WLAN für Einsteiger

Bildqualität

Wir versuchen die Dateigröße zu reduzieren, um die Downloadzeit zu verkürzen. Daher ist die Bildqualität in dieser Download-Datei nicht in allen Fällen optimal. Im Druck tritt dieses Problem nicht auf.

Acrobat Reader: Wie komme ich klar?

F5/F6 öffnet/schließt die Ansicht **Lesezeichen**
Strg+F sucht

Im Menü Ansicht stellst du ein, wie die Datei angezeigt wird
STRG+0 = Ganze Seite **STRG+1** = Originalgröße **STRG+2** = Fensterbreite

Im selben Menü kannst du folgendes einstellen: **Einzelne Seite**, **Fortlaufend** oder **Fortlaufend - Doppelseiten** ... Probiere es aus, um die Unterschiede zu sehen.

Navigation
Pfeil Links/Rechts: eine Seite vor/zurück
Alt+ Pfeil Links/Rechts: Wie im Browser: Vorwärts/Zurück
Strg+**+** vergrößert und **Strg**+**–** verkleinert

Bestellung und Vertrieb für den Buchhandel

KnowWare-Vertrieb, Postfach 3920, D-49029 Osnabrück
Tel.: +49 (0)541 33145-20 Fax: +49 (0)541 33145-33
bestellung@knowware.de
www.knowware.de

Autoren gesucht

Der KnowWare-Verlag sucht ständig neue Autoren. Hast du ein Thema, dass dir unter den Fingern brennt? - ein Thema, das du anderen Leuten leicht verständlich erklären kannst?

Schicke uns einfach ein paar Beispielseiten und ein vorläufiges Inhaltsverzeichnis an folgende Adresse:

lektorat@knowware.de

Wir werden uns deinen Vorschlag ansehen und dir so schnell wie möglich eine Antwort senden.

www.knowware.de

Inhaltsverzeichnis

Herzlich Willkommen

… in der Wireless-LAN-Welt. Lass dich anstecken von Werbespots, wo Laptopbesitzer an den verschiedensten Orten dem kabellosen Surfspaß frönen. Es muss ja nicht unbedingt ein Basiscamp im Himalaya sein – aber surfen in deinem Lieblingscafe oder im Park wäre schon eine angenehme Alternative zum eintönigen Office. Und WLAN macht es möglich.

W steht für „Wireless“ – drahtlos – und **LAN** für „Local Area Network“. Gemeint ist ein lokales Netzwerk, in dem mehrere Computer miteinander kommunizieren ohne das sie verdrahtet sind. Die Technologie dazu ist ausgereift. Moderne Laptops werden mit der Intel Centrino-Mobiltechnologie ausgeliefert bzw. sind mit einer Wireless LAN Karte bestückt.

Besitzt du einen Laptop ohne WLAN-Technologie, ist das kein Problem. Mit einem Adapter in der Form einer Zusatzkarte lässt sich dein Laptop aufrüsten. Was dabei zu beachten ist, erfährst du gleich am Anfang des Heftes.

Ist der Computer dann mit der Wireless-Technologie bestückt und auch sicherheitstechnisch auf dem neuesten Stand, bist du für die drahtlose Kommunikation gerüstet.

Halt – so einfach ist das nicht. Du benötigst Kommunikationspartner – also ein Netzwerk.

Zunächst machen wir uns auf die Pirsch nach einem öffentlichen drahtlosen Internet-Zugang, auch als *Hotspot* bezeichnet. Ihre Zahl erhöht sich rasant. Gaststätten, Hotels, öffentliche Plätze, Flughäfen und auch Tankstellen werden zunehmend mit Hotspots ausgestattet.

Vernetzen möchtest du dich auch zu Hause, den ganzen Kabelsalat hast du satt, auch Löcher bohren und Kabel verlegen ist nicht dein Ding?

Kein Problem – wir bauen mit dir dein eigenes WLAN–Netz auf, rüsten deine Computer nach – und schon besitzt du ein *drahtloses Ad-hoc-Netzwerk*.

Bist du an höherer Sicherheit interessiert, lass die Funkverbindungen über eine zentrale Basisstation, einen *AccessPoint*, laufen. Sie wird zur Schaltzentrale in deinem nun entstandenen *Infrastrukturnetzwerk*.

Die Wünsche wachsen mit den Möglichkeiten. Deine Familie möchte gleichzeitig und über verschiedene Computer ins Internet - aus Kostengründen natürlich über einen zentralen Zugang? Überprüfe, ob dein Provider dieses gestattet. Technisch ist das kein Problem. In diesem Fall soll deine Basisstation eine Verbindung zum Internet gestatten.

Du benötigst einen *AccessRouter*.

Erwartest du hier eine theoretisch-abstrakte Abhandlung, müssen wir dich leider enttäuschen.

Wir wollen dir die WLAN-Welt praktisch nahe bringen, ohne nennenswerte Vorkenntnisse zu fordern. Wie schon gesagt, wir werden

- deinen Laptop mobil machen,
- gemeinsam Hotspots und deren Anbieter aufsuchen, um an öffentlichen Plätzen im Internet zu surfen,
- dir für jedermann beziehbare Hardwarekomponenten vorstellen und
- sinnvolle Tools nutzen, die du als Freeware beziehen kannst.

Keine Sorge, auch das Thema der Computersicherheit wird nicht zu kurz kommen, egal ob du alleine mit deinem Laptop in der Öffentlichkeit unterwegs bist, mit anderen in einem Ad-hoc-Netzwerk arbeitest oder ein Infrastrukturnetzwerk analysierst und schützen willst.

Du hattest bisher noch nichts mit Netzwerken zu tun? Das ist nicht schlimm. In den Kapiteln zu Netzwerken und Protokollen erhältst du grundlegendes Wissen, das dir den Umgang mit dem WLAN und den damit verbundenen Konfigurationen erleichtert.

Auch für dieses Heft haben wir eine Serviceseite erstellt – du findest sie hier: www.bilke.de/wlan.

Und nun viel Spaß beim Aufbau und bei der Pflege deines WLANs wünschen dir

- Petra Bilke
- Steffen Bilke

Drahtlose Netzwerke

Computer brauchen keine Kabel mehr zur Vernetzung. Drahtlos ist in diesem Zusammenhang das Stichwort. Das erspart das lästige Strippenziehen. Mittlerweile gibt es verschiedene Funktechniken, die eine drahtlose Übertragung erlauben.

