eload 24

Der Weg zum perfekten WLAN

Sicheres, schnelles Funknetz

Klicken, Lesen, Weitermachen. So einfach geht das.

CHIP

Rubrik	**Netzwerke**
Thema	**WLAN**
Umfang	**34 Seiten**
eBook	**01463**
Autor	**CHIP Communications GmbH**

Den neuen WLAN-Router aufstellen, grundlegende Eigenschaften konfigurieren und DSL-Verbindung einrichten – schon kann der kabellose Netzwerkspaß beginnen. Das eBook zeigt Ihnen, wie es geht.

Der Weg zum perfekten WLAN

Sicheres, schnelles Funknetz

eload24 AG
Sonnenhof 3
CH-8808 Pfäffikon SZ

info@eload24.com
www.eload24.com

Inhalt

Schnell zum eigenen WLAN

Den neuen WLAN-Router aufstellen, grundlegende **Eigenschaften konfigurieren und DSL-Verbindung einrichten** – schon kann der kabellose Netzwerkspaß beginnen. Wir zeigen Ihnen, wie es geht.

Sie haben sich einen neuen WLAN-Router zugelegt oder planen, demnächst ein solches Gerät zu erwerben? Gut, dann müssen Sie nur noch wissen, wie Sie Ihren WLAN-Router einrichten, um in die Welt der kabellosen Datenübertragung einzusteigen. In diesem Praxis-Artikel gehen wir nicht auf ein bestimmtes Gerät ein, sodass Sie mithilfe der folgenden Tipps und Kniffe nahezu jeden aktuellen WLAN-Router bequem konfigurieren können. Ebenfalls keine Rolle spielt das verwendete Betriebssystem. Ganz egal, ob Sie Windows 7, Vista oder XP nutzen – die Vorgehensweise ist stets identisch.

Auspacken und Inhalt überprüfen

Nicht alle WLAN-Router sind sofort betriebsbereit. Bei einigen Geräten ist es nach dem Auspacken erforderlich, die zum Lieferumfang gehörenden Antennen zu montieren. Meist genügt ein Blick in die beigelegte Schnellstartanleitung, um herauszufinden, wie Sie vorgehen müssen. Ebenfalls in der Verpackung zu finden sind Netzteil, Installations-Datenträger, auf dem das PDF-Handbuch untergebracht ist, und das Patchkabel. Letzteres wird benötigt, um den Router mit dem Computer zu verbinden und die Erstkonfiguration durchzuführen.

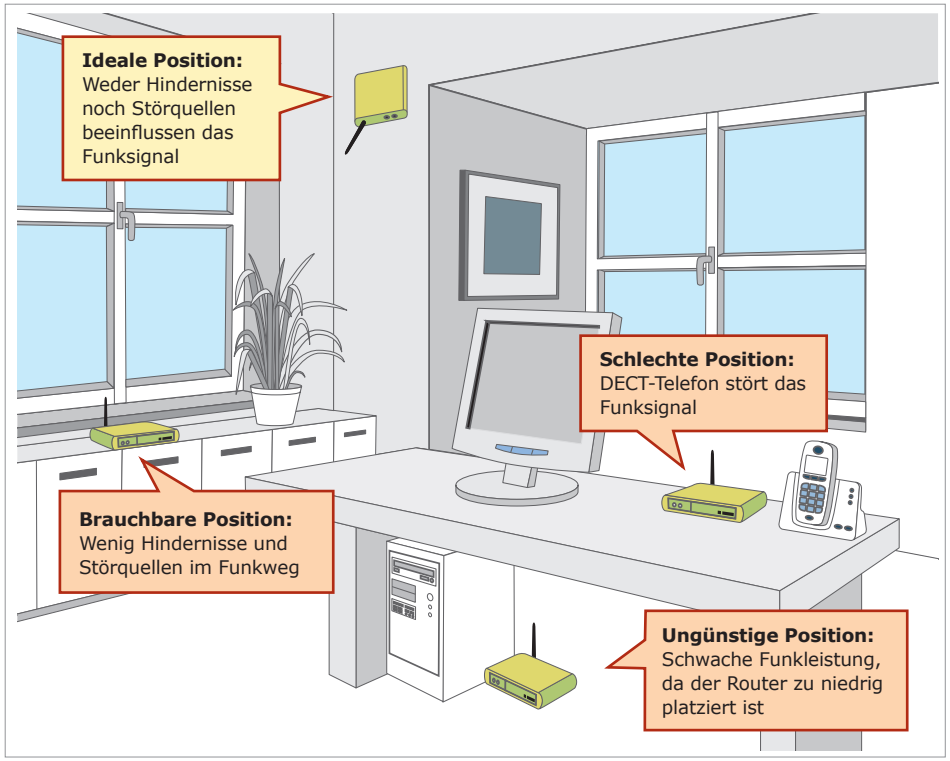
Die wichtigste Frage, die Sie vor Beginn der Konfiguration beantworten müssen: Wie lauten Zugangspasswort und/oder Benutzername für das Konfigurationsmenü des Routers? Die Antwort liefert meist ein Beiblatt, das gedruckte Handbuch oder ein Aufkleber auf der Rückseite des Geräts. Ebenfalls wichtig: Die IP-Adresse, um den WLAN-Router per Browser anzusprechen. Notieren Sie sich diese Daten in digitaler Form als Textdatei, damit Sie sie auch noch ein Jahr später finden, wenn vielleicht eine Neukonfiguration ansteht.

Den idealen Standort finden

Um im WLAN die maximale Leistung zu erreichen, müssen Sie zunächst einmal den optimalen Router-Aufstellort ermitteln. Oft lohnt es sich, Möbel zu verrücken oder den Access Point ein Stück höher zu stellen, um auch auf der Terrasse kabellos – und vor allem schnell – im Internet surfen zu können. Die Devise lautet: Probieren geht über Studieren. Die folgenden Tipps helfen Ihnen bei der Suche nach dem optimalen Router-Standort, ebenso wie das Schaubild auf der vorherigen Seite.

Je höher, desto besser: Ideal ist eine Montage an der Wand, möglichst weit oben. Hier stören weder PCs noch andere elektrische Geräte wie DECT-Telefon oder Mikrowelle. Richten Sie die Antenne des WLAN-Routers schräg nach unten, um eine maximale Abdeckung zu erreichen. Ist das nicht möglich, achten Sie darauf, dass der Access Point nicht genau hinter einem Computer oder einem anderen Gerät steht, das stark strahlt oder das Funksignal durch ein Metallgehäuse abschirmt.

Störquellen umgehen: Access Points, die nach dem b-, g- oder n-Standard arbeiten, funken auf dem 2,4-GHz-Band. Allerdings steht ihnen diese Frequenz nicht exklusiv zur Verfügung. Auch Bluetooth-Geräte, einige DECT-Telefone sowie Baby-Phones nutzen diesen Frequenzbereich. Stellen Sie deshalb den Access Point nicht in der Nähe solcher Geräte auf. Ein Abstand von zwei bis drei Metern reicht im Normalfall aus, um auf der sicheren Seite zu sein.



Je höher, desto besser: *Treffender kann die Suche nach dem optimalen Aufstellort nicht beschrieben werden.*

Leistung verstärken: Kann das Funksignal Betonmauern oder tragende Decken nicht durchdringen, müssen Sie nicht gleich verzweifeln. Abhilfe schafft beispielsweise eine Richtantenne. Diese bündelt die Funkstrahlen in eine Richtung und sendet das Signal auch durch schwierige Materialien hindurch.

Ein Manko gibt es allerdings: Durch die gerichtete Strahlung verringert sich die Abdeckungsbreite des WLANs. Bei einem Desktop-Computer ist das natürlich kein Problem. Wollen Sie aber ein Notebook oder ein anderes mobiles Endgerät, etwa ein iPad, in das drahtlose Netzwerk einbinden, sollten Sie in Betracht ziehen, einen zusätzlichen Access Point einzusetzen oder einen Repeater zu verwenden.

Geräte kombinieren: Bei mehrstöckigen Häusern reicht die Sendeleistung eines einzelnen Access Points oft nicht für das gesamte Gebäude aus. Hier sollten Sie mehrere Geräte zusammenschließen, die dann ein großes WLAN-Netz bilden. Diese Funktion heißt WDS (Wireless Distribution System) – die meisten aktuellen Geräte beherrschen dieses Verfahren bereits von Haus aus. Am einfachsten stellen Sie ein WDS natürlich mit baugleichen Routern auf die Beine, da die Geräte perfekt aufeinander abgestimmt sind.

WLAN-Router anschließen

Haben Sie den optimalen Aufstellort ermittelt, schließen Sie den WLAN-Router an die Stromversorgung an. Warten Sie einige Minuten, bis die Lämpchen am Router permanent leuchten. Der PC sollte bereits laufen. Nehmen Sie das Patchkabel und verbinden Sie den Rechner (Netzwerkbuchse) mit dem

Mit aktuellen Telekom-Routern *nehmen Sie über die Adresse „Speedport.ip" Kontakt auf.*

entsprechenden Anschluss am WLAN-Router. Je nach Gerät ist diese Buchse mit LAN bezeichnet oder es stehen die Ziffern 1 bis 4 respektive LAN1 bis LAN4 über den Ports. Welche der vier Anschlüsse Sie wählen, spielt keine Rolle.

Router-Menü aufrufen

Der schnellste Weg, sich in den WLAN-Router einzuwählen, führt über die IP-Adresse. Haben Sie durch einen Blick in das Handbuch herausgefunden, dass die IP-Adresse Ihres WLAN-Routers 192.168.0.1 oder 192.168.1.1 lautet, tippen Sie diese Adresse in Ihren Internet-Browser ein und drücken die Eingabetaste.

Bei einigen Routern, darunter die beliebten Fritzboxen und die Speedports der Telekom, müssen Sie sich nicht einmal eine IP-Adresse merken. Es genügt, „fritz.box" respektive „speedport.ip" in die Adresszeile des Browsers zu tippen und mit der Eingabetaste zu bestätigen. Dadurch nehmen Sie sofort eine Verbindung mit Ihrem Router auf.

Stimmt die IP-Adresse, erscheint das Menü. Wenn nicht, liegt ein Fehler vor. In diesem Fall müssen Sie die Kabelverbindung überprüfen oder checken, ob Sie aus Versehen eine falsche IP-Adresse eingetippt haben.

Das Konfigurationsmenü

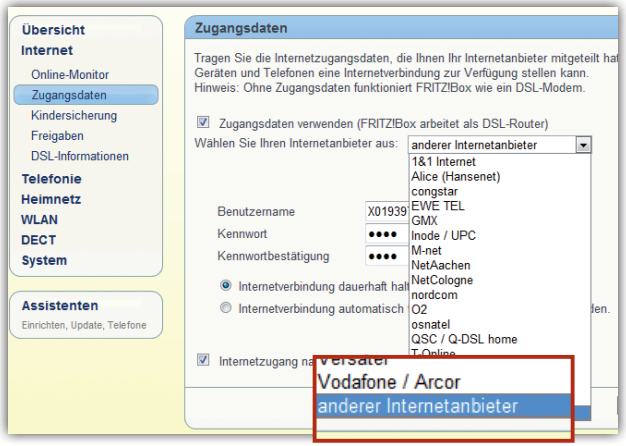
Die Benutzeroberfläche sieht bei jedem Router anders aus – nur innerhalb der Produktlinie eines Herstellers gleichen sich die Abläufe. Lobenswert: Viele Hersteller haben inzwischen erkannt, dass Anwender eine schrittweise Konfiguration bevorzugen, so dass immer mehr WLAN-Router über einen speziellen Assistenten verfügen.

Sind Sie beispielsweise im Besitz eines Speedport-Gerätes, klicken Sie nach der Eingabe des Gerätepasswortes in der linken Spalte auf den Eintrag „Schritt für Schritt", um die Konfiguration mithilfe eines Assistenten durchzuführen. Und wer einen Netgear-Router verwendet, klickt im Hauptmenü auf den Eintrag „Setup-Assistent".

DSL-Verbindung einrichten

Da Sie den Router meist nicht nur als WLAN-Zentrale nutzen möchten, sondern damit auch Ihr Netzwerk ins Internet bringen wollen, steht als Erstes die Konfiguration Ihrer DSL-Verbindung an. Dazu benötigen Sie die Zugangsdaten, die Ihnen Ihr Internet-Anbieter nach Vertragsabschluss zur Verfügung gestellt hat.

Egal, bei welchem Provider Sie Ihren DSL-Anschluss geordert haben: Sie bekommen immer einen Stapel von Unterlagen, in denen



Die Fritzbox *kennt eine ganze Reihe deutscher Internetprovider, was die DSL-Einrichtung deutlich erleichtert.*

auch Ihre Anschlussdaten stehen. Ist es Ihr erster DSL-Anschluss, müssen Sie das Standardpasswort und den Benutzernamen ändern. Dieses Prozedere sollten Sie nicht über das WLAN abwickeln, sondern ganz klassisch – per Kabel. Erst wenn dieser Schritt erledigt ist, verwenden Sie die neuen Zugangsdaten für die Konfiguration des WLAN-Routers. T-Online-Kunden notieren sich bei dieser Gelegenheit die Anschlusskennung, die zugehörige T-Online-Nummer, Mitbenutzernummer/Suffix und das persönliche Kennwort.

Einwahldaten eingeben

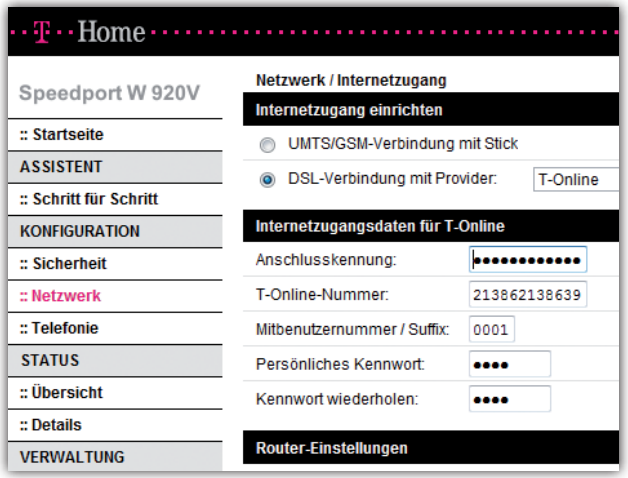
Rufen Sie das Router-Menü auf, um die Einwahldaten des Providers einzutragen.

Bei der Fritzbox verstecken sich die entsprechenden Menüs für die Verbindungseinstellungen unter „Internet“ und „Zugangsdaten“. Praktischerweise sind einige Provider bereits in einer Liste eingetragen. So sehen Sie, welche Daten beim jeweiligen Internetanbieter einzutragen sind.

T-Online-Kunden können sich diese Recherche von vornherein schenken, in aller Regel gibt es keine spezielle Eingabemaske für T-Online. Ausnahmen stellen die Fritzbox und die von T-Online zur Verfügung gestellten Speedport-Geräte dar. Besitzen Sie einen anderen WLAN-Router, müssen Sie einen kleinen Umweg gehen und die einzelnen Zugangsdaten zu einem Benutzernamen zusammenfassen. Setzen Sie die Mitbenutzernummer direkt hinter die T-Online-Nummer, und ergänzen Sie das Resultat um „@t-online.de“. Beispiel: Ihre T-Online-Nummer ist „7898765123456“ und Ihre Mitbenutzernummer ist „0001“, dann ergibt das zusammen die Zeichenfolge „78987651234560001@t-online.de“. Das ist der alphanumerische Benutzername, den Sie im Routermenü eintragen müssen.

PPPoE-Verbindung einrichten

Wichtig bei einem Internetzugang via DSL: Aktivieren Sie das Protokoll PPPoE bzw. alternativ den PPPoA-Zugang. Dazu reicht ein einfacher Mausklick. Weitergehende Einstellungen sind nicht nötig. Falls Sie einmal keine Verbindung mit der Vermittlungsstelle – dem so genannten DSLAM – aufbauen können, liegt meistens ein PPPoE- bzw. Portfehler zugrunde. Bei der Fritzbox zum Beispiel erscheint dann die Fehlermeldung „Grund des Verbindungsabbaus: PPPoE-Fehler“. Bei anderen Routern finden Sie einen entsprechenden Eintrag in der Protokolldatei. Die Ursache hierfür kann sowohl in der Hardware vor Ort als auch bei der Gegenstelle liegen. Eventuell hilft es, den WLAN-Router für einige Minuten komplett abzuschalten und es dann erneut zu versuchen.



Die Einwahldaten *müssen Sie ebenfalls in die Router-Maske eingeben.*

Automatische Trennung festlegen

Haben Sie eine Flatrate und möchten Sie immer mit dem Web verbunden sein, geben Sie bei „Maximum Idle Time“, „Trennen nach x Sekunden“ oder „Leerlaufzeit“ einfach „0“ Sekunden ein. Manche Modelle bieten auch die entgegengesetzte Option: „Immer online“. Ganz egal, wie der entsprechende Befehl heißt – wenn Sie ihn aktivieren, sorgt der Router dafür, dass die Internetverbindung rund um die Uhr steht. Andernfalls lassen Sie ihn nach wenigen Minuten Inaktivität die Verbindung trennen. Da die DSL-Verbindung im Zweifelsfall sehr schnell wieder aufgebaut ist, können Sie hier „60“ Sekunden eingeben.

