

DER GROSSE WLAN- GUIDE

**Perfektes
Netzwerk**
Garantiert nie wieder
Probleme mit dem
Heimnetz!

EXCLUSIV

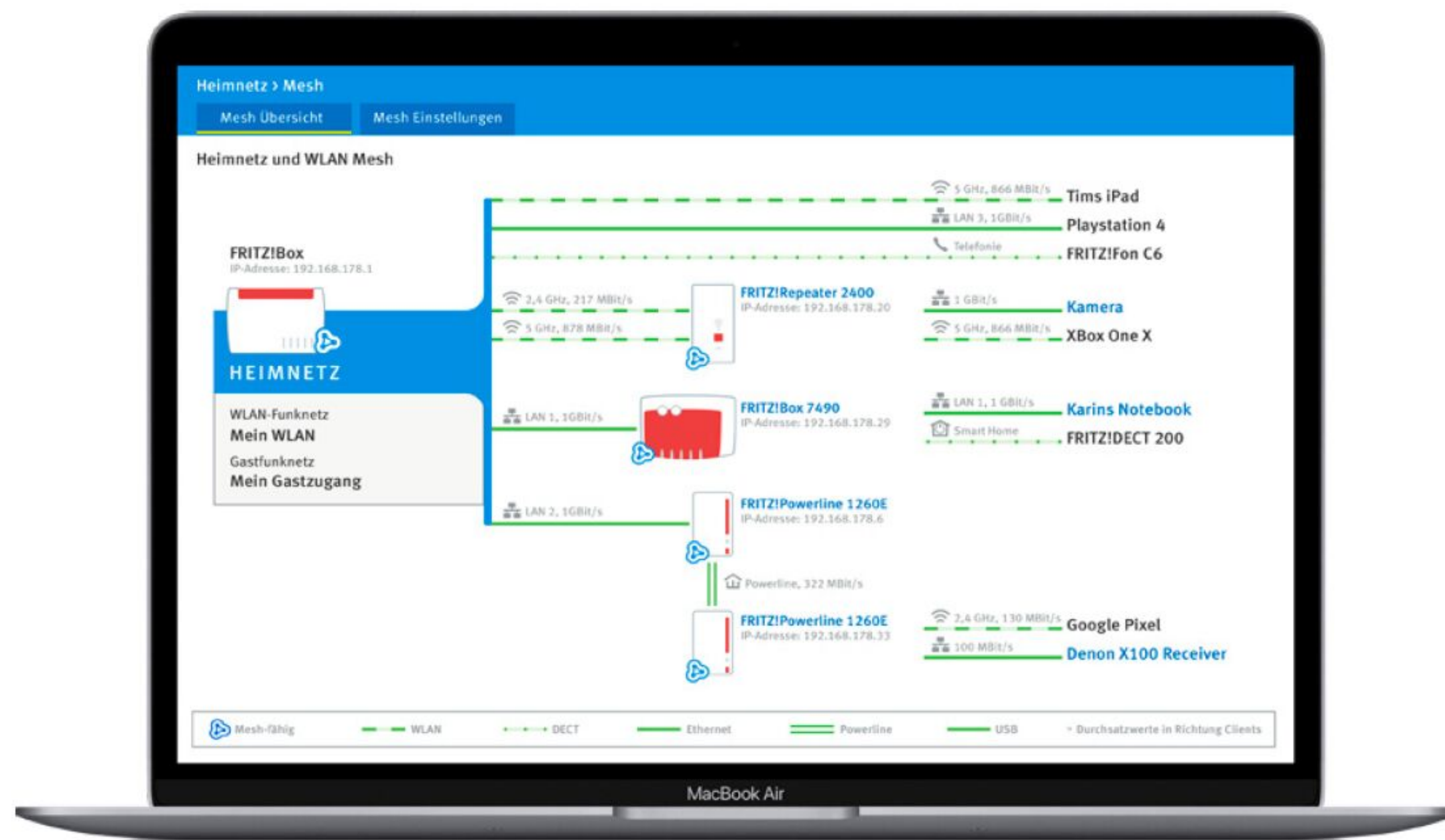


Das Geschenk für jeden Apple-Fan!

Die besten Bücher, die wir je geschrieben haben!



Jetzt bestellen: maclife.de/buecher



Netzwerkverbindungen sind heute so alltäglich wie die Versorgung mit Strom oder Wasser. Und doch gibt es immer wieder Probleme.



Wer schon einmal vor einem Gerät stand oder saß, das eigentlich „online“ sein „musste“, es aber irgendwie doch nicht war, weiß, wie nervenaufreibend der Betrieb und die Wartung selbst relativ überschaubarer Heimnetzwerke sein kann. Auch obschon vieles über die Jahre immer simpler geworden ist, gibt es nach wie vor viele Stolpersteine, die schnell das ganze Konstrukt ins Wanken bringen können.

Die beste Option, mit solchen Unwegsamkeiten umzugehen, ist, sie von vornherein zu vermeiden. Das ist natürlich leichter gesagt, als es in der Praxis umzusetzen ist. Wer aber auf ein paar Grundregeln vertraut, ist bereits gut aufgestellt.

Beispielsweise, dass sich das Sparen bei Netzwerkequipment, etwa dem Router, meist nicht bezahlt macht. Oder die, dass Geräte, die per Kabel angeschlossen werden können, auch per Kabel angeschlossen werden sollten. Wie du dein Netzwerk vernünftig planst, erweiterst und im Zweifel reparierst, erfährst du in diesem Spezial.

Herzlichst,

Sebastian Schack
Sebastian Schack

Aus dem Verlag

Wusstest du, dass wir neben diesem Spezial auch noch zahlreiche weitere Magazine im Angebot haben?



Mit der iPhone Bibel bieten wir zu iOS 17 und dem iPhone ein Kompendium an.



Mac Life erscheint monatlich neu und informiert dich über das aktuelle Apple-Geschehen.

Impressum

Verlag: falkemedia GmbH & Co. KG, An der Halle 400 #1, 24143 Kiel, Tel. +49 (0)431 200 766 00, info@falkemedia.de, HRA 8785 Amtsgericht Kiel **Herausgeber:** Kassian Alexander Goukassian (V.i.S.d.P.) **Chefredakteur:** Sebastian Schack (s.schack@falkemedia.de) **Redaktion (redaktion@maclife.de):** Sophie Bömer (sb), Julia Kemp (jk), Stefan Molz (sm), Sven T. Möller (stm), Holger Sparr (hs), Thomas Raukamp (tr), Matthias Zehden (maz) **Redaktionelle Mitarbeiter:innen:** Uwe Albrecht, Nadine Juliana Dressler, Tobias Friedrich, Gerd M. Hofmann, Joachim Kläschen, Udo Lewalter, Benjamin Otterstein, Matthias Parthesius, Laura Plautz, Ilseken Roscher, Christian Steiner **Titelgestaltung und Layout:** Sven T. Möller **Korrektur und Lektorat:** Julia Kemp, Sophie Bömer **Datenschutz:** Jürgen Koch (datenschutzfragen@falkemedia.de) **Urheberrecht:** Alle hier veröffentlichten Beiträge sind urheberrechtlich geschützt. Reproduktionen jeglicher Art sind nur mit Genehmigung des Verlags gestattet.

Perfektes Netzwerk in jedem Winkel

Ein Netzwerk alltagstauglich einzurichten, ist kein Kinderspiel. Aber wenn du's einmal richtig gemacht hast, brauchst du dich viele Jahre nicht mehr darum zu kümmern.

TEXT: SEBASTIAN SCHACK



Eigentlich ist es eine Schande, dass wir uns als Privatmenschen immer noch mit Infrastrukturthemen befassen müssen. Sollte so etwas, wie das Netzwerk daheim nicht längst gelöst sein? Einfach und verständlich für alle Anwender:innen? Ja, sollte es. Dass wir davon noch weit entfernt sind, daran ist zum Teil auch Apple schuld. Mit der AirPort Express und der AirPort Extreme hatte Apple über Jahre erstklassiges Netzwerk-Equipment im Programm, das nicht nur angenehm fürs Auge war, sondern sich auch kinderleicht konfigurieren und bedienen ließ. Auch machten Apples Geräte bereits von Haus aus vieles richtig, sodass sich niemand weitergehend mit ihnen beschäftigen musste.

Als Apple den Netzwerkgerätemarkt verließ, fehlte es der ganzen Branche merklich an Innovationsdruck und es benötigte eine ganze Zeit, bis andere Apples Lücke zu füllen vermochten. Zumindest Hersteller hochwertigerer Lösungen haben verstanden und bieten inzwischen praktisch durchgängig Geräte an, bei denen sich Anwender:innen zumindest in Sachen Grundlagen um nichts kümmern müssen. Insbesondere auf dem deutschen Markt ist der Branchenprimus AVM mit seiner Fritzbox, bei der nicht nur die Konfigurationsoberfläche, sondern auch das äußere Erscheinungsbild über die Jahre deutlich „menschenfreundlicher“ wurde.

Allerdings: Kaum irgendwo gilt die alte „Werner“-Weisheit, dass

Die Fritzbox von AVM begleitet uns in vielen Varianten schon seit Jahren. Zu Recht. Auf sie ist Verlass.

Arbeit Arbeit nach sich zöge, so sehr wie in der IT. Immer mehr Menschen besitzen immer mehr netzwerk- und internetfähige Geräte, weshalb sie an immer mehr Orten das perfekte Netz erwarten. Nicht zuletzt auch bei sich zu Hause. Egal, ob im Wohn- oder Schlafzimmer, ob in der Küche oder auf der Toilette – die Daten müssen rauschen.

Es reicht also unter Umständen nicht mehr aus, nur einen WLAN-Router irgendwo im Haus oder in der Wohnung zu platzieren. Du benötigst „Repeater“, die das Netzwerk erweitern. Idealerweise sogar solche, die ein sogenanntes „Mesh“-Netzwerk aufspannen. Was das ist und wie das funktioniert, liest du in einem gesonderten Artikel in unserem



Titelthema ab Seite 32 in dieser Ausgabe. An dieser Stelle kümmern wir uns allerdings erst einmal um die Grundlagen.

Kabel vs. Funk

Falls du dich länger nicht mit dem Thema Netzwerkinfrastruktur auseinandergesetzt hast, können wir dich zunächst einmal beruhigen: In der jüngeren Vergangenheit ist vieles deutlich besser geworden. Um die richtige Kanalwahl für dein Funknetzwerk musst du dich nur noch in absoluten Sonderfällen kümmern und auch Überlegungen, welche Verschlüsselungsmethode wohl die bessere (und zugleich kompatibelere) ist, sind längst nicht mehr nötig. Zudem erreichen moderne WLAN-Router bessere Reichweiten und

höhere Übertragungsgeschwindigkeiten. Manche können deine Geräte sogar im dreidimensionalen Raum orten und zielgerichtet ansprechen. Ist es also endlich an der Zeit, alle Netzkabel wegzuschmeißen?

Nein, leider nicht, und wir sind uns auch nicht so sicher, ob wir diese Zeit noch erleben werden. Dabei spricht in vielen Szenarios kaum etwas dagegen, komplett auf Funk zu setzen. Wenn du nur eine überschaubare Fläche und ohnehin nur dein MacBook, dein iPhone und vielleicht noch den „smarten“ Fernseher mit Funknetzwerk versorgen musst, ist das vermutlich kein Problem.

Nach wie vor gilt allerdings, dass direkte Kabelverbindungen weit weniger stör- und ausfallan-

fällig sind, als es Funkverbindungen sind. Unsere Empfehlung ist es also weiterhin, zumindest einmal alle Geräte, die sich in relativer Nähe zum WLAN-Router befinden, mit Netzkabeln anzuschließen. Was nicht im WLAN hängt, kann dort auch nicht für Konfusion sorgen. Außerdem gibt es zahlreiche Geräte, die von dem Stabilitätsplus dieser Art der Verbindung profitieren. Wir denken da etwa an Smarthome-Bridges, wie sie etwa für Philips-Hue-Komponenten nötig sind. Auch Geräte, die regelmäßig große Datenmengen abfragen oder versenden, sind mit Kabelanbindungen oft besser bedient.

Zumindest im privaten Bereich sind Netzkabel allerdings inzwischen kein Muss mehr.

Die richtige Hardware

Netzwerk-Equipment gibt es wie Sand am Meer und dazu auch noch in jeder Preisklasse. Du kannst für die Vernetzung eines klassischen Einfamilienhauses einen niedrigen dreistelligen Betrag genauso ausgeben wie einen hohen vierstelligen. Die gute Nachricht ist: „Viel hilft viel“ gilt nur in Grenzen. Es gibt keine Komponenten, bei denen du partout das neueste, beste und teuerste, das der Markt zu bieten hat, benötigst. Aufpassen und wenn möglich nicht sparen solltest du allerdings beim Herzstück deines Heimnetzwerks: dem Router.

Ein Router vermittelt – im klassischen Sinn – Datenpakete zwischen den einzelnen Teilnehmern in deinem Netzwerk. Das Herstellen der Verbindung zum Internet gehört nicht zu seinen originären Aufgaben. Die Realität sieht inzwischen allerdings anders aus. Praktisch in jedem Haushalt steht ein Gerät, das Internet-Modem, Kabel-Router und WLAN-Zugangspunkt in einem ist. Wenn du nicht genau weißt, dass dein Projekt für jede dieser Aufgaben ganz spezielles Equipment erfordert, raten wir auch nicht von solchen All-in-one-Lösungen ab. Sie sind bequem und verringern das Kabelgewirr. Wir empfehlen dabei nach wie vor gerne die Fritzbox von AVM, mit der wir seit vielen Jahren gute Erfahrungen machen.



WLAN

Die Technologie schreitet immer weiter voran – und das ist gut so. Fakt ist aber auch, dass du nicht jeden Schritt mitzugehen brauchst. Was funktioniert, muss nicht erneuert werden.

Fachbegriffe

Ethernet: Eine Netzwerkverbindung in einem LAN (Local Area Network) per Kabel. Hierfür werden vorwiegend Kabel der Kategorien 6A und 7 (Cat 6A und Cat 7) verwendet. Inzwischen können Übertragungsgeschwindigkeiten von bis zu 10 Gbit/s problemlos erreicht werden.

Glasfaser, auch LWL (Lichtwellenleiter): Eine Kabelverbindung, durch die Daten, anders als in Kupferkabeln, als Lichtimpuls übertragen werden. LWL können Daten mit sehr hoher Geschwindigkeit über sehr weite Distanzen übertragen und kommen daher vor allem beim Ausbau des „schnellen Internets“ und in Rechenzentren zum Einsatz.

Powerline: Eine Technologie, bei der Datenpakete über Stromleitungen übertragen werden. Findet diese Übertragung über die fixen Stromleitungen im Haus statt, wird gelegentlich auch von „PowerLAN“ gesprochen. P. ist eine Alternative für die Vernetzung von Räumen, wenn das Verlegen von neuen Netzkabeln oder der Einsatz von WLAN keine Option sind.

VPN: Ein Virtual Private Network verbindet mehrere getrennte Netzwerke verschlüsselt über ein öffentliches Netz, zum Beispiel das Internet. VPN kommen etwa bei Homeoffice-Lösungen zum Einsatz.

Wifi, auch Wi-Fi: Ein Kunstwort zur Bezeichnung von Funknetzwerken, vor allem im englischsprachigen Raum, während in Deutschland eher W-LAN (für Wireless LAN) gebräuchlich ist. Wi-Fi steht für „Wireless Fidelity“, analog zu Hi-Fi aus dem Audibereich.

WPA2, WPA3: Steht für „Wi-Fi Protected Access“ und bezeichnet den Verschlüsselungsstandard, mit dem eine Funkverbindung abgesichert ist. Die Vorgänger WEP und WPA gelten als unsicher und lassen sich inzwischen innerhalb von Sekunden aufbrechen.

Das richtige Kabel

Man mag es kaum glauben: Auch im Jahr 2022 solltest du nicht einfach das erstbeste Netzkabel im Elektro-Fachmarkt kaufen, wenn du Wert auf maximale Performance und bestmögliche Stabilität deines Netzes legst. Tatsächlich ist die Wahl nicht trivial, wenn du dich nicht eingehend mit dem Thema beschäftigst.

Eine Glasfaser-Verkabelung lassen wir dabei als Option einmal außen vor. Ja, sicherlich ist das die zukunftstauglichste Variante, aber auch mit Abstand die teuerste – auch, weil es im privaten Bereich praktisch keine Endgeräte gibt, die direkt mit Glasfaserkabeln angebunden werden können. Für dich hieße das: Adapter, Adapter, Adapter.

Und was heißt eigentlich zukunftstauglich? Ja, durch Glasfaserleitungen können die Daten nur so flutschen, aber auch klassische Netzkabel bieten schon jetzt Übertragungsraten von um die 10 Gigabit pro Sekunde. Hier wiederum empfehlen wir die Verwendung von Kabeln nach dem Standard Cat 6A. Das „A“ ist dabei wichtig, bedeutet es doch, dass die im Kabel liegenden vier Aderpaare einzeln abgeschirmt sind, was eben für mehr Übertragungsgeschwindigkeit und eine geringere Störanfälligkeit sorgt. Außerdem verfügt Cat 6A anders als Cat 6 über keinen festen Kern, was Verlegearbeiten oft deutlich angenehmer macht.

Aber was ist mit dem ebenfalls verfügbaren Cat 7? Ist „mehr“ nicht immer auch gleich „besser“? In der Theorie ist das so. Diese Kabel sind noch einmal anders und in den meisten Fällen auch besser abgeschirmt und ermöglichen grundsätzlich auch noch höhere Übertragungsraten. Aber ganz ehrlich: Der Zeitpunkt, an dem die 10 Gbit/s von Cat 6A für den Heimgebrauch nicht mehr ausreichen, liegt noch in weiter Ferne. Einziger echter Vorteil für Cat 7: Mit diesen Kabeln kannst du Daten in oben genannter Geschwindigkeit unter idealen Bedingungen über eine Strecke von 100 Metern übertragen. Mit Cat 6A ist bereits nach 35 bis 50 Metern Schluss. Technisch gese-



hen gibt es also keinen Grund, der gegen Cat 7 spricht. Allerdings sind diese Kabel häufig teurer. Wenn du Cat-7-Kabel in guter Qualität zu einem günstigeren Preis als vergleichbare Cat-6A-Kabel findest, schlag zu!

Der Internet-Zugang
Wenn es dir wie uns geht, hast du schon über praktisch jeden Internetanbieter, der in deiner Gegend aktiv ist, etwas Schlechtes gehört. Das ist sicherlich auch darin begründet, dass Menschen gerne von besonders schlechten und besonders guten Erlebnissen erzählen. Wenn also der Internetzugang „einfach funktioniert“, dann ist das nichts, was einen gesteigerten Nachrichtenwert hätte. Wir wollen hier allerdings auch gar keinen Provider empfehlen, sondern vielmehr Zugangstechnologien diskutieren.

Was innerhalb deiner vier Wände gilt, gilt auch außerhalb: Funk funktioniert, aber wenn du die Wahl hast, solltest du zum Kabel greifen. Hier wiederum ist die erste Wahl eine Glasfaser-Anbindung. Schneller, moderner und zukunftssicherer geht nicht. Solltest du in einem Gebiet leben, in dem ein Glasfasernetz dem-



nächst ausgebaut werden soll, kann es sich lohnen, schnell einzusteigen: Anbieter auf Kund:innenjagd erlassen Kund:innen, die früh mit dabei sind, häufig die Anschlussgebühren, die schnell vierstellig sein können.

Wenn Glasfaser für dich aktuell keine Option ist, ist es unsere dringende Empfehlung, dich zunächst mit klassischen oder modernen DSL-Angeboten, also A-DSL oder V-DSL zu befassen, wobei Letzteres mehr Geschwindigkeit bietet. Wenn es dir irgendwie möglich ist, solltest du auf Internetzugänge über das TV-Kabel verzichten. Diese locken zwar oft mit günstigen Preisen und hohen Geschwindigkeiten, sorgen aber immer wieder für Probleme.

Diese sind in der Natur der Sache begründet: Bei Kabel-TV-Internetzugängen handelt es sich in aller Regel um „Shared Medium“-Zugänge, was bedeutet, als dass sich mehrere Anschlüsse die Netzressourcen teilen müssen. Wenn das Netz schlecht ausgebaut ist und ein Anbieter in einer Region („Cluster“) trotzdem sehr erfolgreich ist, nutzen viele Haushalte das Internet praktisch über eine Leitung, weshalb die Übertra-

gungsgeschwindigkeiten für alle einbrechen (können).

Der Gedanke von „Shared Medium“ ist nicht per se schlecht. Mobilfunk ist so organisiert, oder, wenn auch auf einer ganz anderen Skalengröße, dein WLAN zu Hause. Erste Wahl für den Internetzugang sollte es dennoch nicht sein.

Benötige ich eine Firewall?

Die kurze Antwort lautet: wahrscheinlich nicht. Aber was tut eine Firewall überhaupt? Du kannst „Firewall“ getrost wörtlich übersetzen: Brandmauer. Eine Brandmauer in Gebäuden sorgt dafür, dass ein ausgebrochenes Feuer nicht so leicht von einem in den nächsten Gebäudeteil überspringen kann. Eine Netzwerk-Firewall erledigt eine ganz ähnliche Aufgabe, indem sie versucht, das lokale Netzwerk vor all dem schädlichen Zeug da draußen zu schützen. Professionelle Firewalls sind eigenständige Geräte und verfahren im Allgemeinen nach dem System, erst einmal alles zu blockieren und nur durchzulassen, was über einen Satz von Regeln explizit erlaubt wird.

Ein guter Kompromiss für den Hausgebrauch sind Software-Fire-



Internet

Der Zugang zum Internet ist ein heikles Thema. Während grundsätzlich alle das Gleiche anbieten, gibt es im Detail teils eklatante Unterschiede – nicht nur beim Preis. Sich ausführlich zu informieren und Fragen zu stellen, lohnt sich unbedingt.

walls. Wie der Name vermuten lässt, laufen sie nicht auf gesonderter Hardware, sondern direkt auf deinem Computer. Dein Mac kommt selbstverständlich mit einer Software-Firewall.

Ob du sie versehentlich ausgeschaltet hast, kannst du in den Systemeinstellungen unter „Sicherheit & Datenschutz“ auf dem Reiter „Firewall“ sehen. Dort kannst du sie auch weitergehend konfigurieren.

Der Nachteil einer Software-Firewall: Sie schützt nur das Gerät, auf dem sie installiert ist und nicht das ganze Netzwerk, wie es eine Hardware-Firewall tut. Hinzu kommt allerdings, dass Netzwerk-Router ebenfalls eine Firewall integriert haben.

Um eine Firewall für dein Netzwerk musst du dich also wahrscheinlich nicht kümmern, weil du sehr wahrscheinlich bereits über eine verfügst – vielleicht ohne es zu wissen.

WLAN in alle Räumen

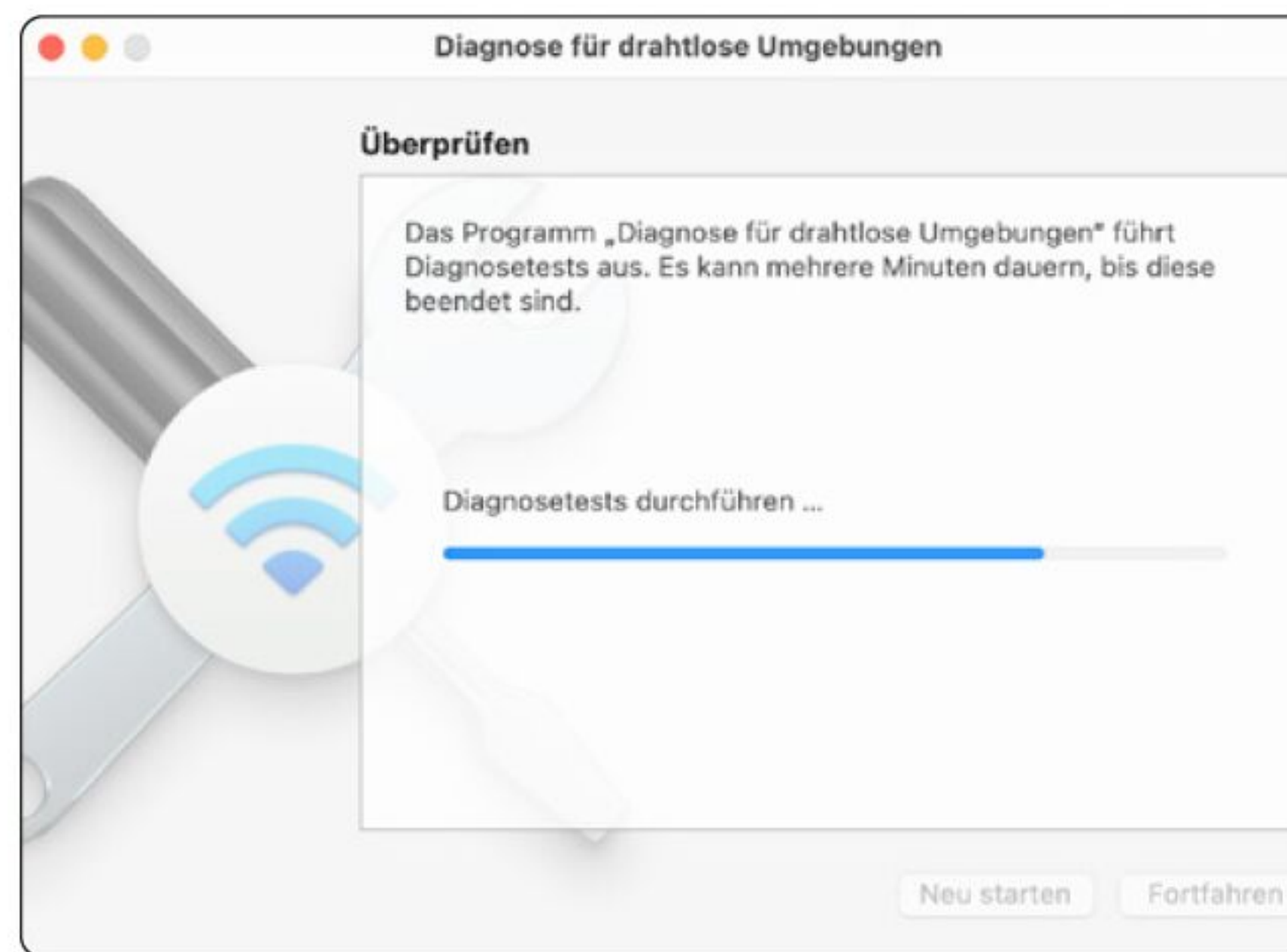
Wenn du dich mit den Grundlagen auseinandergesetzt und eine gute Basis geschaffen hast, kannst du dich gewissermaßen mit der Königsdisziplin des Heimnetzwerks beschäftigen: Wie gelingt es, überall guten Empfang zu haben? Die Lösung für diese Herausforderung heißt „Mesh“ und mehr dazu erfährst du auf den folgenden Seiten.

Was leistet der neue Funkstandard Wifi 6?

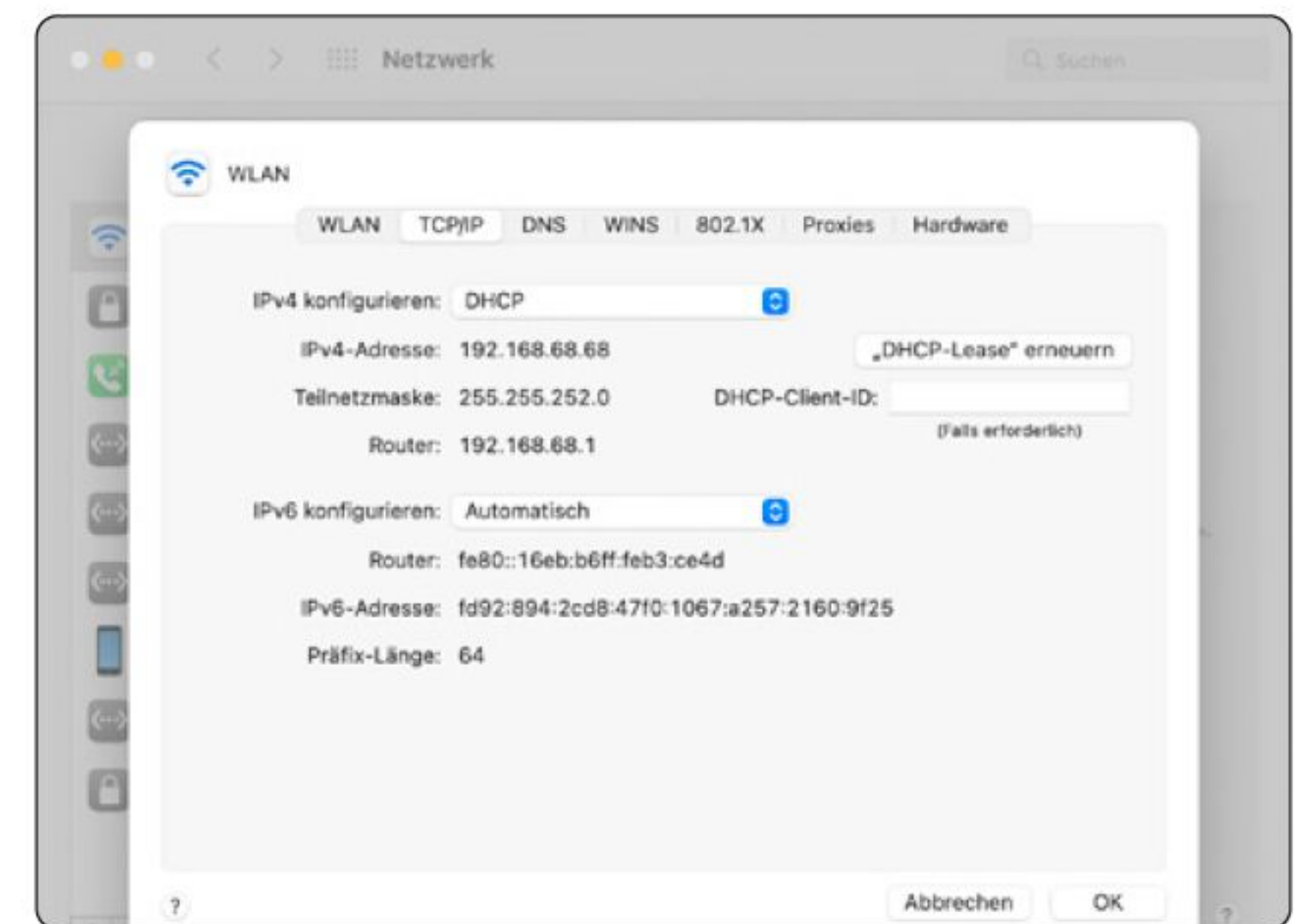
Zunächst einmal ist Wifi 6 nur ein Marketingname. Der eigentliche Name der neuen Technik lautet IEEE 802.11ax. Mit dem neuen Standard soll dem Umstand Rechnung getragen werden, dass sich inzwischen immer mehr WLAN-Geräte auf immer engerem Raum tummeln – und sich dabei mit ihrem Gefunke gegenseitig stören, was die Verbindungsqualität für alle beeinträchtigt. Mit einer OFDMA (Orthogonal Frequency Division Multiple Access) genannten Technologie gelingt es Wifi-6-kompatiblen Geräten, die Funkkanäle effizienter auszunutzen und so für mehr Bandbreite und geringere Latenzen zu sorgen. Großer Bonus: Auch für Geräte, die „nur“ im 2,4-GHz-Spektrum funken können, verdoppelt Wifi 6 die Datenrate.

