Windows 11 für Profis

Insider-Wissen - praxisnah & kompetent

Kapitel 10

Benutzerkonten, Kennwörter und Anmeldeinformationen verwalten

Bevor Sie mit einem Gerät arbeiten können, auf dem Microsoft Windows 11 ausgeführt wird, müssen Sie sich mit den Anmeldeinformationen eines Benutzerkontos anmelden, das zur Verwendung dieses Geräts berechtigt ist. Benutzerkonten sind ein wesentlicher Eckpfeiler der Windows-Sicherheit und auch für die Bereitstellung einer personalisierten Benutzererfahrung wichtig. Als Administrator bestimmen Sie, welche Benutzerkonten sich an einem bestimmten Gerät anmelden dürfen. Mit Benutzerkonten auf einem Windows 11-Gerät können Sie außerdem:

- den Zugang zu Ihren Dateien und anderen Ressourcen kontrollieren
- Systemereignisse überwachen, wie Anmeldungen und die Verwendung von Dateien und anderen Ressourcen
- Dateien und Einstellungen zwischen Ihren verschiedenen Computern synchronisieren, sofern die Anmeldungen mit demselben Konto erfolgen
- sich automatisch an E-Mail- und anderen Onlinediensten anmelden
- von jedem Benutzer verlangen, dass er seine Identität durch einen weiteren Faktor beweist (die sogenannte Multi-Faktor-Authentifizierung oder mehrstufige Authentifizierung), wenn er sich das erste Mal bei einem neuen Gerät anmeldet

Die mit einem Benutzerkonto verknüpften Anmeldeinformationen bestehen aus einem Benutzernamen und einem Kennwort, die zur Identifizierung dienen und theoretisch sicherstellen, dass niemand den Computer verwenden oder Dateien, E-Mail-Nachrichten und andere persönliche Daten, die mit einem Benutzerkonto verknüpft sind, einsehen kann, wenn er nicht dazu berechtigt ist.

Wenn Sie der Meinung sind, dass sich Ihr Computer an einem sicheren Ort befindet, an dem nur Personen, denen Sie vertrauen, physischen Zugriff darauf haben, könnten Sie versucht sein, Familienmitgliedern oder Arbeitskollegen zu erlauben, Ihr Benutzerkonto gemeinsam zu nutzen. Wir raten dringend von dieser Konfiguration ab und empfehlen stattdessen, für jede Person, die den Computer benutzt, ein eigenes Benutzerkonto zu erstellen. Auf diese Weise kann jedes Konto auf sein eigenes Benutzerprofil zugreifen, persönliche Dateien und Benutzereinstellungen innerhalb dieses Profils speichern und auf cloudbasierte Ressourcen zugreifen. Mit der schnellen Benutzerumschaltung, die weiter hinten in diesem Kapitel beschrieben wird, ist der Wechsel zwischen Benutzerkonten eine Sache von ein paar Klicks.

Mit der richtigen Hardware und einigen Konfigurationsarbeiten erreichen Sie, dass Sie sich anmelden und abmelden können, ohne Ihre vollständigen Anmeldedaten eingeben zu müssen. Das Feature namens »Windows Hello« bietet die Möglichkeit, sich mit biometrischen Verfahren anzumelden, also beispielsweise per Gesichtserkennung oder einem Fingerabdruck. In diesem Kapitel erfahren Sie außerdem, wie Sie die Microsoft Authenticator-App auf einem vertrauenswürdigen Mobilgerät installieren und sich damit bei einem Microsoft-Konto oder Azure AD-Konto anmelden können, ohne ein Passwort eingeben zu müssen.

Benutzerkonten erstellen und verwalten

Wenn Sie Windows 11 zum ersten Mal auf einem neuen Computer (oder auf einem PC mit einer Neuinstallation von Windows) konfigurieren, erstellt das Setupprogramm ein Profil für ein Benutzerkonto, das ein Administratorkonto ist. (Ein *Administratorkonto* ist ein Konto, das volle Kontrolle über den Computer hat. Weitere Informationen finden Sie im Abschnitt »Administrator- oder Standardbenutzerkonto?« weiter hinten in diesem Kapitel.) Je nachdem, welche Art von Konto Sie bei der Einrichtung auswählen, kann dieses erste Konto ein Microsoft-Konto, ein Azure Active Directory (Azure AD)-Konto oder ein lokales Benutzerkonto sein. Ein vierter Benutzerkontotyp – ein Konto in einer lokalen Active Directory-Domäne – ist nur in einem verwalteten Netzwerk verfügbar, nachdem dieses anfängliche lokale Konto erstellt wurde und Sie den Computer mit der Windows-Domäne verbunden haben. (Informationen zu den Unterschieden zwischen diesen Kontotypen finden Sie im nächsten Abschnitt, »Kontotyp auswählen«.)

Falls Sie Ihren Windows 10-Computer auf Windows 11 aktualisieren und bereits lokale Konten vorhanden sind, migriert Windows diese Konten zu Ihrer Windows 11-Installation. Diese migrierten Konten behalten ihre Gruppenmitgliedschaften und Kennwörter.

Nachdem Sie sich zum ersten Mal angemeldet haben, können Sie unter *Einstellungen* | *Konten* neue Benutzerkonten erstellen und routinemäßige Änderungen an bestehenden Konten vornehmen. Auf der Seite *Ihre Infos* können Sie Ihr Kontobild konfigurieren und auf die Kontoeinstellungen zugreifen (siehe Abbildung 10.1).

Unter *Konten* finden Sie verschiedene Optionen und Einstellungen, je nachdem, welche Art von Konto Sie verwenden (Microsoft-Konto, Azure AD-Konto oder lokales Konto), ob Ihr Konto Mitglied der Gruppe *Administratoren* ist und – wenn Ihr Computer einer Domäne angehört – ob Gruppenrichtlinien wirksam sind. Auf einem Computer, der mit einer Active Directory-Domäne verbunden ist, wird die gesamte Verwaltung von Benutzerkonten, die über grundlegende Aufgaben wie die Auswahl eines Bilds hinausgeht, normalerweise von einem Domänenadministrator durchgeführt.

Einige kontobezogene Einstellungen befinden sich unter der Überschrift *Benutzerkonten* in der Systemsteuerung, die in Abbildung 10.2 dargestellt ist. Manche dieser Einstellungen duplizieren Funktionen, die auch unter *Einstellungen* | *Konten* verfügbar sind.

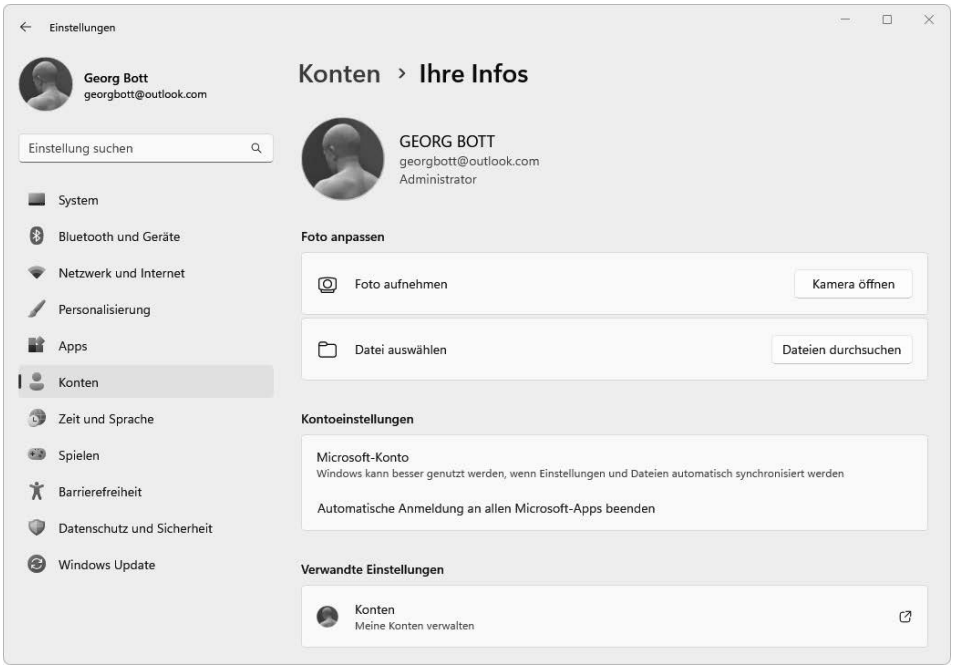

Abbildung 10.1 Auf der Seite *Ihre Infos* werden Ihre Kontodaten angezeigt.