Soll die Verbindung immer bestehen bleiben, dann sollte sich der Router auch neu verbinden, wenn die Verbindung ungewollt gekappt wurde. Nach rund 24 Stunden macht das T-Online normalerweise auch bei Flatrates. Klicken Sie also noch das Kästchen „Reconnect“ oder „Neu verbinden nach Verbindungsabbruch“ an.

Nachdem Sie die DSL-Funktionen Ihres WLAN-Routers konfiguriert haben, klicken Sie auf die Schaltfläche „Save“, „Speichern“ oder „Laden & Sichern“. Für gewöhnlich müssen Sie dann noch den Router neu starten – die entsprechende Option nennt sich meist „Reboot“. Danach sollte sich die

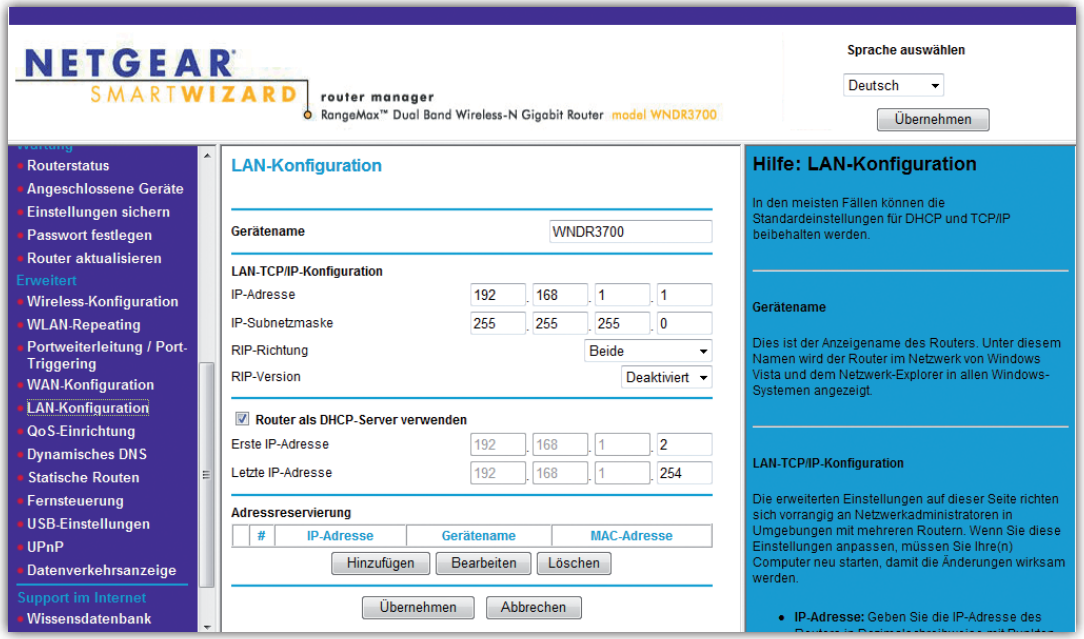
Verbindung innerhalb weniger Sekunden aufbauen, wenn Sie auf „Connect" oder „Verbinden" klicken.

DHCP-Server aktivieren

Dass Ihr WLAN-Router einen integrierten DHCP-Server (Dynamic Host Configuration Protocol) besitzt, ist wahrscheinlich. Zumal, wenn das Gerät zur neuesten Router-Generation gehört. Mit Sicherheit ist der eingebaute DHCP-Server standardmäßig aktiviert. Dennoch kann es nicht schaden, kurz einen prüfenden Blick auf die jeweilige Einstellung zu werfen. Ist die entsprechende Funktion nämlich abgeschaltet, müssten Sie im Zweifelsfall Ihr WLAN von Hand konfigurieren. Finden Sie in der Konfigurationsmaske Ihres WLAN-Routers keinen Menüpunkt namens „DHCP", sollten Sie unter „Netzwerk" nachsehen. Je nach Modell können Sie bei den DHCP-Einstellungen eventuell auch Start- und End-IP-Adresse definieren. Diese Vorgabe ist dann wichtig, wenn in Ihrem WLAN sehr viele drahtlose Empfänger vorhanden sind.

Die maximale Anzahl der zulässigen DHCP-Benutzer können Sie ebenfalls bei vielen Routern vorgeben. Wenn beispielsweise zwei PCs (Arbeitsplatzrechner und Notebook) per WLAN-Router mit dem Internet kommunizieren sollen und noch ein WLAN-Radio hinzukommt, würde man den Wert „3" eintragen. Damit wären die Rechner des Nachbarn von vornherein aus Ihrem Funknetz ausgeschlossen, da sie keine IP-Adressen vom DHCP-Server anfordern können. Potenzielle Hacker tun sich dann ebenfalls schwerer.

Hinweis: An Ihren Clients (beispielsweise USB-Adapter oder zusätzliche WLAN-Radios) muss später die Option zum automatischen Bezug der IP-Adressen per DHCP-Server selbstverständlich auch aktiviert werden.



***Soll der WLAN-Router** auch das Heimnetz verwalten, müssen Sie die DHCP-Funktion aktivieren.*

WLAN-Funktion aktivieren

Es hört sich unsinnig an, bei einem WLAN-Router die WLAN-Funktion einzuschalten, doch nicht bei allen Geräten ist die drahtlose Übertragung standardmäßig aktiviert. An die entsprechenden Einstellungen gelangen Sie, indem Sie im Hauptmenü der Konfigurationsmaske auf „WLAN", „Wireless" oder „Netzwerk" klicken. Hier können Sie bei vielen Geräten sogar noch zusätzliche Optionen ein- und ausschalten. Unter anderem können Sie den Kanal, auf dem gesendet wird, auswählen.

Das Ändern der Voreinstellung kann etwa dann sinnvoll sein, wenn die Sendeleistung des WLAN-Routers unterdurchschnittlich

ist. Außerdem können Sie bei vielen Geräten angeben, welcher Übertragungsstandard unterstützt werden soll und ob das WLAN rund um die Uhr oder nur zu bestimmten Uhrzeiten zur Verfügung stehen soll.

Sinnvolle Zusatzfunktionen im Router aktivieren

Moderne WLAN-Router bieten eine Vielzahl von Optionen, die natürlich immer gerätespezifisch sind. Im Folgenden möchten wir Ihnen einige Punkte aufzeigen, die man bei der weiteren Konfiguration des Routers ebenfalls berücksichtigen sollte, etwa Sicherheitseinstellungen oder Energiesparoptionen.

WPA2-Schlüssel verwenden

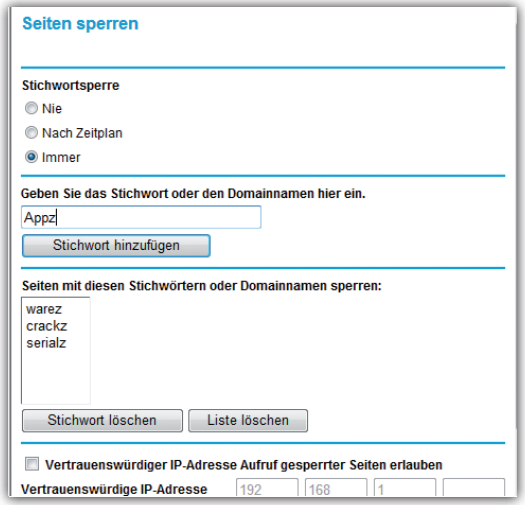
Wie sicher Ihr WLAN gegenüber Eindringlingen ist, hängt nicht zuletzt davon ab, welche Verschlüsselungsvariante Sie wählen. Wenn Ihr WLAN-Router nicht ab Werk auf WPA2 eingestellt ist, sollten Sie schnellstmöglich diese Variante aktivieren. Die Option WEP ist ein Auslaufmodell und gilt als großes Sicherheitsrisiko. Die entsprechenden Einstellungen finden Sie in der Regel in den Untermenüs oder Unterrubriken des Routermenüs, etwa im Abschnitt „Wireless".

Um Hackern das Leben noch ein wenig schwerer zu machen, empfiehlt es sich, zusätzlich die Option „Wireless-SSID-Übertragung" abzuschalten. Einen absoluten Schutz bietet das allerdings nicht, da man mit speziellen Tools trotzdem an die SSID rankommt.

Wesentlich cleverer ist es, die MAC-Adressen-Filterliste zu aktivieren und die entsprechenden Geräte aus Ihrem Netzwerk in diese Liste einzutragen. Die MAC-Adresse eines WLAN-Geräts finden Sie meist auf dessen Unterseite. Und so sieht eine solche Adresse aus: 00:20:04:A4:12:BC.

Interne Firewall einschalten

Eine interne Firewall – soweit vorhanden – sollte man ebenfalls aktivieren. Unter



***Einige WLAN-Router** erlauben es, Webseiten anhand von Schlüsselwörtern zu sperren.*

Umständen kommt es allerdings zu Problemen, wenn Sie zum Beispiel Online-Spiele nutzen wollen. Hier hilft dann nur ein Blick in das PDF-Handbuch des jeweiligen Routers, dort steht, wie die Filtereinstellungen zu korrigieren sind. Ebenso lassen sich anonyme Internet-Anfragen blockieren: Setzen Sie einfach ein Häkchen, um die entsprechende Option zu aktivieren. Bei etwaigen Problemen korrigieren Sie die Einstellung wieder. Weitere Informationen rund um das Thema Firewall lesen Sie auf Seite 28.

Gezielt Webseiten blockieren

Bei Linksys- und Netgear-Routern haben Sie zum Beispiel die Möglichkeit, die Internet-Zugriffe der Rechner im WLAN nach Uhrzeiten und Wochentagen zu beschränken. Wenn Ihre Kinder einen eigenen Computer besitzen, können Sie so nächtliche Surfaktionen wirkungsvoll unterbinden. Die jeweiligen Rechner erkennt der Router an der MAC-Adresse.

Ebenso lassen sich bei vielen aktuellen Routermodellen gezielt einzelne Webseiten sperren. Bei Routern von Linksys und Netgear können Sie sogar eigene Schlüsselwörter definieren. Kommen diese Ausdrücke auf einer Internet-Seite vor, wird sie kurzerhand geblockt.

Firmware regelmäßig aktualisieren

Haben Sie Ihren Router vor kurzem gekauft, sollte er eigentlich auf dem neuesten Stand sein. Trotzdem lohnt sich alle paar Monate ein Blick auf die Versionsnummer der Firmware. Auf der Herstellerseite steht, welche Firmware gerade aktuell ist. Falls sie neuer ist als Ihre, laden Sie die entsprechende Datei herunter und installieren Sie diese. So kommen Sie oft ohne finanziellen Aufwand zu einem leistungsfähigeren Gerät. Und fast immer enthält die neue Firmware wichtige Fehlerkorrekturen.

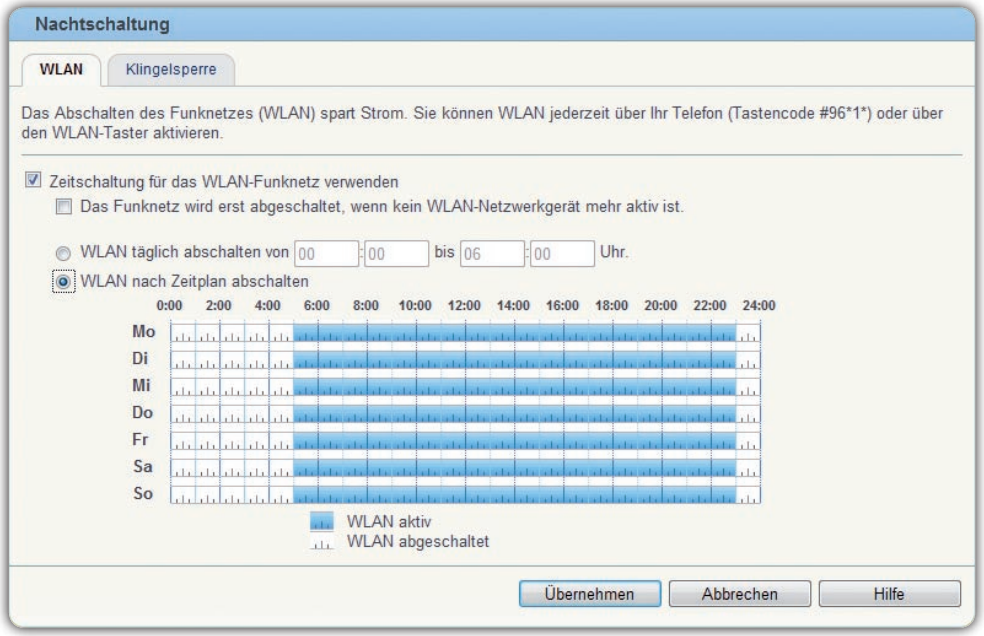
Strom sparen, Leistung reduzieren

Je nach Standort muss der WLAN-Router nicht mit voller Leistung funken. Auch sollte das Gerät nicht die ganze Nacht über sinnlos Energie verpulvern (Standby-Modus).

Besitzer einer Fritzbox haben es gut: Denn bei diesen Modellen kann man in den Systemeinstellungen ganz genau festlegen, zu welchen Tages- und Nachtzeiten das WLAN Sendepause hat. Sie müssen lediglich auf „System" klicken, sich für „Nachtschaltung" entscheiden und dann angeben, wann der Router in den Energiesparmodus gehen kann.

Praktisch: Entweder legen Sie eine bestimmte Zeitspanne wie „zwischen 00:00 und 06:00 Uhr" fest, die für jeden Tag gilt, oder Sie definieren anhand eines Stundenplans, zu welchen Zeiten der WLAN-Router an den einzelnen Wochentagen Pause machen darf. Letzteres ist beispielsweise dann sinnvoll, wenn Sie am Wochenende auch nach 00:00 Uhr noch online gehen möchten. Ähnliche Funktionen finden sich aber auch in anderen Routermodellen, zum Beispiel in den Speedports der Telekom.

Artur Hoffmann



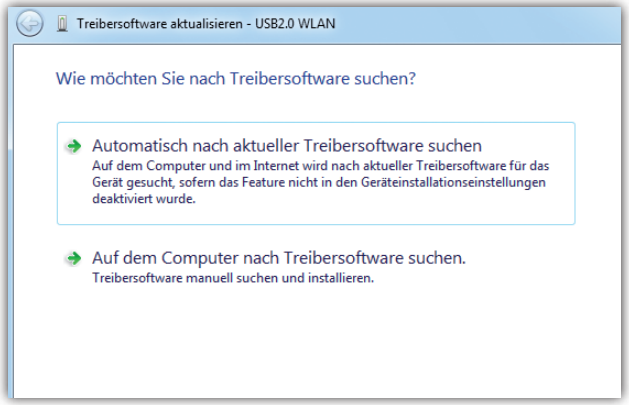
Die Fritzbox bietet *Ihnen viele Energiespar-Optionen, etwa das zeitgesteuerte Abschalten.*

WLAN mit Windows 7

Prinzipiell ist die **WLAN-Verbindung unter Windows 7** in wenigen Minuten eingerichtet. Doch manchmal liegt die Tücke im Detail. Diese Tipps helfen weiter.

Windows 7 und WLAN – diese Kombination macht richtig Laune. Zum einen ist das Betriebssystem kinderleicht zu bedienen, zum anderen ist Windows 7 im Handumdrehen für die kabellose Kommunikation eingerichtet. Allerdings kommt es immer wieder einmal vor, dass das Betriebssystem Zicken macht, und einen nicht mehr ganz so aktuellen WLAN-USB-Stick oder ein exotisches Funkmodul nicht erkennt, sodass Sie nicht in den Genuss der automatischen Einrichtung kommen. Und genau auf diese Fälle gehen wir in diesem Beitrag ein.

Darüber hinaus erklären wir Ihnen, wie Sie vorgehen müssen, um einen Windows-7-PC in Ihr WLAN zu integrieren. Dabei gehen wir selbstverständlich davon aus, dass der WLAN-Router bereits konfiguriert ist und ein Funknetz zur Verfügung steht. Wie Sie dabei vorgehen, erfahren Sie im Beitrag auf Seite 3.



***Handelt es sich beim WLAN-USB-Stick** um ein exotisches Modell, muss Windows 7 passen.*

1 Treiber automatisch einspielen

Darf man den Aussagen von Microsoft Glauben schenken, unterstützt Windows 7 wesentlich mehr Hardware-Komponenten als sein Vorgänger. Aus diesem Grund ist es ratsam, vor der Suche nach dem passenden Treiber die Probe aufs Exempel zu machen und auf die im Betriebssystem integrierte Routine zur „Gerätetreiberinstallation" zu vertrauen.

Schließen Sie den WLAN-Adapter am Rechner an und warten Sie einfach ab, was passiert. Installiert Windows 7 die passenden Treiber, sind Sie fein raus und können gleich mit Schritt 6 fortfahren. Meldet sich das Betriebssystem hingegen mit der Meldung „Die Gerätetreibersoftware wurde nicht installiert" zu Wort, steht die manuelle Installation an.

