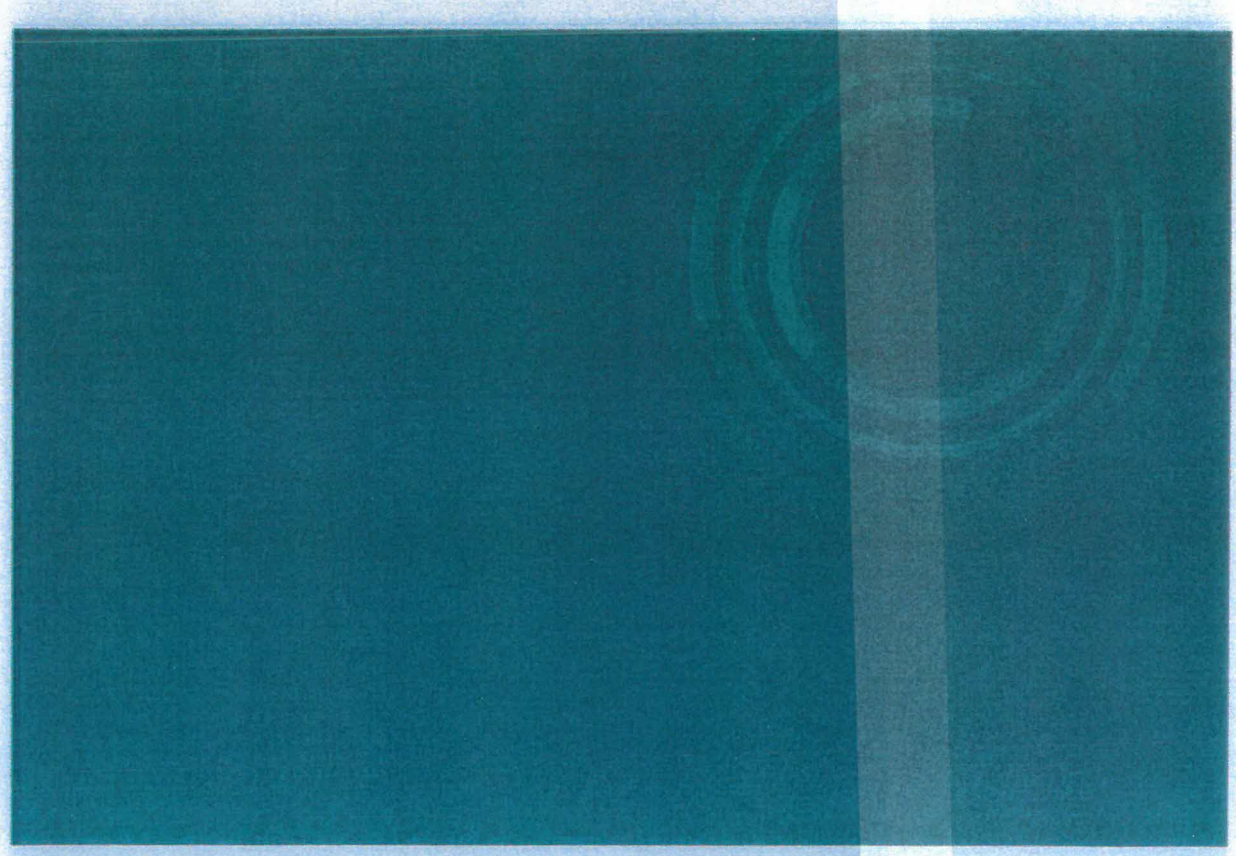
Sicherheitstipps im privaten und öffentlichen WLAN

Den Router sicher einrichten und vorsichtig im fremden WLAN bewegen



Solider Schutz für den Router – Das Fundament für die IT-Sicherheit zu Hause

Im ungesicherten Zustand sind Router ein Einfallstor für Cyber-Angriffe. Wenn es Angreifenden gelingt, von außen in den Router einzudringen, können sie das Gerät selbst, aber auch alle angeschlossenen Geräte kompromittieren und den Nutzenden persönlichen oder finanziellen Schaden zufügen:

Das BSI empfiehlt dazu folgende Maßnahmen:

Basisempfehlungen

- **Ändern Sie die Standardpasswörter!**
  Die Anwendung zur Verwaltung des Routers ist durch ein Passwort geschützt. Inzwischen ist bei bestimmte Routermodelle werksseitig ein individuelles Passwort voreingestellt. Sie erkennen das daran, dass dieses Passwort im Benutzerhandbuch als "individuell" gekennzeichnet ist oder überhaupt nicht mehr aufgeführt ist. Allerdings

gibt es immer noch Router, die mit Standardpasswörtern wie "admin" oder "1234" ausgeliefert werden. Solche Zugangscodes sollten Sie sofort ändern, denn auch Angreifende kennen (und nutzen!) diese Standardpasswörter. Das BSI empfiehlt Passwörter mit mindestens acht Zeichen und aus verschiedenen Zeichenarten wie Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen. Tipps, ein sicheres Passwort zu erstellen, finden Sie hier.

