

Heimnetz und Smart Home

Der Router ist das Tor zu allem, was zu Hause vernetzt ist. Wie man ihn absichert, wohin unsichere Geräte gehören und warum Portfreigaben so selten nötig sind.

THEMEN IM ÜBERBLICK

Router als Türsteher

WLAN richtig einrichten

Gastnetz nutzen

Geräte auswählen

Kameras & Sprachassistenten

Portfreigaben

DNS im Heimnetz

Befallenes Gerät

Diese Broschüre setzt dort an, wo „**Cybersecurity im Alltag**“ mit einer Karte zum WLAN aufhört. Phishing, Passwörter und DNS-Anbieter werden dort behandelt und hier nur verknüpft.

01	Der Router ist der Türsteher	3
02	WLAN richtig einrichten	4
03	Das Gastnetz ist die wichtigste Funktion	5
04	Vernetzte Geräte auswählen	6
05	Kameras, Mikrofone und Sprachassistenten	7
06	Portfreigaben und Fernzugriff	8
07	DNS im Heimnetz	9
08	Wenn ein Gerät befallen ist	10
09	Spickzettel zum Ausdrucken	11
10	Quellen und weiterführende Hinweise	12
11	Impressum und Weitergabe	13

Jeder Router ist anders

Die Menüs unterscheiden sich je nach Hersteller und Anbieter deutlich. Diese Broschüre nennt deshalb, wonach Sie suchen und warum — nicht den genauen Klickweg. Die Bezeichnungen in Anführungszeichen sind die üblichen Suchbegriffe.

Der Router ist der Türsteher

Jedes Gerät im Haushalt hängt an ihm: Rechner, Handys, Fernseher, Drucker, Heizungssteuerung, Kamera. Wer den Router kontrolliert, sieht und steuert den gesamten Verkehr. Er ist deshalb das erste und wichtigste Gerät, das abgesichert gehört.

Eigenes Admin-Passwort

Das Kennwort für die Router-Oberfläche ist nicht das WLAN-Passwort. Werkseinstellungen und Aufkleber-Kennwörter ersetzen.

Automatische Updates

Die meisten aktuellen Geräte können das. Einschalten und einmal prüfen, ob es auch greift.

Fernzugriff aus

„Zugriff aus dem Internet“ braucht fast niemand. Ist er an, steht die Verwaltungsoberfläche weltweit offen.

Alter prüfen

Auch Router bekommen irgendwann keine Updates mehr. Fünf Jahre sind ein realistischer Anhaltspunkt zum Nachsehen.

DIE HALBE STUNDE, DIE SICH LOHNT

Admin-Passwort ändern, Firmware aktualisieren, Fernzugriff und WPS abschalten, Gastnetz einrichten. Damit sind die vier häufigsten Einfallstore geschlossen – und das gilt für die nächsten Jahre.



Geräte vom Anbieter

Bei gemieteten Routern verwalten manche Anbieter die Firmware selbst. Das ist bequem, aber Sie sollten wissen, ob es so ist – sonst warten Sie auf ein Update, das nie von Ihnen kommen muss. Im Zweifel beim Anbieter nachfragen.

WLAN richtig einrichten

EINSTELLUNG	EMPFEHLUNG	WARUM?
Verschlüsselung	WPA3, sonst WPA2	WEP und WPA sind seit Jahren gebrochen. Steht im Menü noch „WPA/WPA2 gemischt“, ist das ein Hinweis auf sehr alte Geräte im Netz.
WLAN-Passwort	lang, einzigartig	Ein aufgedrucktes Werkskennwort ist meist gut — solange es nicht auf einem Foto im Netz landet. Selbst gewählte kurze Passwörter sind schlechter.
WPS	abschalten	Die Komfortfunktion mit Knopfdruck oder PIN war in mehreren Umsetzungen angreifbar. Der Gewinn ist gering.
Netzname (SSID)	ohne Personenbezug	„Familie Meier, 2. OG“ verrät Nachbarn und Vorbeigehenden mehr als nötig. Verstecken bringt dagegen keinen Schutz.
MAC-Filter	kein Sicherheitsmerkmal	Lässt sich in Minuten umgehen und macht vor allem Ihnen Arbeit. Kein Ersatz für gute Verschlüsselung.

Das WLAN-Passwort weitergeben

Besuch bekommt das Gastnetz, nicht das Hauptnetz — siehe nächstes Kapitel. Viele Router erzeugen dafür einen QR-Code zum Abscannen. Das ist bequemer als Diktieren und verrät das Kennwort nicht nebenbei am Tisch.