Netzwerk-Probleme aufspüren

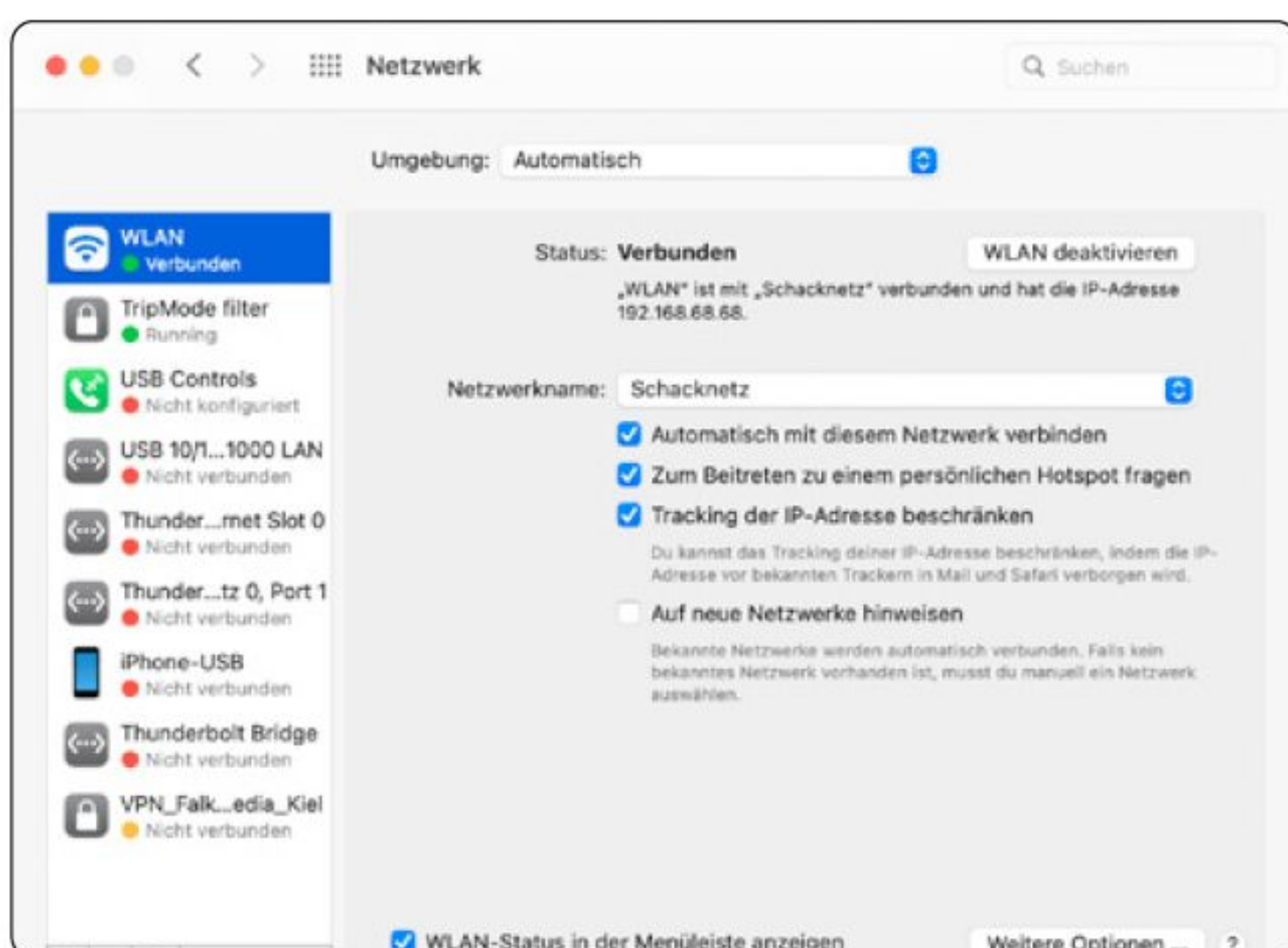
Wenn Probleme immer wiederkehren oder dein Netzwerk komplett lahmlegen, musst du etwas genauer hinschauen, um den Störenfried auszumachen. Sei dir nicht zu schade dafür, mit dem klassischen „Aus- und wieder Einschalten“ sämtlicher Geräte zu beginnen, wenn du eine bestimmte Netzwerkkomponente in Verdacht hast. Lasse das Gerät dabei für mindestens eine Minute ausgeschaltet. Wenn das dein Problem nicht löst, kannst du die folgenden Schritte ausprobieren, um das Problem zu lösen oder zumindest einzugrenzen. Glücklicherweise können dabei schon Bordmittel deines Mac hilfreich sein.



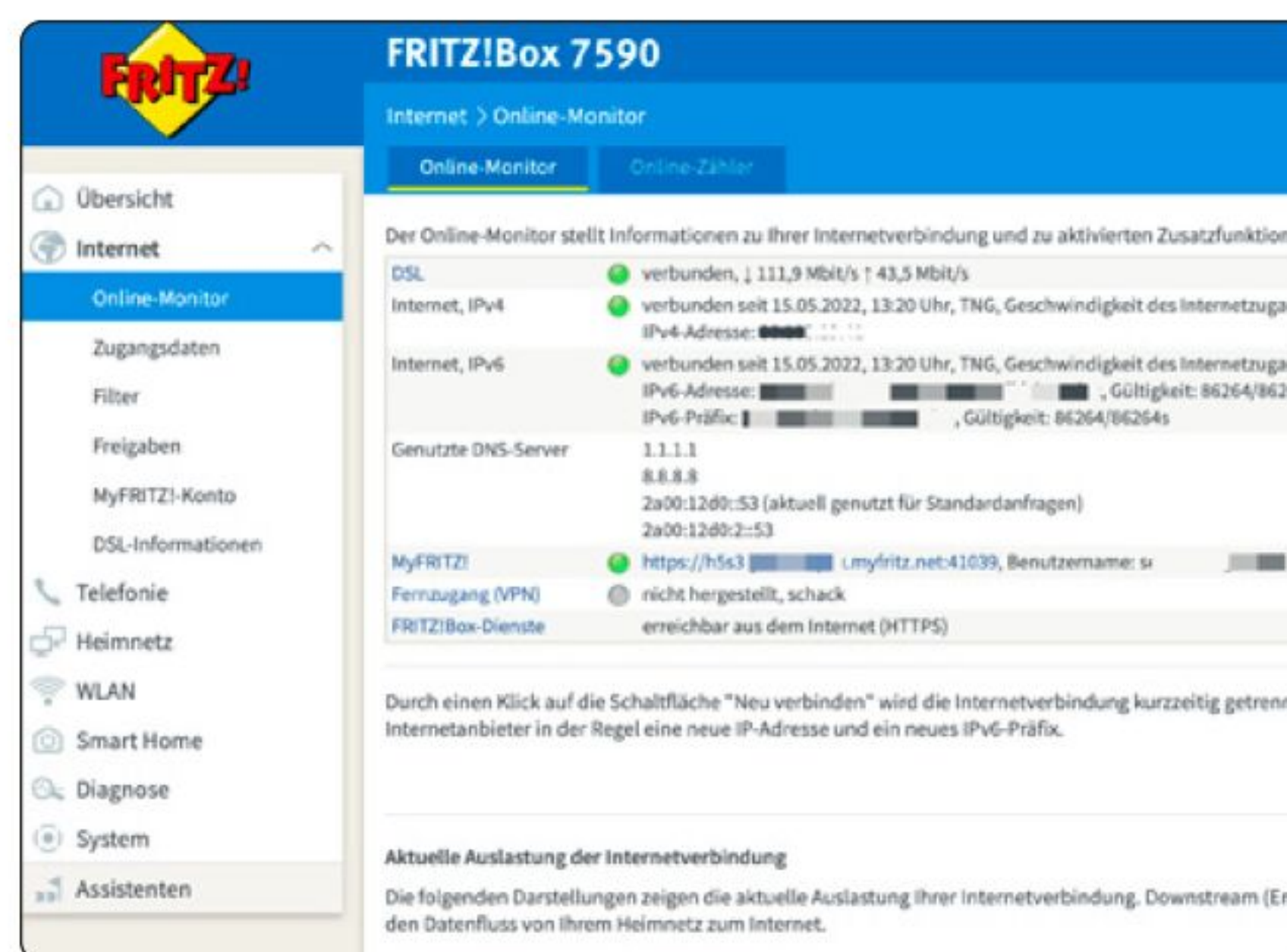
1 Nutze Spotlight auf deinem Mac. Suche und starte „Diagnose für drahtlose Umgebungen“, eine Analysesoftware von Apple. Ergänzend kann das „Netzwerkdienstprogramm“ Anhaltspunkte liefern.



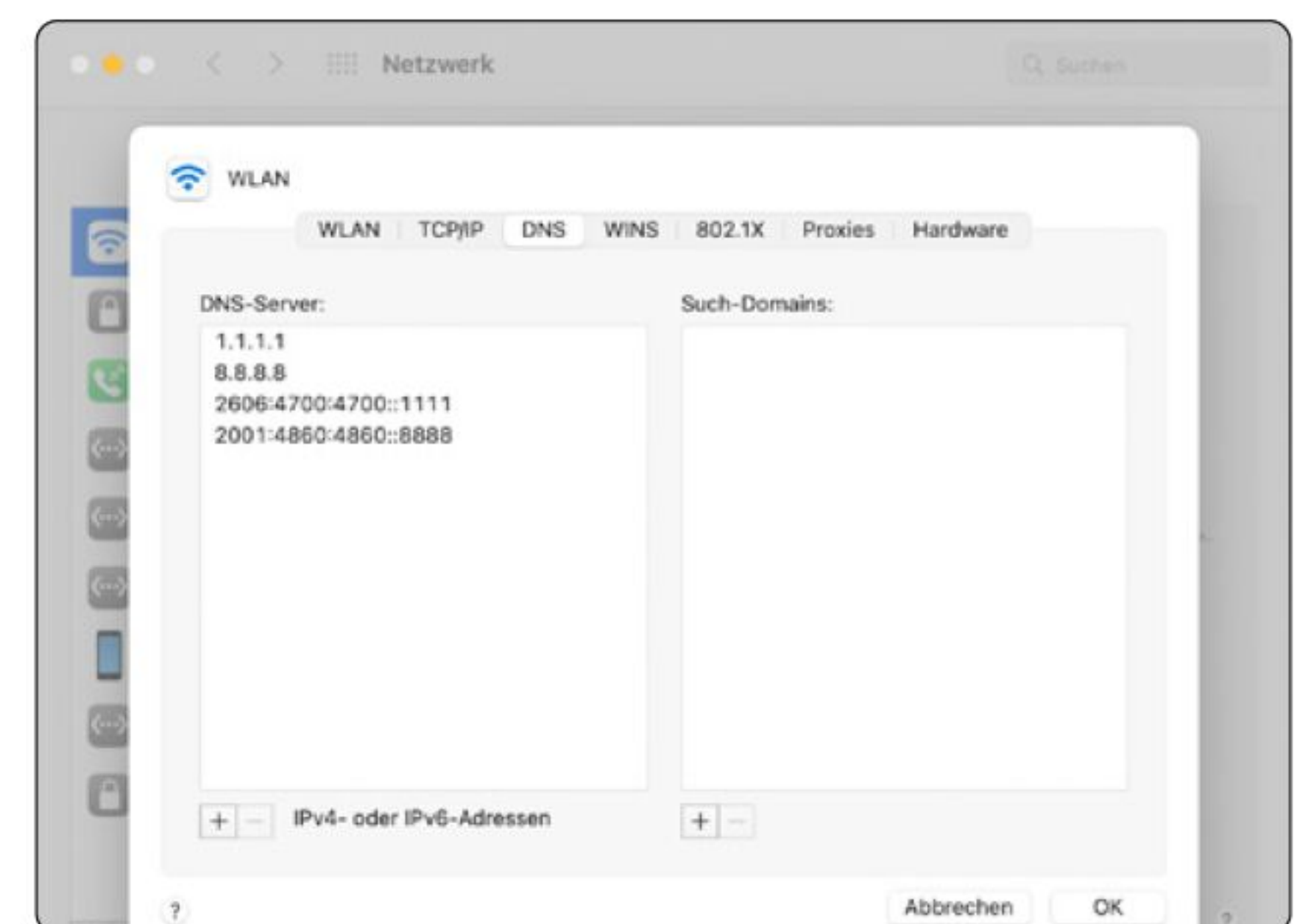
2 Wenn du keine Verbindung zum Netzwerk hast, öffne „Netzwerk“ in den Systemeinstellungen und prüfe, ob unter „Weitere Optionen > TCP/IP“ eine manuelle IP-Adresse konfiguriert oder DHCP aktiviert ist.



3 Wähle links deine Netzwerkverbindung aus und deaktiviere diese. Nach 30 Sekunden kannst du die Verbindung wieder aktivieren. Eine WLAN-Verbindung solltest du löschen und neu einrichten.



4 Prüfe auf deinem Router, ob eine Internetverbindung besteht, um den Fehler weiter einzugrenzen. Hat der Router keine Verbindung, kontaktiere am besten deinen Anbieter. Ist er online, ist vermutlich das Endgerät das Problem.



5 Wenn die Internetverbindung funktioniert, Webseiten sich aber nicht aufbauen, ist ein DNS-Problem wahrscheinlich. Konfiguriere in den Netzwerk-Systemeinstellungen einen neuen DNS-Server, etwa den mit der Adresse 1.1.1.1

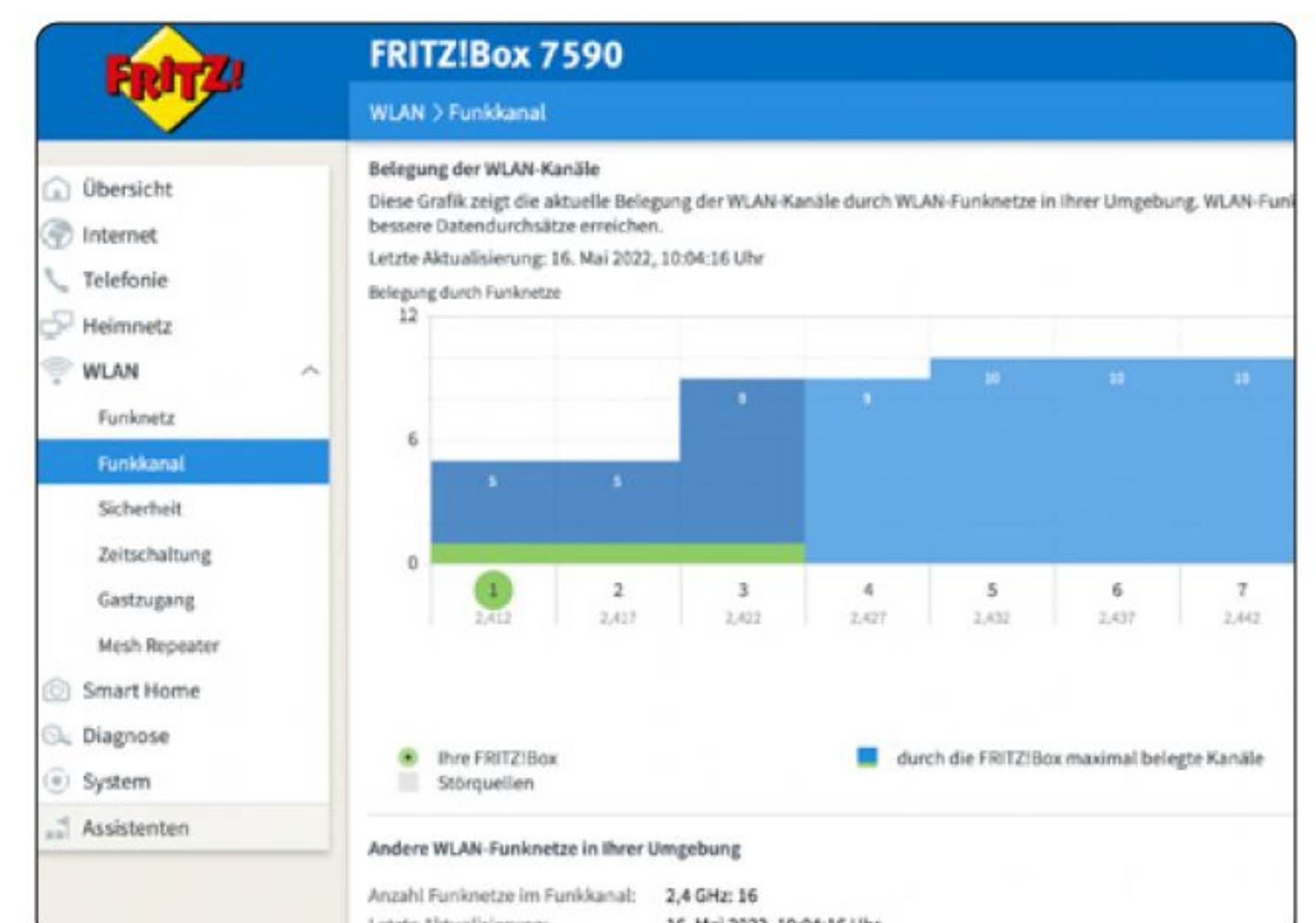
Störungen im Netzwerk beheben

ID	Network Name	Vendor	Signal	Channel	Channel Width
1F:...41:94	Sch...netz	TP-Link...	92%	36	160 MHz
E:...8:69:3D	Ring...p 3d	Ring	44%	1	20 MHz
D:...4:44:C7	FRIT...0 JD	AVM	28%	52	80 MHz
E:...A:3B:18	WLA...0139	Arcadyan...	26%	36	80 MHz
D:...4:44:C6	FRIT...0 JD	AVM	51%	1	20 MHz
B:B:...CE:52	Schacknetz	TP-Link...	60%	36	160 MHz
C:...3:41:D1	WLA...0139	Arcadyan...	48%	36	80 MHz
B:B:...D4:21	Schacknetz	TP-Link...	40%	36	160 MHz
C:...3:41:D2	WLA...0139	Arcadyan...	67%	6	20 MHz
D:...8:9B:6B	devolo-86b	devolo	66%	11	40 MHz
9:...0:86:6B	WLA...4868	Arcadyan...	48%	11	40 MHz
E:...A:3B:1C	WLA...0139	Arcadyan...	56%	6	20 MHz
B:...3:D4:20	Schacknetz	TP-Link...	61%	5	40 MHz
E:...2:6A:9C	alph...rs.de	AVM	1%	100	160 MHz
E:...A:3B:1B	Hidd...work	Arcadyan...	28%	36	80 MHz
C:...8:0B:5C	WLA...9478	Arcadyan...	48%	11	20 MHz

1 Suche den „WiFi Explorer Lite“ im Mac App Store und installiere die App. Beim Start zeigt dir die Anwendung eine Liste aller erkannten Netzwerke in der Umgebung. Wähle den passenden Eintrag aus.



2 Unter der Liste siehst du einen Graphen, der anzeigt, welche Kanäle die jeweiligen Netze belegen. Das in der Liste ausgewählte Netzwerk ist hervorgehoben. Je höher der Graph reicht, desto stärker ist das Signal.



3 Wenn das Netzwerk sich mit anderen überlappt, wechsele, wenn möglich, auf einen weniger stark belegten Kanal. Bleib mit dem Netz im störungsärmsten Kanal und überprüfe diese Einstellung von Zeit zu Zeit.

Jetzt Mitglied werden und **Vorteile sichern!**

Satte Rabatte:

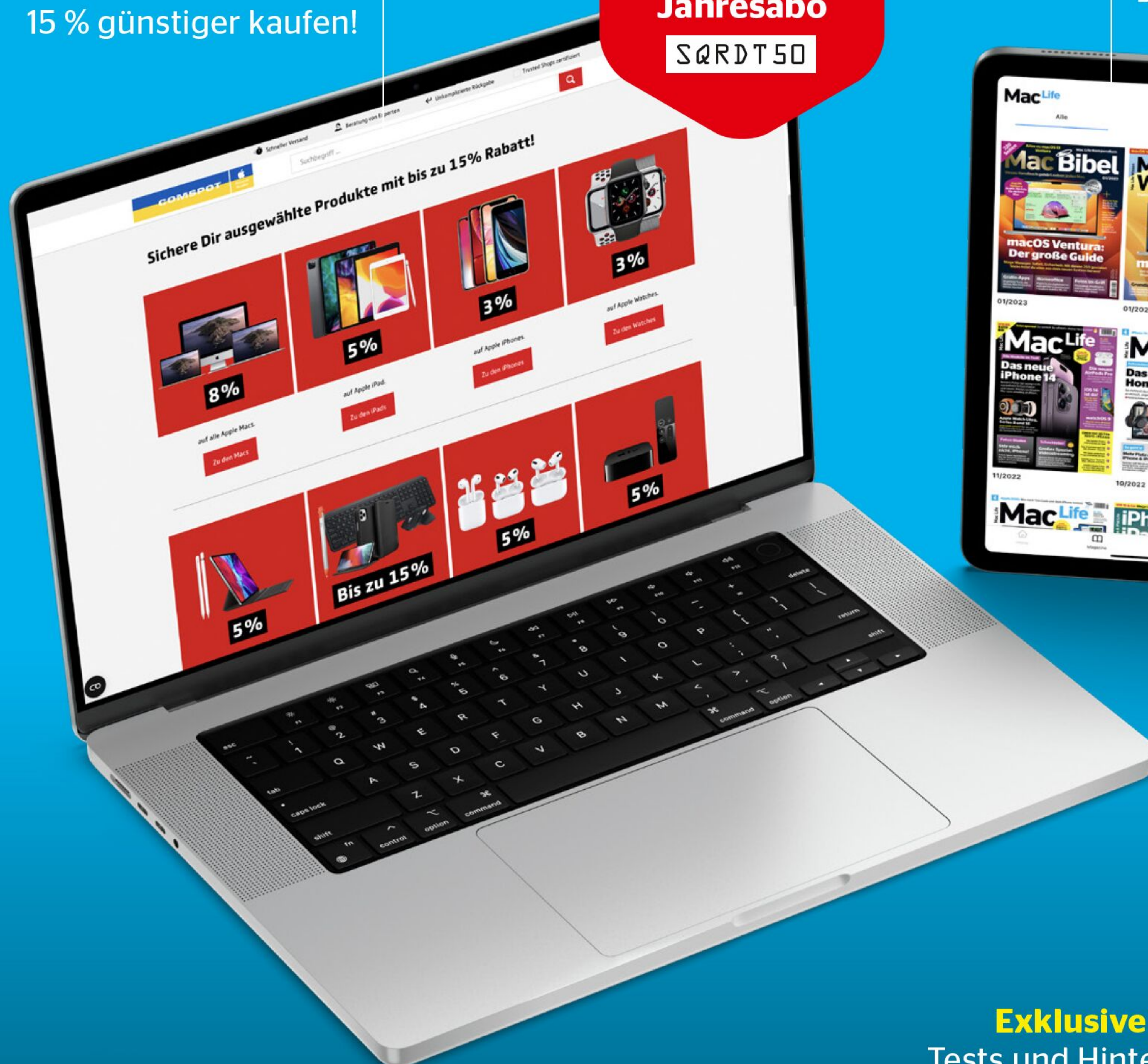
Mac, iPhone und iPad
sowie Zubehör bis zu
15 % günstiger kaufen!

**Extra:
50 % Rabatt
auf das
Jahresabo**

SQRDT50

Alle Ausgaben:

Das gesamte Archiv sowie
alle kommenden Hefte und
Bücher digital genießen!



Noch einfacher:
Scanne den Code
mit der Kamera
deines iPhone!



Exklusive Artikel:

Tests und Hintergrund-
berichte vorab und ohne
Werbung lesen!

Jetzt einen Monat ganz ohne Risiko
ausprobieren: www.maclife.de/plus

Häufige Netzwerk-Probleme

5 Netzwerk-Mythen

WLAN-Hotspots mit Passwort sind sicher: Nicht alle Hotspots verwenden die derzeit bestmögliche Verschlüsselung nach WPA2-PSK – nicht einmal die mit einem Passwort geschützten. In öffentlichen WLANs solltest du daher stets eine VPN-Verbindung nutzen.

5-GHz-WLAN ist immer besser als 2,4 GHz: 5-GHz-Netze sind deutlich schneller, wenn du dich nah am Router befindest. 2,4-GHz-Netze haben aber die größere Reichweite.

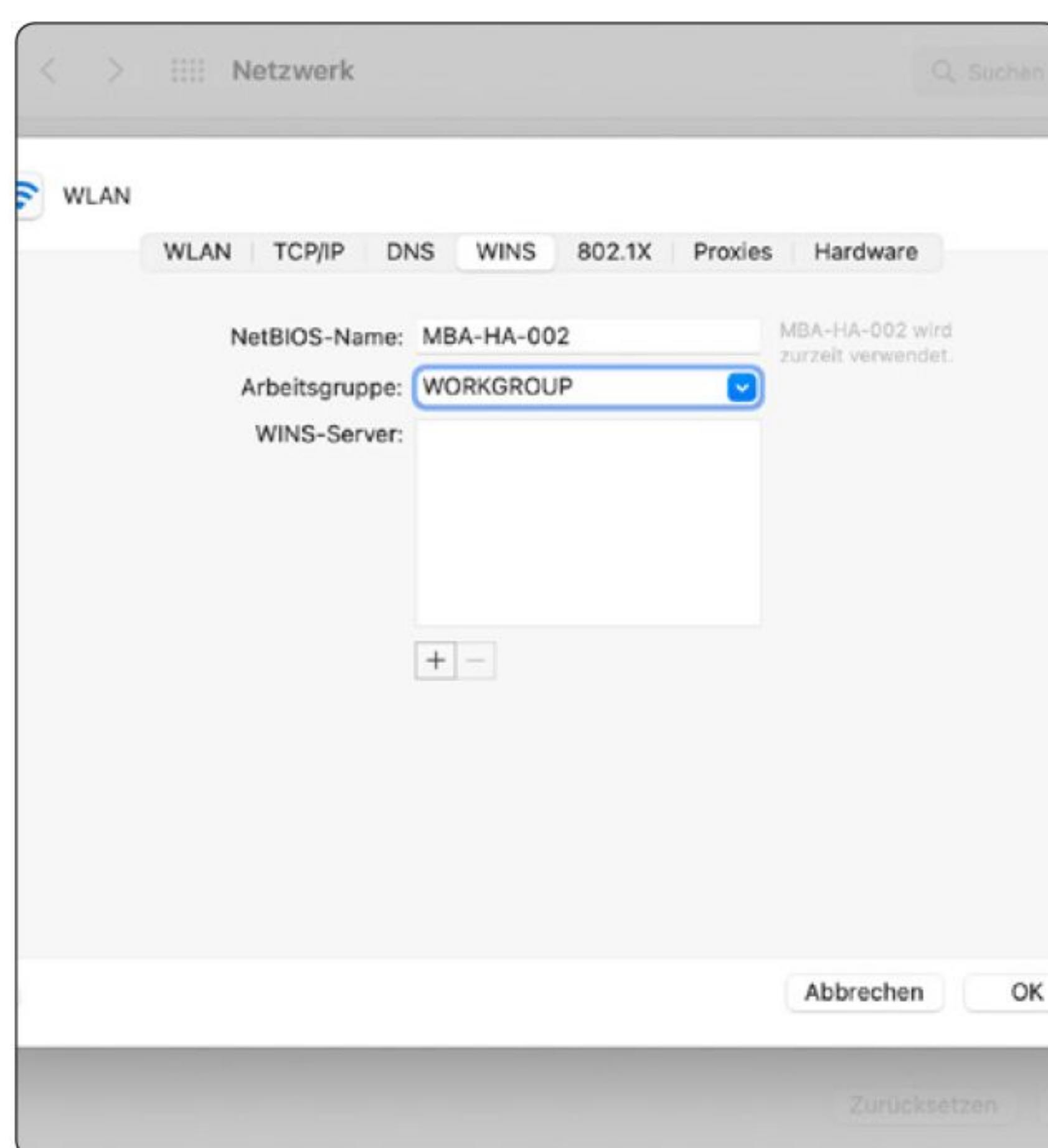
Störende Geräte sind leicht zu identifizieren: Funkstörungen können von allen möglichen Quellen stammen: dem Babyfon, schlecht abgeschirmten Stromleitungen, Mikrowellengeräten und mehr.

Abends ist das Internet langsam: In der Regel stimmt das nur für Nutzer:innen von Internetverbindungen per TV-Kabel. Hier teilen sich viele Anschlüsse eine Zuleitung und die ist abends oft ausgelastet. Mit (V)DSL oder Glasfaser sollte dieses Problem nicht auftreten.

Ohne SSID ist dein Netzwerk unauffindbar: Das Aussenden des Netzwerknamens im Router zu deaktivieren hilft tatsächlich – allerdings leider nur gegen sehr faule Angreifer:innen. Unsichtbar wird dein Netz dadurch nicht.

Zugriff auf Windows-PCs

Um Dateien mit einem Windows-PC auszutauschen, öffne die Systemeinstellungen des Mac und navigiere zum Eintrag „Freigaben“. Aktiviere dort die Dateifreigabe.



Wenn die Netzwerkkonfiguration deines Windows-PCs vom Standard abweicht, musst du Anpassungen auf deinem Mac vornehmen.

Falls dein Windows-PC nicht in der Standardarbeitsgruppe „WORKGROUP“ zu finden sein sollte, navigiere zu den Netzwerkeinstellungen deines Mac und wähle ganz oben „Umgebung: Automatisch“. Klicke dann unten links auf das Zahnrad, wähle „Dienst duplizieren“ und vergebe einen neuen Namen. Klicke danach unten rechts auf „Weitere Optionen“ und wähle den Reiter „WINS“. Klicke auf das „+“ und trage als WINS-Server die IP-Adresse deines Routers ein. Im Feld „Arbeitsgruppe“ trage den Arbeitsgruppennamen deiner Windows-Geräte ein. Danach ist ein Neustart deines Mac erforderlich.

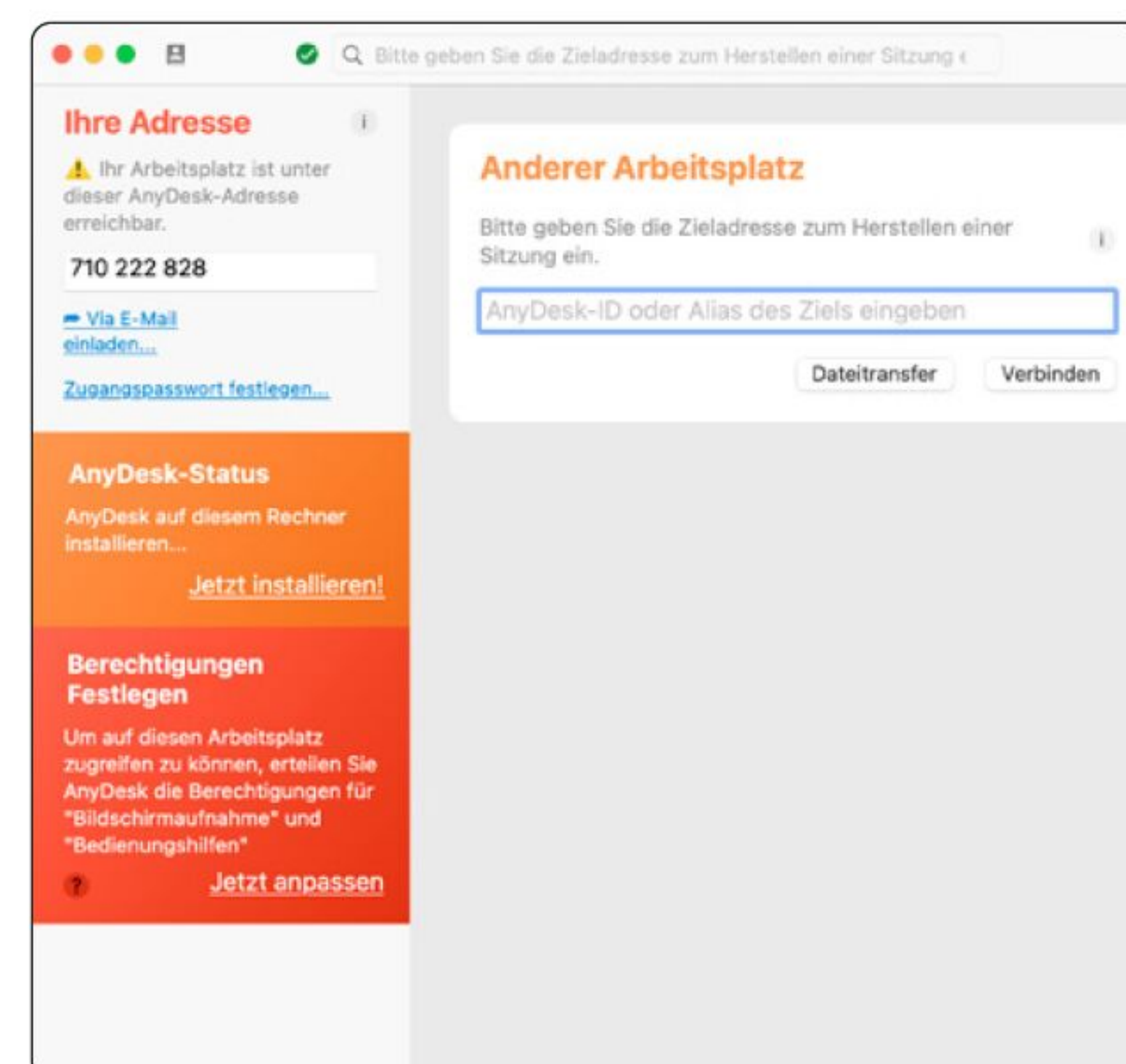
Falls dein PC trotzdem nicht im Finder unter „Netzwerk“ auffindbar sein sollte, drücke (immer noch im Finder) [cmd]+[K] und tippe „smb://pcname“ oder „smb://192.168.17.2“ ein, wobei du unsere Beispiel-IP-Adresse durch die deines Windows-PCs ersetzt. Du wirst dann nach Zugangsdaten gefragt: Wähle die Login-Daten deines Windows-PCs.