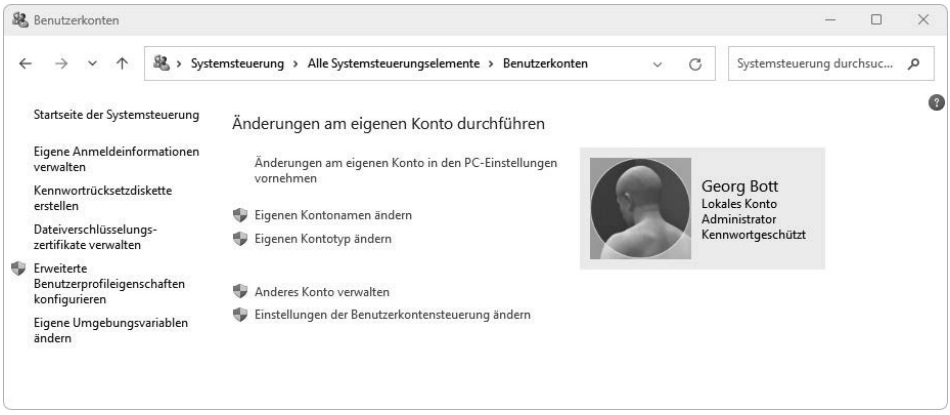

Abbildung 10.2 Der Besuch dieser Seite in der Systemsteuerung ist selten notwendig, da die meisten Optionen zum Erstellen und Verwalten von Konten in der App Einstellungen verfügbar sind.

Sie können ein neues Konto nur über die Seite *Konten* in den *Einstellungen* hinzufügen. Sie können entweder von dieser Seite oder von der entsprechenden Seite in der Systemsteuerung ein Konto entfernen oder seinen Typ ändern. Alle esoterischen Optionen auf der linken Seite der Seite *Benutzerkonten* sowie die Option *Einstellungen für die Benutzerkontensteuerung ändern* sind nur in der Systemsteuerung verfügbar.

Kontotyp auswählen

Wie bereits erwähnt, unterstützt Windows 11 vier verschiedene Arten von Benutzerkonten, die jeweils durch die Art der Authentifizierung definiert sind.

Microsoft-Konto

Wenn Sie auf einem Windows 11-Gerät ein neues Konto einrichten, wird Ihnen nachdrücklich empfohlen, sich mit einem Microsoft-Konto anzumelden. Wahrscheinlich haben Sie schon seit Jahren Microsoft-Konten verwendet, vielleicht sogar, ohne es zu wissen. Wenn Sie sich für einen Microsoft-Dienst angemeldet haben, zum Beispiel Outlook.com (oder dessen Vorgänger Hotmail), Microsoft 365 Family oder Personal, Skype oder Xbox Live, haben Sie bereits ein Microsoft-Konto. Jede E-Mail-Adresse, die auf *hotmail.com*, *msn.com*, *live.com, outlook.com* oder *outlook.de* endet, ist per Definition ein Microsoft-Konto.

Während der Einrichtung können Sie die mit einem bestehenden Microsoft-Konto verknüpfte E-Mail-Adresse eingeben oder in der Domäne *outlook.com* eine neue E-Mail-Adresse erstellen. Sie müssen sich jedoch nicht für eine Microsoft-E-Mail-Adresse anmelden, um ein Microsoft-Konto zu erstellen. Sie können ein Microsoft-Konto mit einer vorhandenen persönlichen E-Mail-Adresse eines beliebigen E-Mail-Anbieters einrichten, einschließlich Google Mail und anderer Dienste, die nicht zu Microsoft gehören.

Expertentipp

Verwenden Sie keine geschäftliche E-Mail-Adresse als Microsoft-Konto

Wie bereits erwähnt, können Sie jede persönliche E-Mail-Adresse als Microsoft-Konto verwenden. Dazu gehören kostenlose Gmail- und Yahoo-Mail-Konten sowie Konten, die von einem Internetprovider bereitgestellt werden.

Wenn Sie eine E-Mail-Adresse auf einer benutzerdefinierten Domäne haben, die auf Microsoft 365 Exchange Online- oder Google Workspace-Servern gehostet wird, erlaubt Microsoft Ihnen jedoch nicht mehr, diese Adresse als Microsoft-Konto zu verwenden. Der neue Kontoerstellungsprozess erkennt kommerzielle Konten mit benutzerdefinierten Domänen, die auf einem dieser Servertypen gehostet werden, und lehnt Versuche ab, sie für ein Microsoft-Konto zu verwenden.

Das ist, offen gestanden, eine willkommene Änderung. Wenn Sie bisher eine geschäftliche E-Mail-Adresse für ein Microsoft-Konto verwendet haben, wurden Sie jedes Mal belästigt, wenn Sie versuchten, sich bei einem der beiden Dienste anzumelden, weil Windows 11 fragte, ob Sie Ihr Microsoft-Konto oder Ihr Geschäfts-, Schul- oder Unikonto verwenden wollten. Wenn Sie mit dieser unglücklichen Konfiguration konfrontiert sind, können Sie die Dinge in Ordnung bringen, indem Sie Ihrem Microsoft-Konto einen neuen E-Mail-Alias zuweisen, den Alias zur primären Adresse machen und dann die unerwünschte geschäftliche Adresse aus dem Microsoft-Konto entfernen. Detaillierte Anweisungen für diese Aufgabe finden Sie weiter hinten in diesem Abschnitt.

Wenn Sie sich mit einem Microsoft-Konto anmelden, können Sie die PC-Einstellungen zwischen mehreren Computern synchronisieren. Wenn Sie mehr als einen PC verwenden, zum Beispiel einen Desktop-PC auf der Arbeit, einen anderen Desktop zu Hause, einen Laptop für unterwegs und ein Tablet zu Hause, können Sie durch die Anmeldung mit einem Micro-

soft-Konto mühelos denselben Desktophintergrund, dieselben gespeicherten Kennwörter, dasselbe Kontobild, dieselbe Zugriffskonfiguration usw. verwenden. Die Synchronisierung erfolgt automatisch und fast augenblicklich.

Einige Windows 11-Features, einschließlich OneDrive und Familieneinstellungen, erfordern die Verwendung eines Microsoft-Kontos oder eines Azure AD-Kontos. Es ist möglich, OneDrive und andere Dienste, die von einem Microsoft-Konto abhängen, auch dann zu verwenden, wenn Sie sich mit einem anderen Kontotyp bei Windows anmelden. In dieser Konfiguration müssen Sie sich jedoch bei jedem Dienst einzeln anmelden und einige Funktionen sind möglicherweise nicht verfügbar oder weniger bequem zu verwenden.

Normalerweise verknüpfen Sie eine einzige persönliche E-Mail-Adresse mit Ihrem Microsoft-Konto und verwenden diese Adresse für die Anmeldung bei Windows. Da jedoch jedes Microsoft-Konto bis zu zehn E-Mail-Aliasse unterstützt, können Sie für die Anmeldung an Ihrem Microsoft-Konto auch einen beliebigen Alias verwenden, der mit Ihrer primären Adresse verknüpft ist.

Die Aliasse für ein Microsoft-Konto verwalten Sie, indem Sie zur Seite *https://account.live.com/names/Manage* gehen und sich mit Ihrem Microsoft-Konto anmelden. Klicken Sie im Abschnitt *Kontoalias auf E-Mail-Adresse hinzufügen*, um einen neuen Alias zu erstellen oder eine vorhandene persönliche E-Mail-Adresse als Alias zu verwenden. Sobald die neue E-Mail-Adresse verifiziert wurde, können Sie sie zur primären Adresse machen und (wenn Sie möchten) die alte Adresse löschen. (Jeder Alias verwendet dasselbe Kennwort wie das ursprüngliche Konto.)

Im Abschnitt *Anmeldeeinstellungen* können Sie die Einstellungen für E-Mail-Aliasse so ändern, dass ein bestimmter Alias nicht für die Anmeldung an Ihrem Microsoft-Konto benutzt werden darf. Diese Vorsichtsmaßnahme ermöglicht es, einen Alias zum Senden und Empfangen von E-Mail zu nutzen, verhindert aber, dass er für den Zugriff auf Ihr Microsoft-Konto verwendet wird.

Lokales Benutzerkonto

Ein *lokales Konto* ist ein Konto, das seine Anmeldeinformationen und andere Kontodaten auf Ihrem PC speichert. Ein lokales Konto funktioniert nur auf einem einzigen Computer. Es benötigt weder eine E-Mail-Adresse als Benutzernamen noch kommuniziert es mit einem externen Server, um die Anmeldedaten zu überprüfen.

Diese Kontenart war jahrzehntelang der Standard in Windows. Für Windows 11 empfiehlt Microsoft, auf Computern, die keine Mitglieder von verwalteten Netzwerken sind, statt lokaler Konten Microsoft-Konten zu benutzen. Es ist aber nicht zwingend erforderlich, ein Microsoft-Konto zu verwenden. Lokale Benutzerkonten werden weiterhin voll unterstützt.

Möglicherweise bevorzugen Sie ein lokales Konto, wenn Ihr Heim- oder Firmennetzwerk auch Computer mit Windows 7 oder früheren Versionen umfasst (also Versionen, die die Verwendung von Microsoft-Konten nicht ausdrücklich unterstützen).