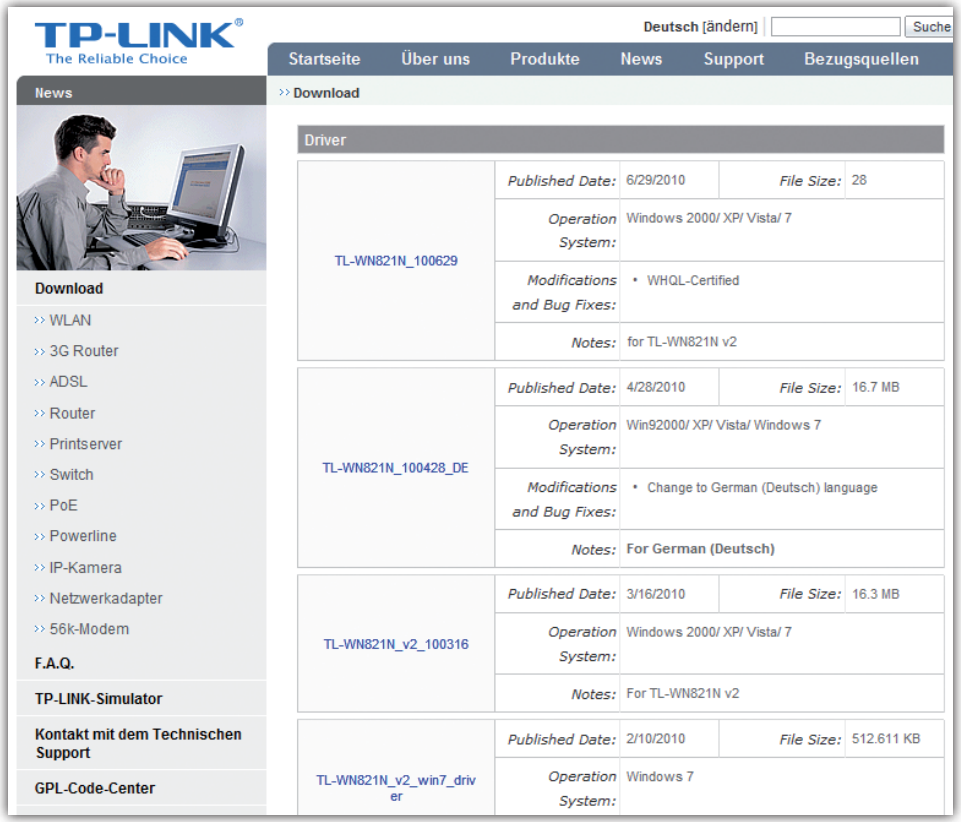
Die weitere Vorgehensweise hängt davon ab, ob Sie einen Datenträger besitzen, auf dem die Treiber des Geräts zu finden sind, oder ob Sie die Steuerungssoftware erst einmal im Web suchen und herunterladen müssen.

2 Treiber suchen lassen

Auch wenn der Assistent keine Treiber gefunden hat, kann es nicht schaden, noch einmal eine Online-Suche zu starten. Klicken Sie auf „Start", „Alle Programme" und „Systemsteuerung". Öffnen Sie den „Geräte-Manager", doppelklicken Sie auf die zu installierende Hardware, die Sie im Normalfall im Bereich „Andere Geräte" finden, und bringen Sie das Register „Treiber" in den Vordergrund. Klicken Sie auf die Schaltfläche „Treiber aktualisieren" und wählen Sie dann die Option „Automatisch nach aktueller Treibersoftware suchen" aus. Wird diese Suche ebenfalls nicht von Erfolg gekrönt, fahren Sie mit dem nächsten Schritt fort.

3 Treiber von CD installieren

Legen Sie die zum Lieferumfang des WLAN-Sticks gehörende CD-ROM in das



***Die meisten Hersteller** bieten im Internet aktuelle Hardware-Treiber an.*

Laufwerk ein und schließen Sie den Dialog „Treibersoftware aktualisieren". Im Fenster „Eigenschaften von" klicken Sie erneut auf „Treiber aktualisieren" und entscheiden sich diesmal für die Option „Auf dem Computer nach Treibersoftware suchen". Im folgenden Fenster klicken Sie auf „Durchsuchen", navigieren im Dialog „Ordner suchen" zum Laufwerk, in dem sich der Datenträger befindet, und bestätigen mit „OK". Klicken Sie auf „Weiter", damit Windows 7 nach dem passenden Treiber sucht. Hat das Betriebssystem das Gesuchte auf dem Datenträger entdeckt, beginnt die automatische Installation des Treibers.

In den allermeisten Fällen werden Sie während des Einspielvorgangs durch eine Hinweismeldung darauf aufmerksam gemacht, dass der Herausgeber des Treibers nicht überprüft werden konnte. Sie können die Warnung durch einen Klick auf „Diese Treibersoftware trotzdem installieren" schließen, da Sie ja wissen, dass keine Gefahr droht. Schließlich spielen Sie den Treiber von der CD ein, die vom Hersteller des WLAN-Sticks stammt. Nach Abschluss der Installation teilt Ihnen Windows 7 mit, dass die Treibersoftware erfolgreich aktualisiert wurde.

4 Treiber aus dem Web laden

Ein wenig komplizierter gestaltet sich die Installation, wenn Sie nicht mehr im Besitz der Original-Treiber-CD sind oder Windows 7 keinen der Treiber akzeptiert. In diesem Fall kommen Sie leider nicht um die manuelle Suche auf der Hersteller-Homepage herum.

Suchen Sie in den Bereichen „Support" oder „Download" nach den Treibern. Alternativ dazu führt oft auch die Suchfunktion zum Erfolg. Tippen Sie die exakte Bezeichnung der WLAN-Komponente in die Suchmaske und bestätigen Sie mit der Eingabetaste. Ist das Gerät von einem namhaften Hersteller, stehen die Chancen überdurchschnittlich gut, dass Sie speziell für Windows 7 entwickelte Treiber finden.

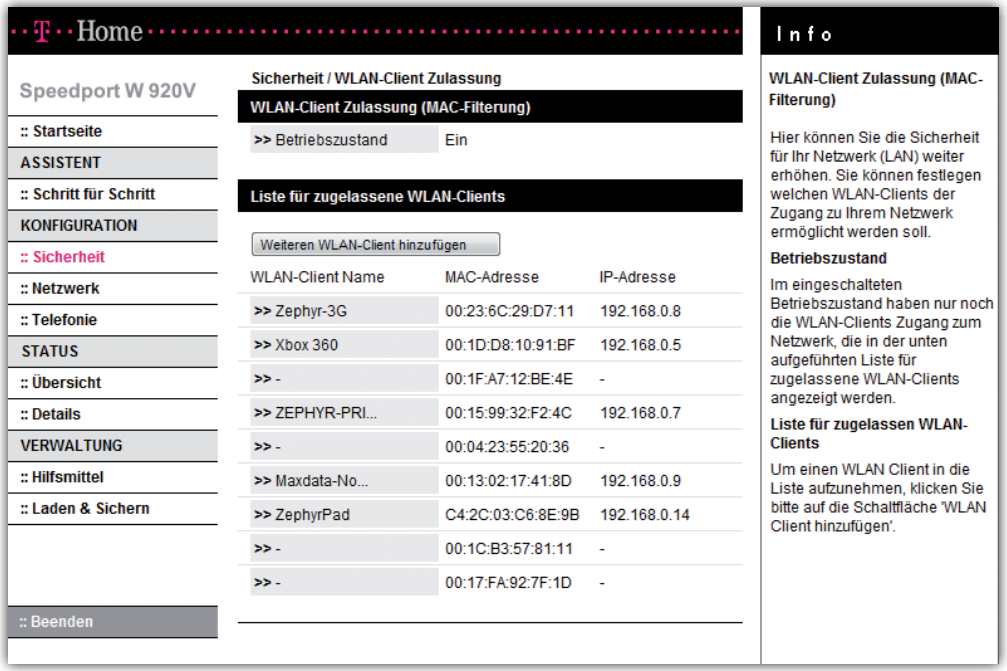
5 Treiber von Festplatte einspielen

Laden Sie die Datei von der Hersteller-Homepage herunter und – falls erforderlich – entpacken Sie das Archiv. Merken Sie sich den Ordner, in den die extrahierten Dateien gespeichert sind, und gehen Sie dann so vor wie im vorigen Schritt beschrieben. Sobald Windows 7 wissen will, in welchem Verzeichnis nach den Treibern gesucht werden soll, geben Sie den Pfad an, um die Installation zu starten.

Hinweis: Finden Sie keine speziellen Treiber für Windows 7, müssen Sie nicht gleich die Flinte ins Korn werfen. Denn das neue Betriebssystem kann auch Treiber, die eigentlich für Windows Vista gedacht sind, verwenden. Das funktioniert nicht immer, ist aber durchaus einen Versuch wert.

6 WLAN-Zugang erlauben

Ist der WLAN-Adapter unter Windows 7 eingebunden, können Sie noch nicht gleich Kontakt mit Ihrem WLAN aufnehmen. Der Grund: Sie haben Ihren WLAN-Router hoffentlich so konfiguriert, dass nur diejenigen Geräte eine Verbindung herstellen dürfen, deren MAC-Adresse bekannt ist. Und da der Router die soeben angeschlossene Komponente noch nicht kennt, müssen Sie den Kontakt zwischen Computer und WLAN-Router über eine kabelgebundene Verbindung herstellen.



Damit die Verbindung klappt, *müssen Sie die MAC-Adresse des WLAN-USB-Sticks freigeben.*

Tippen Sie die Adresse des Routers, zum Beispiel „http://fritz.box" oder „http://192.168.1.1" in die Adresszeile des Internet-Browsers und bestätigen Sie mit der Eingabetaste. Melden Sie sich mit den korrekten Zugangsdaten an der Konfigurationsmaske an und wechseln Sie dann zu dem Bereich, in dem Sie die MAC-Adressen eintragen können. Bevor Sie nun die entsprechende Änderung durchführen können, müssen Sie natürlich die MAC-Adresse des WLAN-Adapters kennen.

Am einfachsten ist es, auf „Start" zu klicken, „cmd" in die Eingabebox zu tippen und dann in der Liste der Fundstellen den Eintrag „cmd" anzuklicken. Tippen Sie in die DOS-Box den Befehl „ipconfig /all" ein und bestätigen Sie mit der Eingabetaste. Suchen Sie nach dem Eintrag „Drahtlos-LAN-Adapter". Direkt darunter steht in der Zeile „Beschreibung" der vollständige Name des WLAN-Geräts; die MAC-Adresse ist in

der Zeile „Physikalische Adresse“ zu finden. Schreiben Sie sich diesen zwölfstelligen Code auf, wechseln Sie zur Konfigurationsmaske des WLAN-Routers und legen Sie fest, dass das Gerät mit dieser MAC-Adresse zukünftig mit dem Router kommunizieren darf.

7 WLAN-Adapter konfigurieren

Ziehen Sie das Netzwerkkabel ab, um mit der Konfiguration des WLAN-Adapters fortzufahren. Klicken Sie mit der rechten Maustaste auf das WLAN-Symbol in der Systray und wählen Sie den Befehl „Netzwerk- und Freigabecenter öffnen“. Klicken Sie auf „Neue Verbindung oder neues Netzwerk einrichten“, markieren Sie „Manuell mit einem Drahtlosnetzwerk“ verbinden und bestätigen Sie mit „Weiter“.

***Windows 7** zeigt alle entdeckten Verbindungen an – Sie müssen nur noch entscheiden, welches WLAN es sein soll.*

In folgenden Dialog tippen Sie die geforderten Angaben ein. Unter anderem will Windows 7 von Ihnen den „Netzwerknamen“ (das ist übrigens die SSID Ihres WLANs), den „Sicherheitstyp“ und natürlich den „Sicherheitsschlüssel“ wissen. All diese Angaben finden Sie in der Konfigurationsmaske des Routers. Gut: Im Gegensatz zu Windows XP und Vista zeigt Ihnen Windows 7 den „Sicherheitsschlüssel“ standardmäßig im Klartext an. Das ist eine große Hilfe. Haben Sie alle geforderten Felder ausgefüllt, können Sie zum Abschluss noch auswählen, ob die Verbindung zukünftig automatisch hergestellt werden soll. Klicken Sie dann auf „Weiter“, meldet sich Windows 7 mit einer Erfolgsmeldung zu Wort.

8 WLAN-Verbindungen verwalten

Wie XP und Vista ist natürlich auch Windows 7 in der Lage, verschiedene WLANs zu verwalten. Klicken Sie mit der linken Maustaste auf das entsprechende Icon in der Systray, zeigt Ihnen das Betriebssystem alle in der Nähe befindlichen WLANs an, die eine SSID senden.

Um sich mit einem dieser Drahtlosnetzwerke zu verbinden, müssen Sie lediglich den entsprechenden Eintrag anklicken, den daraufhin geforderten „Netzwerksicherheitsschlüssel“ eintippen und mit „OK“ bestätigen.

Artur Hoffmann

XP und Vista: Fit fürs WLAN

Windows XP und Windows Vista stehen inzwischen im Schatten von Windows 7, sind aber immer noch im Einsatz. Nutzern dieser Betriebssysteme zeigen wir, **wie sie eine WLAN-Verbindung aufbauen.**

Auch wenn es Microsoft nicht gerne hört: Windows XP lebt! Auf unzähligen Zweit- und Dritt-PCs sowie -Notebooks ist das Volksbetriebssystem immer noch im Einsatz. Allein schon die Tatsache, dass die Systemvoraussetzungen gering sind, macht Windows XP zum idealen Begleiter für alle nicht mehr ganz so gut ausgestatteten Rechner.

Noch besser: Auf die WLAN-Nutzung müssen Sie auch nicht verzichten, da Windows XP prima kabellos kommunizieren kann.

In diesem Beitrag zeigen wir Ihnen, wie Sie Windows XP im Handumdrehen flott fürs WLAN machen. Der Vollständigkeit halber gehen wir auch auf die Einrichtung unter Windows Vista ein, da der eine oder andere Anwender dieses Betriebssystem einsetzt.

1 Treiber automatisch installieren

In den meisten Fällen führt die automatische Treiberinstallation im Handumdrehen zum Erfolg – und zwar sowohl unter Windows XP als auch bei Windows Vista.

Allerdings kann es in Einzelfällen passieren, dass beim Einspielen der Treiber noch zusätzliche Anwendungen auf dem PC installiert werden. Legen Sie die zum Lieferumfang des WLAN-Adapters gehörende CD- oder DVD-ROM in das Laufwerk, und schließen Sie dann den WLAN-Adapter an oder stecken Sie die PCI-Karte in den dafür vorgesehenen Steckplatz des Computers.

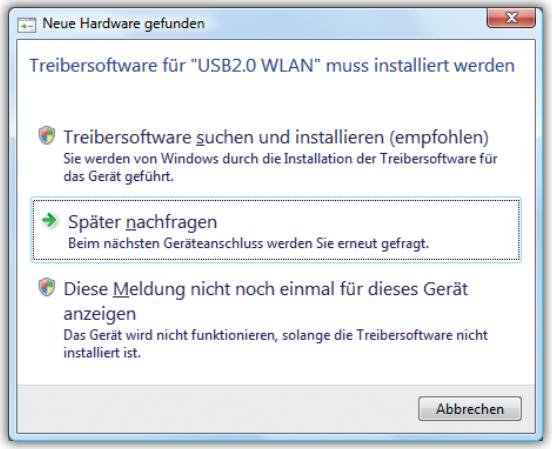
Windows XP: Das Betriebssystem wird Sie nun darauf hinweisen, dass eine neue Hardware erkannt wurde. Sollte dieser Hinweis nicht erscheinen, wählen Sie „Start", „Systemsteuerung" und „Hardware", um den Hardware-Assistenten zu starten. Markieren Sie die Option „Nein, diesmal nicht" und klicken Sie auf die Schaltfläche „Weiter". Im nächsten Dialog markieren Sie die Option „Software automatisch installieren (empfohlen)" und klicken auf „Weiter". Nun durchsucht der Assistent den im Laufwerk steckenden Datenträger nach dem passenden Treiber.

Auch wenn Windows XP schon ein paar Jahre auf dem Buckel hat, *ist die Installation der WLAN-Hardware ein Kinderspiel.*

Hat der Hardware-Assistent mehrere Treiber gefunden, wählen Sie den passenden Eintrag aus der Liste aus. Ist hingegen nur ein Treiber vorhanden, wird er automatisch eingespielt. Findet Windows keinen Treiber im System oder auf dem Datenträger, müssen Sie die manuelle Installation durchführen.

Zum Abschluss der Treiberinstallation meldet sich der Hardware-Assistent mit einer Erfolgsmeldung zu Wort. In diesem Dialog wird Ihnen auch die vollständige Bezeichnung der soeben installierten Hardware angezeigt; in unserem Beispiel ist das „TP-LINK TL-WN821N 11N Wireless Adapter". Ein Klick auf „Fertig stellen" beendet die Installation. Die neue Hardware sollte jetzt korrekt funktionieren.

Windows Vista: Unter Vista gehen Sie auf die gleiche Art und Weise vor. Im Dialog



Windows Vista *ist bereits ab Werk mit einer Vielzahl von Treibern für WLAN-Hardware ausgestattet, was die Installation erleichtert.*

„Neue Hardware gefunden" wählen Sie „Treibersoftware suchen und installieren (empfohlen)" und klicken dann auf „Fortsetzen".