Back to My Mac ersetzen

Seit macOS Mojave hat Apple „Back to my Mac“, einen Dienst, mit dem du mittels des Internets auf deinen Mac zugreifst, gestrichen. Eine (für den privaten Einsatz) kostenfreie Lösung ist „Anydesk“ (www.anydesk.com). Lade es herunter und installiere es auf deinem Mac. Beim App-Start präsentiert dir die App eine Anydesk-Adresse, die du notieren solltest. Unter „AnyDesk > Preferences > User Interface“ kannst du die Programmsprache auf Deutsch umstellen. In den App-Einstellungen musst du im Eintrag „Sicherheit“ noch den „Unbeaufsichtigten Zugang erlauben“ und ein Passwort vergeben.

Mit der Anydesk-App kannst du von einem anderen Mac auf deinen Mac zu Hause zugreifen, solange die Anwendung dort läuft. Dazu benötigst du die zuvor notierte Anydesk-Adresse – und natürlich die Zugangsdaten zu deinem Mac. Mit der entsprechenden App für

iPhone und iPad ist der Zugang auch von Apples Mobilgeräten aus möglich.

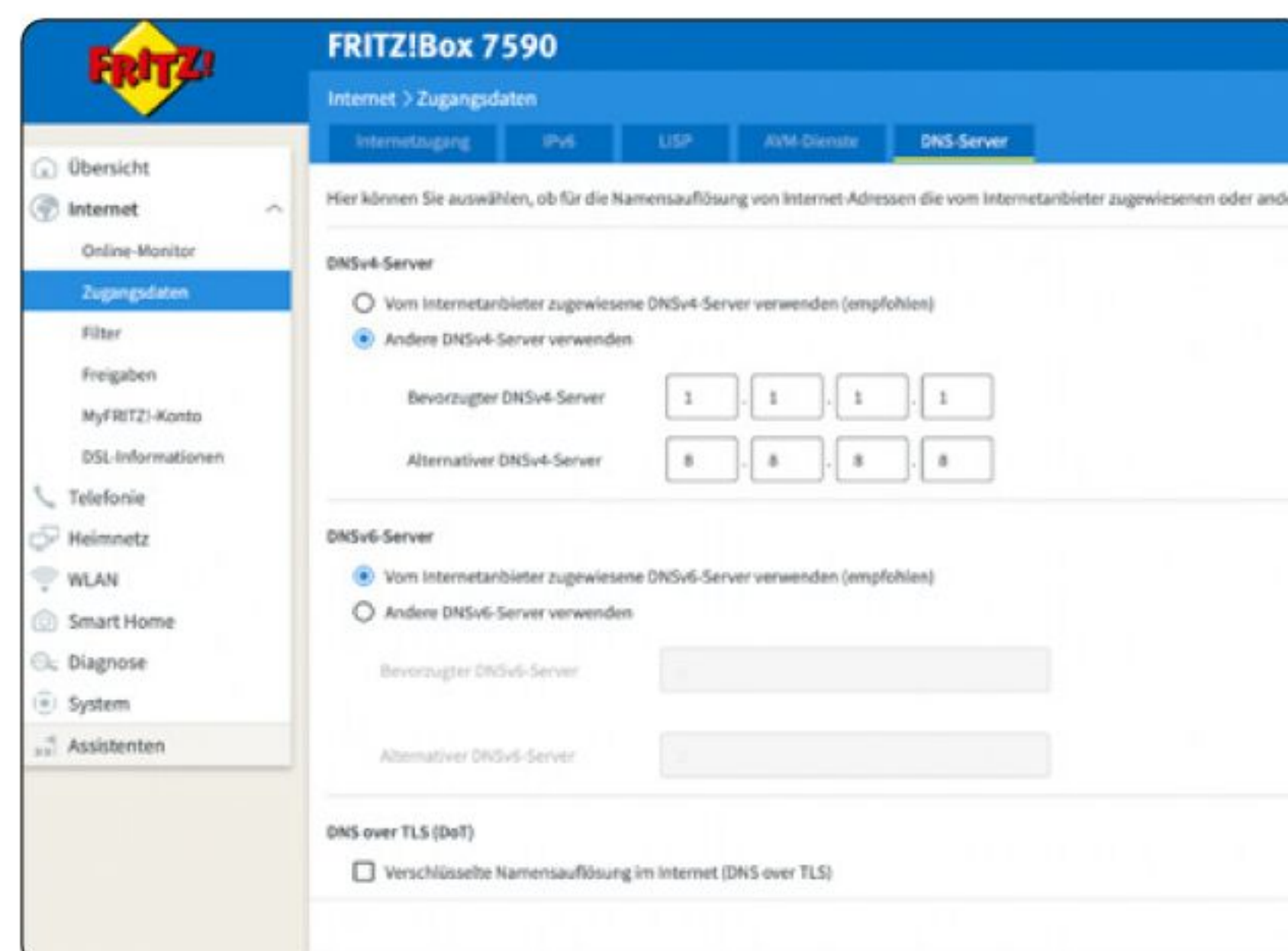


Nach dem Ende von „Back to my Mac“ bietet Anydesk eine gute Möglichkeit, um sich von unterwegs auf dem heimischen Mac einzuloggen.

DNS-Server konfigurieren



- 1 Öffne auf deinem Mac „Systemeinstellungen > Netzwerk > Weitere Optionen > DNS“. Auf iPad oder iPhone öffne „Einstellungen > WLAN“ und tippe auf das „i“-Symbol neben deinem Netzwerk.



- 2 Auf jedem Router ist der Weg leider anders. Suche nach den DHCP-Einstellungen. Meist findest du dort eine Option, um den DNS-Server einzustellen. Das hat Auswirkungen auf alle Geräte im Netzwerk.

Router zurücksetzen

Manchmal hilft nur noch das Zurücksetzen deines Routers auf seine Werkseinstellungen. Dazu gibt es in der Regel zwei Möglichkeiten. Bevor du beginnst, stelle sicher, dass dein Mac per Kabel mit dem Router verbunden ist.



Nichts geht mehr? Dann hilft oft nichts anderes mehr als den Router komplett auf den Auslieferungszustand zurückzusetzen.

Öffne die Konfigurationsoberfläche deines Routers im Browser und mache am besten Screenshots von allen Einstellungen. Einige Router bieten auch die Option, alle Einstellungen zu exportieren. Fast alle Geräte haben ein Menü, in dem es einen Eintrag zum Zurücksetzen des Routers gibt.

Falls du einen solchen Eintrag bei deinem Router nicht findest, suche auf der Rückseite des Geräts nach einem kleinen Schalter, der meist mit „Reset“ beschriftet ist. Diesen musst du mit einem Kugelschreiber oder Zahnstocher für etwa zehn Sekunden gedrückt halten. Der Router quittiert den Vorgang durch das Aufblinken aller LEDs. Jetzt kannst du dich mit dem Standard-Passwort einloggen und den Router neu konfigurieren.

WLAN-Interferenzen minimieren

Besonders im 2,4-GHz-Frequenzband gibt es eine große Anzahl möglicher Störungsquellen, die die Übertragungsqualität in deinem WLAN beeinträchtigen können. Du solltest es vermeiden, den Router in unmittelbarer Nähe zu anderen

Funkgeräten zu betreiben. Denke dabei auch an Babyfon, Funktürklingeln oder schnurlose Telefone. Falls du beim Standort deines Routers keine Wahl hast, probiere die WLAN-Kanäle 1, 6 und 11 aus und prüfe, ob sich die WLAN-Qualität dadurch

verbessern lässt. Auch per USB angeschlossene Geräte können stören, wenn deren Kabel nicht gut abgeschirmt sind. Kommt dir ein USB-Kabel sehr dünn vor, dann solltest du es austauschen.

Langsame Powerline-Verbindung

Ähnlich wie bei WLAN-Verbindungen wirst du im Stromnetz praktisch nie die beworbenen Übertragungsgeschwindigkeiten erreichen. Wenn dir die Verbindung jedoch deutlich zu langsam vorkommt und etwa Videostreams nicht möglich sind, kannst du mehrere Dinge überprüfen.

Zunächst solltest du sicherstellen, dass du Powerline-Adapter desselben Typs verwendest. Wenn einer von Haus aus langsamer ist als die anderen, wird dieser Adapter den Takt für alle Geräte vorgeben.

Auch die Qualität deiner Stromleitungen hat natürlich einen nicht zu unterschätzenden Einfluss auf die Übertragungsgeschwindigkeit. Bevor du allerdings anfängst, neue Stromleitungen zu verlegen, kannst du auch gleich ein Netzwerkkabel durch die Wohnung legen. Du solltest aber darauf achten, die Powerline-Adapter immer direkt in eine Steckdose und nicht in eine Mehrfachsteckdosenleiste zu stecken.

Auch andere Elektrogeräte direkt neben dem Powerline-Adapter können störend sein. Wenn möglich, betreibe nur den Powerline-Adapter direkt an der Steckdose und verbinde andere Geräte mit einem Verlängerungskabel.



Du bist von der Powerline-Performance enttäuscht? Steckt der Adapter direkt in der Steckdose?

Mehr WLAN mit Mesh

Wenn du jede Ecke deiner Räumlichkeiten mit WLAN erreichen möchtest, ist der Aufbau eines Mesh-Netzwerks die aktuell sinnvollste Lösung. Das besonders Gute daran: Im Prinzip funktioniert alles vollautomatisch.

Der Zugang zum Internet ist für viele inzwischen auf einem Wichtigkeitsniveau mit der Strom- und Wasserversorgung. Nicht ganz zu Unrecht, wie uns unter anderem die immer noch laufende Pandemie gezeigt hat. Spätestens, wenn das Schlafzimmer auf einmal zum Arbeitszimmer wird und die Kinder in ihren Zimmern dem Unterricht beiwohnen müssen und nicht länger nur gelangweilt durch Tiktok scrollen, wird ein solides Netzwerk essenziell.

Nur, wie lässt sich das am besten realisieren? Nicht nur in gemieteten Objekten ist das Durchbohren von Wänden häufig ungerne gesehen und eine freischwebende Verkabelung im Flur stört spätestens nach wenigen Tagen das ästhetische Empfinden.

Vorhang auf die Mesh-Technologie. „Mesh“ ist englisch und bedeutet „Masche“ und damit ist das grundlegende Konzept von Mesh-Netzwerken auch schon ganz gut erklärt. Mehrere im Haus verteilte Geräte erzeugen jeweils eigene Funknetzwerke und fassen diese zu einem einzigen „Gesamt-WLAN“ zusammen.

Qualität statt Quantität

Das bedeutet jedoch nicht, dass in jeder Ecke des Hauses ein WLAN-Zugangspunkt installiert werden muss. Im Gegenteil: Zu viele solcher „Access Points“ können das Gesamtergebnis sogar verschlechtern.

Vielmehr geht es darum, die einzelnen Knotenpunkte des Mesh-Netzwerks intelligent zu installieren, nämlich so, dass sie ein-



Passwörter

Praktisch: Auch wenn die einzelnen Bestandteile des Mesh-Netzwerks technisch autark sind, gibt es nur einen Namen und auch nur ein Passwort.

ander gut „sehen“, also erreichen können. Dabei geht es natürlich nicht um eine echte Sichtverbindung. Aber wenn ein Knotenpunkt die Netze der anderen kaum noch erreichen kann, ist den wiederum an ihm hängenden Geräten nur wenig geholfen.

Als Schema kannst du dir das von einem Knotenpunkt ausgehende WLAN-Netz wie eine Kugel vorstellen. Installierst du etwa drei solcher Knotenpunkte (Wobei dein hauptsächlicher WLAN-Router, das Gerät also, das das heimische Netzwerk ins Internet überführt, bereits der erste ist.), solltest du darauf achten, dass sich diese drei Kugeln teilweise überlappen.

Wenn du in einer „normal großen“ Wohnung oder einem eben solchen Haus wohnst, ergibt sich



AVM Fritz Mesh Set

Der Berliner Hersteller AVM ist technisch immer vorne mit dabei. Großer Vorteil: Das Geräteportfolio ist bestens auf den deutschen Markt abgestimmt, sodass praktisch alle AVM-WLAN-Router mit einem Modem für alle hierzulande gebräuchlichen Internetzugänge zu haben sind. AVM-Produkte sind praktisch nie die günstigste Wahl, dafür funktionieren sie zuverlässig und das über viele Jahre. Beim Design und damit der Wohnzimmerkompatibilität könnte AVM allerdings noch zulegen.

 **Web:** www.avm.de/mesh



Netgear Orbi

Netgear gehört zu den Veteranen der Netzwerktechnologie und hat erst kürzlich für sich entdeckt, was wir bei AVM bemängeln: Auch Router und WLAN-Access-Points dürfen schön oder zumindest interessant aussehen. Letzteres trifft auf jeden Fall auf die Orbi-Reihe zu, die für manchen Geschmack vielleicht schon wieder zu außergewöhnlich, zu futuristisch geraten ist. Technisch jedenfalls sind die Orbis voll auf der Höhe der Zeit. Nachteil: Du brauchst zusätzlich ein Modem.

 **Web:** www.netgear.de



TP-Link Deco

Ein Modem für den Internetzugang erfordern auch die Deco-Geräte von TP-Link. Wenn dir das egal ist, etwa weil du schon eins besitzt oder einfach eine bestehende Fritzbox zum Modem umfunktionieren kannst, bekommst du Technik auf dem Stand der Dinge. Außerdem sind die TP-Link-Geräte diejenigen, die optisch am wenigstens auffällig sind. Für uns ein klarer Pluspunkt. Aber auch hier gibt es einen Haken: Diverse softwaretechnische Zusatzfunktionen erfordern ein Abo.

 **Web:** www.tp-link.com

das mit aktuellem Equipment und dessen Sendeleistung meist schon automatisch. Wenn du ein besonders großes Anwesen dein Eigen nennst oder die Wände an deinem Wohnort besonders „funkfeindlich“ sind, kann es sich lohnen, die Netzwerkstärke zu messen. Dazu benötigst du keine speziellen Geräte: Der App Store ist voll von Apps, die dein WLAN analysieren können. Dabei lesen sie alle lediglich die WLAN-Messwerte deines iPhone aus und stellen diese mehr oder weniger hübsch dar. Für private Projekte ist das komplett ausreichend. Möchtest du die Räume deines Unternehmens netzwerktechnisch ausleuchten, solltest du dich aber vielleicht doch lieber an Profis wenden.

Automatisches Roaming

Die folgende Analogie trifft nur bedingt zu, veranschaulicht allerdings hervorragend, wie dein neues Mesh-Netzwerk funktioniert. Nämlich in etwa so, wie das Internet selbst es tut. Die einzel-

Mit einem Mesh-Netzwerk gelingt es dir fast spielend einfach, alle Räume deines Hauses, vom Keller bis in den Dachstuhl, mit WLAN zu versorgen.

nen Knotenpunkte sind mehrfach untereinander vernetzt, sodass sich Datenpakete immer den besten, also schnellsten Weg suchen können. Selbst der Ausfall eines Knotenpunktes ist kurzfristig kein Drama, solange die oben erwähnte mehrfache Vernetzung gewährleistet ist.

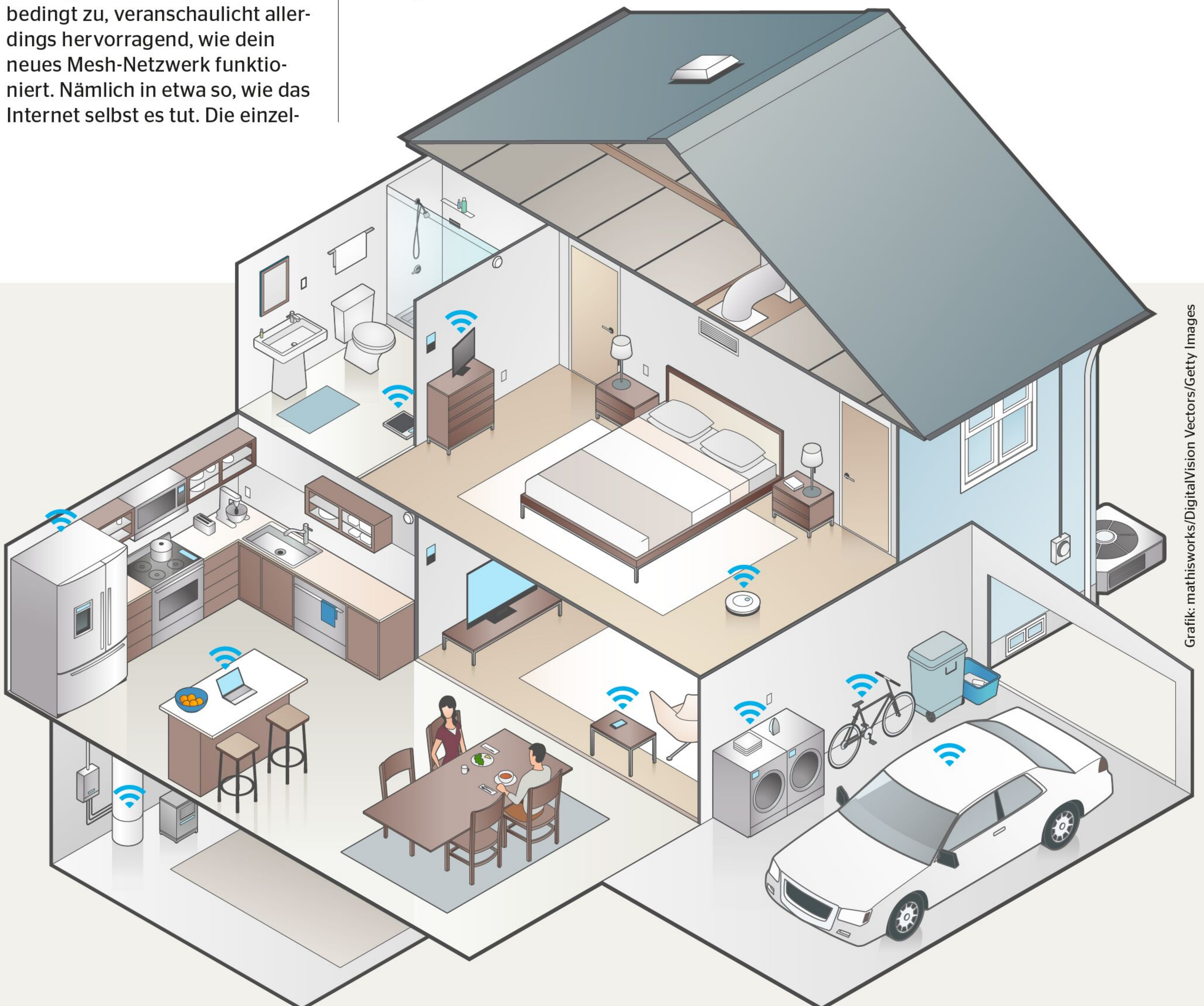
In modernen Mesh-Umgebungen ist uns noch nicht untergekommen, was wir aus klassischen privaten WLAN-Installationen nur zu gut kennen. Oft war es da nämlich so, dass etwa ein mit dem Access Point „A“ verbundenes iPhone partout mit diesem verbunden blieb, auch wenn die Verbindung über Access Point „B“ längst die bessere Wahl gewesen wäre. In einem Mesh-Netzwerk funktioniert die Übergabe der

Endgeräte zwischen den Knotenpunkten deutlich intelligenter.

Fazit

Dich wichtigste Erkenntnis im Zusammenhang mit der Mesh-Technologie ist: Wenn bei dir auch ohne Mesh-Netzwerk alles gut funktioniert, gibt es keinen Grund für ein Upgrade. Zwar sind viele moderne Router schon darauf ausgelegt, Teil eines Mesh-Netzwerks zu sein. Ganz ohne Investitionen ist der Umstieg aber dennoch nicht möglich.

Wenn du allerdings regelmäßig mit „schlechtem Netz“ in verschiedenen Räumen haderst, solltest du dich mit Mesh-fähigen Geräten auseinandersetzen, bevor du den Bohrer anwirfst, um alle Räume zu verkabeln.



Grafik: mathisworks/DigitalVision Vectors/Getty Images

Umstieg von der Fritzbox auf Unifi

Vor rund eineinhalb Jahren übertrug ich die Verantwortung für das heimische WLAN auf Hard- und Software von Ubiquiti. Doch warum schickte ich die treu gediente Fritzbox dennoch nicht in Rente?

TEXT: STEFAN MOLZ

Der hiesige Markt dürfte Herstellern von Netzwerkhardware ein Graus sein, denn die Berliner:innen von AVM haben mit der Fritzbox das ultimative All-in-one-Gerät im Angebot. Die weiß-roten-Plastikboxen kombinieren DSL-, LTE-, Kabel- respektive Glasfaser-Modem, WLAN-Access-Point, DECT-Basis und mehr. Das drückt den Preis für das Komplettpaket, senkt den Stromverbrauch, vereinfacht die grundlegende Inbetriebnahme und sorgt für mehr Ordnung im Netzwerkschrank.

Sich in Sachen Heimnetzwerk auf etwas anderes als eine Fritz-

Wer kennt sie nicht, die Zimmerecke, in der sich die Netzwerk- und Smarthome-Hardware stapelt?

Eineinhalb Jahre Unifi: ein Erfahrungsbericht



Was ist Unifi?

Unifi ist ein modulares (WLAN)-Netzwerk-System für den (semi)professionellen Einsatz. Egal, ob Privathaushalt, kleines Büro, Schule oder ein mittelständisches Unternehmen: Unifi findest du ob seiner Skalierbarkeit und leicht zu handhabenden Administration auch hierzulande an vielen Orten. Eine Unifi-Installation besteht aus mehreren Kernkomponenten und kann über Access Points und Switches an die individuellen Erfordernisse vor Ort angepasst werden. Je nach Ausbaustufe lassen sich sogar Überwachungskameras und ein Zugangssystem einbinden. Für den Einstieg braucht es lediglich die sogenannte Dream Machine für um die 300 Euro, die Kosten für zusätzliche Komponenten lassen den Preis für ein komplettes Set-up aber schnell die 1.000-Euro-Mauer durchbrechen.

box einzulassen, hat etwas vom sprichwörtlichen Gegen-den-Strom-Schwimmen. Ein gewisses Interesse an einer Fritzbox-Alternative war bei mir schon immer da, aus dem Angebot der AVM-Mitbewerber stachen dabei die Produkte von Ubiquiti heraus. Kein Wunder, denn Ubiquiti-Gründer Robert Pera gilt nicht nur als Verehrer der Arbeit eines gewissen Steve Jobs, sondern war auch zeitweilig bei Apple beschäftigt. Mit genug an dort getankter Apple-DNA übertrug Ubiquiti die Erfolgsformel Apples, nämlich etwas so Langweiliges wie einen Computer zu einem Designstück und Erlebnis zu machen, auf schnöde Netzwerkhardware. Egal, ob Ethernetswitch, WLAN-Access-Point oder Überwachungskamera: Die Geräte sehen toll aus und sind hochwertig verarbeitet. Und trotz der vielen in Software gegebenen Möglichkeiten in Funktion und deren Konfiguration ist zumindest die grundlegende Einrichtung und Wartung auch für Nichtprofis noch gut und einfach zu handhaben.

Mein ursprüngliches Set-up ...

Eingestiegen bin ich in das Unifi-System Ende 2020 mit der Dream Machine. Das Gerät im Look eines kleinen R2D2 kombiniert die Unifi-Kernkomponenten. Das heißt aber auch, dass das Gerät zunächst einmal nicht viel mehr beziehungsweise sogar weniger kann als eine Fritzbox – und das auch noch ohne integriertes Modem. Überdies gingen mit an den Start: Ein Vigor 165 (ein VDSL-Modem von Draytek) sowie, hier darf gelacht werden, meine Fritzbox 6890. Letzteres, um unsere Festnetz-Telefone weiter verwenden zu können.

Da ich zudem mehr Clients kabelgebunden einbinden wollte, kamen je noch ein Ethernetswitch für all die Wohnzimmer-Technik und die Hardware im Arbeitszimmer hinzu. Ein weiterer WLAN-Access-Point sorgte ergänzend zum in der Dream Machine integrierten Access-Point für bestes Netz in der gesamten Wohnung (und bis hinüber auf die andere Straßenseite). Du siehst: Je nach Anspruch ist bereits der Einstieg



nicht günstig, schnell ist mehr als das Doppelte des Preises einer Fritzbox ausgegeben.

Den vielen Komponenten zum Trotz ging die grundlegende Einrichtung schnell und ohne größere Probleme von der Hand. Begeistert war ich umgehend von der deutlich besseren WLAN-Abdeckung und dem höheren Datendurchsatz – die rührten aber auch daher, dass im neuen Heimnetz eben vieles an Daten nicht länger via WLAN durch die Gegend flatterte, sondern ganz klassisch über Netzkabel übertragen wurde. Von der Unifi-Netzwerk-Software profitierte ich unter anderem durch ein separates Netz, dass ich für all unsere „Internet of things“-Geräte aufspannen konnte, um so Smart-home-Geräte weitestgehend vom Rest des Netzwerks abzuschotten. Über deren Nutzwert darf gestritten werden, doch die vielen Informationen und Statistiken zu Geräten und deren Netzwerkverkehr waren und sind ebenfalls spannend – auch um für die Arbeit im Homeoffice sinnvolle Quality-of-

service-Einstellungen zu treffen: Im Zweifel geht der Netzwerkverkehr des Mac am Schreibtisch dem des Apples TVs der Tochter vor, das separate Gästernetz (mit Vorschaltseite und Token für dessen Nutzung) funkt bandbreitenbeschränkt. Ob das alles für einen Privathaushalt nicht vielleicht einen drüber ist? Klar!

... und dessen Upgrade

Wenige Monate später stand ein Umzug an. Einerseits war das ob der zuvor gelegten Ethernetkabel ein klein wenig ärgerlich, aber auch eine Chance auf ein Upgrade! Da ich das neue Zuhause unter anderem mit einer Videoüberwachung ausstatten wollte, lag der Wechsel von der Dream Machine zur Dream Machine Pro nah. Statt als kompaktes Standgerät kommt die Dream Machine Pro als Einschub mit einer Höheneinheit für 19-Zoll-Racks. Im Gegensatz zur Dream Machine können auf dem Pro-Modell zusätzlich zur Netzwerk-Software auch noch die Anwendungen für Videoüberwachung, Zugangssysteme und VoIP laufen. Drei Kameras habe ich in das System integriert, welche auf die selbst in der Dream Machine Pro einzubauenden Festplatte aufzeichnen (hier eine Skyhawk von Seagate). Via Homebridge sind die Kameras sogar inoffiziell in HomeKit integriert und können dort auch als Bewegungsmelder genutzt werden.

Mein Fazit

Würde ich wieder von der Fritzbox zu Unifi wechseln? Für mich kann ich diese Frage mit einem „Ja“ beantworten. Bezüglich WLAN-Abdeckung, Datendurchsatz, Netzwerkgestaltung und dessen Kontrolle habe ich mich im Vergleich zu meiner Solo-Fritzbox verbessert – dafür aber auch einiges an Geld und Zeit investiert. Wenn du mit deiner Fritzbox zufrieden bist, besteht rational betrachtet keine Notwendigkeit für einen Umstieg. Vieles lässt sich mit der Fritzbox kosten- und platzsparender erreichen, doch für mich persönlich ist der Spaßfaktor bei Unifi größer – „Spaß“ und „Netzwerk“ in einem Satz, wer hätte das gedacht!

Unifi: Netzwerk mit System

Unifi Security Gateway

Das Unifi Security Gateway (USG) stellt die Verbindung zum Internet her, dient als Router mit integrierter Firewall und erlaubt die Verwaltung und Kontrolle des Netzverkehrs im Zusammenspiel mit dem Unifi Controller. Die Dream Machine (Pro) beinhaltet bereits ein USG.

Unifi Switch

Ein Switch dient der Erweiterung eines Unifi-Systems, hier finden etwa kabelgebundene Endgeräte Anschluss, aber auch Access Points zur WLAN-Erweiterung können hier angeschlossen werden. Die Dream Machine Pro integriert einen 8-Port-Switch, allerdings ohne Power-over-Ethernet.

Unifi Access Point

Die Unifi Access Points sind die WLAN-Zugangsknoten des Systems. Es sind verschiedene Modelle auch mit Wi-Fi 6 erhältlich, darüber hinaus gibt es Hardware für Richtfunk-Verbindungen über mehrerer hundert Meter hinweg sowie LTE-Modems für Fallback-Verbindungen.

Unifi Controller und Cloud Key

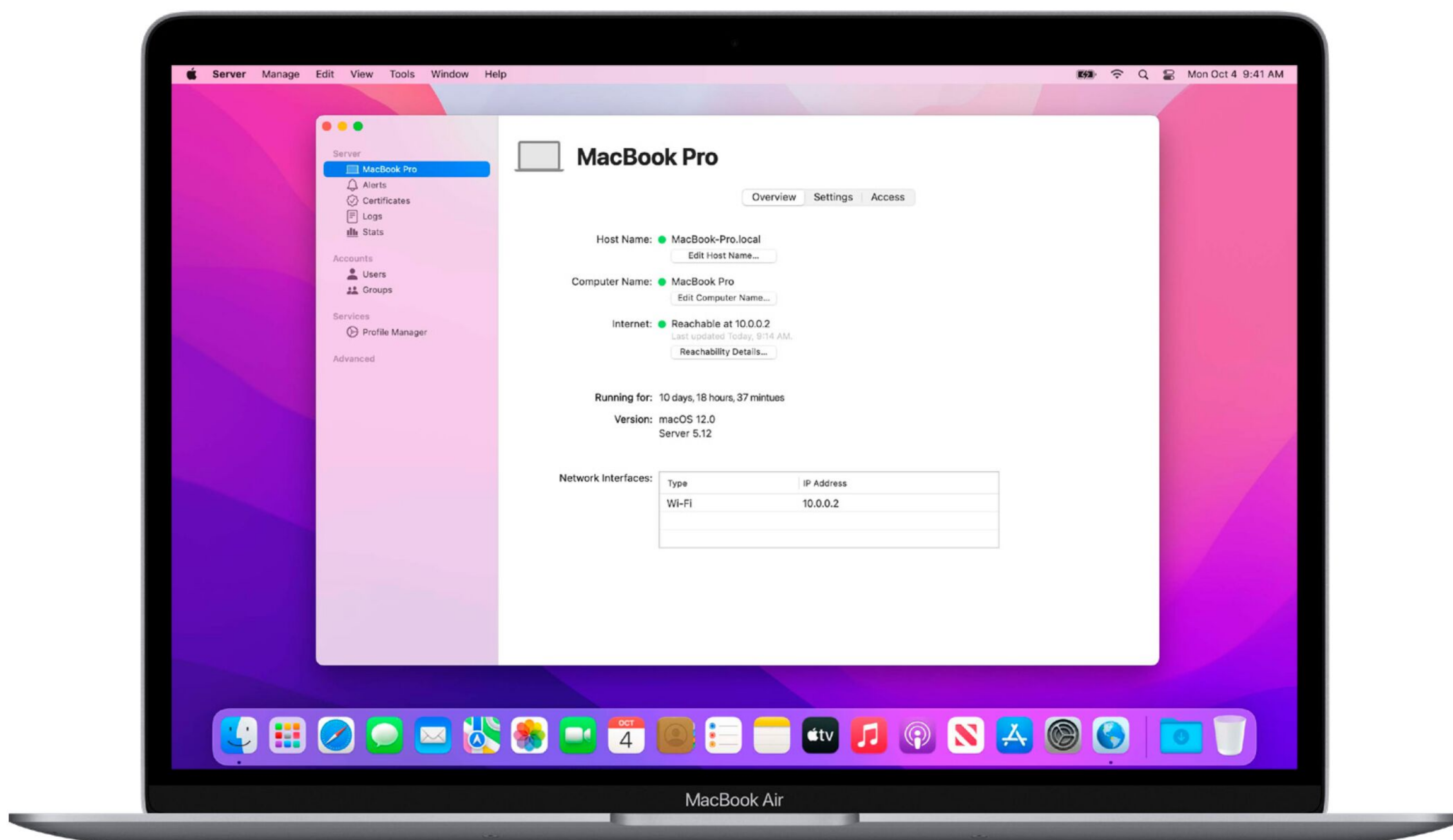
Der Controller ist die zentrale Komponente, über die ein Unifi-System eingerichtet und verwaltet wird. Als „Gehirn“ des Ganzen kann es auf einem Computer oder einem unterstützten NAS im Hintergrund laufen. Die Dream Machine (Pro) kommt mit integriertem Controller.

Und mehr!

Geld lässt sich bei Ubiquiti auch für eine Vielzahl verschiedener Überwachungskameras lassen. Außerdem arbeitet Ubiquiti an Klingeln, Zugangssystemen und mehr – viele Produkte sind vor ihrem eigentlichen Verkaufsstart im Early-Access-Shop erhältlich.



Mit diesem Satz an Hardware startete ich in die Unifi-Welt – die Fritzbox ist weiterhin im Einsatz, allerdings nur für die Festnetztelefonie via VoIP und als DECT-Basis.



macOS Server auf Monterey installieren

Die Serversoftware für macOS steht in einer neuen Version zur Verfügung, welche die Installation auf macOS 12 voraussetzt. Wir zeigen in diesem Beitrag die Möglichkeiten und die Praxis von macOS Server.

