichweite der Funksignale kann mit zusätzlichen Routern, die das Funksignal als Repeater auffangen und weiterleiten, verlängert werden. Direkte WLAN-Verbindungen zwischen zwei oder mehreren Endgeräten ohne feste Infrastruktur nennt man auch Ad-hoc-Modus.

DSL – die Varianten

Es gibt verschiedene Möglichkeiten, ins Internet zu gelangen. Für den privaten Haushalt sind vor allem zwei Varianten üblich. Die erste ist der traditionelle Zugang über die Telefonleitung. Digital Subscriber Line (DSL) bezeichnet dabei einen

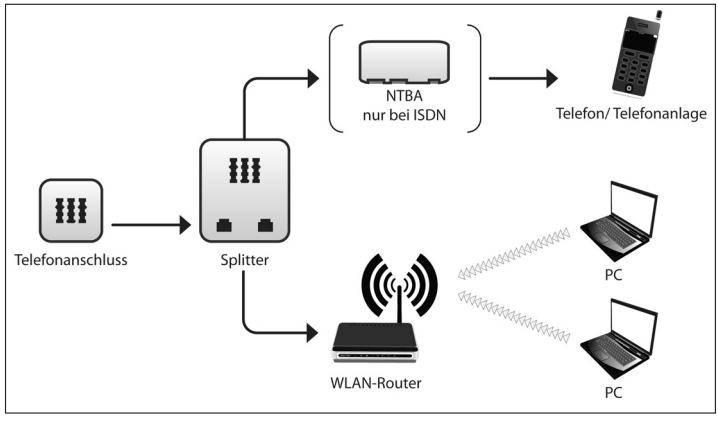

Abbildung 30: Verkabelung der notwendigen Geräte bei einem DSL-/Anschluss über die Telefonleitung (WLAN-Router mit integriertem Modem)

Übertragungsstandard, der Daten mit hohen Übertragungsraten über einfache Telefonleitungen zum Internet sendet und von dort empfängt.

Die zweite Variante ist der Zugang über das Netz eines Kabelbetreibers, also über die Steckdose, an die auch der Fernseher angeschlossen ist. Bei dieser Variante ist in der Regel ein «Telefonanschluss» mit integriert, wodurch die eigentliche Telefonleitung eventuell überflüssig wird. Allerdings muss hier teilweise noch mit Qualitätseinbußen gerechnet werden (siehe Seite 128f.).

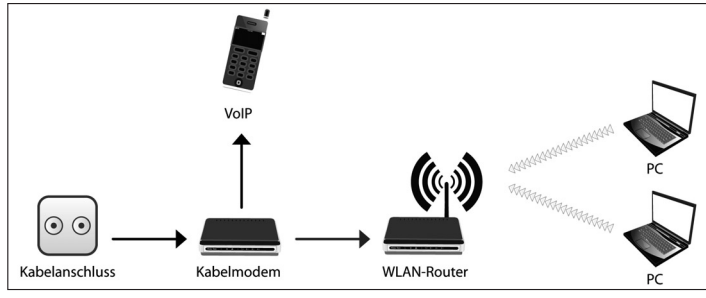

Abbildung 31: Verkabelung der notwendigen Geräte bei einem DSL-Anschluss über das Kabelnetz

Je nach Anschlussart erhält der Kunde ein DSL- oder Kabelmodem für den Telefonanschluss, das gemäß der beiliegenden Anleitung angeschlossen wird. Bei DSL über den Telefonanschluss wird außerdem ein Splitter verwendet, der das Telefon- und das Datensignal trennt. Bei Verwendung von ISDN kommt hinter dem Splitter in der Telefonleitung noch eine Box namens NTBA zum Einsatz. Zusätzlich erhält der Kunde im Allgemeinen einen WLAN-Router. Dieser wird mit dem jeweiligen Modem beziehungsweise über ein Kabel direkt mit dem Telefonanschluss verbunden (sofern das Mo-

dem bereits im Router integriert ist). Für Nutzer, die sich das Einrichten des Internetzugangs nicht selbst zutrauen, bieten die Internetanbieter mittlerweile die Einrichtung der Geräte zu einem Pauschalpreis an.

