

Kapitel 2

Der erste Start mit Windows 10

Fahren Sie Ihren Windows 10-Computer das erste Mal hoch, sind zunächst einige Angaben erforderlich, bevor Sie mit der Arbeit am PC beginnen können. Dieses Kapitel führt Sie Schritt für Schritt durch die Ersteinrichtung.

Wer einen neuen Windows 10-Computer oder ein frisch installiertes Windows 10 das erste Mal startet, muss sich zunächst durch eine Fülle an Dialogen arbeiten. Manche der Fragen, die es dabei zu beantworten gilt, sind selbsterklärend, etwa wenn es um die Herstellung einer Internetverbindung geht. Bei anderen sollte man doch kurz überlegen, bevor man vor schnell eine der vorgegebenen Optionen auswählt. Dies betrifft vor allem das Thema Datenschutz, denn mit so manch einer Einstellung gibt der Anwender mehr über sich preis, als ihm womöglich lieb ist. Eine zentrale Rolle bei der Ersteinrichtung spielt auch die Entscheidung, welche Art von Benutzerkonto man wählt. Darf es ein Microsoft-Konto sein, das sich – überspitzt formuliert – munter mit Microsoft austauscht? Oder doch lieber das bereits aus früheren Windows-Versionen bekannte lokale Benutzerkonto, womit man aber wiederum auf zahlreiche neue Funktionen unter Windows 10 verzichten muss? Welche Vor- und Nachteile beide Varianten mit sich bringen, wird gleich im ersten Abschnitt dieses Kapitels beleuchtet.

In Abschnitt 2.2 begleite ich Sie Schritt für Schritt durch die erste Einrichtung des Windows 10-Computers, in der das eben erwähnte erste Benutzerkonto angelegt wird und einige wichtige Einstellungen vorgenommen werden. Einige dieser Dialoge bekommen Sie auch zu Gesicht, wenn Sie sich das erste Mal an einem neu angelegten Benutzerkonto anmelden.

Ist die Ersteinrichtung erfolgreich abgeschlossen, ist der Blick frei auf den Desktop von Windows 10. Wer gerade erst von Windows 7 auf Windows 10 umgestiegen ist, dem fällt die Orientierung zunächst vielleicht etwas schwer. Aus diesem Grund werden in Abschnitt 2.3 die wichtigsten Elemente der Benutzeroberfläche kurz vorgestellt.

2.1 Die Qual der Wahl: Microsoft-Konto oder lokales Benutzerkonto?

Im Rahmen der Ersteinrichtung des Windows 10-Computers wird zugleich das erste Benutzerkonto angelegt. Zur Auswahl stehen das von Microsoft präferierte Microsoft-Konto und das von einigen Anwendern weiterhin bevorzugte lokale Benutzerkonto. Was ein lokales Benutzerkonto ist, lässt sich schnell erklären: Wie der Name bereits impliziert, ist ein lokales Benutzerkonto lokal beschränkt. Es gilt nur auf dem Computer, auf dem es eingerichtet wird.

Damit stehen dem Anwender auch nur die lokalen Ressourcen zur Verfügung. Ein lokales Benutzerkonto wird gerne als *Offlinekonto* bezeichnet, während man beim Microsoft-Konto von einem *Onlinekonto* spricht. Denn für die Verwendung eines Microsoft-Kontos spielt die Internetverbindung eine große Rolle.

Wirklich neu ist das Microsoft-Konto nicht. Es existiert bereits seit mehreren Jahren, erhielt im Laufe der Zeit aber immer wieder einen neuen Namen. Manch einem Leser ist vielleicht eine der älteren Bezeichnungen wie *Microsoft Passwort*, *.NET Passwort* oder auch *Windows Live ID* geläufig. Der Name *Microsoft-Konto* gilt seit Windows 8. Ein Microsoft-Konto ermöglicht es u. a., sich bei Microsoft-Diensten wie Skype, Outlook und in Zeiten der Clouds natürlich OneDrive anzumelden. Seit Windows 8 lässt sich das Konto aber auch für den Login bei Windows selbst nutzen.

Meldet sich ein Anwender mit einem Microsoft-Konto am Windows 10-Computer an, ist er damit automatisch auch bei den in Windows 10 integrierten Diensten und Apps eingeloggt. Die Windows-Anmeldung fungiert somit als sogenanntes *Single Sign-on*, also als einmalige Anmeldung, der Login bei den einzelnen Diensten entfällt hierdurch. Dies ist aber nicht der einzige Pluspunkt eines Microsoft-Kontos.

Mit einem Microsoft-Konto können Sie sich an verschiedenen Windows-Geräten anmelden. Damit kommen Sie in den Genuss eines weiteren Vorteils, nämlich der Synchronisation: Wenn Sie es wünschen, lässt sich eine Vielzahl an Einstellungen auf allen Windows-Geräten synchronisieren, auf denen Sie sich mit dem gleichen Microsoft-Konto anmelden. Auf diese Weise steht Ihnen z. B. Ihr Aktivitätsverlauf, der mit OneDrive synchronisierte Inhalt der Zwischenablage, alle in OneDrive abgelegten Daten und einiges mehr auf allen Windows-Geräten zur Verfügung. Auch die über den Microsoft Store erworbenen Apps lassen sich auf all diesen Geräten installieren, ohne erneut Geld ausgeben zu müssen.

Um im Microsoft Store einkaufen zu können, ist ein Microsoft-Konto übrigens Pflicht. Einige andere Apps, wie etwa die Sprachassistentin Cortana, erfordern ebenfalls ein Microsoft-Konto. Wer nun befürchtet, dass diese Apps nicht zur Verfügung stehen, wenn ein lokales Benutzerkonto verwendet wird, sei beruhigt. Die meisten Apps unter Windows 10 benötigen gar kein Microsoft-Konto. Diejenigen, die sich ausschließlich mit einem Microsoft-Konto nutzen lassen, erlauben meist eine gezielte Anmeldung, ohne sich deshalb bei Windows selbst mit dem Konto anmelden zu müssen.

Ein Microsoft-Konto bietet dem Anwender zweifelsohne viele Vorteile. Doch auch Microsoft selbst wird belohnt, denn das Unternehmen gelangt auf diese Weise an viele Informationen über Sie. Dies beginnt bei den Standorten, an denen Sie sich mit Ihrem Windows 10-Gerät aufhalten, setzt sich bei den besuchten Websites fort und hört mit den von Ihnen getätigten Einkäufen im Store noch lange nicht auf. Den gesammelten Daten lässt sich durch das Microsoft-Konto quasi ein Gesicht zuordnen. Solche Daten sind heutzutage viel wert, denn sie lassen sich gewinnbringend weiterverarbeiten, z. B. als individualisierte Werbung. Mit dieser

Strategie steht Microsoft selbstredend nicht allein da, denn auch Google, Apple und Konsorten agieren so.

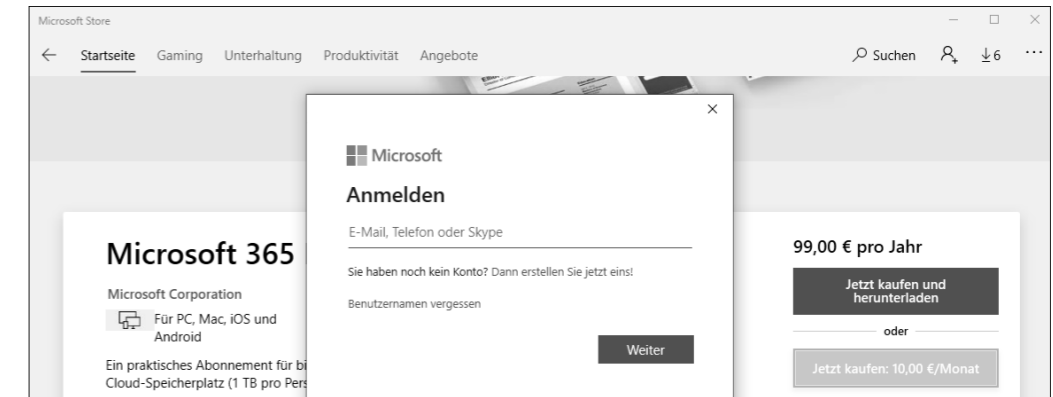


Abbildung 2.1 Manche Apps, wie hier der Microsoft Store, erfordern die Anmeldung mit einem Microsoft-Konto.

Die Unternehmen versuchen deshalb mit immer trickreicheren Methoden, den Anwender zur Nutzung ihrer Konten zu überreden, manchmal auch gar zu zwingen. Auch Microsoft stellt hier keine Ausnahme dar. War es früher unter Windows 10 Home bei der Ersteinrichtung des Computers immer noch möglich, ein lokales Benutzerkonto statt des Microsoft-Kontos zu wählen, wird seit Februar 2020 nur noch das Microsoft-Konto angeboten. Für Windows 10 Pro und Enterprise gilt dies nicht. Wie lange dem Anwender hier noch eine Auswahlmöglichkeit bleibt, wird die Zukunft zeigen. Für diejenigen, die – trotz aller Vorteile eines Microsoft-Kontos – bei der Ersteinrichtung weiterhin ein lokales Benutzerkonto wählen möchten, steht eine Hintertür offen, wie im folgenden Abschnitt gezeigt wird. Das Microsoft-Konto kommt in diesem Abschnitt aber selbstverständlich auch nicht zu kurz. Denn beide Kontenarten haben ihre Berechtigung, die Qual der Wahl liegt also beim Anwender.

2.2 Die ersten Schritte in Windows 10

Nach dem allerersten Start des Betriebssystems folgt immer die Ersteinrichtung, ganz egal, ob Sie selbst Windows 10 auf einem älteren Gerät neu installiert haben oder der Computerhersteller dies auf dem Neugerät erledigt hat. In den Dialogen, die es dabei abzuarbeiten gilt, werden diverse Windows-Einstellungen vorgenommen, und das erste Benutzerkonto wird eingerichtet. Ein wichtiger Bestandteil stellen auch die Privatsphäre-Einstellungen dar. Für diesen Bereich wurde Microsoft seit den Anfängen von Windows 10 stark kritisiert. Vor allem die Expresseinstellungen, mit denen man in den ersten Versionen von Windows 10 mit nur einem Mausklick Microsoft einen Freifahrtschein zum Datensammeln erstellte, sorgten zu Recht für großen Unmut. Hier hat sich seitdem doch einiges geändert, denn mittlerweile

entscheiden Sie, in welchem Umfang welche Daten erfasst werden dürfen. Ganz verhindern, das sei vorweg bereits gesagt, lässt sich das Sammeln von Informationen allerdings nicht.

Die folgende Beschreibung basiert auf einer Ersteinrichtung von Windows 10 Oktober 2020 Update (auch *Windows 10 20H2* genannt). Sollten Sie mit einer anderen Version arbeiten, kann es sein, dass sich der ein oder andere Unterschied in der Abfolge ergibt. Die Anleitung beschreibt nicht die Installation von Windows 10, sondern lediglich die Schritte, die anschließend nach einem Neustart anstehen. Dem letzten Part dieser Schritte begegnen Sie auch dann, wenn Sie sich das erste Mal an einem neu angelegten Benutzerkonto anmelden. Wie das Hinzufügen von Benutzerkonten funktioniert, erfahren Sie in Kapitel 26, »Windows 10 sicher mit mehreren Benutzern nutzen«. Hinweise zur Installation von Windows 10 erhalten Sie in Kapitel 33, »Windows 10 installieren«.

Spracheinstellungen

Starten Sie ein neues Windows 10-System das erste Mal, müssen Sie als Erstes die Region festlegen. In den meisten Fällen dürfte die Voreinstellung DEUTSCHLAND passen, sodass Sie sofort mit JA fortfahren können. Dies gilt auch für die folgende Frage nach dem Tastaturlayout. Das als Nächstes angebotene zweite Tastaturlayout ist dann sinnvoll, wenn Sie häufig Texte in einer anderen Sprache tippen müssen, für die das zuerst gewählte Tastaturlayout nicht geeignet ist. Benötigen Sie das zweite Tastaturlayout nicht, überspringen Sie diesen Schritt.

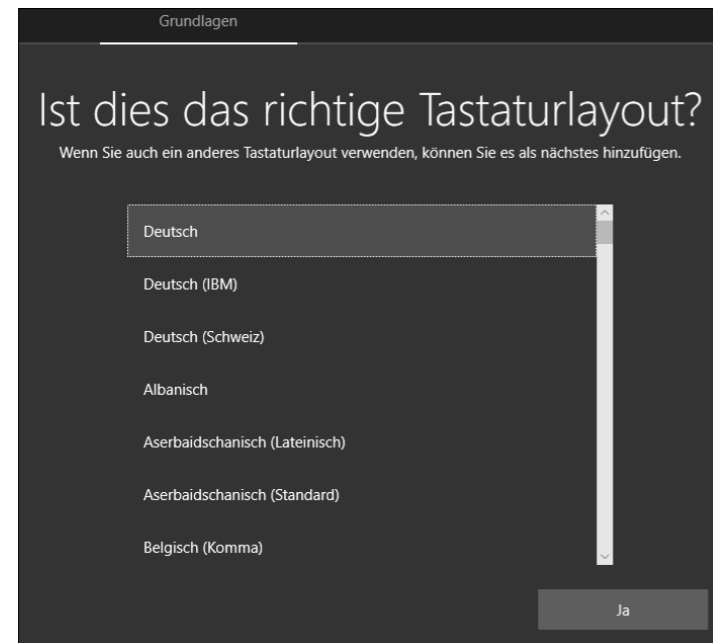


Abbildung 2.2 Wählen Sie für das Tastaturlayout die gewünschte Spracheinstellung aus.

Internetverbindung

Verfügt Ihr Computer über einen WLAN-Adapter, bietet Ihnen Windows als Nächstes an, eine Internetverbindung per WLAN herzustellen. Falls Sie das Gerät bereits per Ethernet-Kabel mit dem Router verbunden haben, erscheint der entsprechende Dialog nicht. Bevor Sie die WLAN-Verbindung einrichten, sollten Sie kurz innehalten. Denn genau an dieser Stelle verbirgt sich ein ganz einfacher Trick, falls Sie für das erste Benutzerkonto ein lokales Benutzerkonto statt des Microsoft-Kontos wählen möchten. Für die Einrichtung des Microsoft-Kontos wird eine Internetverbindung benötigt. Existiert diese nicht, besteht zwangsläufig nur die Möglichkeit, ein lokales Konto hinzuzufügen. Unter Windows 10 Home stellt dieser Trick mittlerweile den einzigen Weg dar, während der Ersteinrichtung ein lokales Benutzerkonto einzurichten. In den Editionen Pro und Enterprise lässt sich zurzeit (Stand Oktober 2020) auch bei bestehender Internetverbindung im Dialog KONTO HINZUFÜGEN noch ein OFFLINEKONTO auswählen (siehe Abbildung 2.4).

Für die Anmeldung mit einem Microsoft-Konto markieren Sie Ihr WLAN in der Liste der verfügbaren Funknetze, geben den Netzwerkschlüssel ein und klicken auf VERBINDEN. Für ein lokales Konto verzichten Sie auf diese Angaben und klicken stattdessen auf ICH HABE KEIN INTERNET. Microsoft versucht Sie anschließend nochmals von den Vorzügen einer Internetverbindung und somit der Anmeldung mit einem Microsoft-Konto zu überzeugen, was Sie mit einem Klick auf WEITER MIT EINGESCHRÄNKTEM SETUP ablehnen können. Sollten Sie den Computer bereits per Netzkabel mit dem Router verbunden haben, ziehen Sie das Kabel einfach wieder ab. Sobald die Ersteinrichtung erfolgreich abgeschlossen ist, können Sie die Internetverbindung selbstverständlich sofort herstellen.

Persönliche Verwendung oder für eine Organisation?

Falls Sie Windows 10 Pro von einem Installationsmedium neu installieren, werden Sie im Verlauf der Ersteinrichtung gefragt, ob Sie Ihr Gerät zur persönlichen Verwendung einrichten oder für eine Organisation.

Für den heimischen Gebrauch bzw. wenn Ihr Computer in eine Windows-Domäne eingebunden wird, wählen Sie die persönliche Verwendung.

Wird Ihr Computer hingegen von einer Organisation (z. B. ein größeres Unternehmen, Universität oder auch Schule) verwaltet, entscheiden Sie sich für die Organisation. In diesem Fall erhalten Sie anschließend die Möglichkeit, sich mit Ihrem *Azure Active Directory-Konto* anzumelden und die von Ihrer Organisation genutzten Azure Active Directory-Dienste, wie etwa Microsoft 365, einzurichten.

Ein Geschäfts- oder Schulkonto lässt sich später auch in der Einstellungen-App in der Kategorie KONTEN • AUF ARBEITS- ODER SCHULKONTEN ZUGREIFEN hinzufügen. Weitere Informationen zu Microsofts Azure Active Directory erhalten Sie unter der Webadresse <https://azure.microsoft.com/de-de/services/active-directory>.

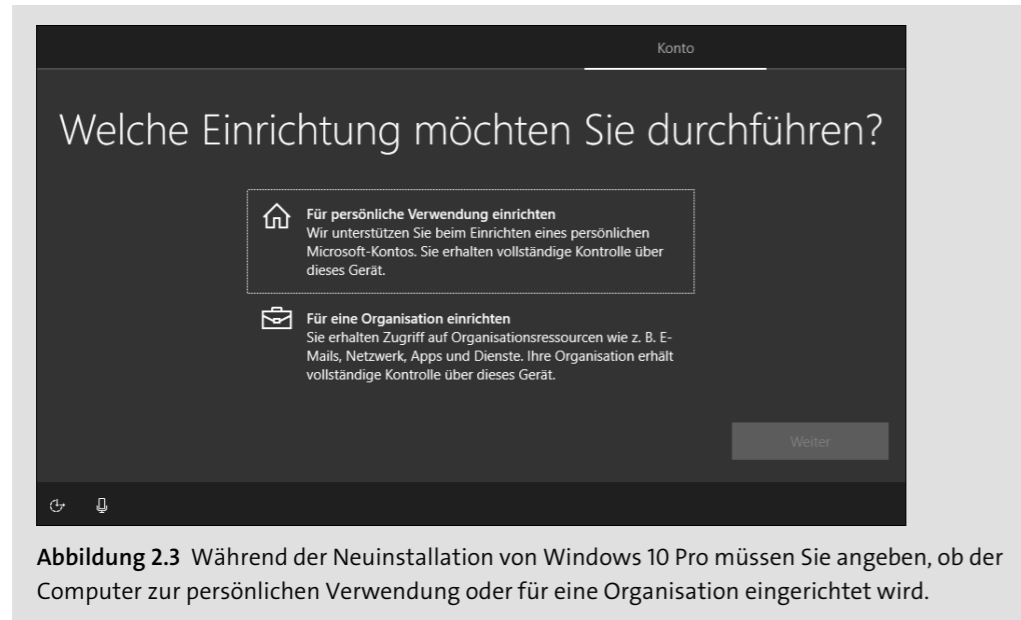


Abbildung 2.3 Während der Neuinstallation von Windows 10 Pro müssen Sie angeben, ob der Computer zur persönlichen Verwendung oder für eine Organisation eingerichtet wird.

Benutzerkonto hinzufügen

Nun geht es an die Einrichtung des bereits häufig erwähnten ersten Benutzerkontos. Sehen wir uns zunächst das Vorgehen im Falle eines Microsoft-Kontos an: Falls Sie noch kein Microsoft-Konto besitzen, können Sie dies im Dialog **KONTO HINZUFÜGEN** über die Schaltfläche **KONTO ERSTELLEN** nachholen. Die anschließend notwendigen Schritte ähneln denen in Abschnitt 26.3.1, »Microsoft-Konto hinzufügen«, vorgestellten, wobei die Einrichtung des Microsoft-Kontos dort über die Webadresse *account.microsoft.com* erfolgt. Falls Sie einen anderen Computer mit Internetanschluss zur Verfügung haben, empfehle ich Ihnen, den Weg zur Anlegung des Kontos über die Webadresse zu wählen. Sind Sie bereits im Besitz eines Microsoft-Kontos, geben Sie im Dialog **KONTO HINZUFÜGEN** die E-Mail-Adresse des Microsoft-Kontos ein. Nach einem Klick auf **WEITER** werden Sie zur Angabe des Kennwortes aufgefordert. Ein kleiner Hinweis am Rande: Über den Pfeil in der linken oberen Ecke eines jeden Dialogs können Sie immer wieder zum vorherigen Dialog zurückkehren.

Das Kennwort Ihres Microsoft-Kontos sollte im Idealfall möglichst komplex und lang sein. Ein solches Kennwort kann man sich aber meist nur schwer merken. Um Ihnen die Anmeldung am Computer zu erleichtern, werden Sie deshalb im nächsten Dialog dazu aufgefordert, eine PIN zu erstellen. Diese PIN gilt nur auf diesem Computer und wird nicht über das Internet übertragen. Sie ermöglicht Ihnen außerdem, sich auch dann mit Ihrem Microsoft-Konto am Computer anzumelden, wenn dieser nicht mit dem Internet verbunden ist. Die Anmeldung per Kennwort erfordert hingegen eine Internetverbindung. Nach einem Klick auf **PIN ERSTELLEN** geben Sie einen Zahlencode ein und wiederholen diesen im folgenden Feld. Mit **OK** schließen Sie die Einrichtung des Microsoft-Kontos ab. Manchmal kommt es an

dieser Stelle zu einer Fehlermeldung, in der Sie darauf hingewiesen werden, dass die PIN nicht erzeugt werden konnte. Wer nicht einen neuen Versuch starten möchte, überspringt diesen Schritt einfach. In Abschnitt 3.4 lernen Sie einige weitere Anmeldeoptionen kennen, zu der auch die Erstellung einer PIN gehört. Sie können die Einrichtung also auch gut auf später verschieben.

Wer statt des Microsoft-Kontos lieber ein lokales Benutzerkonto wählen möchte, klickt im Dialog **KONTO HINZUFÜGEN** unten links auf den gut versteckten Link **OFFLINEKONTO** (siehe Abbildung 2.4) und im nächsten Dialog auf **INGESCHRÄNKTE ERFAHRUNG**. Falls Sie, wie zuvor empfohlen, keine Verbindung zum Internet hergestellt haben, wird der Dialog **KONTO HINZUFÜGEN** gar nicht erst eingeblendet. Stattdessen gelangen Sie direkt zum Dialog **VON WEM WIRD DIESER PC GENUTZT?**. Geben Sie einen Namen für das Benutzerkonto ein und nach einem Klick auf **WEITER** ein Kennwort, das Sie im nächsten Dialog bestätigen.

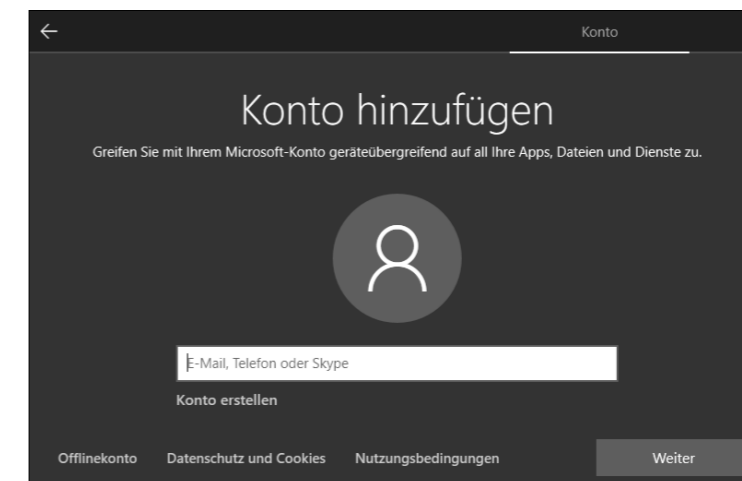


Abbildung 2.4 Im Dialog »Konto hinzufügen« wird von Microsoft die Angabe der E-Mail-Adresse eines Microsoft-Kontos vorgezogen. Der Link »Offlinekonto« ist noch unter Windows 10 Pro verfügbar, aber womöglich nicht mehr lange.

Als Nächstes müssen Sie aus insgesamt sechs Sicherheitsfragen drei auswählen und jeweils beantworten. Sollten Sie das Kennwort einmal vergessen, bietet Ihnen Windows an, das lokale Konto mithilfe der dann hoffentlich korrekt beantworteten Fragen wiederherzustellen. Zur Wiederherstellung eines lokalen Kontos gibt es aber auch andere Methoden, wie etwa die seit vielen Windows-Versionen bekannte Kennwortrücksetzdiskette (siehe Abschnitt 3.4.2). Ob Sie an dieser Stelle also die drei Sicherheitsfragen ehrlich beantworten oder aber schnell einen unsinnigen Text eingeben, bleibt ganz Ihnen überlassen. Um die Angabe kommen Sie jedenfalls nicht herum, es sei denn, Sie haben in den beiden Schritten zuvor auf die Angabe eines Kennwortes verzichtet. Dies ist aus Sicherheitsgründen aber keineswegs zu empfehlen. Mit der Auswahl der Sicherheitsfragen ist auch die Einrichtung des lokalen Benutzerkontos abgeschlossen.



Abbildung 2.5 Aus Sicherheitsgründen sollten Sie für das lokale Benutzerkonto ein Kennwort erstellen.

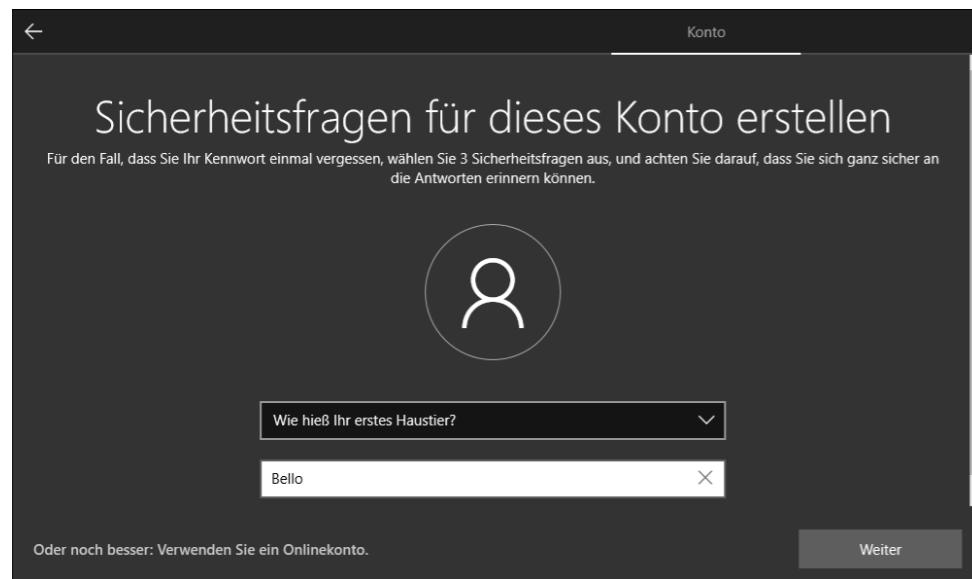


Abbildung 2.6 Die Sicherheitsfragen sind zweifelsohne lästig, müssen aber auch nicht ehrlich beantwortet werden.