- **Halten Sie die Firmware aktuell!**
  Überprüfen Sie regelmäßig, ob die sogenannte Router-Firmware noch aktuell ist. Als Firmware bezeichnet man die Betriebssoftware eines Geräts. Eine Aktualisierung (also ein "Update") dient dem Nachrüsten mit neuen Funktionen oder der Korrektur von Fehlern, einschließlich dem Stopfen von Sicherheitslöchern. Haben Sie Ihr Gerät von Ihrem Internet-Zugangs-Provider erhalten, fragen Sie diesen, ob er die Aktualisierung der Firmware regelmäßig über eine Fernwartung vornimmt. Auch im Konfigurationsmenü des Routers findet sich zumeist die Option, Aktualisierungen ("Updates") automatisch zu installieren. Machen Sie von dieser Option Gebrauch.

- **Langes und komplexes WLAN-Passwort**

  Das WLAN-Passwort ist nicht identisch mit dem Router-Passwort. Es dient speziell dem drahtlosen Zugang in das lokale Funknetz. In der Regel haben die Router werksseitig bereits ein sicheres WLAN-Passwort eingestellt, das aus 20 Zeichen besteht. Sollte dies bei Ihrem Router nicht der Fall sein, vergeben Sie ein Passwort, das aus mindestens 20 zusammenhanglosen Zeichen besteht.
- **Ersetzen Sie den voreingestellten Standard-Netzwerknamen!**
  Manche Router tragen im Namen des WLAN ausführliche Informationen zu etwa Hersteller oder Modell des Geräts. Diese Angaben können einem potentiellen Angreifer von Nutzen sein. Ändern Sie daher den Namen des Netzwerks in eine Bezeichnung, die nichts über Ihren Router verrät.
- **Deaktivieren Sie nicht benötigte Funktionen ihres Routers!**
  Moderne Router ermöglichen außer dem Zugang zum Internet eine Vielzahl zusätzlicher Funktionen. So können Router zum Beispiel als Medienplayer eingesetzt werden. Diese Funktionen können allerdings auch ein Einfallstor für Angreifer darstellen. Deaktivieren Sie auf Ihrem Router daher alle Dienste, die Sie nicht benötigten. Informationen zu den Diensten Ihres Routers und deren Konfiguration finden Sie im Handbuch oder auf der Homepage Ihres Routerherstellers.
- **Deaktivieren Sie den Fernzugang ihres Routers!**
  Viele Router ermöglichen es, sie auch von außerhalb des Heimnetzwerks zu konfigurieren. Prüfen Sie, ob bei Ihrem Router diese Funktion vorhanden und gegebenenfalls aktiviert ist und **deaktivieren** Sie diese, falls Sie sie nicht benötigen.

- **Richten Sie ein Gast-Netzwerk ein**

  Für unsichere Geräte oder für die Geräte Ihrer Gäste sollten Sie, wenn möglich, ein Gast-Netzwerk einrichten. Damit trennen Sie diese Zugänge von sensiblen Diensten wie Onlinebanking oder Homeoffice-Anwendungen.

- **Beachten Sie die IT-Sicherheitskennzeichen**

  Router-Anbieter können für ihre Produkte das IT-Sicherheitskennzeichen des BSI erhalten. Voraussetzung dafür: Sie sichern zu, dass ihre Produkte bestimmte Sicherheitseigenschaften besitzen. Falls Sie die Anschaffung eines neuen Routers planen, nutzen Sie dieses Kennzeichen als Kaufkriterium.

Erweiterte Einstellungen

- **Nutzen Sie https!**
  Bei der Konfiguration des Routers sollte außerdem darauf geachtet werden, dass die

Routerkonfiguration über https aufgerufen wird. Erkennbar ist das in der Adresszeile Ihres Browsers.

- **Ändern Sie Einstellungen an der Firewall**
  Viele Router haben eine eingebaute Firewall. Ändern Sie Einstellungen an ihr nur, wenn Sie entsprechende Kenntnisse über die einzelnen Ports besitzen.
- **Richten Sie den MAC-Filter ein!**
  Die MAC-Adresse (Media-Access-Control-Adresse) ist die Hardware-Adresse jedes einzelnen Netzwerkadapters. Sie dient die als eindeutiger Identifikator des Geräts in einem Rechnernetz. Bei Apple wird sie auch Ethernet-ID, Airport-ID oder Wi-Fi-Adresse genannt, bei Microsoft Physikalische Adresse. Wenn Ihr Router die Möglichkeit bietet einen MAC-Filter einzurichten, dann nutzen Sie diese Möglichkeit. Nur den von Ihnen freigegebenen Netzwerkkarten wird nach Überprüfung ihrer MAC-Adressen der Zugang gestattet. MAC-Adresse ermitteln.