DSL-Router sicher konfigurieren

Ein Router ist ein Netzkoppelelement, das im Einsatzfeld Heimnetzwerk die Schaltstelle zwischen dem Hausanschluss in den eigenen vier Wänden und dem Internet bildet. Ein Router entscheidet, welche Daten aus dem Internet wohin ins Heimnetzwerk geschickt werden und umgekehrt. Er ist für die Internetverbindung jedoch nicht zwingend notwendig. Wird nur ein einziger Computer angeschlossen, kann dieser direkt mit dem Modem verbunden werden. Das ist heutzutage aber eher unüblich und im Hinblick auf die Erweiterbarkeit und Sicherheit auch nicht sinnvoll. Um sämtliche Sicherheits-, Mobilitäts- und Praktikabilitätsvorteile nutzen zu können, sind Router Standard, die auch WLAN anbieten, also WLAN-Router. An einen handelsüblichen WLAN-Router lassen sich im Normalfall vier Computer per Kabel anschließen und meist 253 Geräte per WLAN (zumindest theoretisch, mehr als fünf sind jedoch nicht empfehlenswert).

Die Konfiguration des Routers ist je nach Hersteller und Internetanbieter unterschiedlich, lässt sich aber im Normalfall über die mitgelieferte Software von einem angeschlossenen Computer aus durchführen. Dabei gilt es immer drei Dinge zu erledigen:

- Einstellen der Verbindung zum Internetanbieter mit Zugangsdaten (bei Internetverbindungen über das Kabelnetz fällt diese Einstellung meist weg)

- Einstellen der WLAN-Funktionen
- Überprüfen/Konfigurieren der Sicherheitseinstellungen

Um den Nutzer bei diesen Aufgaben zu unterstützen, denken sich die Hersteller immer neue Assistenzprogramme und Methoden aus. Deshalb können hier nicht alle Möglichkeiten der Routerkonfiguration beschrieben werden. Stattdessen wird ein Weg vorgestellt, der – unabhängig vom verwendeten Modell und Internetanbieter – eigentlich immer funktioniert.

Alle Router können über ihr sogenanntes Webinterface bedient werden. Verbinden Sie dazu zunächst den Router über ein Kabel mit dem Computer (das Modem muss entsprechend der Anleitung in die Telefon- oder Kabeldose eingesteckt sein). Dann öffnen Sie auf dem angeschlossenen Computer den Browser und geben in die Adresszeile die Adresse des Routers ein. Diese lautet in der Regel 192.168.1.1, 192.168.2.1 oder 192.168.1.0. Genauere Angaben finden Sie in der Anleitung Ihres Geräts. Haben Sie die richtige Adresse aufgerufen, geben Sie die Zugangsdaten, die ebenfalls in der Anleitung angegeben sind, in Form von Benutzername und Passwort in die entsprechende Eingabemaske ein. Im Anschluss daran zeigt der Router sein Webinterface, in dem Sie alle notwendigen Einstellungen vornehmen können. Nutzen Sie dazu den Einrichtungsassistenten, sofern einer vorhanden ist. Als Allererstes aber sollten Sie das Passwort des Routers ändern, da es sich im Auslieferungszustand um ein Standardpasswort handelt, damit nur Sie als Administrator des Routers Zugriff haben.

Die Abbildung 32 zeigt beispielhaft das Webinterface eines Routers. Je nach Hersteller wird es kleine Unterschiede geben, aber die Grundfunktionen sind immer dieselben.

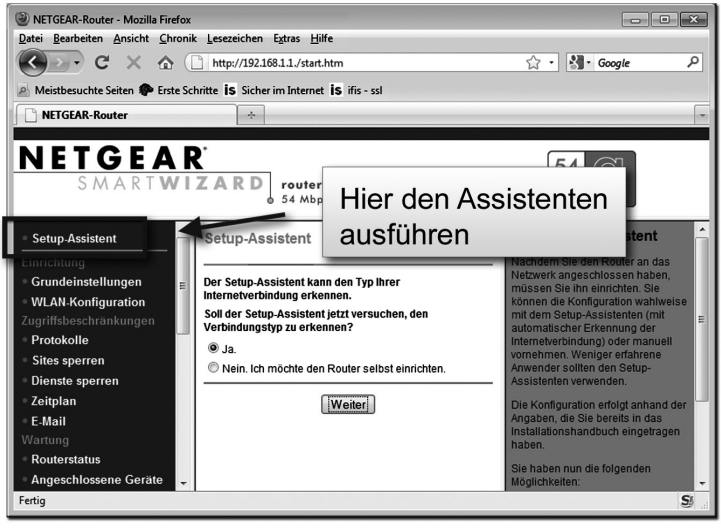

Abbildung 32: Webinterface eines Routers in der Übersicht

Ziehen Sie nun die Betriebsanleitung des jeweiligen Modells zurate, um alle notwendigen Einstellungen durchzuführen. Wichtig ist an dieser Stelle zu verstehen, zwischen welchen Geräten die jeweiligen Verbindungen aufgebaut werden. Das WLAN wird nur zwischen WLAN-Router und dem empfangenden Computer aufgebaut. Die Internetverbindung dagegen wird zwischen Router, Modem und Internetanbieter aufgebaut. Die häufigsten Fehler, die dabei passieren können, sind:

- Ein WLAN-Router kann erst eine Verbindung zum Internet aufbauen, wenn alle Geräte ordnungsgemäß verbunden sind und die Zugangsdaten des Internetanbieters korrekt in den Router beziehungsweise das Modem (bei Anschlüssen über Kabel) eingegeben wurden.
- WLAN funktioniert normalerweise nicht sofort, sondern muss erst konfiguriert werden. Dafür ist beim Einrichten

meist eine Kabelverbindung zwischen WLAN-Router und Computer notwendig. Es gibt allerdings auch WLAN-Router, die eine Funkverbindung mit einem dazugehörigen Empfänger (zum Beispiel USB-WLAN-Stick) per Knopfdruck einrichten können.

Ein grundsätzliches Vorgehen beim Router lautet – auch in Bezug auf die Sicherheit: Alles was nicht gebraucht wird, gehört ausgeschaltet. Deaktivieren Sie dementsprechend die WLAN-Funktion im Webinterface, wenn Sie diese nicht verwenden. Keine Sorge, sie lässt sich jederzeit wieder aktivieren. Auch der WLAN-Router selbst sollte ausgeschaltet werden, wenn er über längere Zeit nicht gebraucht wird. Das spart Strom, vermeidet Fehler und vermindert potenzielle Angriffsflächen.

Übrigens: Fast alle WLAN-Router verfügen über eine zusätzliche Sicherheitsfunktion, die immer angeschaltet sein sollte – eine Firewall.

Diese Firewall überprüft den Netzwerkverkehr zwischen dem Internet und dem Heimnetzwerk und achtet darauf, dass keine Ungereimtheiten auftreten, die auf einen Angriff schließen lassen. Standardangriffe von außen wehrt die Firewall im Router direkt ab. Sie ist damit eine prima Ergänzung zur Personal Firewall auf den Computern (siehe Seite 14 ff.), kann diese aber nicht ersetzen.

Im Regelfall wird Ihr Router noch weitere (Profi-)Einstellungen bieten, die aber für den Hausgebrauch im Allgemeinen bereits vorkonfiguriert sind. Diese Funktionen und Einstellungen sollten Sie nur verwenden beziehungsweise verändern, wenn Ihnen die Auswirkungen genau bekannt sind (Router konfigurieren, siehe Softlink 411).

TIPP: Routerkonfiguration

- Wenn Sie sich mit der Technik gar nicht auskennen, lassen Sie sich den Internetzugang vom Internetanbieter einrichten. Das kostet oft nur eine kleine Pauschale oder ist sogar im Angebot enthalten.
- Schalten Sie den WLAN-Router ab, wenn Sie ihn länger nicht benutzen. Das spart Strom und entzieht eventuellen Angreifern die Angriffsfläche.
- Deaktivieren Sie die WLAN-Funktion, wenn Sie sie nicht verwenden.
- Aktivieren Sie die Firewall des Routers (normalerweise ist das per Voreinstellung gegeben).
- Ändern Sie bei der Inbetriebnahme eines Routers das Zugangspasswort und bewahren Sie es sicher auf, am besten im Gedächtnis.

Die richtige WLAN-Verschlüsselung

Grundsätzlich lässt sich jede Funkverbindung für den normalen Gebrauch bedenkenlos einsetzen, wenn im Vorfeld die entsprechenden Sicherheitsvorkehrungen getroffen wurden. Das Wichtigste ist die Verschlüsselung der Daten, denn über das WLAN übertragene, unverschlüsselte Daten können von jedem, der sich in Reichweite des WLANs befindet, abgefangen werden – auch ohne große technische Kenntnisse. Heikel wird das vor allem dann, wenn es sich dabei um persönliche und sicherheitskritische Daten handelt. Für ein Firmennetzwerk gilt das natürlich erst recht.