TEXT: THOMAS JOOS

Der Fokus von macOS Server liegt auf der Verwaltung von Geräten und Speichermedien im Netzwerk. Wenn im Netzwerk ein Mobile Device Management-Server (MDM) zum Einsatz kommen soll, ist macOS Server ein Weg für die zentrale Verwaltung der Geräte mit einem MDM-System. Allerdings gibt es bereits Alternativen. Die Funktionen können auch in der Familie oder im Verein zum Einsatz kommen, setzen aber Erfahrung beim Umgang mit Richtlinien, Profilen und der Anbindung von Apple-Geräten an ein MDM-System voraus.

Der Server benötigt keinen eigenen Monitor, da die Verwaltung von einem Client über das Netzwerk erfolgen kann. Dazu steht ein eigenes Verwaltungsprogramm und zusätzlich noch die Bildschirmfreigabe in macOS zur Verfügung. Auch der Zugriff von Linux und macOS zur Verwaltung des Servers ist möglich. In diesem Fall nutzt du einfach einen kostenfreien VNC-Viewer, der auf die Bildschirmfreigabe von macOS zugreifen kann.

Der Profilmanager-Dienst in macOS Server ermöglicht es dir, iPhones oder iPads zu verwalten

und Konfigurationsprofile auf den Geräten zu verteilen. Diese Profile richten Mac-Computer sowie die iPhone-, iPad-, iPod touch und Apple TV-Geräte der angeschlossenen Benutzer:innen so ein, dass sie deinen Server als MDM-Lösung nutzen.

macOS Server 5.12 mit macOS 12 einsetzen

Ab Version 5.12 benötigt macOS Server als Betriebssystem mindestens macOS 12 (Monterey). Wenn auf einem Mac bereits macOS Server installiert ist, muss der Server auf macOS 5.12 aktualisiert wer-

den und macOS zu Version 12. Ältere macOS Server-Versionen wie macOS Server 5.11.1 sind nicht kompatibel mit macOS 12.

Mit der neuen Version von macOS Server hat Apple wieder einige Funktionen entfernt. In 5.12 ist die Xsan-Verwaltung (Speicher-Netz- und Cluster-Dateisystem) nicht mehr Bestandteil des Servers. Im Fokus von macOS Server steht in Version 5.12 die zentrale Verwaltung von Apple-Geräten in der Familie, im Verein oder im Unternehmen. Wir zeigen dazu die Einrichtung in einem eigenen Workshop. Wer bereits eine Lizenz des Servers hat, darf kostenfrei zu 5.12 aktualisieren, wer keine Lizenz hat, kann sich diese für 20 Euro im App-Store kaufen. Du solltest ab und zu im App-Store bei „Updates“ überprüfen, ob eine neue Version von macOS Server vorliegt und diese dann manuell installieren. Automatisch führt macOS keine Installation durch.

Benutzungsverwaltung mit macOS Server

Mit macOS Server ist eine Verwaltung von Benutzerkonten im Netzwerk möglich, auch auf Basis von Open Directory. Eine Anbindung an Microsoft Active Directory ist mit dem Server ebenfalls möglich. Zusammen mit der Profilverwaltung für die angebunde-

nen Apple-Geräte ist die Benutzungsverwaltung der zweite Schwerpunkt von macOS Server. Damit sind zudem Anbindungen an Unternehmensnetzwerke möglich. Du kannst diese Funktionen auch in der Familie und im Verein nutzen. Mit etwas Einarbeitung lassen sich diese Dienste mit den Bordmitteln von macOS verwalten.

Die Funktionen ermöglichen eine einheitliche Benutzungsverwaltung im lokalen Netzwerk. Dabei kann es sich um Familien, Vereine, Organisationen oder Unternehmen handeln. Viele Funktionen des macOS Server hat Apple mittlerweile direkt in macOS integriert. Dazu gehören zum Beispiel die Funktionen des Dateiservers, Cachingservers und des Time Machine-Servers. Der Xcode-Server gehört mittlerweile direkt zu Xcode. Die Verwaltung von Xsan integriert Apple direkt in macOS. Diese Funktionen arbeiten wiederum mit macOS Server zusammen und lassen sich damit gemeinsam mit den Serverfunktionen betreiben.

Wenn du macOS Server installiert hast, kannst du in der Verwaltungsoberfläche des Servers bei „Benutzer:innen“ und „Gruppen“ lokale Benutzerkonten auf dem Server anlegen und für Berechtigungen nutzen, zum Beispiel



macOS Server

Bereits seit 1999 veröffentlicht Apple regelmäßig auch eine Server-Variante seines Betriebssystems für den Mac. Inzwischen ist aus dem eigenständigen OS eine App für das „normale“ macOS geworden.

für Freigaben. Über den Menüpunkt „Verzeichnisdienste“ bei „Werkzeuge“ kannst du nach der Anmeldung an macOS Server eine Anbindung des Servers an andere Verzeichnisdienste vornehmen, zum Beispiel zu Microsoft Active Directory.

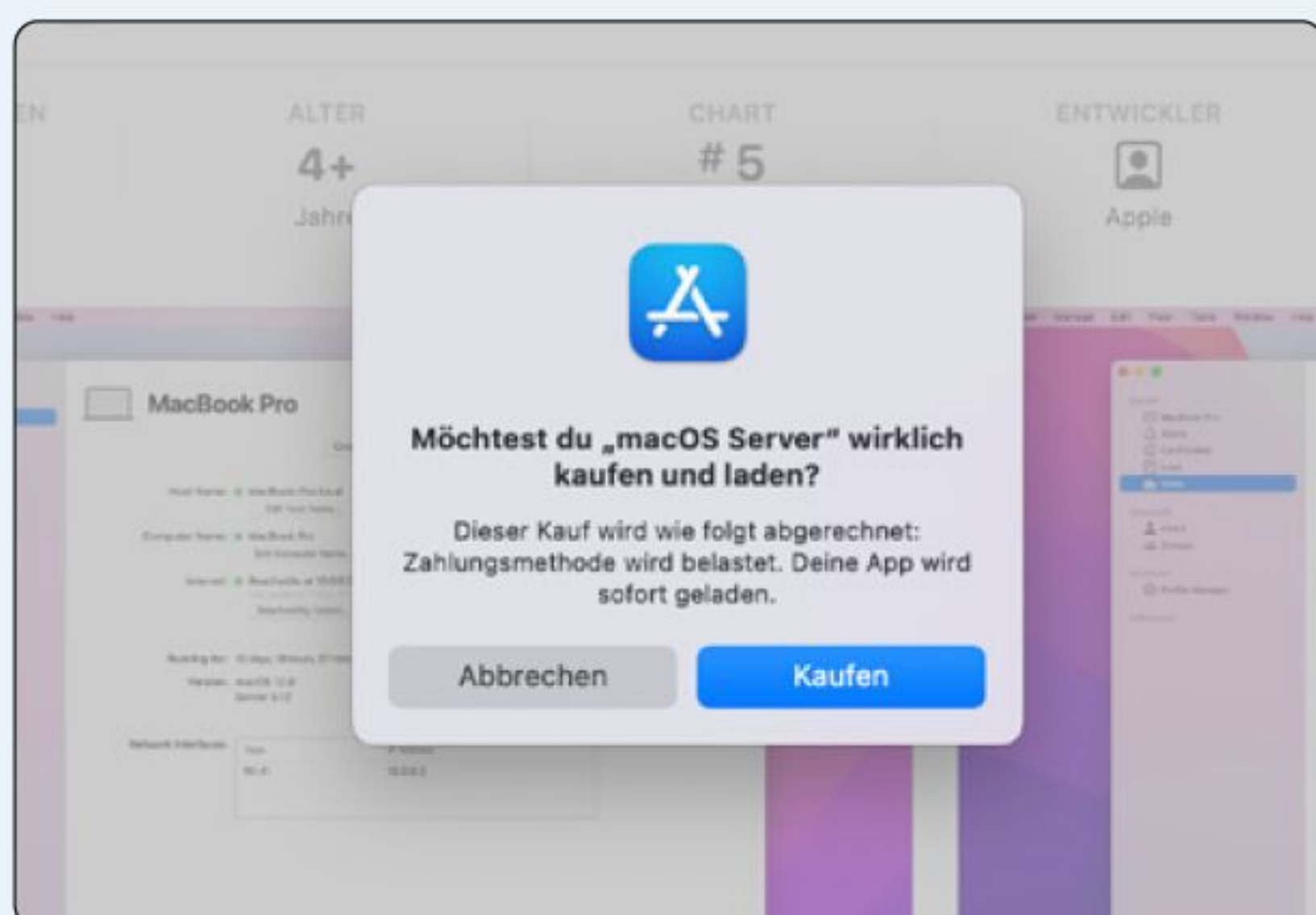
Zusätzlich steht bei „Werkzeuge“ auch „Bildschirmfreigabe“ zur Verfügung. Dadurch kannst du über die Server-App mit der Bildschirmfreigabe auf einen macOS-Server im Netzwerk zugreifen. Du brauchst dazu nur den Namen des Servers und die Anmeldedaten.

macOS Server als Zusatz-App für macOS installieren

Generell kann aus jedem Mac mit macOS ab Version 12 ein Server konfiguriert werden. Du musst dazu nur für 20 Euro die macOS-Server App im App-Store herunterladen und auf dem Mac installieren und einrichten. Für die Installation sind mindestens 8 GB Arbeitsspeicher und 10 GB freier Speicherplatz notwendig. Die Einrichtung dauert wenige Minuten.

Danach lassen sich auf diesem Mac die Server-Dienste einrichten. Die Apple-Geräte im Netzwerk greifen auf den Server zu und können die Ressourcen nutzen, die auf dem Server zur Verfügung stehen. Aktualisierst du deinen Mac zu macOS 12 und danach einen

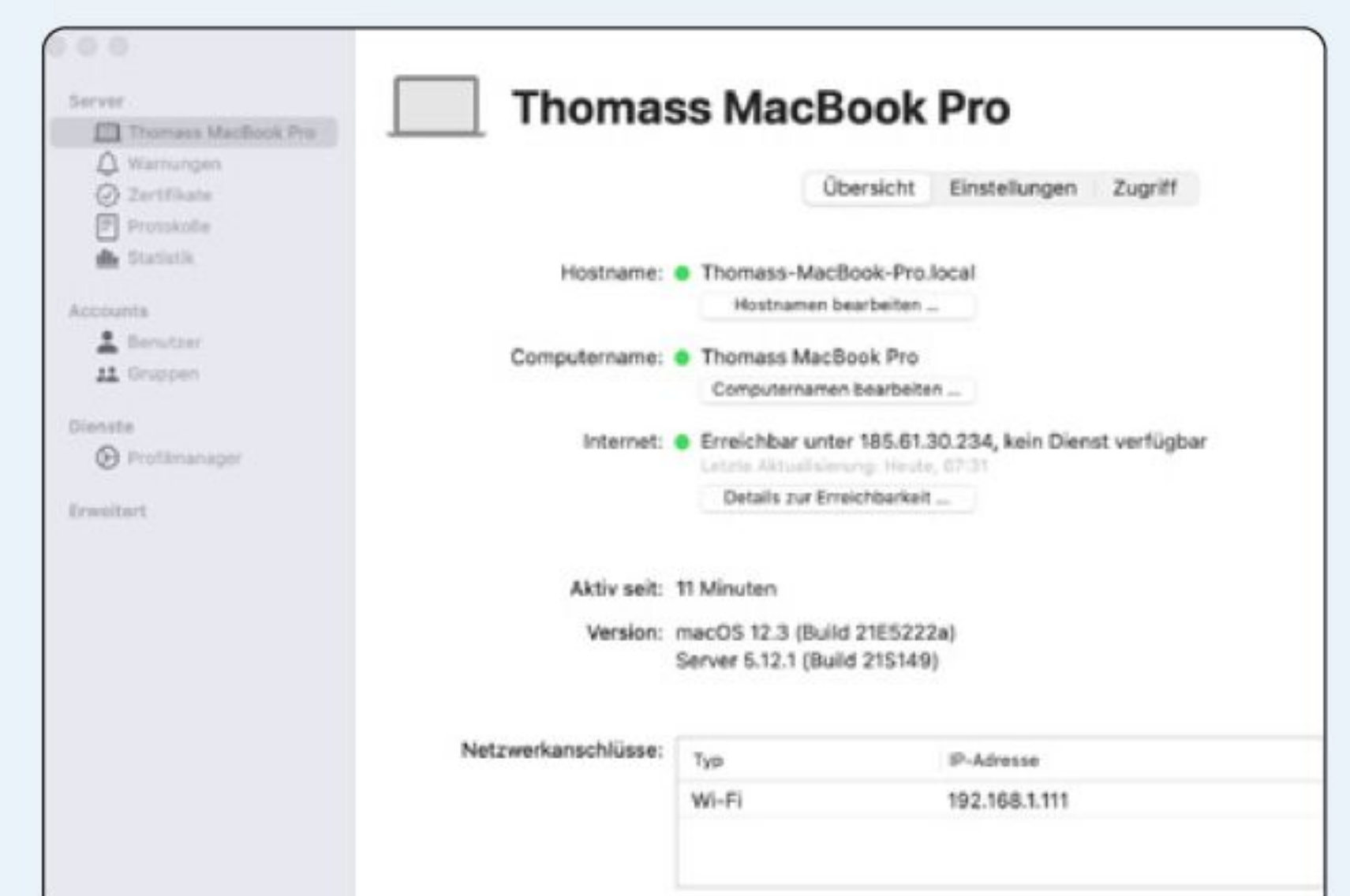
Workshop: So installierst du macOS Server auf deinem Mac



1 Im ersten Schritt kaufst du die App für macOS Server im App-Store und installierst danach die App auf deinem Mac. Die Einrichtung findet erst nach der Installation statt.



2 Starte die App „Server“. Mit „Fortfahren“ startest du die Einrichtung. Bestätige die Lizenzbedingungen und gib das Administratorkennwort für macOS ein.



3 Danach richtet die Assistenz den Server ein. Starte dann den Mac neu. Darauf startest du die Server-App. Es startet die Verwaltungsoberfläche von macOS Server.

bereits vorhandenen macOS Server zur Version 5.12.1 erscheint die Meldung, dass die Server-App ersetzt wird. Bei diesem Vorgang bleiben allerdings die vorhandenen Einstellungen von macOS Server erhalten. Die Aktualisierung von macOS Server erfolgt nicht automatisch. Apple will Dienstunterbrechungen verhindern. Daher musst du die Updates selbst installieren.

Mobile Device Management auch für kleine Netzwerke

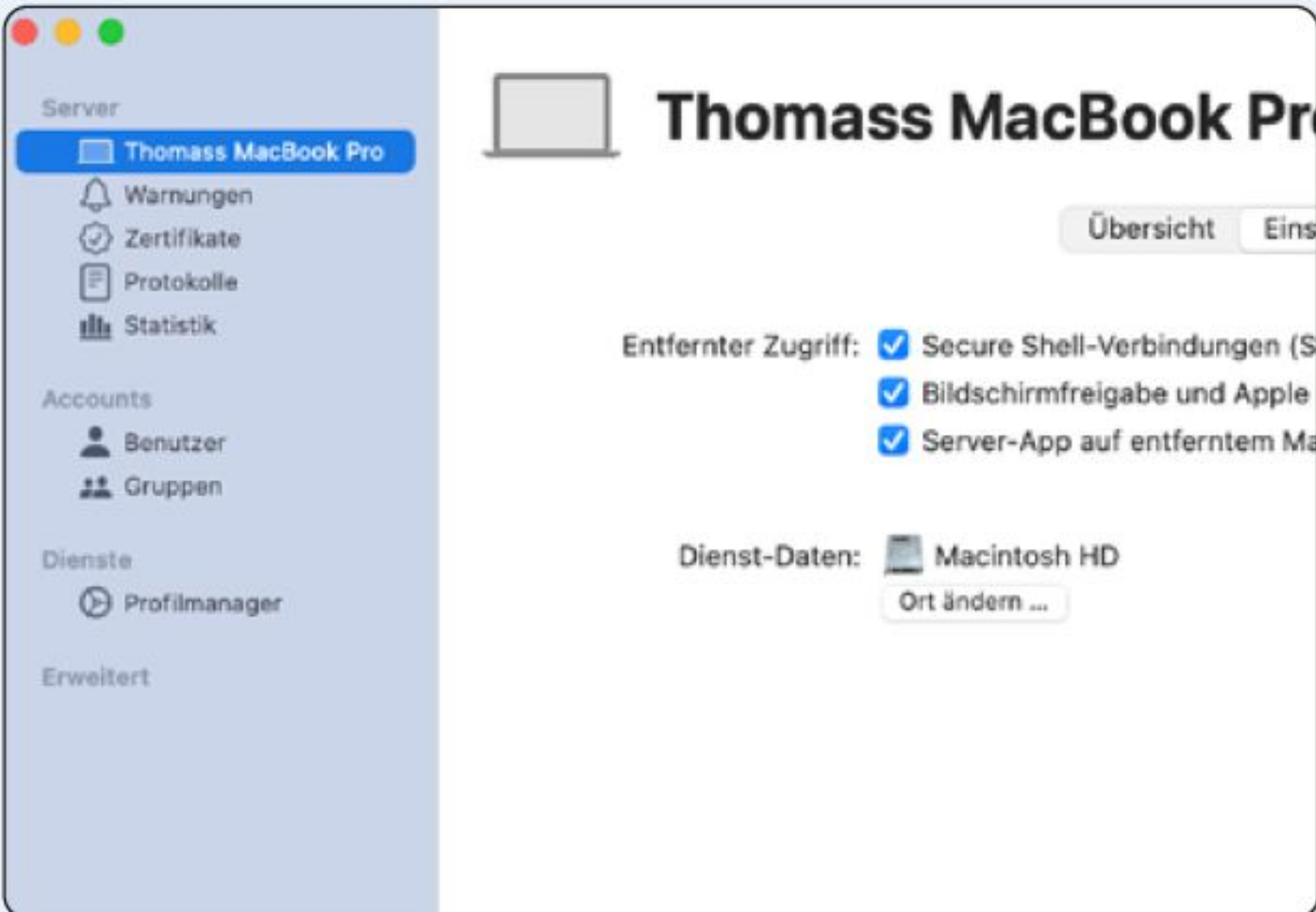
Da Apple immer mehr Funktionen aus macOS Server entfernt, ist mittlerweile das zentrale Element des Servers die Verwaltung von Apple-Geräten im Netzwerk. Dazu muss in der Verwaltungsoberfläche der Dienst eingerichtet



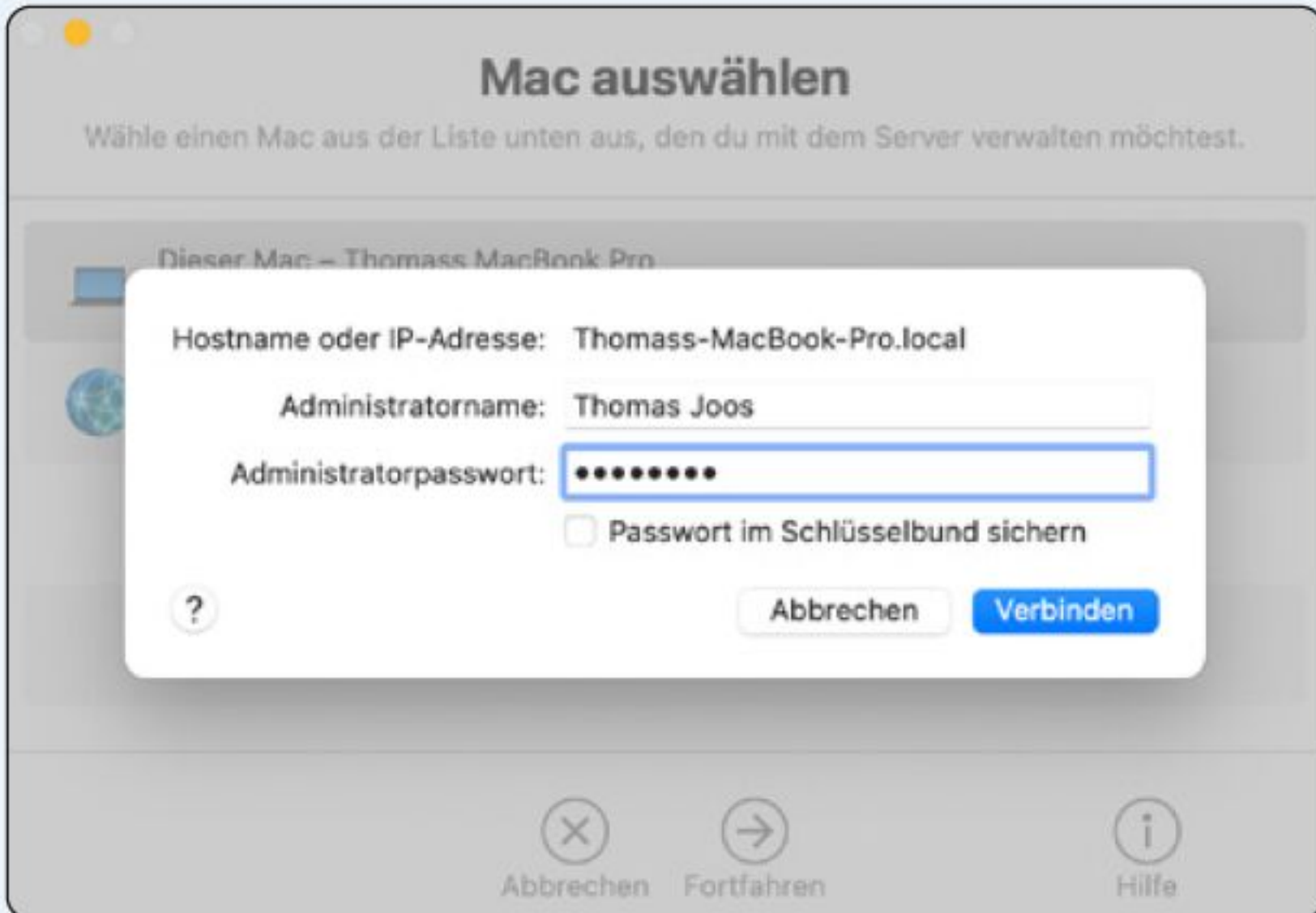
und bei Apple registriert werden. Standardmäßig ist die Funktion nicht aktiv, du musst sie zuerst einrichten. Danach bindest du deine Geräte in der Familie, Verein oder im kleinen Netzwerk an den Server an. Dazu steht eine Web-Oberfläche zur Verfügung, die du von den Endgeräten aus verwenden kannst, um dich bei dem System zu registrieren. Zusätzlich kannst du als Admin der Umgebung über den Webbrowser Einstellungen und Sicherheitsoptionen vorgeben.

Der sogenannte „Profilmanager“ gehört zu den Kernelementen der macOS-Server-Umgebung und erlaubt die zentrale Verwaltung diverser Apple-Geräte.

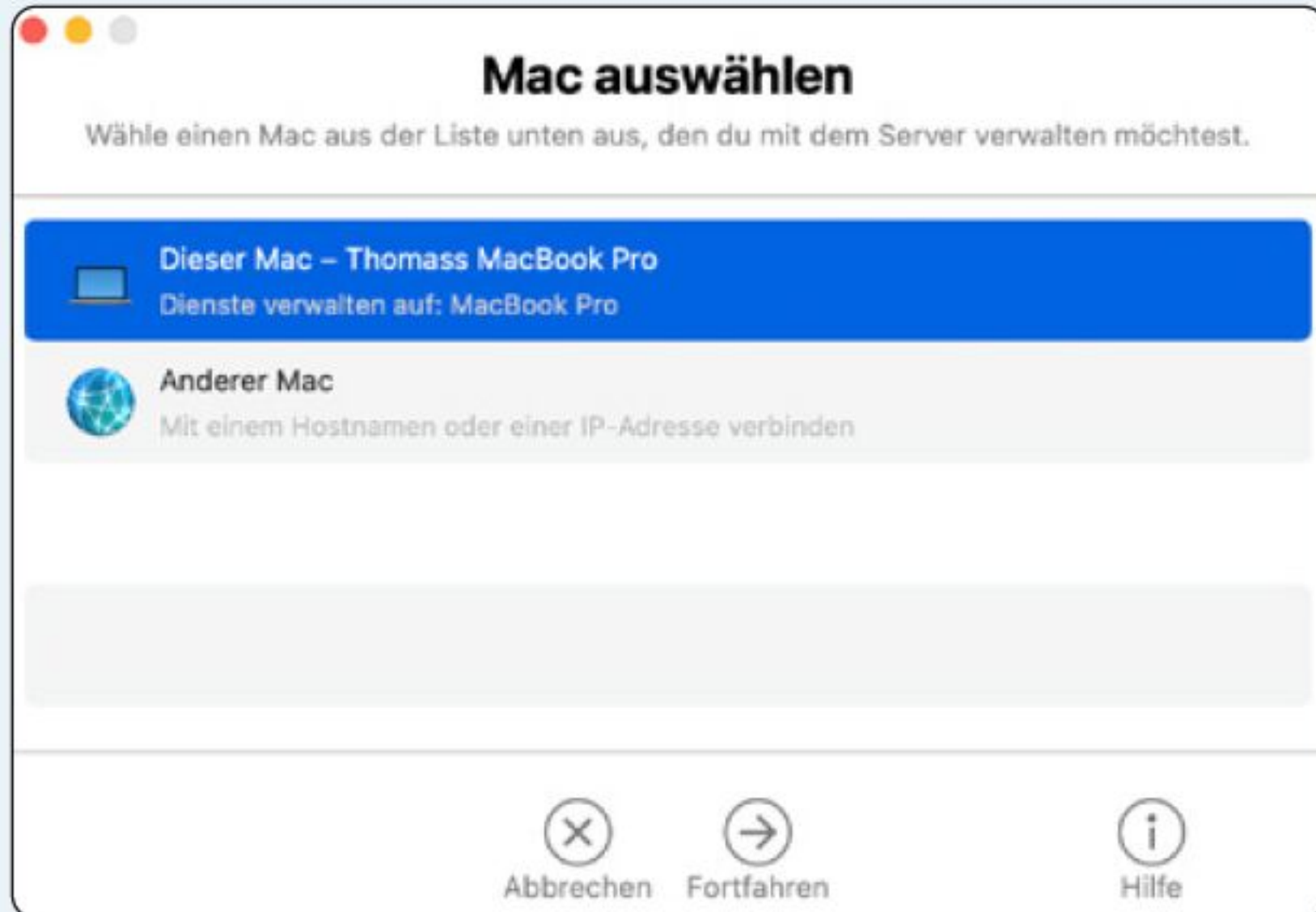
Workshop: So verwaltest du macOS Server über das Netzwerk



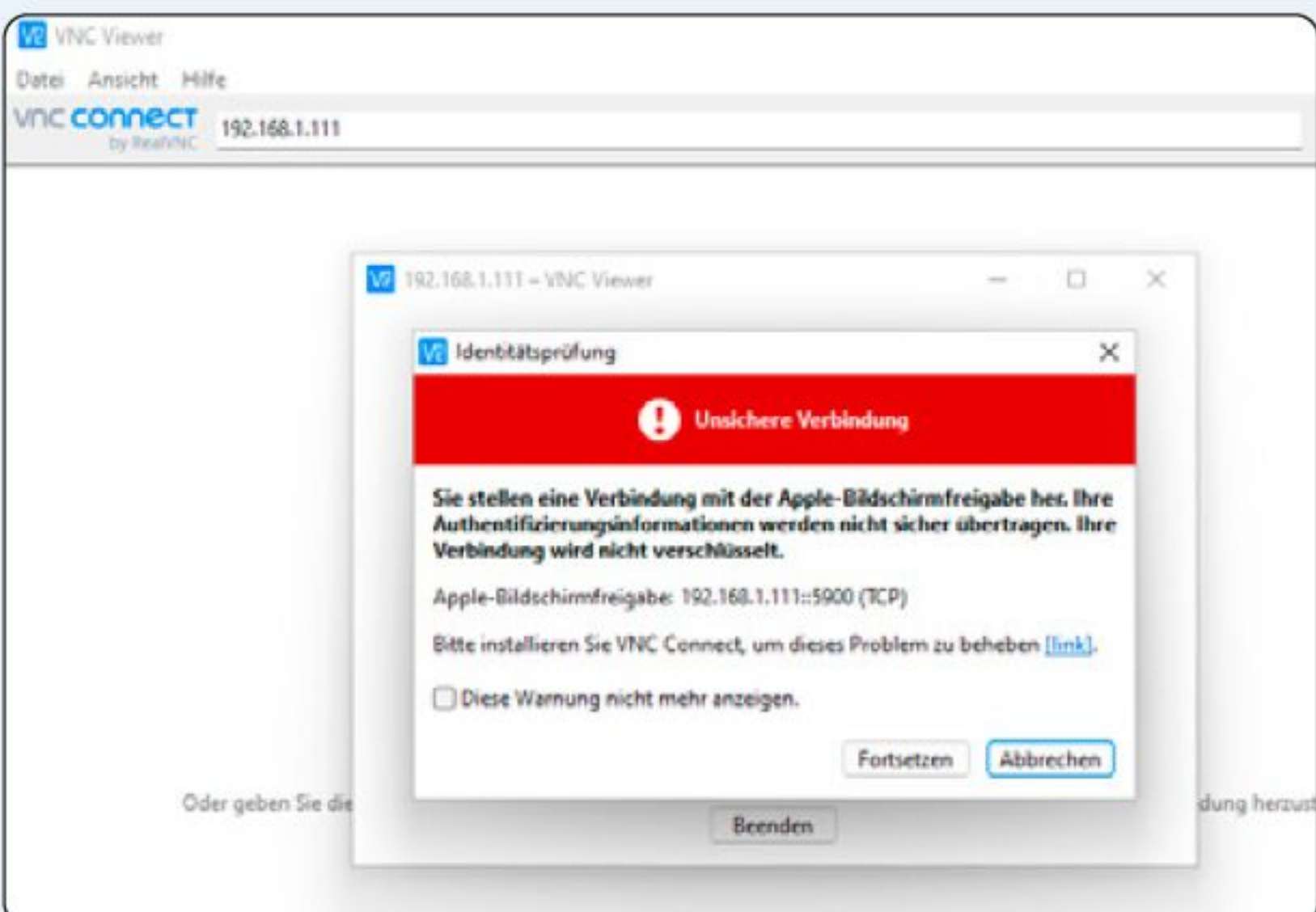
1 Starte die App „Server“ auf dem Mac und melde dich am lokalen macOS Server an. Klicke nach dem Start links auf den Namen des Computers.



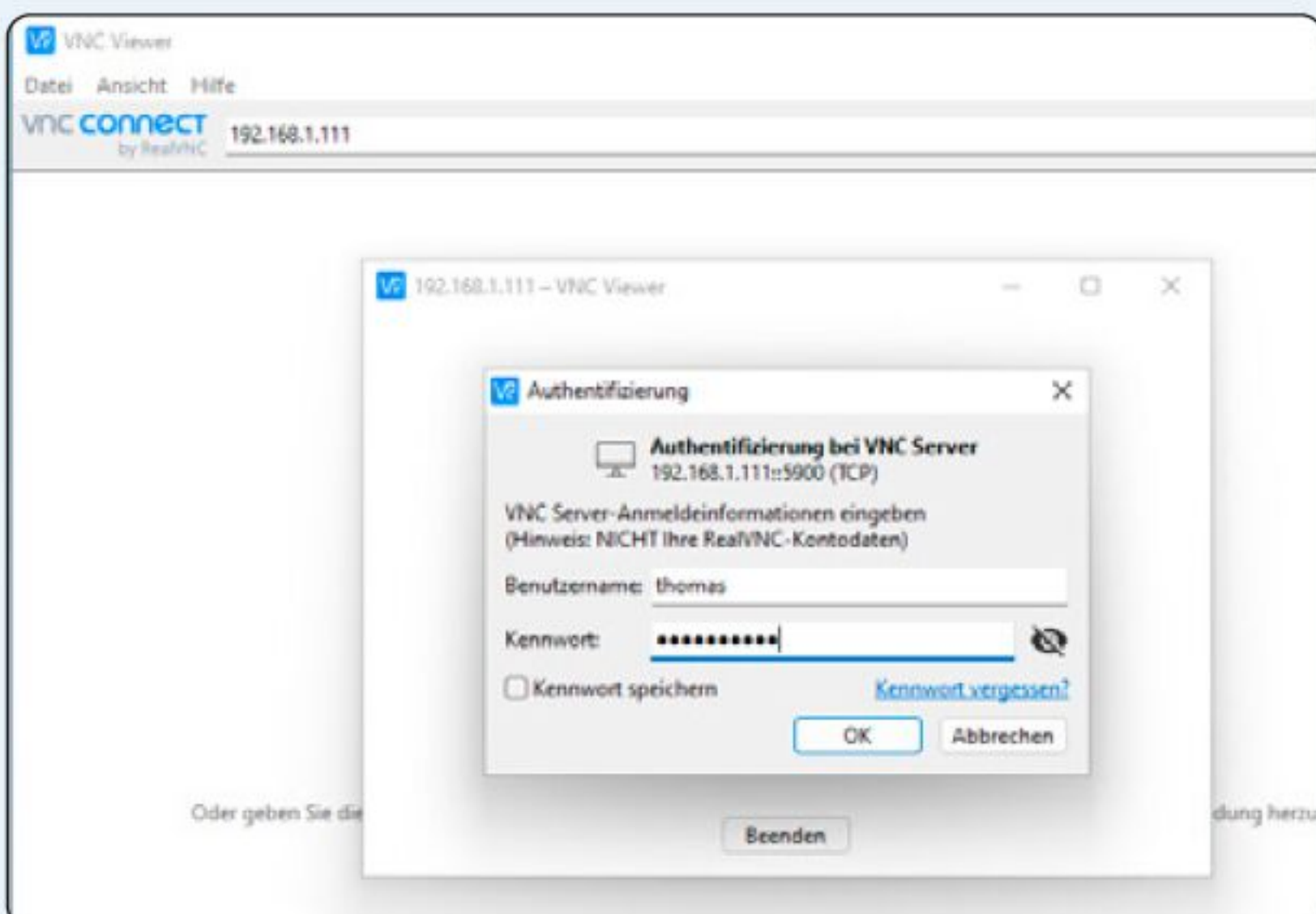
2 Aktiviere in den „Einstellungen“ bei „Entfernter Zugriff“ „Server-App auf entferntem Mac verwenden“. Du kannst auch Apple Remote Desktop und SSH aktivieren.