Microsoft-Dienste konfigurieren

Die folgenden Einstellungen haben zunächst den Anschein, nur dem Komfort des Anwenders zu dienen. Sieht man sich die einzelnen Dialoge allerdings genauer an, wird deutlich,

dass es sich hier auch um Ihre Privatsphäre und somit den Datenschutz handelt. Denn stimmen Sie der Verwendung eines der angebotenen Dienste zu, hat dies in den meisten Fällen zur Folge, dass einige durchaus sensible Daten in der Cloud gespeichert und auch an Microsoft weitergeleitet werden. Es lohnt sich also, nicht alles sofort abzunicken, sondern zu hinterfragen, ob einem die Nutzung eines bestimmten Dienstes wirklich wichtig ist oder ob man eventuell auch darauf verzichten kann. Alle hier vorgenommenen Einstellungen können später problemlos korrigiert werden. Sollten Sie bei einem Dienst also z. B. die Verwendung abgelehnt haben, stellen später aber fest, dass Sie ihn doch nutzen möchten, aktivieren Sie ihn einfach. Die meisten der Dienste, um die es sich gleich dreht, lassen sich in der Einstellungen-App in der Kategorie DATENSCHUTZ konfigurieren. In Kapitel 22, »Windows 10 und der Datenschutz«, finden Sie hierzu ausführliche Informationen.

Die erste Entscheidung, die Sie im Rahmen der Microsoft-Dienste fällen müssen, betrifft die Spracheingaben, genauer gesagt die Online-Spracherkennung. Ist sie aktiviert, können Sie cloudbasierte Apps wie die Sprachassistentin Cortana per Sprache steuern. Diese Sprachdaten werden allerdings auch an Microsoft weitergeleitet. Da Cortana eine recht neugierige App ist, lautet meine Empfehlung bei dieser Einstellung, sie mit ONLINE-SPRACHERKENNUNG NICHT VERWENDEN zunächst abzulehnen. Markieren Sie Ihre gewünschte Einstellung, und klicken Sie dann auf ANNEHMEN. In Abschnitt 14.4, »Suchen mit Cortana«, lernen Sie die Sprachassistentin genauer kennen.

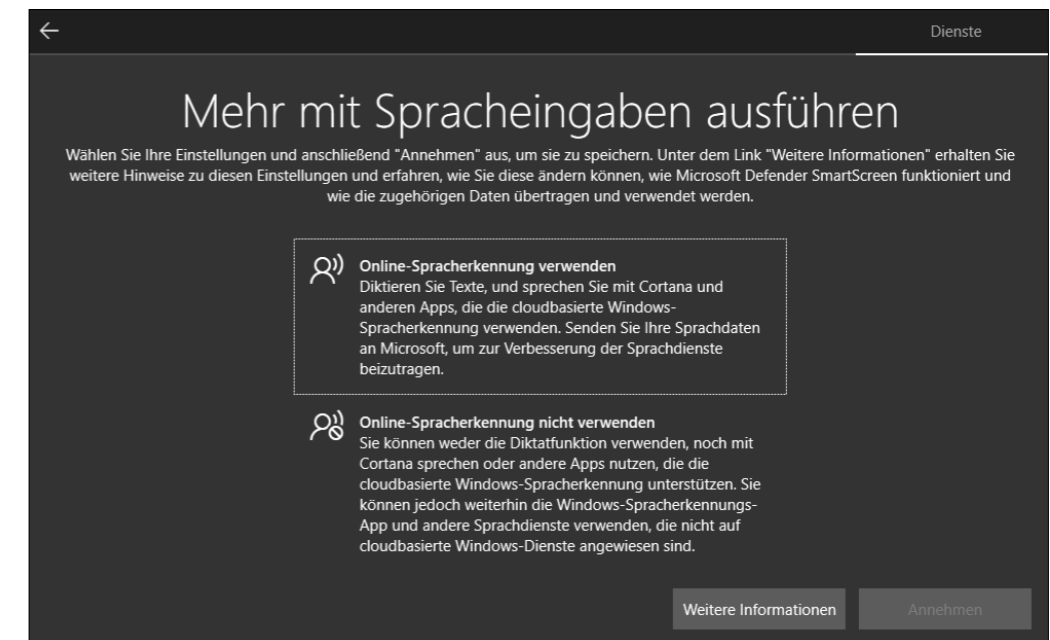


Abbildung 2.7 Stimmen Sie der Verwendung der Online-Spracherkennung zu, werden die Sprachdaten auch an Microsoft weitergeleitet.

Die nächste Einstellung betrifft die Ermittlung Ihres Standortes. Dieses Feature ist sicherlich interessant, wenn man unterwegs ist und eine Wegbeschreibung benötigt oder ein Restaurant in der Nähe sucht. Ob man den Positionsdienst aber daheim in Anspruch nehmen muss und damit in Kauf nimmt, dass Microsoft auch diese Informationen über Sie in die Hände bekommt, ist Ansichtssache. Ähnlich verhält es sich mit der nächsten Einstellung GERÄT SUCHEN. Nutzen lässt sich die Funktion nur, wenn Sie zuvor der Verwendung des Standortes zugestimmt haben. Denn nur so kann das Windows-Gerät anhand der zuletzt gespeicherten Standortdaten geortet werden, falls Sie es verloren haben oder das Gerät geklaut wurde. Eine weitere Voraussetzung der Ortung: Sie müssen bei Windows mit einem Microsoft-Konto angemeldet sein, und die Internetverbindung des Geräts muss aktiviert sein. WEITERE INFORMATIONEN zur Nutzung dieser Funktion erhalten Sie nach einem Klick auf den gleichnamigen Link.

Erfassung von Diagnosedaten

Mit welcher Hardware sind die Windows 10-Computer ausgestattet? Mit welchen Programmen arbeiten die Anwender bevorzugt? Welche Probleme tauchen bei der Bedienung auf? An diesen Informationen ist Microsoft sehr interessiert und sammelt diese sogenannte *Diagnosedaten* deshalb auch eifrig.



Abbildung 2.8 Wem Datenschutz und Privatsphäre wichtig sind, sollte sich für »Erforderliche Diagnosedaten senden« entscheiden und nicht für die hier im Bild halb eingerahmte Einstellung »Erforderliche und optionale Diagnosedaten senden«.

Mithilfe der Daten soll Windows weiterentwickelt und vor allem optimiert werden. In gewissem Umfang lässt sich das Interesse nachvollziehen. Passt man allerdings bei den Einstellungen nicht auf, gewährt man Microsoft erheblichen Einblick in die eigene Computerarbeit. Ganz lässt sich das Erfassen der Diagnosedaten nicht unterbinden, Sie haben aber zumindest ein kleines Mitspracherecht, was den Umfang der übermittelten Informationen angeht. Im Dialog DIAGNOSE DATEN AN MICROSOFT SENDEN können Sie das Senden auf die erforderlichen Diagnosedaten beschränken oder zusätzlich zu diesen auch optionale Diagnosedaten an Microsoft verschicken. Letzteres führt u. a. dazu, dass Microsoft auch über besuchte Websites und alle genutzten Anwendungen und Funktionen informiert wird. Und nicht nur das! Sollte die Bearbeitung einer Datei zu einer Fehlermeldung führen, wird nicht nur die Meldung an Microsoft weitergeleitet, sondern auch die entsprechende Datei. Bedenken Sie dies, wenn Sie die Entscheidung über den Umgang mit den Diagnosedaten fällen.

Ähnlich kritisch ist auch die nächste Einstellung FREIHAND UND EINGABE VERBESSERN ZU bewerten. Möchten Sie tatsächlich, dass Microsoft Ihre Tastatureingaben und im Falle eines Touchscreens Ihre Freihandeingaben in Erfahrung bringt? Treffen Sie die gewünschte Entscheidung, und übernehmen Sie diese wie üblich mit ANNEHMEN.

Werbung erwünscht?

In den nächsten zwei Dialogen legen Sie fest, welche Art von Werbung, Tipps und Tricks Sie von Microsoft erhalten möchten. Im Dialog MITHILFE VON DIAGNOSE DATEN ANGEPASSTE ERFAHRUNGEN ERHALTEN führt die Wahl eines JA dazu, dass Microsoft die gesammelten Telemetriedaten auswertet, um Ihnen auf Basis dieser Informationen Werbung zukommen zu lassen. Mit einem NEIN werden Sie nur allgemeine Tipps erhalten. Eine ähnliche Wirkung hat die im Dialog APPS WERBE-ID VERWENDEN LASSEN vorgenommene Einstellung. Bei der Nutzung von Windows wird für jeden Anwender eine Werbe-ID erzeugt. Falls Sie erlauben, dass Apps auf diese Identifikationsnummer zugreifen dürfen, erhalten Sie personalisierte Werbung. Wer dies nicht wünscht, beantwortet die Frage mit NEIN.

Geräteübergreifende Dienste

Der Vorteil eines Microsoft-Kontos ist, dass Sie es auf mehreren Geräten nutzen können. Stimmen Sie einer Synchronisierung zu, stehen Ihnen so Einstellungen, Daten und mehr auf allen Geräten zur Verfügung. In den folgenden Dialogen können Sie bereits festlegen, welche geräteübergreifende Dienste Sie nutzen möchten. Dazu zählt etwa der Aktivitätsverlauf, in dem die besuchten Webseiten oder auch geöffnete Dateien festgehalten werden, aber auch die Datensicherung in der Cloud OneDrive. Voraussetzung ist natürlich jeweils, dass Sie mit einem Microsoft-Konto am Computer angemeldet sind und dieses auch auf den anderen Geräten nutzen. Wer sich zunächst mit den Funktionen auseinandersetzen möchte, die alle auch in diesem Buch besprochen werden, kann die Dialoge in der Einrichtungsphase mit NEIN bzw. SPÄTER ERLEDIGEN beantworten. Falls Sie Ihre Bilder, Dokumente und mehr nicht in OneDrive speichern möchten, klicken Sie auf DATEIEN NUR AUF DIESEM PC SPEICHERN.

Wie alle vorherigen Einstellungen lässt sich die jetzt vorgenommene Auswahl auch später noch korrigieren.



Abbildung 2.9 Sie können Ihre Daten in der Cloud OneDrive speichern oder auch lokal auf dem PC.

Die Anmeldung mit einem Microsoft-Konto ist auch dann erforderlich, wenn Sie Cortana nutzen möchten. Bis Windows 10 Version 2004 war die Sprachassistentin fest im Betriebssystem integriert und mischte vor allem bei Suchanfragen mit. Genau dies wurde immer wieder heftig kritisiert, da Cortana dabei viele Daten sammelte, die damit auch Microsoft zugänglich waren. Mittlerweile ist Cortana eine eigenständige App, die sich, wie Sie in Abschnitt 14.4, »Suchen mit Cortana«, sehen werden, noch im Ausbau befindet. Die Nutzung von Cortana bietet dem Anwender derzeit also noch keinen allzu großen Mehrwert, was sich mit jedem weiteren Update aber sicherlich ändern wird. Auch für Cortana gilt natürlich: Falls Sie sich noch nicht sicher sind, ob Sie Cortana verwenden möchten, verschieben Sie die Entscheidung mit JETZT NICHT einfach auf später.

Damit ist die Ersteinrichtung auch schon abgeschlossen. Windows wird nun entsprechend Ihren Vorgaben vorbereitet, was nochmals ein paar Minuten Zeit in Anspruch nimmt. Anschließend erhalten Sie endlich einen Blick auf die Desktopoberfläche und seit dem Oktober 2020 Update auch auf den neuen Browser Edge Chromium, den Sie in Abschnitt 17.1, »Der Browser Microsoft Edge Chromium«, genauer kennenlernen werden. Das Browserfenster können Sie zunächst auch wie gewohnt per Klick auf das Schließen-Symbol oben rechts schließen.

Sollte der Computer bereits mit dem Internet verbunden sein, erscheint am rechten Fenster Rand die Nachfrage, ob Ihr Computer von anderen Geräten innerhalb des Netzwerkes gefun-

den werden darf. Im eigenen Netzwerk oder Firmennetzwerk können Sie diese Frage mit JA beantworten. Sollten Sie sich an einem öffentlichen WLAN angemeldet haben, wählen Sie zum Schutz Ihres Computers stattdessen NEIN.

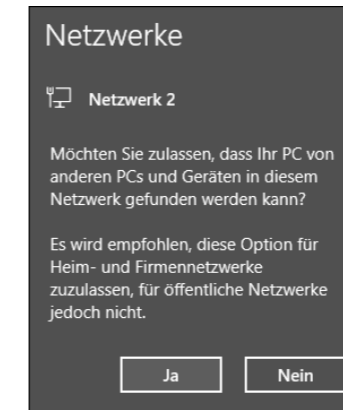






Abbildung 2.10 Ist Ihr Computer mit dem heimischen Netzwerk verbunden, können Sie hier mit »Ja« antworten. In einem öffentlichen Netzwerk sollten Sie hingegen auf »Nein« klicken.

Internetverbindung einrichten

Sollten Sie bei der Ersteinrichtung keine Internetverbindung hergestellt haben, können Sie dies natürlich jederzeit nachholen. Um den Computer per Netzwerkkabel mit dem Router zu verbinden, reicht es, das Kabel einfach in den entsprechenden Anschluss zu stecken. Bereits nach einem kurzen Moment steht die Internetverbindung, wie Sie an dem Symbol  im Infobereich der Taskleiste überprüfen können. Um eine WLAN-Verbindung herzustellen, klicken Sie im Infobereich auf das Symbol . Es klappt eine Liste mit allen in der näheren Umgebung verfügbaren Funknetzen auf. Markieren Sie das gewünschte WLAN, und klicken Sie dann auf VERBINDEN. Nach Eingabe des Netzwerksicherheitsschlüssels klicken Sie auf WEITER. In Kapitel 19 erhalten Sie weitere Informationen rund um die Einrichtung eines Netzwerkes.

2.3 Die Oberfläche von Windows 10

Wer früher bereits mit Windows 7 gearbeitet hat, dem wird die Bildschirmoberfläche, die nach dem Start von Windows 10 zu sehen ist, recht bekannt vorkommen. Am unteren Rand des Desktops findet sich wie gewohnt die Taskleiste. Klicken Sie hier auf das Windows-Logo  ganz links, öffnet sich das Startmenü. Alternativ hierzu können Sie auch die Taste  auf der Tastatur drücken. Sollten Sie ein Gerät mit Touchscreen nutzen, nimmt das Startmenü den gesamten Bildschirm ein. Welche Besonderheiten es hier zu beachten gibt, erfahren Sie in Kapitel 10, »Windows 10 und der Tabletmodus«.

In der mittleren Spalte des Startmenüs finden Sie eine Liste mit allen auf dem Computer installierten Apps und Programmen. Für einige dieser Anwendungen finden Sie im Kachelbereich eine Verknüpfung in Form einer Kachel. Ein Klick hierauf genügt, und die damit verbundene App wird gestartet. In Kapitel 5 erfahren Sie, wie Sie das Startmenü und damit auch den Kachelbereich individuell anpassen können. Gefallen Ihnen das Hintergrundbild und die Farbgebung von Startmenü und Taskleiste nicht? In Abschnitt 7.1, »Hintergrund und Farbschema anpassen«, wird beschrieben, wie Sie dem Desktop eine persönliche Note geben.

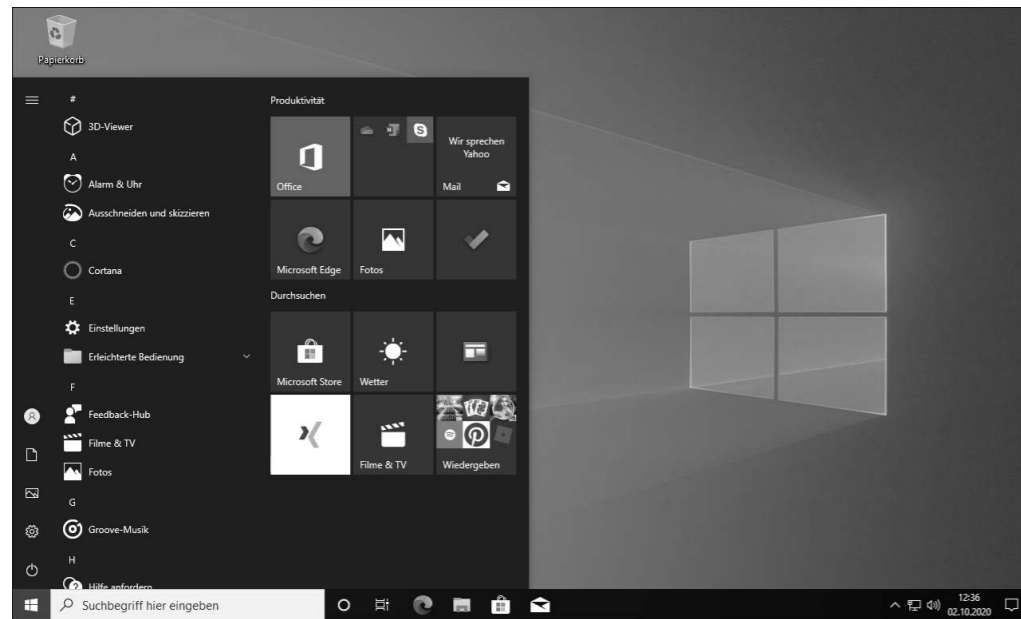


Abbildung 2.11 Die Desktopoberfläche mit geöffnetem Startmenü

Die schmale Spalte am linken Rand zeigt zunächst nur Symbole an. Fahren Sie mit dem Mauszeiger über eines der Symbole, wird jeweils ein kleiner Hinweis zur Funktion der Symbole eingeblendet. Gleiches erreichen Sie, wenn Sie am oberen Rand der Spalte auf das Hamburger-Menü ☰ klicken. Nach einem Klick auf den Ein-/Ausschalter ⏻ wird ein Menü mit den Befehlen zum Herunterfahren oder auch Neustarten des PCs angezeigt. Über das Zahnradsymbol ⚙️ gelangen Sie zur Einstellungen-App, in der Sie die wichtigsten Konfigurationsoptionen finden. Klicken Sie auf die Symbole BILDER oder DOKUMENTE, wird der Explorer mit dem jeweiligen Ordner geöffnet. Möchten Sie den Computer sperren oder sich vom System abmelden, ohne den PC herunterzufahren, klicken Sie auf das Benutzersymbol 👤 und wählen den gewünschten Befehl. Die Schaltfläche KONTOEINSTELLUNGEN ÄNDERN führt Sie direkt zur Kategorie KONTEN in der Einstellungen-App, in der Sie z. B. die Anmeldeoptionen ändern können. Mehr zu diesem Thema erfahren Sie in Abschnitt 3.4. Falls Sie das Startmenü wieder ausblenden möchten, ohne hierüber eine der Apps oder Funktionen aufzurufen, reicht ein erneuter Klick auf das Windows-Logo 🪟.

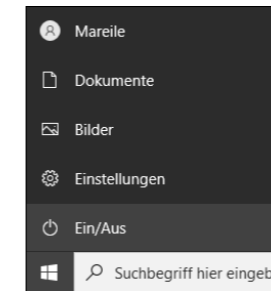


Abbildung 2.12 Fahren Sie mit dem Mauszeiger über die Symbole am linken Rand des Startmenüs, werden Hinweise zu den Funktionen eingeblendet.

Windows 10 zeigt sich sehr mitteilungsfreudig. So erfahren Sie selbstverständlich sofort, wenn eine neue E-Mail eingetroffen ist oder gar ein Sicherheitsproblem festgestellt wurde. Über das Benachrichtigungssymbol 🗨️ am äußersten rechten Rand der Taskleiste blenden Sie das sogenannte *Info-Center* ein, in dem im oberen Abschnitt all diese Benachrichtigungen aufgeführt werden.

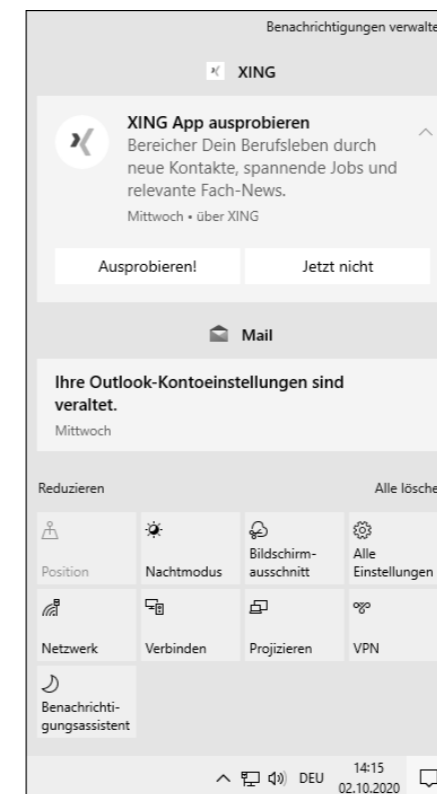


Abbildung 2.13 Manche Benachrichtigungen im Info-Center sind sinnvoll, andere hingegen überflüssig.

Manche davon sind wichtig, andere – wie etwa die Empfehlung einer App – können mit der Zeit aber auch nerven. In Abschnitt 6.3, »Benachrichtigungen und Aktionen im Info-Center«, zeige ich Ihnen, wie Sie selbst festlegen, welche Informationen Sie erhalten möchten und welche nicht. Dort erfahren Sie auch, wie Sie die Schaltflächen für schnelle Aktionen geschickt nutzen, um schnell Funktionen ein- oder auszuschalten oder wichtige Einstellungen aufzurufen.

Kapitel 12

Datensicherung mit Windows 10

Auch wenn den meisten Anwendern durchaus bewusst ist, wie wichtig eine Datensicherung ist, setzen doch die wenigsten sie konsequent um. Dabei ist ein Backup selbst mit den Bordmitteln von Windows 10 schnell eingerichtet. In diesem Kapitel lernen Sie verschiedene Varianten kennen.

Gefahren für Ihre Daten drohen von überall: So reicht ein unbedachter Moment, und schon gibt die Festplatte aufgrund eines umgestürzten Wasserglases ihren Dienst auf. Oder Ihr System wird von sogenannter *Ransomware* infiziert. Durch diesen Erpressungstrojaner werden alle Daten auf der Festplatte verschlüsselt und lassen sich nie wieder entschlüsseln. Selbst im Rahmen eines Updates kann es passieren, dass Daten gelöscht werden, wie es einige Nutzer leider beim Update zur Windows 10 Version 1809 zu spüren bekamen. Nur wer regelmäßig seine Daten sichert, kann solchen Momenten relativ entspannt begegnen.

Doch was ist die richtige Backup-Strategie? Eine gute Orientierung bietet hier die *3-2-1-Backup-Regel*. Sie empfiehlt

- ▶ mindestens drei Kopien der Daten zu erstellen,
- ▶ die auf zwei unterschiedlichen Speichermedien gesichert werden,
- ▶ von denen eines an einem anderen Ort aufbewahrt wird.

Der andere Ort bezeichnet dabei tatsächlich einen Platz außerhalb Ihres Hauses bzw. des Bürogebäudes. Denn nur so ist das Backup auch im Falle eines Einbruchs oder – noch schlimmer – Hausbrandes gesichert. Ein solcher Platz könnte z. B. ein Onlinespeicher wie OneDrive sein, aber auch das Haus eines sehr guten Freundes oder Familienmitglieds, der für Sie die externe Festplatte mit der Datensicherung aufbewahrt.

Wie häufig Sie ein Backup durchführen, hängt davon ab, wie häufig Sie Änderungen an den Dateien vornehmen. Auch der Wert, den die Daten für Sie haben, spielt eine Rolle. Wenn Sie gerade Hunderte von unwiederbringlichen Urlaubsbildern auf den PC überspielt haben, schreit dies regelrecht nach einer sofortigen Datensicherung, während das Begleitschreiben an eine Versicherung wahrscheinlich keine allzu hohe Priorität hat. Hier müssen Sie also selbst abwägen, ab welchem Moment ein Datenverlust für Sie schmerzhaft wird.

Die für ein Backup nötigen Programme bringt Windows 10 bereits mit. Eines davon, die Funktion *Sichern und Wiederherstellen*, kennt der ein oder andere bereits aus Windows 7-Zeiten. Das Tool zum Erstellen eines Systemabbilds hat seine Vor- und Nachteile, besser als gar

keine Datensicherung ist es aber allemal. Durchaus gute Dienste leistet der *Dateiversionsverlauf*, mit dem Sie, wie der Name bereits deutlich macht, die unterschiedlichen Versionen Ihrer Dateien sichern. Er hielt bereits mit Windows 8 Einzug ins Betriebssystem, wurde seitdem aber stark weiterentwickelt. Eine weitere Backup-Möglichkeit, die Sie in diesem Kapitel kennenlernen werden, stellt die Cloud *OneDrive* dar. Mit der Einrichtung eines Microsoft-Kontos stehen Ihnen als Privatanwender automatisch 5 GB kostenloser Speicherplatz in der Cloud zur Verfügung. Verfügen Sie z. B. über ein Microsoft 365 Family-Abonnement (früher Office 365 Home genannt) oder ein Microsoft 365 Single-Abonnement (früher als Office 365 Personal bekannt), beläuft sich der kostenlose Speicherplatz sogar auf 1 TB pro Benutzer.

12.1 Backup mit dem Dateiversionsverlauf

Mit dem in Windows 10 integrierten Dateiversionsverlauf speichern Sie all Ihre Daten aus Ihrem persönlichen Benutzerprofil auf einem lokalen oder externen Laufwerk oder auf einem Netzwerklaufwerk.

Sobald die Funktion aktiviert und die erste Datensicherung durchgeführt wurde, prüft der Dateiversionsverlauf in den von Ihnen vorgegebenen Abständen, ob neue oder geänderte Dateien vorliegen und führt diese automatisch dem Backup hinzu. Die Datensicherung lässt sich bequem durchsuchen, was eine Wiederherstellung verloren gegangener oder beschädigter Daten, aber auch älterer Dateiversionen sehr einfach gestaltet.

12.1.1 Den Dateiversionsverlauf einrichten

Bevor der Dateiversionsverlauf seinen Dienst antreten kann, müssen Sie die Funktion aktivieren und einrichten. Verwenden mehrere Benutzer den Computer, muss der Dateiversionsverlauf für jeden getrennt vorgenommen werden. Ein Bestandteil der Konfiguration ist die Auswahl des Speicherortes für die Datensicherung. Hierfür sollten Sie keinesfalls den Datenträger wählen, auf dem sich das Systemvolumen befindet. Gut geeignet sind hingegen z. B. eine externe Festplatte oder auch ein Netzwerkspeicher, für den Sie über die nötige Lese- und Schreibberechtigung verfügen. Entscheiden Sie sich für das externe Laufwerk, erfolgt die Aktivierung des Dateiversionsverlaufs über die Einstellungen-App. Bei einem Netzwerkspeicher (engl. »Network Attached Storage«, kurz *NAS* genannt) führt Sie der Weg noch in die Systemsteuerung, wie Sie etwas weiter unten in diesem Abschnitt sehen werden. Mit jedem neuen Funktionsupdate verlagert Microsoft Funktionen aus der Systemsteuerung in die Einstellungen-App. Es ist also nur eine Frage der Zeit, wann sich auch der Dateiversionsverlauf komplett über die App konfigurieren lässt.

