WLAN sichern - 10 praktische Tipps

Lassen Sie beim Verlassen der Wohnung Türen und Fenster für Einbrecher geöffnet? Eher nicht? Dann sollten Sie auch Ihr WLAN gegen Fremde sichern!
Denn: Als Betreiber eines Funknetzwerkes haften Sie ggf., wenn über Ihr ungeschütztes WLAN Straftaten verübt werden.

1. Den Router absichern

Gleich nach dem Aufbau und Anschluss des Routers sollte dessen Passwort geändert werden. Die besten Sicherheitseinstellungen sind wertlos, wenn sie jeder wieder ändern kann. Einstellungen an Ihrem Router sollten Sie dabei am besten über eine Kabelverbindung vornehmen, dann kann es nicht passieren, dass Sie sich durch eine falsche Einstellung selbst aus dem WLAN aussperren.

Bei vielen Routern werden als Standard-Passwort ab Werk einfache Passwörter wie "0000" oder "admin" eingesetzt. Werden diese Standard-Passworte nicht geändert, kann jeder ohne großen Aufwand in Ihren Router eindringen und die Routereinstellungen verändern.
Im Zweifel werden Sie aus Ihrem eigenen WLAN ausgesperrt.

Mit Hilfe der Web-Oberfläche eines jeden Routers lässt sich das Passwort ändern (meist über die Menüpunkte "Sicherheit" oder "System"). Die Adresse Ihres Routers, die Sie in die Adressleiste Ihres Browsers eingeben müssen, - bspw. 192.168.2.1 - entnehmen Sie dessen Handbuch. Wählen Sie als Router-Passwort eine komplexe Zeichenfolge mit mindestens acht Stellen, die Klein- und Großbuchstaben enthalten sollte sowie Zahlen und - wenn möglich - Sonderzeichen.

2. Die Router-Firmware aktualisieren

Jeder Router hat ein Betriebssystem, das Firmware genannt wird. Diese Software kann, wie jedes andere Betriebssystem auch, Sicherheitslücken aufweisen, über die der Router manipuliert werden kann. Diese Software-Fehler werden, wie bei Windows auch, vom Hersteller des Routers mit Updates behoben. Sie sollten daher regelmäßig kontrollieren, ob es für Ihren Router ein Firmware-Update gibt. Dies erfahren Sie auf der Web-Oberfläche Ihres Routers oder auf der Website des Herstellers Ihres Routers, von der Sie das Update regelmäßig auch direkt herunterladen können.

Einige Router updaten ihre Firmware auch automatisch, Sie sollten sich aber trotzdem in regelmäßigen Abständen davon überzeugen, dass Ihr Router auf dem neuesten Stand ist.

Firmware-Updates bringen oft auch neue oder verbesserte Funktionen für den Router mit sich, so beherrscht ein älterer Router plötzlich doch die bessere WPA2-Verschlüsselung.

3. Die Verschlüsselung des Funknetzes

Sie sollten sowohl den Zugang zum Netzwerk als auch die gesendeten Datenpakete verschlüsseln. Veraltete Verschlüsselungsstandards wie WEP (Wired Equivalent Privacy) und WPA (Wi-Fi Protected Access) können innerhalb weniger Sekunden geknackt werden, indem der Datenverkehr mitgelesen wird. Es sollte daher auf jeden Fall die WPA2-Verschlüsselung verwendet werden! Dieser Standard bietet momentan die größtmögliche Sicherheit.

Wichtig: Alle Geräte im WLAN müssen die gewählte WPA2-Verschlüsselung unterstützen. Kann eines der Geräte dies nicht, sollten Sie überlegen, es per Netzwerkkabel mit dem Router zu verbinden.

Sie sollten für Ihr WLAN ein möglichst langes WLAN-Passwort verwenden, das aus eher wild zusammengewürfelten Buchstaben, Ziffern und Sonderzeichen bestehen sollte. Empfehlenswert ist ein Passwort mit mindestens 20 Zeichen. Dieses Passwort sollte sich unbedingt von dem obigen Router-Passwort unterscheiden.