Aktuell gibt es drei grundsätzliche Verschlüsselungsmethoden zur Absicherung des WLAN-Funkverkehrs: WEP (Wired Equivalent Privacy), WPA (Wi-Fi Protected Access) und

WPA2. Die WEP-Verschlüsselungsmethode ist bereits vor Jahren geknackt worden und nicht mehr sicher genug, da sie innerhalb von nur zwei Minuten mit einfachsten Mitteln entschlüsselt werden kann. Die darauf aufbauende WPA-Verschlüsselungsmethode ist noch nutzbar, aber nicht mehr zukunftsorientiert. Der Nachfolger WPA2 ist aktuell die sicherste Verschlüsselungsart und sollte Ihre erste Wahl bei der Verschlüsselung der WLAN-Verbindung sein.

TIPP: Die richtige WLAN-Verschlüsselungsmethode auswählen

- Sie müssen Ihr WLAN immer verschlüsseln.
- Verwenden Sie, wenn möglich, immer eine WPA2-Verschlüsselung.
- Nur wenn Sie Geräte betreiben, die WPA2 noch nicht unterstützen, sollten Sie WPA nutzen.
- Beobachten Sie die Nachrichten in den Medien oder die aktuellen Informationen im Internet, um zeitnah reagieren zu können, sollte die WPA-Methode geknackt werden.

Die WLAN-Verschlüsselung einstellen

Haben Sie sich für eine Verschlüsselungsmethode entschieden, müssen Sie die WLAN-Verschlüsselung entsprechend konfigurieren. Zuerst benötigt das WLAN einen Namen. Dieser wird SSID genannt. Die SSID (Service Set Identifier), auch Netzwerkname genannt, bezeichnet die Kennung eines Funknetzwerks. Diese sollte keine Rückschlüsse auf den Betreiber zulassen, wenn es sich um ein privates WLAN handelt, damit ein potenzieller Angreifer nicht schon anhand des Namens sein Ziel erkennen kann. Die SSID kann durch eine Einstellung im WLAN-Router auch verborgen werden, was

die Sicherheit zusätzlich erhöht. Doch zurück zur Verschlüsselung: Jeder, der eine verschlüsselte WLAN-Verbindung nutzen möchte, benötigt einen Schlüssel, um seine Nutzungsberechtigung nachzuweisen. Schließlich sollen ja nur bestimmte Personen, zum Beispiel Familienangehörige oder Freunde, die einen besuchen, das WLAN verwenden können.

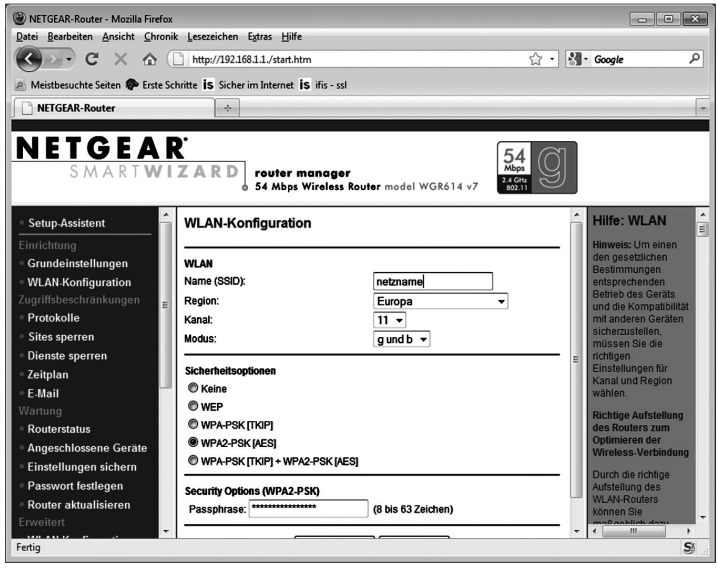

Abbildung 33: WLAN-Konfiguration des Routers – Sicherheitseinstellungen

Dazu stehen grundsätzlich zwei Verfahren zur Auswahl: PSK oder Radius. Radius ist ein Protokoll, das nur in Unternehmen genutzt wird, weshalb für Sie als Privatanwender nur der PSK infrage kommt. PSK steht für Pre-Shared Key. Dieser Schlüssel wird von demjenigen, der das WLAN konfiguriert, mithilfe einer sogenannten Passphrase erzeugt und an die Teilnehmer, die «Zutritt» zum WLAN erhalten sollen, weitergegeben. Die Passphrase besteht aus Buchstaben, Zahlen und

Sonderzeichen, die in das dafür vorgesehene Feld eingegeben werden (siehe Abbildung 33).

