Tipps für ein sicheres Heimnetzwerk

Router einrichten

Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Basisschutz für den Router – das Herzstück der digitalen Vernetzung zu Hause.

Der Router bildet den Knotenpunkt für die Kommunikation aller netzwerkfähigen Geräte – Computer, mobile Geräte, Smart-TVs und intelligente Haustechnik – sowohl mit dem Internet als auch untereinander. Als zentrale Schnittstelle zwischen dem Internet und dem Heimnetzwerk ist es enorm wichtig, den Router gegen unberechtigte Zugriffe und Angriffsversuche von außen zu schützen. Wenn es Angreifenden gelingt, von außen in den Router einzudringen, können sie den Nutzenden persönlichen oder finanziellen Schaden zufügen, wie z. B. Daten abgreifen oder Schadsoftware installieren.

8 Tipps für ein sicheres Heimnetzwerk

Wer sein Heimnetzwerk und alle damit verbundenen, internetfähigen Geräte schützen möchte, muss vor allem seinen Router sicher einrichten und gut absichern. Mit den folgenden Basis-Tipps legen Sie den Grundstein für den sicheren Betrieb Ihres (W)LANs.

Disclaimer: Abhängig von Ihrem Routermodell und der derzeitigen Firmware-Version können Begrifflichkeiten geringfügig abweichen. Genaue Anleitungen finden Sie im Benutzerhandbuch Ihres Routers.

1. Standard-Passwort für die Weboberfläche des Routers ändern
2. Firmware und Updates aktuell halten
3. Langes und komplexes WLAN-Passwort vergeben
4. Standard-Netzwerknamen ersetzen
5. Status der Firewall prüfen
6. Sichere WLAN-Verschlüsselung beachten
7. Fernzugriff deaktivieren
8. Gast-Netzwerk einrichten

Schon gewusst?

Nutzen Sie das IT-Sicherheitskennzeichen des BSI als Kaufkriterium.

Mit dem IT-Sicherheitskennzeichen des BSI für Router sichern Hersteller zu, dass ihre Produkte den Sicherheitsanforderungen des BSI entsprechen.

Nutzen Sie das IT-Sicherheitskennzeichen (IT-SiK) als Kaufkriterium, wenn Sie einen neuen Router kaufen. Schauen Sie auf der Verpackung nach, ob der Router das IT-SiK trägt. Scannen Sie den aufgedruckten QR-Code mit dem Smartphone und informieren Sie sich auf der zugehörigen Produktinformationsseite des BSI über die IT-Sicherheitseigenschaften des Produktes.

Weitere Informationen

Schritt für Schritt zum Gäste-WLAN

Router & WLAN sicher einrichten: Warum der Schutz des Routers so wichtig ist

IT-Sicherheitskennzeichen für den Router

Impressum

Herausgeber:
Bundesamt für Sicherheit in der Informationstechnik – BSI
Godesberger Allee 185-189, 53175 Bonn

Kontakt:
E-Mail: service-center@bsi.bund.de
Internet: www.bsi.bund.de
Service-Center: +49 (0) 800 274 1000

Artikelnummer:
BSI-IFB 23/150

1. Ändern Sie das Standard-Passwort Ihres Routers.

Standard-Passwörter wie z.B. „admin“ sollten Sie sofort ändern, denn auch Angreifende kennen (und nutzen!) diese für Cyberangriffe.

Rufen Sie die **Benutzeroberfläche** Ihres Routers auf, indem Sie im **Browser** die **IP** oder **Kurzadresse** eingeben. Diese finden Sie meist im Handbuch oder auf der Rückseite des Routers. Suchen Sie im Menü unter **Einstellungen** nach **Router-Passwort** oder **Gerätepasswort ändern** und vergeben Sie dort ein neues, starkes Passwort. Grundsätzlich gilt: Je länger, desto besser. Verwendet werden können alle verfügbaren Zeichen.

2. Halten Sie die Firmware mit automatischen Updates aktuell.

Softwareupdates sind wichtig, weil sie bekannte Sicherheitslücken schließen. Damit Sie kein Update verpassen und Ihr Router sich selbstständig aktualisiert oder Sie über neue Updates informiert, sollten Sie – wenn möglich – automatische Updates aktivieren.

