

# ROUTER CHECKLISTE

---

- Standardpasswort ändern**
- Gerätebezeichnung ändern**
- 2-Faktor Authentifizierung für Adminbereich**
- Gastnetzwerk einrichten**
- Regelmäßig updaten**
- Testen mit Routersploit**
- Stärkste Verschlüsselung wählen**
- WPS deaktivieren**

# ROUTER CHECKLISTE

## **Standardpasswort ändern**

Standardpasswörter für diverse Router sind online leicht zu finden und sollten deshalb sofort geändert werden.

## **Gerätebezeichnung ändern**

Mit [Hersteller + Version] kann ein Angreifer leicht nach Schwachstellen suchen.

## **2-Faktor Authentifizierung für Adminbereich**

Die Adminoberfläche sollte besonders geschützt sein, etwa durch ein starkes Passwort und eine zusätzliche 2-FA.

## **Gastnetzwerk einrichten**

Gäste (oder IoT Geräte) sollten keinen Zugang zum Hauptnetz erhalten sondern in ein Gastnetzwerk ausgelagert werden.

## **Regelmäßig updaten**

Die Firmware des Routers sollte immer auf dem neuesten Stand sein. Geräte die keine Updates mehr erhalten, sollten entsorgt werden.

## **Testen mit Routersploit**

Mit dem Framework Routersploit können Router automatisiert auf Schwachstellen getestet werden.

## **Stärkste Verschlüsselung wählen**

Immer nur die stärkste mögliche Verschlüsselung verwenden (aktuell WPA2), ältere Versionen wie WEP sollten nicht zum Einsatz kommen.

## **WPS deaktivieren**

WPS ist eine bequeme Möglichkeit Geräte in das Netzwerk einzubinden, stellt aber auch ein Sicherheitsrisiko dar und sollte deshalb deaktiviert werden.