Soll nun ein Computer mit dem WLAN verbunden werden, fragt dieser nach der Passphrase. Zusätzlich kann bei der Konfiguration zwischen den Verschlüsselungsprotokollen TKIP (Temporal Key Integrity Protocol) und AES (Advanced Encryption Standard) gewählt werden. Das sind die Verschlüsselungsprotokolle, die in der jeweiligen Spezifikation festgelegt sind. Für WPA wird normalerweise das Protokoll TKIP und für WPA2 das Protokoll AES verwendet. In seltenen Fällen ist es auch möglich, WPA mit AES zu wählen.

Eine WLAN-Verschlüsselung einzurichten, ist mit den heutigen handelsüblichen Routern sehr einfach. Die Verschlüsselung findet zwischen einem sogenannten Access Point im Router und dem Computer statt. Bei neueren Computern, aber auch bei immer mehr Handys, ist WLAN bereits integriert. Ist dies bei Ihrem Computer nicht der Fall, benötigen Sie entweder eine WLAN-Karte oder even-

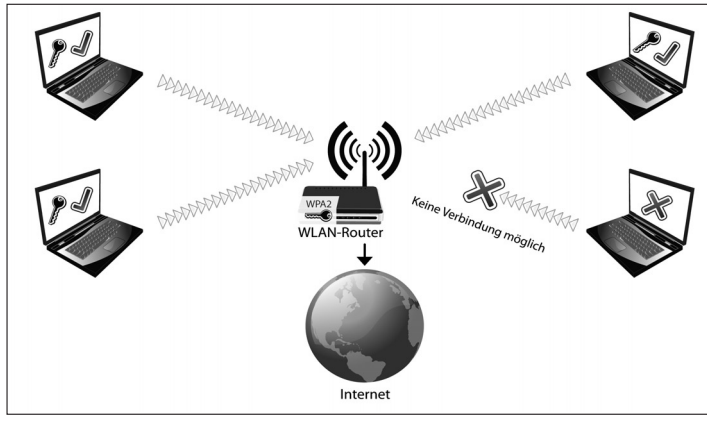

Abbildung 34: Aufbau eines WLANs mit Anbindung an das Internet über einen WLAN-Router

tuell einen WLAN-USB-Stick, um WLAN-Empfang zu erhalten.

Teilweise kann die Verschlüsselung auch ganz einfach per Knopfdruck vorgenommen werden. Der Schlüssel wird dann automatisch generiert. Grundsätzlich gilt: Wer die Passphrase (Schlüssel beziehungsweise Key) kennt, kann sich bei dem WLAN-Router anmelden. Daher muss die Passphrase wie ein Passwort aus großen und kleinen Buchstaben, Zahlen und Sonderzeichen bestehen und sollte mindestens 13 Stellen lang sein. Der Einsatz einer WPA2-Verschlüsselung mit der Passphrase «Sonne» bringt keinen Schutz, da die Passphrase sehr schnell durch automatisiertes Ausprobieren gefunden werden kann.

TIPP: Einstellen der WLAN-Verschlüsselung

- Nutzen Sie für WPA2 beziehungsweise WPA einen mehr als 13-stelligen Schlüssel mit Groß- und Kleinschreibung, Sonderzeichen und Zahlen.
- Verwahren Sie Ihren Schlüssel gut und geben Sie ihn nur an vertrauenswürdige Personen weiter, die Ihr Heimnetzwerk verwenden dürfen.

Verschlüsselung ist notwendig

«Aber wozu der ganze Aufwand?», werden Sie sich jetzt vielleicht fragen, schließlich haben Sie ja nichts zu verheimlichen. Doch auch, wenn es nichts zu verheimlichen gibt, bleibt die Tatsache bestehen, dass jeder x-beliebige Außenstehende ein unverschlüsseltes WLAN verwenden und im schlimmsten Fall für kriminelle Handlungen missbrauchen kann. Werden über das WLAN dann kinderpornographische Inhalte heruntergeladen oder Anleitungen zum Bombenbau ins Internet gestellt,

richtet sich die Fahndung zuerst gegen den Inhaber des WLANs. Der unbedarfte WLAN-Nutzer gerät so ins Fadenkreuz der Polizei. Auf die spannende rechtliche Seite der unterlassenen WLAN-Verschlüsselung geht das Kapitel «Ihre Rechte und Pflichten als Internetnutzer» (siehe Seite 162ff.) genauer ein.