Wireless-LAN

Mit dieser Technologie werden wir uns intensiv in diesem Heft beschäftigen. Ein LAN verbindet Computer in einem begrenzten Gebiet miteinander. Bei einem Wireless LAN werden die Daten per Funk übertragen. WLAN bietet umfangreiche Vorteile.

- Es müssen fast keine Kabel verlegt werden.
- Mit einem Notebook hast du als Benutzer eine hohe Bewegungsfreiheit.

Verschiedenste WLAN-Einsatzfälle sind denkbar:

- Du willst deinen Laptop an wechselnden Orten einsetzen: am Schreibtisch, im Beratungsraum, im Labor oder beim Kunden.
- Bautechnische Gegebenheiten, wie Denkmalschutz, Asbestprobleme oder Brandschutz, erschweren den Einbau von herkömmlichen Kabeln mit ihren Kanälen.
- Bei Umbauten und Ausfällen ist der Ersatz des Festnetzes durch WLAN eine sinnvolle Lösung.
- Kurzzeitige Nutzungsfälle, wie Messen und Konferenzen, lassen eine feste, dauerhafte Verkabelung nicht sinnvoll erscheinen.
- Netzwerke für Veranstaltungen, in Schulen oder bei Ausstellungen haben meist eine wechselnde Zahl von temporären Zugängen – sie gewinnen ihre notwendige Flexibilität durch drahtlose Lösungen.
- Für öffentliche Internetzugänge an Flughäfen, Hotels, Gaststätten oder in Stadtzentren bietet sich WLAN besonders an.
- Im häuslich-privaten Bereich kann auch die „Nachbarschaft“ versorgt werden.

Eine Zusammenstellung der Vor- und Nachteile von WLANs im Vergleich zu herkömmlichen Netzwerken siehst du in nachfolgender Tabelle.

<table>
<tr><th></th><th colspan="2">WLAN</th><th>Herkömmliches Netzwerk</th></tr>
<tr><td>Verkabelung</td><td colspan="2">Aufbau von Netzwerken an Orten, wo keine Kabel verlegt werden dürfen.</td><td>Verkabelung ist oft schon vorhanden.</td></tr>
<tr><td>Flexibilität</td><td colspan="2">Hohe Bewegungsfreiheit und Flexibilität</td><td>Feste Anschlüsse und geringe Bewegungsfreiheit</td></tr>
<tr><td rowspan="5">Übertragung</td><td colspan="2">Übertragungsraten werden durch Bausubstanz stark gedämpft.</td><td rowspan="5">Höhere Übertragungsgeschwindigkeiten sind gegeben.</td></tr>
<tr><td>Dämpfung</td><td>Substanz</td></tr>
<tr><td>gering</td><td>Holz, Gips, Pappe, Glas</td></tr>
<tr><td>mittel</td><td>Wasser, Mauersteine, Geschoßdecken</td></tr>
<tr><td>hoch</td><td>Massive Wände, Beton-, Stahlbetonwände, Sicherheitsglas, massives Metall</td></tr>
<tr><td>Stabilität</td><td colspan="2">Funkstörungsbedingte Stabilitätsschwankungen sind möglich.</td><td>Höchstmögliche Stabilität kann gewährleistet werden.</td></tr>
<tr><td>Sicherheit</td><td colspan="2">Jeder kann Daten eines Funknetzwerkes empfangen, wenn er sich in seiner Reichweite befindet.</td><td>Höhere Sicherheit liegt vor.</td></tr>
</table>

Industrie-Standards

Aufgepasst – jetzt wird es technisch!

Für ein WLAN gilt die Funk-LAN Spezifikation IEEE 802.11, die den Industriestandard für drahtlose Netzwerkkommunikation definiert und die das Institute of Electrical and Electronics Engineers (IEEE) herausgegeben hat.

Die erste Version des Standards wurde 1997 verabschiedet. In den folgenden Jahren wurde dieser Standard weiter entwickelt.

Auf Seite 58 findest du eine Zusammenfassung aller IEEE 802.11-Standards.

Im Zusammenhang mit der Hardware sind folgende Standards von Interesse – und auch hier stellen wir Vor- und Nachteile sowie Einsatzgebiete einander gegenüber.

	IEEE 802.11a	IEEE 802.11b	IEEE 802.11g	IEEE 802.11 a/g
Max. Datentransferrate (Mbit/s)	54	11 22 bei IEEE 802.11b+	54 108 bei IEEE 802.11g+	54
		Verdoppelung der Transferrate		
Frequenz (GHz)	5	2,4	2,4	2,4 und 5
Kompatibilität		zu 802.11g	zu 802.11b	zu 802.11a, b, g
Nicht überlappende Kanäle	8	3	3	8 bzw. 3
Reichweite in einer typischen Büroumgebung	ca. 20m	ca. 25m	ca. 25m	entspricht dem jeweiligen Standard
Vorteile	Frei von Störungen durch 2,4 GHz-Geräten wie z.B. Mikrowellen, 8 nicht überlappende Kanäle sind verfügbar.	Viele Hotspots in Hotels, Flughäfen usw. sind mit dieser Technik ausgestattet. Die geringsten Kosten im Vergleich aller Wireless-Standards.	Höherer Datentransfer ist möglich. Kosten sind nur unwesentlich höher als bei 802.11b-Geräten.	Durch Abdeckung aller aufgeführten Standards lassen sich die Geräte in jedes 802.11 Wireless-Netzwerk integrieren.
Nachteile	Geringere Reichweiten und höhere Investitionskosten als 802.11b/g. In Deutschland bestehen Einschränkungen bezüglich der Sendeleistung. Von den zwei Frequenzbereichen kann nur der Bereich 5,15 bis 5,25 GHz mit weniger als der halben Sendeleistung genutzt werden.	Mit 11 Mbit/s liegen die niedrigsten Datentransferraten vor.	Durch stark zunehmende Nutzung des 2,4 GHz-Bandes kann es zu Interferenz-Störungen kommen.	Die Kosten sind höher als bei vergleichbaren 803.11g-Produkten.
		Nur 3 nicht überlappende Kanäle sind verfügbar.		
Empfohlenes Einsatzgebiet	In Umgebungen, wo Interferenzstörungen vermieden werden sollen. In kritischen Einsatzorten wie z.B. Krankenhäusern.	In Umgebungen, wo Benutzer mit möglichst geringen Investitionskosten mobil angebunden werden sollen.	Für alle Einsatzgebiete und Anwendungen mit hoher Datentransferleistung.	Mit diesen Geräten kann man sicherstellen, dass mobile Benutzer unabhängig von dem verwendeten Standard überall auf Netzwerke zugreifen können.
		In Deutschland kommen in erster Linie Geräte dieser Standards zum Einsatz.		
ISM-Frequenzbereich		Diese Standards arbeiten auf dem 2,4 GHz-Band. Es liegt im so genannten ISM-Frequenzbereich. ISM steht für Industrial Scientific und Medicine. Diese Frequenzen können lizenzfrei von der Industrie, der Wissenschaft und der Medizin genutzt werden. In diesem Frequenzband, beginnend bei 2412 MHz, stehen in Europa 13 Kanäle mit einem Frequenzabstand von 5 MHz zur Verfügung. Bei einer Kanalbreite von ca. 22 MHz können jedoch nur 3 Kanäle gleichzeitig überlappungsfrei genutzt werden.		