Im nächsten Dialog klicken Sie auf „Nicht online suchen" und entscheiden sich im folgenden Schritt für „Weiter", damit Windows Vista die CD nach dem Treiber durchsucht. Wird das Betriebssystem fündig, kümmert es sich natürlich auch gleich um die Installation. Nach dem Einspielen des Treibers schließen Sie den Dialog „Die Software für dieses Gerät wurde erfolgreich installiert".

Hat alles geklappt, und hat der Assistent einen Treiber gefunden, geht es oft mit der Warnmeldung weiter, dass die verwendete Hardware den Windows-Logo-Test nicht bestanden habe. Das ist aber nicht besonders schlimm. Klicken Sie einfach auf die Schaltfläche „Installation fortsetzen", um mit dem Einspielen des Treibers fortzufahren.

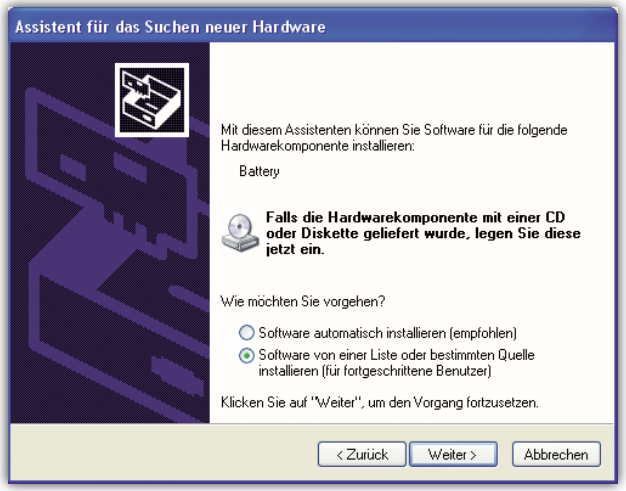
2 Treiber manuell einspielen

Hat die automatische Treiberinstallation nicht geklappt, ist das kein auch kein großes Problem. Denn Sie können den Treiber auch von Hand einspielen. Dabei spielt es keine Rolle, ob Sie den Treiber von der mitgelieferten CD installieren wollen oder einen bereits von der Hersteller-Homepage heruntergeladenen und auf Festplatte gespeicherten Treiber einspielen möchten.

Windows XP: Das Betriebssystem startet den Hardware-Assistenten und weist Sie darauf hin, dass neue Hardware erkannt wurde.

Klicken Sie erst auf „Software von einer Liste oder bestimmten Quelle installieren (nur für fortgeschrittene Benutzer)", dann auf „Weiter". Nun können Sie einen Pfad zum Treiber, den Sie installieren möchten, angeben. Standardmäßig ist „Wechselmedien durchsuchen (Diskette, CD)" aktiviert.

Wollen Sie selbst auf der Installations-CD nach dem Treiber suchen, markieren Sie „Folgende



Klappt die automatische Installation *nicht, müssen Sie Windows XP verraten, wo die zu verwendenden Treiber gespeichert sind.*

Quelle ebenfalls durchsuchen:" und klicken anschließend auf die Schaltfläche „Durchsuchen".

Im daraufhin angezeigten Dialog wählen Sie Ihr CD-ROM-Laufwerk aus, in das Sie die mitgelieferte Installations-CD eingelegt haben. Lassen Sie sich die Ordner anzeigen, indem Sie auf das „+"-Kästchen klicken. Wählen Sie den Ordner für Windows XP aus, den Sie meist daran erkennen, dass im Verzeichnisnamen „XP" oder „WinXP" steht. Klicken Sie auf „OK".

Haben Sie dem Hardware-Assistenten von Windows XP gezeigt, welcher Treiber installiert werden soll, klicken Sie auf „Weiter".

Eventuell macht Sie ein Hinweis-Dialog darauf aufmerksam, dass der Treiber den Windows-Logo-Test nicht bestanden hat. Wie schon im vorigen Abschnitt erwähnt, können Sie diesen Hinweis getrost ignorieren und mit „Installation fortsetzen" fortfahren.

Ein Klick auf „Fertig stellen" beendet den Assistenten. Sie können die korrekte Installation im Geräte-Manager überprüfen: Klicken Sie in der „Systemsteuerung" auf „System", „Hardware" und „Geräte-Manager". Ihr Gerät finden Sie unter der Kategorie „Netzwerkadapter".

Windows Vista: Bei Windows Vista funktioniert es ähnlich einfach. Um den Einrichtungsassistenten zu starten, wählen Sie „Start" und „Systemsteuerung" und doppelklicken auf „Hardware". Im ersten Schritt klicken Sie auf „Weiter", markieren dann die Option „Hardware manuell aus einer Liste wählen und installieren (für fortgeschrittene Benutzer)" und bestätigen mit einem Klick auf „Weiter". Markieren Sie im Bereich „Gängige Hardwaretypen" den Eintrag „Alle Geräte anzeigen", klicken Sie auf „Weiter" und wählen Sie im folgenden Schritt „Datenträger" aus.

Wählen Sie nach einem Klick auf „Durchsuchen" das CD-ROM-Laufwerk aus und öffnen Sie den Ordner, in dem der Treiber abgelegt ist. Markieren Sie die Treiberdatei, die Sie an

Ein Klick genügt, *damit Windows Vista alle in der Nähe befindlichen Drahtlos-Netzwerke, die eine SSID senden, auflistet.*

der Endung „INF" erkennen, und schließen Sie die Dialoge mit Klicks auf „Öffnen" und „OK". Wieder im Assistenten markieren Sie das gewünschte Gerät, klicken auf „Weiter" und schließen die Installation ab.

Passen die ausgewählten Treiber zur WLAN-Hardware, *steht der Installation nichts mehr im Weg.*

3 WLAN-Verbindung wählen

Sollten Sie schon ein Wireless-LAN in Betrieb haben, zeigt Ihnen Windows XP nach einem Klick auf das Netzwerk-Icon in der Systray nun alle verfügbaren Netze an.

Wählen Sie Ihr Drahtlos-Netzwerk aus und klicken Sie auf „Verbinden". Damit ist die Funkverbindung im Grunde genommen schon eingerichtet, sofern in diesem WLAN keine Verschlüsselung zum Einsatz kommt. Andernfalls geben Sie noch den Netzwerkschlüssel in das darunter liegende Feld ein.

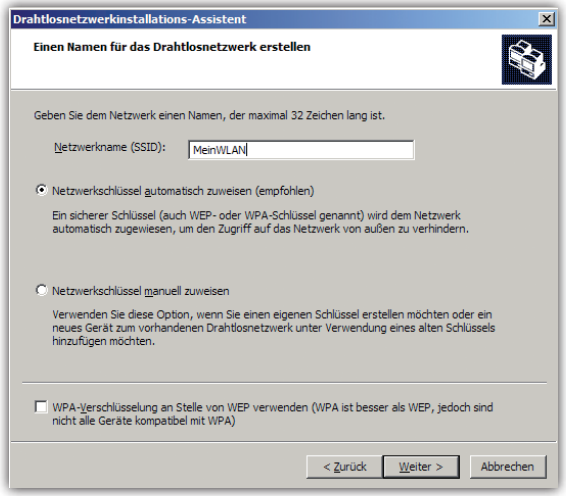
Windows Vista zeigt Ihnen ebenfalls alle Funknetze an, die aktiv und erreichbar sind. Klicken Sie dazu im Startmenü auf „Verbindung herstellen". Diesen Dialog erreichen Sie übrigens auch über einen Klick mit der rechten Maustaste auf das Netzwerksymbol im Systray und die Auswahl des Befehls „Verbindung mit einem Netzwerk herstellen".

Sie sehen nun alle erreichbaren Drahtlos-Netzwerke. Vista zeigt neben den WLANs auch Einwahl- und VPN-Verbindungen an. Um die Anzeige auf drahtlose Netze zu beschränken, wählen Sie bei „Anzeigen" die Option „Drahtlosnetzwerke" aus.

Markieren Sie Ihr Funknetzwerk, und klicken Sie auf „Verbindung herstellen". Anschließend

fordert Windows Vista Sie zur Eingabe der „Passphrase" beziehungsweise des Sicherheitsschlüssels auf. Tragen Sie an dieser Stelle das Kennwort ein, das Sie bei der Konfiguration des Access Points definiert haben. Damit niemand mitlesen kann, wird die Passphrase standardmäßig in Form schwarzer Punkte angezeigt. Wollen Sie sich die Eingabe erleichtern, aktivieren Sie „Zeichen anzeigen". Klicken Sie abschließend auf „Verbinden".

Haben Sie die richtige Passphrase eingegeben, erscheint eine Erfolgsmeldung. In diesem Fenster können Sie mit „Dieses Netzwerk speichern" bestimmen, dass sich Vista die Einstellungen



Müssen Sie das WLAN manuell konfigurieren, *benötigen Sie einige Informationen, unter anderem den Netzwerknamen.*

für das WLAN merken soll. Über „Diese Verbindung automatisch starten" speichern Sie die Passphrase auf dem Computer; Vista meldet sich dann automatisch beim Netz an.

4 WLAN-Verbindung manuell einrichten

Bei dem im vorigen Abschnitte demonstrierten Vorgehen ermitteln Windows XP und Vista nach der Auswahl des gewünschten WLANs automatisch Verschlüsselungsmethode und Schlüsseltyp. Das ist bequem, aber nicht in jedem Fall möglich, etwa weil das WLAN nicht gefunden wurde oder nicht aktiv ist.
Klicken Sie in diesen Fällen im Fenster „Verbindung mit einem Netzwerk herstellen" zunächst auf die Schaltfläche mit den beiden Pfeilen. Windows wiederholt nun die Suche nach erreichbaren WLANs.

Windows XP: Taucht das gewünschte Netzwerk unter Windows XP auch danach nicht in der Liste der WLAN-Verbindungen auf, müssen Sie die Einstellungen manuell vornehmen.

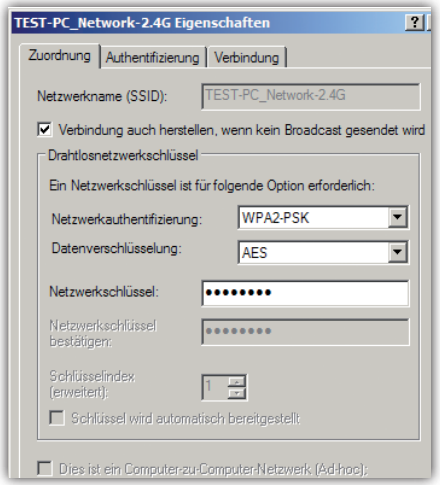
Wählen Sie „Drahtlosnetzwerk für Heim- bzw. kleines Firmennetzwerk einrichten" und klicken Sie im folgenden Schritt auf „Weiter". Tippen Sie den „Netzwerknamen (SSID)" ein, wählen Sie die Verschlüsselungsmethode aus, die Sie in Ihrem WLAN-Router eingerichtet haben, und klicken Sie auf „Weiter".

Markieren Sie im nächsten Schritt „Netzwerk manuell einrichten" und schließen Sie den Assistenten mit „Weiter" und „Fertig stellen". Die neue Verbindung taucht nun in der Liste der verfügbaren Drahtlosnetzwerke auf; per Doppelklick stellen Sie die Verbindung her.

Windows Vista: Unter Windows Vista klicken Sie auf den Link „Eine Verbindung oder ein Netzwerk einrichten". Wählen Sie im Fenster die Option „Manuell mit einem Drahtlosnetzwerk verbinden" aus, und klicken Sie auf „Weiter". Im folgenden Dialog fragt Vista die Einstellungen Ihres WLANs ab.

Geben Sie nun ganz oben neben „Netzwerkname" die SSID an, die Sie auf dem Access Point für Ihr Funknetz ausgewählt haben. Darunter wählen Sie in der Liste neben „Sicherheitstyp" die verwendete Verschlüsselungsmethode aus. Eine Zeile tiefer folgt neben „Verschlüsselungstyp" die Einstellung des benutzten Schlüssels. Das Feld „Sicherheitsschlüssel/Passphrase" schließlich nimmt das Kennwort auf, mit dem der Datenverkehr verschlüsselt wird.

Kreuzen Sie „Diese Verbindung automatisch starten" an, damit Vista sich automatisch einloggt, sobald das Netzwerk in Reichweite ist. Die Option „Verbinden, selbst wenn das Netzwerk keine Kennung aussendet" lässt Vista auch dann mit dem WLAN Verbindung



Es ist problemlos möglich, *die WLAN-Parameter nachträglich zu ändern.*

aufnehmen, wenn auf dem Access Point die Veröffentlichung der SSID deaktiviert wurde. Klicken Sie auf „Weiter", im nun folgenden Fenster auf „Verbindung herstellen mit" und dann auf „Schließen". Falls das Funknetz erreichbar ist, wird die Verbindung aufgebaut.

5 WLAN-Einstellungen neu konfigurieren

Müssen Sie die Einstellungen für den WLAN-Zugriff ändern, etwa weil Sie sich einen neuen Access Point gekauft haben oder sich für ein anderes Verschlüsselungsverfahren entschieden haben, ist das auch kein großes Problem.

Windows XP: Im Dialog „Drahtlose Netzwerkverbindung" markieren Sie das gewünschte WLAN und klicken in der linken Spalte auf „Erweiterte Einstellungen ändern". Im Register „Drahtlosnetzwerke" wählen Sie das WLAN, das Sie neu konfigurieren wollen, aus und klicken auf „Eigenschaften". Im daraufhin angezeigten Dialog können Sie unter anderem „Netzwerkauthentifizierung", „Datenverschlüsselung" und „Netzwerkschlüssel" bearbeiten. Mit „OK" weisen Sie die Änderungen zu und schließen den Dialog.

Windows Vista: Auch unter Vista beginnen Sie mit einem Klick auf „Verbindung mit einem Netzwerk herstellen". Klicken Sie den Eintrag für das Netz rechts an, und wählen Sie „Eigenschaften". Nun öffnet sich die Registerkarte „Sicherheit", in der Sie eine andere Verschlüsselungsmethode und ein neues Kennwort definieren können. Im Register „Verbindung" finden Sie dagegen die Einstellungen für die automatische Verbindungsaufnahme und steuern das Verhalten von Vista, wenn das Funknetz keine SSID ausstrahlt. Außerdem steht hier die Option „Mit einem verfügbaren bevorzugteren Netzwerk verbinden"; sie ist standardmäßig aktiviert. Über diesen Befehl können Sie angeben, ob Windows beim Erkennen eines anderen, bereits eingerichteten WLANs die bestehende Verbindung beenden und Kontakt mit dem neuen Funknetz aufnehmen soll.

Praktisch: Sie können in Windows Vista die Einstellungen für mehrere drahtlose Netzwerke definieren, speichern und dabei auch eine individuelle Rangfolge festlegen.

Sind Sie mit einem niedrig eingestuften Funknetz verbunden und geraten in den Bereich eines höherrangigen, kappt das Betriebssystem die alte Verbindung und wechselt automatisch zum neuen Funknetzwerk.

Die eigentliche Konfiguration nehmen Sie im „Netzwerk- und Freigabecenter" vor, welches Sie in der Systemsteuerung über „Netzwerk und Internet", „Netzwerk- und Freigabecenter" oder im Startmenü über „Netzwerk" und den Button „Netzwerk- und Freigabecenter" erreichen. Klicken Sie auf „Drahtlosnetzwerke verwalten" und entscheiden Sie sich für „Ein Netzwerkprofil manuell erstellen". Geben Sie die Daten ein, und klicken Sie auf die Schaltflächen „Weiter" und „Schließen".

Wenn Sie jetzt wieder den Dialog „Drahtlosnetzwerke verwalten" öffnen, können Sie die soeben eingerichteten WLANs mit der Maus markieren und über die Schaltflächen „Nach oben" und „Nach unten" eine beliebige Reihenfolge festlegen. Voraussetzung ist natürlich, dass bei jedem Drahtlosnetzwerk die Option „Mit einem verfügbaren bevorzugteren Netzwerk verbinden" aktiviert ist.

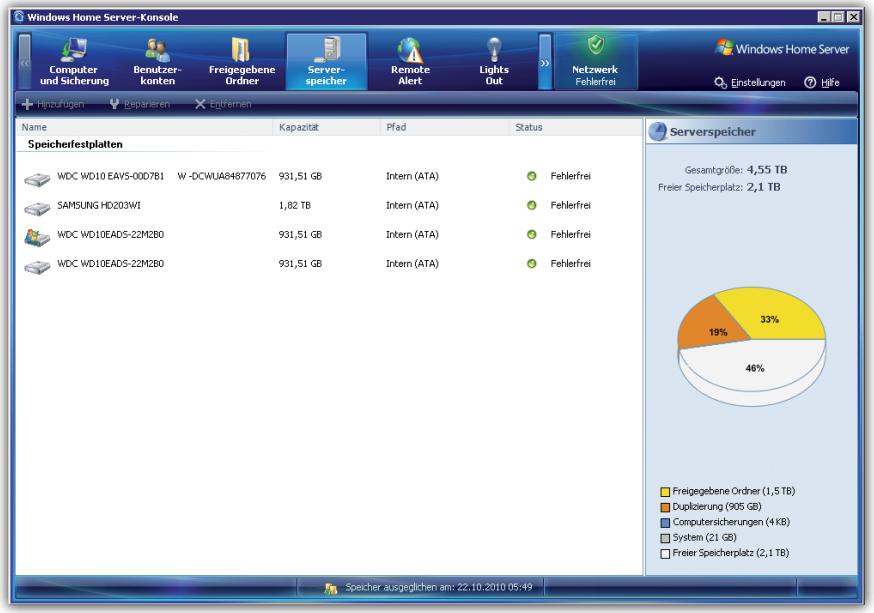
Artur Hoffmann

Das eigene Netzwerk

Auch **in den eigenen vier Wänden** macht das **Vernetzen** mehrerer Rechner Sinn. Kompliziert ist die Einrichtung eines Heim-LANs nicht.