Um die Datensicherung auf einem externen Laufwerk, etwa einer per USB an den PC angeschlossene Festplatte, durchzuführen, gehen Sie folgendermaßen vor:

1. Nachdem Sie das Laufwerk angeschlossen haben, rufen Sie in der Einstellungen-App **UPDATE UND SICHERHEIT • SICHERUNG** auf. Nach einem Klick auf **LAUFWERK HINZUFÜGEN** listet Windows 10 alle für die Datensicherung geeigneten Laufwerke auf. Markieren Sie das gewünschte Laufwerk. Nach einem kurzen Moment erscheint statt der Schaltfläche **LAUFWERK HINZUFÜGEN** nun der bereits eingeschaltete Regler **MEINE DATEIEN AUTOMATISCH SICHERN**. Der Dateiversionsverlauf ist damit aktiviert.

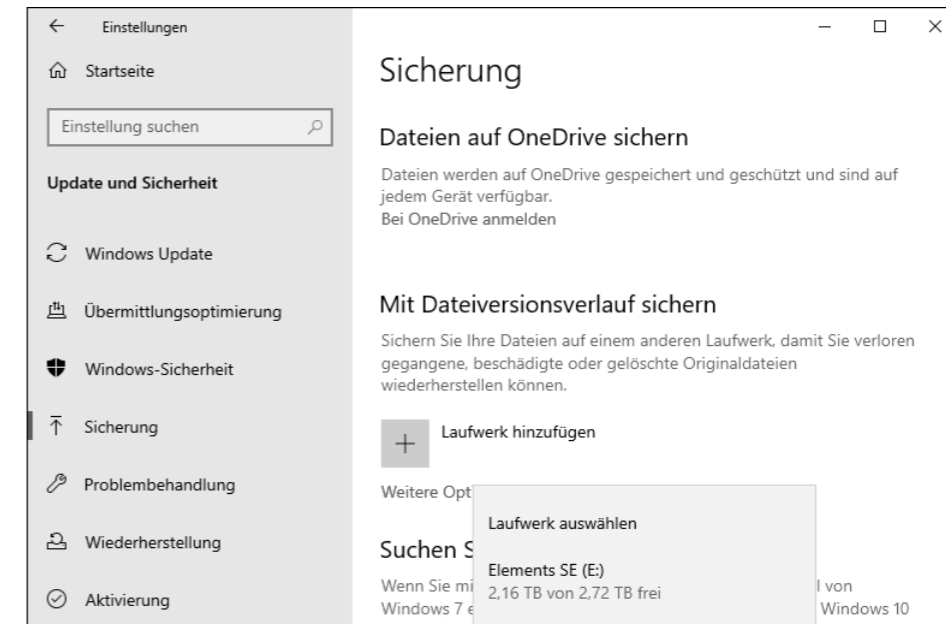


Abbildung 12.1 Der Dateiversionsverlauf wird automatisch aktiviert, sobald Sie ein Laufwerk ausgewählt haben.

2. Klicken Sie auf **WEITERE OPTIONEN**, um dort weitere Einstellungen für die Funktion vorzunehmen.
3. Per Standardeinstellung prüft Windows 10 stündlich, ob neue Dateien oder Dateiversionen verfügbar sind und sichert diese. Sie können das Intervall aber auch von **ALLE 10 MINUTEN** bis hin zu **TÄGLICH** anpassen. Eine noch feinere Justierung ist per Aufgabenplanung möglich, wie im nächsten Abschnitt gezeigt.
4. Irgendwann einmal kommt der Zeitpunkt, an dem der verfügbare Speicherplatz auf einem Speichermedium erschöpft ist. Standardmäßig werden die Sicherungen immer beibehalten. Sie können in den Sicherungsoptionen des Dateiversionsverlaufs aber auch festlegen, dass ältere Dateiversionen z. B. bereits nach einem Monat, erst in zwei Jahren oder dann, wenn Platz benötigt wird, gelöscht werden.
5. Im Bereich **DIESE ORDNER SICHERN** werden alle Ordner aufgelistet, die vom Dateiversionsverlauf bei der Datensicherung berücksichtigt werden. Dabei handelt es sich um die

Ordner Ihres Benutzerprofils, die klassischerweise unter `C:\Users\<Benutzer>` gespeichert sind. Nutzen Sie OneDrive, werden auch die zwischen Gerät und Onlinespeicher synchronisierten Daten berücksichtigt, die lokal auf dem Gerät verfügbar sind. Enthält die Liste ein Element, das nicht gesichert werden soll, markieren Sie es und klicken dann auf **ENTFERNEN**. Umgekehrt können Sie über die Schaltfläche **ORDNER HINZUFÜGEN** Verzeichnisse auswählen, die bisher noch nicht aufgeführt wurden.

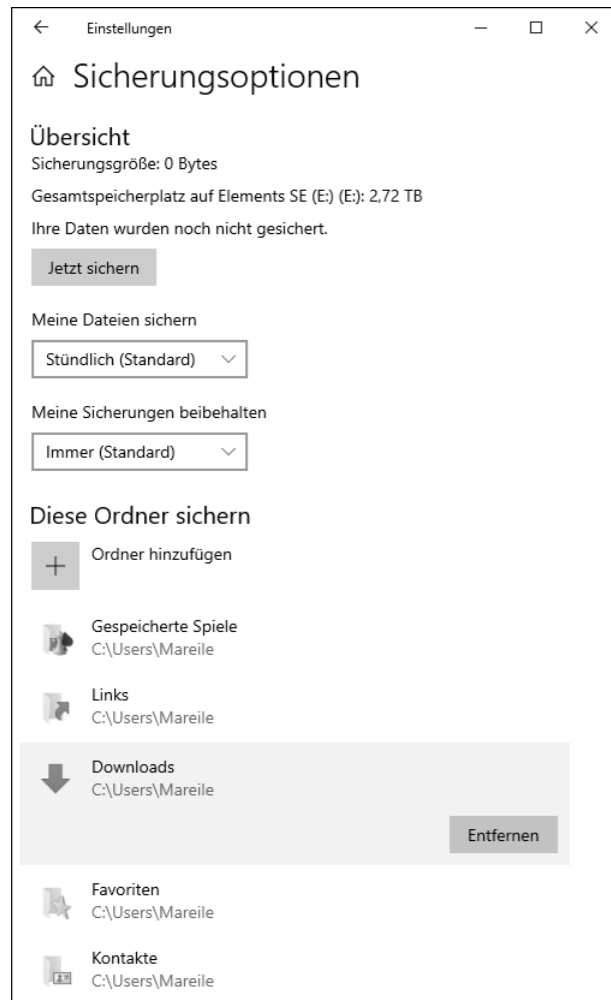


Abbildung 12.2 Um Speicherplatz zu sparen, entfernen Sie nicht benötigte Ordner aus der Liste der zu sichernden Ordner.

- Die unter **DIESE ORDNER SICHERN** aufgeführten Pfade beinhalten jeweils auch die Unterordner eines Verzeichnisses. Gibt es einen Ordner z. B. innerhalb des Verzeichnisses *Dokumente*, der beim Backup nicht berücksichtigt werden soll, ergänzen Sie diesen über

die Schaltfläche **ORDNER HINZUFÜGEN** unterhalb von **DIESE ORDNER AUSSCHLIESSEN** (siehe Abbildung 12.3).

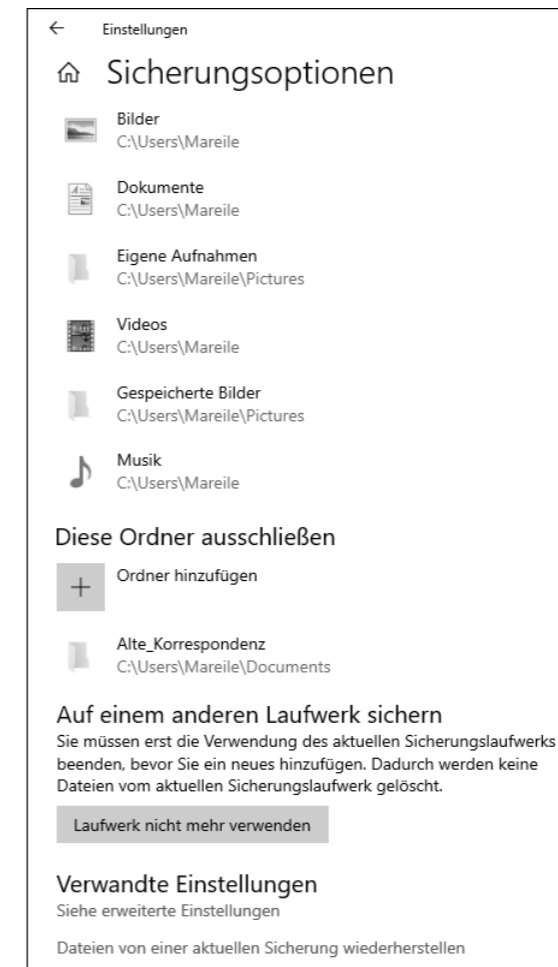


Abbildung 12.3 Bevor Sie ein neues Laufwerk für den Dateiversionsverlauf wählen können, müssen Sie die Verwendung des bisherigen beenden.

- Haben Sie alle Einstellungen vorgenommen, kehren Sie zum Seitenanfang zurück. Wenn Sie noch keine Sicherung durchgeführt haben, wird als Sicherungsgröße 0 BYTES angezeigt. Mit einem Klick auf **JETZT SICHERN** stoßen Sie die Datensicherung manuell an.

Zukünftig übernimmt Windows 10 diese Aufgabe automatisch nach dem von Ihnen vorgegebenen Intervall. Sie können aber natürlich auch zwischendurch eine Datensicherung starten, falls Ihnen der nächste turnusmäßige Zeitpunkt zu weit entfernt scheint. Das erste Backup nimmt etwas Zeit in Anspruch, alle folgenden sind schneller erledigt, da dann lediglich geänderte sowie neue Daten erfasst werden.

Sollten Sie das Laufwerk für die Datensicherung nicht mehr verwenden bzw. gegen ein anderes austauschen wollen, rufen Sie wieder die Seite SICHERUNGSOPTIONEN in der Einstellungen-App auf. Klicken Sie am Ende der Seite auf LAUFWERK NICHT MEHR VERWENDEN. Der Dateiversionsverlauf ist damit so lange deaktiviert, bis Sie wie in Schritt 1 beschrieben ein neues Laufwerk hinzugefügt haben.

Statt einer externen Festplatte können Sie für die Datensicherung via Dateiversionsverlauf auch ein Netzlaufwerk verwenden, sofern Sie denn über die nötigen Lese- und Schreibberechtigungen verfügen. Um das Backup zu aktivieren und einzurichten, rufen Sie in der Einstellungen-App SICHERHEIT UND UPDATE • SICHERUNG auf. Klicken Sie auf WEITERE OPTIONEN und auf der Seite SICHERUNGSOPTIONEN auf SIEHE ERWEITERTE EINSTELLUNGEN. Damit gelangen Sie automatisch zum Dialog DATEIVERSIONSVERLAUF innerhalb der Systemsteuerung, in dem Sie auf LAUFWERK AUSWÄHLEN klicken. Über die Schaltfläche NETZWERKADRESSE HINZUFÜGEN bestimmen Sie den Netzwerkspeicherort, in dem das Backup abgelegt werden soll. Zurück im Dialog DATEIVERSIONSVERLAUF, können Sie über die Schaltfläche ORDNER AUSSCHLIESSEN noch festlegen, welche Verzeichnisse nicht beim Backup berücksichtigt werden sollen. Den Zeitrahmen für die Datensicherung bestimmen Sie in den ERWEITERTEN EINSTELLUNGEN. Im Gegensatz zur Einstellungen-App, in der der Dateiversionsverlauf mit dem Hinzufügen des Laufwerks automatisch aktiviert wird, müssen Sie die Funktion in der Systemsteuerung noch EINSCHALTEN. Damit wird zugleich die erste Datensicherung gestartet.

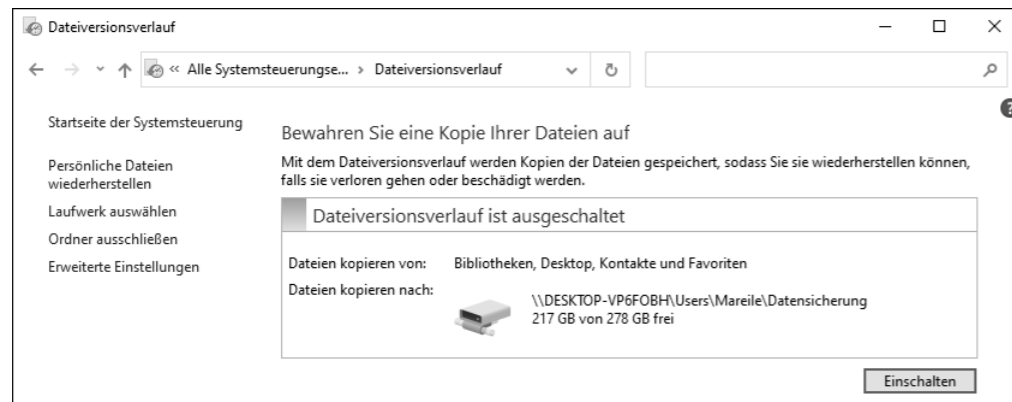


Abbildung 12.4 In der Systemsteuerung muss der Dateiversionsverlauf explizit eingeschaltet werden.

Ereignisprotokoll des Dateiversionsverlaufs überprüfen

Immer wieder hört man bei Backup-Programmen als Kritikpunkt, dass nicht alle Dateien zuverlässig gespeichert werden. Der Grund hierfür sind häufig zu lange Dateipfade, die durch zu stark verschachtelte Unterverzeichnisse entstehen. Beim Dateiversionsverlauf werden zudem alle gespeicherten Dateien um das aktuelle Datum sowie die Uhrzeit erweitert, was

wiederum zu einem längeren Dateinamen führt. Die Kombination aus vielen Unterverzeichnissen und einem langen Dateinamen führt dann teilweise dazu, dass die in Windows maximal zulässige Pfadlänge von 260 Zeichen überschritten wird. Diese Dateien werden damit beim Dateiversionsverlauf nicht berücksichtigt. Auch beim Versuch, sie zu löschen, kommt es häufig zu Fehlermeldungen. Damit solche Probleme gar nicht erst entstehen, sollten Sie von vornherein auf möglichst kurze Pfade sowie Dateinamen achten. Ob bei der Datensicherung via Dateiversionsverlauf alles vorschriftsmäßig geklappt hat, lässt sich über das Ereignisprotokoll überprüfen. Rufen Sie hierzu in der Einstellungen-App UPDATE UND SICHERHEIT • SICHERUNG • WEITERE OPTIONEN auf und auf der Seite SICHERUNGSOPTIONEN dann SIEHE ERWEITERTE EINSTELLUNGEN. Im Dialog DATEIVERSIONSVERLAUF der Systemsteuerung klicken Sie auf ERWEITERTE EINSTELLUNGEN und dann auf ÖFFNEN SIE DIE DATEIVERSIONSVERLAUF-EREIGNISPROTOKOLLE, UM KÜRZLICH AUFGETRETENE EREIGNISSE ODER FEHLER ANZUZEIGEN.

12.1.2 Dateiversionsverlauf per Aufgabenplanung steuern

Manchen Anwendern genügen die Optionen nicht, die sich über die Einstellungen-App oder auch die Systemsteuerung für den Dateiversionsverlauf festlegen lassen. Hier bietet das Kommandozeilentool `fhmanagew` weitaus mehr Konfigurationsmöglichkeiten. Möchten Sie etwa gezielt ältere Dateiversionen aus der Datensicherung entfernen, um so selbst für freien Speicherplatz auf der externen Festplatte zu sorgen, lässt sich dies schnell mithilfe des Tools realisieren. Rufen Sie hierzu z. B. über das Suchfeld der Taskleiste die Eingabeaufforderung auf. Um Dateiversionen zu löschen, die älter als 45 Tage sind, geben Sie dann den Befehl `fhmanagew -cleanup 45` ein. Wenn Sie lediglich die aktuellsten Dateiversionen beibehalten möchten, ersetzen Sie die Angabe »45« durch »0«, also `fhmanagew -cleanup 0`. Die Wiederherstellung älterer Versionen einer Datei ist damit nicht mehr möglich.

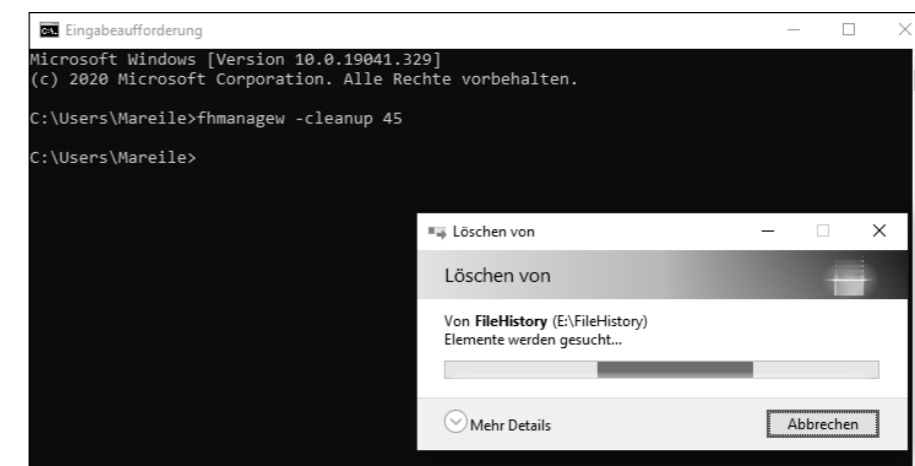


Abbildung 12.5 Mit dem Kommandozeilentool »fhmanagew« lassen sich gezielt ältere Dateiversionen löschen.

Kombinieren Sie das Kommandozeilentool mit der Aufgabenplanung, ergeben sich zusätzliche interessante Szenarien. So lässt sich z. B. auf die Minute genau festlegen, wann die Datensicherung durchgeführt werden soll. Im folgenden Beispiel soll dies täglich um 16:00 Uhr geschehen. Und so legen Sie die Aufgabe fest:

1. Drücken Sie die Tastenkombination **Win** + **X**, und wählen Sie im aufklappenden Schnellzugriffsmenü die **COMPUTERVERWALTUNG** aus. Markieren Sie dort die **AUFGABENPLANUNG**, und rufen Sie im Menü **AKTION** den Befehl **AUFGABE ERSTELLEN** auf.
2. Im Register **ALLGEMEIN** des Dialogs **AUFGABE ERSTELLEN** vergeben Sie für die Aufgabe einen aussagekräftigen Namen.
3. Im Register **TRIGGER** klicken Sie auf **NEU**, um im folgenden Dialog **NEUER TRIGGER** die Bedingungen für die Aufgabe festzulegen. Für unser Beispiel behalten Sie die Einstellung **NACH EINEM ZEITPLAN** im Feld **AUFGABE STARTEN** bei. Nach Auswahl der Option **TÄGLICH** werden Datum und Uhrzeit für den Start der Aufgabe festgelegt. Die Wiederholung soll jeden Tag erfolgen, die Angabe 1 kann also übernommen werden. Erweiterte Einstellungen sind für das einfache Beispiel nicht nötig. Wichtig ist hier lediglich, dass **AKTIVIERT** mit einem Häkchen versehen ist, bevor Sie den Dialog mit **OK** schließen.

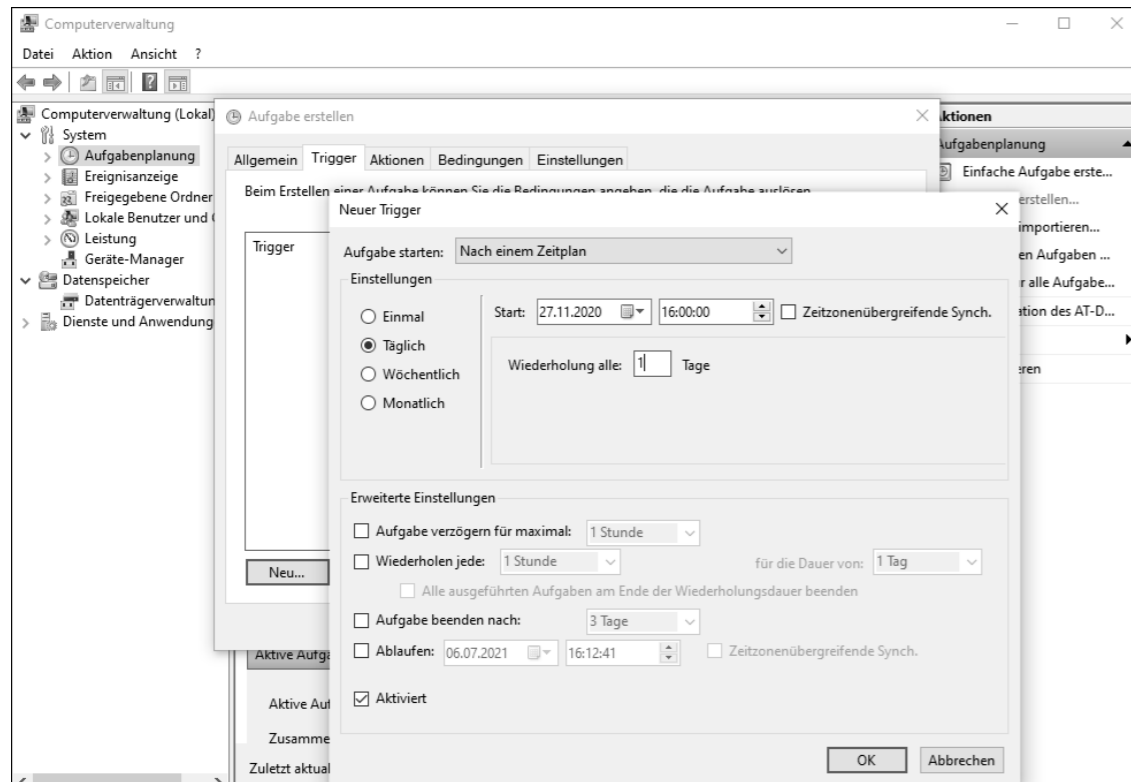


Abbildung 12.6 Die Datensicherung lässt sich nach einem exakten Zeitplan durchführen.

4. Wechseln Sie in das Register **AKTIONEN**, und klicken Sie dann auf **NEU**. Im Feld **AKTION** behalten Sie die Auswahl **PROGRAMM STARTEN** bei. Im Feld **PROGRAMM/SKRIPT** geben Sie »fhmanagew.exe« ein. Wer den Namen nicht selbst vollständig tippen will, klickt auf **DURCHSUCHEN**. Bereits nach Eingabe der ersten drei Buchstaben wird das gesuchte Tool **FHMANAGEW.EXE** vorgeschlagen, das Sie nur noch markieren müssen.

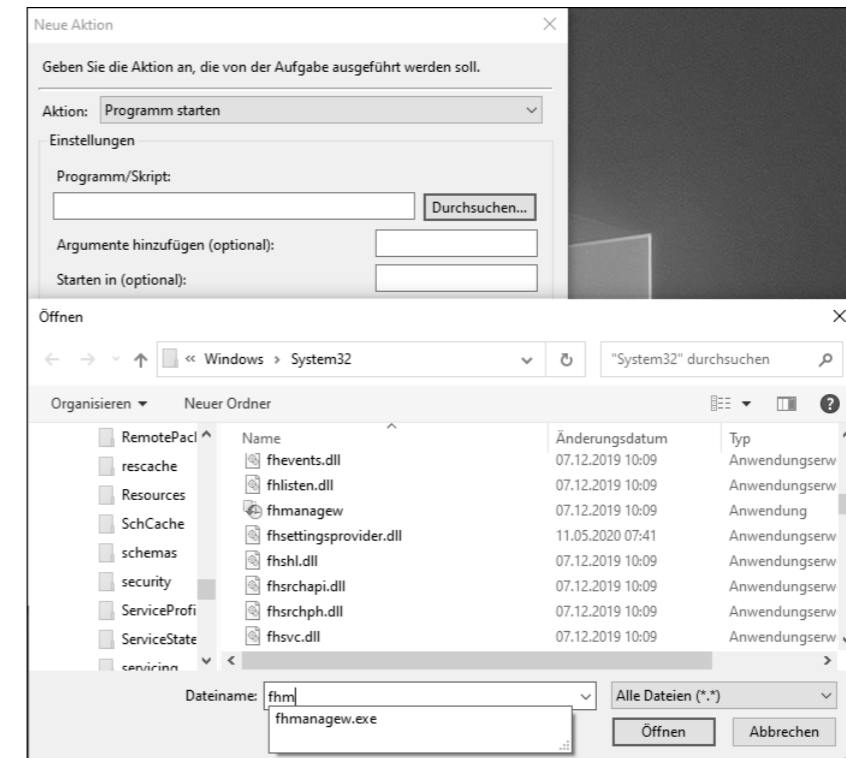


Abbildung 12.7 Sie müssen den Namen des Kommandozeilentools nicht einmal selbst eingeben.

Sobald Sie alle geöffneten Dialoge mit **OK** bestätigt haben, wird der Dateiversionsverlauf automatisch zum festgelegten Zeitpunkt durchgeführt.

12.1.3 Daten aus dem Dateiversionsverlauf wiederherstellen

Bei der Datensicherung durch den Dateiversionsverlauf legt Windows 10 auf dem Speichermedium einen Ordner namens *FileHistory* an. Dieser enthält wiederum einen Unterordner mit dem Namen des Benutzers. Sollten mehrere Benutzer das Speichermedium für die Datensicherung nutzen, finden Sie für jeden einen eigenen Ordner. Jeder dieser Benutzerordner enthält wiederum ein Unterverzeichnis für das Gerät, auf dem die Datensicherung durchgeführt wurde. Öffnen Sie diesen Geräteordner, finden Sie die beiden Ordner **CONFIGURATION** sowie **DATA** vor. Der Ordner **CONFIGURATION** enthält insgesamt vier Dateien,

die u. a. eine schnelle Suche im Dateiversionsverlauf sicherstellen. Im Ordner DATA werden alle durch den Dateiversionsverlauf gespeicherten Dateien abgelegt, und das in genau der Hierarchie, die auch am Originalspeicherort vorherrscht. Sie können im Explorer also wie vom Originalspeicherort gewohnt von Ordner zu Ordner navigieren, um zu einer Datei oder einem Ordner zu gelangen, den Sie wiederherstellen möchten. Ebenfalls praktisch: Per Copy & Paste lassen sich so die zuvor z. B. auf einer externen Festplatte gesicherten Daten auf einen neuen PC übertragen.