Das Gastnetz ist die wichtigste Funktion

Ein Gastnetz ist ein zweites WLAN mit eigenem Passwort, dessen Geräte untereinander und zum Hauptnetz keinen Zugriff haben. Es kostet nichts, steckt in fast jedem Router — und wird selten benutzt.

✓ INS GASTNETZ

Besuch, Fernseher, Saugroboter, Steckdosen, Lampen, Waage, Drucker, alles ohne Updates, alles aus günstiger Produktion. Kurz: alles, dem Sie nicht wirklich vertrauen.

✗ INS HAUPTNETZ

Nur, was Ihre Daten trägt und gepflegt wird: Rechner, Handys, Netzwerkspeicher. Und auch das nur, solange es Updates bekommt.

WARUM DAS SO WIRKSAM IST

Vernetzte Kleingeräte sind der schwächste Punkt im Haushalt: billig, selten aktualisiert, oft jahrelang unbeachtet. Im Gastnetz bleibt ein übernommenes Gerät ein einzelnes Problem, statt zum Sprungbrett zu allen anderen zu werden.

- ✓ Im Router prüfen, ob das Gastnetz auch die **Trennung der Geräte untereinander** aktiviert hat — die Option heißt oft „Geräte dürfen untereinander kommunizieren“ und gehört aus.
- ✓ Eigenes, langes Passwort vergeben. Ein Gastnetz mit „12345678“ ist kein Gastnetz.
- ✓ Manche Steuerung funktioniert dann nur noch über die Hersteller-Cloud statt direkt. Das ist der Preis — meist ist er es wert.
- ✓ Für Besuch ein zeitlich begrenztes Gastnetz nutzen, wenn der Router das anbietet.

Vernetzte Geräte auswählen

Die wichtigste Entscheidung fällt vor dem Kauf. Ein Gerät, das keine Updates bekommt, lässt sich später nicht absichern — es bleibt so unsicher, wie es ausgeliefert wurde.

Wie lange Updates?

Seriöse Hersteller nennen einen Zeitraum. Steht dazu nichts, ist das die Antwort.

Geht es ohne Cloud?

Geräte, die nur über einen Server des Herstellers funktionieren, sind wertlos, wenn dieser abgeschaltet wird. Das passiert regelmäßig.

Welches Konto?

Jedes Gerät bringt ein weiteres Konto mit. Eigenes Passwort, wo möglich 2FA — sonst hängt die Wohnungssteuerung an einem schwachen Kennwort.

Was passiert bei Ausfall?

Türschloss, Heizung und Rauchmelder sollten auch ohne Internet und ohne App funktionieren.

Nach dem Auspacken

- 1 **Werkskennwort ändern** — bei vielen Geräten lautet es „admin“ oder steht in der Anleitung, die jeder lesen kann.
- 2 **Firmware aktualisieren**, oft schon zur Einrichtung nötig.
- 3 **Ins Gastnetz hängen**, nicht ins Hauptnetz.
- 4 **Nicht benötigte Funktionen abschalten**: Mikrofon, Fernzugriff, Statusmeldungen an den Hersteller.
- 5 **Notieren**, was im Haushalt vernetzt ist. Diese Liste brauchen Sie beim nächsten Sicherheitsvorfall — und bei einem Umzug.

Kameras, Mikrofone und Sprachassistenten

Geräte mit Kamera und Mikrofon verdienen eine eigene Betrachtung — nicht weil sie technisch anders sind, sondern weil ein Fehler hier unmittelbar die Privatsphäre trifft, auch die von Gästen und Kindern.

- ✓ Keine Kamera in Schlaf-, Bade- und Kinderzimmer. Auch nicht „nur zur Sicherheit“ und auch nicht mit abgeklebter Linse.
- ✓ Aufnahmen möglichst lokal speichern, nicht in einer Hersteller-Cloud, deren Zugriffe Sie nicht sehen.
- ✓ Sprachassistenten haben eine Stummschalttaste, die das Mikrofon körperlich trennt. Sie ist genau dafür da.
- ✓ Gespeicherte Sprachaufzeichnungen im Konto des Anbieters regelmäßig löschen und die Auswertung zur „Verbesserung“ abschalten.
- ✓ Babyfone mit Internetanbindung sind besonders häufig betroffen. Ein Gerät ohne Cloud ist hier die bessere Wahl.