Weitere Funktechniken

Neben WLAN gibt es weitere Funktechniken. Beispielhaft seien hier die folgenden genannt:

- DECT
- HomeRF / SWAP
- Bluetooth
- Infrarot
- UMTS

Sehen wir uns diese Techniken kurz an.

DECT

DECT ist dir vermutlich im Zusammenhang mit schnurlosen Telefonen ein Begriff.

Die Abkürzung steht für Digital Enhanced Cordless Telecommunications. Übersetzen lässt sich das mit „digitale, verbesserte, schnurlose Telekommunikation“. Bei diesem Verfahren werden die Telefongespräche per Funk an eine Basisstation übertragen, die ans Telefonnetz angeschlossen ist.

Aber auch Computer lassen sich vernetzen. Mit der COM-ON-AIR Basisstation von Dorsch und Amand (www.dasystems.de) kannst du bis zu zwölf einzelne Computerarbeitsplätze schnurlos verkabeln. Die COM-ON-AIR Basisstation wird einfach an ein vorhandenes ISDN- bzw. die DSL-Kabelmodem angeschlossen – und versorgt dann das ganze Haus und den Garten mit einem abhörsicheren ISDN-Komfortdienst für DECT-Telefone. Den Drucker kannst du ohne zusätzlichen Konfigurationsaufwand direkt an die Basisstation anschließen, worauf er dann jedem Computer mit COM-ON-AIR-Netzwerkkarte zur Verfügung steht. Damit stehen Datendienste wie Internet, E-Mail, Fax, Filetransfer und Drucken schnurlos zur Verfügung.

HomeRF/SWAP

Die „HomeRF Working Group“ vereinigte 1999 die Standards DECT und IEEE802.11 zu einem neuen System, dem *Shared Wireless Access Protocol* (SWAP) – mit dem Ziel, eine perfekte Wireless-Lösung für den Endverbraucher zu schaffen. Und auf dem Papier ist HomeRF ein hervorragendes System.

DECT ist eine Protokollkomponente von SWAP. Sprachdienste sind somit kein Problem. Auch paketorientierte Datenvermittlung beherrscht der neue Standard.

Ein nützliches Feature von HomeRF ist die Unterstützung von QoS (Quality of Service). Damit kann gezielt für eine bestimmte Paket-Datenübertragung Bandbreite reserviert werden; das Streaming von Audio- oder Video-Inhalten ist also kein Problem mehr.

Die reine Datenrate beträgt bei der älteren Version von HomeRF 1.x 2 MBit/s, der neue Standard HomeRF 2.0 lässt bis zu 10 MBit/s zu. In beiden Fällen kann unter ungünstigen Bedingungen auf geringere Raten zurückgeschaltet werden.

Theoretisch müsste HomeRF eigentlich allen anderen Verfahren den Rang ablaufen – da die Marktmacht hier aber zu ungunsten von HomeRF steht, ist es in der Praxis wenig verfügbar.

Bluetooth

... ist ein offener Industriestandard (IEEE 802.15.1-2002 www.ieee802.org/15/pub/TG1.html) für ein lizenzfreies Nahbereichsfunkverfahren zur kabellosen Sprach- und Datenkommunikation zwischen IT-Geräten.

Die Entwicklung von Bluetooth geht auf eine Initiative der so genannten Bluetooth Special Interest Group (www.bluetooth.org) im Jahre 1998 zurück, der heute über 2.500 Hersteller angehören.

Die Bluetooth-Technik basiert auf einer kostengünstigen Nahbereich-Funkverbindung und kann unterschiedlichste digitale Geräte kabellos miteinander verbinden – sogar ohne Sichtkontakt.

Soll eine Verbindung aufgebaut werden, müssen sich zwei Bluetoothfähige Geräte lediglich bis auf etwa 10 Meter nähern.

Schon heute werden Mobiltelefone, PCs und Laptops mit dieser Technik ausgeliefert.

Infrarot

Die Infrarot-Technik ist von Geräten unterschiedlichster Art bekannt. Die Datenübertragung mit dieser Technik wird in den verschiedensten Geräten benutzt – von Fernbedienungen über Taschenrechner, PDAs, Mobiltelefone, Drucker und Notebooks bis hin zum Desktop-System.

Bereits 1994 verabschiedete die Infrared Data Association einen Standard zur Spezifizierung der Infrarot-Schnittstelle als Alternative zum seriellen Port. Die damals auf 9600 bit/s festgeschriebene Datenrate war natürlich nicht gerade üppig. Doch schon die zweite Version des als Serial Infrared (SIR) beschriebenen Standards erlaubt Transferraten von bis zu 4 Mbit/s. Die heute gebräuchlichste Geschwindigkeit bei Infrarot-Übertragungen liegt bei 115,2 kbit/s. Als maximale Reichweite dieses Standards wird 1 Meter angegeben; es existieren aber durchaus Lösungen auf dem Markt, die längere Strecken überbrücken.

Für eine erfolgreiche Kommunikation müssen sich die Partner in direkter Sichtlinie befinden; und eben das ist der größte Nachteil der Infrarot-Technik. Die geringe Reichweite verhindert den effektiven Datenaustausch zwischen mehreren Kommunikationspartnern.

UMTS

UMTS wurde im Zusammenhang mit den UMTS-Lizenzen bekannt, die im Sommer 2000 für Milliardenbeträge verkauft wurden.

Die Abkürzung steht für „Universal Mobile Telecommunications System“. Dieses System bezeichnet den Mobilfunk einer neuen Generation. Bei Datenübertragungsraten von zwei Megabit pro Sekunde sollen sich Fotos, Straßenkarten und sogar Filme auf dein Handy übertragen lassen.

> Mit dem heutigen Mobilfunkstandard GSM können Daten mit 9,6 KBit pro Sekunde übertragen werden. UMTS ist also mehr als 200-mal schneller als GSM.