Am einfachsten lässt sich eine verschlüsselte Verbindung zwischen Router und PC mit dem so genannten Wi-Fi Protected Setup (WPS) herstellen, sofern beide Geräte dies unterstützen. Mit WPS können Sie auf Knopfdruck am Router einen Netzwerkschlüssel erstellen und diesen automatisch an die angeschlossene Hardware senden lassen. Hierdurch entfällt das Eintippen langer Schlüssel am jeweiligen Endgerät, was insbesondere bei WLAN-fähigen Druckern und Internet-Radios Vorteile bietet, da es im Vergleich sehr

bequem ist. Zu erwähnen ist jedoch, dass WPS in der näheren Vergangenheit wegen Sicherheitsbedenken in die Kritik geraten ist.

4. Unbekannten Geräten den Zugang verweigern

Lassen Sie nicht zu, dass sich jedes Gerät in Ihr WLAN einloggen kann! Ein Einloggen unbekannter Geräte verhindern Sie durch die Nutzung einer MAC-Filtertabelle.
MAC bedeutet "Media Access Control" und ist nichts anderes als eine zwölfstellige Zeichenkette, eine Art Identifikationsnummer, die in jeder WLAN-Hardware gespeichert ist. Diese Zeichenkette ist so etwas wie ein Fingerabdruck bzw. ein unverwechselbarer Name des jeweiligen Gerätes. Ist eine MAC-Filtertabelle im Router hinterlegt, werden nur noch die dazu passenden Geräte ins Netzwerk gelassen, dies auch dann, wenn auf dem unbekannten Gerät der Netzwerkname und Ihr Netzwerkpasswort richtig eingegeben wurden.

Zwar ist es möglich, MAC-Adressen zu fälschen und sich so Zugang zum WLAN zu verschaffen, dies ist jedoch aufwendig und dürfte die Fähigkeiten der meisten Hobby-Hacker übersteigen.

Eine MAC-Filtertabelle in Ihrem Router anzulegen und so nur bestimmte Geräte in Ihr WLAN zu lassen, ist relativ einfach: Sie müssen nur die MAC-Adresse des jeweiligen Endgerätes in eine dafür vorgesehene Tabelle im Router eintragen, die Sie über die Web-Oberfläche des Routers - meist unter dem Menüpunkt "Sicherheit" oder "Netzwerk" - finden.

Viele Router listen alle Endgeräte automatisch auf, die sich in Ihr WLAN einloggen möchten. Diese können Sie dann mit einem einfachen Klick freischalten, der bewirkt, dass dieses Gerät in die MAC-Filtertabelle aufgenommen wird und so Zugang erhält.

Sollten Sie die jeweilige MAC-Adresse manuell eingeben müssen, finden Sie diese - wenn es sich bei dem Endgerät um einen Windows-Rechner handelt - über die "Eingabeaufforderung" im Windows-Menü. Geben Sie hier den Befehl "ipconfig/all" ein und drücken Sie die Enter-Taste. Daraufhin wird Ihnen eine Liste angezeigt, die die MAC-Adresse des "WLAN-Adapters" unter "Physikalische Adresse" angibt.
Dies ist die MAC-Adresse Ihres PC.

Bei vielen Geräten ist die MAC-Adresse auch auf dem Gehäuse angegeben, auf die Verpackung gedruckt oder steht im jeweiligen Handbuch.

5. Der Name Ihres WLANs

Ändern Sie unbedingt den ab Werk voreingestellten Namen Ihres Funknetzes. Dieser so genannte "Service Set Identifier" (SSID) lautet meist "wlan", "wireless" oder ähnelt der

Typenbezeichnung Ihres Routers. Dies gibt Angreifern wichtige Hinweise über Ihren Router, etwa von welchem Hersteller er ist. Mit ein bisschen "googeln" kann dann leicht herausgefunden werden, welches Passwort bei diesem Gerät voreingestellt ist und welche Schwachstellen dessen Firmware aufweist.