Windows 10 bietet Ihnen für die Wiederherstellung gelöschter oder kaputter Dateien und Ordner aber auch eine recht komfortable Methode an. Der hierfür nötige Dialog DATEIVERSIONSVERLAUF lässt sich auf unterschiedlichen Wegen öffnen:

- ▶ Einer führt z. B. über die Einstellungen-App, in der Sie UPDATE UND SICHERHEIT • SICHERUNG • WEITERE OPTIONEN aufrufen und dann am unteren Rand der Seite SICHERUNGSOPTIONEN auf DATEIEN VON EINER AKTUELLEN SICHERUNG WIEDERHERSTELLEN klicken. Per Doppelklick auf einen Ordnernamen oder über die Adressleiste am oberen Fenster Rand hangeln Sie sich nun bis zu dem Verzeichnis vor, in dem sich das wiederherzustellende Element befindet.
- ▶ Alternativ zur Einstellungen-App navigieren Sie direkt im Explorer zum gewünschten Verzeichnis oder auch zu der Datei. Markieren Sie das Element, und klicken Sie im Register START in der Gruppe ÖFFNEN auf VERLAUF, wird ebenfalls der Dialog DATEIVERSIONSVERLAUF geöffnet.

Der Dialog zeigt zunächst die aktuellste Version des Ordners. Handelt es sich um eine Datei, erhalten Sie sogar eine Vorschau auf ihren Inhalt. Sollte dies bei Ihnen noch nicht der Fall sein, doppelklicken Sie die Datei im Dialog einfach an.

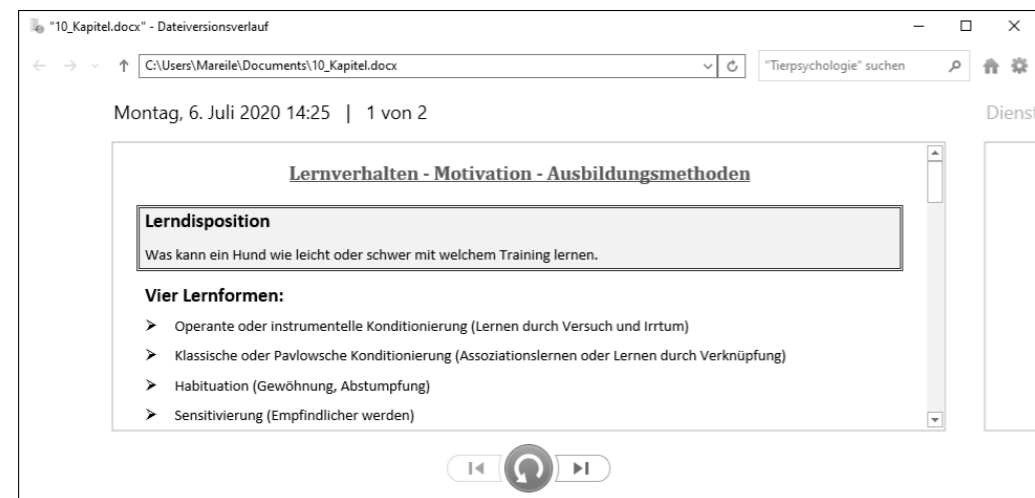


Abbildung 12.8 Über den Dialog »Dateiversionsverlauf« lassen sich mühelos ältere Datei- oder Ordnerversionen wiederherstellen.

Wann die Sicherung des ausgewählten Elements erfolgt ist, entnehmen Sie dem Datum und der Uhrzeit unterhalb der Adressleiste. Rechts von den Zeitangaben erfahren Sie, wie viele Sicherungen, sprich Versionen existieren. Über die beiden Pfeiltasten am unteren Fensterrand gelangen Sie zu den älteren bzw. neueren Versionen. Haben Sie die Version gefunden, die Sie wiederherstellen möchten, müssen Sie sich nur noch entscheiden, an welchem Ort diese gespeichert werden sollen. Mit einem Klick auf die grüne Schaltfläche wählt Windows 10 automatisch den Ursprungsort aus. Neuere Datei- oder Ordnerversionen an diesem Ort werden hierdurch automatisch überschrieben. Soll dies nicht geschehen, klicken Sie die grüne Schaltfläche mit der rechten Maustaste an. Wählen Sie nun WIEDERHERSTELLEN IN, und bestimmen Sie den Ordner, in dem die ausgewählte Version gespeichert werden soll.

12.2 Eine Komplettsicherung des Systems vornehmen

Der zuvor vorgestellte Dateiversionsverlauf ist ein solides Tool, um all Ihre Dateien und Ordner zu speichern. Um das gesamte System inklusive Einstellungen, Anwendungen und Daten zu sichern, erstellen Sie am besten ein Systemabbild, auch *Systemimage* genannt. Das Programm, das Windows 10 hierfür vorsieht, war bereits Bestandteil von Windows 7, wie der Zusatz im Namen *Sichern und Wiederherstellen (Windows 7)* deutlich macht. Sobald Sie eine Komplettsicherung durchgeführt haben, können Sie Ihren PC jederzeit in genau diese Konfiguration zurücksetzen, in der sie sich zum Zeitpunkt der Sicherung befand. Im Gegensatz zum Dateiversionsverlauf ist es aber nicht möglich, nur einzelne Elemente wie Dateien aus der Systemabbildsicherung wiederherzustellen. Das Systemabbild ist somit nicht als Backup-Alternative zum Dateiversionsverlauf zu sehen, sondern als sinnvolle Ergänzung.

12.2.1 Ein Systemabbild erstellen

Der neue Computer ist perfekt eingerichtet, alle persönlichen Einstellungen sind vorgenommen. Vor allem aber haben Sie auch den PC von all den überflüssigen Anwendungen befreit, mit denen so manch ein Hersteller seine Geräte vollpflastert, und stattdessen Ihre Lieblingsprogramme installiert. Damit ist der perfekte Zeitpunkt für das Erstellen des ersten Systemabbilds gekommen. Sollte später eine kritische Situation entstehen, können Sie Ihren Computer schnell in genau diesen Zustand zurücksetzen, ohne anschließend wieder all die nervenden Arbeiten des Neueinrichtens durchführen zu müssen. Für die Speicherung des Systemabbilds benötigen Sie eine interne oder externe Festplatte, die im NTFS-Dateisystem formatiert ist. Alternativ können Sie für die Komplettsicherung auch ein freigegebenes Netzwerk wählen.

Um das Systemabbild zu erstellen, rufen Sie in der Einstellungen-App UPDATE UND SICHERHEIT • SICHERUNG auf und klicken auf ZU SICHERN UND WIEDERHERSTELLEN (WINDOWS 7) WECHSELN. Alternativ hierzu können Sie im Suchfeld der Taskleiste auch »sdclt« eingeben und in den Suchergebnissen den entsprechenden Befehl auswählen.

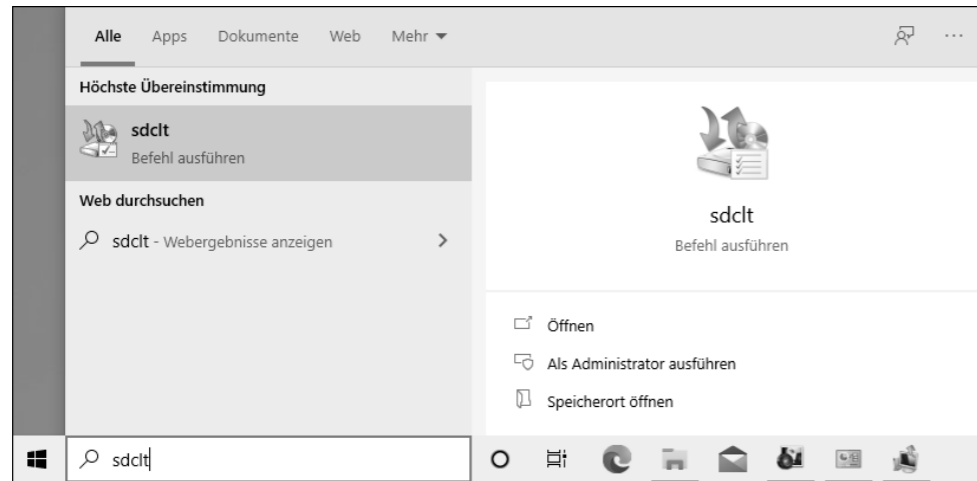


Abbildung 12.9 Die Funktion »Sichern und Wiederherstellen« lässt sich auch über das Suchfeld der Taskleiste starten.

Im Dialog SICHERN UND WIEDERHERSTELLEN (WINDOWS 7) der Systemsteuerung klicken Sie links auf SYSTEMABBILD ERSTELLEN. Als Nächstes legen Sie fest, wo die Sicherung gespeichert werden soll. Zur Auswahl stehen Festplatte, DVD-Laufwerk und Netzwerkadresse. Da auf neueren Computermodellen meist gar kein DVD-Laufwerk mehr vorhanden ist, wird die zweite Option AUF DVD(S) als Speichermedium für einige Anwender gar nicht mehr infrage kommen. Davon abgesehen benötigt ein Systemabbild viel Speicherplatz, sodass meist eine einzelne DVD nicht ausreicht. Eine externe Festplatte oder ein Netzlaufwerk stellen somit den bequemer Weg dar.

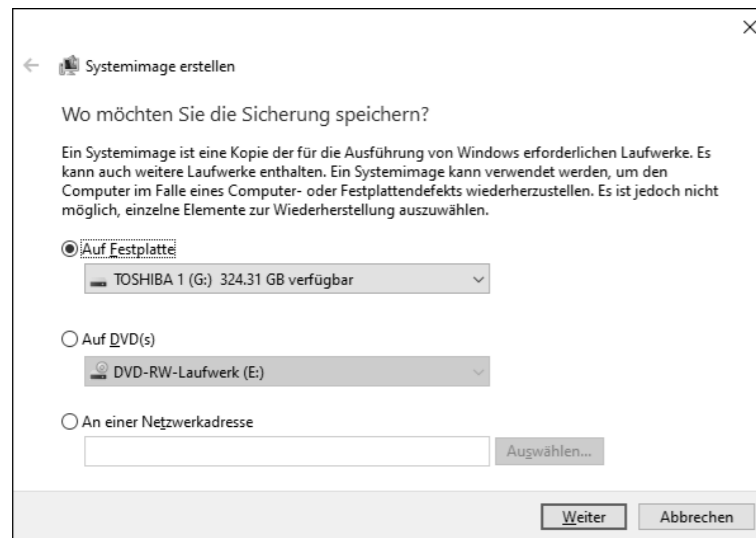


Abbildung 12.10 Bestimmen Sie den Speicherort für das Systemabbild.

Haben Sie bereits eine geeignete Festplatte angeschlossen, wird diese im Feld AUF FESTPLATTE angezeigt. Bestätigen Sie mit WEITER, und bestimmen Sie dann, welche Laufwerke in die Sicherung mit eingeschlossen werden sollen. Das Systemlaufwerk wird von Windows 10 bereits automatisch ausgewählt. Bestätigen Sie Ihre Auswahl mit WEITER und SICHERUNG STARTEN.

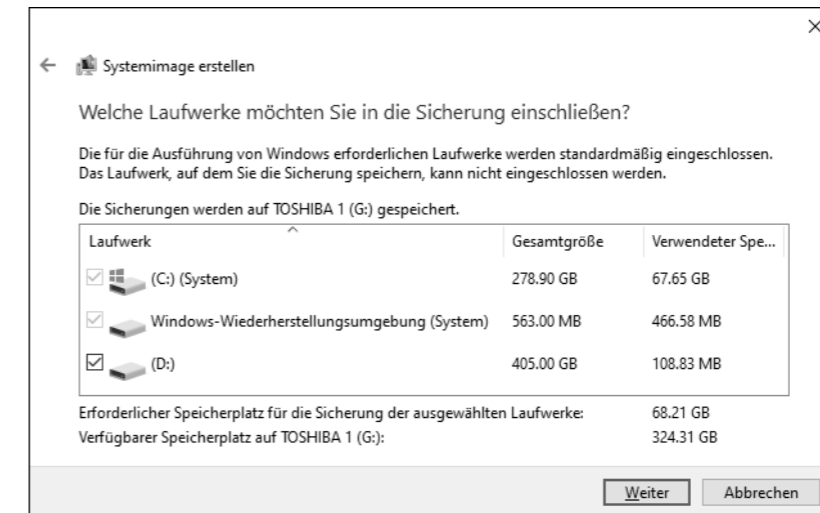


Abbildung 12.11 Das Systemlaufwerk wird von Windows 10 automatisch markiert.

Haben Sie Zugriff auf ein Netzlaufwerk, können Sie auch die Option AN EINER NETZWERK-ADRESSE wählen (siehe Abbildung 12.10). Nach einem Klick auf AUSWÄHLEN werden Sie aufgefordert, die Netzwerkadresse, den Benutzernamen sowie das Kennwort für diese Adresse einzugeben. Die Komplettsicherung stoßen Sie dann ebenfalls mit WEITER und SICHERUNG STARTEN an. Das Systemabbild wird im gewählten Speicherort im Ordner *WindowsImageBackup* abgelegt.

Nach erfolgreicher Sicherung des Systemabbilds bietet Ihnen Windows 10 an, einen Systemreparaturdatenträger zu erstellen. Mit dieser DVD lässt sich ein Computer im Fall der Fälle wieder booten und Windows aus einem gesicherten Systemabbild wiederherstellen. Alternativ hierzu können Sie aber auch – sofern vorhanden – die Windows 10-Installations-CD nutzen. Nähere Informationen hierzu erhalten Sie in Kapitel 32, »Den PC wiederherstellen oder zurücksetzen«.

12.2.2 Ein Systemabbild wiederherstellen

Läuft Ihr Computer nicht mehr rund oder ist das System beschädigt, können Sie ihn auf ein gesichertes Systemabbild zurücksetzen bzw. ein solches wiederherstellen. Sollten Sie die Festplatte aufgrund eines Defekts ausgetauscht haben, achten Sie darauf, dass die neue Festplatte über mindestens so viel Speicherplatz verfügt wie die alte. Ist die neue Festplatte klei-

ner, lässt sich das Systemabbild nicht wiederherstellen, selbst wenn genügend Speicherplatz zur Verfügung stünde. Sollten Sie auf dem Quellsystem mehrere Laufwerke in die Systemabbildsicherung aufgenommen haben, muss auch das Zielsystem über die entsprechende Anzahl verfügen.

Bevor Sie mit der Wiederherstellung beginnen, sollten Sie berücksichtigen, dass alle Änderungen, die Sie seit der Erstellung des Systemabbilds am Computer vorgenommen haben, hierdurch verloren gehen. Das betrifft sowohl vorgenommene Einstellungen, neu installierte Anwendungen als auch alle Änderungen an Dateien und Ordnern.

Um das Systemabbild wiederherzustellen, müssen Sie den Computer über den *Erweiterten Start* neu starten.

1. Rufen Sie in der Einstellungen-App **UPDATE UND SICHERHEIT • WIEDERHERSTELLUNG** auf, und klicken Sie im Bereich **ERWEITERTER START** auf **JETZT NEU STARTEN**. Alternativ hierzu können Sie auch auf das Windows-Logo in der Taskleiste klicken und dann auf **EIN/AUS**. Halten Sie nun die **⇧**-Taste gedrückt, während Sie auf **NEU STARTEN** klicken.



Abbildung 12.12 Die Wiederherstellung einer Systemabbildsicherung muss über den erweiterten Start erfolgen.

Sollte sich der Computer nicht mehr starten lassen, müssen Sie ihn von einem Installationsmedium (z. B. DVD oder USB-Stick) booten. Nach Auswahl der gewünschten Sprache klicken Sie auf **COMPUTERREPARATUROPTIONEN**.



Abbildung 12.13 Während des Windows Setups über ein Installationsmedium wählen Sie die »Computerreparaturoptionen«.

2. Im folgenden Dialog wählen Sie die Option **PROBLEMBEHANDLUNG** aus, klicken auf **ERWEITERTE OPTIONEN** und dann auf **SYSTEMIMAGE-WIEDERHERSTELLUNG**.



Abbildung 12.14 Über die Problembehandlung gelangen Sie zu den erweiterten Optionen, in denen Sie die Systemimage-Wiederherstellung aufrufen.

3. Als Nächstes werden Sie aufgefordert, ein Benutzerkonto auszuwählen und anschließend das Kennwort einzugeben.
4. Liegt das Systemabbild auf einem lokalen Datenträger vor, wird dieses im folgenden Dialog sofort angezeigt. Windows empfiehlt Ihnen, das jüngste verfügbare Systemimage zu verwenden. Entspricht das auch Ihrem Wunsch, bestätigen Sie den Dialog mit **WEITER**.

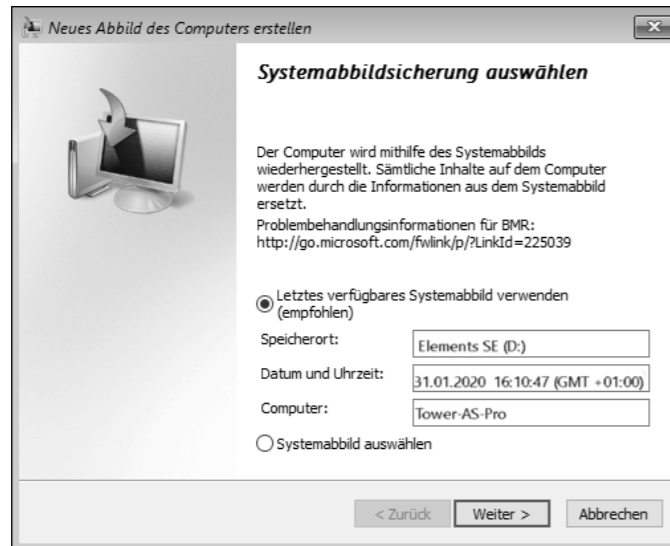


Abbildung 12.15 Wählen Sie das gewünschte Systemabbild aus, das wiederhergestellt werden soll.

5. Falls das Systemabbild auf einem Netzlaufwerk gespeichert wurde oder eine ältere Sicherung von einem lokalen Laufwerk wiederhergestellt werden soll, markieren Sie stattdessen die Option SYSTEMABBILD AUSWÄHLEN und klicken auf WEITER.
6. Sie sehen nun eine Liste mit allen auf dem lokalen Laufwerk vorhandenen Systemabbild-dateien. Wählen Sie das gewünschte Systemimage aus, und bestätigen Sie mit WEITER.
7. Befindet sich das wiederherzustellende Systemabbild auf einem Netzlaufwerk, klicken Sie stattdessen auf ERWEITERT und dann auf IM NETZWERK NACH EINEM SYSTEMABBILD SUCHEN. Nach Eingabe der Netzwerkadresse werden Sie aufgefordert, den Benutzernamen und das Kennwort einzugeben. Wählen Sie dann das gesuchte Systemabbild aus, und bestätigen Sie mit WEITER.
8. Sollte auf dem Datenträger bereits ein Windows-System vorhanden sein, haben Sie nun die Möglichkeit, den Datenträger zu formatieren und neu zu partitionieren. Liegen mehrere Datenträger vor, lässt sich über die Schaltfläche DATENTRÄGER AUSSCHLIESSEN ein Ausschluss veranlassen.
9. Mit einem Klick auf FERTIG STELLEN und JA starten Sie die Wiederherstellung des Systemabbilds.

Kapitel 19

Eine Netzwerkverbindung einrichten

Viele Funktionen von Windows 10 erfordern die Verbindung mit dem Internet oder einem lokalen Netzwerk. In diesem Kapitel lernen Sie, wie einfach die Konfiguration von Netzwerken in Windows 10 erfolgt.

Es gibt wohl kaum einen Windows 10-Computer, der heutzutage nicht über einen Netzwerkadapter verfügt. Dabei kann es sich um einen Ethernet- oder einen WLAN-Adapter handeln. In vielen Mobilgeräten ist gleich beides integriert. Wer seinen Computer per Kabel an den Router anschließt, muss sich meist keine weiteren Gedanken um die Netzwerkverbindung machen, denn Windows 10 konfiguriert diese automatisch. Soll das Gerät mit einem WLAN verbunden werden, muss zumindest der Netzwerkschlüssel eingegeben werden, sofern dieser denn eingerichtet wurde. Wieso dies aus Sicherheitsgründen so wichtig ist und welche weiteren Einstellungen in einem kabelgebundenen oder auch kabellosen Netzwerk vorgenommen werden sollten, erfahren Sie im Verlauf dieses Kapitels. Zuvor werden aber ein paar Grundlagen zum Aufbau eines Netzwerkes beleuchtet, um u. a. Begriffe wie *IPv4*, *IPv6* oder auch *Subgateway* zu erläutern. Diese spielen eine wichtige Rolle bei der Konfiguration eines Netzwerkes.

Ethernet-Adapter für den USB-Anschluss

Bei Notebooks im kleineren Format verzichten die Hersteller immer häufiger auf einen Ethernet-Anschluss. Wer z. B. im Rahmen eines Backups nicht auf die meist schnellere und vor allem stabilere kabelgebundene Netzwerkverbindung verzichten möchte, setzt am besten einen USB-Ethernet-Adapter ein. Berücksichtigen Sie beim Kauf den USB-Anschluss Ihres Mobilgeräts. Verfügt dieses über einen USB 3.0- oder auch USB 3.1-Port (USB-C), lässt sich mit dem entsprechenden Ethernet-Adapter eine Datenübertragungsrate mit bis zu 1 GBit/s (1000 MBit/s) erreichen.

19.1 Ein paar Grundlagen vorweg

Um besser verstehen zu können, welche Einstellungen Sie im Verlauf dieses Kapitels prüfen bzw. selbst vornehmen, möchte ich Sie mit ein paar Begriffen rund um das Thema »Netzwerk« vertraut machen.

Client-Server-Netzwerke

Vereinfacht gesagt sind in einem Netzwerk mindestens zwei oder mehr Computer miteinander oder mit anderen elektronischen Geräten (z. B. Router, Drucker) verbunden, sodass ein Datenaustausch möglich ist. Bei Netzwerken, in denen ein Rechner Ressourcen zur Verfügung stellt, die von anderen Computern in Anspruch genommen werden, spricht man auch von *Client-Server-Netzwerken*. Der Server übernimmt die Rolle des Dienstleisters, die Ressourcen oder auch Funktionen werden von den Clients (Kunden) genutzt. In einem heimischen Netzwerk fungiert z. B. der Router als Server, der anderen Computern (sprich Clients) den Zugang zum Internet ermöglicht.

Die TCP/IP-Protokollfamilie

Die Kommunikation zwischen den Geräten wird durch die Netzwerkprotokolle reguliert. Das Internet basiert auf der sogenannten *TCP/IP-Protokollfamilie*. Die Abkürzung TCP steht für *Transmission Control Protocol*, IP wiederum für *Internet Protocol*. Die Bezeichnung *TCP/IP* wird als Überbegriff für die gesamte Protokollfamilie verwendet, zu der aber auch Protokolle wie HTTP (*Hypertext Transfer Protocol*), FTP (*File Transfer Protocol*) oder auch IMAP (*Internet Message Access Protocol*) zählen. Die Protokollfamilie ist von der Hard- und Software unabhängig und steht in allen gängigen Betriebssystemen zur Verfügung. Das gilt natürlich auch für Windows 10. Sie sorgt für einheitliche Kommunikationsstandards und regelt die Adressierung im Netzwerk.

Das TCP/IP-Referenzmodell

Wie Anwendungen, Netzwerkprotokolle und Hardware zusammenspielen, lässt sich anhand von Schichtenmodellen verdeutlichen. Für die TCP/IP-Protokollfamilie dient das TCP/IP-Referenzmodell, in dem vier Schichten unterschieden werden:

- ▶ **Anwendungsschicht:** Die Anwendungsschicht stellt die Schnittstelle für Anwendungen dar, die einen Zugriff auf das Netzwerk benötigen. Hier kommen Protokolle wie HTTP, HTTPS oder FTP zum Einsatz.
- ▶ **Transportschicht:** Die Transportschicht stellt eine Ende-zu-Ende-Verbindung her. Das wichtigste Protokoll dieser Schicht ist das Transmission Control Protocol (TCP), das Verbindungen zwischen jeweils zwei Netzwerkteilnehmern zum zuverlässigen Versenden von Datenströmen herstellt.
- ▶ **Internetschicht:** Die Internetschicht ist für die Weitervermittlung von Paketen und die Wegwahl (Routing) zuständig. Das hierfür zuständige Protokoll ist das Internet Protocol, kurz IP.
- ▶ **Netzwerkschicht:** Die Netzwerkschicht ist zwar im TCP/IP-Referenzmodell spezifiziert, sie enthält aber keine Protokolle der TCP/IP-Protokollfamilie. Sie dient als Platzhalter für die verschiedenen Techniken (z. B. WLAN oder auch Ethernet) zur Datenübertragung zwischen mehreren Punkten.

Die Kommunikation erfolgt nicht zwischen den Schichten einer Ebene (also etwa von Anwendungsschicht zu Anwendungsschicht), sondern von der Anwendungsschicht nach unten zur Netzwerkschicht, dann zum Übertragungsmedium und von dort aus wieder von der Netzwerkschicht nach oben bis zur Anwendungsschicht.