- **Einzelheiten finden Sie im Abschnitt »Dateien, Drucker und andere Ressourcen über ein lokales Netzwerk freigeben« in Kapitel 11, »Windows-Netzwerke konfigurieren«.**

Darüber hinaus haben einige Leute Bedenken hinsichtlich des Datenschutzes und der Datensicherheit, wenn persönliche Informationen auf den Servern eines großen Unternehmens gespeichert werden, unabhängig davon, ob diese Infrastruktur von Microsoft, Google, Apple, Amazon oder einem anderen Cloudanbieter verwaltet wird. Wenn Sie sich mit einem lokalen Benutzerkonto anmelden, sendet Ihr Computer weniger Daten an die Microsoft-Server.

Expertentipp

Wie sollten Sie die Sicherheitsfragen für ein lokales Konto konfigurieren?

Wenn Sie mit Windows 11 ein neues, kennwortgeschütztes lokales Konto einrichten, müssen Sie drei Sicherheitsfragen (aus einer Liste von sechs) auswählen und die Antworten auf diese Fragen eingeben. (Sie können diesen Schritt überspringen, indem Sie die Internetverbindung trennen, bevor Sie beim Erstellen des neuen Kontos diese Seite erreichen.)

Die vorbereiteten Fragen bieten keine gute Sicherheit. Einige der Informationen, zum Beispiel der Name Ihres ersten Haustiers oder Ihr Geburtsort, sind kaum ein Hindernis für einen Angreifer, der Sie persönlich kennt. Ein Dieb, der Ihr Notebook mitgenommen hat, kommt wahrscheinlich nicht so einfach an diese Informationen, aber jemand aus Ihrem Bekanntenkreis weiß möglicherweise die Antworten.

Auf einem Heim-PC, der an einem sicheren Platz steht, mag diese Maßnahme sinnvoll sein, besonders wenn Sie einen PC für vergessliche Verwandte einrichten. Aber wenn Sie es zu gefährlich finden, diese Fragen zu beantworten, ist hier ein anderer Ansatz: *Lügen Sie drauflos!* Windows prüft natürlich nicht, ob Ihre Antworten wahr oder auch nur sinnvoll sind. Statt die gestellten Fragen zu beantworten, können Sie sich eine aus mehreren Wörtern zusammengesetzte Phrase ausdenken und sie statt der tatsächlichen Antwort eintragen. Wenn Sie es für sich selbst wie auch für einen Angreifer unmöglich machen wollen, mithilfe der Sicherheitsfragen das Kennwort zurückzusetzen, können Sie einfach wild auf die Tastatur einhämmern und eine lange Abfolge von Unsinn als Antwort auf jede Frage eintippen.

Alternativ bietet es sich an, eine Kennwortrücksetzdiskette zu erstellen, die Sie – getrennt von Ihrem PC – an einem sicheren Ort verwahren. Sie brauchen dazu einen Wechseldatenträger, zum Beispiel einen USB-Speicherstick, ein externes Festplattenlaufwerk oder eine Speicherkarte. Melden Sie sich mit Ihrem Konto an, öffnen Sie *Systemsteuerung* | *Benutzerkonten* und klicken Sie auf *Kennwortrücksetzdiskette erstellen*. Folgen Sie nun den Anweisungen des Assistenten für vergessene Kennwörter. Sie können für jedes lokale Benutzerkonto nur eine einzige Kennwortrücksetzdiskette erstellen. Wenn Sie eine neue erstellen, wird die alte ungültig und kann nicht mehr benutzt werden. Wie Sie Ihr Kennwort mithilfe dieses Datenträgers zurücksetzen, beschreiben wir weiter hinten in diesem Kapitel.

Sie können zwischen der Verwendung eines Microsoft-Kontos und eines lokalen Kontos wechseln, indem Sie zu *Einstellungen* | *Konten* | *Ihre Infos* gehen. Auf dieser Seite (siehe Abbildung 10.1) klicken Sie auf *Stattdessen mit einem lokalen Konto anmelden*. Windows führt Sie durch ein paar einfache Schritte, um ein lokales Konto zu erstellen, das Sie dann für die Anmeldung verwenden.

Wenn Sie derzeit mit einem lokalen Konto angemeldet sind, lautet der Link auf dieser Seite *Stattdessen mit einem Microsoft-Konto anmelden*. Klicken Sie auf diesen Link, um Ihr lokales Konto durch ein Microsoft-Konto zu ersetzen. Im Rahmen der Umstellung müssen Sie Ihr lokales Kennwort ein weiteres Mal eingeben. Ein paar Bildschirme später sind Sie mit einem bestehenden oder einem neu erstellten Microsoft-Konto verbunden. Von diesem Zeitpunkt an melden Sie sich mit Ihrem Microsoft-Konto an.

Azure Active Directory-Konto

Der dritte Kontentyp, der bei der Ersteinrichtung von Windows 11 Pro, Enterprise oder Education verfügbar ist, ist ein Geschäfts-, Schul- oder Unikonto mit Azure Active Directory. Azure AD bietet einige der Vorteile eines Microsoft-Kontos, einschließlich der Unterstützung für die Multi-Faktor-Authentifizierung und die einmalige Anmeldung (single sign-on) bei Onlinediensten, wobei Netzwerkadministratoren gegebenenfalls mit der entsprechenden Verwaltungssoftware Beschränkungen festlegen können. Diese Konten sind am häufigsten in mittleren und großen Unternehmen, Organisationen, Schulen, Universitäten und anderen Bildungseinrichtungen zu finden.

Organisationen, die Microsofts Onlinedienste abonnieren, die sich vor allem an Unternehmen richten – einschließlich der Business- oder Enterprise-Editionen von Microsoft 365 (früher bekannt als Office 365), Microsoft Intune und Microsoft Dynamics CRM Online –, verfügen im Rahmen ihres Abonnements automatisch über Zugang zu Azure AD-Diensten. Für jedes Benutzerkonto in diesen Diensten existiert automatisch ein entsprechender Azure AD-Verzeichniseintrag.

Sie können bei einer Windows 11-Neuinstallation ein Azure AD-Konto verwenden, wie wir in »Durchführen einer Neuinstallation« in Kapitel 2, »Installieren eines neuen Windows 11-PCs« erklären. Sie können ein Windows 11-Gerät auch mit Azure AD verknüpfen, nachdem es für die Verwendung eines lokalen Kontos oder eines Microsoft-Kontos eingerichtet wurde. Gehen Sie dazu zu *Einstellungen* | *Konten* | *Auf Geschäfts-, Schul- oder Unikonto zugreifen* und klicken Sie dann auf *Verbinden*. Das daraufhin angezeigte Dialogfeld, das in Abbildung 10.3 dargestellt ist, bietet Ihnen zwei Optionen.

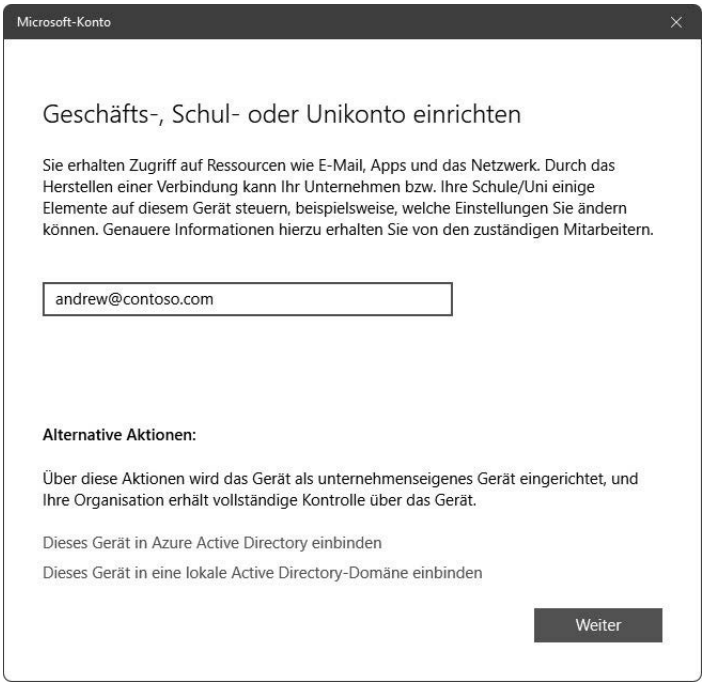

Abbildung 10.3 Das Hinzufügen eines Geschäfts-, Schul- oder Unikontos über die Einstellungen-App bietet mehrere Optionen. Die Links *Dieses Gerät einbinden* geben Ihrer Organisation die Kontrolle über das Gerät.

Die Standardoption ermöglicht es Ihnen, sich weiterhin mit Ihrem Microsoft-Konto oder Ihrem lokalen Konto bei Windows anzumelden, und fügt einfach Ihr Azure AD-Konto hinzu, um den Zugriff auf Microsoft 365-Dienste, einschließlich Exchange Online-E-Mail und OneDrive for Business, zu erleichtern. Wenn das Ihr Ziel ist, klicken Sie auf *Weiter* und folgen Sie den Aufforderungen.