Ebenso unsicher wie die voreingestellten WLAN-Namen sind Namen wie "dachgeschoss" oder "hausnummer5" sowie etwa "Jan und Stefanie". Durch solche SSIDs bekommen Angreifer ggf. wichtige Details über das Netzwerk heraus, die für einen erfolgreichen Angriff hilfreich sein können.

Ein sicherer SSID sieht etwa so aus: "#h5KmelusI$$mxx". Lange Kombinationen aus Zahlen, Groß- und Kleinbuchstaben sowie Sonderzeichen gelten als weitgehend sicher, zudem sollte der Netzwerkname nicht in einem Wörterbuch stehen. Außerdem sollte der SSID-Broadcast ausgeschaltet werden, dann muss ein Angreifer, will er sich in das Funknetz einloggen, den Namen des WLANs kennen, was einen Angriff zusätzlich erschwert.

Um mit seinem Funknetzwerk unsichtbar zu werden, reicht es bei den meisten Routern aus, in der Kategorie "WLAN" oder "Netzwerk" ein Häkchen vor dem Eintrag "Unsichtbar" zu setzen.

Zwar können mit spezieller Software auch versteckte Funknetzwerke gefunden werden, höchst fraglich ist jedoch, ob der Hobby-Hacker von nebenan dazu auch wirklich in der Lage ist. Außerdem gilt auch hier: Was er nicht weiß, macht ihn nicht heiß! Wenn ihm nicht ins Auge sticht, dass "Jan und Stefanie", die im "dachgeschoss" wohnen, ein WLAN haben, macht er sich dann wirklich die Mühe nach einem solchen zu suchen? Nur so auf Verdacht? Wohl eher nicht!

6. Die DHCP-Funktion ausschalten

Eine sehr wirkungsvolle Methode zum Abwehren von Angreifern ist das Ausschalten der DHCP-Funktion im WLAN-Router. DHCP weist allen Computern und sonstigen Geräten in Ihrem WLAN eine IP-Adresse zu. Das macht es einem Angreifer einfach, denn sobald sich sein PC in Ihr Netzwerk eingeloggt hat, erhält er automatisch eine IP-Adresse und wird so Teil des Netzwerkes. Ist der Hacker erstmal "drin", ist das für ihn dann sehr bequem, wird sein Computer doch automatisch erkannt und von allen anderen Geräten als einer der ihren "herzlich willkommen geheißen".

Die DHCP-Funktion kann meist sehr einfach im Optionspunkt "Netzwerk" → "LAN" deaktiviert werden.

Bei abgeschaltetem DHCP-Server ist es jedoch erforderlich, dass Sie an jedem Rechner und sonstigem Endgerät, das sich in ihrem Funknetz bewegen soll, die nötigen Einstellungen "per Hand" vornehmen. Neben der IP-Adresse müssen Sie am Endgerät die "Subnetzmaske" und den "Gateway" manuell festlegen. Diese Einstellungen müssen exakt mit denen des Routers übereinstimmen. Wie Ihr Router in dieser Hinsicht voreingestellt ist, erfahren Sie in der Bedienungsanleitung.

7. Die Router-Firewall aktivieren

Eine Firewall im Router ist fast wichtiger als eine auf dem PC, bildet sie doch die erste Verteidigungslinie. Sie sollten daher sicherstellen, dass die Firewall in Ihrem Router aktiviert ist.

Router-Firewalls lassen sich individuell einstellen, so können Sie kontrollieren, über welche "Ports" Zugriffe auf das Internet und von außen auf Netzwerk-PCs und andere Endgeräte vorgenommen werden können. Solche "Ports" sind die Türen für den Internetverkehr. Welche Türen Sie in Ihrem Router gegebenenfalls zusperren können, ist jedoch keine leichte Entscheidung. Sperren Sie die falschen zu, kann es u. a. vorkommen, dass ihr Rechner oder andere Geräte nicht mehr mit Updates versorgt werden.