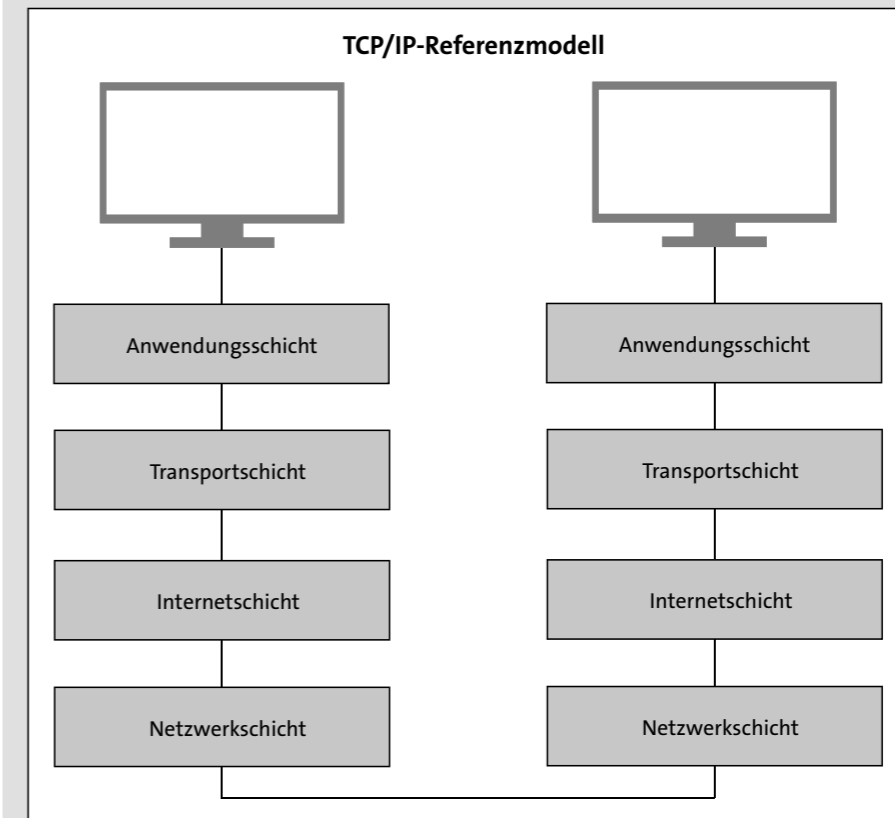


Abbildung 19.1 Das TCP/IP-Referenzmodell

Netzwerkadressen zur eindeutigen Identifikation

Damit die Kommunikation zwischen zwei Geräten (z. B. Computer oder auch Drucker) in einem Netzwerk funktioniert, müssen diese eindeutig identifizierbar sein. Dies geschieht mithilfe der IP-Adresse, die jedem Gerät (dem sogenannten *Host*) eindeutig zugewiesen wird. Das Internet Protocol ist mittlerweile in zwei verschiedenen Versionen verfügbar: IPv4 und IPv6. Entsprechend gibt es auch zwei verschiedene Adressversionen, nämlich die bereits seit längerem verfügbaren IPv4-Adressen und die neueren IPv6-Adressen.

IPv4-Adressen bestehen aus 32 Ziffern und ermöglichen somit die Generierung von 4,3 Milliarden IP-Adressen. Diese Zahl klingt zunächst immens. Im Gegensatz zu früher steigt aber auch die Zahl der internetfähigen Geräte: So lassen sich mittlerweile nicht nur Computer

oder Smartphones mit dem Internet verbinden, sondern auch Fernseher, Kühlschränke, Autos und vieles mehr. IPv6-Adressen sollen das Problem der Adressknappheit zukünftig lösen. Hier besteht jede Adresse aus 128 Stellen, woraus sich ca. 340 Sextillionen (das ist eine 340 mit 36 Nullen) Adressen ergeben.

IPv4-Adressen werden dezimal dargestellt. Die 32 Zeichen werden in Gruppen zu je 8 gruppiert, den sogenannten *Oktetts*, die durch Punkte voneinander getrennt werden. Jedes Oktett kann dabei Werte zwischen 0 und 254 annehmen (z. B. 192.168.254.254). Für IPv6-Adressen wird die hexadezimale Darstellung gewählt, wobei jeweils vier Hexadezimalstellen zu einem Block gruppiert werden. Die Trennung der Blöcke erfolgt hier durch Doppelpunkte (z. B. 2001:0cb7:81a3:08a3:1319:7a1b:0351:6132).

Ein wichtiger Aspekt in der TCP/IP-Konfiguration sind die Subnetze, die zusammengehörende, aufeinanderfolgende IPv4-Adressen zusammenfassen. Um ein Gerät innerhalb eines IPv4-Netzwerkes identifizieren zu können, muss auch das Subnetz bekannt sein. Dies wird mithilfe der *Subnetzmaske* ermittelt. Anhand der Subnetzmaske lässt sich bestimmen, ob sich der Host im lokalen Subnetz oder in einem anderen Netzwerk befindet. Das Pendant zu den Subnetzmasken sind bei IPv6-Adressen die *Präfixe*, die eingesetzt werden, um ein Netzwerk eindeutig zu definieren.

Möchte ein Computer mit einem Gerät in einem anderen Netzwerk kommunizieren, geschieht dies im Normalfall über einen Router. Dieser wird in der TCP/IP-Terminologie als *Standardgateway* bezeichnet. Das Standardgateway stellt quasi die Verbindungsstelle zwischen Ihrem privaten Netzwerk und dem Internet dar. Der Router ist im Internet mit einer öffentlichen IP-Adresse sichtbar, die ihm von Ihrem Internetprovider zugeordnet wird. *DNS-Server* sorgen für die Übersetzung von IP-Adressen in Domainnamen (z. B. www.rheinwerk-verlag.de oder auch www.google.de). DNS ist die Abkürzung für *Domain Name System*.

19.2 Das Netzwerk konfigurieren

Wie in den Grundlagen bereits erwähnt, verfügt jedes Gerät in einem Netzwerk über eine eindeutige IP-Adresse. Dabei kann es sich um eine dynamisch erzeugte Adresse handeln oder um eine statische Adresse.

19.2.1 Dynamische IP-Adressvergabe per DHCP

In den meisten Routern ist heutzutage ein DHCP-Server integriert, der einen Pool an IP-Adressen für alle Geräte verwaltet, die im Netzwerk erreichbar sein müssen. *DHCP* ist die Abkürzung für *Dynamic Host Configuration Protocol*. Sobald der Computer per Kabel oder auch drahtlos an den Router angeschlossen wird, übernimmt dieser Server automatisch die Vergabe der IP-Adresse sowie die Zuordnung zu einer Subnetzmaske und weiteren Einstellungen. Sie selbst müssen sich im Grunde genommen um nichts mehr kümmern.

Der DHCP-Server sollte im Router normalerweise per Standardeinstellung aktiviert sein. Sie können dies natürlich überprüfen, wie im Folgenden exemplarisch für die FRITZ!Box gezeigt wird.

1. Rufen Sie zunächst über den Browser die Webadresse <http://fritz.box> auf. Alternativ hierzu können Sie auch die IP-Adresse 192.168.178.1 eingeben. Melden Sie sich bei der FRITZ!Box mit dem entsprechenden Kennwort für den Router an.
2. Nach erfolgreicher Anmeldung klicken Sie in der linken Spalte nacheinander auf HEIMNETZ • NETZWERK. Wechseln Sie rechts in das Register NETZWERKEINSTELLUNGEN.
3. Blättern Sie nun nach unten bis zum Bereich IP-ADRESSEN. Hier klicken Sie auf IPv4-ADRESSEN.
4. Stellen Sie sicher, dass das Kontrollkästchen DHCP-SERVER AKTIVIEREN mit einem Häkchen versehen ist. Darunter führt die FRITZ!Box den Adressbereich auf, aus dem die IP-Adressen für die verschiedenen Geräte im lokalen Netzwerk vergeben werden. Hier sollten Sie keinerlei Änderungen vornehmen. Schließen Sie den Dialog mit OK, und melden Sie sich wieder bei der FRITZ!Box ab.

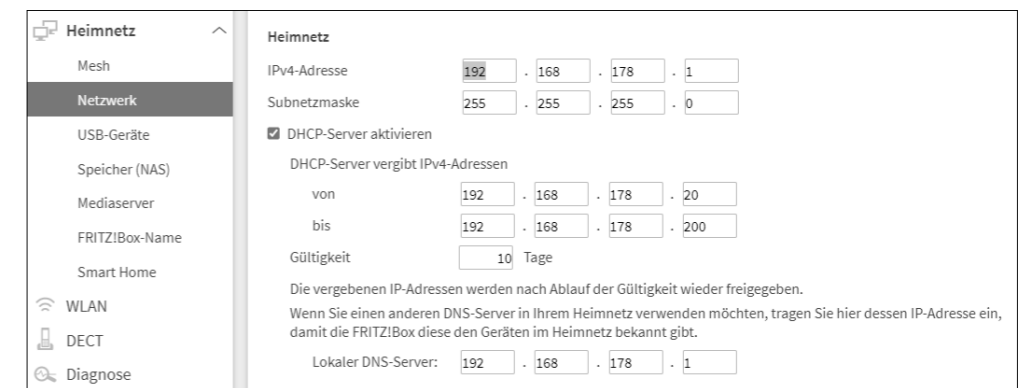


Abbildung 19.2 Aktivieren des DHCP-Servers in der FRITZ!Box

Der Windows 10-Computer ist im Normalfall so eingestellt, dass er die IP-Adresse automatisch per DHCP vom Router bezieht. Um dies zu überprüfen, öffnen Sie die Einstellungen-App z. B. über die Tastenkombination **Windows + I** und rufen die Kategorie NETZWERK UND INTERNET auf. In der Unterkategorie STATUS wird der Verbindungstyp angezeigt – also Ethernet oder auch WLAN. Klicken Sie direkt darunter auf die Schaltfläche EIGENSCHAFTEN. Blättern Sie auf der folgenden Seite nach unten, sehen Sie unter IP-EINSTELLUNGEN, ob die IP-Zuweisung AUTOMATISCH PER DHCP erfolgt. Ist hier MANUELL eingestellt, obwohl Sie DHCP bevorzugen, können Sie die Einstellung über die Schaltfläche BEARBEITEN korrigieren. Im Bereich EIGENSCHAFTEN der Seite NETZWERK sehen Sie die IP-Adressen, die dem Computer aktuell zugeordnet sind.



Abbildung 19.3 Übersicht über die IP-Einstellungen und Eigenschaften eines Ethernets in der Einstellungen-App

Diese Netzwerkdaten können Sie sich übrigens auch in der Windows PowerShell über den Befehl `ipconfig /all` anzeigen lassen. Das Befehlszeilentool rufen Sie über die Tastenkombination **Windows** + **X** und dann Auswahl von **WINDOWS POWERSHELL** auf.

19.2.2 Statische IP-Adressen zuweisen

Der Vorteil von dynamischen IP-Adressen ist, dass Sie sich um nichts kümmern müssen, da dem Computer die Adresse automatisch über den DHCP-Server zugewiesen wird. Diese Adressen werden allerdings regelmäßig ausgetauscht und sind somit nicht über einen längeren Zeitraum hinweg gültig. Möchten Sie, dass der Computer auch von außerhalb für andere Computer immer über die gleiche IP-Adresse erreichbar ist, müssen Sie ihm eine statische IP-Adresse zuweisen. Ein Tipp: Nutzen Sie zunächst die Möglichkeit des DHCP-Servers, um dem Computer eine dynamische IP-Adresse zuzuweisen. Lassen Sie sich dann wie im vorherigen Abschnitt beschrieben über den Befehl `ipconfig /all` in der Windows PowerShell die aktuelle Netzwerkkonfiguration anzeigen. Notieren Sie sich alle wichtigen Angaben wie IP-Adresse, Subnetzmaske, Standardgateway und mindestens einen DNS-Server. Diese Daten können Sie nun für die Zuweisung der statischen IP-Adresse nutzen:

1. Rufen Sie **EINSTELLUNGEN • NETZWERK UND INTERNET • STATUS** auf, und klicken Sie rechts auf **ADAPTEROPTIONEN ÄNDERN**.
2. Im folgenden Dialog klicken Sie mit der rechten Maustaste auf die Netzwerkverbindung, die Sie konfigurieren möchten, und im Kontextmenü auf **EIGENSCHAFTEN**.
3. Markieren Sie das Element **INTERNETPROTOKOLL.VERSION 4(TCP/IPV4)**, und klicken Sie dann auf **EIGENSCHAFTEN**.
4. Aktivieren Sie die Option **FOLGENDE IP-ADRESSE VERWENDEN**. In den folgenden Feldern geben Sie die IP-Adresse, die Subnetzmaske und das Standardgateway an.
5. Aktivieren Sie außerdem die Option **FOLGENDE DNS-SERVERADRESSEN VERWENDEN**, und geben Sie die Adresse mindestens eines DNS-Servers an.
6. Beenden Sie die geöffneten Dialoge mit **OK** und **SCHLIESSEN**.

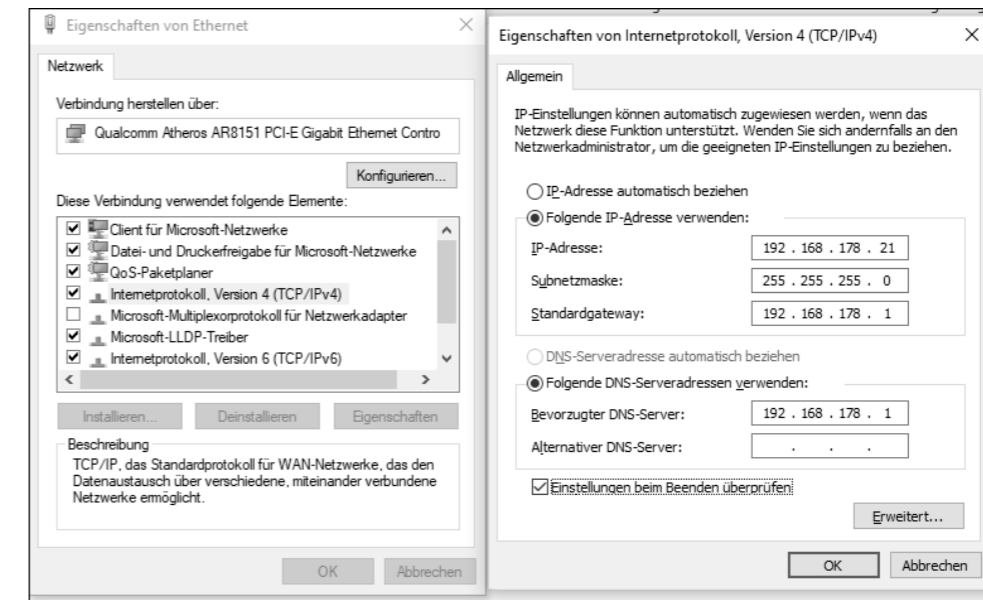


Abbildung 19.4 Vergabe einer statischen IPv4-Adresse

Analog hierzu können Sie auch die Eigenschaften für das **INTERNETPROTOKOLL, VERSION 6 (TCP/IPV6)** ändern. Sie müssen lediglich in Schritt 3 das gleichnamige Element markieren. In Schritt 4 ist zudem die Angabe der Subnetzpräfixlänge nötig.

Adresszuordnung via APIPA

Ein Computer erhält seine IP-Adresse im Normalfall entweder dynamisch über einen DHCP-Server, oder es wird eine statische IP-Adresse festgelegt. Ist in Ihrem Netzwerk kein DHCP-Server verfügbar und fand auch die statische Zuordnung nicht statt, weist Windows dem Gerät automatisch eine private IP-Adresse aus dem privaten Adressbereich 169.254.0.0 bis

169.254.255.255 zu. Diese Vergabe von IP-Adressen wird *Automatic Private IP Addressing*, kurz *APIPA*, genannt. Die private IP-Adresse ermöglicht es dem Computer, im lokalen Netzwerk mit anderen Geräten zu kommunizieren.

19.3 Verbindung mit einem WLAN herstellen

Nicht jeder schätzt den Kabelsalat eines Ethernets, und so ist es nicht verwunderlich, dass sich Funknetzwerke auch in den eigenen vier Wänden einer großen Beliebtheit erfreuen. Die meisten modernen Router stellen heutzutage eine Kombination aus WLAN Access Point, Switch und eigentlichem Router dar, mit denen das Heimnetzwerk in wenigen Minuten eingerichtet ist. Wer sich einen neuen WLAN-Router zulegen möchte, sollte darauf achten, dass dieser mindestens nach dem Standard IEEE 802.11n arbeitet, der eine maximale Übertragungsgeschwindigkeit von 600 MBit/s sowie eine höhere Reichweite als sein Vorgänger IEEE 802.11g bietet. Erreicht wird dies durch mehrere Antennen und Signalverarbeitungseinheiten (MIMO), die Verdopplung der Funkkanal-Bandbreite auf 40 MHz, sowie die parallele Nutzung des 2,4- und 5-GHz-Frequenzbandes. Wer auch für die Zukunft optimal gerüstet sein möchte, setzt sogar auf den Standard IEEE 802.11ac (manchmal auch *5G Wifi* genannt), der eine maximale theoretische Übertragungsgeschwindigkeit im Gigabit-Bereich erreicht.

19.3.1 WLAN und die Sicherheit

Die Einrichtung eines WLAN-Routers ist mittlerweile kein großes Hexenwerk mehr. Schon nach wenigen Minuten steht die Verbindung zum Internet, und es können die WLAN-Geräte verbunden werden. Das bequeme Vorgehen verführt allerdings viele Anwender dazu, sich keine weiteren Gedanken um die Konfiguration des Routers zu machen, sondern einfach die Werkseinstellungen beizubehalten. Genau diese stellen aber ein großes Sicherheitsrisiko dar. Gelingt Cyberkriminellen über eine Sicherheitslücke z. B. der Zugriff auf den Router, stehen ihm damit auch alle angeschlossenen Geräte offen. Manch einen Angriff bekommt der Anwender mit, etwa wenn die Telefonrechnung überraschend um ein Vielfaches teurer ist als gewohnt. Manche Attacken bleiben aber auch vollkommen unbemerkt, etwa wenn der eigene PC plötzlich Teil eines sogenannten *Botnetzes* wird. Hierbei werden Tausende von Computern, die mit einem speziellen Schadprogramm infiziert wurden, zu einem Netzwerk zusammengeschlossen. Das Botnetz nutzt die Rechenleistung und Daten des infizierten Computers, ohne dass dessen Besitzer Kenntnis davon hat, geschweige denn seine Einwilligung hierfür erteilt hat. Ist ein Computer erst einmal Teil eines Botnetzes, wird er häufig für illegale Zwecke wie etwa das Versenden von Spam-Mails eingesetzt. Dieser illegale Einsatz ist vor allem deshalb für Sie fatal, da Sie für alles haften (legal oder illegal), was über Ihre Internetverbindung geschieht.

Bevor Sie Ihre Geräte mit dem WLAN verbinden, sollten Sie deshalb unbedingt einige Sicherheitseinstellungen des Funknetzwerkes anpassen, um das Funknetz vor Angriffen von außen zu schützen. Mit ein paar Kniffen lässt sich hier bereits viel erreichen – worum es sich dabei im Einzelnen dreht, werde ich Ihnen direkt im Folgenden erläutern.

Vergeben Sie einen eigenen Namen für das WLAN

Jedes Funknetzwerk, also auch Ihr eigenes privates WLAN, verfügt über einen Namen, die sogenannte *SSID* (Abkürzung für *Service Set Identifier*). Hersteller wie AVM vergeben hier per Werkseinstellung meist den Namen des Routers, also z. B. *FRITZ!Box 4790*. Anhand dieses Namens lässt sich leider häufig auch das per Werk vergebene Passwort in Erfahrung bringen. Ein erster Schritt, das eigene WLAN sicherer zu machen, besteht somit darin, die SSID zu ändern. Achten Sie bei der Wahl des Namens darauf, dass keinesfalls der Name des Routers auftaucht, geschweige denn Ihr Name, die Straße oder auch Hausnummer. Wählen Sie außerdem keinen Namen, der bereits für ein Funknetz in der Nachbarschaft vergeben wurde.

Abbildung 19.5 Vergeben Sie einen eigenen Namen für Ihr WLAN.

Funknetzname unsichtbar machen

Immer wieder hört man den Ratschlag, den Namen eines WLANs unsichtbar zu machen. Denn was man nicht sieht, kann man angeblich auch nicht finden. Dieser Tipp mag geeignet sein, um das WLAN vor neugierigen Nachbarn zu verstecken. Die Umsetzung ist auch schnell erfolgt: Wie man in Abbildung 19.5 am Beispiel einer FRITZ!Box sieht, reicht es, das Häkchen vor **NAME DES WLAN-FUNKNETZES SICHTBAR** zu entfernen. Ein Profi, der über das nötige Spähprogramm verfügt, lässt sich von diesem simplen Trick allerdings nicht abhalten!

Das Passwort des WLANs ändern

Drehen Sie Ihren WLAN-Router einmal um, werden Sie auf seiner Rückseite häufig das Passwort finden, das zur Anmeldung beim WLAN benötigt wird. Was Sie selbst können, ist finden Nachbarn ebenfalls möglich. Damit diese sich nicht ungefragt an Ihrem Funknetzwerk anmelden können, sollten Sie das Passwort (auch *WLAN-Netzwerkschlüssel* genannt) also unbedingt durch ein eigenes, möglichst komplexes Passwort ersetzen. Bei einer FRITZ!Box darf dieses z. B. zwischen 8 und 63 Zeichen lang sein und aus einer Kombination von Ziffern, Groß- und Kleinbuchstaben sowie Sonderzeichen bestehen.

WPA- statt WEP-Verschlüsselung wählen

Die Datenübertragung sollte im WLAN unbedingt verschlüsselt erfolgen. Die teilweise in älteren Routermodellen noch zur Verfügung stehende WEP-Verschlüsselung ist extrem unsicher und sollte daher nicht mehr verwendet werden. In neueren Modellen steht sie meist gar nicht mehr zur Auswahl. Stellen Sie hier am besten den als sehr sicher geltenden WPA2 (CCMP) ein. Bei dieser Verschlüsselungsmethode kommt der AES-Verschlüsselungsalgorithmus mit einer Schlüssellänge von bis zu 256 Bit zum Einsatz.



Abbildung 19.6 Die WPA-Verschlüsselung in Kombination mit einem komplexen WLAN-Netzwerkschlüssel bietet eine hohe Sicherheit.

Firmware auf dem aktuellsten Stand halten

Nicht nur Microsoft versorgt Windows 10 regelmäßig mit Updates. Auch die Hersteller von Routern veröffentlichen neue Versionen der Firmware (sprich des Betriebssystems des Routers). Diese enthalten nicht nur neue Funktionen, sondern auch Fehlerbehebungen, was vor allem im Zusammenhang mit dem Schließen von Sicherheitslücken wichtig ist. Achten Sie daher unbedingt darauf, dass die Firmware Ihres Routers immer auf dem neuesten Stand ist. Sollte für Ihren Router der Fernzugriff aktiviert sein, überlegen Sie sich, ob Sie diesen wirklich benötigen. Es mag zwar praktisch sein, unterwegs vom Smartphone aus auf eine an die FRITZ!Box angeschlossene USB-Festplatte zuzugreifen, doch was Ihnen möglich ist, könnte auch Angreifern gelingen.

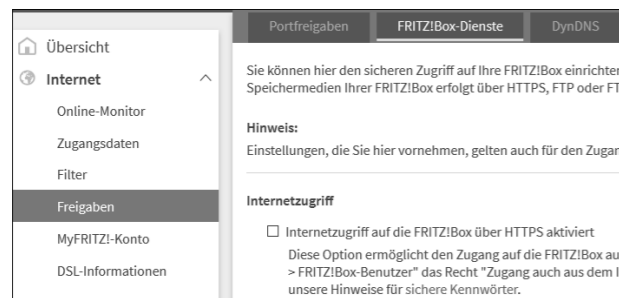


Abbildung 19.7 Wer den Fernzugriff (in der FRITZ!Box »Internetzugriff« genannt) auf den Router nicht unbedingt benötigt, sollte ihn deaktivieren.

Diese kleinen Kniffe umzusetzen dauert nicht lange. Sie erreichen damit aber bereits einiges, um die Sicherheit des eigenen WLANs zu verbessern.

19.3.2 Mit WLAN verbinden

Ist Ihr Computer mit einem WLAN-Adapter ausgestattet und ist dieser auch eingeschaltet, begibt sich Windows 10 automatisch auf die Suche nach Drahtlosnetzwerken in der Nähe. Funknetzwerke finden sich fast überall – sei es in der Firma, bei Freunden, am Flughafen, in Hotels oder auch Restaurants. Es ist daher nur eine Frage von Sekunden, bis Windows fündig wird und Sie die Verbindung zum WLAN herstellen können.

Verbindung mit einem gesicherten, sichtbaren WLAN herstellen

Um eine Verbindung zum WLAN herzustellen, klicken Sie auf das Netzwerksymbol im Infobereich der Taskleiste. Sollte der WLAN-Adapter ausgeschaltet sein, erscheint ein entsprechender Hinweis. Ein Klick auf die Schaltfläche WLAN reicht, um ihn einzuschalten. Sie erhalten nun eine Übersicht über alle verfügbaren Netzwerke – auch die kabelgebundenen, falls der Computer bereits per Kabel mit dem Ethernet verbunden ist. Die kabellosen Netzwerke werden nach Signalstärke sortiert aufgelistet. Die Anzahl der wellenförmigen Linien im WLAN-Symbol geben Aufschluss darüber, wie stark das Signal ist.

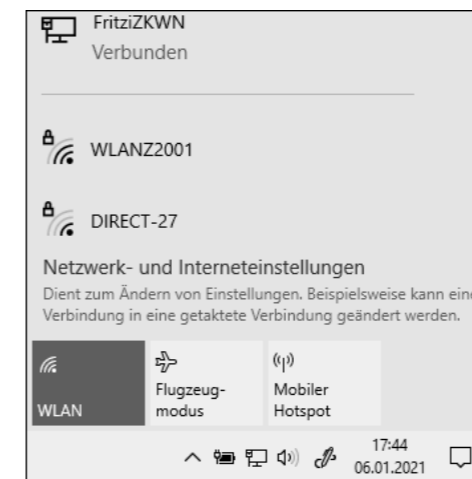


Abbildung 19.8 Übersicht über verfügbare Netzwerke. Es besteht bereits eine Verbindung zu einem Ethernet.

Wählen Sie das WLAN, mit dem Sie die Verbindung herstellen möchten, per Mausklick aus. Um nicht immer wieder den Netzwerksicherheitsschlüssel eingeben zu müssen, der kurz darauf angefordert wird, sollten Sie das Kästchen AUTOMATISCH VERBINDEN aktivieren. Klicken Sie anschließend auf VERBINDEN.

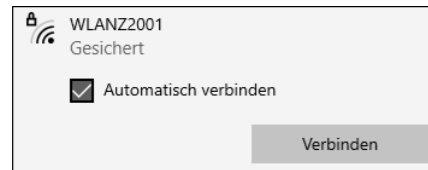


Abbildung 19.9 Nutzen Sie das WLAN häufiger, aktivieren Sie »Automatisch verbinden«, um nicht immer wieder den Netzwerksicherheitsschlüssel eingeben zu müssen.

Geben Sie als Nächstes den Netzwerksicherheitsschlüssel ein. Diesen haben Sie im Idealfall selbst vergeben, falls es sich bei dem WLAN um Ihr eigenes handelt. Sollten Sie unterwegs sein, müssen Sie den Betreiber des WLANs bitten, Ihnen diesen zu geben. Gerade bei komplexen Kennwörtern ist es sinnvoll, sich diese im Klartext anzeigen zu lassen, um die korrekte Eingabe überprüfen zu können. Klicken Sie hierzu auf das Augensymbol am rechten Rand des Eingabefeldes. Haben Sie sich nicht vertippt, bestätigen Sie mit WEITER. Wenn Sie sich das erste Mal bei diesem WLAN anmelden, müssen Sie nun festlegen, ob andere Geräte innerhalb des Netzwerkes gefunden werden dürfen. Im eigenen Netzwerk oder Firmennetzwerk können Sie diese Frage mit JA beantworten. Damit ist zugleich die erste Weiche gestellt, um später Dateien und Ordner zwischen verschiedenen Geräten im Netzwerk freigeben zu können. In einem öffentlichen Netzwerk sollten Sie aus Sicherheitsgründen unbedingt mit NEIN ablehnen.