TIPP: Unerlässlich: die Verschlüsselung
Auch wer nichts zu verheimlichen hat, muss seinen WLAN-Zugang schützen, um sicherzustellen, dass darüber keine kriminellen Handlungen erfolgen (siehe Seite 170ff.).

Zusätzliche Sicherheit durch den MAC-Adressenfilter

Ein zusätzlicher Schutz wird durch den MAC-Adressenfilter (MAC = Media Access Control) erreicht. Jedes Gerät, das eine WLAN-Funkverbindung aufbauen kann, hat eine eindeutige MAC-Adresse. Um andere daran zu hindern, sich in das eigene WLAN einzuklinken, kann im Router eine Liste der autorisierten MAC-Adressen eingerichtet werden, die Zugriff auf das WLAN bekommen sollen. Alle anderen WLAN-Geräte – mit MAC-Adressen, die nicht auf der Liste stehen – werden abgewiesen.

Um die MAC-Adressen der eigenen Geräte herauszufinden, sind verschiedene Wege denkbar. Der einfachste führt wieder über das Webinterface des Routers. Hier gibt es einen Menüpunkt «Angeschlossene Geräte», unter dem eine Liste mit allen aktuell verbundenen Geräten angezeigt wird. Nun sollten Sie alle Geräte, die eine Berechtigung erhalten sollen, mit dem WLAN verbinden, damit sie in der Liste auftauchen. Dann kopieren Sie die MAC-Adressen und fügen sie unter

dem Menüpunkt «Erweiterte WLAN-Konfiguration» in die Liste der «zugriffsberechtigten WLAN-Geräte» ein. Abschließend müssen Sie nur noch die Zugriffssteuerung unter dem gleichen Menüpunkt aktivieren. Danach haben nur noch die Geräte aus der Liste Zugriff auf das WLAN. Ein neues Gerät fügen Sie hinzu, indem Sie es ebenfalls in die Liste eintragen. Es gibt auch andere Möglichkeiten, die MAC-Adresse eines Geräts herauszufinden, und die Menüpunkte des Routers lauten je nach Router unterschiedlich. Weitere Informationen erhalten Sie im Workshop «MAC-Adressenfilter» unter Softlink 412.

TIPP: MAC-Adressenfilter

Nutzen Sie den MAC-Adressenfilter, um festzulegen, welche WLAN-Geräte Zugriff auf Ihr WLAN bekommen dürfen. Das erhöht die Sicherheit Ihres WLANs zusätzlich. Der MAC-Adressenfilter alleine bietet jedoch keinen ausreichenden Schutz.

Öffentliche WLANs (Hotspots)

WLAN in den eigenen vier Wänden macht Schluss mit Kabelchaos und schafft optimale Mobilität, aber so richtig interessant wird es erst unterwegs. Schnell am Bahnhof noch E-Mails abrufen oder gemütlich im Straßencafé surfen – das sind doch die echten Vorteile. Die WLANs an öffentlichen Plätzen werden als Hotspots bezeichnet. Sie werden zum Beispiel von der deutschen Telekom an Bahnhöfen und in einigen ICEs installiert und fallen unter deren Abrechnungssystem. Geschäfte oder Cafés stellen dagegen eine eigene Infrastruktur für den Zugang ins Internet zur Verfügung. Und bei beiden ist Vorsicht geboten, denn die Access Points werden

von Fremden betrieben und sind für jeden zugänglich. Nicht verschlüsselte Daten können «mitgeschnitten» werden, und selbst Angriffe auf verschlüsselte Daten sind theoretisch möglich, wenn ein Angreifer Zugriff auf den Access Point besitzt. Manche Angreifer stellen sogar extra eigene Access Points auf, die als «offizielle» Access Points getarnt sind.

TIPP: Vorsicht bei öffentlichen WLANs (Hotspots)
Geben Sie keine sicherheitskritischen Daten – zum Beispiel Ihre Kreditkartenummer – bei einer Internetanwendung ein, wenn Sie in einem öffentlichen WLAN surfen. Insbesondere Onlinebanking ist von öffentlichen WLANs aus tabu.