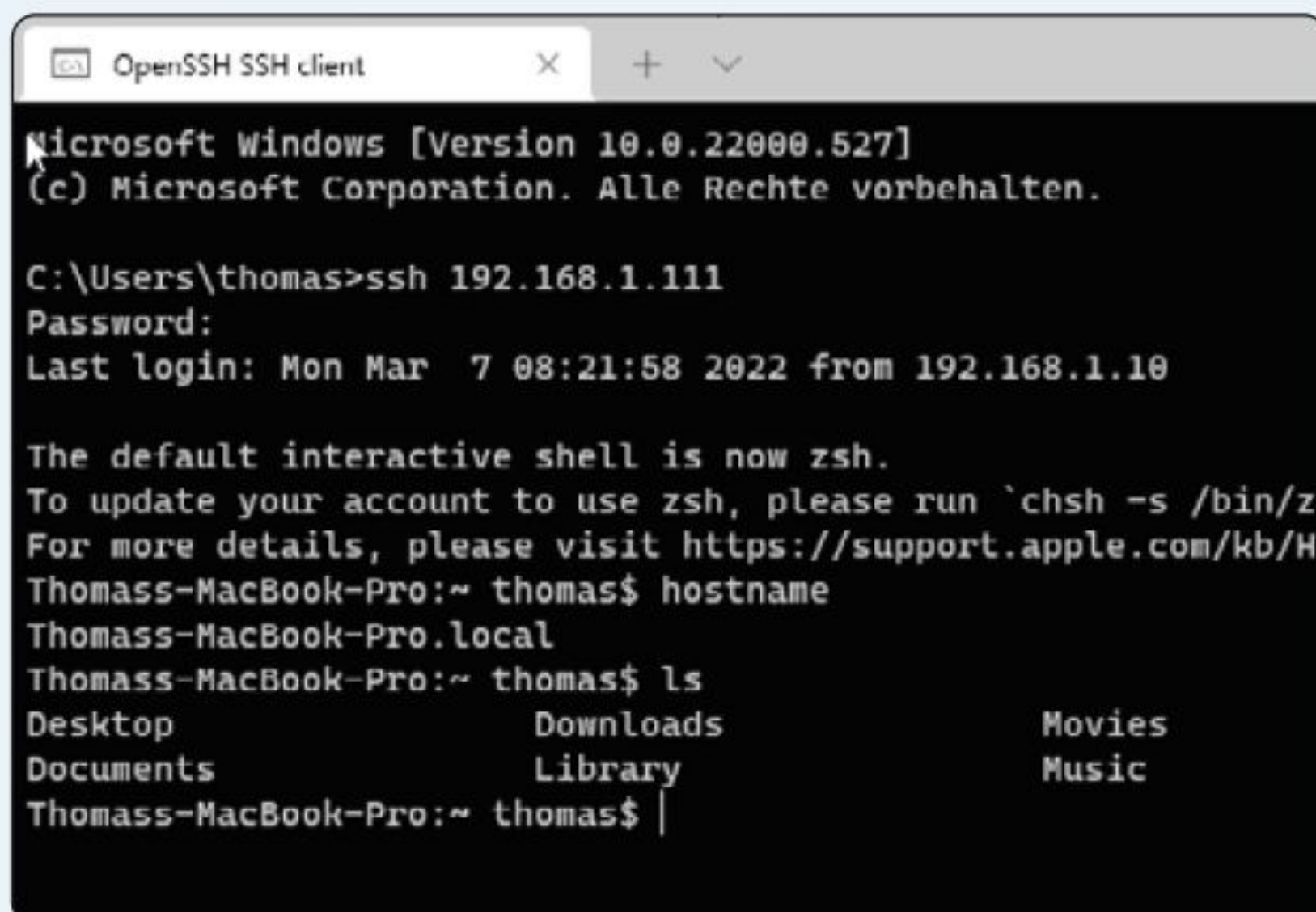
3 Installiere die macOS Server-App auf dem Mac, mit dem du deinen Server in Zukunft verwalten willst. Wähle die Option „Anderer Mac“ und gib die Daten ein.



4 Hast du „Bildschirmfreigabe“ aktiviert, kannst du mit einem kostenfreien VNC-Viewer über das Netzwerk von Linux und Windows aus auf einen macOS Server zugreifen.

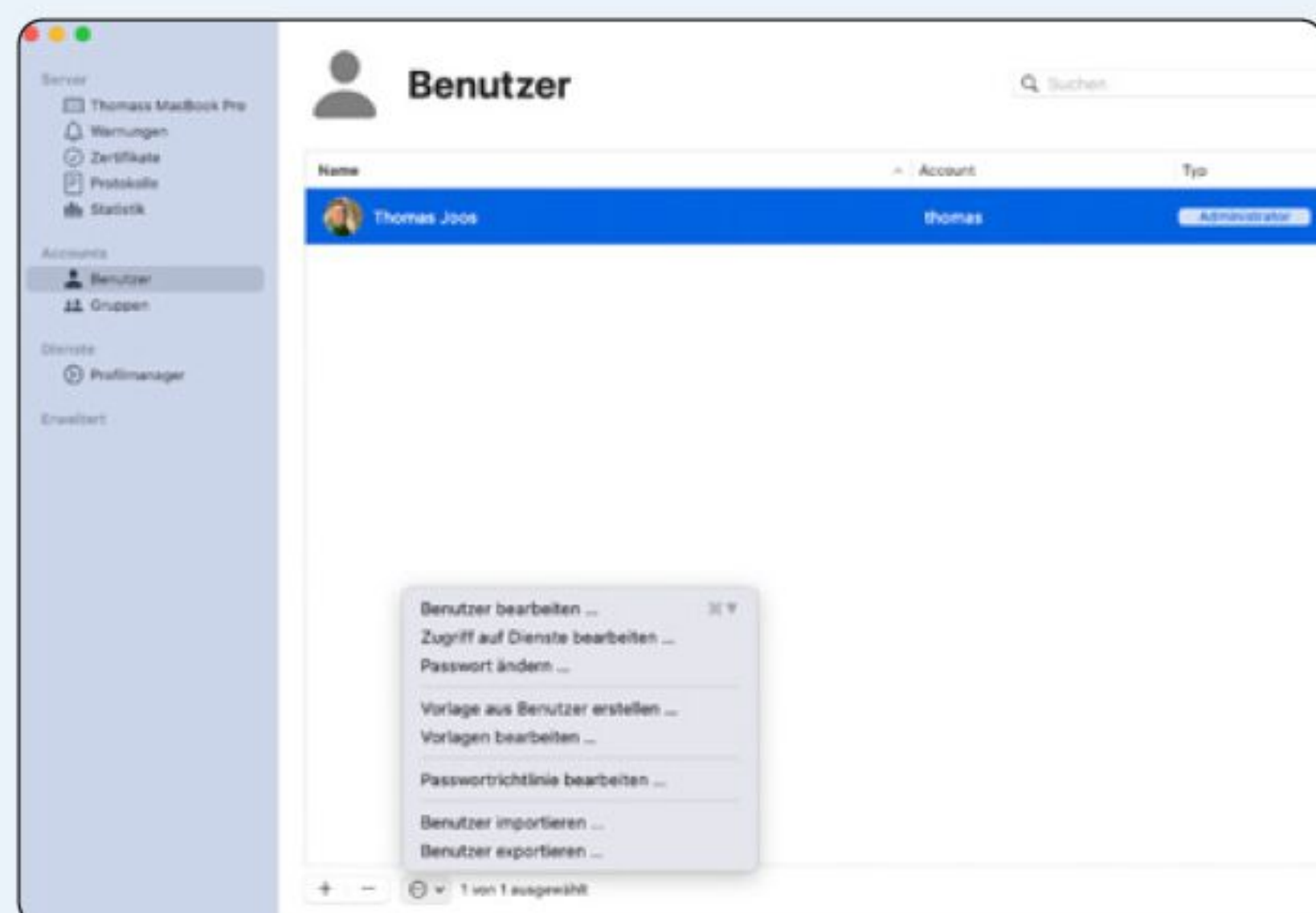


5 Bestätige die Warnung und melde dich an deinem Mac mit dem VNC-Viewer an. Du kannst deinen Mac im Remote-Fenster steuern und die Anmeldedaten speichern.

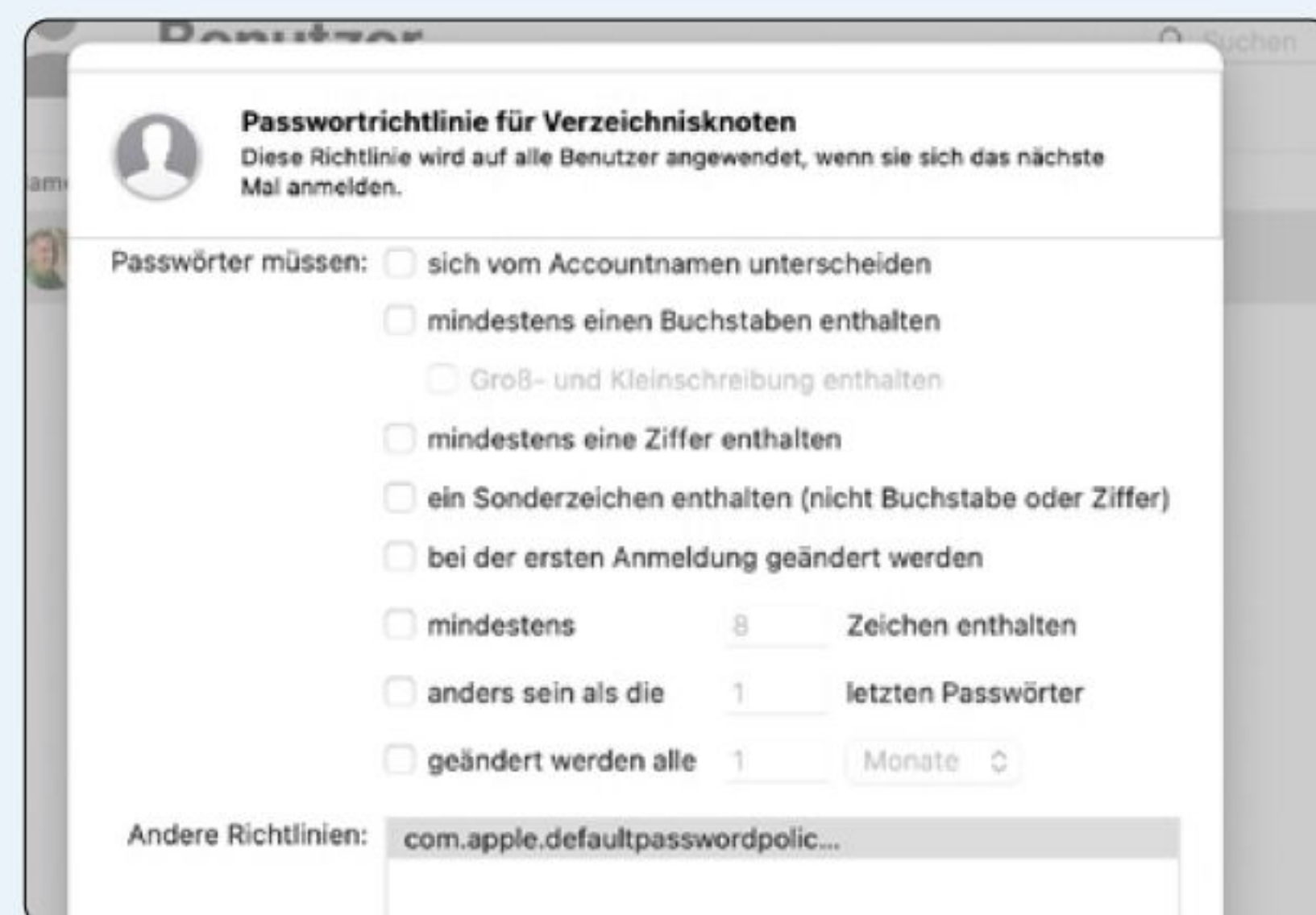


6 In der Befehlszeile von Windows und Linux kannst du mit ssh [IP-Adresse] eine Verbindung zu deinem Mac im Terminal aufbauen. Melde dich als Admin an.

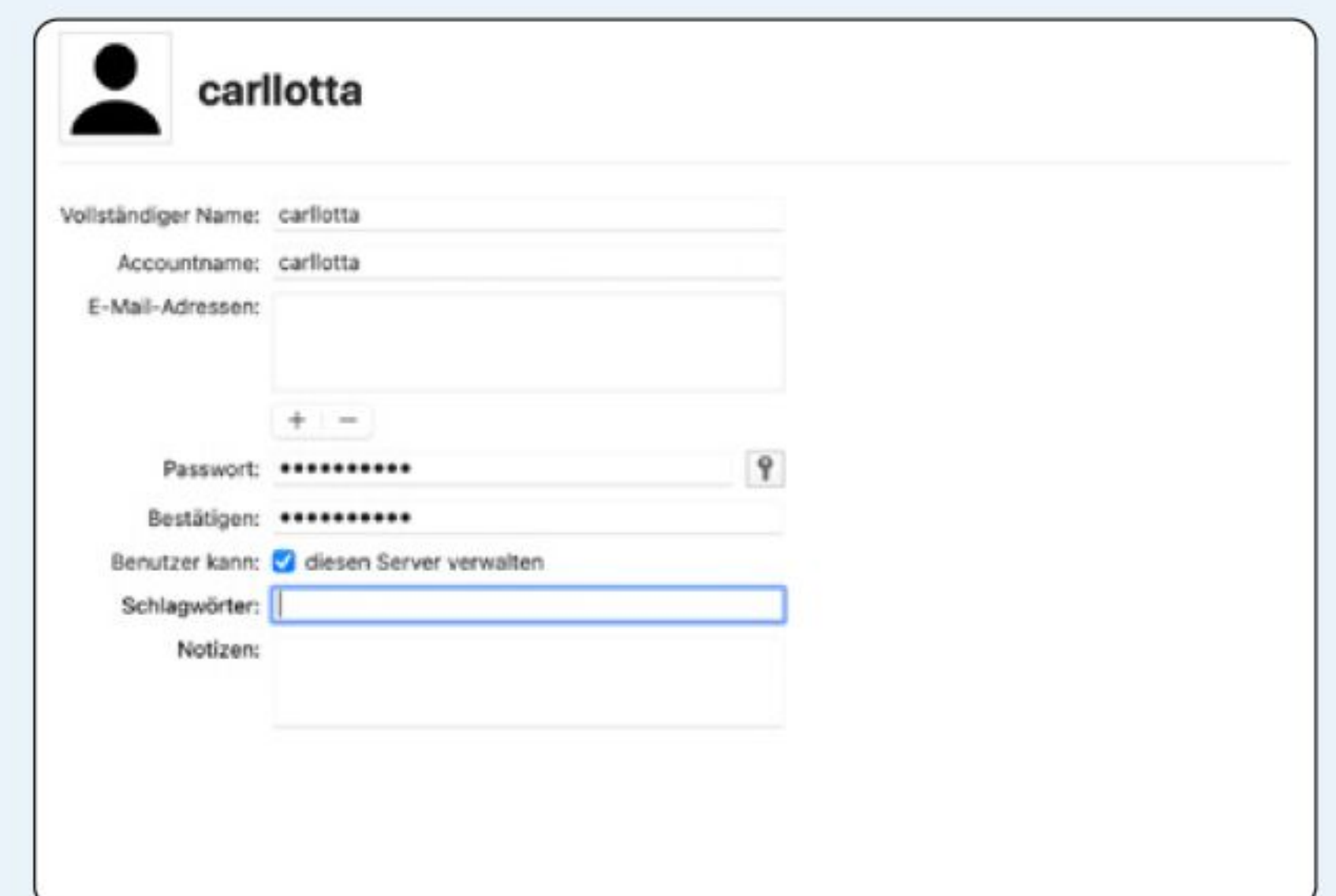
Workshop: So verwaltest du Benutzer:innen und Kennwörter für den Serverzugriff



1 Klicke auf „Benutzer:innen“. Unten links kannst du neue Benutzer:innen anlegen, solltest aber zuerst „Passwortrichtlinie bearbeiten“ in den Optionen auswählen.

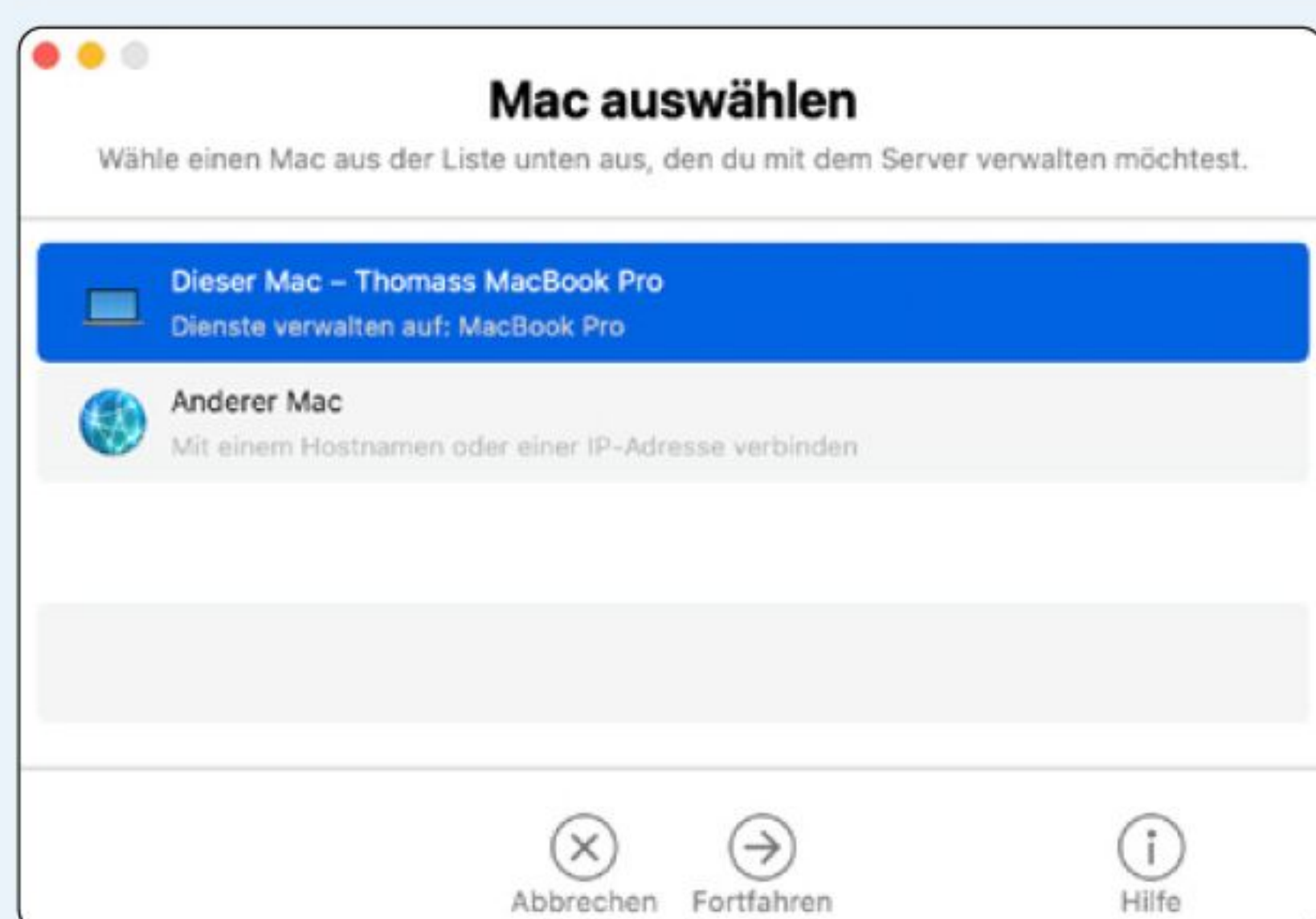


2 Im Fenster „Passwortrichtlinien für Verzeichnisknoten“ kannst du festlegen, wie das Kennwort konfiguriert sein muss, damit sie auf Ressourcen zugreifen dürfen.



3 Mit dem Plus legst du ein neues Benutzungskonto an. Fülle die Felder aus und lege fest, ob die neuen Benutzer:innen das Recht erhalten sollen, den Server zu verwalten.

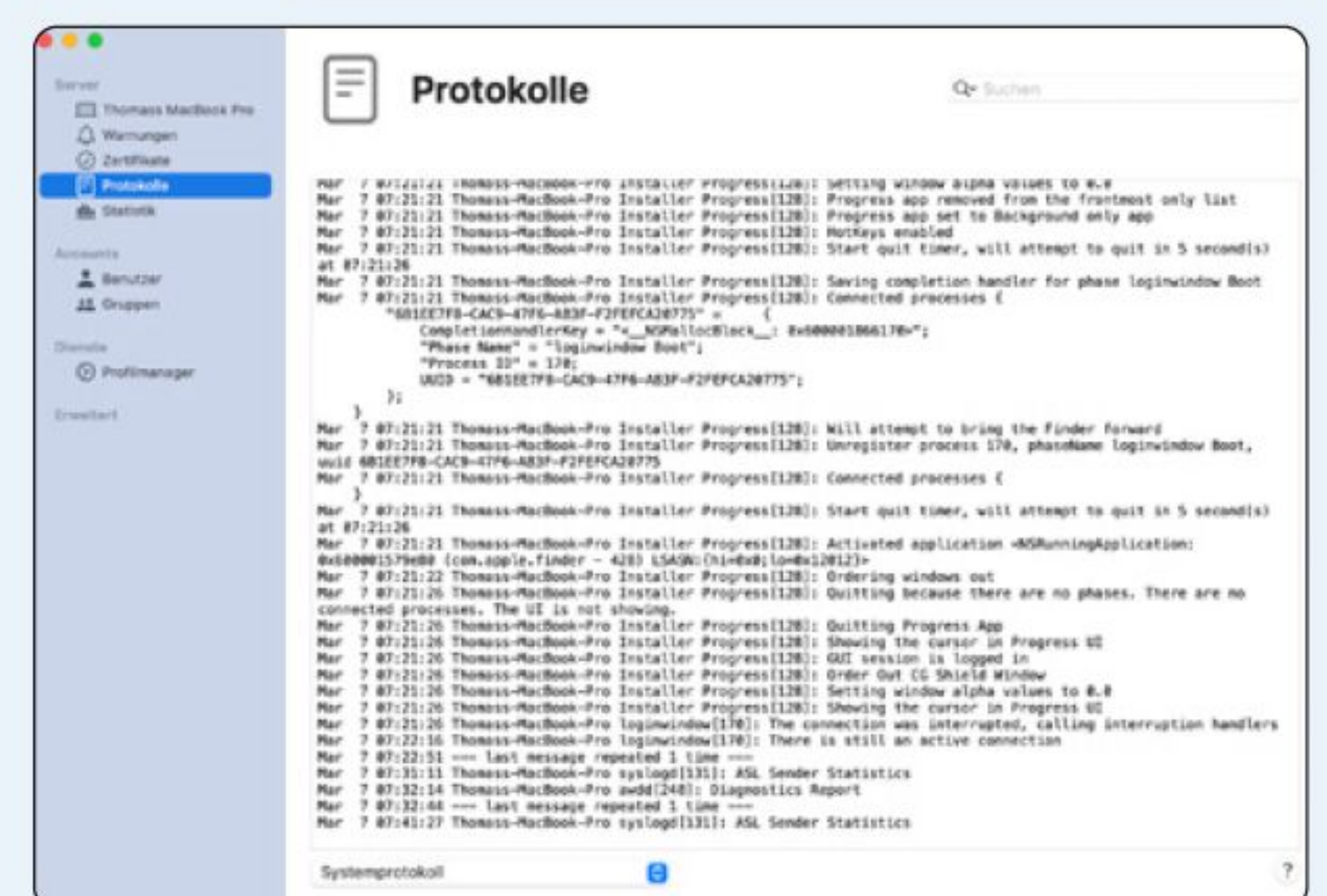
Workshop: So gehst du deine ersten Schritte mit macOS Server



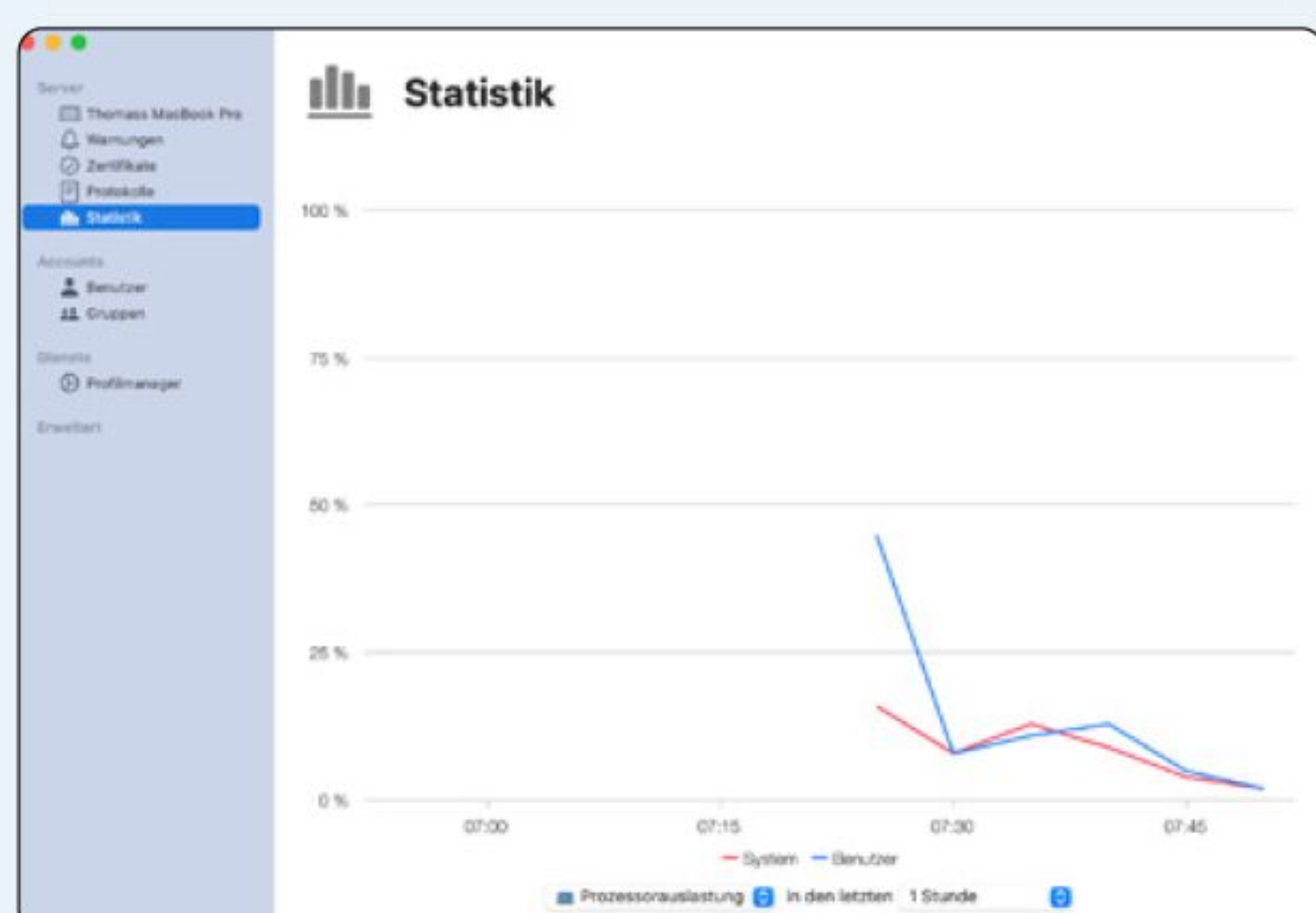
1 Starte die Server-App und melde dich an. Stelle in der „Übersicht“ sicher, dass der jeweilige Status bei „Hostname“, „Computernamen“ und „Internet“ grün ist.



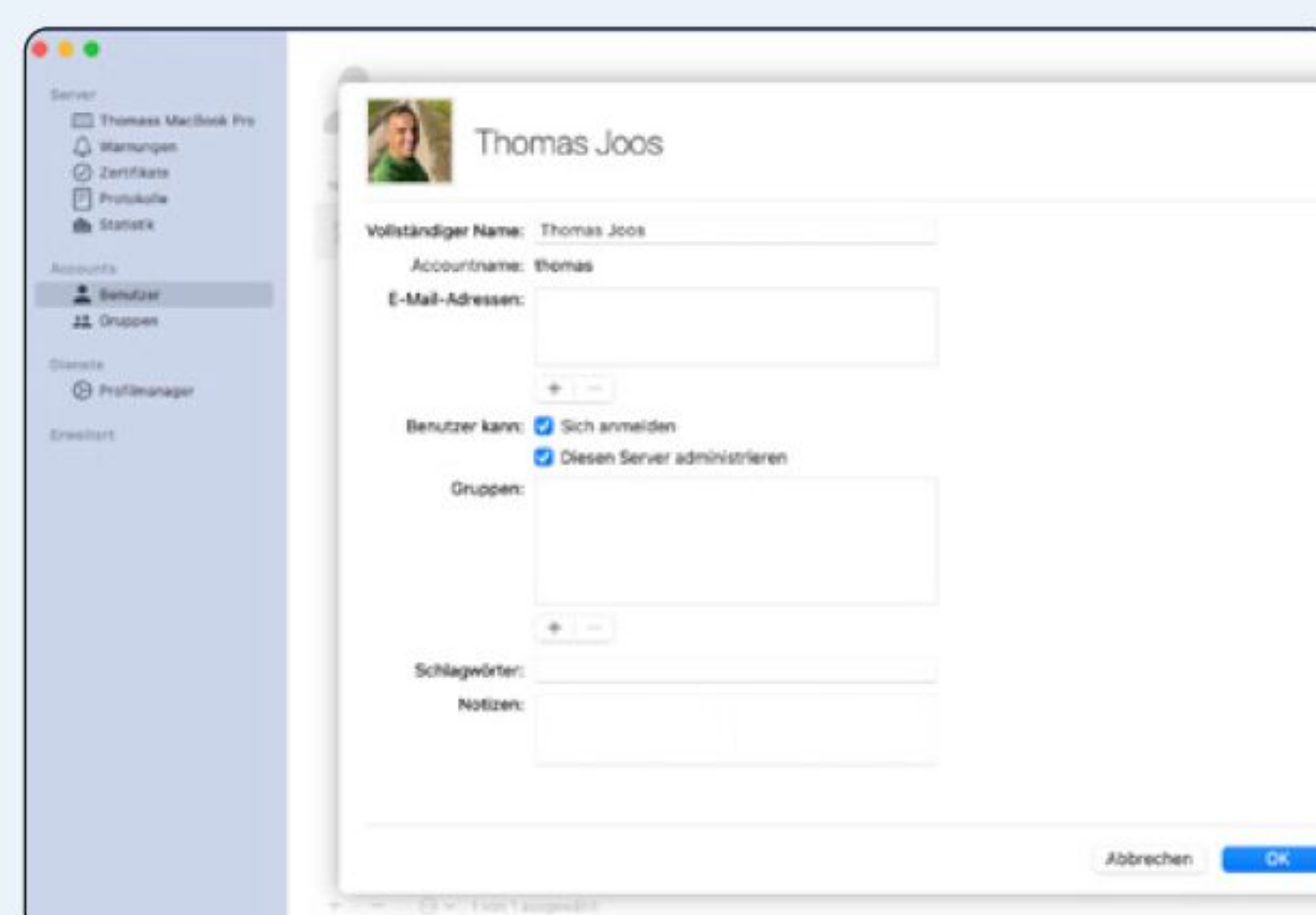
2 Überprüfe, ob bei „Version“ die aktuelle Version 12 von macOS zu sehen ist und mindestens die Version 5.12.1 bei „Server“ angezeigt wird.