Wenn Sie den PC so umkonfigurieren möchten, dass Sie sich mit Ihrem Azure AD-Konto bei Windows anmelden, geben Sie im Dialogfeld *Geschäfts-, Schul- oder Unikonto einrichten* keine E-Mail-Adresse ein, sondern klicken Sie unten im Dialogfeld auf den Link *Dieses Gerät in Azure Active Directory einbinden*. Diese Option öffnet das in Abbildung 10.4 gezeigte Dialogfeld. Nachdem Sie sich mit Ihren Azure AD-Anmeldeinformationen angemeldet haben, haben Sie eine letzte Möglichkeit, zu bestätigen, dass Sie sich mit den Anmeldeinformationen Ihrer Organisation anmelden und Administratoren erlauben möchten, Richtlinien auf Ihr Gerät anzuwenden.

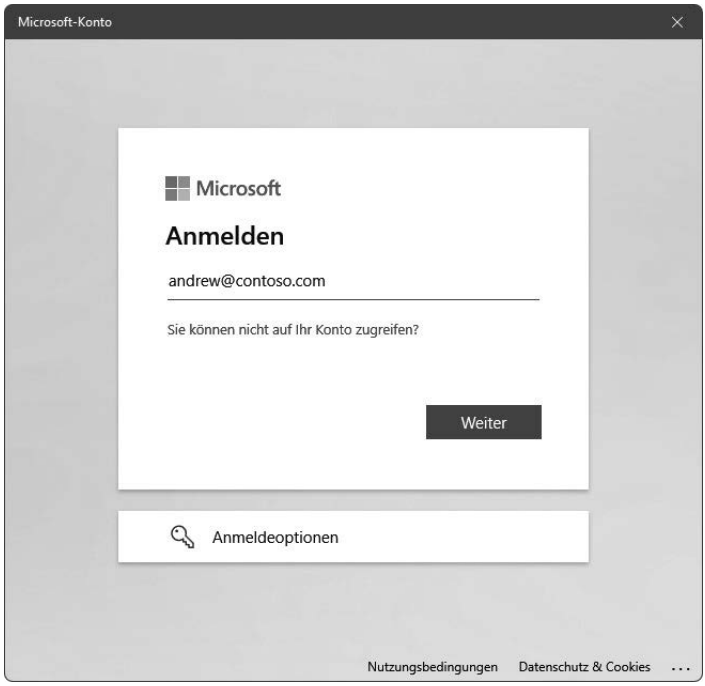

Abbildung 10.4 Geben Sie die Anmeldeinformationen eines Azure Active Directory-Kontos ein, z.B. eines Microsoft 365 Enterprise-Abonnements, um das Gerät in diese Organisation einzubinden.

Nachdem Sie einen Windows 11-PC in Azure AD eingebunden haben, können Sie Ihr Benutzerprofil anzeigen und bearbeiten, indem Sie zu *Einstellungen* | *Konten* | *Ihre Infos* und auf *Meine Konten verwalten* klicken. Sie können die Registerkarten verwenden, um Sicherheitsinformationen zu verwalten, einschließlich Anmeldemethoden und Multi-Faktor-Authentifizierung. Je nach den von Ihrem Unternehmen vorgenommenen Einstellungen können Sie möglicherweise Ihr eigenes Kennwort zurücksetzen.

Active Directory-Domänenkonto

In Organisationen mit einem Windows-Domänenserver, auf dem die Active Directory-Dienste ausgeführt werden, können Administratoren einen PC mit der Domäne verbinden und ein Domänencomputerkonto erstellen. (Diese Option ist nur in den Editionen Windows 11 Pro, Enterprise und Education verfügbar.) Nachdem dieser Schritt abgeschlossen ist, kann sich jeder Anwender, der in der Domäne ein Benutzerkonto besitzt, an diesem Computer anmelden und auf lokale und domänenbasierte Ressourcen zugreifen. Dieser Kontotyp wird in Kapitel 19, »Windows-PCs in Unternehmen verwalten«, ausführlicher behandelt.

Administrator- oder Standardbenutzerkonto?

Das Rückgrat der Windows-Sicherheit ist die Möglichkeit, jeden Benutzer eindeutig zu identifizieren. Bei der Einrichtung eines Computers – oder auch zu jedem späteren Zeitpunkt – erstellt ein Administrator ein oder mehrere Benutzerkonten, von denen jedes durch einen Benutzernamen identifiziert und normalerweise durch ein Kennwort geschützt ist. Wenn sich der Benutzer mit diesen Anmeldeinformationen am PC anmeldet, steuert Windows den Zugriff auf die Systemressourcen auf der Grundlage der Berechtigungen und Rechte, die den einzelnen Benutzerkonten von den Eigentümern der Ressourcen und dem Systemadministrator zugewiesen wurden.

Windows klassifiziert jedes Benutzerkonto als einen von zwei Kontotypen:

- **Administrator** Die Mitglieder der Gruppe *Administratoren* werden als Administratorkonten eingestuft. Die Gruppe *Administratoren* umfasst standardmäßig das erste Konto, das Sie beim Einrichten des Computers erstellen, sowie ein Konto namens *Administrator*, das standardmäßig deaktiviert und ausgeblendet ist. Im Gegensatz zu anderen Kontotypen besitzen Administratoren die volle Kontrolle über das System.
- **Standardbenutzer** Mitglieder der Gruppe *Benutzer* werden als Standardbenutzerkonten eingestuft. Benutzer haben nur begrenzten administrativen Zugriff, können aber grundlegende administrative Funktionen ausführen, beispielsweise die Eigenschaften ihres eigenen Kontos ändern oder Windows-Updates verwalten.

Den Personen, die einen Computer benutzen, einen geeigneten Kontotyp zuzuweisen, ist ganz einfach. Mindestens ein Benutzer muss ein Administrator sein; das sollte natürlich die Person sein, die die Nutzung und Wartung des Computers verwaltet. Alle anderen regelmäßigen Benutzer sollten standardmäßige Benutzerkonten haben.

> **Hinweis**
>
> **Für Computer mit Windows 11, die Sie mit Azure AD verbinden, können Sie einen Benutzer innerhalb Ihres Azure AD-Tenants als Geräteadministrator festlegen. Diese Aufgabe kann automatisch ausgeführt werden, während Sie das Gerät in Azure AD einbinden.**

Was ist mit dem Konto Administrator passiert?

Jeder Computer, auf dem Windows läuft, hat ein spezielles Konto namens Administrator. In den Windows-Versionen vor Windows 7 war der Administrator das primäre Konto für die Verwaltung des Computers. Wie andere Administratorkonten hat auch das Konto *Administrator* volle Rechte auf dem gesamten Computer. In Windows 11 ist das Konto *Administrator* jedoch standardmäßig deaktiviert.

In Windows 11 besteht nur selten die Notwendigkeit, das Konto *Administrator* anstelle eines anderen Administratorkontos, also eines Benutzerkontos, das Mitglied der Gruppe Administratoren ist, zu verwenden. In den Standardeinstellungen von Windows besitzt das Konto *Administrator* ein besonderes Merkmal: Für dieses Konto wird die Benutzerkontensteuerung (UAC, user account control) nie ausgeführt, und zwar auch dann nicht, wenn die Benutzerkontensteuerung für alle anderen Konten aktiviert ist. Alle anderen Administratorkonten (die manchmal auch als geschützte Administratorkonten bezeichnet werden) werden mit Standardbenutzerberechtigungen ausgeführt, es sei denn, der Benutzer stimmt der Ausführung mit erhöhten Rechten zu. Das Konto *Administrator* wird immer mit vollen Administratorrechten ausgeführt; daher wird niemals Ihre Zustimmung für die Erhöhung der Rechte benötigt. (Aus diesem Grund bringt die Nutzung dieses Konto bestimmte Risiken mit sich. Jede Anwendung, die als Administrator ausgeführt wird, hat die volle Kontrolle über den Computer, was bedeutet, dass Anwendungen, die von böswilligen oder unerfahrenen Programmierern geschrieben wurden, Ihrem System erheblichen Schaden zufügen können.)

Expertentipp

Und was ist mit dem Gastkonto?

In der Vergangenheit bot das integrierte Gastkonto eine Möglichkeit, gelegentlichen Benutzern begrenzten Zugriff zu gewähren. Nicht so in Windows 11. Obwohl dieses Konto immer noch existiert, ist es standardmäßig deaktiviert, und die unterstützten Tools zur Aktivierung (beispielsweise die Konsole *Lokale Benutzer und Gruppen*) funktionieren nicht so, wie Sie es vielleicht erwarten. Unserer Erfahrung nach wird der Versuch, Windows 11 dazu zu bringen, diese Funktion zu aktivieren, mit ziemlicher Sicherheit in Frustration enden. In der cloudzentrierten Welt von Windows 11 funktioniert das Gastkonto nicht mehr wie früher, und seine Aktivierung kann zu den unterschiedlichsten Problemen führen. Eine bessere Lösung (wenn Ihre Gäste kein eigenes Gerät haben, das eine Verbindung zu Ihrem drahtlosen Netzwerk herstellen kann) ist die Einrichtung eines Standardbenutzerkontos für die Nutzung durch Gäste.