Verhalten im öffentlichen WLAN

Die meisten mobilen, internetfähigen Geräte können Sie in WLAN-Netzwerke einbinden. Diese Möglichkeit wird von Anwendern oft und gerne genutzt, da die Datenmengen, die über das Mobilfunknetz versendet werden können, häufig vertraglich begrenzt werden. Außerdem sind die Übertragungsgeschwindigkeiten über WLAN derzeit meist noch höher als über ein Mobilfunknetz.

Doch die Nutzung eines WLAN-Netzes birgt auch Risiken, vor allem dann, wenn es sich um ein fremdes WLAN-Netz handelt, dessen Betreiber und Hintergründe Sie nicht kennen. Daten können abgegriffen, Schadsoftware auf Ihr Gerät eingeschleust werden.

WLAN-Hotspots anbieten: Das gibt es Rechtliches zu wissen

Ob Kunden-WLAN oder einen **öffentlichen Hotspot** betreiben: Trotz der abgeschafften Störerhaftung gibt es **Rechtlich einiges zu wissen**. Wir klären auf.

2017 war es so weit: Die **Störerhaftung**, ein ebenso sperriges wie unbeliebtes Wort, wurde rechtssicher abgeschafft. Betreiber von öffentlichen WLAN-Hotspots sollten nun **nicht mehr juristisch belangt** werden können, wenn sich User:innen im Hotspot illegal verhalten hatten. Nun, drei Jahre später, gibt es zwar immer noch keine WLAN-Oase Deutschland, so wie sich Brigitte Zypris das damals sinngemäß gewünscht hatte, aber es ist deutlich einfacher geworden, freies Kunden-WLAN bereit zu stellen oder einen öffentlichen Hotspot anzubieten. Dennoch gibt es weiterhin einiges zu beachten.

Hotspot anbieten – Rechtliches:

- **Passwortschutz**: Netzwerkbetreiber müssen ihre öffentlichen Hotspot-Anschlüsse durch Passwörter sichern. Wollen sie dies nicht, müssen sie bestimmte **Internetseiten sperren**, um illegalen Up- oder Download zu verhindern. Diese Maßnahmen soll den Urheberschutz stärken, damit z.B. Musikproduzent:innen – sollte es doch zum illegalen Up- oder Download kommen– eine Handhabe gegen die Täter:innen haben.

- **Netzsperren (Portsperrung)**: Verhalten sich User:innen in einem WLAN-Hotspot wiederholt falsch, müssen Hotspot-Betreiber diese registrieren und als letzte Option deren Zugang komplett sperren.

- Um sich zusätzlich gegen Missbrauch des angebotenen Hotspots zu schützen, ist es ratsam, eine **Klausel in die Nutzungsbedingungen** einzubauen. Diese sollte User:innen vor Surfbeginn angezeigt werden und explizit darauf hinweisen, dass der Internetzugang nur zu rechtlich zulässigen Zwecken genutzt werden darf.

Leider ist die Unsicherheit, was das Betreiben von öffentlichen WLAN-Hotspots angeht, noch immer groß, da das sog. WLAN-Gesetz (die Neuentscheidung über Störerhaftung) in vielen

Punkten rechtlich weiter vage bleibt. Sicher ist, dass Inhaber von Urheberrechten von Anbietern öffentlicher Hotspots **weder Schadensersatz noch Abmahngebühr** verlangen dürfen.

Mahnbescheide werden trotzdem weiterhin an den WLAN-Betreiber verschickt, da die Rechteinhaber in der Regel häufig nicht wissen, dass die Rechtsverletzung über einen offenen WLAN-Zugang begangen wurde und in erster Linie der / die Anschlussinhaber:in über die IP-Adresse ermittelt wird. Es besteht dann eine **Darlegungspflicht der Betreiberseite**, dass er die Rechtsverletzung nicht selbst begangen und ein offenes WLAN angeboten hat. Mahnbescheide werden aus Unwissenheit über ihre Rechte von Hotspot-Betreibern auch ebenso häufig bezahlt.

Fazit zum eigenen öffentlichen Hotspot

Obwohl die Gesetzeslage auch in ihrer relativ neuen Version noch einige Unklarheiten offenlässt, gibt es eine Lösung: einige Anbieter haben sich darauf spezialisiert, **rechtssicheres WLAN** anzubieten, das meist auch DSGVO-konform ist. Das Internet läuft so im Regelfall über einen **Sicherheitsserver** des jeweiligen gebuchten Hotspot-Zwischen-Anbieters – kommt es zu einem rechtlichen Zwischenfall, haftet der Zwischen-Anbieter. So können Unternehmen, Cafés und andere Interessierte öffentliche WLAN-Hotspots anbieten. Von der einfachen und flächendeckenden WLAN-Abdeckung ist Deutschland aber dennoch weiterhin weit entfernt.

Autorin: Kathrin Strauß
Artikel veröffentlicht am: 06. Februar 2020