Noch vor gar nicht so langer Zeit stellte die Vernetzung mehrerer Computer eine echte Herausforderung dar: PCs wurden per Nullmodemkabel zusammengeschlossen oder mithilfe exotischer Lösungen, die am seriellen Anschluss oder Parallelport eingestöpselt wurden, vernetzt. Heutzutage sieht die Sache anders aus: Zwei Computer, ein WLAN-Router und ein paar Netzwerkkabel – mehr ist nicht nötig, um zu Hause ein kleines Netzwerk auf die Beine zu stellen.

Die Vorteile solch einer Vernetzung liegen auf der Hand: Sie können Ordner und Laufwerke freigeben, sodass jeder Nutzer des Netzwerks darauf zugreifen kann. Dateien lassen sich im Handumdrehen von einem PC auf einen anderen übertragen. Und wenn ein netzwerkfähiger Drucker zur Verfügung steht, kann er von allen Rechnern genutzt werden.



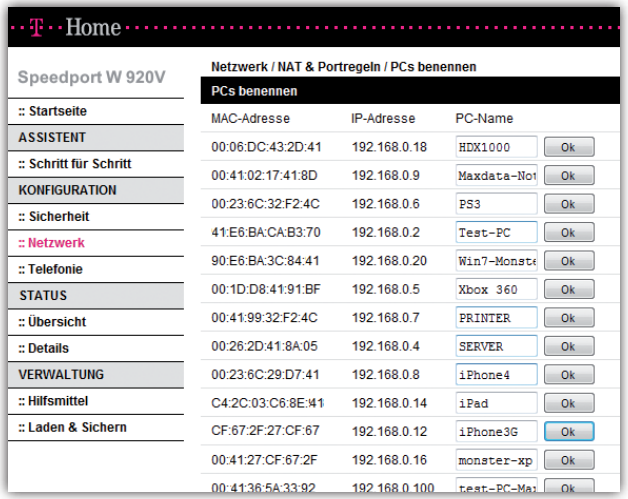
In Client-Server-Netzwerken *greifen alle Computer auf die vom Server bereitgestellten Daten und Funktionen zu.*

In diesem Artikel gehen wir davon aus, dass alle Computer bereits netzwerkfähig sind, dass also die Rechner schon über die entsprechende Netzwerk-Hardware verfügen.

Arbeiten Sie mit Windows 7, können Sie bei der Einrichtung eines Netzwerks, in dem sich ausschließlich Win-7-Rechner tummeln, von der neuen und überaus benutzerfreundlichen Funktion „Heimnetzwerk" profitieren.

Windows ist die Basis des Heim-LANs

Vereinfacht ausgedrückt lassen sich Netzwerke in zwei große Gruppen einteilen: Client-Server-Netzwerke, bei denen der Server im



Damit die Datenpakete an die richtigen Empfänger gelangen, *muss jedes Netzwerkgerät über eine eindeutige IP-Adresse verfügen.*

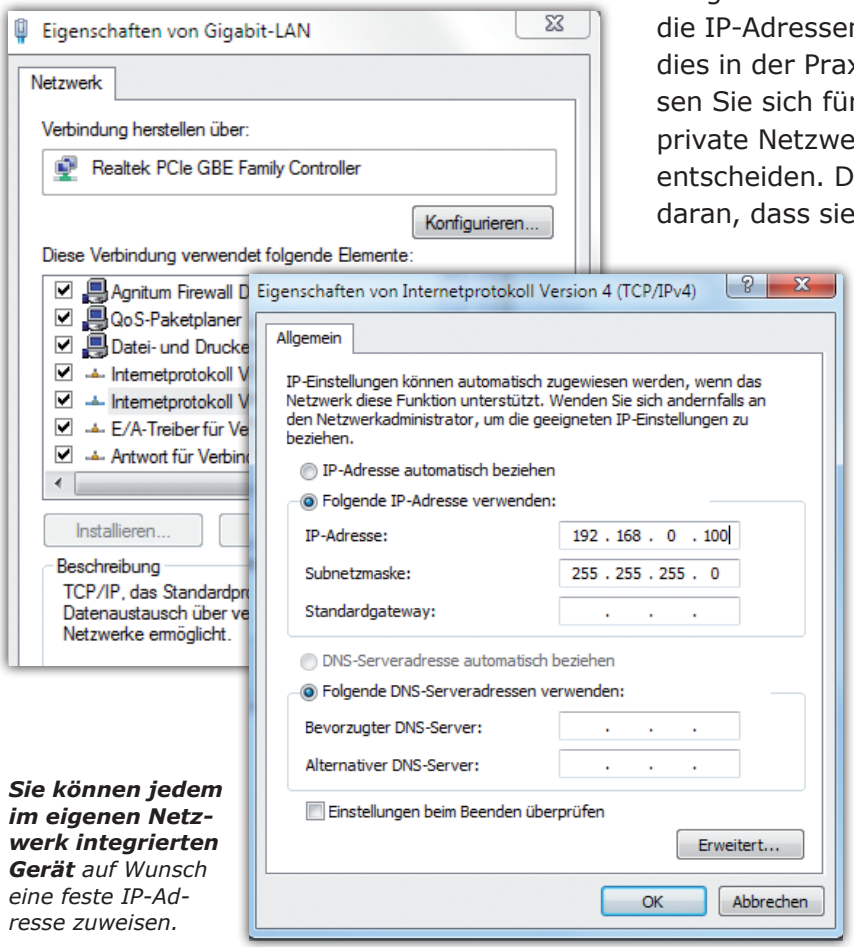
Mittelpunkt steht, sowie Peer-to-Peer-Netzwerke, in denen die einzelnen Computer quasi gleichberechtigte Partner sind.

Größere – in den meisten Fällen in Firmen, Behörden und Bildungseinrichtungen zum Einsatz kommende – Netzwerke sind ausschließlich als Client-Server-Netzwerke konzipiert: Dienste, Dateien und spezielle Funktionen werden von Servern zur Verfügung gestellt, die angeschlossenen Clients greifen dann auf diese Ressourcen zu. Um solch ein Netzwerk aber zu realisieren, ist der Einsatz eines Server-Betriebssystems wie Linux, Windows Server 2008 R2 oder Windows Home Server unumgänglich. In Heimnetzwerken macht dies keinen Sinn, da Anschaffungskosten und administrativer Aufwand in keinem Verhältnis zum Nutzwert stehen.

Weitaus sinnvoller ist es in solchen Fällen, zwei und mehr Rechner zu einem Peer-to-Peer-Netzwerk zusammenzuschließen. Bei dieser Netzwerkvariante kann jeder Rechner Serverfunktionen übernehmen und gleichzeitig alle bereitgestellten Ressourcen der gesamten Arbeitsgruppe nutzen. Windows ist bereits seit der Version 3.11 for Workgroups mit dem nötigen Rüstzeug zum Betrieb eines solchen Peer-to-Peer-Netzwerks ausgestattet.

IP-Adressen identifizieren Computer

Um innerhalb eines Netzwerks die einzelnen Computer voneinander unterscheiden zu können, muss jedem PC eine eindeutige IP-Adresse zugewiesen werden.



***Sie können jedem im eigenen Netzwerk integrierten Gerät** auf Wunsch eine feste IP-Adresse zuweisen.*

Dieses Adressierungsschema erlaubt es, alle im Netzwerk eingebundenen Geräte zu identifizieren – ganz egal, ob es sich dabei um einen Rechner, eine Spielekonsole, ein iPad oder ein Festnetztelefon handelt. Praktisch: Solange im privaten Netzwerk keine Verbindung mit dem Internet besteht, können Sie die IP-Adressen nach Belieben vergeben. Da dies in der Praxis aber kaum vorkommt, müssen Sie sich für eine IP-Adresse aus dem für private Netzwerke reservierten Adressbereich entscheiden. Diese IP-Adressen erkennen Sie daran, dass sie mit „192.168." beginnen.

Setzen Sie in Ihrem Netzwerk einen Router ein, der das Dynamic Host Configuration Protocol (DHCP) unterstützt, entfällt die manuelle Vergabe der IP-Adressen, da die Adressierung vom Router vorgenommen wird. Das ist eine sehr große Hilfe und verhindert, dass Sie den Überblick verlieren.

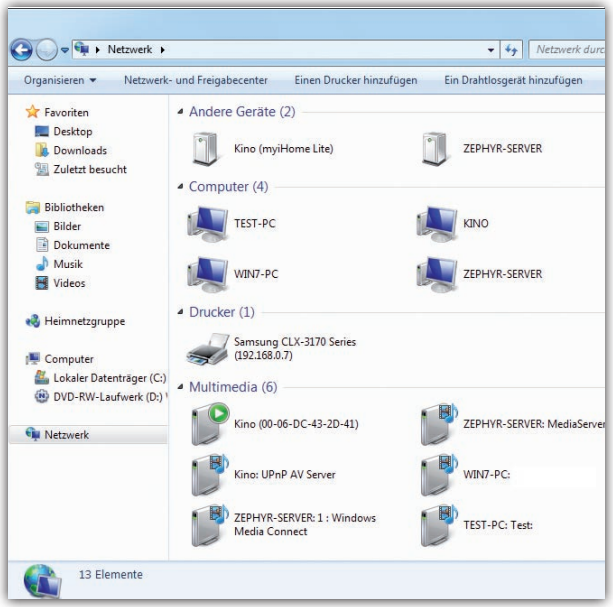
Manuelle Vergabe der IP-Adressen

Ist Ihr WLAN-Router nicht mit DHCP-Funktionalität ausgestattet, was eigentlich ein Grund ist, sich auf der

Stelle ein neues Gerät zuzulegen, müssen Sie die IP-Adressen manuell verteilen. Das ist nicht besonders kompliziert.

Arbeiten Sie mit Windows XP, ist noch ein kleiner Zwischenschritt nötig. Öffnen Sie den „Arbeitsplatz", klicken Sie links auf „Netzwerkumgebung" und wählen Sie dann „Kleines Firmen- oder Heimnetzwerk einrichten". Nach zwei Klicks auf „Weiter" markieren Sie „Dieser Computer stellt eine Verbindung mit dem Internet über ...". Klicken Sie dann so oft auf „Weiter", bis der Assistent Ihnen die Frage stellt: „Wie möchten Sie vorgehen?". Markieren Sie „Windows XP-CD verwenden" und verlassen Sie den Dialog mit „Weiter" und „Fertig stellen". Nach einem Neustart ist Windows XP für die Integration in ein Netzwerk bereit. Anschließend klicken Sie auf „Start" und „Systemsteuerung" und doppelklicken auf „Netzwerkverbindungen".

Unter Windows 7 und Vista entscheiden Sie sich in der „Systemsteuerung" für „Netzwerk- und Freigabecenter" und klicken auf „Netzwerkverbindungen verwalten" (Vista) respektive „Adaptereinstellungen ändern". Klicken Sie den Eintrag, der die im PC verbaute Netzwerkkarte repräsentiert, mit der rechten Maustaste an und wählen Sie „Eigenschaften". Im folgenden Dialog bringen Sie das Register „Allgemein" bzw. „Netzwerk" (bei Windows 7 und Vista) nach vorne.



***Verfügt jeder PC** über eine eindeutige Bezeichnung, erleichtert das die Übersicht.*

Im Bereich „Diese Verbindung verwendet folgende Elemente" markieren Sie den Eintrag „Internetprotokoll (TCP/IP)" bzw. „Internetprotokoll Version 4 (TCP/Ipv4)" und klicken auf „Eigenschaften". Im Register „Allgemein" klicken Sie auf den Befehl „Folgende IP-Adresse verwenden" und tippen als „IP-Adresse" die Zahl „192.168.0.1" ein. Sobald Sie die Einfügemarke in das Feld „Subnetzmaske" setzen, trägt das Betriebssystem automatisch die dazu passende Zahl „255.255.255.0" ein. Mit „OK" weisen Sie die neuen Werte zu.

Tipp

Windows 7 in gemischten Netzen

Eine Heimnetzgruppe ist, wie erwähnt, nur unter Computern möglich, die allesamt mit dem Betriebssystem Windows 7 ausgestattet sind. Mit einem Netzwerk aus unterschiedlichsten PCs – und mit verschiedenen Betriebssystemen – hat die Heimnetzgruppe also nur am Rande zu tun. Wer einen älteren XP-Rechner mit einem Windows-7-PC etwa im WLAN zusammenschließen will, sollte zunächst einige Grundvoraussetzungen schaffen: Laden Sie für den XP-Rechner ein Hotfix (http://support.microsoft.com/kb/922120) herunter und installieren Sie diese Datei. Die Aktualisierung ermöglicht Vista- und Windows-7-PCs, auch XP-Rechner in der Netzwerkumgebung anzuzeigen.

Achten Sie darauf, dass Sie sowohl auf dem XP-Rechner als auch auf dem Windows-7-PC ein Benutzerkonto mit gleichem Namen und identischem Passwort eingerichtet haben. Damit beide PCs im Netz kommunizieren können, müssen sie auch in der gleichen Arbeitsgruppe sein (siehe Abschnitt Computername und Arbeitsgruppe).

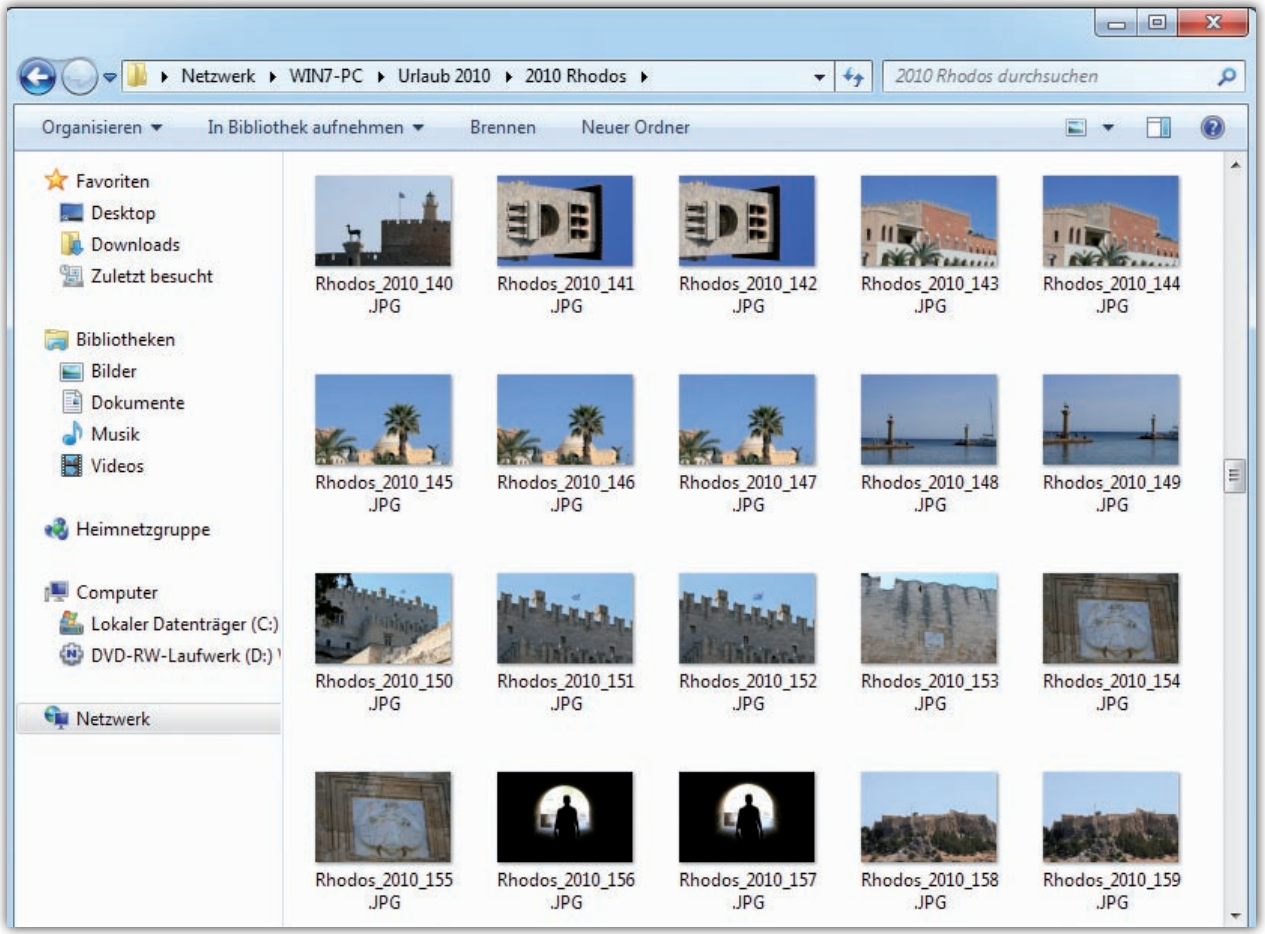
Diesen Arbeitsschritt wiederholen Sie anschließend bei allen im Netzwerk angeschlossenen Rechnern, wobei Sie bei der IP-Adresse die letzte Zahl jeweils um eins erhöhen. Der zweite Rechner im Netzwerk erhält somit die IP-Adresse „192.168.0.2", das dritte Gerät

„192.168.0.2“ und so weiter; die „Subnetzmaske“ ändert sich hingegen nicht.