Bluetooth – der «Blauzahn»

Der für eine Technologie durchaus ungewöhnlich anmutende Name stammt von dem dänischen Wikingerkönig Harald Blauzahn, der im 10. Jahrhundert lebte und für seine Kommunikationsfähigkeit bekannt war. Und genauso kommunikativ gibt sich der heutige Blauzahn – vor allem bei kurzen Entfernungen (je nach Ausführung bis 100 Meter, wobei er eher für Entfernungen bis 10 Meter gedacht ist). Inzwischen kennt fast jeder die schnurlosen Bluetooth-Headsets für ein kabelfreies Telefonieren. Auch Handys lassen sich über Bluetooth mit dem Computer synchronisieren oder als Fernbedienung für elektronische Geräte verwenden.

Insgesamt gesehen ist Bluetooth eine prima Sache – solange Sie im Umgang damit einige Tipps beherzigen und die Hersteller bei der Umsetzung alles richtig machen. Denn es gab bereits einige Vorfälle, bei denen aufgrund falscher Imple-

mentierung, also einer fehlerhaften Umsetzung der Bluetooth-Spezifikation, Sicherheitslücken in Handys entstanden sind. Über die betroffenen Handys konnte mithilfe eines einfachen Angriffs eine SMS verschickt oder das Telefonbuch ausgelesen werden. Ist das schlimm? Wenn der Angreifer vor jede Nummer im Telefonbuch eine Mehrwertnummer (0900) für 3,50 Euro setzt und es wieder in das Handy hochlädt, schon.

Der richtige Umgang mit Bluetooth – So schützen Sie sich

Allerdings ist der Nutzer solchen Angriffen nicht hilflos ausgeliefert, weil es einfache Gegenmaßnahmen gibt. Bevor der Angreifer versuchen kann, ein Telefonbuch aus einem Handy herunterzuladen, muss er das Telefon technisch «sehen» können. Das bedeutet, er muss die eindeutige Kennung (MAC-Adresse) des Bluetoothgeräts herausbekommen. Zwar kann die Umgebung mit einem bluetoothfähigen Notebook oder Handy relativ einfach nach aktiven Bluetoothgeräten «gescannt» werden, fündig wird der Suchende aber nur, wenn sich das Bluetoothgerät im sogenannten Sichtbarkeitsmodus befindet. Diesen Modus benötigen Bluetoothgeräte jedoch ausschließlich, wenn sie sich das erste Mal verbinden (auch Pairing genannt), also beispielsweise das Handy mit dem Notebook oder das Handy mit dem Headset. In diesem Moment geben die Geräte der unmittelbaren Umgebung ihre eindeutige Kennung öffentlich preis, damit sie sich gegenseitig finden können. Werden Bluetoothgeräte zum ersten Mal verbunden (gepairt), wird zur Absicherung eine PIN ausgetauscht, die in beide Geräte eingegeben werden muss. Diese PIN kann bis zu 16 Stellen lang sein – und die sollten auch

genutzt werden. Denn es gilt: Je mehr Stellen, desto sicherer ist die Verbindung. Danach kann das Bluetoothgerät sofort zurück in den «Unsichtbarkeitsmodus» gestellt werden und ist damit nicht mehr für alle sichtbar. Waren zwei Geräte einmal verbunden, müssen sie für eine erneute Verbindung eigentlich nicht mehr gepairt werden; bei manchen günstigen Geräten kann das automatische erneute Verbinden allerdings manchmal Probleme bereiten.

Im Sichtbarkeitsmodus wird außerdem der Name des Bluetoothgeräts übertragen. Handys tragen als Namen im Allgemeinen ihre Typenbezeichnung, solange der Nutzer ihn nicht ändert. Ist Bluetooth «sichtbar» geschaltet, kann der Name ausgelesen werden, und der Angreifer sieht anhand der Typenbezeichnung sofort, ob ein Gerät dabei ist, das angreifbar ist. Das gilt natürlich genauso für Geräte, deren Name identisch mit dem Namen des Eigentümers ist. Der beste Name für ein Bluetoothgerät ist daher eine für einen Fremden völlig zusammenhangslose Zeichenfolge.

Wie bei allen Kommunikationstechnologien gilt auch hier das Credo: Schalten Sie Bluetooth vollständig ab, wenn Sie es nicht verwenden. Das spart obendrein Strom und verlängert somit die Akkulaufzeit.

TIPP: Der richtige Umgang mit Bluetooth

- Schalten Sie Bluetooth immer auf «unsichtbar». Nur für die erste Verbindung mit einem anderen Gerät muss das Bluetoothgerät «sichtbar» sein. Aktuelle Geräte schalten sich deshalb automatisch nach kurzer Zeit wieder auf «unsichtbar».
- Ändern Sie die voreingestellte Typenbezeichnung eines Bluetoothgeräts auf einen unscheinbaren, auf den ersten Blick nichtssagenden Namen – aber nicht auf den eigenen.