Öffnen Sie in der **Benutzeroberfläche** Ihres Routers den Menüpunkt **System** bzw. suchen Sie nach einem ähnlichen Begriff. Schauen Sie dort nach **(Firmware-)Update** oder **Laden & Sichern** und dort nach **Firmware-Version** und klicken Sie dann auf einen Button wie **Neue Firmware suchen**. Ist ein Update verfügbar, wählen Sie **Update starten.**
Damit Sie kein Update verpassen, suchen Sie nach einem Button wie **Auto-Update** und übernehmen Sie eine Einstellung wie z.B. **Über neue Versionen informieren und neue Versionen automatisch installieren (empfohlen).**

3. Vergeben Sie ein langes und komplexes WLAN-Passwort.

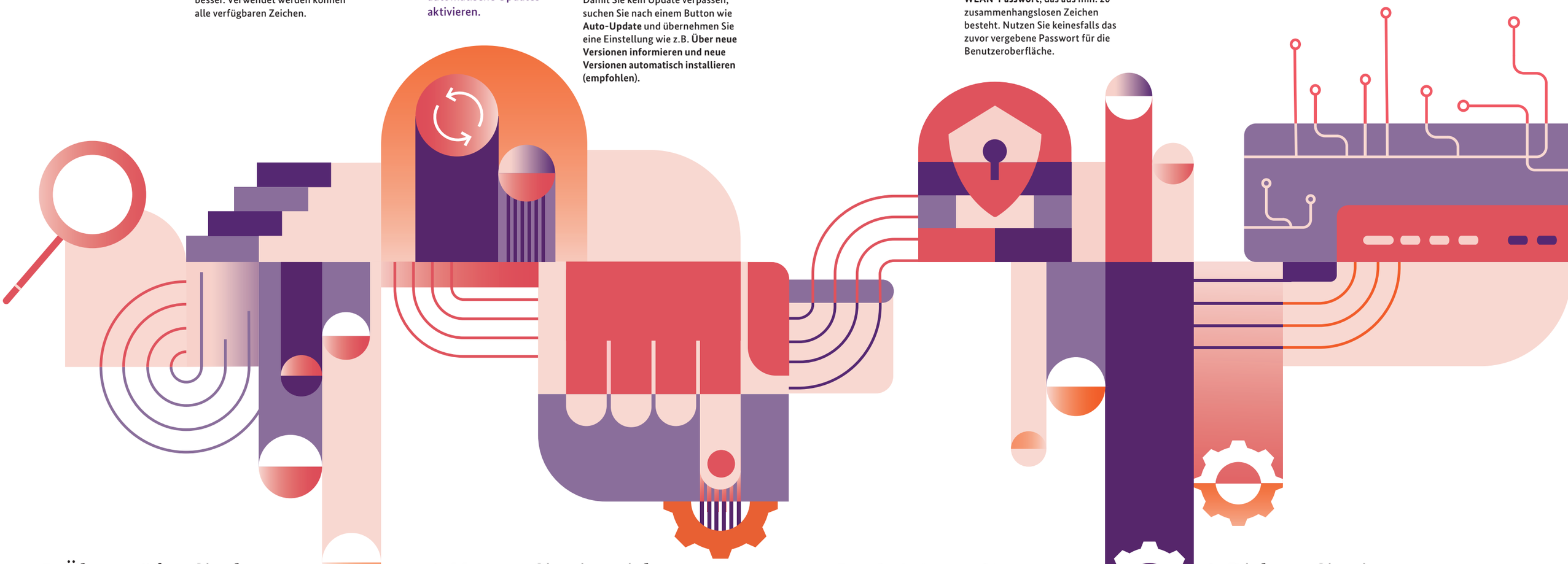
Das WLAN-Passwort ist nicht identisch mit dem Router-Passwort, sondern dient speziell der Absicherung und Zugangsbeschränkung Ihres WLAN. Sofern das WLAN-Passwort weniger als 20 Zeichen besitzt, sollte es geändert werden.