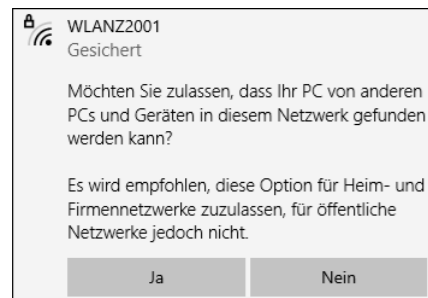


Abbildung 19.10 Handelt es sich bei dem Netzwerk um Ihr privates WLAN oder das Firmennetzwerk, können Sie die Freigabe mit »Ja« erteilen.

Windows 10 stellt nun die Verbindung zum WLAN her. Klicken Sie auf das Netzwerksymbol im Infobereich der Taskleiste, sollte als Status beim Namen des WLANs VERBUNDEN erscheinen.

Manuelle Verbindung zu einem versteckten WLAN herstellen

Im Normalfall sendet jedes Funknetzwerk seinen WLAN-Namen, also die im vorherigen Abschnitt bereits näher definierte SSID. Anhand dieses Namens können Sie das gewünschte WLAN in der Übersicht der Netzwerke auswählen, die Windows 10 Ihnen nach einem Klick

auf das Netzwerksymbol im Infobereich der Taskleiste einblendet. Wurde die SSID vom Betreiber des Funknetzwerkes versteckt, erscheint das WLAN nicht in dieser Liste. Wenn Sie dennoch eine Verbindung zu solch einem versteckten Netzwerk herstellen möchten, müssen Sie die SSID sowie die Sicherheitseinstellungen kennen. Ist dies der Fall, geben Sie diese Daten manuell ein. Klicken Sie hierzu mit der rechten Maustaste auf das Netzwerksymbol im Infobereich der Taskleiste, und wählen Sie NETZWERK- UND INTERNETEINSTELLUNGEN ÖFFNEN. Hierdurch wird die Einstellungen-App mit der Kategorie NETZWERK UND INTERNET geöffnet, in der Sie nun links WLAN markieren. Klicken Sie jetzt rechts auf BEKANNTE NETZWERKE VERWALTEN und auf der folgenden Seite auf NEUES NETZWERK HINZUFÜGEN. Im gleichnamigen Dialog geben Sie nun den Netzwerknamen ein und wählen die Verschlüsselungsmethode aus, die für das WLAN eingestellt wurde. Anschließend erscheint das Feld zur Eingabe des Sicherheitsschlüssels, in dem Sie den Netzwerksicherheitsschlüssel eintragen. Versehen Sie die Kästchen AUTOMATISCH VERBINDEN und VERBINDEN, AUCH WENN DIESES NETZWERK NICHT ÜBERTRÄGT jeweils mit einem Häkchen. Damit stellen Sie sicher, dass die Verbindung zum WLAN hergestellt wird, sobald es verfügbar ist. Mit einem Klick auf SPEICHERN schließen Sie die manuelle Einrichtung ab.

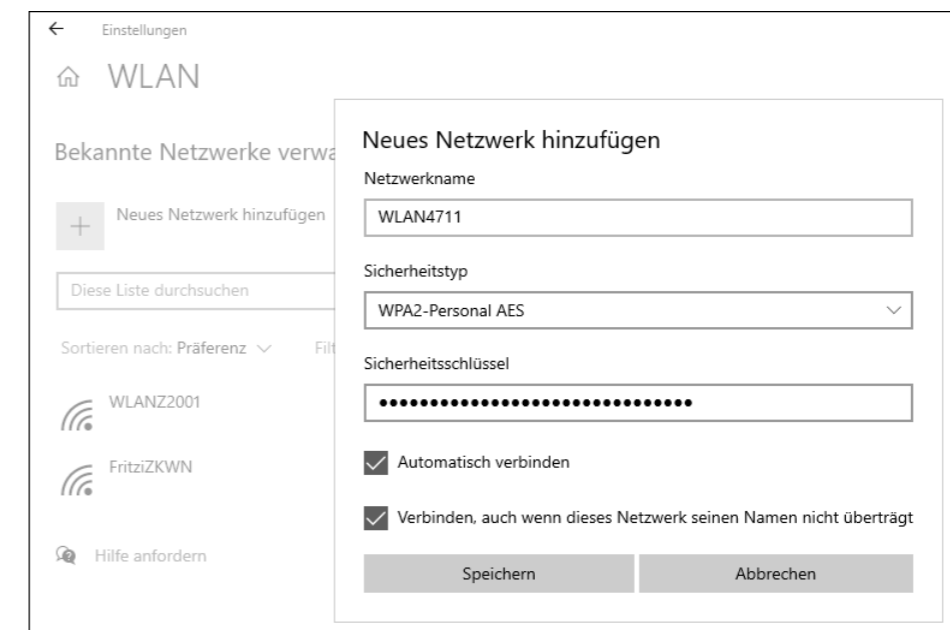


Abbildung 19.11 Manuelle Einrichtung eines Funknetzwerkes, das seine SSID nicht sendet.

Funknetzwerke vorübergehend trennen

Wenn Sie mit dem Flugzeug reisen, werden Sie aufgefordert, während des Starts und der Landung alle Funkverbindungen Ihrer Mobilgeräte auszuschalten. Auf dem Windows 10-Gerät sind hierfür lediglich zwei Mausklicks bzw. Fingertipps nötig. Der erste führt auf das Netz-

werksymbol im Infobereich der Taskleiste. Am unteren Rand des aufklappenden Dialogs sehen Sie nun die Schaltfläche FLUGZEUGMODUS. Ein Klick darauf, und es werden automatisch alle drahtlosen Funknetzwerke wie WLAN, Mobilfunk oder auch Bluetooth auf dem Gerät deaktiviert. Ist die Kommunikation mit den Funknetzwerken wieder erlaubt, klicken Sie auf das Flugzeugsymbol im Infobereich der Taskleiste und dann auf FLUGZEUGMODUS.

Gerade unterwegs hat man nicht immer das Glück, ein gleichbleibend stabiles und starkes Funksignal zu haben. Bricht das Signal zwischendurch sogar ganz ab, wirkt sich dies besonders negativ auf den Akku aus, da das Windows-Gerät immer wieder versucht, eine Verbindung zum WLAN herzustellen. Benötigen Sie die WLAN-Verbindung nicht unbedingt, ist es durchaus sinnvoll, diese vorübergehend auszuschalten. Hierzu klicken Sie auf das Netzwerksymbol im Infobereich der Taskleiste und anschließend auf die blaue Schaltfläche WLAN. Über das Feld WLAN ERNEUT AKTIVIEREN können Sie nun einstellen, ob Sie das WLAN später selbst einschalten möchten oder ob Windows dies für Sie nach 1 STUNDE, 4 STUNDEN oder 1 TAG übernehmen soll. Entscheiden Sie sich für MANUELL, klicken Sie zum Aktivieren auf das Netzwerksymbol und dann auf WLAN. Dies gilt natürlich auch, wenn Sie das WLAN vor Ablauf der vorgegebenen Zeit selbst wieder einschalten möchten.

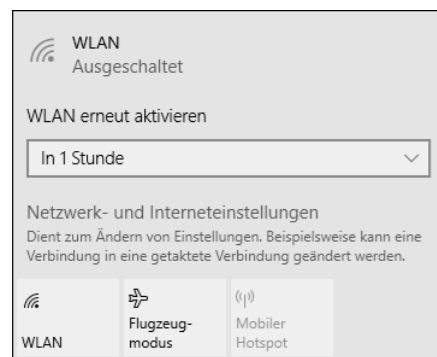


Abbildung 19.12 Über die Schaltfläche »WLAN« deaktivieren Sie nur die WLAN-Verbindung, mit »Flugzeugmodus« werden jegliche Funkverbindungen des Geräts ausgeschaltet.

19.3.3 Besonderheiten von mobilen Hotspots

Viele Smartphones bieten mittlerweile die Möglichkeit, die eigene Mobilfunkverbindung anderen Geräten wie etwa Tablets oder Computern zur Verfügung zu stellen, sodass diese ebenfalls eine Verbindung zum Internet herstellen können. Das ist vor allem unterwegs praktisch, wenn Sie z. B. mit Ihrem Notebook arbeiten müssen, aber kein WLAN zur Verfügung steht. Solch eine gemeinsame Nutzung einer Datenverbindung wird *Tethering* genannt. Das Gerät, das die Verbindung zur Verfügung stellt, bezeichnet man als *Hotspot*. Sie können natürlich auch umgekehrt Ihren Windows 10-Computer zum mobilen Hotspot machen, indem Sie die Internetverbindung für andere Geräte freigeben. Beide Varianten werden im Folgenden beschrieben.

Verbindung zu einem mobilen Hotspot herstellen

Wie Ihr eigenes Smartphone oder natürlich auch das einer anderen Person zum mobilen Hotspot wird, ist von Gerät zu Gerät unterschiedlich. Wichtigste Voraussetzung ist, dass der Mobilfunkvertrag eine solche Funktion auch beinhaltet. Informieren Sie sich zur Sicherheit bei Ihrem Mobilfunkanbieter, denn einige Anbieter beschränken das Tethering oder berechnen zusätzliche Gebühren. Lässt der Mobilfunkvertrag das Tethering zu, erfolgt die Aktivierung auf dem Smartphone über die Einstellungen, in denen Sie die Verbindungseinstellungen aufrufen und dort eine Funktion namens MOBILER HOTSPOT (Android) oder PERSÖNLICHER HOTSPOT (iPhone und iPad) einschalten. Gegebenenfalls müssen Sie erneut auf die jeweilige Schaltfläche tippen, um sich die Verbindungsdaten wie den Name des WLAN Access Points und das Passwort anzeigen zu lassen. Diese Daten benötigen Sie, um von Ihrem Windows 10-Gerät aus eine Verbindung zum Smartphone herstellen zu können.

Auf dem Windows 10-Gerät erfolgt die Anmeldung beim mobilen Hotspot wie bereits in Abschnitt 19.3.2 für ein klassisches WLAN beschrieben. Klicken Sie also auf das Netzwerksymbol im Infobereich der Taskleiste, und stellen Sie sicher, dass WLAN aktiviert ist. Der mobile Hotspot wird nun zusätzlich zu allen anderen in Reichweite befindlichen Netzwerken aufgelistet. Markieren Sie ihn. Im Gegensatz zum klassischen WLAN empfiehlt es sich beim Hotspot, das Kontrollkästchen AUTOMATISCH VERBINDEN nicht zu aktivieren. So stellen Sie sicher, dass nicht versehentlich eine Verbindung zwischen Smartphone und Computer hergestellt wird, falls Sie vergessen sollten, die Funktion später auf dem Smartphone zu deaktivieren. Es können sonst schnell unnötige Kosten entstehen.

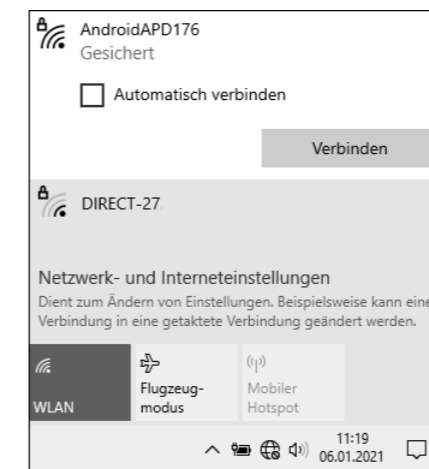


Abbildung 19.13 Beim Verbindungsaufbau mit einem mobilen Hotspot sollten Sie darauf verzichten, die automatische Verbindung zu aktivieren.

Nach einem Klick auf VERBINDEN werden Sie aufgefordert, den Netzwerksicherheitsschlüssel einzugeben, also in diesem Fall das Passwort, das auf dem Smartphone für den WLAN Access Point generiert wurde. Bestätigen Sie mit WEITER. Falls Sie keine Daten zwischen dem

eigenen Smartphone und dem Windows 10-Gerät austauschen müssen, beantworten Sie den folgenden Hinweis mit NEIN. Nach diesem letzten Schritt stellt Windows die Verbindung zum Hotspot her.

Je nach Mobilfunkvertrag lässt sich der Mobilfunkanbieter das Tethering gut bezahlen. Hier sollte man also durchaus vorsichtig sein und nicht allzu große Datenmengen übertragen. Dies ist auch dann sinnvoll, wenn der Vertrag ein monatliches Datenlimit vorsieht, denn ist dies erreicht, hat dies die Drosselung der Datengeschwindigkeit zur Folge. Windows 10 bietet eine praktische Einstellung – die sogenannte *getaktete Verbindung* –, die dafür sorgt, dass nicht unnötig Daten übertragen werden. So werden z. B. keine Updates mehr geladen, und auch die Cloud OneDrive wird nicht automatisch synchronisiert. In den meisten Fällen stuft Windows 10 die Verbindung zu einem mobilen Hotspot automatisch als getaktete Verbindung ein. Zur Sicherheit sollten Sie die Einstellung aber überprüfen.

1. Klicken Sie hierzu auf das Netzwerksymbol im Infobereich der Taskleiste. Markieren Sie den Hotspot, mit dem Sie gerade verbunden sind, und klicken Sie auf EIGENSCHAFTEN.
2. Es wird die Einstellungen-App geöffnet, die nun einige Informationen zur aktiven Verbindung anzeigt. Blättern Sie auf der Seite nach unten bis zum Bereich GETAKTETE VERBINDUNG. Sollte der Regler ALS GETAKTETE VERBINDUNG FESTLEGEN noch nicht aktiviert sein, holen Sie dies nach.

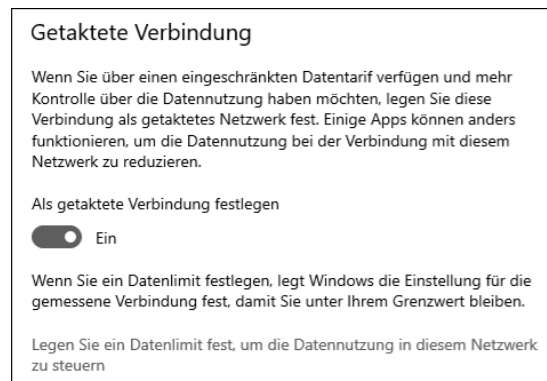


Abbildung 19.14 Bei einer getakteten Verbindung sorgt Windows 10 dafür, dass die übertragene Datenmenge reduziert wird.

3. Möchten Sie selbst einen Grenzwert festlegen, klicken Sie auf LEGEN SIE EIN DATENLIMIT FEST, UM DIE DATENNUTZUNG IN DIESEM NETZWERK ZU STEUERN. Sie kehren damit zur Statusseite der aktuellen Netzwerkverbindung zurück. Klicken Sie hier auf DATENNUTZUNG.
4. Auf der folgenden Seite sehen Sie in einer Übersicht, wie viele Daten die diversen Apps über das am oberen Seitenrand angezeigte Netzwerk während der letzten 30 Tage übertragen haben. Nach einem Klick auf GRENZWERT legen Sie nun selbst ein Datenlimit fest. Bestimmen Sie außerdem, ob dies für einen Monat, einmalig oder unbegrenzt gilt. Entschei-

den Sie sich für monatlich, sollten Sie noch den Tag angeben, an dem das Limit wieder zurückgesetzt wird. Schließen Sie den Dialog mit SPEICHERN.

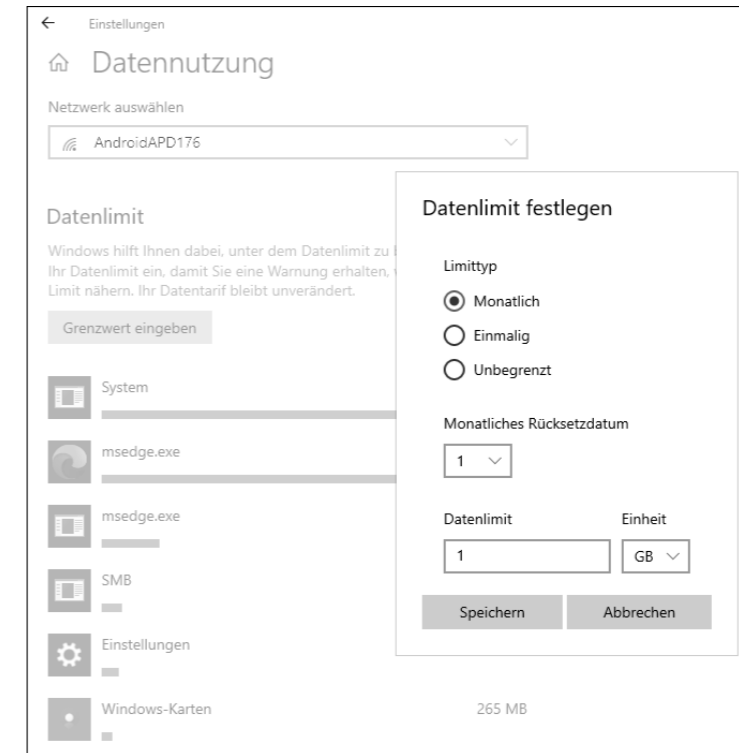


Abbildung 19.15 Sie können selbst das Datenlimit vorgeben, um die Menge der übermittelten Daten im Netzwerk festzulegen.

Vorsicht bei der Nutzung öffentlicher Hotspots

Häufig werden auf größeren Veranstaltungen oder auch an öffentlichen Plätzen wie Flughäfen mobile Hotspots angeboten. Diese stehen Ihnen nicht nur kostenlos zur Verfügung, sondern lassen sich zudem ohne Authentifizierung, sprich Eingabe eines Kennwortes, nutzen. Wenn Sie sich bei solch einem öffentlichen Hotspot anmelden, sollten Sie keinesfalls der Datenfreigabe zustimmen, da Sie sonst jedem, der das gleiche Netzwerk nutzt, quasi freien Zugang auf Ihr Gerät gewähren. Dass über ein ungesichertes WLAN kein Onlinebanking, Onlineshopping oder andere Aktionen getätigt werden sollten, bei dem hochsensible Daten übertragen werden, sollte sich von selbst verstehen. Setzen Sie in einem öffentlichen WLAN außerdem am besten ein VPN (Abkürzung für *Virtual Private Network*) ein. Dieses sorgt dafür, dass alle Ihre Daten zunächst verschlüsselt werden, bevor Sie über ein Netzwerk übertragen werden. Dies verhindert, dass Cyberkriminelle Ihre Daten abfangen können. Empfehlenswerte VPN-Dienste sind z. B. *ProtonVPN* (www.protonvpn.com/de), *CyberGhost VPN* (www.cyberghostvpn.com/de_DE) und *PureVPN* (www.purevpn.com/de).

Das eigene Windows 10-Gerät als Hotspot einrichten

Speziell in Hotels kommt es immer wieder vor, dass Sie einen WLAN-Zugang kostenpflichtig buchen können, der dann aber nur für ein Gerät genutzt werden darf. Benötigen Sie das WLAN auch für andere Geräte wie etwa Ihr Smartphone, richten Sie Ihr Windows 10-Gerät einfach als Hotspot ein. Hierzu sind nur wenige Schritte nötig. Bevor Sie damit beginnen, stellen Sie sicher, dass Ihr Gerät bereits mit dem Netzwerk verbunden ist. Anschließend geht es so weiter:

1. Rufen Sie in der Einstellungen-App die Kategorie NETZWERK UND SICHERHEIT und dort die Unterkategorie MOBILER HOTSPOT auf.
2. Setzen Sie den Regler MEINE INTERNETVERBINDUNG FÜR ANDERE GERÄTE FREIGEBEN auf EIN. Im Feld EIGENE INTERNETVERBINDUNG FREIGEBEN VON wird automatisch das gerade aktive Netzwerk, also etwa WLAN, angezeigt.
3. Windows 10 legt automatisch einen Namen und ein Kennwort für das Netzwerk fest. Nach einem Klick auf BEARBEITEN können Sie diese Angaben aber auch ändern. Mit SPEICHERN schließen Sie den Dialog NETZWERKINFOS BEARBEITEN wieder.
4. Damit nicht unnötig Energie verbraucht wird, aktivieren Sie am besten den Energiesparmodus. In diesem Fall schaltet sich der Hotspot automatisch aus, wenn keine Geräte mit ihm verbunden sind.



Abbildung 19.16 Ihr Windows 10-Computer lässt sich schnell als mobiler Hotspot einrichten.

Ihr Windows 10-Computer ist damit fertig als Hotspot eingerichtet und auch bereits aktiviert, wie Sie nach einem Klick auf das Netzwerksymbol im Infobereich der Taskleiste überprüfen können. Statt einer deaktivierten Schaltfläche mit der Bezeichnung MOBILER

HOTSPOT sollte hier nun der von Windows oder Ihnen selbst vergebene Netzwerkname erscheinen. Dass der Hotspot eingeschaltet ist, erkennen Sie an der blauen Schaltfläche. Bis zu acht Geräte können nun mit diesem Hotspot verbunden werden. Um den Hotspot zu deaktivieren, klicken Sie auf das Netzwerksymbol und dann auf die Schaltfläche mit dem Namen des Hotspots.

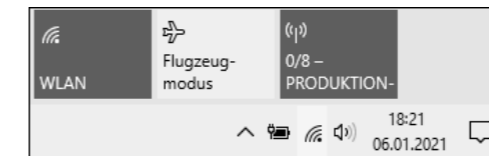


Abbildung 19.17 Der mobile Hotspot ist eingeschaltet, allerdings ist kein Gerät damit verbunden, wie die Anzeige »0/8« zeigt.

Windows 10 und Hotspot 2.0

Windows 10 unterstützt den WLAN-Standard 802.11u für Hotspot 2.0, der die Verbindung zu öffentlichen WLANs etwa an Flughäfen oder in Restaurants und Hotels nicht nur einfacher, sondern vor allem auch sicherer macht. Bei *Hotspot 2.0* (auch *HS2*, *Next Generation Hotspot* oder *WLAN Certified Passport* genannt) handelt es sich um einen Standard der Wi-Fi Alliance, der es Mobilgeräten ermöglicht, sich automatisch mit einem in Reichweite befindlichen WLAN-Hotspot zu verbinden und zu authentifizieren. Alle Hotspot 2.0-Netzwerke setzen die WPA2 Enterprise-Verschlüsselung ein. Für die Authentifizierung muss sich der Nutzer einmalig bei einem der Netzwerkanbieter zertifizieren. Um eine Liste der Hotspot 2.0-Netzwerkanbieter in der Umgebung zu erhalten, rufen Sie in der Einstellungen-App NETZWERK UND SICHERHEIT • WLAN auf und setzen den Regler ONLINEREGISTRIERUNG ZUM VERBINDEN VERWENDEN auf EIN. Sobald Sie das erste Mal ein Hotspot 2.0-Netzwerk auswählen und sich dort anzumelden versuchen, blendet Windows 10 eine Liste der verfügbaren Netzwerkanbieter ein. Wählen Sie einen Anbieter aus, und folgen Sie den weiteren Anweisungen, um bei diesem ein Konto einzurichten und das Profil herunterzuladen. Kommen Sie zukünftig in die Nähe eines Hotspot 2.0-Netzwerkes, stellt Ihr Windows 10-Gerät automatisch eine Verbindung zu diesem her. Für die Anmeldung wird dabei das zu Ihrem Konto gehörige Zertifikat verwendet, sodass Sie selbst keinerlei Anmeldeinformationen eingeben müssen.

19.3.4 Den Netzwerkstandort ändern

Wer sein Notebook, Hybridgerät oder auch Tablet nicht ausschließlich an einem einzigen Ort nutzt (sei es daheim oder im Büro), wird immer wieder Verbindungen zu unterschiedlichen Drahtlosnetzwerken herstellen. Aktivieren Sie bei der ersten Einrichtung eines WLANs die Option AUTOMATISCH VERBINDEN, WENN IN REICHWEITE, müssen Sie zukünftig keinen Handgriff mehr tätigen, um sich bei diesem Funknetzwerk anzumelden. Windows 10 erledigt alles automatisch. Dazu zählt auch die Auswahl des Netzwerkstandorts, den Sie bei der

ersten Einrichtung festlegen. Entsprechend der Auswahl passt Windows 10 die Firewall- und Sicherheitseinstellungen an. Es wird zwischen drei verschiedene Netzwerkstandorttypen unterschieden:

- **Öffentlich:** Hierzu zählen alle Netzwerke an öffentlichen Plätzen (Flughäfen, Hotels, Restaurants etc.). Ein öffentliches Netzwerk gilt als nicht vertrauenswürdig. Die Netzwerkerkennung ist entsprechend ausgeschaltet und der Computer für andere Geräte im Netzwerk nicht sichtbar. Sollte ein nicht autorisierter Zugriff erfolgen, wird dieser abgewiesen.
- **Privat:** Diese Einstellung beinhaltet alle vertrauenswürdigen Netzwerke, wie etwa Ihr Netzwerk daheim. Ihnen sind die Geräte bekannt, die mit diesem Netzwerk verbunden werden und auch die Personen, die es nutzen. Bei einem als privat eingestuften Netzwerk aktiviert Windows automatisch die Netzwerkerkennung und ermöglicht so den Datenaustausch zwischen den Geräten innerhalb des Netzwerkes.
- **Domäne:** Dieser Typ bezeichnet Verbindungen zu Unternehmensnetzwerken, in denen Ihr Computer Teil einer Windows-Domäne ist. Diese Einstellung wird Ihnen daher auch nur in diesem Fall angeboten. Die Netzwerkerkennung ist bei diesem Typ eingeschaltet, sodass alle Geräte innerhalb des Netzwerkes sichtbar sind.

Wurde das Netzwerk als PRIVAT eingestuft, können Daten im Netzwerk für andere Geräte freigegeben werden. Sollten Sie der Datenfreigabe versehentlich zugestimmt haben, obwohl es sich beim aktuellen Netzwerk um ein öffentliches und damit nicht vertrauenswürdige Netzwerk handelt, sollten Sie das Profil des Netzwerkes unbedingt korrigieren.

Um zu prüfen, welcher Netzwerkstandort aktiviert wurde, klicken Sie auf das Netzwerksymbol im Infobereich der Taskleiste und dann auf NETZWERK- UND INTERNETEINSTELLUNGEN. Es wird nun die Einstellungen-App mit der Kategorie NETZWERK UND INTERNET • STATUS geöffnet. Der kleinen Grafik rechts können Sie entnehmen, ob eine Internetverbindung besteht und welches Netzwerkprofil hierfür gewählt wurde.