Bis zur Verfügbarkeit dürften allerdings noch einige Jahre ins Land gehen – für UMTS muss ein komplett neues Funknetz mit kleineren Zellen und neuer Hardware errichtet werden.

Zwei Eckdaten hat die Regulierungsbehörde für Telekommunikation und Post jedoch eindeutig gesetzt:

Bis Ende 2003 muss ein Versorgungsgrad von 25 Prozent in der Bevölkerung erreicht sein, bis Ende 2005 sogar 50 Prozent. Andernfalls verfällt die Lizenz.

In letzter Zeit werden immer wieder Stimmen laut, dass WLAN-Netze dem UMTS ernsthaft Konkurrenz machen könnten.

Schaden Funkwellen der Gesundheit?

Das ist ein Thema, das die Gemüter in Deutschland seit der Einführung der Mobilfunknetze erhitzt. Viele Leute diskutieren seit langem, ob Funkwellen die Gesundheit des Menschen beeinträchtigen können. Es lässt sich tatsächlich nicht abstreiten, dass es Menschen gibt, die in der Nähe von Funkmasten sensibel reagieren.

Schauen wir uns Parameter verschiedener Funkenwellenerzeuger an.

- Fernsehsender haben eine abgestrahlte Sendeleistung von maximal 500 000 Watt in einem Frequenzbereich zwischen 50 und 850 MHz.
- Radiosender haben eine abgestrahlte Sendeleistung von maximal 10 000 Watt in einem Frequenzbereich zwischen 88 und 108 MHz.
- Mobilfunksender erzeugen Signale mit einer Leistung von 5 bis 40 Watt auf folgenden Frequenzen:
  - D-Netz: 890-915 MHz
  - E-Netz: 1710-1880 MHz
  - UMTS: 1920-2170 MHz

Die Sendeleistung von WLAN-Geräten dagegen ist weitaus geringer – im Allgemeinen bieten die Bauteile dieser Technik eine Sendeleistung von

maximal 100 mW. Einige Hersteller konnten die Leistung sogar auf 35 mW senken.

Die in unserem Heft vorgestellten Geräte haben laut Herstellerangaben eine Sendeleistung zwischen 50 und 100 mW. Diese Strahlung wird nach bisherigen wissenschaftlichen Studien als harmlos und nicht gesundheitsgefährdend eingestuft. Unter folgender Internetadresse findest du ein entsprechendes Gutachten: www.dmn.tzi.org/wlan/wlan-emvu-gutachten-bremen.pdf.

Während du dieses Heft liest, liegt ganz in deiner Nähe vermutlich so ein vibrierendes Teil namens *Handy* herum – z.B. ein gebräuchliches Mobilfunktelefon wie das Nokia 6090. Dieses Handy hat eine Sendeleistung von 8 Watt. Der durchschnittliche Wert der Sendeleistung liegt bei vielen Handys um 5 Watt.

Funk-LAN-Systeme haben also eine weit niedrigere Leistung als ein Handy.

Und noch ein Beispiel: Die meisten Haushalte verfügen über einen Mikrowellenherd. So ein Herd sendet mit mehreren 100, manchmal sogar mit 1000 Watt, damit dein Essen schön warm wird. Natürlich sind diese Herde entsprechend abgeschirmt – dennoch tritt ein gewisses Maß an Strahlung aus.

Mikrowellen senden auf dem gleichen Frequenzband wie WLAN-Geräte; also können sie ein Netzwerkstörfaktor sein.

Zur Beruhigung: Amerikanische und europäische Studien haben nachgewiesen, dass erst bei stark erhöhten Strahlungsmengen Auswirkungen auf Menschen feststellbar sind – und selbst dann nur in geringem Maße. Die Spezialisten stellten in ihren Laboren fest, dass es keinerlei Bedenken gegenüber Funk-LAN-Komponenten gibt. Außerdem stellten sie auch fest, dass Fehlfunktionen von Herzschrittmachern und anderen medizinischen Geräten nicht zu befürchten sind. WLANs kommen deswegen auch in Krankenhäusern und Kliniken zum Einsatz – und haben hier ihre Tauglichkeit in sensiblen Umgebungen unter Beweis gestellt.

Übrigens: Viele Hersteller von Funk-LAN-Bauteilen lassen ihre Geräte zertifizieren, um die Zulassung der europäischen Norm für medizinische Geräte (EN60601/1/2) zu erlangen.

Computer für den mobilen Einsatz

Centrino™ Mobiltechnologie – Wireless-LAN-Adapter

In diesem Kapitel wollen wir deinen Laptop für den mobilen Einsatz fit machen. Erste Voraussetzung ist da natürlich der Besitz eines Laptops. Hast du ein Gerät auf Basis der Intel Centrino-Mobiltechnologie, sind die hardwaremäßigen Voraussetzungen erfüllt.

Dank der integrierten Wireless-LAN-Funktion kannst du eine Verbindung ins Internet oder mit einem Unternehmensnetzwerk ohne Kabel oder die Erweiterung durch einen Adapter herstellen.

Aber auch Laptops mit anderen Prozessoren werden mit integrierter Wireless LAN-Anbindung ausgeliefert. Entsprechende Geräte werden so oder ähnlich beworben:

Technische Daten	
Besonderheiten	superschnelles Wireless LAN 802.11g mit 54 Mbit/s integriert: sofort ohne Zusatzhardware in ein vorhandenes kabelloses Netzwerk einsteigen, abwärtskompatibel zu 802.11b (11 Mbit/s)

Dein Laptop verfügt von Haus nicht über einen WLAN-Anschluss? Auch kein Problem – lege dir einen Wireless-LAN-Adapter zu. Anbieter, das zeigt die nebenstehende Herstellerliste, gibt es viele.

Die Liste erhebt natürlich keinen Anspruch auf Vollständigkeit – sie soll dir nur zur ersten Orientierung dienen.

Zur Auswahl stehen Wireless-LAN-Adapter, die kompatibel zu IEEE 802.11b/IEEE 802.11b+ sind, wie auch Adapter mit der Kompatibilität zu IEEE 802.11g/IEEE 802.11g+. Die letzteren bieten nur wenige Hersteller an; sie haben aber den Vorteil, dass sie die Datenrate des jeweiligen Standards verdoppeln.

Am preiswertesten sind IEEE 802.11b-Karten. Sie unterstützen Datenübertragungsraten von 11, 5,5, 2 und 1 MBit/Sek. Für den Zugang zum Internet reicht das allemal.