Verfügt Ihr WLAN-Router über DHCP-Funktionen, gestaltet sich die Sache ungleich einfacher. In diesem Fall konfigurieren Sie die Netzwerkkarten dahingehend, dass sie die „IP-Adresse automatisch“ beziehen. Voraussetzung ist, dass Sie den WLAN-Router entsprechend konfiguriert haben. Wie das geht, lesen Sie im Beitrag auf Seite 3.

Computername und Arbeitsgruppe

Der Computername ist fast so wichtig wie die IP-Adresse, da er Ihnen die Identifizierung erleichtert. Aus diesem Grund muss er eindeutig sein, darf also nur einmal im Netzwerk vorkommen. Dies hat folgenden Hintergrund: Windows zeigt Ihnen die im Netzwerk vorhandenen PCs nicht durch die IP-Adresse, sondern durch den Computernamen an. Anstatt sich also den Kopf zu zerbrechen, ob Sie Ihre wichtigen Dateien auf dem Client „192.168.0.3“ oder „192.168.0.6“ gespeichert haben, müssen Sie sich lediglich einprägsame Computernamen wie etwa „Daten-PC“, „Spielekiste“ oder „Familien-Notebook“ merken.



***Entsprechende Benutzerrechte** vorausgesetzt, unterscheidet sich der Zugriff auf freigegebene Dateien und Ordner nicht vom Umgang mit lokalen Dateien.*

Auch sollten alle Netzwerkrechner Mitglieder ein und derselben Arbeitsgruppe sein, da dies die Übersicht ebenfalls erhöht. Allerdings ist es auch möglich, die in einem LAN zusammengefassten Rechner in verschiedene Arbeitsgruppen einzuteilen, um etwa zwischen „Eltern-PCs“ und „Kinder-Computern“ unterscheiden zu können.

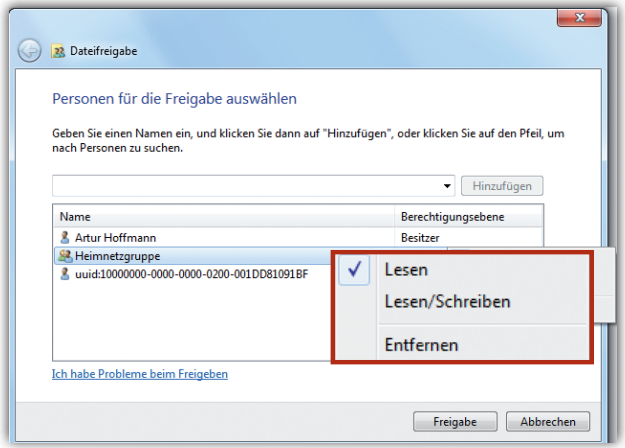
Unter Windows XP doppelklicken Sie in der „Systemsteuerung“ auf „System“ und bringen das Register „Computername“ nach vorne. Bei Vista und Windows 7 wählen Sie

„System", „Erweiterte Systemeinstellungen" und „Computername". Tippen Sie bei „Computerbeschreibung" einen Text ein, der die Funktion des Rechners erläutert.

Ein Klick auf „Ändern" öffnet einen Dialog, in dem Sie bei „Computername" eine eindeutige Bezeichnung, etwa „Thorstens_Kiste" eintippen. Der Name darf nicht länger als 15 Zeichen sein; Leerzeichen sind verboten. Diese Einschränkungen gelten auch für den Namen der „Arbeitsgruppe". Nach einem Klick auf „OK" informiert Sie Windows, dass die Änderungen erst nach einem Neustart übernommen werden. Folgen Sie dieser Anweisung. Bei den anderen Rechnern Ihres Netzwerkes gehen Sie genauso vor, verwenden aber jedes Mal einen anderen, eindeutigen „Computernamen". Als „Arbeitsgruppe" wählen Sie hingegen stets die gleiche Bezeichnung.

Gemeinsamer Zugriff auf Dateien

Der mit Abstand größte Vorteil, den ein Heim-Netzwerk mit sich bringt, besteht in der gemeinsamen Nutzung von Ordnern und Dateien. Anstatt Kopien benötigter Dokumente als E-Mail-Anhang zu versenden oder per USB-Stick von einem PC auf den anderen zu übertragen, können Sie die Dokumente auf ein freigegebenes Laufwerk oder in einem freigegebenen Ordner ablegen.



***Geben Sie Ordner innerhalb** Ihres Netzwerks frei, können Sie festlegen, welchen Personen der Zugriff gestattet ist.*

Geben Sie ein Laufwerk oder einen Ordner frei, erhalten alle anderen Benutzer im Netzwerk Zugriff auf die darin abgelegten Dateien. Diese Benutzer können den Inhalt des Laufwerks oder Ordners anzeigen, Dateien öffnen, Änderungen speichern, neue Dateien auf dem Laufwerk oder in dem Ordner erstellen und Dateien von dem Laufwerk oder aus dem Ordner löschen. Als Administrator des Heim-Netzwerks können Sie den Zugriff aber auch beschränken, sodass nur ausgewählte Personen oder Gruppen mit den Inhalten arbeiten können, und Sie können auch die Arten des Zugriffs beschränken, den Sie einzelnen Personen oder Gruppen gestatten wollen.

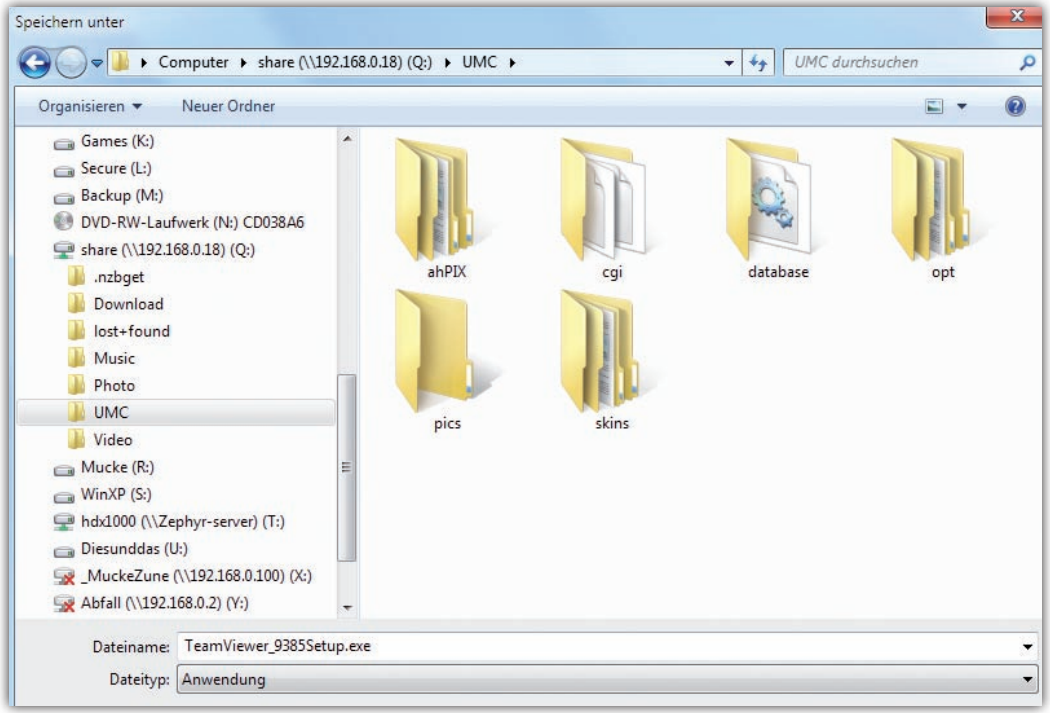
In der Grundeinstellung ist Windows – nicht zuletzt aus Sicherheitsgründen – aber so konfiguriert, dass der Zugriff auf Ordner und Dateien lokal begrenzt ist. Sie müssen dem Betriebssystem also erst einmal mitteilen, dass auch Fremdzugriffe erlaubt sind.

Ordner im Netzwerk freigeben

Da Windows XP und seine beiden Nachfolger von Grund auf für den Einsatz im Netzwerk konzipiert wurden, geht die Freigabe von Dateien und Ordnern recht einfach vonstatten. Allerdings gehen wir in diesem Abschnitt davon aus, dass Sie auf allen PCs bereits Benutzerkonten für alle Nutzer, die auf die freigegebenen Ordner zugreifen dürfen, eingerichtet haben. Dies erledigen Sie bei allen Windows-Versionen über „Systemsteuerung" und „Benutzerkonten".

Im „Windows-Explorer" wechseln Sie in das Verzeichnis, das dem freigegebenen Ordner übergeordnet ist. Möchten Sie etwa den Ordner „G:\Fotos\Urlaub 2010" freigeben, müssen Sie in das Verzeichnis „G:\Fotos" wechseln.

Klicken Sie den freizugebenden Unterordner – in diesem Beispiel „Urlaub 2010" – mit der rechten Maustaste an und wählen Sie unter Windows XP im Kontextmenü den Befehl „Freigabe und Sicherheit". Im folgenden Dialog klicken Sie im Bereich „Netzwerkfreigabe



***Nachdem Sie freigegebene Ordner** gemountet – also dauerhaft verbunden – haben, stehen sie Ihnen in allen Windows-Anwendungen zur Verfügung.*

und -sicherheit" auf den Hyperlink „Klicken Sie hier, wenn Sie sich des Sicherheitsrisikos bewusst sind ...". Im anschließenden Hinweis-Dialog „Dateifreigabe aktivieren" klicken Sie auf die Option „Dateifreigabe einfach aktivieren" und bestätigen mit „OK". Die beiden letztgenannten Schritte sind übrigens nur bei der erstmaligen Freigabe einer Ressource durchzuführen.

Wieder im Dialog „Eigenschaften von", klicken Sie bei „Netzwerkfreigabe und -sicherheit" auf die Option „Diesen Ordner im Netzwerk freigeben", tippen bei „Freigabename" eine aussagekräftige Bezeichnung mit maximal zwölf Zeichen ein und aktivieren auch die Option „Netzwerkbenutzer dürfen Dateien verändern". Nach einem abschließenden Klick auf „OK" richten Sie die Freigaben auch auf allen anderen XP-Rechnern des Netzwerkes ein.

Aus Sicherheitsgründen können die Ordner „Dokumente und Einstellungen", „Programme" und „Windows" nicht freigegeben werden, was in der Praxis aber egal ist.

Unter Windows 7 und Vista klicken Sie im Kontextmenü auf „Eigenschaften", bringen das Register „Freigabe" nach vorne und klicken auf „Freigabe". Im folgenden Dialog können Sie auswählen, welche Personen Zugriff auf den Ordner erhalten sollen.

Möchten Sie den gesamten Inhalt des Verzeichnisses für einen bestimmten Benutzer freigeben, klicken Sie auf den Pfeil, wählen im Ausklappmenü das gewünschte Benutzerkonto aus und bestätigen mit „Hinzufügen". Standardmäßig ist der neu hinzugefügte Benutzer nur mit Leserechten ausgestattet.

Wollen Sie ihm hingegen den Vollzugriff erlauben, klicken Sie unter „Berechtigungsebene" auf „Leser", wählen den Eintrag „Mitbesitzer" (Windows Vista) bzw. „Lesen/Schreiben" aus und schließen den Dialog dann per Klick auf „Freigabe" und „Fertig". Um nun auf einen der freigegebenen Ordner zuzugreifen, öffnen Sie den „Windows-Explorer", klicken auf „Netzwerk" bzw. „Netzwerkumgebung" (Windows XP) und öffnen das gewünschte Verzeichnis.

Sollten Sie zur Eingabe von Benutzername und Passwort aufgefordert werden, fehlen

Ihnen die erforderlichen Zugriffsrechte. In diesem Fall müssen Sie an dem Computer, auf dem der freigegebene Ordner gespeichert ist, die Freigabeeinstellungen überprüfen.

Freigegebene Netzwerk-Ordner verbinden

Nachdem Sie nun Dateien und Ordner freigegeben und den Benutzern die entsprechenden Zugriffsrechte erteilt haben, sollten Sie nicht vergessen, besonders häufig genutzte Netzwerk-Ressourcen zu verbinden.

Diese – auch als Mounten bezeichnete – Funktion erleichtert den Zugriff auf freigegebene Ordner, Festplatten und Wechsellaufwerke, da Sie aus allen Windows-basierten Programmen heraus darauf zugreifen können. Und zwar genau so, als würde es sich um ein lokales Laufwerk des eigenen PCs handeln.

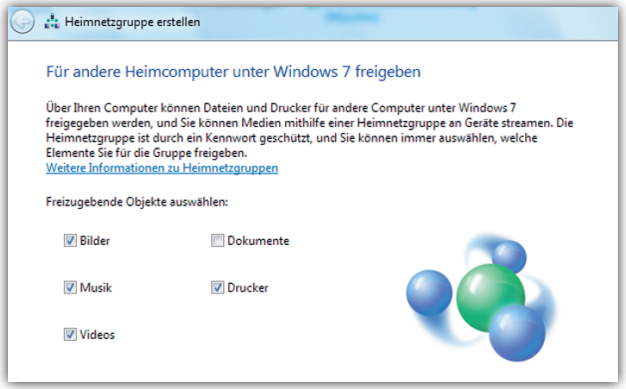
Unter Windows XP klicken Sie auf „Arbeitsplatz", „Netzwerkumgebung" und „Arbeitsgruppencomputer anzeigen". Doppelklicken Sie auf den PC, auf dem sich die freigegebene Ressource befindet. Klicken Sie den Ordner bzw. das zu verbindende Laufwerk mit der rechten Maustaste an und wählen Sie im Kontextmenü den Befehl „Netzlaufwerk verbinden". Im gleichnamigen Dialog wählen Sie bei „Laufwerk" den Buchstaben aus, unter dem das Netzlaufwerk angezeigt werden soll, empfehlenswert sind die letzten Buchstaben des Alphabets. Die Option „Verbindung bei Anmeldung wiederherstellen" muss unbedingt aktiviert werden, damit alle Netzlaufwerke sofort nach dem Start von Windows bereit stehen. Mit „OK" verlassen Sie den Dialog.

Arbeiten Sie mit einer aktuelleren Windows-Version, klicken Sie auf „Computer" und „Netzwerk", doppelklicken auf den gewünschten PC und klicken das zu verbindende Verzeichnis mit der rechten Maustaste an.

Wählen Sie „Netzlaufwerk zuordnen" bzw. „Netzlaufwerk verbinden" (Windows 7), entscheiden Sie sich für ein „Laufwerk", aktivieren Sie „Verbindung bei Anmeldung wiederherstellen" und bestätigen Sie mit „Fertig stellen".

Alle permanent verbundenen Netzlaufwerke werden fortan direkt im „Arbeitsplatz" angezeigt. Wollen Sie eine solche Verknüpfung wieder entfernen, klicken Sie einfach mit der rechten Maustaste auf das entsprechende Laufwerksicon und wählen im Kontextmenü den Befehl „Trennen" aus.

Tipp: Wollen Sie sich mit einem bestimmten Benutzerkonto bei einer freigegebenen Ressource anmelden, ist das auch kein Problem. Dazu müssen Sie nur im Dialog „Netzlaufwerk verbinden" auf den Link „anderem

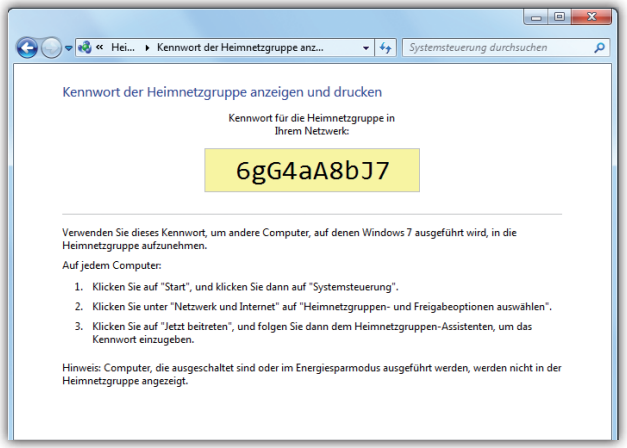


Mithilfe der Funktion „Heimnetzgruppe erstellen" *bauen Sie im Handumdrehen ein Netzwerk aus Windows-7-Rechnern auf.*

Benutzernamen" klicken bzw. auf die Option „Verbindung mit anderen Anmeldeinformationen herstellen" (Windows 7), die entsprechenden Zugangsdaten eintippen und die Änderungen mit einem Klick auf „OK" bestätigen.

