SCHRITT-FÜR-SCHRITT-ANLEITUNG FÜR MEHR WLAN SICHERHEIT

Anleitung WLAN sichern

1. Sichern Sie zunächst den Zugriff auf Ihren Router. Vergeben Sie ein Administrator-Passwort und unterbinden Sie Zugriffsmöglichkeiten aus dem Internet. Sind Updates für den Router vorhanden, sind diese zeitnah einzuspielen.
2. Stellen Sie die Verschlüsselungsmethode des WLANs auf WPA2. Vergeben Sie einen möglichst langen WLAN-Schlüssel mit Groß- und Kleinbuchstaben sowie Zahlen. Der WLAN-Schlüssel darf sich nicht erraten lassen.
3. Verändern Sie die SSID des WLANs so, dass keine Rückschlüsse auf den Router Typ oder Ihre Person möglich sind. Auf ein Verstecken der SSID sollten Sie verzichten.
4. Richten Sie MAC-Adressfilter für Ihre Geräte ein. Nur Endgeräte, die zuvor in den Filtern konfiguriert wurden, erhalten Access auf Ihr WLAN.
5. Minimieren Sie die Sendeleistung des Routers soweit, dass das WLAN möglichst nur dort verfügbar ist, wo Sie es nutzen. Benötigen Sie das WLAN nicht, schalten Sie es manuell aus oder nutzen Sie automatisierte, zeitgesteuerte Schaltlogiken.
6. Verzichten Sie, wenn möglich, auf die WLAN-Einbindung per WPS. Sollte WPS im Router angeschaltet sein, deaktivieren Sie es.
7. Richten Sie Ihren Gästen ein eigenes Gäste-WLAN ein.
8. Prüfen Sie regelmäßig Ihren Router und dessen Konfiguration auf Unregelmäßigkeiten und Verdächtiges. Nutzen Sie hierfür automatisierte Meldungen bei Veränderungen in Ihrem Heimnetz und lesen Sie diese regelmäßig und sorgfältig.

SICHERN SIE ZUERST IHREN ROUTER

Bevor Sie anfangen, das eigene WLAN zu sichern, sorgen Sie zunächst für die Sicherheit an Ihrem Router. Alle Einstellungen, die Sie in den folgenden Schritten durchführen, könnten sonst schnell hinfällig sein. Denn ist der Zugriff auf Ihren Router für Unbefugte möglich, lassen sich alle Konfigurationen beliebig verändern. Zur Absicherung Ihres Routers vergeben Sie zunächst ein nicht zu erratendes Passwort für den Zugriff auf die Konfigurationsoberfläche. Sollte der Zugriff aus dem Internet auf den Router möglich sein

und Sie benötigen diese Option nicht, schalten Sie sie aus. Wichtig ist für die Sicherheit des Routers, dass Sie dessen Software regelmäßig aktualisieren. Nur dann sind bekannte Sicherheitslücken zuverlässig geschlossen. Für Internetrouter wie die FritzBox veröffentlichen die Hersteller regelmäßig neue Firmware, die sich mit wenigen Klicks einspielen lässt. Die FritzBox bietet sogar die Möglichkeit, Updates automatisiert einzuspielen, immer wenn eine neue Firmware verfügbar ist.

VERSCHLÜSSELUNG UND PASSWORT RICHTIG EINSTELLEN

Ist Ihr Router gesichert, können Sie im nächsten Schritt damit beginnen, Ihr WLAN zu konfigurieren. Führen Sie alle Einstellungen am besten mit einem Rechner durch, der per LAN-Kabel mit dem Router verbunden ist. Das verhindert, dass Sie sich selbst aussperren und Einstellungsänderungen an einem noch unsicheren WLAN von Unbefugten mitgelesen werden.