! Kameras und andere Menschen

Eine Kamera, die auf Gehweg, Nachbargrundstück oder gemeinsam genutzte Bereiche zeigt, ist nicht nur unhöflich, sondern rechtlich heikel. Wer Besuch empfängt, sollte auf Kameras und mithörende Geräte hinweisen — auch das ist Teil des Datenschutzes. Welche Rechte Betroffene haben, steht in „**Deine Rechte an deinen Daten**“.

Portfreigaben und Fernzugriff

Eine Portfreigabe macht ein Gerät aus dem Heimnetz weltweit erreichbar. Das ist manchmal gewollt — aber fast immer gibt es einen besseren Weg, und viele Freigaben entstehen versehentlich.

UPnP

Erlaubt Geräten, sich selbst Freigaben einzurichten — ohne Rückfrage. Bequem für Spielekonsolen, riskant für alles andere. Im Zweifel aus.

Manuelle Freigaben

Regelmäßig durchsehen. Freigaben aus einem alten Projekt bleiben sonst jahrelang offen stehen.

Besserer Weg: VPN

Viele Router bringen einen eigenen VPN-Zugang mit. Damit sind Sie von unterwegs im Heimnetz, ohne einzelne Geräte offenzulegen.

Was ohnehin geht

Netzwerkspeicher und Kameras bieten oft einen Hersteller-Zugang. Dann liegt das Vertrauen dort — bewusste Entscheidung, aber keine offene Tür.



Selbsttest

Schauen Sie im Router unter „Portfreigaben“, „Freigaben“ oder „Virtuelle Server“ nach, was dort eingetragen ist. Jeder Eintrag, den Sie nicht erklären können, gehört gelöscht. Ein Gerät, das dadurch nicht mehr funktioniert, meldet sich — dann kann man gezielt entscheiden.

DNS im Heimnetz

Wer den DNS-Server am Router einträgt, ändert ihn für alle Geräte im Haushalt — auch für die, die selbst keine Einstellung dafür haben. Das ist die wirksamste Stelle für einen Schutzfilter und zugleich die mit den meisten Nebenwirkungen.

Vorteil

Ein einziger Eintrag wirkt für Fernseher, Konsole, Gästehandy und jedes vernetzte Kleingerät.

Nachteil

Fehlblockaden treffen alle. Und wer im Haushalt nicht weiß, dass ein Filter aktiv ist, sucht den Fehler an der falschen Stelle.

- ✓ Erst an einem Gerät testen, dann am Router eintragen.
- ✓ Die vorherigen Werte notieren, um zurückstellen zu können.
- ✓ Im Haushalt Bescheid sagen, dass ein Filter aktiv ist und wie eine Warnseite aussieht.
- ✓ Manche Geräte ignorieren den Router-DNS und fragen fest verdrahtet einen eigenen Server. Das lässt sich am Router meist unterbinden — aber nicht immer.



Anbieter, Profile und Adressen

Welche Anbieter es gibt, was sie filtern und warum die Wahl eine Vertrauensfrage ist, steht ausführlich in „Cybersecurity im Alltag“, Kapitel „DNS verstehen: das Telefonbuch des Internets“ und den drei folgenden.

Wenn ein Gerät befallen ist

Anzeichen sind selten eindeutig: Das Netz wird langsam, ein Gerät ist heiß oder aktiv, obwohl niemand es benutzt, im Router tauchen unbekannte Geräte auf, oder der Anbieter meldet auffälligen Verkehr.

- 1 **Gerät trennen** — Stecker ziehen oder im Router sperren. Das begrenzt den Schaden sofort.
- 2 **Router-Zugangsdaten ändern** und prüfen, ob dort unbekannte Freigaben oder ein geänderter DNS-Eintrag stehen. Beides sind typische Spuren.
- 3 **Firmware des betroffenen Geräts aktualisieren** oder es auf Werkseinstellungen zurücksetzen.
- 4 **Passwörter der zugehörigen Konten ändern**, von einem sauberen Gerät aus.
- 5 **Entscheiden, ob das Gerät bleibt**. Bekommt es keine Updates mehr, ist Ersatz die einzige dauerhafte Lösung.

i **Geräteliste im Router**

Die Übersicht der verbundenen Geräte ist das nützlichste Werkzeug für diesen Fall — vorausgesetzt, Sie haben sie einmal im ruhigen Zustand angesehen. Wer weiß, was normal ist, erkennt das Unnormale.