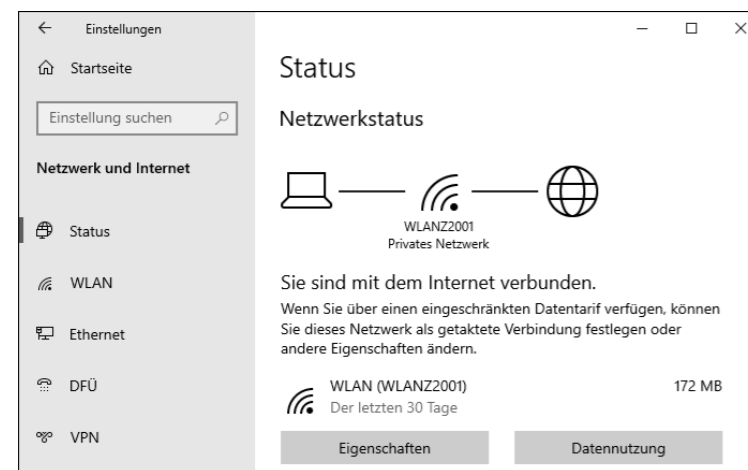


Abbildung 19.18 Der Netzwerkstatus der aktuellen Verbindung

Um ein privates Netzwerkprofil in ein öffentliches umzuwandeln oder auch umgekehrt, klicken Sie unterhalb des Netzwerknamens auf EIGENSCHAFTEN. Auf der folgenden Seite wählen Sie im Bereich NETZWERKPROFIL die gewünschte Option aus, also ÖFFENTLICH oder PRIVAT.

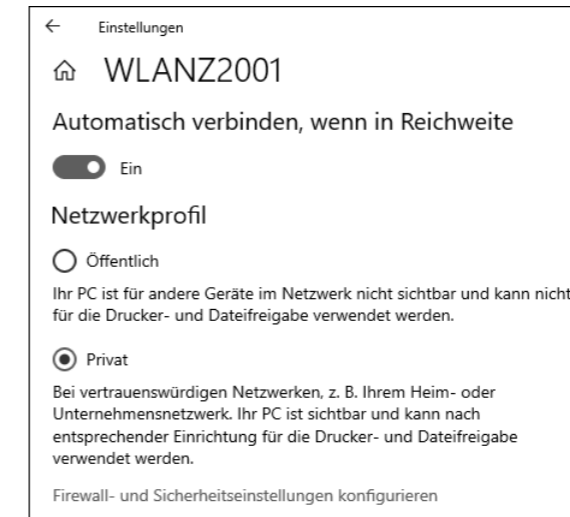


Abbildung 19.19 In einem vertrauenswürdigen Netzwerk kann als Netzwerkprofil »Privat« gewählt werden. Damit ist die Netzwerkerkennung aktiviert und der Computer für andere Geräte innerhalb des Netzwerkes sichtbar.

19.3.5 Nicht mehr genutzte WLAN-Verbindungen entfernen

Windows 10 speichert die Informationen aller WLANs, mit denen der Computer verbunden wurde. Dazu zählen natürlich auch diejenigen, die Sie z. B. im Rahmen eines Urlaubs nur einmalig genutzt haben. Diese Netzwerke, bei denen Sie sich höchstwahrscheinlich nie wieder anmelden werden, lassen sich problemlos aus der Liste der bekannten Netzwerke löschen. Das Vorgehen bietet sich aber auch an, wenn Sie z. B. den Namen des eigenen WLANs oder auch den Sicherheitsschlüssel geändert haben. Anstatt diese Daten zu ändern, entfernen Sie einfach die WLAN-Verbindung mit den alten Daten und verbinden den PC mit dem geänderten WLAN.

Rufen Sie hierzu per Klick auf das Netzwerksymbol im Infobereich der Taskleiste die NETZWERK- UND INTERNETEINSTELLUNGEN auf (siehe Abbildung 19.20). Markieren Sie in der Einstellungen-App links WLAN, und klicken Sie rechts auf BEKANNTE NETZWERKE VERWALTEN. Es wird nun eine Liste aller Drahtlosnetzwerke eingeblendet, mit denen der Computer bisher verbunden wurde. Markieren Sie das Netzwerk, das Sie nicht mehr benötigen, und klicken Sie auf NICHT SPEICHERN. Sollten Sie doch einmal wieder die Verbindung zu diesem WLAN herstellen wollen, müssen Sie bei der ersten Anmeldung wieder den Netzwerksicherheitsschlüssel eingeben.



Abbildung 19.20 Nicht mehr benötigte WLANs können Sie aus der Liste der bekannten Drahtlosnetzwerke entfernen.

Vergessenes WLAN-Passwort in Erfahrung bringen

Sie haben sich ein neues Tablet zugelegt, das Sie gerne mit dem heimischen WLAN verbinden möchten. Unglücklicherweise haben Sie den Netzwerksicherheitsschlüssel für das WLAN nicht parat. Verfügen Sie über ein Windows 10-Gerät, das bereits mit diesem WLAN verbunden ist, lässt sich das Kennwort schnell über einen Kommandozeilenbefehl in Erfahrung bringen. Geben Sie hierzu auf dem Windows 10-Gerät im Suchfeld der Taskleiste »Eingabeaufforderung« ein, und starten Sie diese per Klick auf den Treffer. In der Eingabeaufforderung geben Sie den Befehl `netsh wlan show profile name=WLAN-Name key=clear` ein, wobei Sie den Text »WLAN-Name« durch den Namen Ihres WLANs ersetzen.

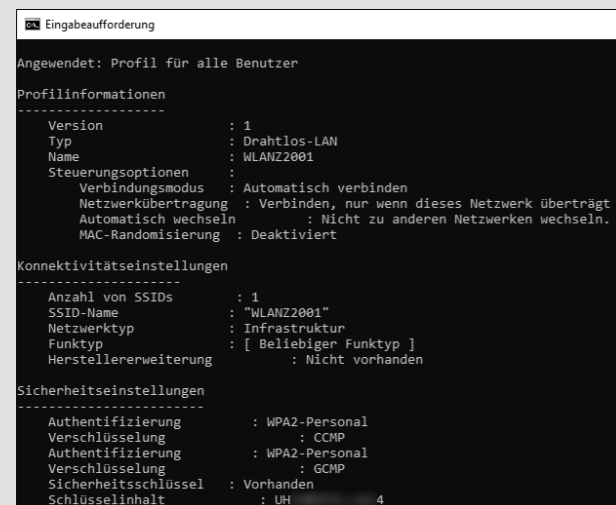


Abbildung 19.21 Im Bereich »Sicherheitseinstellungen« können Sie unter »Schlüsselinhalt« den Netzwerksicherheitsschlüssel des WLANs ablesen.

Nach Drücken der Taste `↵` wird der Netzwerksicherheitsschlüssel angezeigt. Sind Sie sich nicht ganz sicher, wie die Bezeichnung des WLANs lautet, können Sie sich mit dem Befehl `netsh wlan show profiles` eine Liste aller WLANs anzeigen lassen, mit denen das Gerät bisher verbunden wurde.

19.4 Problembehandlung für Netzwerke

Sie erhalten keine E-Mails, der Aufruf einer Website schlägt fehl oder der WLAN-Drucker ist nicht erreichbar? Die Ursache für diese Probleme zu finden ist aufgrund der Komplexität von Netzwerken nicht einfach. Eventuell ist der Netzwerkadapter des Computers defekt, der Router ausgeschaltet, oder es gibt einen Dienstausschfall beim *Internet Service Provider* (kurz *ISP*). Um einem Netzwerkproblem auf die Spur zu kommen, gilt es deshalb als Erstes, den Fehler einzugrenzen.

19.4.1 Netzwerkprobleme eingrenzen

Manchmal ist der Grund für eine nicht funktionierende Internetverbindung ganz simpel. Prüfen Sie deshalb als Erstes, ob das Netzkabel am Computer und am Router richtig eingesteckt ist. Falls Sie das WLAN nutzen, stellen Sie sicher, dass die WLAN-Funktion unter Windows 10 auch aktiviert ist. Der entsprechende Schalter im Bereich SCHNELLE AKTIONEN des Info-Centers sollte also farbig hervorgehoben sein. Vielleicht hatten Sie das WLAN zuvor deaktiviert und nur vergessen, es wieder einzuschalten.

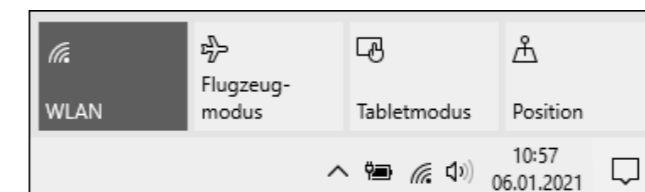


Abbildung 19.22 Manchmal lässt sich ein Netzwerkproblem ganz einfach beheben.

Werfen Sie einen Blick auf den Router. Die meisten Modelle zeigen durch LEDs an, ob sie ordnungsgemäß funktionieren. Blinken eine oder auch alle Statusanzeigen, trennen Sie den Router für mindestens eine Minute von der Stromversorgung. Schließen Sie ihn dann wieder an, und warten Sie einige Minuten, bis das Gerät wieder funktionsbereit ist. Blinken die LEDs weiterhin, spart es häufig Zeit, sich als Nächstes mit dem Internet Service Provider in Verbindung zu setzen. Eventuell werden gerade Wartungsarbeiten durchgeführt, oder der Provider kämpft selbst mit einem Problem.

Kann der Anbieter das Problem nicht identifizieren, müssen Sie selbst die Fehlersuche fortsetzen. Hierfür eignet sich z. B. die Problembehandlung von Windows 10. Um sie aufzurufen, klicken Sie mit der rechten Maustaste auf das Netzwerksymbol im Infobereich der Taskleiste und dann auf PROBLEMBEHANDLUNG. Folgen Sie nun den Anweisungen des Assistenten, um die Netzwerkdiagnose durchzuführen. In vielen Fällen lässt sich das Problem auf diese Weise lösen.

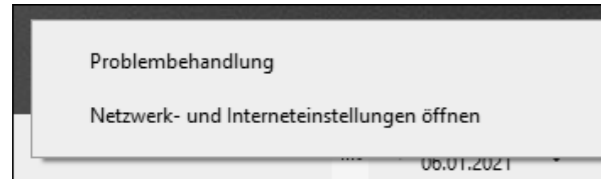


Abbildung 19.23 Die Problembehandlung zur Netzwerkdiagnose lässt sich bequem über das Kontextmenü des Netzwerksymbols im Infobereich der Taskleiste starten.

Wenn gar nichts mehr geht: das Netzwerk zurücksetzen

Lässt sich das Netzwerkproblem nicht lösen, hilft als allerletzter Schritt eventuell das Zurücksetzen des Netzwerkes weiter. Hierdurch werden alle Netzwerkadapter deinstalliert und die damit verbundenen Einstellungen entfernt. Nach einem Neustart des Computers findet die Installation der Netzwerkadapter statt, die Einstellungen werden auf die Standardeinstellungen zurückgesetzt. Sollten Sie VPN-Clientsoftware oder virtuelle Switches im Rahmen einer Virtualisierungssoftware wie Hyper-V verwenden, müssen auch diese gegebenenfalls neu eingerichtet werden. Das Zurücksetzen des Netzwerkes bringt also viel Arbeit mit sich und sollte deshalb nur als allerletzte Lösung angesehen werden. Der Aufruf der Funktion NETZWERK ZURÜCKSETZEN erfolgt über die Einstellungen-App, in der Sie die Kategorie NETZWERK UND INTERNET • STATUS aufrufen.

19.4.2 Tools zum Lösen von Netzwerkproblemen

Windows 10 bietet einige interessante Tools, um Netzwerkprobleme zu diagnostizieren und zu lösen. In Tabelle 19.1 finden Sie ein paar Befehlszeilenprogramme, die diese Aufgabe erfüllen. Gestartet werden sie jeweils aus der Eingabeaufforderung mit erhöhten Rechten. Geben Sie hierzu im Suchfeld der Taskleiste »Eingabeaufforderung« ein, klicken Sie den Treffer mit der rechten Maustaste an, und wählen Sie im Kontextmenü ALS ADMINISTRATOR AUSFÜHREN. Um sich eine Liste aller verfügbaren Parameter eines Tools sowie Erklärungen hierzu anzeigen zu lassen, geben Sie den Namen des Tools ein, gefolgt von einem Leerzeichen und den beiden Zeichen »/?« (beispielsweise `ipconfig /?`).

Befehlszeilentool	Aufgabe
<code>ipconfig</code>	Zeigt die aktuelle TCP/IP-Konfiguration des Netzwerkes an und aktualisiert die Einstellungen für das Dynamic Host Configuration Protocol (DHCP) und das Domain Name System (DNS).
<code>ping</code>	Prüft die Verbindung zu einem Zielcomputer, indem es eine Abfolge von Netzwerkpaketen an ihn sendet. Mit der Eingabe <code>ping localhost</code> lässt sich der eigene Computer überprüfen.
<code>tracert</code>	Dieses Tool bestimmt den Pfad zu einem Zielcomputer.
<code>nslookup</code>	Das Tool dient dazu, die IP-Adresse zu einem bestimmten Hostnamen oder den Domainnamen zu einer bestimmten IP-Adresse zu finden, und ist damit sehr hilfreich, um DNS-Probleme aufzuspüren.
<code>netsh</code>	Mit diesem Tool lässt sich die Netzwerkkonfiguration eines lokalen oder Remotecomputers anzeigen und ändern.

Tabelle 19.1 Befehlszeilentools zur Netzwerkproblembehandlung

Kapitel 34

Am Windows-Insider-Programm teilnehmen

Wer neugierig und experimentierfreudig ist, kann bereits vor der Veröffentlichung einen Blick auf die neuen Funktionen des nächsten Feature-Updates von Windows 10 werfen und diese ausprobieren. Möglich macht dies das Windows-Insider-Programm.

Früher verstrichen einige Jahre, bis eine neue Windows-Version veröffentlicht wurde. Mit Windows 10 hat sich dies geändert, nun kommt man bereits ein- bis zweimal jährlich in den Genuss neuer Funktionen. Für manch einen Anwender ist dies immer noch zu selten. Wer es gar nicht erwarten kann, die neuen Features zu inspizieren, kann am Windows-Insider-Programm teilnehmen. Das Testprogramm, das 2014 von Microsoft ins Leben gerufen wurde, gibt Anwendern die Möglichkeit, Vorabversionen von Windows 10 auszuprobieren. Die Teilnahme am Programm ist kostenlos, Sie benötigen lediglich ein Microsoft-Konto, mit dem Sie sich beim Insider-Programm registrieren.

Während Privatanwender auf diese Weise ihre Neugier bezüglich der weiteren Entwicklung von Windows 10 befriedigen können, stellt das Windows-Insider-Programm für IT-Entwickler eine gute Möglichkeit dar, ihre Anwendungen bereits vorab für die anstehenden Windows-Versionen zu optimieren. Microsoft selbst profitiert selbstverständlich ebenfalls davon, dass Millionen von Testern die Vorabversionen gründlich prüfen. Dabei kann das Unternehmen nicht nur auf das Feedback setzen, das die Anwender an Microsoft weiterreichen. Vor allem die zahlreichen Telemetriedaten, die automatisch erfasst, analysiert und auch an Dritte weitergereicht werden, sind für das Unternehmen von großem Interesse. Der Sammlung und Auswertung dieser Daten stimmt jeder Anwender automatisch in dem Moment zu, in dem er sich beim Windows-Insider-Programm registriert und die entsprechenden Bedingungen akzeptiert.

Die Wissbegierde Microsofts ist für die Entwicklung von Windows 10 von Vorteil, für den Anwender kann dies aber auch Risiken mit sich bringen. Im Folgenden erfahren Sie, welche Vorkehrungen Sie vor der Teilnahme am Insider-Programm treffen sollten. Im weiteren Verlauf des Kapitels zeige ich Ihnen, wie Sie dem Programm beitreten, die Vorabversionen von Windows 10 installieren und sich mit anderen Nutzern über neue Funktionen, aber auch Fehler und Kritikpunkte austauschen können.

34.1 Das Windows-Insider-Programm im Überblick

Frühere Windows-Versionen wurden von Microsoft ausschließlich intern entwickelt und getestet. Lediglich kurz vor Ende der Entwicklungsphase wurden ab und an Technical Previews veröffentlicht. Mit Windows 10 hat sich dieses Vorgehen geändert. Nachdem die Vorabversionen von den Entwicklern innerhalb Microsofts getestet wurden, werden sie recht schnell als sogenannte *Insider Preview Builds* über Windows Updates an die Windows-Insider-Community weitergereicht. Millionen von Anwendern, die sich beim Insider-Programm angemeldet haben, erhalten so die Gelegenheit, die neuen Features der nächsten Windows 10-Version auszuprobieren.

34.1.1 Die Risiken der Insider Preview Builds

Bei den Insider Preview Builds handelt es sich, wie gesagt, um Vorabversionen von Windows 10. Ziel der Testphase ist es, Fehler aufzuspüren und diese zu beheben, bevor die neuen Funktionen im Rahmen der Feature-Updates an alle Windows 10-Geräte weitergereicht werden. Diese Fehler – auch *Bugs* genannt – tauchen je nach Entwicklungsphase mehr oder weniger reichhaltig auf. Programmabstürze bis hin zu Datenverlust sind quasi vorprogrammiert. Dieses Risiko muss jedem bewusst sein, bevor er sich für das Insider-Programm registriert.

Auf einem Produktivsystem, auf dem Sie Ihre Arbeit erledigen, private Fotos und Dokumente archivieren, Onlinebanking oder -shopping durchführen und wichtige Daten (etwa für die Steuererklärung) speichern, hat eine Vorabversion nichts zu suchen. Und das nicht nur wegen der drohenden Abstürze und des damit verbundenen Datenverlustes, sondern auch aufgrund der Tatsache, dass Microsoft all Ihre Daten sammelt, auswertet und gegebenenfalls an Dritte weiterreicht. Sollte es also beispielsweise beim Zusammenstellen der Steuerbelege zu einem Programmabsturz kommen, wird nicht nur das Absturzprotokoll als solches an Microsoft weitergereicht, sondern in manchen Fällen auch die Datei, die Sie gerade bearbeitet haben.

Wer Mitglied der Windows-Insider-Community werden möchte, sollte für die Insider Preview Builds einen eigenen Testrechner nutzen, der für keinerlei andere Tätigkeiten des täglichen Lebens verwendet wird. Wer keinen Testrechner zur Verfügung hat, kann auch einen virtuellen Computer hierfür einrichten. Windows 10 Pro bietet z. B. die Virtualisierungslösung Hyper-V an, die Sie im folgenden Kapitel kennenlernen werden. Ansonsten bietet sich auch ein älteres Gerät an, das sonst nur noch als Staubfänger dient und nicht mehr produktiv genutzt wird.

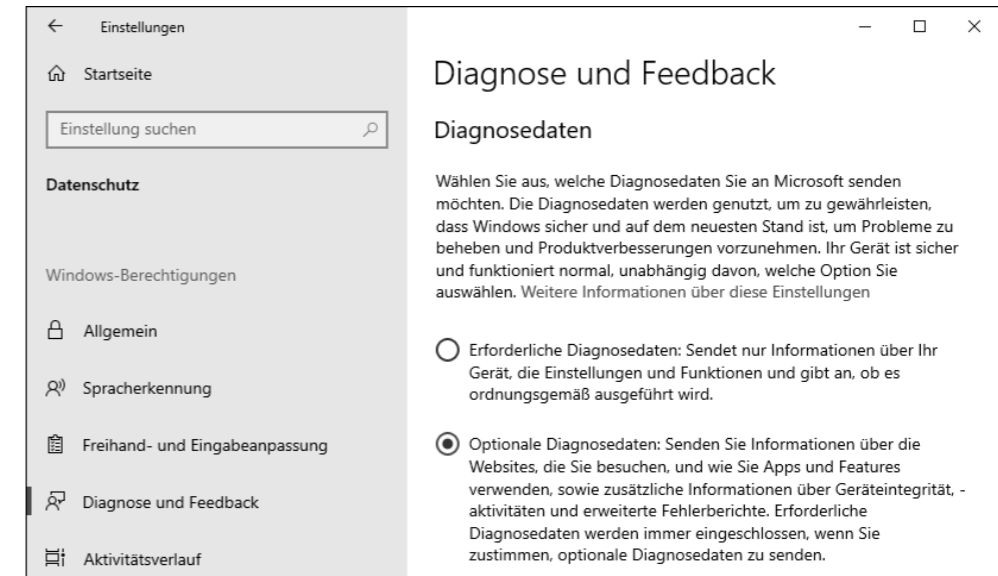


Abbildung 34.1 Wer am Windows-Insider-Programm teilnehmen möchte, muss der vollständigen Übermittlung von Diagnosedaten zustimmen. In der Kategorie »Datenschutz • Diagnose und Feedback« der Einstellungen-App muss entsprechend »Optionale Diagnosedaten« aktiviert sein.

34.1.2 Überblick über die Insider Channels

Die Insider Preview Builds gelangen als Update auf Ihren Computer. Je nach Einstellung, die Sie gewählt haben, kann dies mehrmals pro Woche oder auch nur einmal im Monat geschehen. Zur Auswahl stehen drei verschiedene Kanäle (auf Englisch »Channels«), früher noch *Ringe* genannt:

- ▶ **Dev-Kanal** (ehemals *Fast-Ring*): Sobald Features reif sind, um an die Windows-Insider-Community weitergereicht zu werden, gelangen sie in den Dev-Kanal. Entscheiden Sie sich während des Einrichtens der Insider Previews für diesen Kanal, zählen Sie damit zu den Ersten, die die neuen Funktionen testen können. Damit gehören Sie aber womöglich auch zu den Ersten, die Fehler aufspüren. Denn die in diesem Kanal veröffentlichten Insider Preview Builds gelten als die instabilsten. Funktionen, die hier vorgestellt werden, können, müssen aber nicht in der nächsten Version von Windows 10 erscheinen. Updates im Dev-Kanal erfolgen ein- bis zweimal pro Woche.
- ▶ **Beta-Kanal** (ehemals *Slow-Ring*): Wurden die Insider Preview Builds über einen gewissen Zeitraum hinweg im Dev-Kanal getestet, werden sie an den Beta-Kanal weitergeleitet. Die Updates kommen ca. zwei bis drei Mal im Monat und zeigen sich bereits deutlich stabiler. Alle Funktionen, die in den Insider Preview Builds des Beta-Kanals enthalten sind, erscheinen mit sehr großer Wahrscheinlichkeit auch in der nächsten Windows 10-Version.

- **Release Preview-Kanal** (ehemals *Release Preview-Ring*): Zeigt sich eine Insider Preview Build nach einer längeren Testphase im Beta-Kanal als ausreichend stabil, gelangt sie in den Release Preview-Kanal. Wer sich für diesen Kanal entscheidet, erhält auch Vorabversionen von Qualitätsupdates.

Die Insider Preview Builds sind ähnlich umfangreich wie die halbjährlichen Feature-Updates. Der Download und die Installation nehmen also entsprechend Zeit in Anspruch. Auch dies sollten Sie bei der Auswahl des gewünschten Kanals berücksichtigen.

Wer nicht zu den absoluten Profis zählt, aber durchaus etwas experimentierfreudig ist, dem empfehle ich die Teilnahme am Beta-Kanal. Möchten Sie hingegen nur vorab einen Blick auf die kommenden Funktionen werfen, ist der Release Preview-Kanal das Passende für Sie. Den gewünschten Kanal stellen Sie während der Einrichtung des Windows-Insider-Programms so ein, wie im nächsten Abschnitt gezeigt.

Installation von Vorabversionen verhindern

Insider Preview Builds sind Ihnen zu riskant, Sie möchten deshalb keinesfalls, dass diese auf dem Computer installiert werden? Mithilfe einer Gruppenrichtlinieneinstellung können Sie unter Windows 10 Pro, Enterprise und Education verhindern, dass andere Benutzer genau dies versuchen. Starten Sie hierzu den Editor für lokale Gruppenrichtlinien, indem Sie die Tastenkombination **Windows + R** drücken, im Ausführen-Dialog »gpedit.msc« eingeben und mit OK bestätigen. Im Editor navigieren Sie zum Pfad *Computerkonfiguration/Administrative Vorlagen/Windows-Komponenten/Windows Update/Windows Update für Unternehmen*. Doppelklicken Sie auf **VORABVERSIONEN VERWALTEN**, und aktivieren Sie im gleichnamigen Dialog die Option **AKTIVIERT**. Nun können Sie im Bereich **OPTIONEN** die Einstellung **VORABVERSIONEN DEAKTIVIEREN** auswählen. Schließen Sie den Dialog mit **ÜBERNEHMEN** und OK.

34.2 Dem Windows-Insider-Programm beitreten

Sie sind sich bewusst, welche durchaus fatalen Folgen die Installation von Insider Preview Builds haben kann, trauen sich aber durchaus zu, diese in den Griff zu bekommen? Dann müssen Sie für die Teilnahme am Windows-Insider-Programm nur noch wenige Schritte erledigen. Wie ich Ihnen bereits empfohlen habe, sollten Sie die Vorabversionen von Windows 10 nur auf einem Testcomputer installieren, den Sie ausschließlich für diese Zwecke nutzen. Auf diesem Gerät muss eine lizenzierte Windows 10-Version installiert sein.

Sie sollten am Testcomputer außerdem mit einem Microsoft-Konto angemeldet sein, das Sie nur zu Testzwecken verwenden. Denn denken Sie daran: Mit dem Beitritt zum Windows-Insider-Programm erteilen Sie Microsoft automatisch die Genehmigung, auf all Ihre Daten zuzugreifen und diese auszuwerten. Reale und vor allem sensible Daten sollten deshalb aus

Datenschutz- und Sicherheitsgründen keinesfalls mit den im Testbetrieb ermittelten Daten gemischt werden. Wie Sie ein neues Microsoft-Konto anlegen, erfahren Sie in Kapitel 26, »Windows 10 sicher mit mehreren Benutzern nutzen«. Zum Einrichten des Windows-Insider-Programms benötigen Sie außerdem Administratorrechte.

Das für das Windows-Insider-Programm verwendete Microsoft-Konto muss zunächst für das Programm registriert werden. Wie Sie hierzu vorgehen, erfahren Sie im nächsten Abschnitt. Im darauffolgenden Abschnitt zeige ich Ihnen, wie Sie Ihr Windows 10-Gerät für den Erhalt der Insider Preview Builds vorbereiten.

34.2.1 Beim Windows-Insider-Programm registrieren

Um am Windows-Insider-Programm teilnehmen zu können, müssen Sie sich zunächst mit dem Microsoft-Konto beim Programm registrieren. Dies ist zwar theoretisch aus der Einstellungen-App heraus möglich, gelingt in der Praxis aber nicht immer. Der sichere Weg führt über die englischsprachige Webseite <https://insider.windows.com>:

1. Nach dem Aufruf der Webseite klicken Sie auf **REGISTER** und auf der folgenden Seite auf **SIGN IN NOW**.



Abbildung 34.2 Die Registrierung am Windows-Insider-Programm nehmen Sie am besten über die Webseite vor.