Heimnetzgruppen unter Windows 7

Wie bereits kurz angerissen, geht die Einrichtung eines Netzwerks mit Windows 7 kinderleicht vonstatten – sofern alle im LAN eingebundenen Rechner mit diesem Betriebssystem ausgestattet sind. Denn PCs, auf denen Windows 7 installiert ist, lassen sich zu speziellen Heimnetzgruppen zusammenschließen. Ausnahme: Handelt es sich um zwei Note- oder Netbooks, auf denen jeweils Windows 7 Starter zum Einsatz kommt, funktioniert es nicht.



***Ein Passwort genügt, um anderen Windows-7-PCs** den Zugang zur Heimnetzgruppe zu erlauben.*

Der Grund: In Bezug auf Heimnetzgruppen bestehen zwischen den Windows-7-Versionen Unterschiede. Während von Windows 7 Home Premium aufwärts alle Versionen Heimnetzgruppen auch anlegen können, ist es mit der Starter-Version nur möglich, einer bereits vorhandenen Heimnetzgruppe beizutreten.

Wichtig für die Nutzung von Heimnetzgruppen: Auf allen beteiligten PCs muss das Netzwerk als „Heimnetzwerk" deklariert werden. Ob Sie sich für diese Einstellung entschieden haben, erfahren Sie durch einen Blick in das „Netzwerk- und Freigabecenter", das Sie in der „Systemsteuerung" finden.

Tipp

Nicht schlafen gehen!

Achten Sie darauf, wenn Sie die Freigaben einer Heimnetzgruppe nutzen wollen, dass keiner der beteiligten Rechner die Möglichkeit bekommt, den Energiespar-Modus zu aktivieren oder gar in den Ruhezustand zu gehen. Schalten Sie diese Funktionen aus. Ansonsten ist nämlich keine Verbindung mehr möglich, sodass Sie keinerlei Freigaben nutzen können.

Heimnetzgruppe anlegen

In diesem Beispiel möchten wir einen Desktop-PC und ein Netbook zu einem Heimnetzwerk zusammenschließen. Der Desktop-PC ist bereits mit einem WLAN verbunden. Sobald das Netbook Kontakt mit dem WLAN aufgenommen hat und auf beiden Rechnern die Auswahl „Heimnetzwerk" getroffen wurde, meldet sich Windows 7 mit dem Dialog „Heimnetzgruppe erstellen" zu Wort.

Praktisch: Im nächsten Schritt legt Windows 7 selbst ein Kennwort fest, das Sie für die neue Heimnetzgruppe verwenden müssen. Notieren Sie sich das Kennwort. Der Zugangscode lässt sich später jederzeit problemlos über die Systemsteuerung und den Punkt „Heimnetzgruppe" ändern. Für jede weitere Heimnetzgruppe wird es übrigens neu generiert.

Damit ist im „Computer" beider Rechner nun der neue Eintrag „Heimnetzgruppe" vorhanden. Klicken Sie diesen auf dem zweiten Rechner an – im unserem Beispiel ist das das Netbook – um der Heimnetzgruppe beizutreten. Legen Sie eigene Freigaben fest und geben Sie das soeben notierte Kennwort ein. Anschließend erhalten Sie eine Meldung über den erfolgreichen Beitritt zur Heimnetzgruppe. Nun können Sie auf die Freigaben des anderen Rechners zugreifen.

Solch ein Heimnetzwerk ist besonders dann nützlich, wenn Sie daheim an verschiedenen Rechnern sitzen. Angenommen, Sie wollen von Ihrem Notebook aus per E-Mail ein Foto versenden, das auf dem Desktop-PC gespeichert ist. Kein Problem, wenn Sie beide Geräte in einer Heimnetzgruppe verwalten: Öffnen Sie das Fenster „Bibliotheken" und klicken Sie unter „Heimnetzgruppe" auf den Namen des zweiten PCs. Anschließend klicken Sie auf „Bilder" und suchen das gewünschte Foto. Am einfachsten kopieren Sie dieses dann in die Zwischenablage und fügen das Foto direkt in die E-Mail ein.

Heimnetzgruppen verwalten

In der „Systemsteuerung" finden Sie unter „Netzwerk und Internet" den Eintrag

„Heimnetzgruppen- und Freigabeoptionen auswählen". Damit können Sie die Einstellungen für die Heimnetzgruppe ändern oder ein anderes Kennwort einstellen. Alternativ klicken Sie im „Computer" den Eintrag „Heimnetzgruppe" mit der rechten Maustaste an und wählen „Heimnetzgruppen-Einstellungen ändern".

Wer zum Beispiel Filme oder Musik zu anderen Geräten in der Heimnetzgruppe streamen will, muss diese Funktion noch einmal explizit einschalten. Setzen Sie dazu bei „Medien für Geräte freigeben" einfach ein Häkchen.

Über den Link „Medienstreamingoptionen auswählen" lässt sich genauer festlegen, was gestreamt werden kann. Lassen Sie sich über „Geräte anzeigen in" wirklich „Alle Netzwerke" anzeigen. Falls Sie etwa ein entsprechendes Abspielgerät, zum Beispiel eine Multimedia-Festplatte oder einen der neueren Flachbildschirme mit WLAN-Anbindung haben, werden sie in dieser Liste aufgeführt.

Zu jedem angezeigten Gerät werden weitere Funktionen wie „Anpassen" eingeblendet, sobald Sie mit dem Mauszeiger darauf zeigen. Sie können so für jedes beliebige Gerät innerhalb Ihrer eigenen Heimnetzgruppe ganz genau festlegen, welche Inhalte gestreamt werden sollen. Auf diese Weise lässt sich unter anderem festlegen, ob allgemeine Standardeinstellungen gelten oder ob zum Beispiel ein Gerät nur Medien erhalten darf, die mindestens eine Bewertung von drei oder mehr Sternen erhalten haben, oder mindestens fünf Wochen alt sind.

Auch wer seinen Rechner kurzfristig aus einer Heimnetzgruppe herausnehmen will, findet natürlich in den Heimnetzgruppen-Einstellungen die Lösung. Über „Heimnetzgruppe verlassen" kann man den Beitritt beenden. Aber Vorsicht: Wird dies auf dem Rechner vorgenommen, der auch die bisherige Heimnetzgruppe erstellt hat, wird die gesamte Heimnetzgruppe gelöscht.

Sie müssen anschließend eine neue anlegen, wobei natürlich auch wieder ein neues Kennwort vergeben wird. Die erneute Einrichtung ist ebensowenig kompliziert, allerdings kann die Einrichtung der Freigaben durchaus einige Zeit dauern.

A. Hoffmann

Mehr Sicherheit mit Firewalls

Ganz gleich, ob kabelgebundenes Netzwerk oder WLAN – sobald der Computer mit dem Internet verbunden ist, herrscht höchste Gefahr. Wir zeigen Ihnen, **wie Sie Ihren PC nachhaltig schützen.**

Desktop-Firewall installieren und der Rechner ist fast so sicher wie Fort Knox – nach diesem Motto verfahren immer noch zahlreiche Anwender. Hierbei wird allerdings oftmals übersehen, dass eine Firewall-Software den eigenen Computer nur dann nachhaltig schützen kann, wenn der Anwender sich um die Konfiguration kümmert. Ansonsten stellen Firewalls nichts weiter als Programme dar, die unnötig viele Ressourcen verbrauchen und dem Anwender ein trügerisches Gefühl von Sicherheit vermitteln. Was PC-User brauchen, ist ein Rundumschutz, in dem die Firewall nur eine von mehreren Komponenten darstellt.

***Desktop-Firewalls bieten Schutz** – sofern sie optimal genutzt werden. Und dazu zählen in erster Linie die perfekte Einrichtung und der sachgerechte Umgang mit den Warnmeldungen.*

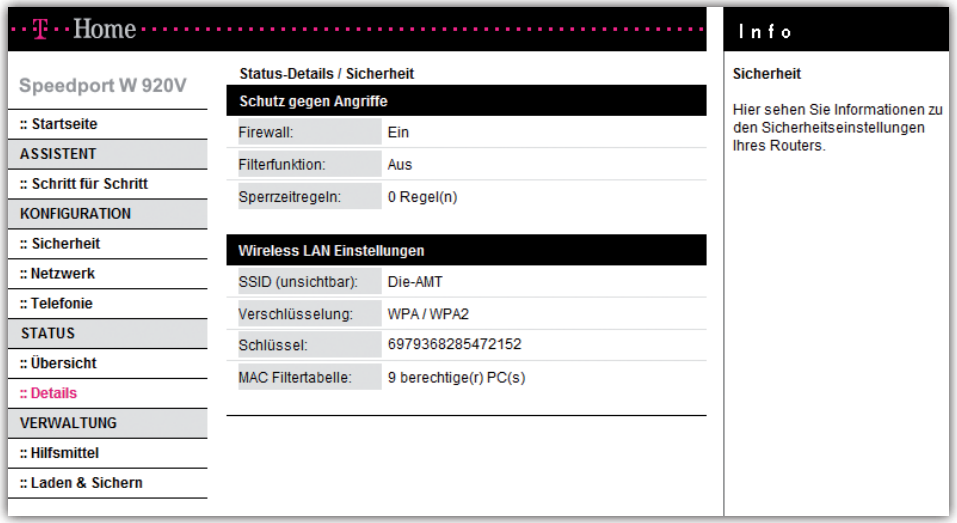
Wir zeigen Ihnen, wie Desktop-Firewalls funktionieren, wie sie ausgetrickst werden können und wie Sie die Schutz-Tools in ein umfassendes Sicherheitskonzept integrieren, um Ihren Computer in einen digitalen Hochsicherheitstrakt zu verwandeln.

Grundlagen: So arbeiten Firewalls

Firmen betreiben in der Regel hardwarebasierte Firewalls, da sie maximalen Schutz versprechen. Solche Firewalls sind allerdings teuer und die Administration ist zeitaufwendig.

Aus diesem Grund greifen Anwender oft zu kostenlosen Software-Lösungen wie zum Beispiel PC Tools Firewall Plus 6.0 (www.pctools.com/de/, ZoneAlarm Firewall 2010 (www.zonelabs.com) und Sunbelt Personal Firewall 4.6 (www.sunbeltsoftware.com) oder schalten die in Windows integrierte Firewall ein. Inzwischen bieten auch die allermeisten aktuellen WLAN-Router eine eigene interne Firewall.

All diese Lösungen untersuchen die ein- und ausgehenden Datenpakete und filtern sie bei Bedarf. Zu den für die Firewall wichtigen Informationen gehören die IP-Adressen von Quell- und Zielrechner sowie die Angabe, über welchen Port mit welchem Protokoll das Paket verschickt beziehungsweise



***Auch in aktuellen WLAN-Routern** ist meist eine Firewall integriert.*

***Gerade weil Firewalls umgangen werden,** ist TeamViewer ein beliebtes Fernwartungs-Tool.*

empfangen wird. Desktop Firewalls haben zusätzlich einen Anwendungsfilter (Application Control), über den man installierten Programmen gezielt den Zugriff auf das Internet erlauben oder verbieten kann. Viele Firewall-Programme bieten eine ganze Reihe von Zusatzfeatures wie einen Lernmodus, der die Filterregeln dem Verhalten des Anwenders anpasst, oder Content-Filter, die ActiveX-Komponenten, Java-Skripte und Ähnliches blockieren. Firewalls mit dieser Funktion werden häufig als „Webshield" oder „Web Application Firewall" angeboten. Verstärkt wird inzwischen auch ein so genannter „Stealth Modus" verkauft. Hier blockiert die Firewall einfach sämtliche Anfragen an ungenutzte Ports (Deny-Mode).

Ein wichtiges Feature, das in fast allen Hardware-Firewalls zu finden ist, heißt „Stateful Packet Inspection (SPI)". Hier werden die gewöhnlichen, starren Filterregeln dynamisch erweitert. Starten Sie beispielsweise den Browser, werden im Hintergrund mehrere Verbindungen parallel aufgebaut und verschiedene Dienste gestartet, die oft gleichzeitig Datenpakete verschicken und empfangen. Die SPI bezieht bei der Überprüfung dieser Datenpakete den Status der Verbindung mit ein. Gehört das Paket zu einer bestehenden Verbindung? Wird es vom Browser benötigt, um ein Antwortpaket zu erhalten? Anhand dieser und vieler weiterer Abfragen entscheidet die Firewall, ob das Paket blockiert oder durchgelassen wird.

Welches Filterverfahren die Firewall auch benutzt, der Zweck ist immer der gleiche: das Abblocken verdächtiger Pakete, die aus dem Internet an Ihren PC geschickt werden (Schutz gegen Angriffe von außen).

Ist Malware bereits auf Ihre Festplatte gelangt, kann die Firewall allerdings nicht mehr helfen – auch wenn einige Hersteller das immer noch felsenfest behaupten. Warum das so ist, zeigen wir Ihnen im nächsten Abschnitt.

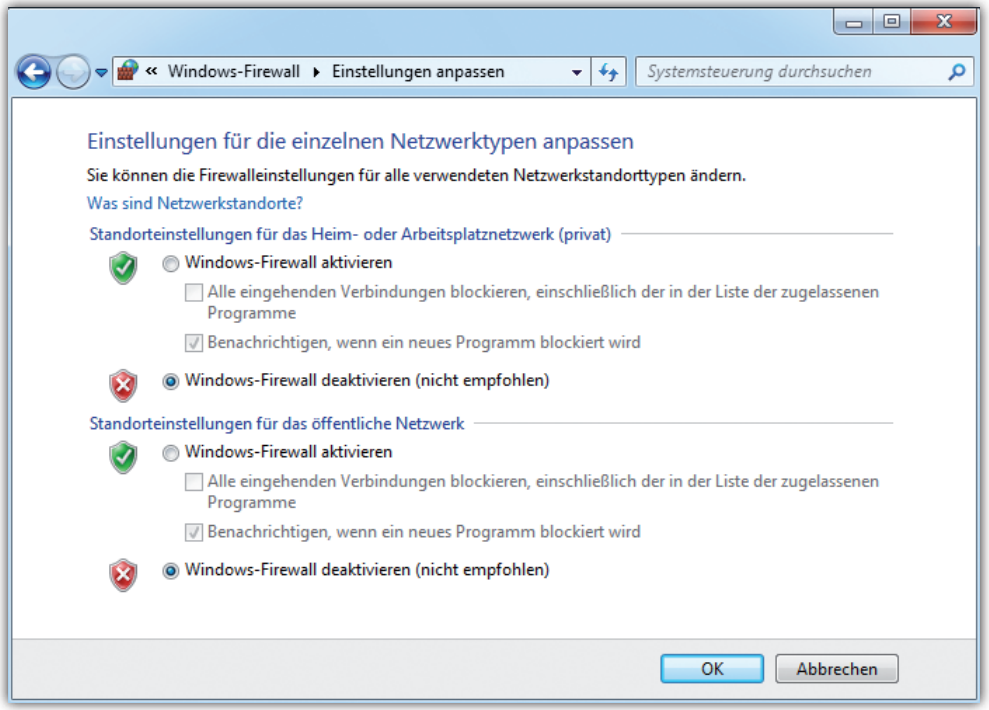
Kein großes Problem: Die Firewall austricksen

Eigentlich, möchte man meinen, sollte die Paketfilterung den PC zuverlässig schützen. Tut sie aber nicht. Wer weiß, wie die

grundlegende Paketfilterung funktioniert, kann sie relativ einfach austricksen – auf folgende Art und Weise:

ANGRIFF VON AUSSERHALB: Bevor ein Hacker die Firewall überwinden kann, muss er herausfinden, welche Sicherheitslücken auf einem Computer vorhanden sind. Das kann ein Bug im Browser sein, ein falsch konfigurierter Windows-Dienst oder eine aus dem Internet erreichbare Datei- und Druckerfreigabe. Was ebenfalls häufig vorkommt: Der Anwender öffnet einen unbekannten Mail-Anhang und fängt sich damit einen Trojaner ein, oder er besucht eine Website, die Schadcode auf den Rechner schleust. All diese Angriffe zielen quasi an der Firewall vorbei. Niemand wird seinem MailProgramm per Filterregel den Internetzugang sperren. Empfängt oder versendet Outlook eine Mail, die einen Trojaner enthält, wird die Firewall den verseuchten elektronischen Brief deshalb ungehindert durchlassen.

ANGRIFF VON INNEN: Ist der Trojaner auf Ihr System gelangt, erhält er die gleichen Benutzerrechte wie Sie und kann sich problemlos als Systemdienst tarnen. Das können Sie – völlig legal – selbst testen, denn vom Funktionsprinzip her unterscheidet sich ein Trojaner kaum von gängiger PC-Fernsteuerungs-Software.