Kontoeinstellungen ändern

Mit den Optionen in der App Einstellungen und in der Systemsteuerung können Sie Änderungen an Ihrem eigenen Konto oder am Konto eines anderen Benutzers vornehmen.

Um Ihr eigenes Konto zu ändern, gehen Sie zu *Einstellungen* | *Konten* | *Ihre Infos*, wie in Abbildung 10.1 gezeigt. Noch schneller geht es so: Öffnen Sie das Startmenü, klicken oder tippen Sie auf Ihr Kontobild und wählen Sie dann *Kontoeinstellungen ändern*.

Hier können Sie Ihr Profilbild ändern. Suchen Sie dazu eine passende Bilddatei heraus oder nehmen Sie mit der Webcam ein Foto auf. Wenn Sie sich mit einem Microsoft-Konto anmelden, öffnet ein Klick auf die Verknüpfung *Meine Konten verwalten* Ihren Standardwebbrowser, der dann Ihre Kontoseite unter *https://account.microsoft.com* lädt. Auf dieser Seite können Sie Ihr Kennwort oder den Namen ändern, der mit dem Microsoft-Konto verknüpft ist. Mit den anderen Verknüpfungen am oberen Rand der Seite prüfen Sie Ihre Dienste und Abonnements, Sicherheitseinstellungen, den Bestellverlauf und die Bezahlung und ändern Ihre Zahlungsoptionen. Sie können auch Informationen über andere Geräte abrufen, die mit Ihrem Microsoft-Konto verknüpft sind.

Wenn Sie zu Ihrem Computer einen oder mehrere Benutzer hinzugefügt haben, können Sie (als Computeradministrator) Änderungen am Konto all dieser Benutzer vornehmen. (Informationen über das Hinzufügen von Benutzern finden Sie im Abschnitt »Ein Benutzerkonto erstellen« weiter hinten in diesem Kapitel.)

Um den Kontotyp eines Benutzers zu ändern, gehen Sie zu *Einstellungen* | *Konten* | *Weitere Benutzer*. Klicken Sie auf den Namen des Kontos, das Sie ändern möchten, und dann auf *Kontotyp ändern*. Sie haben die Wahl zwischen *Standardbenutzer* und *Administrator*, wie im vorherigen Abschnitt beschrieben.

Wenn sich die Person mit einem Microsoft-Konto anmeldet, können Sie keine weiteren Änderungen vornehmen. (Sie können keine Änderungen am Microsoft-Konto einer anderen Person vornehmen; nur der Besitzer dieses Kontos kann das, indem er sich unter *https://account.microsoft.com* anmeldet.) Für Benutzer, die sich mit einem lokalen Benutzerkonto anmelden, können Sie einige zusätzliche Änderungen vornehmen, jedoch müssen Sie dazu in der Systemsteuerung unter *Benutzerkonten* beginnen (siehe Abbildung 10.2). Klicken Sie auf *Anderes Konto verwalten* und dann auf den Namen des Kontos, das Sie ändern möchten. Sie können die folgenden Änderungen vornehmen:

- **Kontoname** Der Name, den Sie hier ändern, ist der vollständige Name, der auf dem Anmeldebildschirm, im Startmenü und in den Benutzerkonten angezeigt wird.
- **Kennwort** Sie können ein Kennwort erstellen und einen Hinweis speichern, der Sie an ein vergessenes Kennwort erinnert. Wenn das Konto bereits durch ein Kennwort geschützt ist, können Sie das Kennwort über Benutzerkonten ändern oder entfernen. Weitere Informationen zu Kennwörtern finden Sie im Abschnitt »Kennwort festlegen oder ändern« weiter hinten in diesem Kapitel.
- **Kontotyp** Die Auswahlmöglichkeiten hier sind dieselben wie unter *Einstellungen* | *Konten*: *Administrator* (damit wird das Konto der Gruppe *Administratoren* hinzugefügt), oder *Standardbenutzer* (damit wird das Konto der Gruppe *Benutzer* hinzugefügt).
- **Löschen** Sie können das Konto löschen und dabei wählen, ob die Dateien des Benutzers gelöscht oder beibehalten werden sollen.

Wenn Sie sich mit einem lokalen Benutzerkonto anmelden, können Sie die folgenden zusätzlichen Änderungen an Ihrem eigenen Konto (also dem Konto, mit dem Sie gerade angemeldet sind) vornehmen, indem Sie auf die Links im linken Fensterbereich klicken:

- **Eigene Anmeldeinformationen verwalten** Dieser Link öffnet den Manager für Anmeldeinformationen, mit dem Sie gespeicherte Anmeldeinformationen verwalten können, die Sie für den Zugriff auf Netzwerkressourcen und Websites verwenden. Beachten Sie, dass der neue Microsoft Edge-Browser, der auf der Chromium-Engine basiert, seinen eigenen Speicher für gespeicherte Anmeldeinformationen hat und diesen ignoriert.

- **Kennwortrücksetzdiskette erstellen** Dieser Link ist nur verfügbar, wenn Sie mit einem lokalen Konto angemeldet sind. Er startet den Assistenten für vergessene Kennwörter, mit dem Sie auf einem Wechseldatenträger ein Tool zur Kennwortrücksetzung erstellen können. Alternativ können Sie mit Windows 11 ein vergessenes Kennwort wiederherstellen, indem Sie die Antworten auf die Fragen zum Zurücksetzen des Kennworts verwenden, die Sie beim Einrichten des Kontos ausgewählt haben.
- **Dateiverschlüsselungszertifikate verwalten** Dieser Link öffnet einen Assistenten, mit dem Sie Zertifikate erstellen und verwalten können, die die Verwendung von Encrypting File System (EFS) ermöglichen. EFS ist nur in den Pro- und Enterprise-Editionen von Windows 11 verfügbar und ermöglicht die Verschlüsselung von Ordnern und Dateien, damit sie nur für Personen mit der entsprechenden Zugriffsberechtigung einsehbar sind. Weitere Informationen finden Sie im Abschnitt »Informationen verschlüsseln« in Kapitel 12, »Sicherheit und Datenschutz in Windows 11«.
- **Erweiterte Benutzerprofileigenschaften konfigurieren** Diese Verknüpfung wird für den Wechsel zwischen einem lokalen Profil, das auf dem lokalen Computer gespeichert ist, und einem Roamingprofil verwendet, das in einer Domänenumgebung auf einem Netzwerkserver gespeichert ist. Bei einem lokalen Profil haben Sie auf jedem Computer, auf dem Sie arbeiten, ein anderes Profil. Ein Roamingprofil bleibt dagegen stets gleich, unabhängig davon, auf welchem Computer aus dem Netzwerk Sie sich anmelden. Ein Roamingprofil setzt ein Domänennetzwerk voraus, in dem die Active Directory-Dienste von Windows Server verfügbar sind. Microsoft-Konten und Azure AD-Konten verwenden einen anderen Mechanismus zum Synchronisieren von Einstellungen.
- **Eigene Umgebungsvariablen ändern** Diese Verknüpfung ist vor allem für Programmierer interessant. Sie öffnet ein Dialogfeld, in dem Sie Umgebungsvariablen erstellen und bearbeiten können, die nur für Ihr Benutzerkonto verfügbar sind; außerdem können Sie die systemweit gültigen Umgebungsvariablen einsehen, die für alle Konten gelten.

Konto löschen

Als lokaler Administrator können Sie jedes lokale Konto oder Microsoft-Konto löschen, das auf einem Windows 11-PC eingerichtet ist, es sei denn, das Konto ist gerade angemeldet. Um ein Konto zu löschen, gehen Sie zu *Einstellungen* | *Konten* | *Weitere Benutzer* und klicken Sie auf den Namen des Kontos, das Sie löschen möchten. Klicken Sie dann auf *Entfernen*. Windows warnt dann vor den Folgen des Löschens eines Kontos, zu denen auch das Entfernen der Dateien des Benutzers gehört.

> Hinweis
>
> **Windows lässt es nicht zu, dass Sie das letzte lokale Konto auf dem Computer löschen, selbst wenn Sie mit dem integrierten Konto *Administrator* angemeldet sind. Diese Einschränkung ist eine weitere Maßnahme, um die Sicherheit zu verbessern; sie soll den Benutzer veranlassen, für die normalen Arbeiten am Computer ein anderes Konto als *Administrator* zu verwenden.**

Nachdem Sie ein Benutzerkonto gelöscht haben, kann sich dieser Benutzer nicht mehr anmelden. Das Löschen eines Kontos hat noch eine weitere Auswirkung, die Sie beachten sollten: Sie können den Zugriff auf Ressourcen, die derzeit für den Benutzer freigegeben sind,

nicht wiederherstellen, indem Sie das Konto einfach neu erstellen. Das betrifft gemeinsam verwendete Dateien sowie die vom Benutzer verschlüsselten Dateien, persönliche Zertifikate und gespeicherte Kennwörter für Websites und Netzwerkressourcen. Der Grund dafür ist, dass die Berechtigungen nicht direkt mit dem Benutzernamen verknüpft sind, sondern mit der Sicherheitskennung (Security Identifier, SID) des Benutzers. Selbst wenn Sie mit demselben Namen und demselben Kennwort ein neues Konto erstellen, hat dieses Konto eine neue SID. Diese Sicherheitskennung ermöglicht keinen Zugriff auf Ressourcen, die für das ursprüngliche Konto zugänglich waren. (Weitere Informationen über Sicherheitskennungen finden Sie im Abschnitt »Grundlagen der Zugriffssteuerung in Windows 11« weiter hinten in diesem Kapitel.)