Prüfen Sie zunächst für die WLAN Sicherheit die Verschlüsselungsmethode des Routers. Optimal ist es, wenn Ihr Router WPA2 (Wi-Fi Protected Access 2) nutzt. Ist dies nicht der Fall, können Sie auf WPA zurückgreifen. Auch diese Verschlüsselungsmethode ist relativ sicher. Zeigt Ihnen der Router nur WEP (Wired Äquivalent Privacy) als Verschlüsselungsstandard an, ersetzen Sie Ihren Router mit einem neuen Modell, das WPA2 unterstützt. WEP stellt keine Hürde mehr für Hacker dar und lässt sich relativ schnell knacken. Auf keinen Fall dürfen Sie ein unverschlüsseltes WLAN einrichten. Bei diesem kann sich jeder mit Ihrem Router verbinden und alle übertragenen Daten sind prinzipiell ungeschützt.

Ist die Verschlüsselungsmethode konfiguriert, müssen Sie das Passwort beziehungsweise den Schlüssel für Ihr WLAN einstellen. Sollte werksseitig ein Passwort eingestellt sein, ändern Sie dieses auf jeden Fall. Denn meist bestehen diese Passwörter nur aus Ziffern und sind relativ kurz. Das Optimum in Sachen WLAN Sicherheit beim Passwort schöpfen Sie aus, wenn Sie die maximale Länge von 63 Zeichen und Zahlen sowie Groß- und Kleinbuchstaben verwenden. Mit Sonderzeichen sollten Sie eher vorsichtig sein, da nicht alle Router und Endgeräte die gleichen Sonderzeichen unterstützen. Das Passwort darf nicht aus Begriffen bestehen, die in Wörterbüchern zu finden sind oder sich durch Ausprobieren erraten lassen.

EINE NEUE SSID WÄHLEN

Jedes WLAN hat einen Namen - die SSID (Service Set Identifier). Router vergeben bei der Erstkonfiguration in der Regel eine eigene SSID, die unter Umständen Rückschlüsse auf den

Router Typ zulässt. Für potentielle Angreifer ist durch eine solche SSID auf den ersten Blick zu erkennen, welcher Router betrieben wird. Der Angreifer kann versuchen, den Router über bereits bekannte Sicherheitslücken anzugreifen. Verändern Sie deshalb die SSID und wählen Sie einen Namen, der weder Rückschlüsse auf den Router noch auf Ihre Person zulässt.

Einige Ratgeber empfehlen, aus Sicherheitsgründen die SSID zu verstecken. Bei dieser Option, die fast alle gängigen Router unterstützen, sendet der Router den SSID Namen nicht. Er ist für andere deshalb nicht zu sehen und nur Geräte, auf denen die SSID zuvor korrekt eingegeben wurde, können sich mit dem WLAN verbinden. Nun möchte man meinen, das macht das Netz sicher. Leider ist dem nicht so und eine versteckte SSID kann sogar ein Security-Risiko für die WLAN Sicherheit darstellen. Geräte, bei denen die SSID manuell eingestellt wurde und die sich normalerweise mit einem WLAN mit versteckter SSID verbinden, beginnen, wenn sie nicht in der Reichweite dieses WLANs sind, die SSID anzufragen und zu senden. Aus diesen Meldungen können Angreifer leicht die versteckte SSID ermitteln. Richten diese anschließend ein ungesichertes WLAN mit dem gleichen Namen ein, verbinden sich Ihre Geräte eventuell ohne Ihr Mitwissen mit diesem „Honeypot-WLAN“ und senden Ihre Daten völlig ungeschützt. Verzichten Sie deshalb auf das Verstecken der SSID.

