müssen lediglich einige Sicherheitsfunktionen aktivieren.

9. Die beste Verschlüsselung

Die meisten Router bieten drei Verschlüsselungstechniken an: WEP, WPA und WPA2. WEP gilt schon lange als knackbar und sehr unsicher. Vor Kurzem wurde auch WPA geknackt, und deshalb ist nun WPA2 die beste Empfehlung.

Wenn Ihr Windows-XP-Notebook den WPA2-Standard nicht beherrscht, fehlt nur ein Betriebssystem-Update. Sobald Sie das Service Pack 3 installiert haben, können Sie auch WPA2 einsetzen.

10. Starkes Passwort wählen

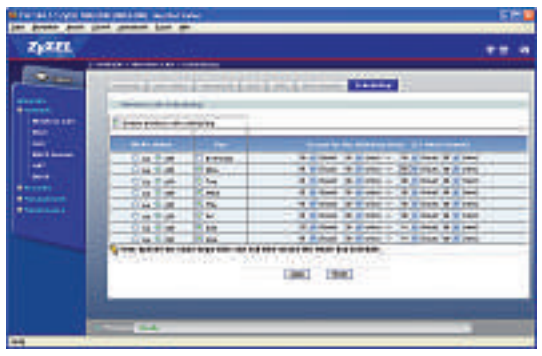
Mit Spezial-Tools gelingt Hackern meist schnell der Zugang zu einem Netz, wenn ein einfaches Passwort verwendet wurde. Viele verwenden leichtsinnig Vor- oder Familiennamen oder etwa den Namen des Hundes. Viel sicherer ist ein Passwort aus Gross- und Kleinbuchstaben sowie Zahlen und Sonderzeichen. Wenn Sie das WLAN-Passwort einmal vergessen, dann können Sie es immer wieder in der Oberfläche des Routers nachlesen.

11. Automatische Verbindung

Viele Router bieten eine sichere, automatische Verbindung eines neuen Clients, etwa eines Netbooks mit USB-WLAN-Stick. Das sogenannte Wi-Fi Protected Setup, kurz WPS, starten Sie meist mit einem Knopf am Router. Danach drücken Sie innerhalb von 30 Sekunden ein Knöpfchen am USB-WLAN-Stick, und die Verbindung ist hergestellt und gesichert.

Bei anderen Geräten, etwa einer Fritzbox von AVM, reicht es, einen Fritz-Stick am Router kurz anzustecken. Der USB-Stick übernimmt dann alle Sicherheitseinstellungen und überträgt sie nach dem Einstecken am Netbook automatisch. Auch hier steht dann schnell eine sichere Verbindung bereit.

Beste Funkleistung: Achten Sie bei Ihrem n-Router darauf, dass die Antennen mindestens sechs Zentimeter auseinander stehen.



Nachtabschaltung: Hier schalten Sie Ihr WLAN zeitgesteuert nachts aus. Das spart nicht nur Strom, sondern unterbindet auch nächtliche Zugriffsversuche.

12. Verstecktes WLAN

Damit Ihr Netz für andere nicht sichtbar ist, schalten Sie die SSID ab. Das ist normalerweise der Name Ihres Funknetzes, der für jeden sichtbar ist. In den WLAN-Einstellungen Ihres Routers finden Sie Optionen wie *SSID unsichtbar machen* oder *Disable SSID Broadcast*. Aktivieren Sie diese Einstellung.

13. Zugang sperren

Jede Hardware besitzt eine besondere MAC-Adresse in der Form "08:00:20:ae:fd:7e". Auch jedes WLAN-Modul hat eine solche Kennung. Legen Sie zur zusätzlichen Sicherheit fest, dass nur bestimmte WLAN-Module freien Zugriff auf Ihr Funknetz haben. Diese Funktion nennt sich in den meisten Routern MAC-Access-List.

Die MAC-Adresse Ihres Windows-PCs finden Sie so heraus: Wählen Sie *Start*, *Systemsteuerung*, *Netzwerk- und Internet-Verbindungen*, *Netzwerkverbindungen*. Klicken Sie dann mit der rechten Maustaste auf *Drahtlose Netzwerkverbindung* und wählen Sie im Kontextmenü *Status*. Wechseln Sie zu *Netzwerkunterstützung*, *Details…* Die im Router einzutragende MAC-Adresse finden Sie unter *Physikalische Adresse*.

14. Offene Ports schliessen

Offene Ports eines Routers laden zu Angriffen aus dem Internet ein. Prüfen Sie deshalb unbedingt, welche Ports bei Ihrem Router geöffnet sind. In der Bedienoberfläche Ihres Routers findet sich meist der Punkt *Ports* oder *Ports Forwarding*. Dort deaktivieren Sie offene Ports und sorgen so für mehr Sicherheit.