Expertentipp

Ein Konto löschen, ohne die Benutzerdaten zu löschen

In früheren Versionen von Windows gab es eine Option, mit der die Datendateien eines Kontos – Dokumente, Fotos, Musik, Downloads und andere im Benutzerprofil gespeicherte Dateien und Ordner – beim Löschen des Benutzerkontos erhalten blieben. Windows 11 bietet diese Option ebenfalls an, aber Sie finden sie nicht in den Einstellungen. Öffnen Sie stattdessen die *Benutzerkonten* in der Systemsteuerung. Klicken Sie auf *Anderes Konto verwalten*, wählen Sie das Konto aus, das Sie entfernen möchten, und klicken Sie dann auf *Konto löschen*.

Die Systemsteuerung lässt Sie auswählen, was mit den Dateien aus dem Benutzerprofil geschehen soll:

- **Dateien löschen** **Nachdem Sie *Dateien löschen* ausgewählt und im nächsten Fenster bestätigt haben, löscht Windows das Konto, sein Benutzerprofil und alle Dateien im Benutzerprofil dieses Kontos.**
- **Dateien behalten** **Windows kopiert bestimmte Teile des Benutzerprofils – insbesondere Dateien und Ordner, die auf dem Desktop und in den Ordnern *Dokumente, Favoriten, Musik, Bilder* und *Videos* gespeichert sind – in einen Ordner auf Ihrem Desktop, wo sie Teil Ihres Profils werden und unter Ihrer Kontrolle bleiben. Alle anderen Ordner im Benutzerprofil werden gelöscht, nachdem Sie Ihre Absicht auf der nächsten Seite bestätigt haben; E-Mail-Nachrichten und andere im Ordner *AppData* gespeicherte Daten werden ebenfalls gelöscht, ebenso wie die in der Registrierung gespeicherten Einstellungen.**

Den Anmeldevorgang sicherer machen

Wie im vorigen Abschnitt erwähnt, ist jedes Konto auf einem Windows 11-PC durch eine Reihe von Anmeldedaten gesichert, die aus einem Benutzernamen (der in Form einer E-Mail-Adresse vorliegen kann) und einem Kennwort bestehen. Sie können diese Anmeldedaten verwenden, um sich bei Ihrem Konto auf einem Windows 11-PC anzumelden: Wählen Sie auf dem Anmeldebildschirm Ihren Namen aus (falls er noch nicht ausgewählt ist) und geben Sie dann Ihr Kennwort ein.

Hinweis

Wenn Sie Ihren Computer zum ersten Mal einschalten oder nach der Abmeldung wieder darauf zugreifen, wird der Sperrbildschirm angezeigt. Der Sperrbildschirm zeigt normalerweise ein Bild, die aktuelle Uhrzeit und das Datum sowie Benachrichtigungen von ausgewählten Anwendungen an. (Sie können ein eigenes Bild für den Sperrbildschirm auswählen und festlegen, welche Informationen auf dem Sperrbildschirm angezeigt werden sollen. Weitere Informationen finden Sie im Abschnitt »Sperrbildschirm und Anmeldebildschirm anpassen« in Kapitel 4.) Um vom Sperrbildschirm zum Anmeldebildschirm zu gelangen, klicken Sie auf eine beliebige Stelle, drücken Sie eine beliebige Taste oder (wenn Sie einen Touchscreen haben) wischen Sie nach oben.

Expertentipp

Ohne Tastatur Strg+Alt+Entf drücken

Manche Netzwerkadministratoren aktivieren eine Richtlinie, die es für den Wechsel vom Sperrbildschirm zum Anmeldebildschirm erforderlich macht, die Tastenkombination Strg + Alt + Entf zu drücken. (Diese Tastenkombination, deren Rolle in der Windows-Sicherheit auf die frühesten Versionen von Windows NT zurückgeht, wird als »Secure Attention Sequence« bezeichnet.) Diese Anforderung kann es schwierig machen, sich auf einem Tablet ohne Tastatur bei Ihrem Unternehmensnetzwerk anzumelden – bis Sie den Trick kennen. Bei modernen hybriden Windows 11-PCs wie den Surface Pro- und Surface Book-Gerätefamilien von Microsoft kann das Display von der Tastatur getrennt werden; drücken Sie in dieser Konfiguration gleichzeitig den Ein-/Aus-Schalter und die Leiser-Taste, um die erforderliche Sequenz zu senden. In dem unwahrscheinlichen Fall, dass Sie Windows 11 auf einem Gerät der Windows 8-Ära mit einer dedizierten ⊞-Taste ausführen, drücken Sie gleichzeitig die ⊞-Taste und den Ein-/Aus-Schalter.

Die Anmeldung mit einem sicheren Kennwort kann lästig sein, vor allem wenn es lang ist und aus einer Mischung aus Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen besteht. Die ganze Sache wird noch schwieriger, wenn Sie das sichere Kennwort auf einem Gerät eingeben müssen, auf dem keine physische Tastatur vorhanden ist.

Um den Anmeldevorgang bequemer zu gestalten, ohne die Sicherheit zu beeinträchtigen, unterstützt Windows 11 mehrere Optionen, die Sie anstelle Ihres Kontokennworts verwenden können. Abbildung 10.5 zeigt die gesamte Palette der Alternativen, die Sie unter *Einstellungen* | *Konten* | *Anmeldeoptionen* finden.

Die ersten drei Optionen in der Liste beziehen sich auf Windows Hello, eine Funktion, die den Windows 11-Anmeldeprozess um eine Form der hardwarebasierten Sicherheit erweitert. Zu den weiteren Anmeldeoptionen auf dieser Seite gehören Tools zum Verwalten von physischen Sicherheitsschlüsseln sowie zum Einrichten und Verwalten der dynamischen Sperre.

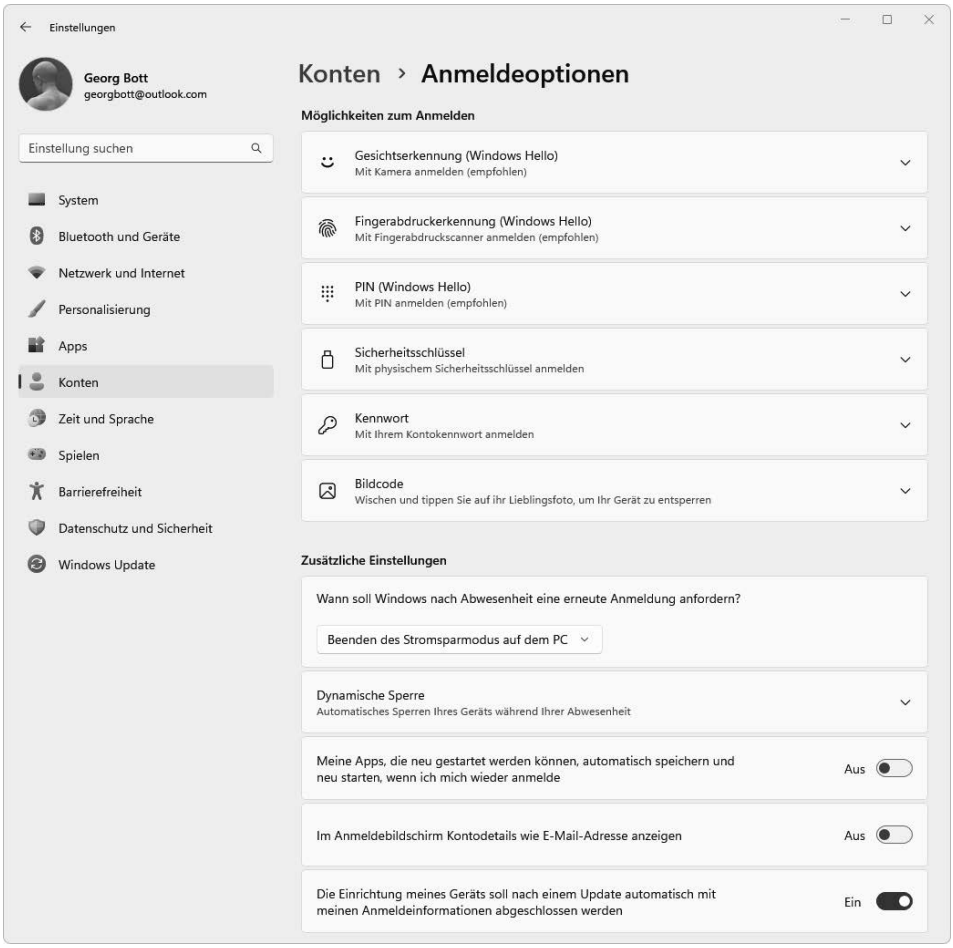

Abbildung 10.5 Die biometrischen Optionen von Windows Hello sind nur verfügbar, wenn Sie über eine kompatible Infrarotkamera oder einen Fingerabdruckleser verfügen.