- Deaktivieren Sie die Bluetoothfunktion, wenn Sie diese nicht benutzen.

Das Bluetooth-Headset – Vorsicht Wanze

Ein wichtiges Gespräch mit dem Chef steht an, in dem Dinge besprochen werden, die nicht unbedingt für die Öffentlichkeit bestimmt sind. Natürlich wird das Handy in solchen Fällen ausgeschaltet. Wenn aber das Bluetooth-Headset neben dem Handy liegt und noch angeschaltet ist, wird es mit der Geheimhaltung eventuell schwierig. Das Headset findet «sein» Handy, mit dem es eine verschlüsselte Verbindung hatte, jetzt nicht mehr und verfällt in einen Modus, in dem es nach einem Gegenstück sucht. In diesem Moment ist es dem Angreifer möglich, sich mit dem Headset zu verbinden und es abzuhören, es also als Wanze zu benutzen. Sehr unschön bei einem geheimen Meeting. In diesem speziellen Fall, in dem es kein Tastenfeld an dem Gerät gibt, verwenden die Hersteller eine voreingestellte Standard-PIN der Art 0000, 1111 oder 1234. Der Angreifer muss lediglich diese Kombinationen ausprobieren und die Kennung (MAC-Adresse) des Headsets wissen, um sich zu verbinden. Die Hersteller könnten jedem Headset eine eigene PIN geben und vielleicht auf das Headset schreiben, aber diese Maßnahmen sind einerseits wohl zu teuer und andererseits ist der Nutzer zu bequem, um diese Absicherung zu nutzen. Der Schutz gegen den dargestellten Lauschangriff ist einfach:

TIPP: Bluetooth-Headsets

Schalten Sie Ihr Headset immer dann aus, wenn Sie auch Ihr Handy ausschalten. Solange das Handy oder ein Computer mit

dem Headset verbunden ist, kann ein Angreifer die Verbindung nicht abhören.

UMTS – State of the Art beim mobilen Internet

«Überall-Internet» ist die Parole für die Zukunft. Egal, wo sich ein Nutzer befindet, soll er Zugang zum Internet bekommen. Dafür extra eine Kabelverbindung oder ein WLAN zu suchen, ist unpraktisch. UMTS (Universal Mobile Telecommunications System) ist ein Mobilfunkstandard der dritten Generation (3G), der das Internet auf das Handy oder auch ins Wohnzimmer bringt. Im Grunde handelt es sich dabei um den Nachfolger von GSM, dem Standard, mit dem auch heute noch die meisten Handys funken.

Entscheidend bei UMTS ist die höhere Übertragungsrate und damit die Datengeschwindigkeit. Durch UMTS werden Geschwindigkeiten vergleichbar mit denen von DSL erreicht – aktuell bis zu 7,2 (10,2) Mbit/s. Die Datenübertragung von UMTS ist zwischen dem Handy und der Basisstation auf dem physikalischen Übertragungsweg gut verschlüsselt, weshalb die Nutzung von UMTS auch für sicherheitsrelevante Daten möglich ist. Natürlich muss auf der Anwendungsebene trotzdem eine SSL/TLS-Verschlüsselung (siehe Seite 36 ff.) verwendet werden, da die Daten nach der Basisstation im Klartext über das Kommunikationsnetz und ins Internet übertragen werden.

UMTS findet nicht nur in Handys Anwendung, sondern oft auch in Notebooks. Für den UMTS-Empfang wird eine SIM-Karte – wie sie auch für Mobiltelefone üblich ist – von einem Mobilfunkanbieter benötigt, der diesen Standard be-

reitstellt. Die Angebote reichen dabei von Zeit- und Volumentarifen bis hin zu Flatrates.

TIPP: UMTS und Sicherheit

UMTS ist mit einer guten Verschlüsselung ausgestattet. Es kann daher auch für sicherheitskritische Vorgänge wie Einkäufe im Internet verwendet werden. Natürlich muss auf Anwenderebene weiterhin eine SSL/TLS-Verschlüsselung verwendet werden (siehe Seite 36ff.).

Freuen Sie sich auf Teil 7:
Ihre Rechte und Pflichten als Internetnutzer – der aktuelle Stand

Ab 18.02.2013 zum kostenlosen Download auf
www.internet-sicherheit.de