Hersteller bzw. Anbieter	Internet
Acer	www.acer.de
Avistron	www.avistron.de
Belkin	www.belkin.de
Cisco	www.cisco.com/global/DE/home.shtml
D-Link	www.dlink.de
DELL	www.dell.de
Digitus	www.digitus.de
Edimax	www.edimax.com.tw
Fiberline	www.fiberlineeurope.de
Gericom	www.gericom.com
Intel	www.intel.com/deutsch
LANCOM	www.lancom-systems.de
Level One	www.level-one.de
Netgear	www.netgear.de
Orinoco	www.orinocowireless.com
Sagem	www.sagem.de
SMC	www.smc.de
TARGA	www.targa.de
pearl	www.pearl.de

Willst du so eine Karte auch in deinem privaten Netzwerk einsetzen, lohnt sich eine 54Mbps-Karte nach den Standard IEEE 802.11g. Karten dieses Typs sind mittlerweile nicht mehr wesentlich teuerer als Karten nach IEEE 802.11b – und da sie abwärtskompatibel sind, unterstützen sie diesen Standard.

Die Datenübertragungsraten gehen hier also dynamisch von höchstens 54 MBit/Sek. nach IEEE 802.11g bis mindestens 1 MBit/Sek. nach IEEE 802.11b.

Sehen wir uns jetzt als Beispiel für eine solche Karte die „freeControl Wireless LAN 54Mbps PCMCIA Cardbus-Card“ an.

Du findest sie bei Pearl unter www.pearl.de

Zurzeit werden 49,90 Euro verlangt. Im Doppelpack wird die Karte noch preiswerter. Und so wirbt die Firma für ihre Karte:

Produktbeschreibung:

- 32-Bit PC Card Bus, PCMCIA Typ II
- Reichweite: bis zu 50 m im Gebäude, bis zu 150 m im Freien
- Volle Kompatibilität mit WireLess-LAN-Adapter (2,4 GHz)
- Datenübertragungsrate: 54/48/36/24/18/12/11/9/6 MBit/Sek. (IEEE 802.11g), 5,5/2/1 MBit/Sek. (IEEE 802.11b), dynamische Anpassung
- Länderspezifische WLAN-Einstellungen
- Software-unterstütztes Profilmanagement
- WiFi-zertifiziert
- Unterstützt 64-/128-/152-Bit-Datenverschlüsselung: TKIP, AES, 152-WEP
- Unterstützt Ad-Hoc- und Infrastructure-Modus
- LED-Anzeige für Link Activity
- Kompatibel zu Windows 98/ME/2000/XP

Da IEEE 802.11b und IEEE 802.11g zum Glück weltweit anerkannte Standards sind, ist es kein Problem, WLAN-Hardwareprodukte verschiedener Hersteller in ein und demselben WLAN zu benutzen.

Treiber und Konfigurationen

Die meisten Hersteller unterstützen unmittelbar Computer mit einem Windows-Betriebssystem, d.h. sie liefern ihre WLAN-Hardware mit Windowstreibern aus. Treiber sind Programme, mit deren Hilfe das Betriebssystem seine Kommandos an Peripheriegeräte gibt und Meldungen von ihnen erhält.

Apple-User mit dem neuesten Betriebssystem Mac OS X haben unter Umständen Glück – die Airport-Software, die normalerweise automatisch installiert wird, unterstützt den IEEE 802/11g-Standard (54MBit), also lassen sich z.B. Karten mit einem Broadcom-Chip unmittelbar einsetzen. Linux-Computer werden treibermäßig seltener unterstützt.

Warum Windows XP?

Die Beispiele im unserem Heft basieren auf Windows XP. Du fragst dich warum? Die Antwort: Fast jeder neue Computer wird mit Windows XP (Home oder Professional) ausgeliefert. Die Versionen Home und Professional unterscheiden sich nicht wesentlich voneinander.

Die Professional-Version beinhaltet erweiterte Funktionen für die Administration und Verwaltung von Computern und größeren Netzwerken. Für unsere Zwecke reicht die Home-Version vollkommen aus. Außerdem wird Windows XP herstellerübergreifend am besten mit aktuellen Treibern versorgt.

Das Betriebssystem ist stabil und einfach zu bedienen. Aktuelle Techniken, wie eben WLAN, werden in diesem System von Haus aus unterstützt.

Das heißt nun aber nicht, dass du deinen Rechner auf Windows XP umrüsten müsstest – WLAN läuft auch mit älteren Windows-Versionen ab 98. Nur sehen die Menüs geringfügig anders aus.

Installation der WLAN-Netzwerkkarte

Die Installation der WLAN-Netzwerkkarte ist nicht schwer und schnell erledigt.

Du musst berechtigt sein, neue Geräte zu installieren!

Beim eigenen Computer verfügst du vermutlich über Administrationsrechte. Benutzt du einen Firmencomputer, können die Benutzerrechte eingeschränkt sein. Setze dich in diesem Fall mit dem verantwortlichen Administrator in Verbindung.

Sehen wir uns am Beispiel von Windows XP an, wie du die „freeControl Wireless LAN 54Mbps PCMCIA Cardbus-Card“ in einem Laptop Computer installierst.

1. Schalte deinen Laptop ein und warte bis das Betriebssystem gestartet ist.
2. Lege die mitgelieferte CD ein.
3. Starte die Datei `setup.exe`, um den Treiber zu installieren.
4. Im Handbuch steht, dass der Computer danach neu zu starten ist. Den Schritt habe ich ausgelassen.
5. Anschließend steckst du die Karte in einen freien PCMCIA-Slot. Beachte, dass das Etikett nach oben zeigen muss.
6. Es meldet sich der Assistent für neu gefundene Hardware, und das Konfigurationsmenü der Wireless-LAN-Karte öffnet sich.

7. Bestätige, dass du die Software automatisch installieren möchtest.
8. Obwohl der Kompatibilitätstest von Windows nicht bestanden wurde und nachfolgendes Fenster erscheint, setzt du die Installation fort ...

9. … und schon hast du es geschafft:
10. Nach einem Klick auf FERTIG STELLEN ist die Installation beendet.

Nun erscheint ein neues Symbol in der Taskleiste.

Die Farbe im Symbol zeigt den Verbindungsstatus an:

- rot – keine oder sehr schlechte Verbindung
- gelb – brauchbare, aber schlechte Verbindung
- grün – gute bis sehr gute Verbindung

Klickst du das Symbol an, erscheint ein Menü; hier kannst du das Netzwerk und die Konfigurationssoftware ein- und ausschalten.