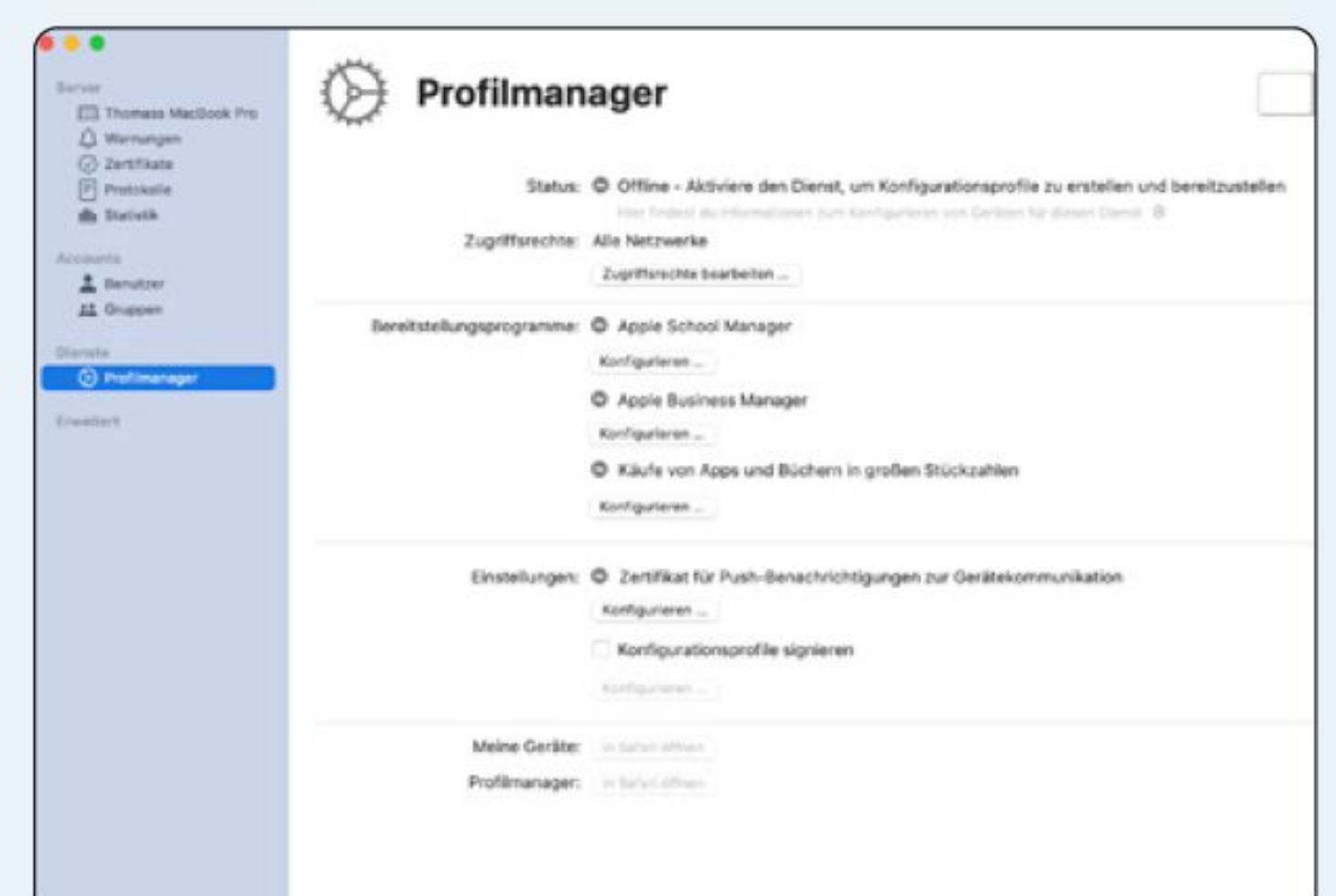
3 Klicke auf „Warnungen“. Hier sollte das Feld leer sein. Wenn nicht, solltest du die Probleme lösen. Bei „Protokolle“ sollten ebenfalls keine Fehler zu sehen sein.



4 Bei „Statistik“ siehst du die aktuelle Auslastung. Du kannst unten von „Prozessorauslastung“ zu „Speicherauslastung“, „Speichernutzung“ und „Netzwerkverkehr“ wechseln.



5 Klicke auf „Benutzer“. Hier muss dein Konto zu sehen sein. Dem Konto muss der Typ „Administrator“ zugewiesen sein. Per Doppelklick öffnen sich die Einstellungen.



6 Bei „Profilmanager“ sollten keine Fehler erscheinen. Der Dienst zum zentralen Verwalten von Profilen für Apple-Geräte ist inaktiv. Du kannst ihn jederzeit einrichten.

macOS im Netzwerk betreiben

In vielen Fällen betreiben Anwender:innen ihre Macs in einem Netzwerk. Bereits bei der Verbindung mit einem WLAN zum Internet baust du ein kleines Netzwerk auf.

TEXT: THOMAS JOOS



Kommen weitere Computer mit macOS, Linux oder Windows zum Einsatz, ist das Netzwerk systemübergreifend und bietet viele Ansatzpunkte für Optimierung, Fehlerbehebung und vor allem Sicherheit. Auch iPhones, iPads und Android-Geräte können Bestandteil eines Netzwerks sein. In diesem Beitrag zeigen wir, wie du Netzwerkverbindungen von macOS konfigurierst und verbesserst. Wir gehen dabei auch auf Neuerungen in macOS 12 (Monterey) ein.

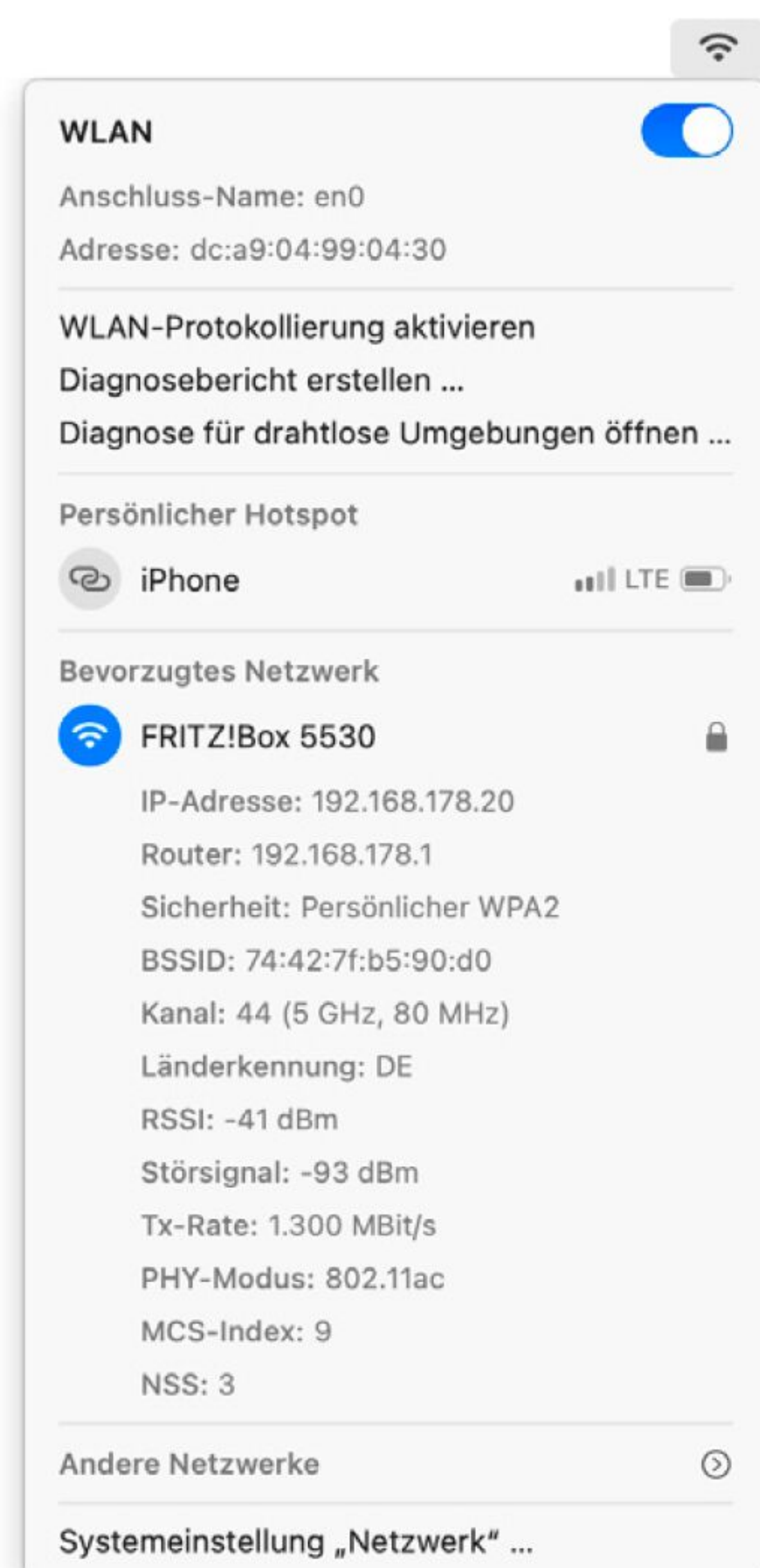
Grundlegende Netzwerkeinstellungen anpassen

Die wichtigsten Einstellungen für die Konfiguration der aktuellen Netzwerkverbindung finden sich in der Menüleiste oben rechts. Rufst du hier die Netzwerkeinstellungen auf, siehst du, mit welchem Netzwerk du verbunden bist und ob das Netzwerk sicher ist. Außerdem kannst du an dieser Stelle das WLAN komplett deaktivieren oder dich mit einem anderen WLAN verbinden. Grundsätzlich ist es sinnvoll, WLAN zu deaktivieren, wenn du aktuell keine Netzwerkverbindung benötigst. Das verhindert unerwünschten Aufbau von Netzwerkverbindungen.

Zusätzlich zeigt macOS an dieser Stelle auch deine persönlichen Hotspots an, zum Beispiel dein iPhone. Auch die aktuelle Internetverbindung des iPhone ist hier zu sehen. Das Netzwerksymbol erscheint aber nur, wenn du in den Systemeinstellungen auf dem Mac bei „Netzwerk“ die Option „WLAN-Status in der Menüleiste anzeigen“ aktiviert hast.

Hältst du die Option-Taste auf dem Mac gedrückt und klickst danach auf das WLAN-Symbol, zeigt macOS ausführlichere Informationen zu der Netzwerkverbindung an. Du siehst an dieser Stelle deine IP-Adresse, die IP-Adresse des Routers und die verwendete Verschlüsselung im Netzwerk. Auch der verwendete WLAN-Kanal und die Geschwindigkeit im aktuellen Netzwerk sind an dieser Stelle zu sehen.

Den dritten wichtigen Bereich für die Konfiguration deiner Netzwerkverbindungen findest du in den Systemeinstellungen bei „Netzwerk“. Hier siehst du ebenfalls, ob dein Mac mit dem Netzwerk verbunden ist und welche



Die Netzwerkeinstellungen in macOS erreichst du über die Menüleiste und die Systemeinstellungen.

IP-Adresse dein Gerät erhalten hat. Die Systemeinstellungen erreichst du auch über das Netzwerksymbol in der Menüleiste.

Wichtige Einstellungen für WLAN-Verbindungen steuern

In den Systemeinstellungen auf dem Mac findest du bei „Netzwerk“ die wichtigsten Optionen zur Steuerung deines Mac in Netzwerken. Nach dem Öffnen siehst du an dieser Stelle zunächst, mit welchem WLAN du verbunden bist. Hier kannst du auch einstellen, ob sich dein Mac mit diesem Netzwerk in Zukunft automatisch verbinden soll. Außerdem kannst du festlegen, ob vor der Netzwerkverbindung zu persönlichen Hotspots von dir, zum Beispiel zu deinem iPhone, eine Meldung erscheinen soll. Über „Weitere Optionen“ kannst du deine bevorzugten WLANs ausmisten und weitere wichtige Optionen einstellen.

Mehr Sicherheit für Netzwerke ab macOS 12 und iOS 15

Ab macOS 12 und iOS 15 kannst du in den Netzwerkeinstellungen von macOS die Option „iCloud Privat-Relay verwenden“ aktivieren. Durch die Aktivierung will Apple den Browser Safari bei der Verbindung mit öffentlichen Netzwerken besser schützen.

Einfach ausgedrückt, verschlüsselt macOS die Datenpakete von Safari, wenn diese das Netzwerk verlassen, bis der Rechner sie in das Internet sendet. Der Dienst leitet die Daten über zwei

Über die Menüleiste erreichst du die wichtigsten Netzwerkeinstellungen in macOS.

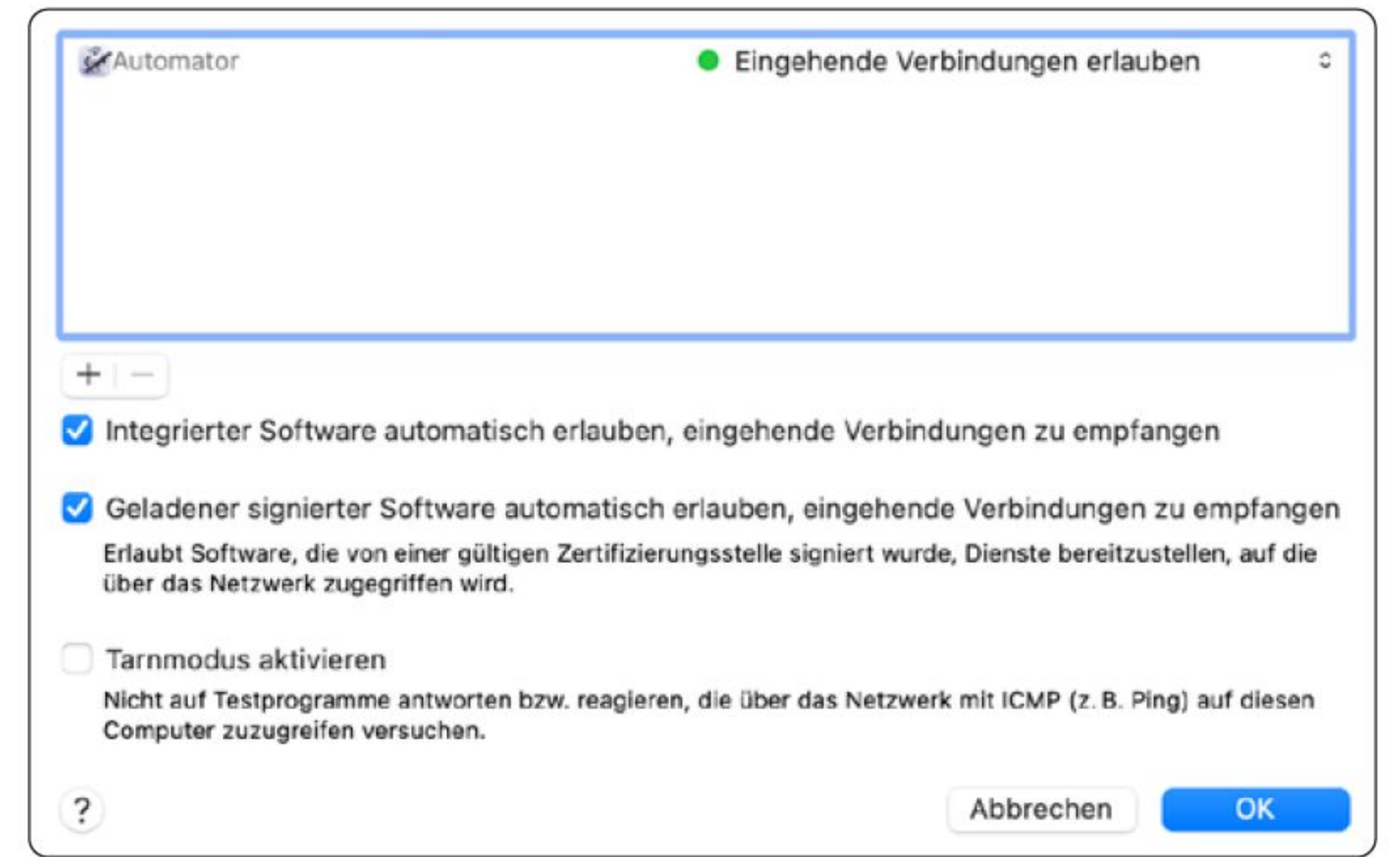
Internet-Relays. Das stellt sicher, dass im lokalen Netzwerk nicht mehr feststellbar ist, welche Internetseiten du aufrufst und wie deine IP-Adresse lautet. Du musst dazu nur diese Option aktivieren und Safari als Browser nutzen sowie ein iCloud-Abonnement besitzen.

Deine IP-Adresse wird dadurch verschlüsselt und ist nicht mehr einsehbar, ähnlich wie bei einem VPN. Aktuell funktioniert die Technik nicht mit anderen Browsern. Auch auf iPhones mit iOS 15 und iPads mit iPadOS 15 kannst du diese Option für Safari nutzen, das hat aber nichts mit den Netzwerkeinstellungen in macOS zu tun. Der Dienst sichert deine Datenverbindungen im Netzwerk zum Internet recht zuverlässig ab.

Tarnmodus aktivieren

Sobald ein Mac im Netzwerk angebunden ist, spielt auch die Sicherheit eine wesentliche Rolle. Zunächst sollte in den Systemeinstellungen von macOS bei „Sicherheit & Datenschutz“ auf der Registerkarte „Firewall“ die interne Firewall von macOS aktiv sein. Nachdem du die Firewall aktiviert hast, kannst du mit „Firewall-Optionen“ deren Einstellungen steuern.

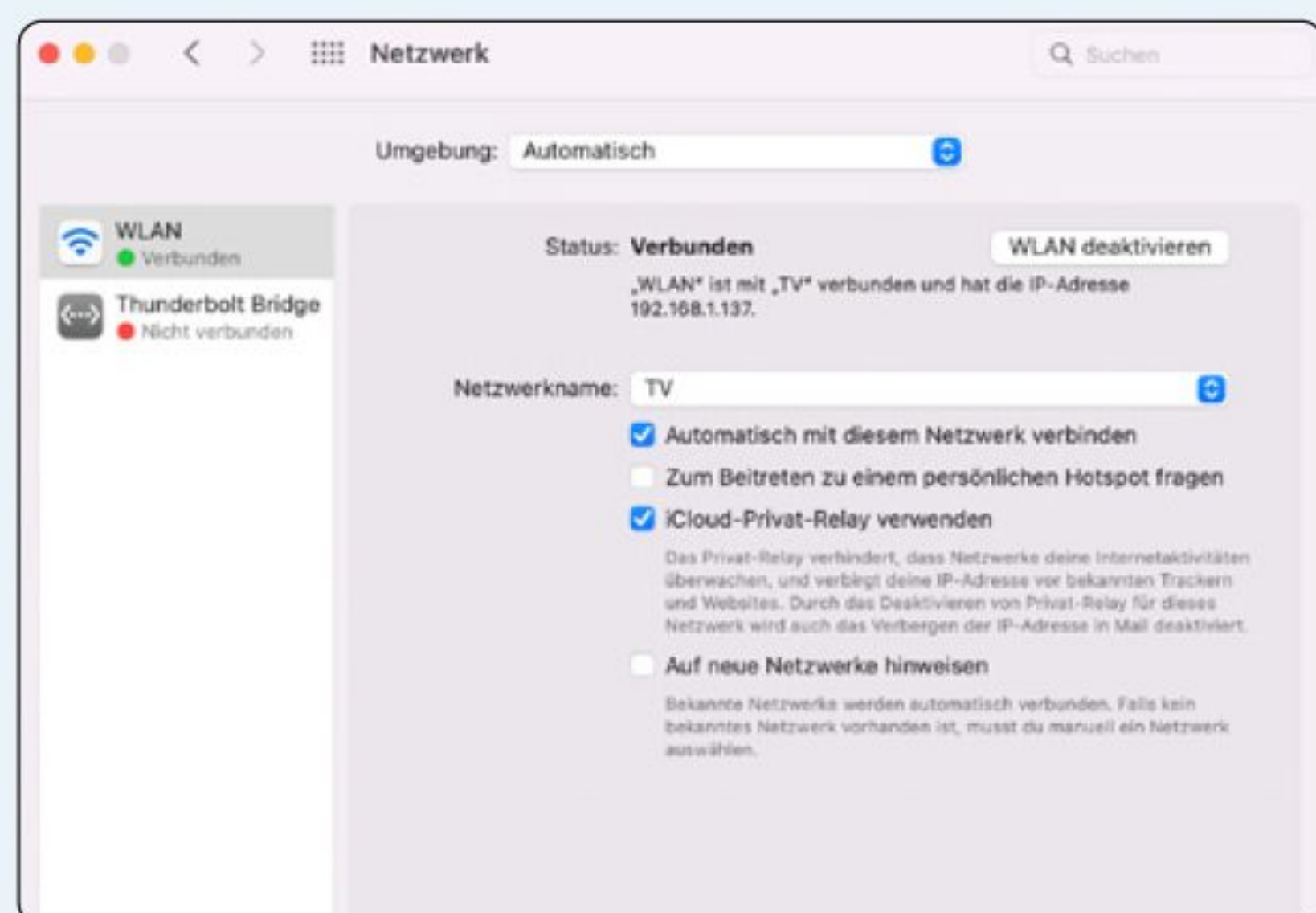
Die Einstellungen sind zunächst optional. An dieser Stelle kannst du zum Beispiel festlegen, welche Programme auf dem Mac eingehende Verbindungen von außen erhalten dürfen. Zur erhöhten Sicherheit kannst du an dieser Stelle noch die Option „Tarnmodus aktivieren“ setzen. In



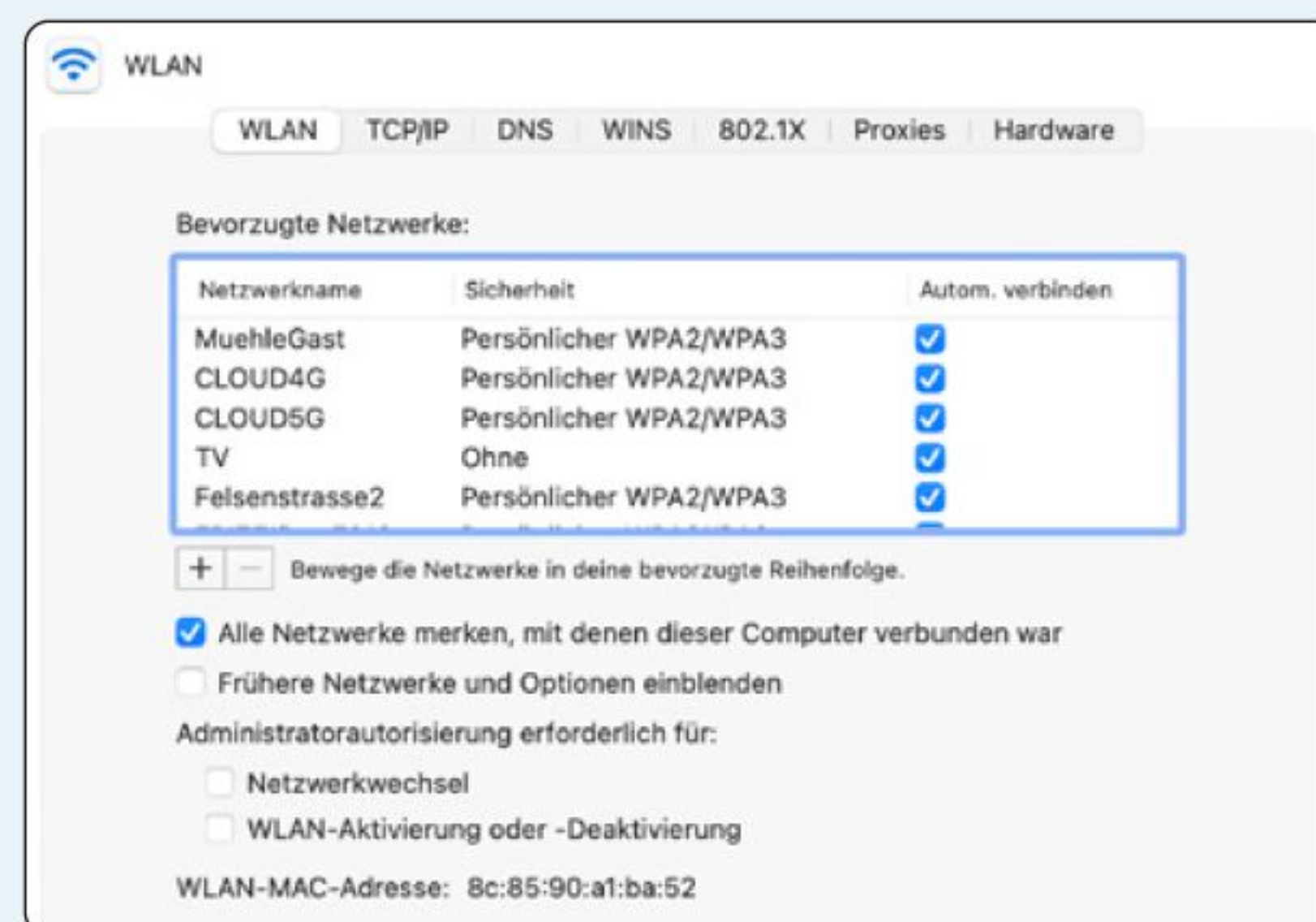
Bei der Verwendung von macOS im Netzwerk solltest du die interne Firewall aktivieren. Das erledigst du in den Systemeinstellungen.

diesem Fall können andere Rechner im Netzwerk deinen Mac nicht anpingen, um dadurch die IP-Adresse oder den Online-Status zu überprüfen.

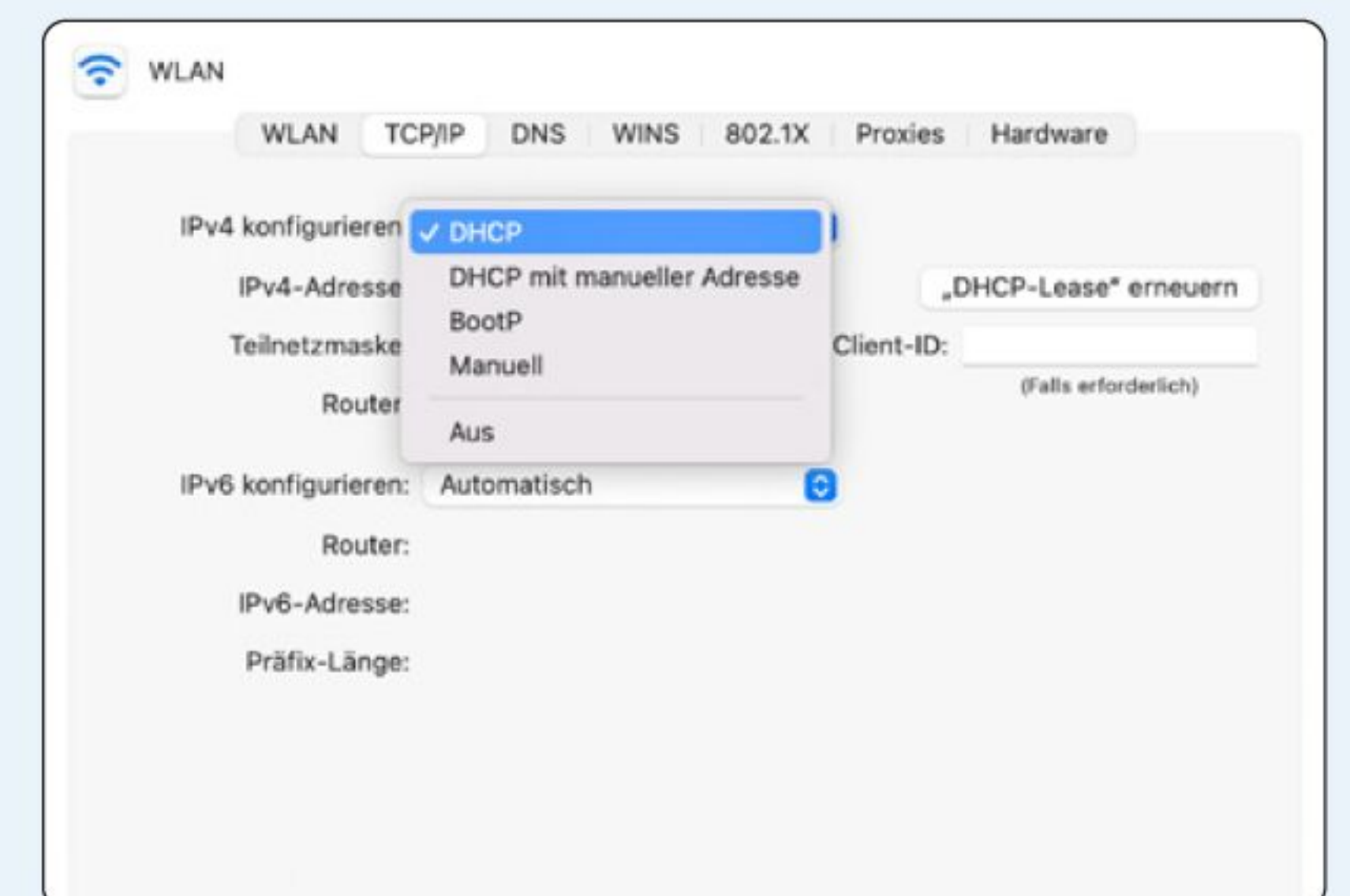
So geht's: Proxy, IP-Adresse und WLAN-Optionen in macOS einstellen



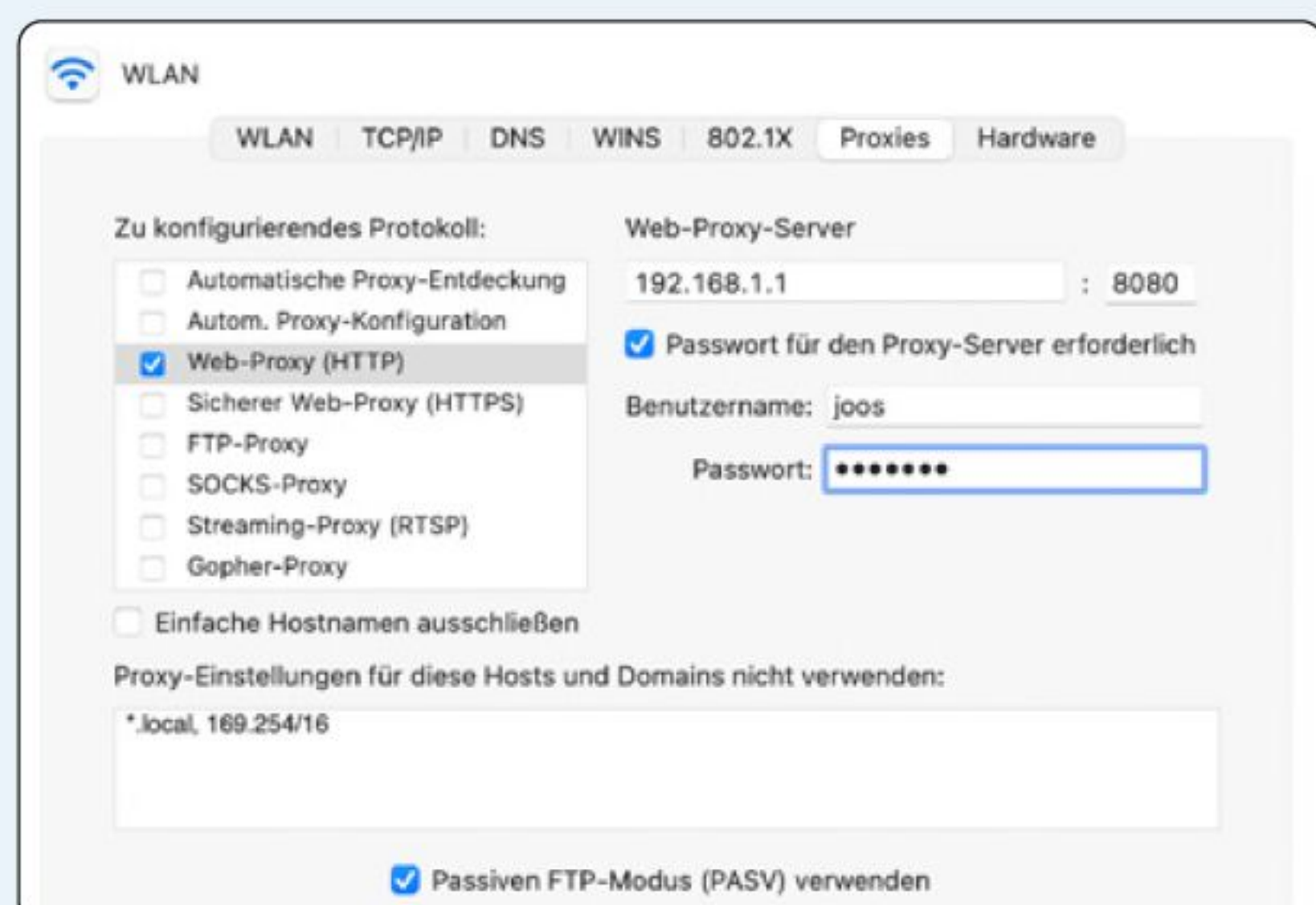
1 Starte „Netzwerk“ über die Systemeinstellungen. Unten rechts findest du die Schaltfläche „Weitere Optionen“. Hier steuerst du auch deine IP-Adresse im Netzwerk.



