CSBW | CYBER SICHERHEITS AGENTUR Baden-Württemberg

Sicheres Zuhause: Wichtige Konfigurations-Tipps zur Absicherung Ihres Heim-Netzwerks

CSBW Factsheet: Cybersecurity-Wissen kompakt

Optimale Konfiguration des Home-Routers

Der Router ist das Herzstück der digitalen Vernetzung zu Hause. Er bildet den Knotenpunkt für die Kommunikation aller internetfähigen Geräte wie Computer oder Smart-TV und verbindet die Geräte sowohl untereinander als auch mit dem Internet.
Deshalb ist der umfassende Schutz des Routers von besonderer Bedeutung[1].

Als Tor zum Internet stellt der Router die Verbindungen zu allen webbasierten Diensten her. Gleichzeitig schützt dieser u.a. durch seine Firewall davor, dass Dritte unberechtigt auf Ihre Inhalte, Geräte und Daten zugreifen können. Allerdings kann der Router dies nur zuverlässig leisten, wenn er richtig konfiguriert ist. In diesem Factsheet stellen wir daher wichtige Konfigurations-Tipps vor, mit denen Sie Ihr Heim-Netzwerk grundlegend absichern und darüber hinaus für eine optimierte Qualität der Verbindung sorgen können. Dies ist insbesondere für Ihre Arbeit aus dem Homeoffice von Relevanz.

Konfiguration des Heimrouters

- Die Routerkonfiguration sollte über **https** aufgerufen werden. Sichtbar an der Adresszeile des Browsers.
- Bevor Änderungen an der Einstellung eines Routers vorgenommen werden, sollte zunächst immer **ein Backup der aktuellen Konfiguration** erstellt werden.
- Falls dies nicht möglich ist, lässt sich der Router jederzeit auf Werkseinstellungen zurücksetzen, um den Anfangszustand wiederherzustellen (eine Anleitung hierzu finden Sie im Benutzerhandbuch des Herstellers).

Wir empfehlen folgende Maßnahmen:

Standard-Passwort und Netzwerkname ändern

- Das werksseitig gesetzte Zugangspasswort des Routers sollte **unverzüglich in ein sicheres Passwort[2] geändert** werden!
- Dasselbe gilt für den Namen des Netzwerks, da aus dem Standardnamen verschiedene Informationen zum Hersteller oder Modell des Geräts abgelesen werden können.

Sichere Verschlüsselung

- Wählen Sie den **Verschlüsselungsstandard WPA2 + WPA3** (Wi-Fi Protected Access).
- Bei älteren Modellen, die noch nicht über WPA3 verfügen, sollte WPA2 bzw. WPA2 (CCMP) gewählt werden.
- **Keinesfalls sollten die veralteten WPA- und WEP-Verschlüsselungsstandards gewählt werden.**

WPS-Methode überprüfen (Wi-Fi Protected Setup)

- Hier wird empfohlen nur die **„Push-Button-Methode“** zuzulassen. Bei allen anderen angebotenen Varianten werden immer wieder Sicherheitslücken entdeckt, die ausgenutzt werden können.

Automatische Updates

- Aktivieren Sie die **automatische Installation von Updates**, um mögliche Sicherheitslücken zu schließen und die Firmware Ihres Routers stets aktuell zu halten.

Fernzugriff und weitere Dienste

- Hochwertige Router bieten die Möglichkeit über das Internet auf verschiedene Inhalte des Routers zuzugreifen. Dies sollte man **aus Sicherheitsgründen** jedoch **unterbinden**.
- Sollte ein Fernzugriff aus dem Internet notwendig sein, empfiehlt es sich, diesen von einer fachkundigen Person einrichten zu lassen, da komplexe Einstellungen zur Absicherung erforderlich sind.
- Des Weiteren empfehlen wir, Ihr WLAN-Passwort nicht zu teilen, sondern stattdessen ein Gast-Netzwerk einzurichten. Nutzen Sie auch einen MAC-Filter.
- Deaktivieren Sie auf Ihrem Router alle Dienste, die Sie nicht benötigen.

Quellen:

[1] https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Router-WLAN-VPN/router-wlan-vpn_node.html

[2] CSBW-Factsheet: Passwortsicherheit

@ CSBW – Abteilung 1: Prävention.
Kontakt: schulungen@cybersicherheit.bwl.de