Herzlichen Glückwunsch – deine WLAN-Netzwerkkarte ist installiert.

…und was ist noch zu beachten?

Da wir ja clever sind, haben wir vor unserem geplanten Ausflug schon einmal eine Instruktionsanleitung eines Hotspotbetreibers besorgt – und lesen hier:

> Bitte beachten Sie folgende Einstellungen auf Ihrem Gerät:
> Tragen Sie als Netzwerknamen (SSID) Ihrer WLAN-Karte …… ein. Stellen Sie unter „Netzwerkeigenschaften“ der WLAN Karte das TCP/IP Protokoll auf DHCP bzw. „automatisch beziehen“. Öffnen Sie Eigenschaften Ihres Browsers, setzen Sie unter Verbindungen „keine“ und deaktivieren Sie unter LAN-Verbindungen „Proxyserver verwenden“. Öffnen Sie Ihren Browser.

Alles klar? Dann kannst du die folgenden Abschnitte überspringen und im Abschnitt *Sicherheitsvorkehrungen* weiter lesen.

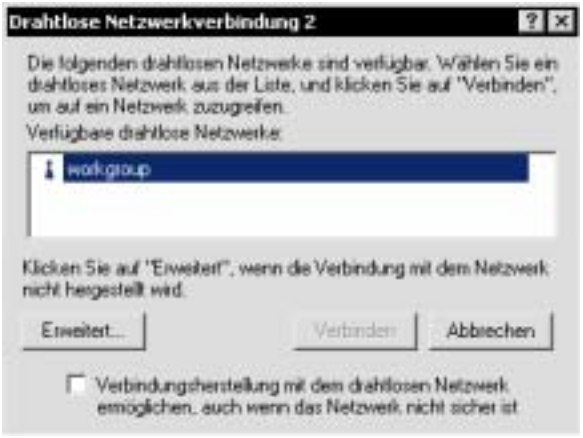
Hast du noch Fragen? Keine Angst – hier folgt des Rätsels Lösung:

SSID – Netzwerkname

SSID (Service Set Identifier) ist der Name für ein Funk-Netzwerk. Möchtest du in diesem Netzwerk arbeiten, benötigt dein Rechner diese Information.

1. Du wählst START|SYSTEMSTEUERUNG, dann die klassische Ansicht und NETZWERKVERBINDUNG.
2. Hier klickst du mit der rechten Maustaste auf *Drahtlose Netzwerkverbindung* und wählst VERFÜGBARE DRAHTLOSE NETZWERKE ANZEIGEN.

3. Es erscheint ein Fenster, das dir alle verfügbaren WLANs namentlich anzeigt. Eintragen musst du hier nichts. Windows XP erkennt die SSID automatisch – in unserem Fall *workgroup*.



Gesetzt den Fall wir haben noch keine Verbindung zu einem Netzwerk, lässt sich eine solche hier erstellen. Sonderwünsche, wie z.B. Verschlüsselungen, nimmst du vor, indem du auf ERWEITERT und dann auf KONFIGURIEREN klickst.

TCP/IP-Adresse automatisch beziehen

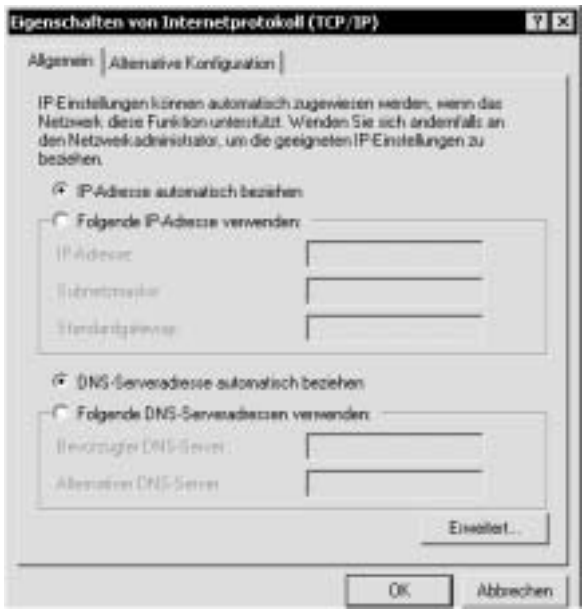
Das Thema SSID wäre geklärt. Was ist nun eine TCP/IP (Transmission Control Protocol/Internet Protocol)-Adresse? Und wie beziehe ich sie automatisch?

TCP/IP-Adressen sind mit Telefonnummern vergleichbar. Dein Telefonanschluss ist durch entsprechende Vorwahl und deine Nummer weltweit erreichbar. Und entsprechend muss auch dein Computer erreichbar sein.

Den Part der Telefonnummer übernimmt hier die TCP/IP-Adresse. Diese kann fest eingetragen – oder eben automatisch bezogen werden. Sehen wir nun, über welche TCP/IP-Eigenschaften dein Netzwerk verfügt.

Du gehst wieder in die NETZWERKVERBINDUNG, klickst mit der rechten Maustaste auf *Drahtlose Netzwerkverbindung* und wählst EIGENSCHAFTEN.

Im nächsten Schritt wählst du die Verbindung *Internetprotokoll (TCP/ IP)* und klickst auf EIGENSCHAFTEN.



Hier sollte die Auswahl auf *IP-Adresse automatisch beziehen* stehen.

Weitere Information zur Protokollfamilie TCP/IP findest du ab Seite 61.

Browsereigenschaften einstellen

Wär's das? Nein – als nächstes müssen wir die Browsereigenschaften überprüfen. Also wählst du in der Systemsteuerung die INTERNETOPTIONEN und das Register VERBINDUNGEN.

Hier klickst du wiederum auf EINSTELLUNGEN.

Du setzt ggf. ein Häkchen in *Automatische Suche der Einstellung* und löschst das Häkchen für *Proxyserver*. Vermutlich brauchst du hier nichts zu tun – bei einer neu installierten WLAN-Karte ist das nämlich die Grundeinstellung.

Sicherheitsvorkehrungen

Der einzig sichere Computer ist bekanntlich ein Rechner ohne Floppy, CD-ROM, Netzwerkkarte oder andere Schnittstellen.

Der logische Umkehrschluss ist durchaus legitim – je mehr Kommunikationsmöglichkeiten ein Computer hat, desto unsicherer ist er auch. Als Internetnutzer bist du den Begehrlichkeiten von Hackern und Unternehmen ausgesetzt. Die einen machen sich einen Spaß daraus, fremde Computer auszuspähen, zu verändern oder einfach nur zum Absturz zu bringen; und die anderen wünschen vor allem mehr Informationen über potenzielle Kunden, damit sie ihr Marketing effizienter gestalten können.