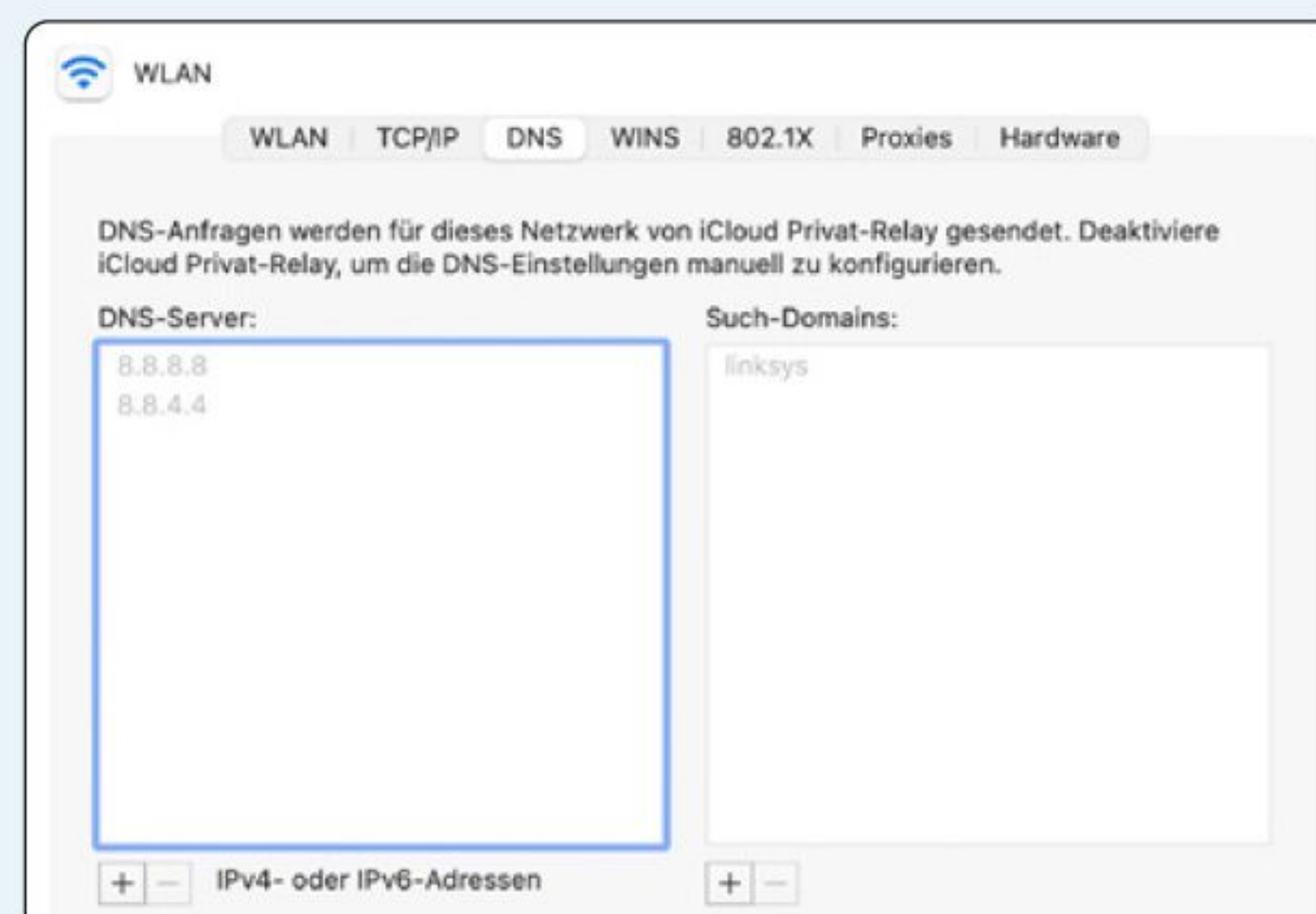
2 Auf der Registerkarte „WLAN“ findest du alle WLANs, die in deiner Apple-ID gespeichert sind. Hier solltest du die Liste regelmäßig ausmisten und damit bereinigen.



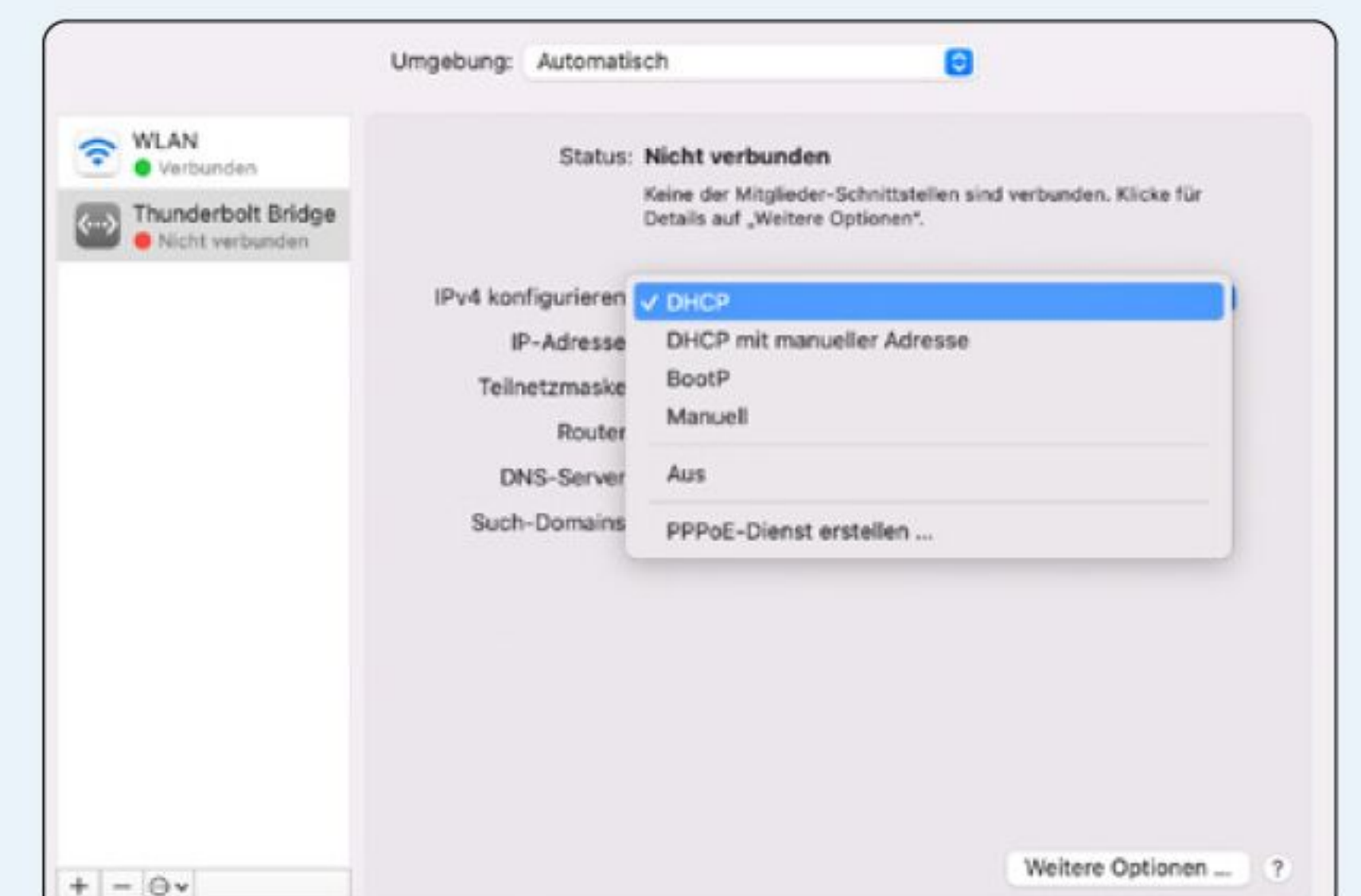
3 Über den Menüpunkt „TCP/IP“ kannst du einstellen, ob dein PC eine statische IP-Adresse erhalten soll. Dazu aktivierst du die Option „Manuell“.



4 In Unternehmensnetzwerken kannst du auf der Registerkarte „Proxies“ die Daten des Internetproxies im Unternehmen und die Anmeldeinformationen hinterlegen.



5 Auf der Registerkarte „DNS“ sind die Server für die Namensauflösung zu finden. Mit dem Plus lassen sich weitere DNS-Server hinzufügen.



6 Über „Thunderbolt Bridge“ kannst du zwei Macs mit einem Thunderbolt-Kabel verbinden. Die Einstellungen dazu nimmst du hier vor und steuerst auch die IP-Adresse.

Namensauflösung im Terminal testen

Wenn Verbindungen im Netzwerk und Internet nicht richtig funktionieren, kannst du im Terminal die Verbindungen und auch die Namensauflösung testen. Die Namensauflösung kannst du mit `nslookup <Computernamen oder Internetadresse>` testen, zum Beispiel `nslookup www.maclife.de`. Erhältst du hier Informationen, funktioniert die Namensauflösung.

Wenn nicht, kannst du in den Netzwerkeinstellungen den DNS-Server ändern, wie im Workshop in diesem Beitrag zu sehen ist. Eine Verbindung kannst du mit `ping <Computernamen oder Inter-`

Mit den Terminal-Befehlen „nslookup“ und „ping“ kannst du Verbindungen im Netzwerk analysieren.

```
The default interactive shell is now zsh.
To update your account to use zsh, please run `chsh -s /bin/zsh`.
For more details, please visit https://support.apple.com/kb/HT208050.
Thomass-MacBook-Pro:~ thomas$ nslookup www.maclife.de
Server:      8.8.8.8
Address:     8.8.8.8#53
```

```
Non-authoritative answer:
Name:   www.maclife.de
Address: 138.201.149.7
```

```
Thomass-MacBook-Pro:~ thomas$ ping maclife.de
PING maclife.de (138.201.149.7): 56 data bytes
64 bytes from 138.201.149.7: icmp_seq=0 ttl=57 time=12.945 ms
64 bytes from 138.201.149.7: icmp_seq=1 ttl=57 time=15.859 ms
64 bytes from 138.201.149.7: icmp_seq=2 ttl=57 time=12.708 ms
^C
--- maclife.de ping statistics ---
3 packets transmitted, 3 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 12.708/13.837/15.859/1.433 ms
Thomass-MacBook-Pro:~ thomas$
```

netadresse> testen, zum Beispiel `ping www.maclife.de`. Dabei verschickt der Mac ICMP-Pakete. Das Pingen kannst du mit der Tastenkombination `[ctrl]+[C]` beenden.

Blockiert der empfangende Rechner die Verbindung, erhältst du aber keine erfolgreiche Antwort. Beim Pingen ist es also nicht sicher, ob die Verbindung tatsächlich nicht funktioniert oder der Empfänger diese nur blockiert, zum Beispiel über den aktivierten Tarnmodus der Firewall.

Informationen im Terminal auslesen

Wichtige Informationen, wie IP-Adressen, Netzwerkverbindungen und Status der Netzwerkad-

apter sind mit `ifconfig` zu sehen. Der Befehl `netstat -r` zeigt Informationen zu anderen Rechnern im Netzwerk und das Gateway zum Internet.

Über das Terminal kannst du in macOS auch SSH-Verbindungen zu anderen Computern aufbauen. Dazu gibst du im Terminal den Befehl `ssh <Benutzername@><IP-Adresse>` ein. Natürlich muss auf dem entsprechenden Computer SSH aktiviert sein. In macOS rufst du in den Systemeinstellungen „Freigaben“ auf und danach „Entfernte Anmeldung“. Danach kannst du den Zugriff per SSH aktivieren und festlegen, welche Benutzungskonten sich mit SSH verbinden dürfen.

Diagnose-Assistenz

In macOS sind Assistenzen integriert, die bei der Analyse von Netzwerkproblemen umfassende Informationen ausgeben und Tipps zur Problemlösung geben. Das GZip-Archiv der Assistenz zur Diagnose von WLANs enthält zahlreiche Textdateien, die Anwender:innen auch an Profis weitergeben können. Diese erhalten dadurch Informationen, um bei der Problemlösung zu helfen. Die Diagnose-Assistenz sollte der erste Schritt sein, um Netzwerkprobleme von Macs zu lösen, da sie auch Tipps für die schnelle Problembehebung gibt.

So geht's: Fehler bei Netzwerkverbindungen mit Assistenzen beheben



1 Hältst du die Option-Taste gedrückt und klickst auf das WLAN-Symbol in der Menüleiste, kannst du die „Diagnose für drahtlose Umgebungen“ öffnen.



2 Im nächsten Schritt zeigt die Assistenz offensichtliche Fehler an und ermöglicht mit „Meine WLAN-Verbindung analysieren“ erweiterte Tests.



3 Am Ende erstellt die Assistenz einen Diagnosebericht. Danach zeigt macOS Tipps für die Verbesserung des Netzwerks und Informationen zum Netzwerk an.

Alles über iPhone, iPad und Apple Watch



Lies die iPhone Bibel
auch auf deinem iPad
oder iPhone in der
Kiosk-App „Mac Life“!



www.falkemedia-shop.de/iphonebibel

HomeKit aus der Box

Mit der kleinen Box sollst du nicht HomeKit-zertifizierte Geräte in dein Apple-Smarthome integrieren können, ohne Befehle in die Konsole tippen zu müssen. Wir haben sie ausprobiert.

TEXT: SVEN T. MÖLLER

Apple bietet mit HomeKit eine einfache Lösung zur Verwaltung smarterer Geräte wie Leuchten, Überwachungskameras oder Heizungsthermostate in deinem Zuhause. Die Technologie macht die initiale Integration und spätere Interaktion im Alltag für unerfahrene Anwender:innen besonders einfach. Kompatibles Gerät einschalten, HomeKit-Code scannen und wenig später steht es in der Home-App zur Steuerung und für Automationen zur Verfügung. Nennst du zudem einen HomePod, ein Apple TV oder ein entsprechend konfiguriertes iPad dein Eigen, dienen diese automatisch als Steuerzentrale, sodass du dein Zuhause sogar von unterwegs aus steuern kannst.

Auftritt Homebridge

Leider integrieren längst nicht alle Hersteller Apples Technologie. Du hast also folgende Möglichkeiten: Entweder konzentrierst du dich ausschließlich auf Produkte, die für HomeKit zertifiziert sind (und zahlst nicht selten einen höheren Preis) oder du schlägst dich mit einem Dutzend verschiedener Apps herum (die es zudem oft nur für iPhone und iPad, nicht aber für den Mac gibt). Dank einer findigen Community gibt es seit einiger Zeit eine dritte Option namens Homebridge. Die Open-Source-Software dient – der Name legt es nahe – als Brücke zwischen smarten Geräten und deiner HomeKit-Steuerzentrale. Meist kommt sie als Server-Lösung auf einem Raspberry Pi oder als Docker-Container in einem NAS zum Einsatz. Alle benötigten Daten können kostenfrei von der GitHub-Seite des Projektes geladen und anschließend auf eine microSD-Karte geflasht werden. Dir schwirrt jetzt schon der Kopf? Dann ist HOOBS vielleicht die bessere Lösung für dich.

HOOBS steht für „Homebridge Out Of the Box“ und ist seinerzeit aus dem Homebridge-Projekt heraus entstanden, um Anwender:innen das Management nicht HomeKit-zertifizierter Geräte so einfach wie möglich zu machen, indem etwa Änderungen an der Konfigurationsdatei config.json über eine grafische Eingabemaske vorgenommen werden können.

Rundum sorglos

Die Entwickler:innen von HOOBS bieten ihr Homebridge-Derivat in drei Schwierigkeitsstufen (und Preissegmenten) an, beginnend mit einem simplen Image, das du selbst auf eine SD-Karte flashen musst. Zu haben ist es theoretisch kostenfrei, vorgeschlagen wird jedoch ein Preis von 10 Euro. Das Flashen sparst du dir mit der gebrandeten microSD-Karte für 25 Euro, die du einfach in deinen Raspberry Pi steckst. Die wenigste Vorarbeit erkaufst du dir für 220 Euro mit der HOOBS Box, die wir im Folgenden genauer vorstellen und ausprobieren.

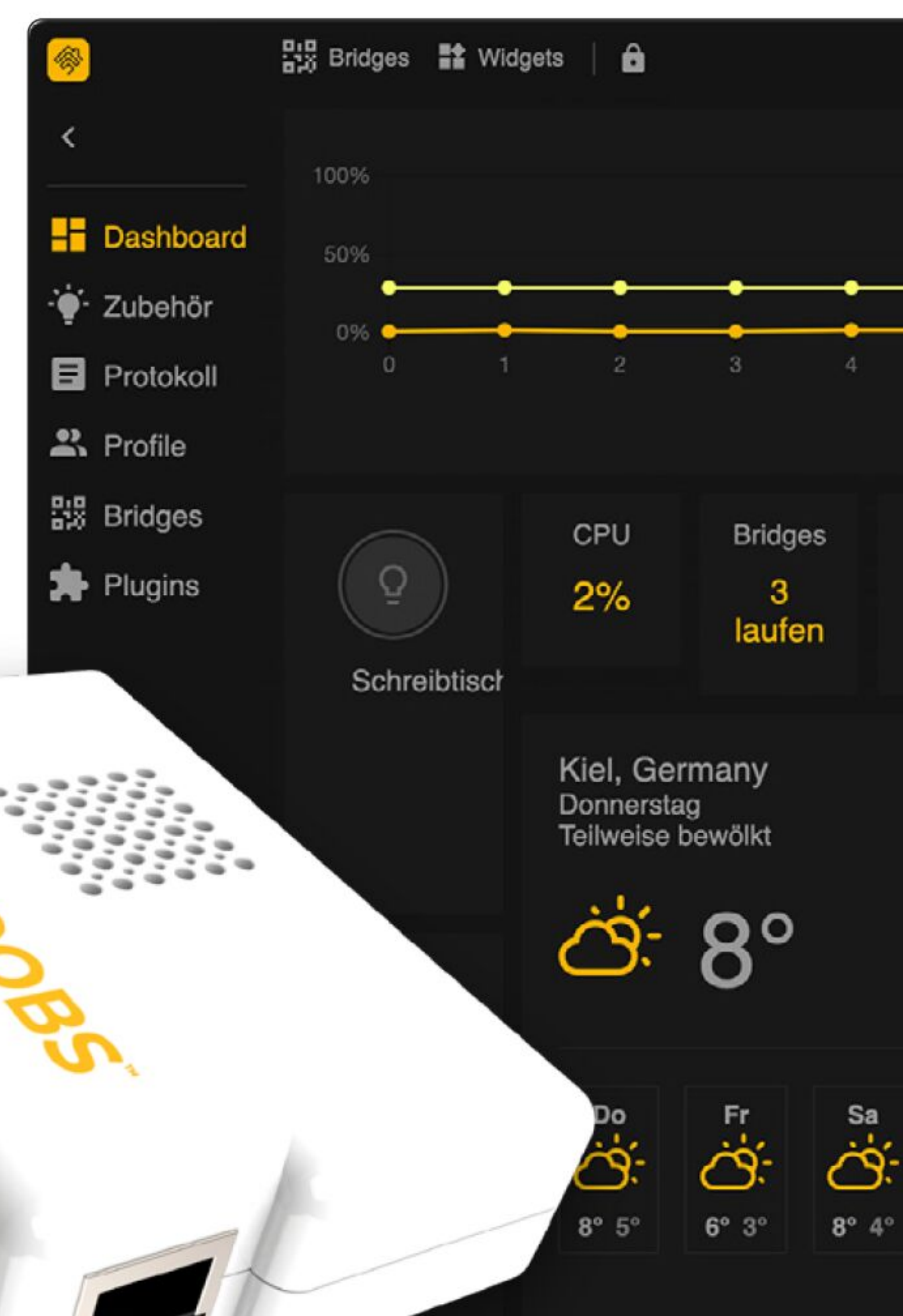
Das Starter-Kit enthält alles, was du zum Loslegen benötigst: einen Raspberry Pi gut verpackt in einem kleinen, weißen Case, ein Netzteil sowie ein Cat-7-Ethernet-Kabel. Du kannst die HOOBS Box auch in dein WLAN einlinken. Dafür verbindest du dich nach dem Start der Box zur weiteren Konfiguration zunächst mit deren Funknetzwerk. Wir wählen den stabileren Weg über das Kabel und starten die Mac-App. Alternativ kannst du die Benutzungsoberfläche im Browser unter der Adresse hoobs.local aufrufen. Beim ersten Start fordert uns die Software auf, einen Benutzungsaccount anzulegen, und präsentiert anschließend eine Übersichtsseite. Hier geben kleine Widgets unter anderem Auskunft

Im Inneren der unscheinbaren Box werkelt ein Raspberry Pi.



Raspberry Pi Spezial

Was du neben Homebridge noch so alles mit einem Raspberry Pi anstellen kannst, liest du in unserem PDF-Spezial: maclife.de/raspberry



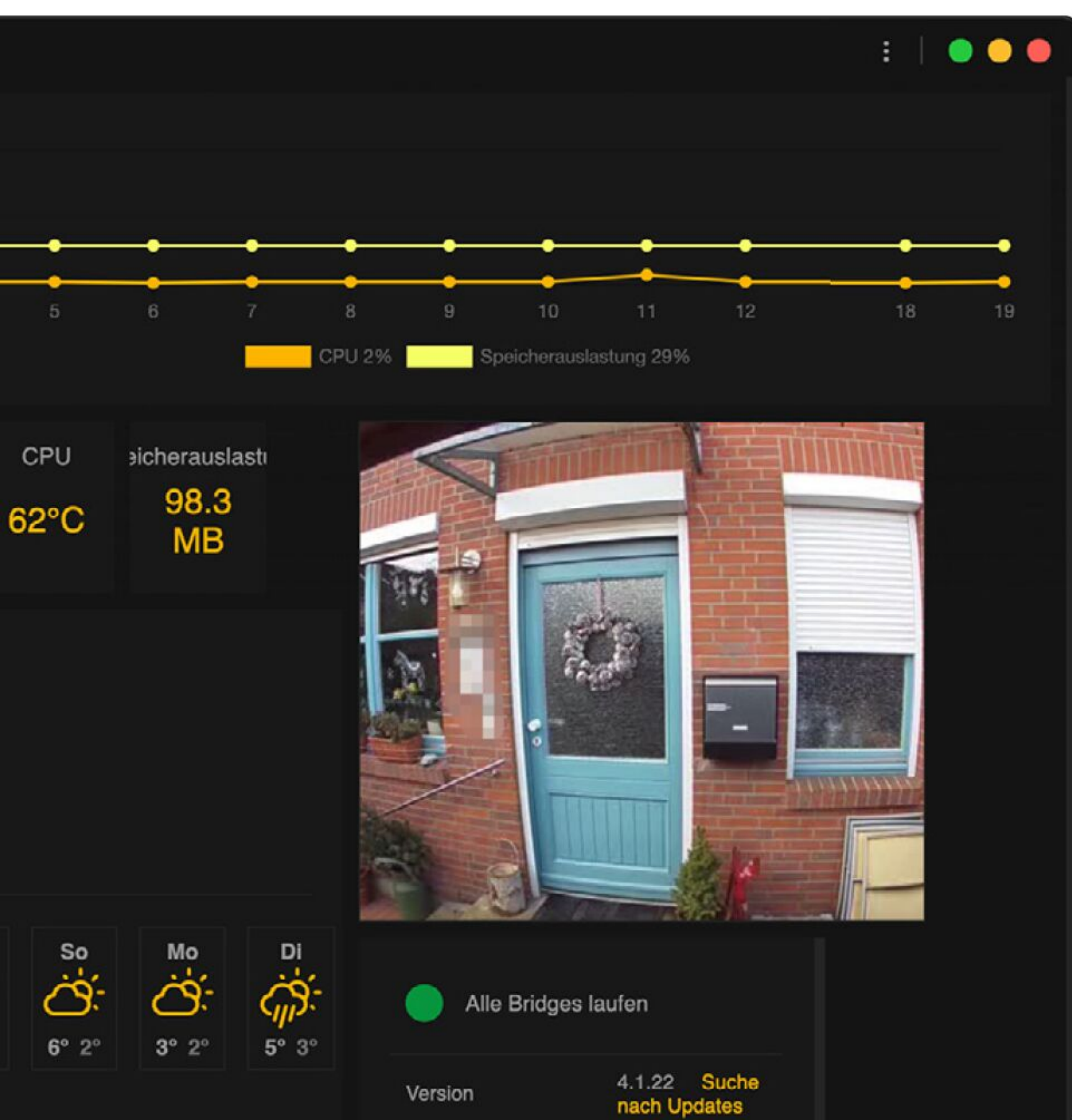
über die aktuelle CPU- und Speicherauslastung. Du kannst das Dashboard nach Belieben sortieren, wenn du oben links auf das kleine Schloss-Symbol klickst.

Der erste Versuch

Unser erstes Zubehör installieren wir, indem wir in der Seitenleiste ganz unten auf „Plugins“ klicken. Unter den vorgestellten und beliebten Plug-ins befinden sich bereits bekannte Namen wie „Nest“, „Philips Hue“ und „Ring“, von denen viele als „Zertifiziert“ deklariert sind, also in jedem Fall unter HOOBS laufen. Laut Statistik umfasst das Verzeichnis mehr als 3.000 Plug-ins. Bei näherer Betrachtung gibt es aber etliche, die als eher experimentell einzustufen sind.

Wir entscheiden uns für die Govee-Integration, um die Stehleuchte Lyra zu integrieren. Auf der Plug-in-Seite erfahren wir, dass neben unseren Govee-Zugangsdaten der API-Schlüssel für die Leuchte benötigt wird. Diesen können wir direkt in der Govee-App anfordern („Einstellungen“ > „Über uns“ > „API-Schlüssel beantragen“) und erhalten ihn gleich darauf per Mail.

Nach erfolgreicher Installation des Plug-ins geben wir den Schlüssel und unsere Zugangsdaten (an dieser Stelle vertrauen wir dem ganzen Projekt einfach



mal, was die Sicherheit angeht) in die entsprechenden Felder der Konfigurations-Seite ein und lassen die übrigen Parameter unberührt. Nach kurzer Bedenkzeit vermeldet die HOOBS Box die Einsatzbereitschaft einer Govee Bridge. Um diese nun mit HomeKit zu verheiraten, scannen wir den QR-Code von der Übersichtsseite mit der Home-App auf dem iPhone. Pflichtgetreu warnt diese vor einem nicht zertifizierten Gerät, was wir mit einem beherzten Tipp auf „Trotzdem hinzufügen“ quittieren. Und siehe da, in diesem Zuge findet die Home-App auch die mit unserem Govee-Account gekoppelte Stehlampe. Der Funktionsumfang ist allerdings limitiert, spezielle Leucht-Modi sind nicht anwählbar. Was aber geht, ist das Ein- und Ausschalten sowie das Justieren von Farbe und Helligkeit. Und natürlich können wir die Leuchte wie jede andere HomeKit-Lampe in Gruppen organisieren und in Szenen einbinden.

Geht da noch mehr?

Als Nächstes versuchen wir es mit einer smarten Birne aus den Anfangstagen der Heimautomation, einer LIFX Original A21, die schon etliche Jahre in den Untiefen einer Schublade vergraben lag. Da es kein zertifiziertes Plug-in gibt, entscheiden wir uns für das „Lifx Plugin“, das Glühbir-

Das Dashboard der HOOBS Box präsentiert dir alle wichtigen Infos auf einen Blick – und zeigt sogar das Kamerabild.

nen anhand ihrer IP-Adresse findet. Wir aktivieren sicherheitshalber die Option „Auto Detect“, die es unnötig macht, die IP-Adresse herauszufinden und einfach alle im Netzwerk befindlichen LIFX-Birnen an HomeKit übergibt. Das Hinzufügen in der Home-App funktioniert wieder problemlos und wir sind erstaunt, wie schnell die Lampe reagiert. Ob das an der Nähe zum Router und damit zur HOOBS Box liegt? Ein kurzer Check an einem anderen Standort beweist: Das Plug-in schaltet wirklich sehr schnell, schneller als so manche HomeKit-zertifizierte Leuchte.

Unser vorerst letztes Testobjekt ist eine Kamera von Ring, genauer eine Stick Up Cam Battery der 2. Generation. Die kabelfreie Outdoorcam ist bereits in der Ring-App eingerichtet, sodass wir für den Zugriff in HOOBS lediglich unsere Account-Daten im Plug-in hinterlegen müssen. Das Kamerabild taucht ohne weiteres Zutun in HOOBS unter „Zubehör“ auf und wir können es wie die Bedienelemente der anderen Geräte zum Dashboard hinzufügen. Da wir kein Abonnement haben, können wir sowohl in HOOBS als auch in der Home-App nur auf den Live-stream, nicht aber auf Snapshots oder Aufnahmen vorangegangener Ereignisse zugreifen. Gleichwohl der Bewegungssensor der Kamera Auslöser für bestimmte Automationen sein kann, etwa das

Licht an der Haustür einschalten, sobald eine Bewegung erkannt wird.

Zusammenfassung

Alles in allem eignet sich die HOOBS Box gut für den Einstieg. Die Hardware ist pflegeleicht, die Software macht dank der grafischen Benutzungsoberfläche vieles einfacher. Die Plug-ins sind von unterschiedlicher Qualität, manche schnell eingerichtet, andere komplexer und bisweilen treffen wir auf Code-Fragmente oder Parameter, die nicht selbsterklärend sind. Glücklicherweise gibt es eine Back-up-Funktion, von der du rege Gebrauch machen solltest, falls doch mal etwas schiefgeht.

In unserem Fall waren wir wohl zu ungeduldig, als wir nach einem Neustart zu früh die Stromversorgung kappten, mit dem Ergebnis, dass nichts mehr ging. Erst ein erneutes Flashen der SD-Karte mit der App BalenaEtcher und Einspielen des letzten Back-ups brachte die HOOBS Box zurück ins Leben. Alles kein Drama, wenn du technisch etwas versiert bist.

Ob die HOOBS Box etwas für dich ist, hängt in gewissem Maße davon ab, wie gern du tüftelst. Denn trotz aller Optimierungen musst du schon etwas Gehirnschmalz einsetzen, bis alles so läuft, wie du es gern hättest. Außerdem hängt es davon ab, welche Geräte du in deinem Smarthome einsetzt (oder künftig einsetzen willst). Ein Blick in das Plug-in-Verzeichnis ist in jedem Fall ratsam. Achte dabei auch auf die Voraussetzungen für die einzelnen Plug-ins.

Zum Schluss dann wäre da noch der Preis: Für 220 Euro bekommst du einen nicht mehr ganz taufrischen Raspberry Pi 3 Model B+, der auch schon mal für unter 50 Euro über die Ladentheke geht. Damit sich das lohnt, solltest du über eine beachtliche Zahl an Geräten verfügen, die gefügig gemacht werden sollen. Alternativ besorgst du dir anderweitig einen Raspberry Pi und beziehst lediglich das Image von HOOBS. Was du mit diesem noch so alles anstellen kannst, liest du in unserem Spezial.

Was nicht geht

Unsere Idee, Geräte des Platzhirschs Philips Hue der HOOBS Box hörig zu machen, scheitert bereits an der Voraussetzung einer Hue Bridge, die allerdings von sich aus HomeKit-kompatibel ist, oder einem Zigbee-Gateway wie dem RaspBee II (40 Euro). Aber das wäre ein ganz anderes Projekt.

Theoretisch ist es auch möglich, Saugroboter zu integrieren – jedoch als Ventilator, denn HomeKit weiß nichts von smarten Putzrobotern. Doch im Falle unseres Roborock müssten wir erst umständlich und mit fragwürdigen Tools den Token auslesen, was trotz aller Anleitungen im Internet nicht ganz einfach aussieht. Daher verschieben wir auch dieses Experiment auf einen späteren Zeitpunkt.