***Bei Einsatz einer Desktop-Firewall** ist das entsprechende Windows-Tool natürlich zu deaktivieren.*

Das beliebte Remote-Tool TeamViewer 5.1 etwa wirbt auf www.teamviewer.com unter „Vorteile" ganz offen damit, dass Firewalls, NAT-Router und gesperrte Ports kein Problem darstellen. TeamViewer installiert sich als Windows-Dienst und erhält damit die gleichen Rechte wie der Benutzer „System".

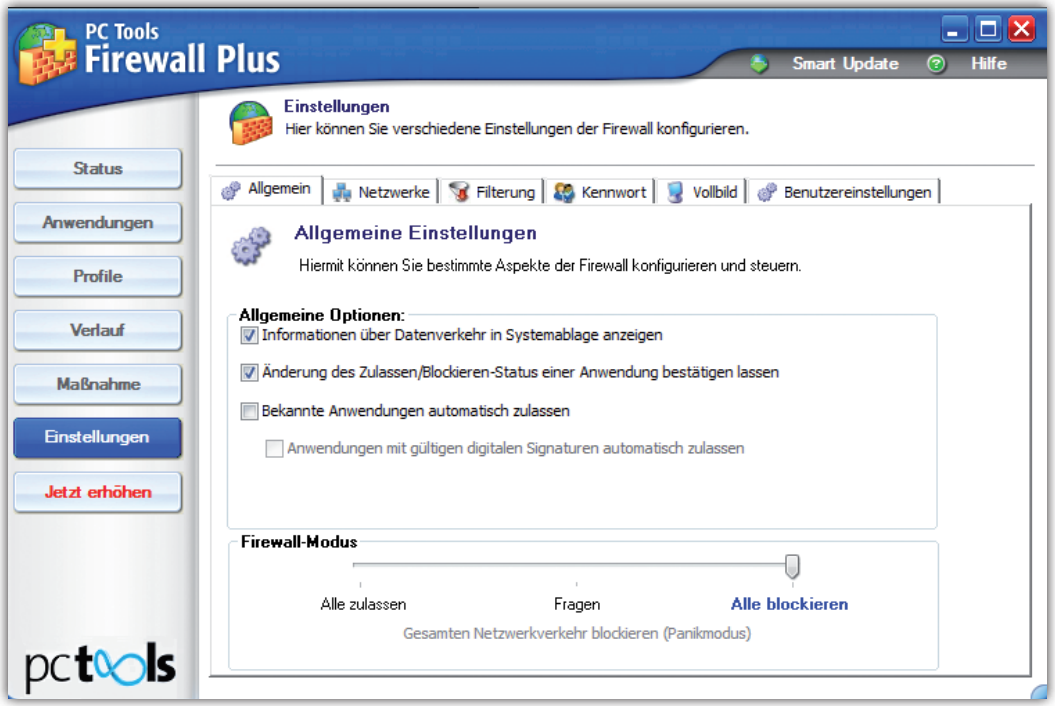
ANDERS AUSGEDRÜCKT: Das Fernwartungs-Tool erhält die gleichen Handlungsmöglichkeiten wie Windows. Zudem kommuniziert TeamViewer über den für HTTP-Verbindungen wichtigen Port 80, der praktisch nie gesperrt ist. In diesem Fall wäre nämlich die Internetverbindung gekappt. Die Firewall ist somit gegen TeamViewer völlig machtlos, weil sie weder Windows noch den Internetzugang blockieren kann.

Wäre TeamViewer bösartig, würde das Tool nun Bankdaten, geheime Dokumente und vieles mehr an einen anderen Rechner übertragen, ohne dass die Firewall Alarm schlägt.

Absichern: Der PC wird zur Festung

Damit stellt sich eine berechtigte Frage: Wozu benötige ich dann eigentlich eine Firewall?

Antwort: Richtig konfiguriert liefert sie wichtige Infos über die Systemsicherheit, verhindert, dass Hacker von außen Sicherheitslücken ausspionieren, und informiert Sie darüber, welche Programme Kontakt mit dem Internet aufnehmen möchten. Gegen gut getarnte Trojaner und ähnliche Schädlinge ist sie aber machtlos. Sie benötigen zusätzliche Tools, um auch Malware, die sich bereits auf der Festplatte eingenistet hat, zu bekämpfen. Bauen Sie nun auf Basis der genannten Angriffs-Szenarien einen Schutzwall auf, der Bedrohungen tatsächlich fernhält.



***Sie können bei einer Desktop-Firewall festlegen**, welche Programme mit dem Internet kommunizieren dürfen.*

ALLES ABSCHALTEN: Um Ihnen das Einrichten der Firewall zu demonstrieren, verwenden wir als Basis das kostenlose Schutzprogramm PC Tools Firewall Plus 6.0 (www.pctools.com/de/). Bei kommerziellen Lösungen wie F-Secure Internet Security 2011 (www.f-secure.de, 30 Euro für 12-Monats-Lizenz), Outpost Firewall Pro 7.0 (www.agnitum.de, 50 Euro für Lizenz auf Lebenszeit) oder Norton Internet Security 2010 (www.symantec.de, 40 Euro für 12-Monats-Lizenz) sollten Sie die vom Hersteller empfohlenen Einstellungen verwenden, denn hier sind verschiedene Komponenten wie Viren- und Spywareschutz aufeinander abgestimmt. Bevor Sie eines der Programme starten, dürfen Sie keinesfalls vergessen, die in Windows integrierte Firewall zu deaktivieren. Sonst blockieren sich die beiden Sicherheits-Tools gegenseitig. Mehr ist in diesem Fall nicht besser (siehe Kasten „Die 10 goldenen Firewall-Regeln"). Dazu wechseln Sie zur Systemsteuerung, klicken in der Kategorien-Ansicht auf „System und Sicherheit", wählen „Windows-Firewall" und klicken auf „Windows-Firewall ein- oder ausschalten".

Eine weitere Alternative wäre die Hardware- beziehungsweise Router-Firewall. Letztere lässt sich oft nicht abschalten. Hängen am Router zusätzliche Geräte wie eine NAS-Festplatte, dürften Sie das auch gar nicht, weil dieses Gerät dann nicht mehr geschützt wäre. Besitzer derart ausgestatteter Router schalten daher besser die Desktop-Firewall ab und gewinnen somit wertvolle Systemressourcen zurück.

Zurück zu unserem Praxisbeispiel: Bei der Installation der PC Tools Firewall Plus lehnen Sie im dritten Schritt des Assistenten die Installation der „Google Toolbar" ab, entscheiden sich dann für „Experte" und starten den Rechner neu.

Wer darf was: Regeln festlegen

Nach dem Hochfahren meldet die PC Tools Firewall Plus 6.0, dass ein neues Netzwerk erkannt wurde. Handelt es sich dabei um Ihr heimisches Netzwerk, entscheiden Sie sich bei „Vertrauensstufe für dieses Netzwerk auswählen" für „Privat" und bestätigen mit „Übernehmen". Nun steht die Einrichtung auf dem Programm. Doppelklicken Sie in der Taskleiste auf das Symbol des Tools, wählen Sie auf der Bedienoberfläche „Einstellungen" und stellen Sie im Register „Allgemein" den Schieberegler auf „Alle blockieren".

Deaktivieren Sie außerdem „Bekannte Anwendungen automatisch zulassen", denn dabei könnte es sich um getarnte Trojaner handeln. Ist das geschehen, starten Sie zur Überprüfung mit dem Tastenkürzel [Strg]+[Alt]+[Esc] den Windows-Task-Manager. Im Register „Netzwerk" darf kein einziges gesendetes oder empfangenes Datenpaket angezeigt werden. Ist der Rechner abgedichtet, ziehen Sie den oben erwähnten Schieberegler zurück auf die Einstellung „Fragen". Anschließend starten

Die 10 goldenen Firewall-Regeln

1 Nur eine einzige Firewall einsetzen
Mehrere gleichzeitig laufende Firewalls stören sich und legen den Rechner lahm.

2 Alle unbekannten Programme und Dienste blocken
Der Windows-Dienst „wklsd45xqy.exe" möchte ein Datenpaket versenden? Verbieten Sie es, solange Sie nicht wissen, was genau dieser Dienst macht und wer der Empfänger der Datenpakete ist.

3 Die Log-Datei enthält wertvolle Sicherheitsinformationen
Nur durch einen Blick in die Protokolldatei der Firewall erfahren Sie, was an den Ports Ihres Rechners passiert.

4 Die Firewall benötigt die Unterstützung anderer Programme
Firewalls können weder Viren noch Trojaner aufhalten. Installieren Sie deshalb zusätzlich einen Virenscanner, ein Antispyware-Tool und ein Intrusion-Detection-System.

5 Sicherheitslücken müssen umgehend geschlossen werden
Hat der Browser ein Leck, marschieren Schädlinge geradewegs durch – ohne dass die Firewall etwas merkt. Regelmäßige Updates sind deshalb Pflicht.

6 Ein NAT-Router bietet nur unzureichenden Schutz
Router mit einer integrierten automatischen Adressumsetzung (Network Adress Translation) erraten mittels eines als Heuristik bezeichneten Verfahrens den richtigen Empfänger. Damit umgehen sie aber die eindeutige Identifizierung via IP-Adresse. Genau das machen sich Hacker zunutze.

7 Nur wirklich benötigte Windows-Dienste laufen lassen
Jeder Windows-Dienst, der ohne Ihr Wissen im Hintergrund läuft, ist eine glatte Einladung für Hacker und Viren. Schalten Sie alles ab, was nicht benötigt wird.

8 Kommunikation mit dem Internet im Zweifelsfall blockieren
Firewalls können Anfragen an nicht benutzte Ports kommentarlos abblocken (Stealth-Modus) oder eine Antwort wie „Dienst nicht erreichbar" an den Absender schicken (Reject-Modus). Letzteres unterbindet unnötige Alarmmeldungen.

9 Alarmmeldungen müssen aufmerksam gelesen werden
Öffnet sich das Firewall-Fenster, machen Sie sich die Mühe und lesen Sie, was Ihnen das Schutz-Tool mitteilen will. Andernfalls gewähren Sie Trojanern freien Zutritt.

10 Auch das Betriebssystem muss richtig konfiguriert werden
Sie gestatten jedermann im Internet den Zugriff auf Ihre freigegebenen Dateien und Drucker? Da kann die beste Firewall nicht mehr helfen. Deswegen muss auch Windows auf maximale Sicherheit getrimmt werden.

***Auf Webseiten wie Trojaner-Info** erfahren Sie, welche Ports von Schadsoftware genutzt werden.*

Sie Ihren Webbrowser und gewähren ihm über „Zulassen" die Internetverbindung. Mittels „Anwendungen" können Sie in den Spalten „Ein" und „Aus" zusätzlich bestimmen, ob das Programm Daten nur senden, nur empfangen oder beides darf. In der Einstellung „Regelbasiert" berücksichtigt die Firewall diese individuell festgelegten Filterregeln.

Auf die gleiche Weise richten Sie nacheinander Regelungen für das Mailprogramm, den Virenscanner und andere Tools ein, die üblicherweise Internetzugang verlangen.

Beachten Sie hierbei ein weiteres Firewall-Gebot: Blockiere alles, was du nicht kennst. Sagt Ihnen der Name eines unter „Anwendungen" aufgeführten Programms oder Dienstes nichts, suchen Sie im Internet nach Informationen. Zusätzlich können Sie über „Maßnahme" feststellen, über welchen Port das unbekannte Programm kommuniziert und per Klick auf „Verbindungen" unter „Externe Adresse" die IP-Adresse des Zielrechners sehen. Geben Sie diese auf der Website www.domaintools.com/reverse-ip ein. Auf diese Weise erfahren Sie, wer hinter dieser Adresse steckt.

Nachhaken: Sicherheitscheck durchführen

Zu guter Letzt prüfen Sie noch, ob die Firewall den Rechner tatsächlich für Hacker unsichtbar macht. Besuchen Sie die Website http://webscan.security-check.ch und lassen Sie dort gegen eine einmalige kostenlose Registrierung den „Full Scan" durchführen. Auf diese Weise erfahren Sie, ob und was ein Hacker über Ihren Rechner herausfinden könnte. Haben Sie die Firewall richtig konfiguriert, erfährt der Möchtegern-Spion natürlich überhaupt nichts.

Die nächste Anlaufstelle ist die Logdatei der Firewall. Dort erfahren Sie, wann ein Datenpaket gesendet und empfangen wurde, ob es blockiert oder durchgelassen wurde, über welchen Port die Übertragung erfolgte und wer es erhielt. Klicken Sie in der PC Tools Firewall auf „Verlauf", um das Protokoll aufzurufen. Ausgehende Pakete sind dort mit einem blauen Pfeil gekennzeichnet, empfangene mit einem grünen. Die unter „Quelle/Ziel" angegebene IP-Adresse können Sie mit der oben genannten Reverse-IP-Suche ganz einfach aufschlüsseln. Ob der angegebene Port besonders häufig von Trojanern benutzt wird, finden Sie beispielsweise über die informative Website www.trojaner-info.de/port.shtml heraus.

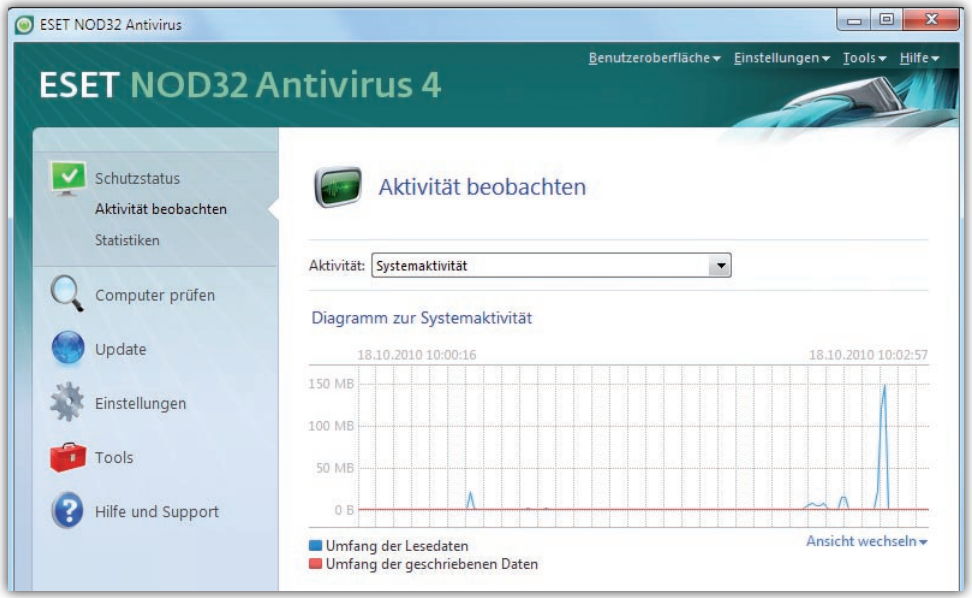
Jetzt haben Sie alles weitgehend unter Kontrolle. Hacker können von außerhalb Ihren Rechner nicht mehr identifizieren und somit auch keine potenziellen Schwachstellen mehr aufspüren. Um auch Angriffe von innen abzuwehren, installieren Sie nun weitere essenzielle Security-Tools.

Unumgänglich: Der PC-Rundumschutz

Gelangt trotz richtig konfigurierter Firewall ein Schädling auf Ihre Festplatte, kann er von einem Virenscanner erkannt und entfernt werden. Verwenden Sie bei akutem Befall das kostenlose Dr. Web CureIT 6.00 (www.freedrweb.com), langfristigen Schutz bieten unter anderem die ressourcenschonenden Virenscanner F-Prot Antivirus 6 (www.f-prot.com, 25 Euro für 12-Monats-Lizenz) und Eset NOD32 Antivirus 4.0 (www.eset.com, 30 Euro für 12-Monats-Lizenz).

Der Virenscanner kann aber nur helfen, wenn die Malware dem Hersteller bekannt ist. Er entwickelt in diesem Fall eine Signatur, die es dem Tool ermöglicht, den Schädling zu identifizieren und zu neutralisieren.

Die kostenlosen Tools LauschAngriff 1.2.5 (www.softwareok.de/?seite=Freeware/LauschAngriff) und Snort 2.8.6.1 (www.snort.org) hingegen helfen gegen Bedrohungen, die noch gänzlich unbekannt sind – so genannte Zero-Day-Exploits. Aber auch der Packet-Sniffer Wireshark (www.wireshark.org) stellt eine große Hilfe dar. LauschAngriff protokolliert alle Änderungen an Dateien und Registry, das englischsprachige Snort eignet sich zum Enttarnen von Trojanern.



***Ein Virenscanner ist ebenfalls** unumgänglich, um den eigenen PC nachhaltig zu schützen.*

Ihre nächste Aufgabe besteht darin, gegen Sicherheitslücken vorzugehen. Aktivieren Sie dazu unbedingt das automatische Windows-Update! Die installierten Anwendungen flicken Sie mit dem Secunia Personal Software Inspector 1.5.0.2 (http://secunia.com/vulnerability_scanning/personal/), einem Tool, das auf sicherheitsrelevante Hotfixes spezialisiert ist.

All diese Schutzmaßnahmen versagen allerdings komplett, wenn Sie E-Mails von Unbekannten öffnen oder auf dubiosen Websites surfen. Denn der beste Rechnerschutz sind immer noch Sie selbst.

Artur Hoffmann