15. Passwort für den Router

Fast jede Router-Bedienoberfläche lässt sich zusätzlich per Passwort schützen. Viele Anwender machen das nicht und wiegen sich in trügerischer Sicherheit, da der Zugriff nur im eigenen Netzwerk möglich ist. Doch einige Trojaner versuchen sofort nach der Infektion des PCs einen Zugriff auf den Router. Dort stellen sie dann per Skript Ports um oder öffnen diese. Selbst wenn der Trojaner gefunden wird, hat er seinen Job bereits unbemerkt erledigt. Ist allerdings der Zugriff auf die Oberfläche per Kennwort geschützt, passiert zumindest dem Router nichts.

Kanal-Scanner: Die Fritzbox zeigt, welche Kanäle bereits belegt sind.

16. Fernzugriff abschalten

Viele Router lassen sich auch über das Internet verwalten. Das ist vielleicht für einen Supportmitarbeiter nötig, aber ansonsten stellt es ein Sicherheitsrisiko dar. Deaktivieren Sie sicherheitshalber permanent den Fernzugriff. Der Menüeintrag im Router lautet meist *Remote Control*, *Fernzugriff* oder *Fernwartung*.

17. WLAN-Nachtabschaltung

Wenn Sie Ihr WLAN nachts nicht brauchen, dann nutzen Sie die zeitgesteuerten Abschaltfunktionen des Routers. Legen Sie etwa fest, dass das WLAN sich ab 2 Uhr nachts abschaltet und um 10 Uhr morgens automatisch wieder anschaltet. Das ist nicht nur sicherer, sondern spart auch noch Energie ein.

Profi-Tipps

Viele WLAN-Router haben Spezialfunktionen für Multimediastreaming, das Priorisieren von Voice-over-IP-Paketen oder die Nutzung von UPnP. Einige besitzen USB-2.0-Schnittstellen, über die eine externe Festplatte oder ein Multifunktionsdrucker angeschlossen werden kann. D-Link hat seinem neuen Router einen BitTorrent Client hinzugefügt und ermöglicht mit der NAS-Funktion, einen NAS- und FTP-Server zu betreiben.

18. Streaming im Netz

Wenn Sie öfters Filme über Ihr WLAN streamen, etwa von einer Netzwerkfestplatte auf einen Multimediaplayer, dann kann es im Film zu Aussetzern kommen. Das Problem liegt dabei oft an der Priorität des Streams im heimischen Netz. Viele Router bieten eine Möglichkeit, festzulegen, wie die Daten behandelt werden sollen. Der Router analysiert dafür kleine Datenpakete und erkennt so, um welche Daten es sich handelt. Meistens nennt sich die Funktion im Router-Menü *Wi-Fi Multimedia*, kurz *WMM*. Aktivieren Sie diese Option, wenn Sie oft Filme streamen.

19. UPnP birgt Gefahren

Eine beliebte Funktion in Routern ist UPnP. Mit diesem Universal Plug & Play spricht eine Windows-Anwendung andere Geräte im Netzwerk an. So arbeiten etwa ein externes Internetradio und eine Windows-Software per Mausklick zusammen.

Zugangspasswort: Schützen Sie auch den internen Zugang zur Routeroberfläche per Passwort.

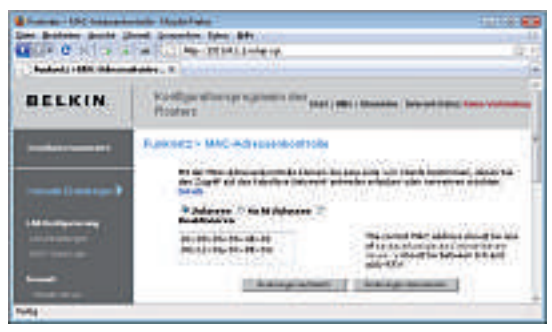
Dies ist nützlich, aber auch gefährlich. Wenn die Funktion nicht in zwei Optionen getrennt ist, kann ein Programm via UPnP auch die Sicherheitseinstellungen des Routers ändern und etwa Ports für einen Angriff öffnen. Router wie die Fritzbox von AVM bieten die Funktion in zwei Teilen an. Dort lässt sich UPnP getrennt für den Informationsfluss einschalten, aber das Verändern der Sicherheitseinstellungen verbieten.

20. USB-Anschlüsse nutzen

Viele Router haben USB-Anschlüsse für weitere Geräte. Darüber machen Sie einen Drucker, USB-Festplatten oder USB-Sticks netzwerkfähig.

Neu sind die virtuellen USB-Schnittstellen. Ist diese Option aktiviert, meldet sich ein am Router angesteckter USB-Drucker so, als wäre er am PC angesteckt. Sie finden diese Funktion, sofern vorhanden, im Router-Menü unter *USB-Fernanschluss*.

Markus Selinger



MAC-Adresskontrolle: Hier schützen Sie den Zugang zu Ihrem WLAN per MAC-Adressliste.