Zum Glück bist du diesem Treiben keineswegs schutzlos ausgeliefert. Das Betriebssystem Windows XP liefert bordeigene Mittel; außerdem gibt es weitere nützliche Programme, die auf keinem PC fehlen sollten. Ob du nun drahtlos oder auf herkömmliche Art und Weise mit deinem Computer ins Internet gehst – in jedem Falle solltest du folgende Sicherheitsvorkehrungen treffen:

- Freigaben deaktivieren
- Firewall verwenden
- Sicherheitsupdates abrufen
- Virenscanner nutzen
- Anti-Trackware einsetzen

Sind das für dich Selbstverständlichkeiten, die du auf deinem Rechner immer zeitaktuell umsetzt, kannst du die folgenden Abschnitte überspringen. Hast du das bisher nicht getan und hast das Gefühl, du solltest mehr für deine Computer-Security tun, solltest du die folgenden Anregungen unbedingt befolgen.

Freigaben deaktivieren

Wenn du in einem Computernetzwerk arbeitest, kannst du Ressourcen wie Ordner oder Laufwerke auf deinem Computer für andere Benutzer im Netzwerk freigeben. Das ist z.B. nützlich, um Dateien von einem Rechner auf einen anderen zu kopieren. Normalerweise solltest du diese Freigabe nach getaner Arbeit wieder deaktivieren – nur vergisst man das leider oft.

Sehen wir also gleich im Fenster COMPUTERVERWALTUNG nach, ob das auf deinem Rechner der Fall ist.

1. In der Systemsteuerung wählst du VERWALTUNG, indem du die klassische Ansicht verwendest,
2. doppelklickst auf Computerverwaltung
3. und wählst im linken Fensterbereich SYSTEM|FREIGEBENE ORDNER|FREIGABEN

Freigegebene Ordner

Wie du in unserem Bild siehst, ist der Ordner *MindManager_X5_WS* freigegeben.

Bei den Freigaben mit dem $-Zeichen handelt es sich um administrative Freigaben. Mit solchen Freigaben kann ein Außenstehender nur dann etwas anfangen, wenn er den Benutzernamen und das Kennwort deiner Administratorkennung kennt.

Du willst die Freigabe beenden?

1. Wähle START und ARBEITSPLATZ,
2. klicke mit der rechten Maustaste auf den betreffenden Ordner
3. und wähle im Kontextmenü FREIGABE UND SICHERHEIT ...

4. Im Register Freigabe entfernst du den Haken: *Diesen Ordner im Netzwerk freigeben.*

Verwende eine Firewall

Hoppla – schon wieder ein Fremdwort?

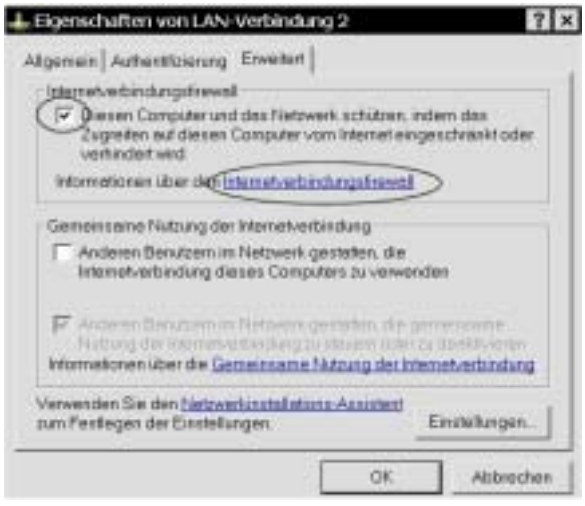
Eine Firewall ist ein Sicherheitssystem, das als Schutzwall zwischen Netzwerkcomputern und der Außenwelt gesetzt wird. Dabei kann es sich um Software oder um Hardware handeln – in jedem Falle versperrt sie Hackern wie auch zahlreichen Computerviren und Würmern den Zugang zum Computer.

Bevor du also deinen Computer ans Internet anschließt, solltest du unbedingt so eine Firewall installieren.

Bei den Firewalls haben sich Produkte von McAfee (www.mcafee.de), Norman (www.norman.com/products_npf.shtml?menulang=de) und ZoneLabs (www.zonelabs.com/download Deutsch1) durchgesetzt – das letztere Produkt ist obendrein für den privaten Benutzer kostenlos.

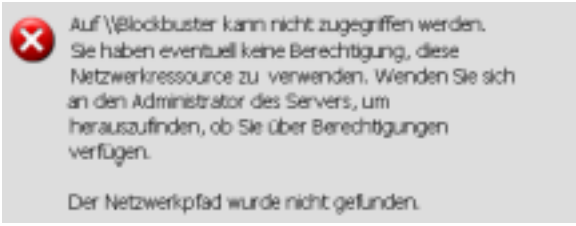
Alternativ kannst auch du die weniger komfortablen Internetverbindungsfirewall des Betriebssystems Windows XP nutzen. Du aktivierst sie wie folgt:

1. In der Systemsteuerung wählst du NETZWERKVERBINDUNG und klickst mit der rechten Maustaste auf die Verbindung, die du schützen möchtest. Dann wählst du im Kontextmenü EIGENSCHAFTEN und die Registerkarte ERWEITERT.



2. Im Dialogpunkt *Internetverbindungsfirewall* wählst du *Diesen Computer und das Netzwerk schützen, indem das Zugreifen auf diesen Computer vom Internet eingeschränkt oder verhindert wird.*
3. Sobald du das EIGENSCHAFTEN-Fenster geschlossen hast, ist die Firewall aktiviert.

Vorsicht Falle!
Es kann sein, dass du bei eingeschalteter Firewall eine Fehlermeldung erhältst, wenn jemand aus dem eigenen Netzwerk auf freigegebene Ressourcen deines Rechners zugreifen möchte.



Fehlermeldung beim Zugriff auf Ressourcen

Das ist natürlich unpraktisch – also musst du in diesem Fall die Internetverbindungsfirewall deaktivieren.

Rufe Sicherheitsupdates ab

Windows-Betriebssysteme und die entsprechende Anwendersoftware machen immer wieder Schlagzeilen bezüglich aufgedeckter Sicherheitsmängel. Entsprechende Updates sollen Abhilfe schaffen. Schaue deshalb regelmäßig auf der Microsoft-Internetseite (www.microsoft.de) nach, ob es in dieser Hinsicht etwas für dich gibt.