STÄRKE DES FUNKSIGNALS ANPASSEN UND UNGENUTZTES WLAN AUSSCHALTEN

Die WLAN Sicherheit lässt sich durch zwei weitere Tipps merklich erhöhen. Ihr WLAN ist am sichersten, wenn es außerhalb Ihrer eigenen vier Wände gar nicht verfügbar ist. Werksseitig sind die Router meist so eingestellt, dass sie mit maximaler Sendeleistung WLAN-Signale aussenden. Ihr WLAN ist dadurch auch in der Nachbarwohnung oder im Nachbarhaus sichtbar. Router wie die FritzBox bieten Ihnen die Möglichkeit, die WLAN-Sendeleistung zu reduzieren. Führen Sie dies schrittweise durch und finden Sie heraus, bis zu welcher minimalen Leistung Sie alle gewünschten Bereiche noch mit WLAN versorgen können.

Den größten Schutz erzielen Sie, wenn Sie das WLAN komplett ausschalten. Dies mag im ersten Moment etwas seltsam klingen, aber in den seltensten Fällen muss das WLAN rund um die Uhr angeschaltet sein. Sind alle Bewohner außer Haus oder es ist Nacht und niemand benötigt das Internet, schalten Sie das WLAN einfach aus. Router bieten Ihnen hierfür unterschiedliche Möglichkeiten. Oft befindet sich wie bei der FritzBox ein WLAN-Schalter oder WLAN-Knopf am Gehäuse, mit dem Sie das WLAN mit einem einzigen Knopfdruck an-

oder ausschalten. Besonders komfortabel sind zeitgesteuerte Schaltungen des WLANs. Auch diese Option ist in vielen Routern vorhanden. Sie können jeweils die Wochentage und Uhrzeiten einstellen, an denen Ihr Router automatisch das WLAN aktiviert oder ausschaltet.

DEAKTIVIEREN SIE WPS

WPS (WiFi Protected Setup) ist dafür gedacht, Geräte schnell und unkompliziert ins WLAN zu bringen. Ist WPS aktiviert, lassen sich Endgeräte durch Drücken des WPS Knopfes an Router und Endgerät oder durch Eingabe eines kurzen Pins ohne langen WLAN-Schlüssel ins drahtlose Netzwerk integrieren. Leider ist die Implementierung teilweise fehlerhaft und es existieren zahlreiche Sicherheitslücken, die sich für einen unbefugten Zugriff auf das WLAN ausnutzen lassen. Es ist deshalb ratsam, WPS zu deaktivieren, sollte es am Router angeschaltet sein. Nutzen Sie WPS nur in Einzelfällen und wenn es unbedingt sein muss.

STELLEN SIE GÄSTEN FÜR MEHR WLAN SICHERHEIT EIN EIGENES GÄSTE-WLAN BEREIT

Haben Sie Gäste, die Internetzugang möchten, stellen Sie diesen ein eigenes Gäste-WLAN zur Verfügung. Viele Router bieten hierfür geeignete Optionen. Endgeräte im Gäste-WLAN sind von Ihrem WLAN getrennt und können keinen Schaden in Ihrem Heimnetz anrichten.

WLAN-SICHERHEIT UND ROUTER REGELMÄßIG PRÜFEN

Haben Sie die Einstellungen, wie in den Absätzen zuvor beschrieben, vorgenommen, sollte Ihr WLAN geschützt sein. Seien Sie sich aber trotzdem niemals zu sicher und kontrollieren Sie regelmäßig Ihren Router auf verdächtige Meldungen und überprüfen Sie seine Einstellungen. Dazu nutzen Sie die Systemmeldungen und die Liste der am Router angemeldeten Endgeräte. Einige Router sind in der Lage, Ihnen selbständig Nachrichten per E-Mail zu senden, sollte sich jemand an der Administrationsoberfläche des Routers anmelden oder Einstellungen verändern. Das Gerät kann Sie zum Beispiel auch informieren, wenn ein neues Endgerät sich per WLAN mit Ihrem Router verbindet. Nutzen Sie solche automatisierten Meldungen und lesen Sie sie sorgfältig. So sind Sie stets über wichtige Vorgänge in Ihrem Heimnetz informiert und Ihnen entgehen keine verdächtigen Aktionen.