In der Regel müssen Sie die Ports-Verwaltung allerdings nicht verändern.

8. Die Nachtabschaltung aktivieren bzw. das WLAN gelegentlich abschalten

Die meisten WLAN-Netze funken nachts unnötigerweise, da die Computer ausgeschaltet sind und die Anwender schlafen. Ein überflüssig aktives WLAN benötigt Strom und bietet Angreifern ein unbeaufsichtigtes Einfallstor. Es bietet sich daher an, das WLAN nachts auszuschalten. Viele Router verfügen hierfür über eine Nachtabschaltung.

Die Nachtabschaltung richten Sie über die Benutzeroberfläche (Web-Oberfläche) Ihres Routers ein. Hier können Sie Uhrzeiten festgelegen, in denen der Router die WLAN-Funktion abschaltet, sofern kein Computer im Funknetzwerk aktiv ist.

Für eine größere Sicherheit bietet sich dies auch tagsüber an, wenn man ohnehin außer Haus ist. Wer für längere Zeit sein Funknetzwerk nicht nutzt, beispielsweise wegen eines Urlaubs, sollte die WLAN-Funktion am Router ebenso abschalten.

Sollte Ihr Router nicht über eine Nachtabschaltung verfügen, dann benutzen Sie vor dem Zubettgehen doch einfach den kleinen Knopf auf der Rückseite vieler Router, um das WLAN ohne viel Aufwand auszuschalten.

9. Die Passwörter nicht auf dem Computer speichern

Dass man sich die Passwörter, die im Zusammenhang mit dem WLAN vergeben wurden, etwa das Passwort für den Router selbst oder das WLAN-Passwort, auf Dauer merken kann, ist selten der Fall. Diese Passwörter sollten daher irgendwo hinterlegt werden, damit man sich nicht selbst aussperrt.

Dies sollte auf gar keinen Fall in einer Word-Datei oder einer anderen ungeschützten Datei auf dem Rechner geschehen. Für jeden Angreifer - ob Mensch oder Computervirus - ist es ein Leichtes, solche Dateien mit Passwörtern zu finden, in der Regel wird er routinemäßig danach suchen.

Auch Programme, die speziell für das Aufbewahren von Passwörtern konzipiert sind, diese etwa in einer verschlüsselten Datei auf dem Rechner ablegen, sind nur bedingt geeignet die vergebenen Passwörter rund um das WLAN zu schützen. Diese weisen oft Schwachstellen auf, zudem kann eine solche Datei entführt werden, um sich "mit roher Gewalt" Zugang zu deren Inhalt zu verschaffen.

Sie sollten daher dazu übergehen, alle Passwörter handschriftlich auf einem einfachen Stück Papier zu vermerken, um auch nach geraumer Zeit noch an Ihr WLAN heranzukommen. Diese Passwortliste sollte dann sicher in Ihrem Haushalt - für Dritte unzugänglich - aufbewahrt werden, etwa wie Sie PINs und TANs Ihrer Bank aufbewahren. Diese Methode hat den entscheidenden Vorteil, dass Sie einem digitalen Angreifer jeglichen Zugriff auf Ihre Passwörter durch Verbringung in die "analoge Welt" abschneiden.

10. Abschließendes Resümee

Trotz aller Sicherheits-Einstellungen und Vorsichtsmaßnahmen wird ein WLAN nie hundertprozentig sicher sein. Wenn ein Angreifer in ein Funknetzwerk eindringen möchte, wird er es schaffen - es ist nur eine Frage der Zeit und seiner Motivation.

Die aufgezeigten Einstellungen und Maßnahmen minimieren nur die Risiken zu einem Opfer zu werden, denn so legen Sie jedem Angreifer Steine in den Weg, deren Beseitigung für ihn in Arbeit ausarten kann und bringen Hobby-Hacker zur Verzweiflung.

Wesentlich mehr Sicherheit gegenüber einem WLAN bietet dagegen ein kabelgebundenes Netzwerk.