Der große WLAN-Guide

Ein funktionierendes WLAN ist ein essenzieller Teil unseres Lebens geworden. Wir erklären die wichtigsten Komponenten, schlüsseln auf, was du für einen soliden Internet-Zugang benötigst und mit welchen Tricks du die Reichweite deines Routers erhöhst.

TEXT: TOBIAS FRIEDRICH

Als vor Jahren die Piraten-Partei ein Novum in der deutschen Politiklandschaft darstellte, kursierte nach den ersten Wahlen mit ihrer Beteiligung der Kalauer, dass sich die technikaffinen Nachwuchskräfte mit folgendem Spruch beim Volk erkenntlich zeigen würden: Wir danken unserem WLAN. Im Jahr 2021 sind wohl die allermeisten für ein funktionierendes WLAN dankbar. Denn ob beruflich im Home-office, für den Betrieb zahlreicher Smart-Home-Komponenten oder für die mediale Freizeitgestaltung mit Streaming-Diensten, Spielekonsolen und anderen Geräten einzelner Familienmitglieder: Das WLAN muss funktionieren, damit wir uns mit der Welt digital verknüpfen. Doch mit immer neuen Standards, neuen Produkten, Systemen und Erweiterungsmöglichkeiten fällt es manchmal schwer, den Überblick zu behalten. Gehen wir also der Reihe nach durch, worauf es ankommt.

Der Anschluss

In Deutschland holst du dir WLAN zumeist per DSL-Anschluss oder über das TV-Kabelnetz ins Haus. Bei DSL kommt das Internet über die Telefonleitung, Geschwindigkeiten von bis zu 250 Mbit pro Sekunde sind damit möglich. In den meisten Gebieten mit Kabelanschluss erhältst du eine fast doppelt so schnelle Verbindung. Dies kannst du lediglich mit einer Glasfaserleitung übertreffen. Zwar

kommt Glasfaser genau genommen bereits jetzt in den meisten Leitungen vor, jedoch nur in einer Art Leitungsmixtur aus Glasfaser- und Kupfer- beziehungsweise Koaxialkabel. Breitband-Leitungen über einen reinen Glasfaseranschluss gibt es derzeit nur von der Telekom und wenigen anderen Anbietern, darunter EWE, M-Net und Deutsche Glasfaser, und das längst nicht flächendeckend.

Im Zweifel solltest du dich vor Abschluss eines Vertrages bei deinem Anbieter erkundigen, welche Art von Internet an deinem Wohnort verfügbar ist. Entscheidend ist hierbei, ob die Glasfaserleitung für deinen Haushalt im Verteilkasten endet und das letzte Stück dann doch über Kupferkabel läuft oder ob der Glasfaseranschluss bis zum Bürgersteig (Fiber-to-the-curb, FTTC), bis ins Gebäude (Fiber-to-the-building, FTTB) oder sogar bis in die Wohnung (Fiber-to-the-home, FTTH) reichen. Letzteres ist fast ausschließlich bei Neubauten der Fall.

Was muss dein Router können?

Zunächst solltest du darauf achten, den für dein Zuhause richtigen Router zu kaufen. Für einen Kabelanschluss musst du zum Beispiel ein explizit hierfür passendes Gerät erwerben. In der Regel sind diese aber von den Herstellern sichtbar gekennzeichnet. Die meisten Internetanbieter liefern dir allerdings kostenfrei oder für

AVM hat mit seinen verschiedenen Fritz! Box-Modellen für jede Konstellation das richtige Gerät.

kleines Geld ein eigenes Gerät, das du nach Ablauf der Vertragszeit wieder zurückgeben musst.

Ein moderner Router sollte möglichst viele Geräte mit schnellem, störungsfreiem WLAN versorgen, bis in die hintersten Winkel deiner Wohnung reichen und alle angeschlossenen Komponenten dabei auch noch absichern. Wie so oft im Leben gilt auch hier: Wer billig kauft, kauft doppelt. In diesem Artikel stellen wir euch zwei hochwertige Modelle vor, die dennoch keine Unsummen kosten.

Für Gamer:innen gibt es spezielle Router, die für genau diese Anforderungen konzipiert wurden. Sie verfügen über niedrigere Ping-Werte, das heißt, der Empfänger antwortet schneller auf Datenpakete und kann auch schneller neue zurückschicken. Zudem lassen sich mit Gaming-Routern bestimmte Geräte priorisieren, sodass bei Spielen eine





Foto: AVM

Unterbrechung zusätzlich ausgeschlossen wird.

Übrigens: Während wir vor Jahren noch mit Router und Modem operiert haben, ist mittlerweile das Modem, mit dem du nur ein einzelnes Gerät via Kabel mit dem Internet verbinden kannst, obsolet. Moderne Router verfügen über ein eingebautes Modem, zudem sind sie fähig, mehrere Geräte untereinander via WLAN (Funk) oder LAN (kabelgebunden) miteinander zu koppeln; sie fungieren also als eine Art Netzwerk.

Die Frequenzbänder

Vereinfacht gesagt, gibt es zwei Frequenzen, die von deinem Router genutzt werden: 5 Gigahertz und 2,4 Gigahertz. Zwei deshalb, weil die niedrigere Frequenz eine größere Reichweite ermöglicht, dafür aber langsamer ist, während du mit der höheren über eine schnellere Datengeschwindigkeit

verfügst, das Signal jedoch nur einen geringen Radius hat.

Moderne Router unterstützen in jedem Fall beide Standards. Der Vorteil: Bei hoher Auslastung können verschiedene Anwender:innen unterschiedliche Frequenzen wählen und sich so virtuell aus dem Weg gehen und Datenstaus und Internet-Engpässe vermeiden. Wichtig ist, dass du bei der Installation deines Routers beide Frequenzen einrichtest, um fortan die Wahl zu haben. Sollten in deinem Wohnhaus zahlreiche weitere Personen das Internet nutzen, kann es, wie auf einer Autobahn, zum Stau kommen. Für diesen Fall kannst du deinen Router zudem auf einen anderen, womöglich weniger ausgelasteten Kanal einstellen. Diese auch WLAN-Bänder genannten Kanäle sind Segmente der Frequenzen. In der 2,4 Gigahertz-Frequenz gibt es beispielsweise 14 unterschiedliche Kanäle.

#

Begriffe

DSL: Digital Subscriber Line (Digitaler Teilnehmer:innenanschluss)

WLAN: Wireless Local Area Network (Kabelloses lokales Funknetz)

MU-MIMO: Multi-User Multiple Input, Multiple Output (Technologie, welche die gleichzeitige Übertragung verschiedener Datenströme über mehrere Antennen am Router ermöglicht.)

MIMO-OFDM: Orthogonal Frequency Division Multiplexing (Von WiFi 6 unterstützte Technik, die bei zahlreichen zeitgleichen Netzwerkzugriffen Verzögerungen bei der Übertragung reduziert.)

Schon jetzt gibt es aufgrund der wachsenden Zahl der Geräte und des Nutzungsverhaltens dennoch Situationen, in denen dein WLAN lahmtr. Geplant sind daher neue Frequenzen im 1-Gigahertz- und im 7-Gigahertz-Bereich, wodurch künftig mehr Daten übertragen werden könnten.

WLAN 4, 5 oder 6?

Jede neue WLAN-Generation erhält eine neue Nummerierung und soll, in Verbindung mit einem entsprechenden Router, prinzipiell stets zu einer Verbesserung des Netzwerkes führen. Praktisch heißt dies, die Anwender:innen sollen einen schnelleren, zuverlässigeren, sichereren Zugang zum Internet für immer mehr angeschlossene Geräte erhalten.

Für einen Haushalt mit mehreren Mitgliedern und entsprechend vielen technischen Bestandteilen, solltest du einen Router wählen, der WiFi 5 (auch WLAN-ac genannt) oder WiFi 6 (WLAN-ax) unterstützt. Letzteres bietet im Optimalfall bis zu elf Gigabit Übertragung pro Sekunde und eine circa siebenunddreißig Prozent höhere Datenübertragung. Bei WiFi 5 sind es schon „nur“ noch 1,3 Gigabit pro Sekunde. Dazu sei gesagt, dass für eine durchschnittliche Beanspruchung WiFi 5 vollkommen ausreicht.

WLAN: Entwicklung, Standard, Allianz

Hinter dem etwas verschrobenen Kürzel **IEEE 802.11ax**, das sich liest, als sei jemand auf der Tastatur eingeschlafen, verbirgt sich schlicht der neueste WLAN-Standard, **WiFi 6**. Die Entwicklung jedes Standards findet beim **IEEE (Institute of Electrical and Electronics Engineers)** statt, einem weltweiten Berufsverband von Ingenieur:innen, Techniker:innen und Wissenschaftler:innen. Darauf basierend vergibt die sogenannte **WiFi-Allianz** die gebräuchlichen und weit leichter über die Lippen gehenden Einstufungen wie **WiFi 4, 5 oder 6**. Die Allianz wiederum ist ein Konsortium aus über **300 Unternehmen**, unter anderem auch **Apple, Microsoft, Nokia, LG oder Sony**. Sie zertifiziert alle auf den Markt kommenden, kompatiblen Router, die mit dem **WiFi-Logo** kenntlich gemacht werden.

Maximale Bandbreiten der einzelnen WiFi-Generationen



Um stets den besten WiFi-Standard zu nutzen, brauchst du nichts zu unternehmen, ein neuer löst einfach den alten ab. Und alle Geräte profitieren davon, denn der Standard ist abwärtskompatibel. Für die höchste Internet-Geschwindigkeit solltest du bei deinem Anbieter zunächst eine entsprechende Leistung gebucht haben. In der Regel bewegt sich diese zwischen 100 oder 200 Mbit pro Sekunde.

Neben Geschwindigkeitsvorteilen bringt jeder neue WiFi-Standard auch in Sachen Sicherheit Verbesserungen. Bei der Verschlüsselung der Funkverbindung kommt bei WiFi 6 zum Beispiel WPA3 zum Einsatz, ein Verfahren, das es Böswilligen wesentlich schwieriger macht, die Verschlüsselung zu knacken.

Der richtige Router

Natürlich könnten wir zahlreiche Geräte vorstellen, die alle solide ihren Dienst verrichten. Stellvertretend haben wir uns für zwei Produktkombinationen von Herstellern entschieden, die immer wieder in den Router-Bestenlisten auftauchen. Der bekannteste Router ist vermutlich die Fritz! Box von AVM, einem Unternehmen, das für nahezu jede häusliche Konstellation eine Gerätelösung parat hat.

In unserem Fall haben wir eine Fritz! Box 6591 Cable (300 Euro) im Zusammenspiel mit einem Fritz! Powerline 1260E-Set (140 Euro) getestet. Während die Geschwindigkeit stets von dem Zusammenspiel von Anbieter, Router und Nutzung abhängig ist, konnten wir

dennoch eine schnellere Reaktionszeit zu dem vorher zum Einsatz gekommenen Vodafone-Router feststellen. Auch die Stabilität war deutlich besser. Denn während das Vodafone-Gerät immer wieder mal defekt war und ausgetauscht werden musste, hielt der Fritz! Router tadellos. Auch eine Auslastung mit diversen Geräten, die zur selben Zeit streamen, große Datenmengen laden und mit aufwendigen Onlinespielen beschäftigt sind, stellte für das Gerät keine Schwierigkeit dar.

Reichweite erhöhen: Repeater, Extender, Mesh

Repeater und Extender erhöhen den Radius der WLAN-Reichweite, halbieren dafür aber die Datenübertragungsrate und verlangsamen so die Netzwerkgeschwindigkeit. Bei dem Fritz! Powerline 1260E-Set (140 Euro) – und auch bei anderen sogenannten PowerLAN-Geräten – werden die Daten zusätzlich über die Stromleitung übertragen. Voraussetzung sind allerdings Stromkreise mit drei Adern; bei älteren Leitungen sind es oft nur zwei. Beim PowerLAN

Das Fritz! Powerline 1260E-Set von AVM sorgt für erweitertes WLAN über die Stromleitung.

Alle namhaften Hersteller bieten Mesh-Netzwerke an, so auch Asus mit seinem Gerät ZenWifi XD6.



empfähmt ein Adapter das Signal über den häuslichen Strom, und von jenem Adapter kannst du per LAN-Kabel selbst an einem entfernten Ort des Hauses oder der Wohnung besser und störungsfreier mit dem Internet verbunden werden.

Wer möglichst kein zusätzliches Kabel verwenden möchte, sollte ein Mesh-Netzwerk ausprobieren, wie es unter anderem Asus mit dem ZenWifi XD6 (450 Euro) anbietet. Dies kommuniziert auf drei Frequenzbändern, einem sogenannten Tri-Band. Der interne Austausch wird auf einem eigenen Frequenzband vollzogen, sodass du weiterhin jene mit 2,4 Gigahertz und 5 Gigahertz nutzen kannst, zusätzlich aber eine stabile Geschwindigkeit und so gut wie keine Einbrüche in der Leistung hast. Auch die Fläche, die du mit einem Mesh-Netzwerk abdecken kannst, ist meist größer als mit Repeatern. Das Mesh-Netzwerk kannst du zudem jederzeit mit einem zusätzlichen Router erweitern, der sich nahtlos einfügen lässt.

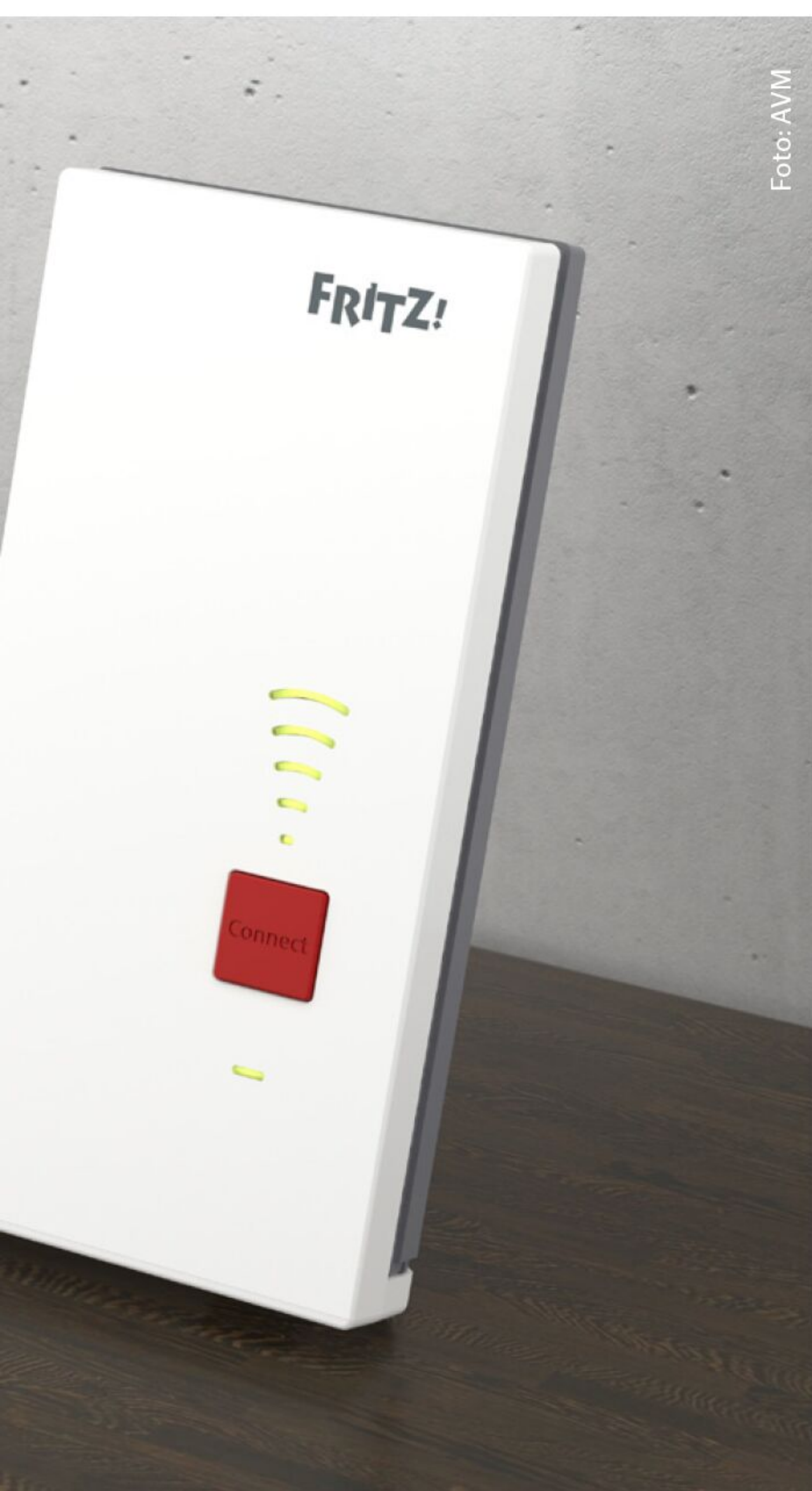


Foto:AVM

WLAN-Signal mit Apps messen

Willst du möglichst schnell und einfach herausfinden, wie gut dein WLAN-Signal ist, helfen dir auch diverse Apps. Speedcheck (gratis + In-App-Kauf 8 Euro/Jahr), Speed Test (gratis + In-App Kauf 8,50 Euro/Jahr) sowie die einfachere Variante von AVM, die Fritz! App WLAN (gratis) zeigen dir sekundenschnell, wie es um deine Upload- und Download-Geschwindigkeit (auch Upstream und Downstream genannt) bestellt ist und geben dir im Falle von Speed Test noch zusätzliche Werkzeuge wie Pingtests, Netzwerkdiagnosen oder Auskünfte über Leistung und Latenz an die Hand. Mit der Fritz! App findest du zudem den besten Standort für Router und Repeater und kannst Besucher:innen einen Gast-Zugang zum WLAN per QR-Code ermöglichen.

Meine Erfahrung mit Anbietern

Ich habe in den letzten Jahren mit den beiden Platzhirschen, also sowohl mit der Telekom als auch mit Vodafone, meine Erfahrungen gemacht und aus diesem überschaubaren Rennen ist die Telekom als eindeutige Siegerin hervorgegangen. Dabei zählte für mich nicht nur die Zuverlässigkeit und die Qualität des WLAN als Kriterium.

Zusammengefasst lag das Bonner Unternehmen in allen Belangen vor dem Britischen. Das WLAN war stabiler, der Service besser, die Abwicklung und Administration deutlich seriöser. Es ist kein Zufall, dass, wenn du bei Google den Begriff Vodafone eingibst, als erster Treffer „Vodafone Störung“ erscheint.

Der größte Unterschied zwischen beiden Anbietern ist, dass du bei Vodafone deinen Anschluss mit anderen in deinem häuslichen Umfeld teilst, während du bei der Telekom eine eigene Leitung erhältst.



6 Tipps für mehr WLAN-Reichweite

- 1 Standort:** Eine Faustregel besagt, dass der Router immer an einem möglichst hoch gelegenen Ort platziert werden sollte, also zum Beispiel auf einem Schrank. Mithilfe von Apps kannst du den besten Standort und den besten Raum für dein Gerät ermitteln.
- 2 Störquellen:** So seltsam es auch klingt: Zu den Hindernissen, die deinen WLAN-Empfang stören können, zählen nicht nur geschlossene Türen, Beton oder Glaswände. Auch Gegenstände mit hohem Metallanteil oder gar oft gegossene Pflanzen und nasse Wände sind schädlich, da die Frequenz 2,4 Gigahertz die Resonanzfrequenz von Wasser ist.
- 3 Router:** Routerjahre sind ein wenig wie Hundejahre: Die Zeit scheint für sie schneller zu vergehen, entsprechend rasch müssen sie (manchmal) ausgetauscht und den technischen Gegebenheiten angepasst werden. Für die beste Übertragungsrate solltest du möglichst einen WLAN-ac-Router oder einen WLAN-ax-Router (WiFi 5 oder 6) zu Hause haben.
- 4 Funkkanal:** Inzwischen kannst du für alle neueren Geräte wählen, ob du sie mit dem 2,4 Gigahertz-Band verbindest oder mit dem 5 Gigahertz-Band. Für eine variable Verbindung empfehlen wir eine Aufteilung deiner Geräte auf beide Bänder.
- 5 Repeater:** Repeater, Extender oder Powerline-Adapter sind valide Mittel, die Reichweite deines WLAN-Signals zu erhöhen, eine Garantie dafür sind sie nicht. Und Achtung: Ein Repeater steigert die Reichweite, drosselt aber die Übertragungsgeschwindigkeit.
- 6 Firmware:** Damit du dich nicht andauernd fragen musst, ob auf deinem Router die neueste Firmware läuft, solltest du in den Einstellungen das automatische Update wählen. Die aktuellste Version kann Einfluss auf die Reichweite des Routers, aber auch auf die Sicherheit haben.

Interview mit Sebastian Schwab, Geschäftsführer SconsultIT

»Bereits vor Jahrzehnten wurden durch politische Entscheidungen die Weichen anders gestellt, sodass wir heute in kürzerer Zeit einiges aufzuholen haben.« **SEBASTIAN SCHWAB**



Mit seiner Beratungsfirma SconsultIT betreut und berät Sebastian Schwab Firmen beim Aufbau und der Administration von Systemen und Netzwerken.

Herr Schwab, wie modern oder rückschrittlich ist die WLAN-Versorgung und Abdeckung in Deutschland?

Die Versorgung der Haushalte mit Breitband-Internet wird zwar stets vorangetrieben, im Vergleich zu anderen Staaten sind wir in Deutschland aber weit im Hintertreffen. Dabei ist der Spagat zu schaffen, dass bei der Versorgung der Haushalte einerseits auf neuere Glasfaser-Technologie umgestellt und gleichzeitig die vor allem in ländlichen Gebieten phasenweise sehr schlecht ausgebaute Grundversorgung massiv verbessert werden muss. Bereits vor Jahrzehnten wurden durch politische Entscheidungen die Weichen anders gestellt, sodass wir heute in kürzerer Zeit einiges aufzuholen haben, was aber im Vergleich zu früher mit deutlich höheren Investitionen verbunden ist.

Wem würden Sie welche Anschlussart empfehlen: DSL, Kabel, Glasfaser, LTE?

Für gelegentliches Browsen im Internet, gepaart mit dem Lesen von E-Mails reicht ein kostengünstiger Anschluss mit niedriger Bandbreite auf Basis von LTE schon aus. Wir sollten aber auf jeden Fall den Verbrauch des monatlichen Datenvolumens im Blick haben, denn dieses ist in Mobilfunk-Tarifen meist begrenzt. Sollten zusätzlich Dienste wie Festnetz-Telefonie in Anspruch genommen werden, empfiehlt sich die Wahl eines Anschlusses auf Basis von DSL beziehungs-

weise Kabel. Für den Fall, dass auch Online-Gaming betrieben wird, führt derzeit kein Weg an einem hochpreisigen V-DSL-Anschluss vorbei. Denn bei diesem Einsatzzweck spielt die Latenzzeit eine tragende Rolle. Die Anbieter offerieren hier meist, die alles entscheidende Ping-Zeit durch hinzubuchen von Zusatzpaketen auf ein Maß zu reduzieren, das ein flüssiges Spielen in Echtzeit zufriedenstellend ermöglicht. Aufgrund der derzeit noch geringen Verfügbarkeit von Internetanschlüssen mittels Glasfaser ist eine Verwendung dieses Anschluss-Typs in allen Belangen zwar wünschenswert, aber meist mit großem Abstand die teuerste Alternative.

Worauf sollten Verbraucher:innen bei der Wahl ihres Routers achten?

Zunächst müssen wir sagen, dass die von den Netzbetreibern zur Verfügung gestellten Router nicht generell schlechter sind als die Geräte, die wir im Handel erwerben können. Betreiberabhängig sind diese aber häufig in der Konfigurierbarkeit eingeschränkt, gelegentlich werden auch noch Produkte der Vorgängergeneration angeboten. Hinzu kommt, dass diese Router meist gemietet werden müssen, sich der Kauf eines eigenen Routers aktueller Generation innerhalb der Mindestvertragslaufzeit bereits wieder amortisiert. Aktuelle Geräte namhafter Hersteller sind bereits kurz nach ihrem Erscheinen durch umfangrei-

che Rabattaktionen gut und günstig zu erwerben. Im Endeffekt entscheidet das eigene Wissen: Wie gut bist du in der Lage, derartige Geräte zu konfigurieren? Der zweite wichtige Aspekt, den jede:r für sich vorab klären sollte: Welche Funktionen des Routers finden hauptsächlich Anwendung?

Ganz ehrlich: Was bringen Repeater, Extender oder ein Mesh-Netz?

Mit den zusätzlichen Access Points können zum Beispiel Außenbereiche mit dem WLAN oder sich im Funk Schatten befindliche Bereiche der Wohnung mit einer besseren Signalstärke versorgt werden. Ein weiterer Nebeneffekt kann nach entsprechender Konfiguration sein, dass beim Ausfall eines Access Points die Endgeräte automatisch auf einen anderen Zugangspunkt wechseln können und diese dabei die schnellstmögliche Verbindung aufbauen. Die Geräte können also durchaus sinnvoll sein.

WiFi 4, 5 oder 6 sind für Konsument:innen erst mal nur abstrakte Namensschilder. Ab wann gibt es einen spürbaren Unterschied?

Die Bandbreite des eigenen WLAN ist nicht der Flaschenhals bei der Internet-Geschwindigkeit. Hier kommt eher die durch den Internetprovider zur Verfügung gestellte Bandbreite zum Tragen. Bei WiFi 6 teilen sich acht Kanäle die maximale Bandbreite. Diese Neuerung entfaltet sich allerdings erst in hoch

ausgelasteten WLANs, über welche gleichzeitig mehrere Streaming-Dienste oder zeitgleich auch Online-Games der Spiele-Konsolen-Hersteller genutzt werden sollen.

Was bringen Router, die MU-MIMO-fähig sind?

Die MU-MIMO-Technologie – allgemein auch unter AC-WLAN oder AC Wave 2 bekannt – ermöglicht es einem WLAN-Router, gleichzeitig mit mehreren Geräten zu kommunizieren. In Zeiten von Smart-Home steigt die Anzahl der WLAN-Geräte stetig an. MU-MIMO sorgt für eine erhebliche Verbesserung des zur Verfügung stehenden WLAN-Netzwerkes. Router, welche nur die WLAN-Standards A (WLAN 802.11a), B (WLAN 802.11b), G (WLAN 802.11g) und N (WLAN 802.11n) unterstützen, sind hier außen vor. Nur AC-WLAN-Router oder passende Access Points unterstützen die neue Technologie. Bei den angebundenen Endgeräten macht es fast keinen Unterschied, ob diese den neuen Standard schon selbst unterstützen. Diese profitieren in den meisten Fällen schon davon, wenn ein Router/Access Point auf Basis des neuen Standards AC Wave 2 arbeitet.

Fast geschenkt!

Hol dir das Probe-Abo und du erhältst eine Ausgabe als E-Paper für nur 1 Euro.



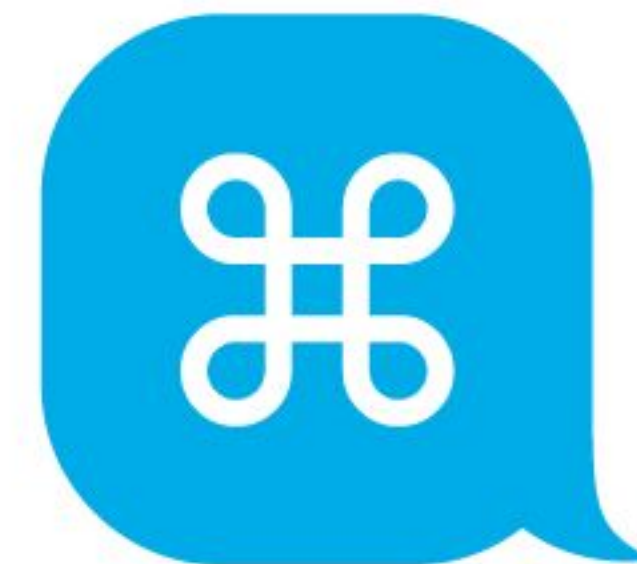
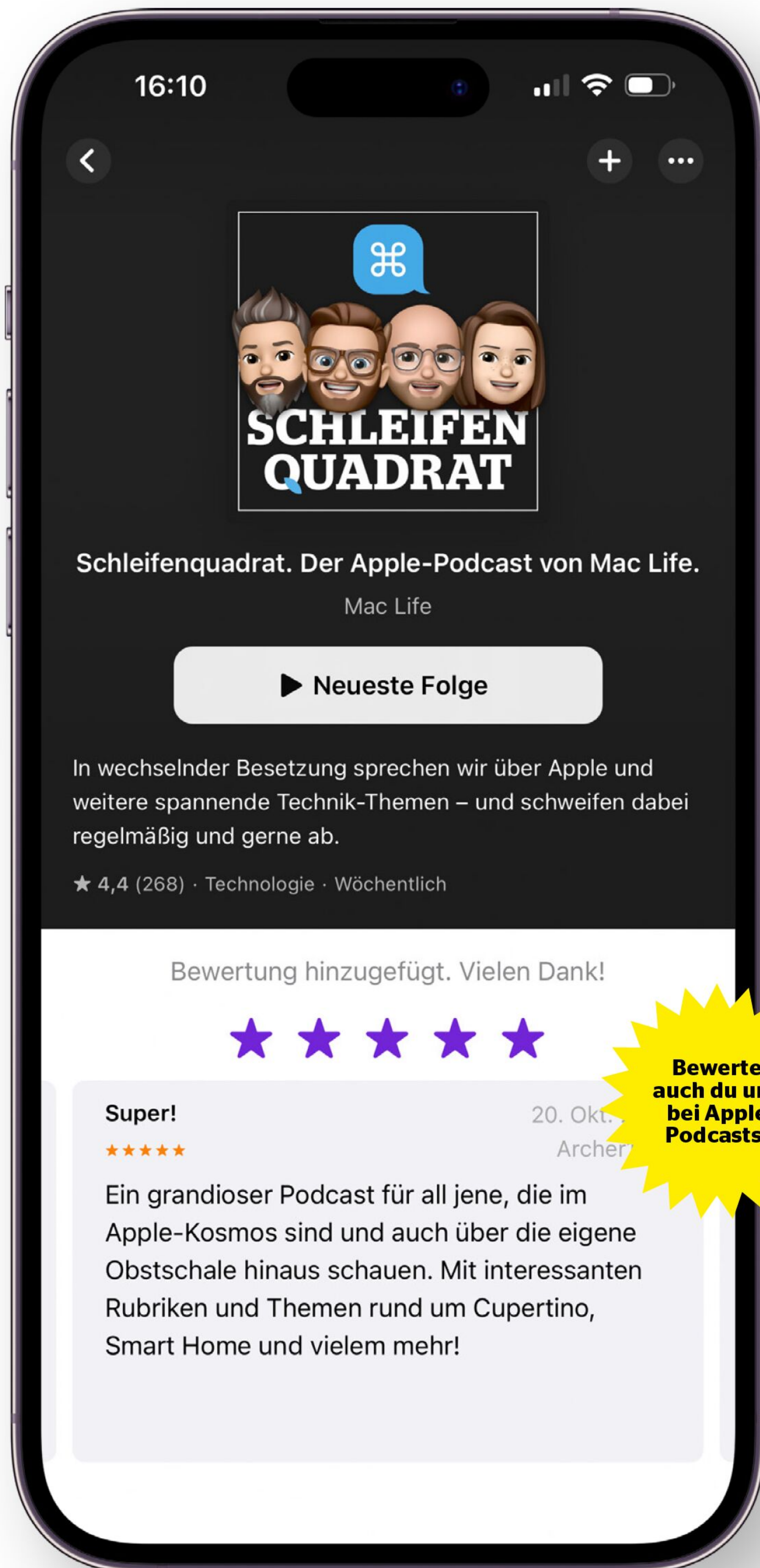
Hintergrundbild: t_trifonoff/iStock / Getty Images Plus

Jetzt bestellen unter
www.maclife.de/nur1euro



Schleifenquadrat

Der Apple-Podcast von Mac Life



**Jetzt gratis
abonnieren!**

Du liest Mac Life. Vielleicht sogar regelmäßig. Aber hörst du uns auch schon? Wir, die Köpfe hinter Mac Life, diskutieren im „Schleifenquadrat“-Podcast jeden Freitag über Neuigkeiten aus dem Apple-Universum, Fundstücke, Lieblingsgeräte – und wagen dabei auch immer wieder einen Blick über den Tellerrand hinaus. Regelmäßig um spannende Gäste aus der Szene bereichert, ist Schleifenquadrat die perfekte Ergänzung zu Magazin und Website – Mac Life für die Ohren!



Jetzt neu: Hoodies,
Shirts und mehr unter
maclife.de/shirtshop