Wenn Sie mehr als eine Option für die Anmeldung eingerichtet haben, können Sie eine andere Methode als die Standardmethode wählen, indem Sie auf dem Anmeldebildschirm auf *Anmeldeoptionen* klicken. Diese Möglichkeit könnte sich als nützlich erweisen, wenn beispielsweise Windows Hello Ihr Gesicht oder Ihren Fingerabdruck nicht erkennen kann. Die Symbole für jede der von Ihnen eingerichteten Optionen werden dann wie in Abbildung 10.6 zu sehen angezeigt; klicken oder tippen Sie auf eine, um die Methode zu wechseln.

Abbildung 10.6 Klicken Sie auf *Anmeldeoptionen*, um eine andere Anmeldemethode zu wählen. Wenn die biometrische Authentifizierung Windows Hello eingerichtet ist, werden hier möglicherweise Symbole für Gesichts- oder Fingerabdruckerkennung angezeigt.

Beachten Sie, dass diese alternativen Anmeldemöglichkeiten auch für einige Apps funktionieren, wie im Microsoft Store.

In den folgenden Abschnitten erläutern wir, wie Sie jede dieser Anmeldemethoden einrichten und verwalten können. Wir beginnen mit der wichtigsten sicheren Anmeldeoption von allen, die in den Einstellungen nicht verfügbar ist.

Mehr Sicherheit durch Multi-Faktor-Authentifizierung

Der größte Vorteil der Anmeldung mit einem Microsoft-Konto oder einem Azure AD-Konto ist unseres Erachtens die Unterstützung der Multi-Faktor-Authentifizierung, die für die Sicherheit Ihres PC und seiner Daten sorgt. (Diese Funktion wird oft als Zwei-Faktor-Authentifizierung oder 2FA bezeichnet, kann aber auch als Verifizierung in zwei Schritten oder »two-step verification« bezeichnet werden.) Die Einrichtung dauert nur wenige Minuten, und das Ergebnis ist eine Schutzschicht, die verhindert, dass eine böswillige Person gestohlene Anmeldedaten verwendet, um sich als Sie auszugeben.

Die gängigste Form der 2FA verwendet eine auf einem Smartphone installierte Authentifizierungs-App, um bei Bedarf eine zweite Form des Identitätsnachweises zu erbringen. In diesem Fall sind die beiden Faktoren das klassische »etwas, das Sie wissen« (Ihr Kennwort) und »etwas, das Sie haben« (das mobile Gerät, das Sie als vertrauenswürdiges Gerät eingerichtet haben). Die Kombination dieser beiden Faktoren stellt eine Hürde dar, die alle außer den entschlossensten Angreifern aufhalten wird.

Um diese Funktion für ein Microsoft-Konto zu aktivieren, gehen Sie zu *https://account.live.com/proofs* und melden Sie sich an. Auf dieser Seite können Sie Möglichkeiten zum Nachweisen Ihrer Identität hinzufügen und die mehrstufige Überprüfung aktivieren.

Für Geräte, die über Azure AD mit einer Organisation verbunden sind, muss ein Administrator die Multi-Faktor-Authentifizierung aktivieren. Nachdem dieser Schritt abgeschlossen ist, können Benutzer die Sicherheitsüberprüfung über das Azure AD-Portal *My Account* verwalten. Beginnen Sie auf *https://myaccount.microsoft.com*, melden Sie sich mit Ihrem Geschäfts-, Schul- oder Unikonto an und klicken Sie dann auf der Seite *Sicherheitsinformationen* auf *Anmeldemethode hinzufügen*; Sie können auch direkt mit *https://mysignins.microsoft.com/security-info* zu dieser Seite wechseln.

Für Windows 11 funktioniert die Identitätsüberprüfung am besten mit der App Microsoft Authenticator, die sowohl für Android- als auch für iOS-Smartphones im Store der jeweiligen Plattform oder unter *https://www.microsoft.com/authenticator* erhältlich ist. Diese App

verwaltet die Authentifizierung für Azure AD- und Microsoft-Konten; sie unterstützt auch die meisten Konten von Drittanbietern, einschließlich der Konten von Google, Facebook und Amazon. Die Authenticator-App unterstützt fingerabdruck- und gesichtsbasierte Überprüfungen auf kompatibler Hardware und funktioniert mit verschiedenen Arten von Smartwatches.

Wenn die Multi-Faktor-Authentifizierung aktiviert ist, müssen Sie diesen zusätzlichen Faktor verwenden, um Ihre Identität in Situationen nachzuweisen, die laut Microsoft zusätzliche Sicherheit erfordern, beispielsweise wenn Sie sich zum ersten Mal auf einem neuen Gerät anmelden oder Änderungen an den Kontoeinstellungen vornehmen; in der Regel müssen Sie dazu auf einem zuvor verifizierten Gerät eine Benachrichtigung bestätigen, beispielsweise mit der Microsoft Authenticator-App auf einem Smartphone.

Windows Hello verwenden

Mit dem Feature »Windows Hello« können Sie Ihren Windows 11-PC als vertrauenswürdiges Gerät konfigurieren, das Sie mit biometrischer Hardware oder einer gerätespezifischen PIN entsperren können. In dieser Konfiguration werden Ihre Anmeldedaten in verschlüsselter Form auf dem Gerät gespeichert. Um sich anzumelden, entsperren Sie diese Anmeldedaten mit einer PIN oder einer biometrischen Identifizierung (mit Ihrem Fingerabdruck oder Ihrem Gesicht).

Um Windows Hello einzurichten, müssen Sie zunächst Ihre Identität bestätigen, indem Sie Ihre Anmeldedaten korrekt eingeben. Nachdem Sie diesen Test bestanden haben, können Sie eine PIN hinzufügen und, insofern die erforderliche Hardware vorhanden ist, Ihre biometrischen Merkmale registrieren. Wenn dieser Registrierungsprozess abgeschlossen ist, können Sie das Kennwort überspringen und sich bei Windows 11 anmelden, indem Sie Ihre PIN eingeben oder das, was die Microsoft-Ingenieure als »biometrische Geste« bezeichnen, mithilfe der Gesichtserkennung oder eines Fingerabdrucklesers eingeben.

Das Gerät, mit dem Sie sich anmelden, fungiert als Authentifizierungskomponente, da Sie Ihre Identität bei seiner Einrichtung festgelegt haben; Ihre zusätzlichen Informationen (die PIN oder Ihre biometrischen Daten) sind mit dem angemeldeten Gerät verknüpft und werden nicht auf einem Remote-Server gespeichert. Diese Anordnung verhindert sogenannte Shoulder-Surfing-Angriffe, bei denen jemand versucht, Ihr Kennwort zu stehlen, indem er, während Sie sich anmelden, Ihre Tastatureingaben beobachtet. Da Windows Hello eine gerätespezifische PIN verwendet, können sich andere Personen nicht bei Ihrem Konto anmelden, es sei denn, sie stehlen auch Ihren Computer.

Wenn Sie möchten, können Sie ein Gerät auch so konfigurieren, dass die einzigen verfügbaren Anmeldeoptionen die Windows Hello-PIN oder biometrische Merkmale sind; in dieser Konfiguration sind die Anmeldeoptionen Kennwort und Bildcode nicht verfügbar. Um diese Option zu aktivieren, gehen Sie zu *Einstellungen* | *Konten* | *Anmeldeoptionen* und aktivieren Sie die Einstellung *Zur Verbesserung der Sicherheit, Windows Hello-Anmeldung nur für Microsoft-Konten auf diesem Gerät zulassen (empfohlen)*.

Expertentipp

Windows Hello for Business konfigurieren

Bei PCs mit Windows 11 in nicht verwalteten Umgebungen verwendet Windows Hello eine »Komfort-PIN« oder »benutzerfreundliche PIN«, um verschlüsselte Anmeldeinformationen auf dem Gerät zu entsperren. In verwalteten Bereitstellungen können Administratoren die Einstellungen für Windows Hello for Business mithilfe von Gruppenrichtlinien oder Software zur Verwaltung mobiler Geräte wie Microsoft Intune konfigurieren. Wenn diese Richtlinien aktiviert sind, werden die Anmeldeinformationen des Geräts durch ein Zertifikat oder einen Verschlüsselungsschlüssel gesichert, der wiederum an das Trusted Platform Module (TPM) auf dem Gerät gebunden ist; beim Entsperren des Geräts wird ein auf dem Zertifikat oder Schlüssel basierendes Authentifizierungstoken bereitgestellt. Diese Architektur macht die netzwerkbasierte Authentifizierung weniger anfällig für »Replay«-Angriffe (Angriffe durch Wiedereinspielung). Weitere Einzelheiten zu Windows Hello for Business finden Sie unter *https://bit.ly/windowsHelloForBusiness*.