Suchen Sie in der **Benutzeroberfläche** nach **Netzwerk, Heimnetzwerk** oder **WLAN** und dann nach einem Menüpunkt wie **WLAN-Grundeinstellungen.** Je nach Routermodell finden Sie danach Einträge wie **Passwort, Zugang** oder **Verschlüsselung** und dahinter einen Begriff wie **WLAN-Passwort** oder **WLAN-Schlüssel.** Vergeben Sie dort ein neues, individuelles **WLAN-Passwort**, das aus min. 20 zusammenhangslosen Zeichen besteht. Nutzen Sie keinesfalls das zuvor vergebene Passwort für die Benutzeroberfläche.

4. Ändern Sie den voreingestellten Standard-Netzwerknamen.

Manche Router tragen im WLAN-Namen Informationen zum Modell des Geräts, die potenziellen Angreifenden nützlich sein können.

Rufen Sie wie zuvor beschrieben die **Benutzeroberfläche** Ihres Routers auf und loggen Sie sich mit Ihrem (neuen) Passwort ein. Suchen Sie im Menü in den **Einstellungen** nach **WLAN** und dort nach dem Unterpunkt **WLAN-Name** oder **SSID**. Ändern Sie den Netzwerknamen in eine Bezeichnung, die nichts über Ihren Router oder Sie persönlich verrät.



5. Überprüfen Sie den Status der Firewall.

Die Firewall kontrolliert den Datenfluss zwischen dem internen (Hausnetz) und dem öffentlichen Netzwerk (Internet) und schützt Ihr System vor unbefugten Zugriffen und potenziellen Gefahren von außen.

Suchen Sie in der Benutzeroberfläche nach **Internet** und dort nach **Filter** oder **Freigaben** oder nach Menüpunkten wie **Sicherheitseinstellungen Firewall**. Die Firewall ist standardmäßig aktiviert. Sollte dies nicht der Fall sein, **aktivieren** Sie die Firewall über die entsprechende Option und speichern Sie Ihre Einstellungen.

6. Nutzen Sie eine sichere WLAN-Verschlüsselung.

WPA2 und WPA3 beschreiben die aktuell sichersten Verschlüsselungsmethoden für WLAN-Netze. Ein verschlüsseltes WLAN schützt vor unbefugten Zugriffen.

Suchen Sie in der Benutzeroberfläche unter **WLAN** und dann nach **Sicherheit** oder unter **Konfiguration starten** nach **Laden & Sichern** und stellen Sie den WLAN-Modus **WPA2** oder **WPA3** ein, geben Sie Ihren **WLAN-Schlüssel** ein und übernehmen Sie die Einstellungen. Falls Ihr Router keinen dieser beiden Standards unterstützt, sollten Sie auf ein neues Router-Modell umsteigen.

7. Deaktivieren Sie den Fernzugriff.

Extrafunktionen des Routers wie z.B. der Fernzugriff können ein Einfallstor für Angreifende sein und sollten deaktiviert werden, wenn sie nicht genutzt werden.

Um den Fremdzugriff zu deaktivieren, suchen Sie unter **Internet** nach **Freigabe** und dort nach Unterpunkten wie **(Router-) Dienste** oder **Internetzugriff**. Entfernen Sie dort, falls gesetzt, den Haken bei **Internetzugriff auf Router aktiviert.**

8. Richten Sie ein Gastnetzwerk ein.

Mit einem Gast-Netzwerk trennen Sie z. B. die Geräte Ihrer Gäste von Ihren eigenen Geräten, auf denen Sie sensible Dienste wie Onlinebanking oder Homeoffice-Anwendungen nutzen.

Suchen Sie im Menü der Benutzeroberfläche unter **WLAN** nach **Gastzugang** o.ä. und **aktivieren** Sie diesen. Vergeben Sie unter **Name des Gastfunknetzes** einen Netzwerknamen und unter **WLAN-Netzwerkschlüssel** ein sicheres WLAN-Passwort für Ihre Gäste. Wenn möglich, aktivieren Sie auch dort unter **Verschlüsselung** WPA2 oder WPA3.