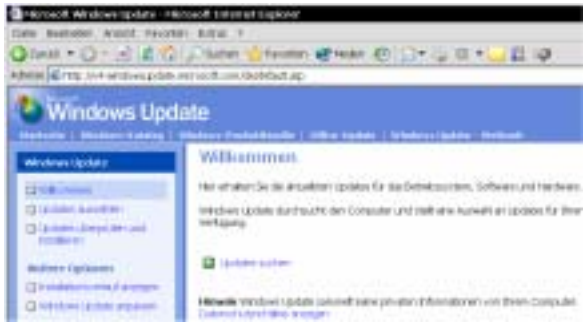
Vertraust du Microsoft hinsichtlich des Datenschutzes, kannst die im Betriebssystem enthaltene Funktion AUTOMATISCHE UPDATES nutzen. Diese Funktion kann die neuesten Sicherheitsupdates von Microsoft automatisch laden, während der Computer eingeschaltet und mit dem Internet verbunden ist.

Willst du dieses AUTOMATISCHE UPDATE für den Download und die Installation wichtiger Sicherheitsupdates von Microsoft nutzen, machst du das so:

1. Du öffnest die SYSTEMSTEUERUNG und doppelklickst auf SYSTEM, um das Dialogfenster SYSTEMEIGENSCHAFTEN zu öffnen.
2. Hier aktivierst du auf der Registerkarte AUTOMATISCHE UPDATES den Punkt *Den Computer auf dem neuesten Stand halten*
3. und wählst eine der drei nachfolgenden *Einstellungen*:

Von nun an erscheint jedes Mal, wenn ein neues Update angeboten wird, ein entsprechendes Benachrichtigungssymbol in der Taskleiste.

Microsoft bietet auch die Möglichkeit an, prüfen zu lassen, ob dein Computer sicherheitstechnisch auf dem aktuellsten Stand ist – und zwar unter dieser Adresse:
v4.windowsupdate.microsoft.com/de/default.asp



Mit Microsoft den Computer prüfen lassen.

Stehst du auf der Windows Update-Seite, klickst du auf UPDATES SUCHEN. Nun wird dein Computer durchsucht, und es erscheint eine Liste der wichtigsten Updates mit Bewertung einschließlich Service Packs.

Hast du etwas dagegen, dass Microsoft die Konfiguration deines Computers erfährt, solltest du dich regelmäßig auf dem Microsoft-Sicherheitsportal über die neuesten Sicherheitsupdates informieren:

www.microsoft.com/germany/ms/security/winsec.mspx.

Nutze einen Virenscanner

Heute ist ein effektiver Virenscanner leider unentbehrlich, wenn du dich im Internet tummelst. Diese Antivirus-Software schützt deinen Computer vor Viren, Würmern, trojanischen Pferden und anderen unerwünschten Eindringlingen.

Übeltäter dieser Arten führen oft bösartige Aktivitäten durch, wie etwa die Löschung von Dateien oder den Zugriff auf persönliche Daten; und es gibt sogar Exemplare dieser Gattungen, die deinen Computer für den Angriff auf andere Computer nutzen.

Beispiele für Antivirus-Software:

- Norton AntiVirus 2004
  www.symantec.de
- AntiVirenKit 2004 Professional
  www.GData.de
- Panda Antivirus Titanium 2004
  www.panda-software.de
- Anti-Virus Complete
  www.buhl.de
- McAfee VirusScan 2004
  www.mcafee.de

Bist du an einem kostenlosem Produkt interessiert, empfehlen wir das *AntiVir 6.21 Personal Edition.* Für private Anwender ist *AntiVir* in den Versionen für Windows 95/98/ME und NT/2000/XP kostenlos. Das betrifft auch die regelmäßigen Updates per Internet. Du findest *AntiVir* im Internet unter www.free-av.de.

Das Programm bietet die grundlegenden Funktionen mit Virenscanner, Virenwächter und Online-Update. Es fehlt allerdings eine E-Mail-Prüfung.

Empfehlenswert ist das verständlich geschriebene und informative Handbuch im PDF-Format, das auf der angegebenen Webseite zum Download bereit steht.

Standardmäßig durchsucht der Scanner nur bestimmte Dateitypen – also solltest du die Option *Alle Dateien* aktivieren, die du unter OPTIONEN|KONFIGURATIONSMENÜ|SUCHE findest.

Achte darauf, dass die Antivirus-Software auf dem neuesten Stand ist. Eine veraltete Version ist unwirksam.

Soll Antivirus-Software vor aktuellen Bedrohungen schützen, muss sie regelmäßig aktualisiert werden. Die meisten Antivirus-Programme aktualisieren sich selbsttätig, sobald sie mit dem Internet verbunden sind. Bist du nicht sicher, ob das auf deinem Computer der Fall ist, öffne das Antivirus-Programm und suche den Aktualisierungsstatus. Wende dich im Zweifelsfall an den Hersteller der Software.

Kontrolliere auch, ob die Antivirus-Software ordnungsgemäß installiert ist – nur dann wird der bestmögliche Schutz gewährt. Die Überprüfung beim Zugriff oder in Echtzeit sollte aktiviert sein.

Die meisten Antivirus-Produkte zeigen durch ein Symbol im Benachrichtigungsbereich unten rechts auf dem Bildschirm an, dass diese Einstellung aktiviert ist.

Anti-Trackware-Lösungen einsetzen

Vermutlich bist du mit der Thematik Cookies vertraut. Diese „Kekse“ können Codes oder Komponenten enthalten, dank derer die

Anwendungsentwickler Informationen über deren Benutzer abrufen und verbreiten können.

Wozu das aber auch führen kann? Nun – es werden

- deine Surfgewohnheiten nachvollzogen,
- deine Vorlieben beim Online-Shopping herausgefunden,
- die Startseite deines Browsers manipuliert oder
- wichtige Systemdateien verändert.

Und wahrscheinlich passiert das alles ohne dein Wissen oder Einverständnis.

Ad-aware bietet dir Schutz für vertrauliche Daten.

Das Programm *Ad-aware Standard Edition* durchsucht den Speicher, die Registry und die Laufwerke nach bekannten schädlichen Daten, lästiger Werbung und Tracking-Komponenten.

Wurden infizierte Objekte analysiert, kannst du dir Objektinformationen anzeigen lassen.

Ein Tracking Cookie wurde identifiziert.

Du findest dieses nützliche Tool auf der Seite www.lavasoft.de.