2. Geben Sie die E-Mail-Adresse des Microsoft-Kontos an, das Sie für das Windows-Insider-Programm nutzen möchten. Anschließend wird das Kennwort des Microsoft-Kontos abgefragt.

- Auf der folgenden Seite lesen Sie sich die Programmvereinbarungen durch, bevor Sie diesen durch Setzen des Häkchens vor I ACCEPT THE TERMS OF THIS AGREEMENT (REQUIRED) zustimmen.
- Mit einem Klick auf REGISTER NOW schließen Sie die Registrierung ab.

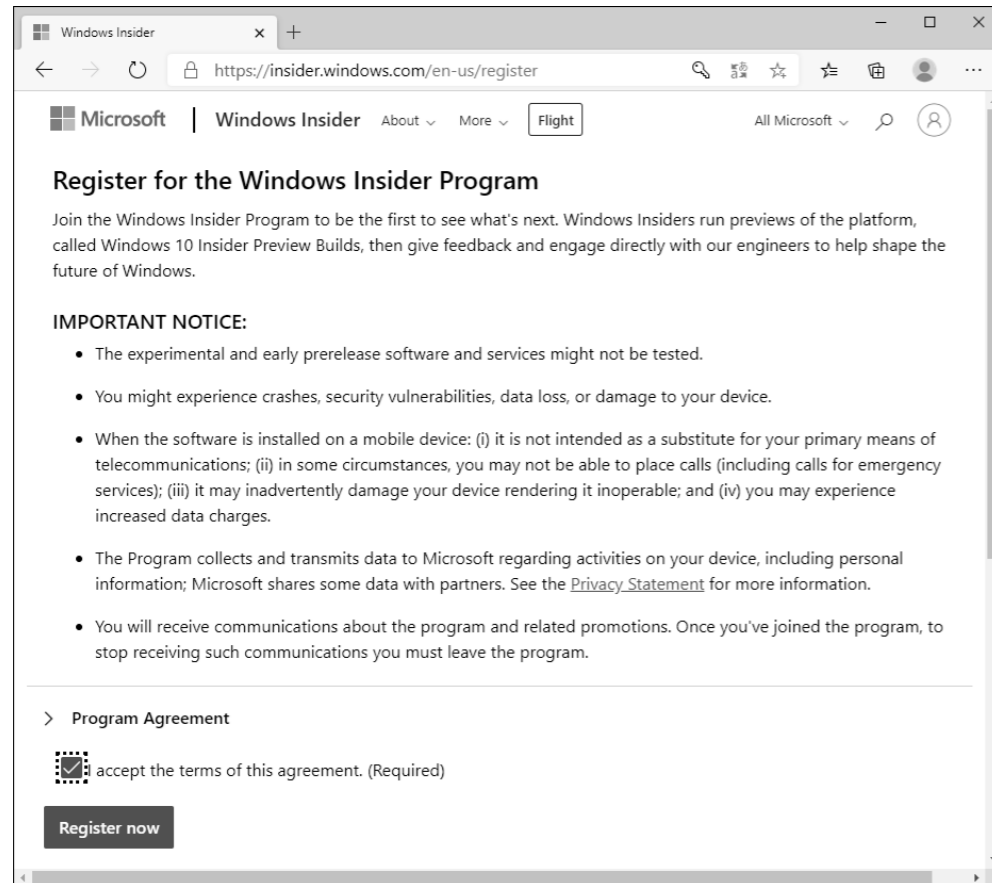


Abbildung 34.3 Den Programmvereinbarungen müssen Sie zustimmen, um die Registrierung abschließen zu können.

- Auf der folgenden Seite werden Sie beim Windows-Insider-Programm willkommen heißen. Klicken Sie auf FLIGHT NOW, erfahren Sie, welche weiteren Schritte auf dem Windows 10-Computer nötig sind, um die Insider Preview Builds zu erhalten. Sie können sich aber an dieser Stelle auch auf der Webseite abmelden und der Anleitung im folgenden Abschnitt folgen. Zur Abmeldung klicken Sie in der rechten oberen Seitenecke auf das Profilbild Ihres Microsoft-Kontos. Im aufklappenden Dialog wählen Sie SIGN OUT.

34.2.2 Windows-Insider-Programm auf dem Windows 10-Computer einrichten

Sobald Sie sich beim Windows-Insider-Programm registriert haben, können Sie mit der Einrichtung auf dem Windows 10-Computer fortfahren, auf dem die Insider Preview Builds installiert werden sollen. Rufen Sie auf diesem Gerät über die Tastenkombination **Windows + I** die Einstellungen-App auf, und wechseln Sie in die Kategorie UPDATE UND SICHERHEIT • WINDOWS-INSIDER-PROGRAMM. Sollten Sie die Ermittlung der Diagnosedaten noch nicht auf OPTIONALE DIAGNOSE DATEN umgestellt haben (siehe Abbildung 34.1), werden Sie hierzu auf der Seite WINDOWS-INSIDER-PROGRAMM aufgefordert. Sobald Sie die Einstellung in der Kategorie DATENSCHUTZ • DIAGNOSE UND FEEDBACK korrigiert haben, wird Ihnen auf der Seite WINDOWS-INSIDER-PROGRAMM die Schaltfläche ERSTE SCHRITTE angeboten, die Sie nun anklicken.

Nach einem Klick auf KONTO VERKNÜPFEN wählen Sie das zuvor für das Windows-Insider-Programm registrierte Microsoft-Konto aus. Sind Sie mit diesem Konto am Computer angemeldet, sollte es Ihnen bereits angezeigt werden.

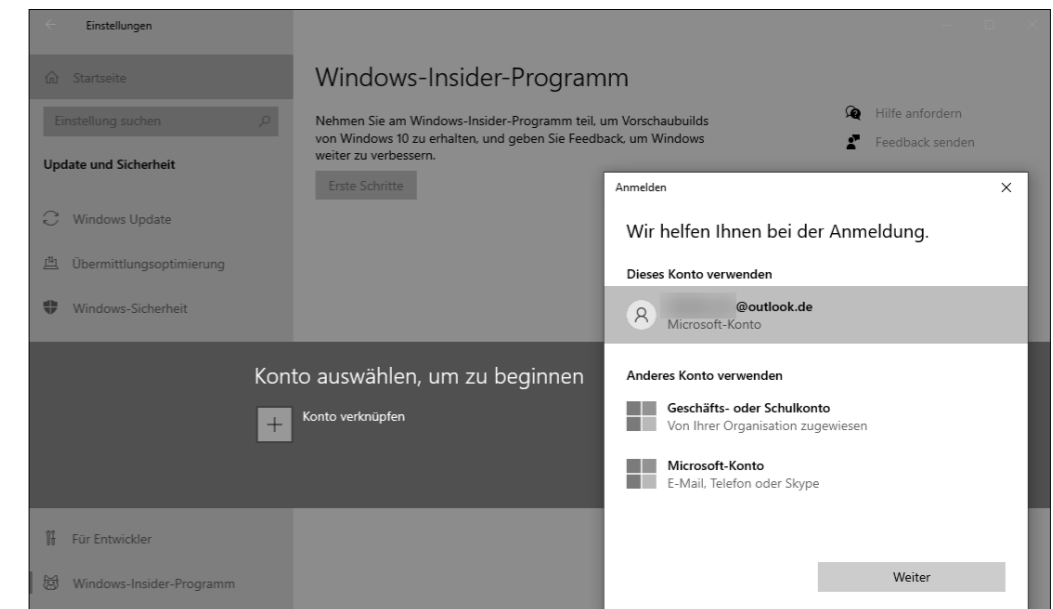


Abbildung 34.4 Wählen Sie das Microsoft-Konto aus, mit dem Sie sich zuvor beim Windows-Insider-Programm registriert haben.

Als Nächstes legen Sie in den Insider-Einstellungen fest, wie häufig Sie Insider Preview Builds erhalten möchten. Zur Auswahl stehen die drei Kanäle DEV-KANAL, BETA-KANAL und RELEASE PREVIEW-KANAL, die ich Ihnen in Abschnitt 34.1.2, »Überblick über die Insider Channels«, bereits kurz vorgestellt habe. Bestätigen Sie Ihre Auswahl.



Abbildung 34.5 In den Insider-Einstellungen stehen Ihnen die drei Kanäle »Dev-Kanal«, »Beta-Kanal« und »Release Preview-Kanal« zur Auswahl.

Im folgenden Dialog haben Sie über die beiden Links **DATENSCHUTZBESTIMMUNGEN FÜR MICROSOFT-INSIDER LESEN** und **VEREINBARUNG ZUM MICROSOFT-INSIDER-PROGRAMM LESEN** nochmals die Gelegenheit, sich ausführlich über das Windows-Insider-Programm zu informieren, bevor Sie den Dialog mit **BESTÄTIGEN** schließen.

Abschließend ist ein Neustart des Computers notwendig, den Sie mit **JETZT NEU STARTEN** gleich ausführen können. Nach dem Neustart kann es sein, dass Sie sich noch etwas in Geduld fassen müssen, bevor Ihnen die erste Insider Preview Build in der Einstellungen-App unter **UPDATE UND SICHERHEIT • WINDOWS UPDATE** angeboten wird. Sehen Sie einfach immer mal wieder auf der Seite nach, und klicken Sie auf **NACH UPDATES SUCHEN**. Die Vorabversion wird Ihnen wie ein Funktionsupdate angeboten. Den Download und die Installation starten Sie mit einem Klick auf **HERUNTERLADEN UND INSTALLIEREN**.



Abbildung 34.6 Eine Insider Preview Build wird Ihnen wie ein Funktionsupdate über das Windows Update zur Verfügung gestellt.

Nach der Installation einer Insider Preview Build wird oberhalb des Infobereichs der Taskleiste der Hinweis »Evaluierungskopie« sowie die aktuelle Build-Nummer angezeigt. Neigt sich der Entwicklungsprozess dem Ende zu, verschwindet die Anzeige wieder. Möchten Sie die Versionsnummer der installierten Vorabversion in Erfahrung bringen, geben Sie im Suchfeld der Taskleiste »winver« ein und wählen in der Trefferliste den entsprechenden Befehl aus. Im Dialog **INFO** erhalten Sie nun die entsprechende Information. Alternativ hierzu können Sie auch in der Einstellungen-App in die Kategorie **SYSTEM • INFO** wechseln und einen Blick in den Bereich **WINDOWS-SPEZIFIKATIONEN** werfen.



Abbildung 34.7 Sowohl in der Einstellungen-App als auch im Dialog Info können Sie die aktuelle Version der Insider Preview in Erfahrung bringen.

Je nach gewähltem Kanal erhalten Sie mehr oder weniger häufig die nächsten Insider Preview Builds. Für Teilnehmer am Windows-Insider-Programm gilt die Dauer von 35 Tagen, die Sie Updates maximal aussetzen können, nicht. Hier sind es lediglich sieben Tage. Möchten

Sie tatsächlich etwas warten, bis die nächste Insider Preview auf Ihrem Gerät installiert wird, rufen Sie die Einstellungen-App auf und wechseln in die Kategorie UPDATE UND SICHERHEIT • WINDOWS UPDATE. Nach einem Klick auf ERWEITERTE OPTIONEN wählen Sie im Bereich UPDATES AUSSETZEN im Feld DATUM AUSWÄHLEN den gewünschten Termin aus.

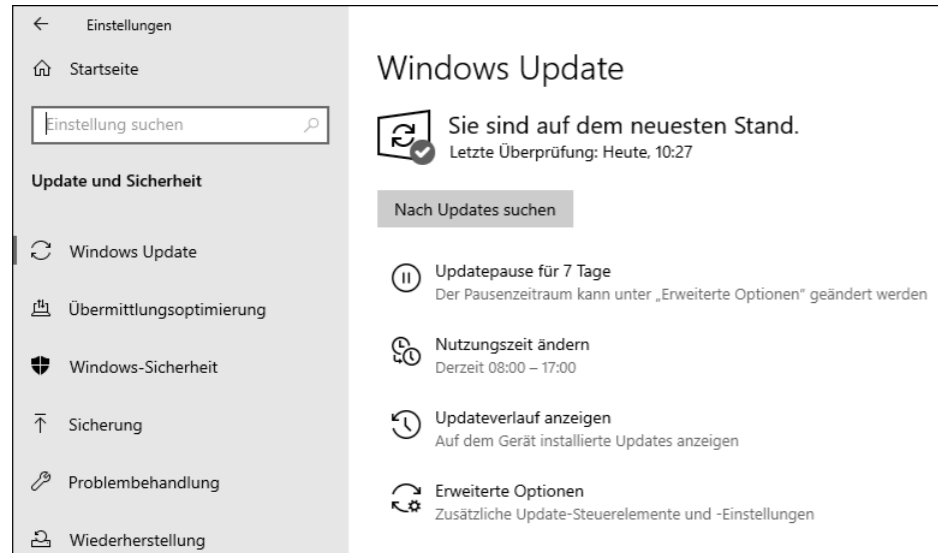


Abbildung 34.8 Während der Teilnahme am Windows-Insider-Programm können Updates für maximal sieben Tage pausiert werden.

34.3 Informationen einholen, Feedback abgeben

Manche neuen Funktionen springen einem sofort ins Auge, kaum dass eine Insider Preview Build installiert ist. Das gilt z. B. dann, wenn das äußere Erscheinungsbild wie etwa das Startmenü geändert wurde. Andere Aktualisierungen hingegen sind tief im System versteckt. Wer sich nicht selbst umständlich auf die Suche begeben möchte, wirft am besten einen Blick in den Windows-Insider-Blog, in dem Microsoft sowohl Hinweise auf neue Funktionen als auch Fehlermeldungen bzw. Fehlerkorrekturen (sogenannte *Bugfixes*) veröffentlicht. Den englischsprachigen Blog erreichen Sie unter der Webadresse <https://blogs.windows.com>. Blättern Sie auf der Webseite nach unten bis zum Abschnitt WINDOWS INSIDER PROGRAM, und wählen Sie Ihre Insider Preview Build aus. Wie Sie die Build-Nummer in Erfahrung bringen, haben Sie im vorherigen Abschnitt erfahren. Ein besonderes Augenmerk sollten Sie im Blog auf die »Known Issues« legen, in denen die bereits bekannten Fehler aufgeführt werden, die Microsoft zu beheben versucht.

Ein wichtiges Ziel des Windows-Insider-Programms ist es, Fehler frühzeitig zu entdecken und zu korrigieren, bevor eine neue Windows-Version der Allgemeinheit zur Verfügung gestellt wird. Dass dies nicht immer gelingt, zeigte sich Ende 2018, als Microsoft die kurz zuvor

veröffentlichte Version 1809 wieder zurückziehen musste, da ein gravierender Fehler übersehen worden war, der auf einigen Systemen zu Datenverlust führte.

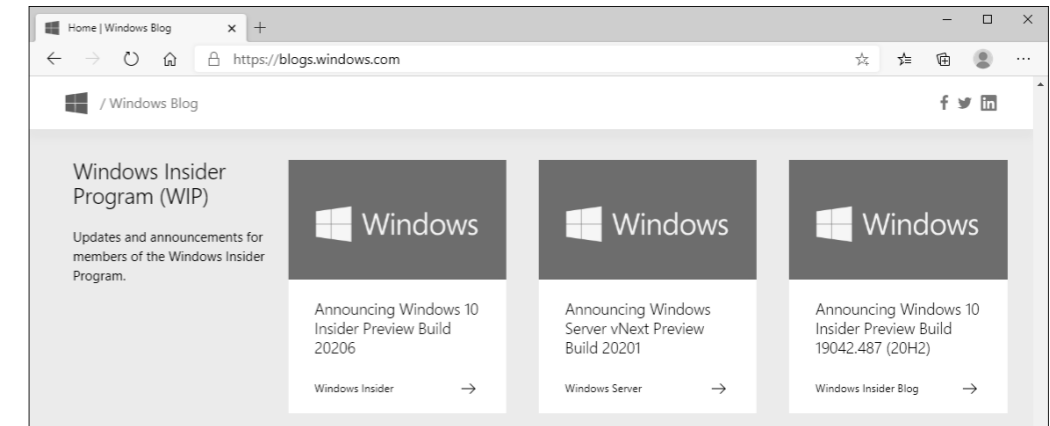


Abbildung 34.9 Über den Windows-Insider-Blog können Sie sich über die neuesten Funktionen, aber auch über bereits korrigierte sowie neu entdeckte Fehler informieren.

Dieses Beispiel macht deutlich, dass nicht nur die Auswertung von Diagnosedaten wichtig ist, sondern auch das Feedback der Anwender. Die Erfahrungen, die Sie mit den Insider Preview Builds machen, können Sie Microsoft über die *Feedback-Hub-App* mitteilen. Zum Öffnen der App wählen Sie den gleichnamigen Eintrag in der App-Liste des Startmenüs. Die Nutzung der App erfordert die Anmeldung mit Ihrem Microsoft-Konto. Auch in der Feedback-Hub-App können Sie sich über die Aktualisierungen in den neuesten Insider Preview Builds informieren. Klicken Sie hierzu links auf die Kategorie ANKÜNDIGUNGEN. Werden die Kategoriebeschriftungen nicht angezeigt, blenden Sie sie per Klick auf das Hamburger-Menü oben links ein.

Sind Sie zunächst etwas ratlos, was Sie in der Insider Preview testen sollten, hilft Ihnen die Kategorie AUFTRÄGE weiter (siehe Abbildung 34.10). In der rechten Fensterhälfte werden nun einige Aufgaben aufgelistet, die getestet werden sollten. Wählen Sie eine aus, und folgen Sie der Anleitung. Haben Sie den Auftrag erfüllt, klicken Sie in der Feedback-Hub-App auf FERTIG. Anschließend werden Sie aufgefordert, Ihre Erfahrung mit der getesteten Funktion an Microsoft zu übermitteln.

Interessiert es Sie, welche Erfahrungen andere Mitglieder der Windows-Insider-Community gemacht und welche Fehler sie gegebenenfalls entdeckt haben, wechseln Sie in der Feedback-Hub-App in die Kategorie FEEDBACK (siehe Abbildung 34.11). Sie können hier die Bewertungen anderer Anwender sortieren, Filter setzen und die Sprache sowie den verwendeten Gerätetyp auswählen. Über das Feld KATEGORIE lässt sich die Feedbackanzeige auch auf bestimmte Themen eingrenzen. Benötigen Sie gezielte Informationen zu einem Problem, geben Sie das Stichwort einfach im Suchfeld ein. Das ist vor allem dann interessant, wenn Sie auf einen Fehler gestoßen sind und feststellen möchten, ob dieser bereits per Feedback-Hub

an Microsoft übermittelt wurde. Haben Sie die gleichen Erfahrungen gemacht wie ein anderer Teilnehmer, können Sie dies über die Schaltfläche ZUSTIMMEN an Microsoft weiterreichen. Bedarf es eines Kommentars hierzu, fügen Sie ihn einfach hinzu.

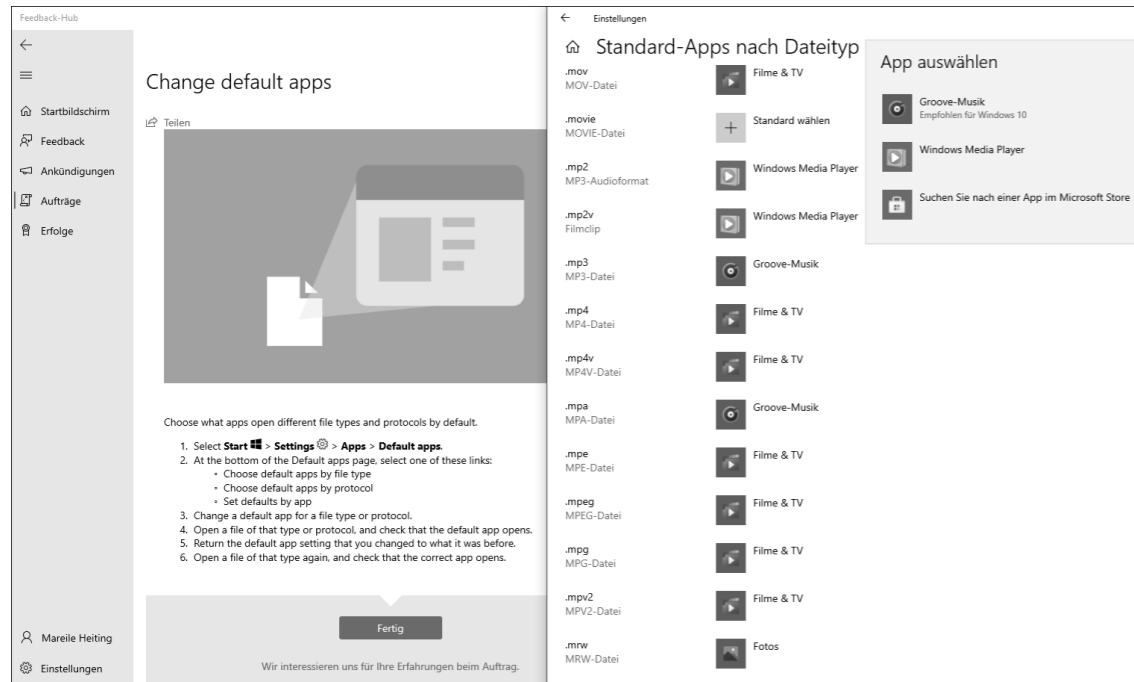


Abbildung 34.10 Mithilfe der »Aufträge« können Sie die Funktionen der Vorabversion testen und Ihre Erfahrungen dann an Microsoft weiterleiten.

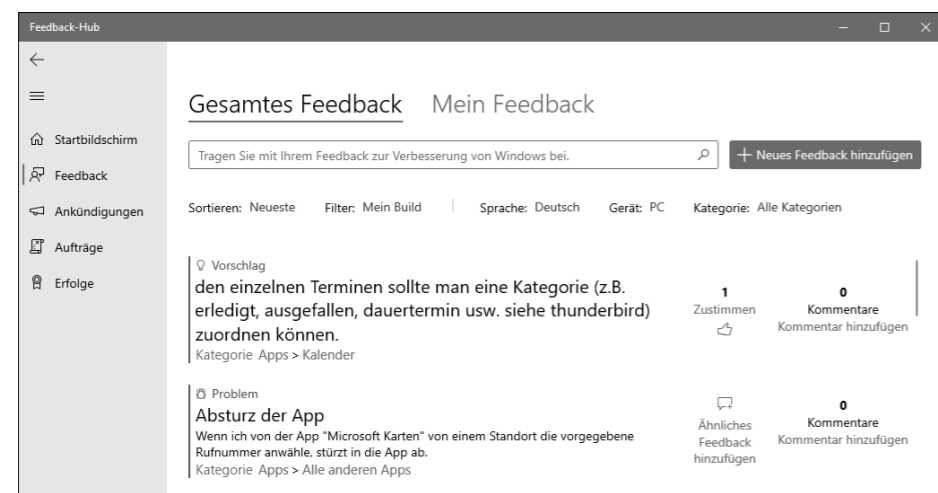


Abbildung 34.11 In der Kategorie »Feedback« können Sie sich über die Erfahrungen der anderen Teilnehmer informieren.

Möchten Sie der Community und natürlich auch Microsoft Ihre eigenen Erfahrungen mitteilen, klicken Sie auf die Schaltfläche NEUES FEEDBACK HINZUFÜGEN und füllen den Fragebogen aus.

34.4 Das Windows-Insider-Programm beenden

Für eine gewissen Zeit fanden Sie das Testen der Vorabversionen ganz interessant, doch jetzt würden Sie das Windows-Insider-Programm gerne verlassen? Das ist selbstverständlich möglich. Den entsprechenden Regler hierfür finden Sie in der Einstellungen-App in der Kategorie UPDATE UND SICHERHEIT • WINDOWS-INSIDER-PROGRAMM.

Setzen Sie den Regler ERHALT VON VORABVERSIONEN BEENDEN auf EIN, hängt es von der aktuellen Entwicklungsphase und der auf Ihrem System installierten Build ab, ob Sie sofort aus dem Programm aussteigen können oder auch weiterhin noch mit Updates versorgt werden. Steht das Entwicklungsende und damit die Veröffentlichung des nächsten Funktionsupdates kurz bevor, können Sie den Regler problemlos auf EIN setzen. In diesem Fall erhalten Sie vorab nur noch die kumulativen Updates für die anstehende Version. Wurde der Entwicklungszyklus hingegen gerade erst begonnen, ist das Verlassen des Windows-Insider-Programms nicht ganz so einfach. Sie können durch Einschalten des Reglers zwar veranlassen, dass keine weiteren Updates mehr auf Ihrem Gerät installiert werden, eine Möglichkeit, zu einer früheren finalen Version von Windows 10 zurückzukehren, gibt es allerdings nicht. Es sei denn, Sie nehmen eine komplette Neuinstallation von Windows 10 vor. Hinweise hierzu erhalten Sie in Kapitel 33, »Windows 10 installieren«.

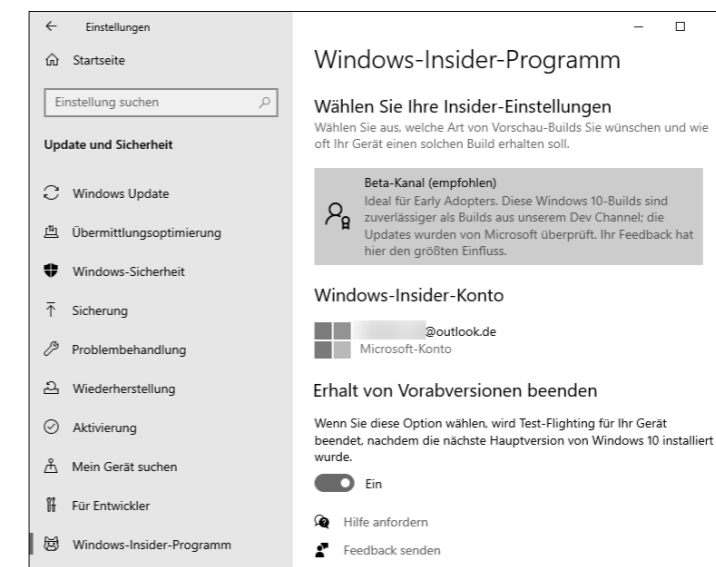


Abbildung 34.12 Der Erhalt von Vorabversionen kann auch beendet werden. Um seltener Updates zu erhalten, reicht die Auswahl eines anderen Kanals aus.

Wer vor diesem Schritt zurückschreckt, für den ist es eventuell sinnvoller, den Kanal und damit die Häufigkeit zu ändern, mit der Sie die Insider Preview Builds erhalten. Die entsprechende Korrektur können Sie ebenfalls auf der Seite `WINDOWS-INSIDER-PROGRAMM` im Bereich `WÄHLEN SIE IHRE INSIDER-EINSTELLUNGEN` vornehmen. Waren Sie bisher z. B. Teilnehmer des Dev-Kanals, lässt sich die Updatehäufigkeit mit der Auswahl des Beta-Kanals bereits erheblich minimieren.