! **Der Router selbst**

Ist der Router betroffen, hilft nur ein Zurücksetzen auf Werkseinstellungen mit anschließender Neueinrichtung — und ein neues Admin-Passwort. Danach alle Einstellungen aus dieser Broschüre erneut prüfen, denn sie sind mit zurückgesetzt.

Spickzettel zum Ausdrucken

ROUTER

- ☐ Admin-Passwort geändert
- ☐ Automatische Updates an
- ☐ Fernzugriff aus
- ☐ WPS aus

WLAN

- ☐ WPA3 oder WPA2
- ☐ Langes, einzigartiges Passwort
- ☐ Netzname ohne Namen/Adresse
- ☐ Gastnetz eingerichtet

VERNETZTE GERÄTE

- ☐ Werkskennwörter ersetzt
- ☐ Alle im Gastnetz
- ☐ Keine Kamera in privaten Räumen
- ☐ Portfreigaben durchgesehen

MEINE ANGABEN

Routermodell:

Anbieter-Hotline:

Alter DNS-Eintrag:

Letzte Prüfung am:

WENN SIE NUR EINE SACHE TUN

Richten Sie ein Gastnetz ein und hängen Sie jedes vernetzte Kleingerät hinein. Kein anderer Handgriff trennt Wichtiges und Unsicheres so wirksam voneinander.

Quellen und weiterführende Hinweise

BSI: Router, WLAN und VPN

bsi.bund.de → Verbraucher → Netzwerk-Sicherheit

BSI: Smart Home und Internet der Dinge

bsi.bund.de → Verbraucher → Smart Home

BSI: Sicherheitskennzeichen für vernetzte Produkte

bsi.bund.de → IT-Sicherheitskennzeichen

Verbraucherzentrale: Smart-Home-Geräte und Datenschutz

verbraucherzentrale.de → Digitale Welt → Smart Home

Wi-Fi Alliance: WPA3

wi-fi.org → Security

Quad9: Service Addresses & Features

quad9.net/service/service-addresses-and-features/

DNS4EU: Public Service

joindns4.eu/for-public

Cloudflare: 1.1.1.1 Setup and Families

developers.cloudflare.com/1.1.1.1/setup/

**Hinweis**

Diese Broschüre ersetzt keine individuelle IT-Beratung. Router-Menüs unterscheiden sich stark und ändern sich mit Firmware-Updates. Im Zweifel gilt die Anleitung Ihres Herstellers.

Weitere Broschüren dieser Reihe

- Cybersecurity im Alltag** — Links, Phishing, Passwörter, 2FA, DNS, öffentliche WLANs und Notfälle.
- Social Media Sicherheit** — Konten, Privatsphäre-Einstellungen, Fake-Profile, Datenweitergabe.
- Smartphone absichern** — Sperre, Berechtigungen, App-Quellen, Verlust, Gerätewechsel, Backups.
- Heimnetz und Smart Home** — diese Broschüre
- Kinder online begleiten** — Für Eltern: Altersgrenzen, Regeln, Mobbing, Grooming, Anlaufstellen.
- Deine Rechte an deinen Daten** — DSGVO praktisch: Auskunft, Löschung, Übertragbarkeit, Musterschreiben.
- Gruppen sicher organisieren** — Rollen, Regeln, Störer, Treffen, Voice, Minderjährige in der Gruppe.
- Allergene und Kennzeichnung** — Die 14 Pflichtangaben, Zutatenlisten lesen, „kann Spuren enthalten“.
- Erste Schritte** — Zweiseitiges Merkblatt zum Einstieg — kein Heft.

Weitergabe und Lizenz

Herausgeber

Plotspace.eu · info@plotspace.eu
Anschrift und Verantwortlicher im Impressum:
plotspace.eu/impressum

Lizenz

CC BY 4.0 — Kopieren, Weitergeben und Bearbeiten ausdrücklich erlaubt. Bitte „Plotspace.eu“ als Quelle nennen und Änderungen kenntlich machen; bearbeitete Fassungen dürfen nicht so wirken, als kämen sie von Plotspace.eu. creativecommons.org/licenses/by/4.0/deed.de
Schriften: Public Sans und IBM Plex Mono, SIL Open Font License 1.1.

Diese Broschüre darf einzeln weitergegeben werden. Sie ist so aufgebaut, dass sie für sich allein verständlich bleibt; Querverweise auf die übrigen Hefte sind Ergänzung, keine Voraussetzung.