PIN für Windows Hello einrichten

Windows 11 fordert Sie auf, eine PIN einzurichten, wenn Sie zum ersten Mal ein neues Benutzerkonto erstellen. Wenn Sie diesen Schritt bei der Einrichtung übersprungen haben, gehen Sie zur Seite *Einstellungen* | *Konten* | *Anmeldeoptionen* und klicken Sie auf *PIN (Windows Hello)*. Klicken Sie dann auf *Einrichten* und folgen Sie den Anweisungen auf dem Bildschirm. Sie müssen Ihre Identität bestätigen, indem Sie zunächst Ihr Kontokennwort eingeben. Geben Sie dann Ihre neue PIN ein und bestätigen Sie sie, wie in Abbildung 10.7 dargestellt. Die Mindestlänge beträgt vier Ziffern (nur 0–9), aber Ihre PIN kann so lang sein, wie Sie möchten. Wenn Sie eine komplexere und schwieriger zu erratende PIN wünschen, schalten Sie das Kontrollkästchen *Buchstaben und Symbole einschließen* ein.

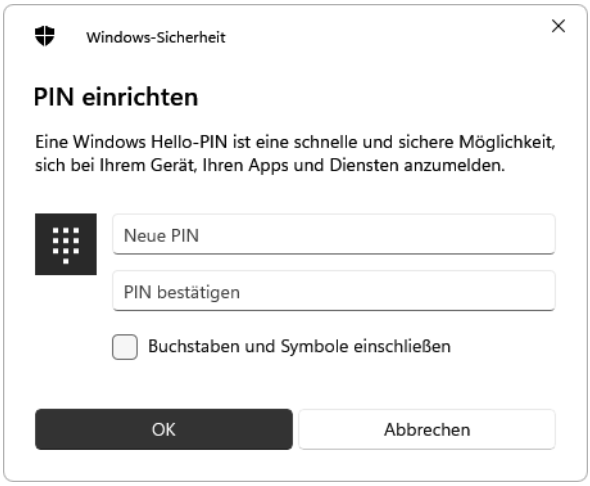

Abbildung 10.7 Eine PIN dient als bequeme Alternative für die Anmeldung bei Windows und die Überprüfung Ihrer Identität in Anwendungen und Diensten. Sie können eine PIN wählen, die länger als das Minimum von vier Zeichen ist.

Wenn Sie Ihre PIN ändern möchten, wählen Sie auf der Seite *Anmeldeoptionen* die Option *PIN (Windows Hello)* und klicken dann auf *PIN ändern*. Befolgen Sie die Anweisungen auf dem Bildschirm, um den Vorgang abzuschließen.

Um sich mit einer PIN anzumelden, geben Sie die Zahlen auf Ihrer Tastatur ein. Beachten Sie, dass Tasten, die Sie auf dem Ziffernblock der Tastatur eingeben, als Zahlen registriert werden, wenn Sie sich im Feld *PIN* auf den Anmeldebildschirm befinden, und zwar unabhängig davon, ob die Num-Sperre aktiviert ist. Wenn Ihr Computer nicht über eine Tastatur verfügt, wird auf dem Bildschirm ein Ziffernblock angezeigt, in den Sie Ihre PIN eingeben können. (Wenn der Ziffernblock nicht angezeigt wird, tippen Sie in das Feld für die PIN-Eingabe.)

Expertentipp

Machen Sie Ihre PIN noch sicherer

Vielleicht ist eine vierstellige PIN Ihrer Meinung nach zu einfach zu erraten. Aber Windows 11 lässt nur fünf Fehlversuche zu, bevor es keine weiteren Anmeldeversuche mehr annimmt. Nach vier Falscheingaben werden Sie aufgefordert, eine bestimmte Zeichenfolge einzugeben. Damit soll überprüft werden, ob Ihre Tastatur richtig arbeitet. Nach dem fünften Fehlversuch wird ein potenzieller Eindringling ausgesperrt. An diesem Punkt fordert Windows Sie auf, Ihr Gerät neu zu starten und sich erneut anzumelden. Nach einer Handvoll Fehlversuche akzeptiert Windows keine neuen Versuche mehr und fordert Sie auf, Ihr Kennwort einzugeben.

Stellen Sie sich die Überraschung eines Gauners vor, wenn er feststellt, dass eine PIN länger als vier Stellen sein kann. Wenn Sie eine sechsstellige PIN statt einer vierstelligen wählen, gibt es bereits eine Million möglicher Kombinationen. Auch der hartnäckigste Angreifer wird kaum diese Geduld aufbringen. Aber selbst eine achtstellige PIN ist einfacher als ein komplexes Kennwort einzugeben, obwohl sie bereits 100 Millionen Kombinationen zulässt.

Als noch sicherere Alternative können Sie das Kontrollkästchen *Buchstaben und Symbole einbeziehen* aktivieren und eine komplexe PIN einrichten, die aus acht Zeichen besteht, die mehr als eine Billion möglicher Kombinationen aus Zahlen, Buchstaben und Symbolen darstellen.

Wenn Sie sich bei einer Active Directory-Domäne oder Azure AD anmelden, kann ein Netzwerkadministrator mithilfe von Gruppenrichtlinien unter Windows 11 Pro oder Enterprise eine Mindestlänge für die PIN festlegen und die Verwendung von Buchstaben und Zahlen erzwingen, sodass die PIN praktisch nicht erraten werden kann. Diese Einstellungen befinden sich im Gruppenrichtlinien-Editor unter *Computerkonfiguration* | *Administrative Vorlagen* | *Windows-Komponenten* | *Windows Hello For Business*.

Windows Hello für biometrische Authentifizierung verwenden

Mit der entsprechenden Hardware können Sie sich mit einem Fingerabdruck anmelden oder, noch einfacher, indem Sie in die Kamera Ihres Computers schauen. Möglicherweise können Sie auch Ihre Identität mit Windows Hello verifizieren, wenn Sie einen Einkauf tätigen oder auf einen sicheren Dienst zugreifen.

Um Windows Hello für biometrische Anmeldungen auf einem PC zu verwenden, benötigen Sie eines der folgenden Geräte:

- Ein Fingerabdrucklesegerät, das das Windows Biometric Framework unterstützt. Falls diese Hardware nicht bereits im Gerät integriert ist, können Sie einen externen Fingerabdruckleser verwenden, der über USB angeschlossen wird.
- Eine spezielle 3D-Infrarotkamera, wie sie in Surface-Laptops und -Tablets von Microsoft sowie anderen modernen Geräten zu finden ist; beachten Sie, dass eine Standard-Webcam nicht funktioniert. Es gibt jedoch auch externe Webcams, die die biometrische Anmeldung mit Windows Hello unterstützen.

> **Hinweis**
>
> **Sie müssen eine PIN hinzufügen, wie weiter vorne in diesem Kapitel beschrieben, bevor Sie die biometrischen Funktionen von Windows Hello nutzen können. Diese PIN dient als Backup-Anmeldeoption für den Fall, dass Ihre biometrische Hardware nicht funktioniert oder Sie nicht erkennen kann.**

Um Windows Hello einzurichten, gehen Sie zu *Einstellungen* | *Konten* | *Anmeldeoptionen*. Erweitern Sie unter *Möglichkeiten zum Anmelden* entweder *Gesichtserkennung (Windows Hello)* oder *Fingerabdruckerkennung (Windows Hello)*. Klicken Sie dann für das biometrische Gerät, das Sie verwenden möchten, auf *Einrichten*.

Windows fordert Sie auf, Ihre PIN einzugeben, um Ihre Identität zu überprüfen. Danach müssen Sie Ihre biometrischen Daten erfassen. Bei der Gesichtserkennung müssen Sie in die Kamera schauen (siehe Abbildung 10.8); um einen Fingerabdruckleser einzurichten, folgen Sie den Aufforderungen, Ihren Finger mehrmals auf das Lesegerät aufzulegen, bis Windows Hello die benötigten Daten erfasst hat.

Wenn Sie das Scannen von Fingerabdrücken einrichten, können Sie zusätzliche Finger registrieren, damit Sie eine Alternative haben, wenn der Finger, den Sie normalerweise verwenden, zum Beispiel mit einem Pflaster oder Verband bedeckt ist. Klicken Sie auf *Weiteren hinzufügen*, nachdem Sie die Registrierung für einen Fingerabdruck abgeschlossen haben. Wenn Sie später einen weiteren Fingerabdruck hinzufügen möchten, kehren Sie zu *Einstellungen* | *Konten* | *Anmeldeoptionen* | *Fingerabdruckerkennung* zurück und klicken Sie auf *Finger hinzufügen*. Sie können einen zusätzlichen Fingerabdruck auch mit einem anderen Benutzerkonto auf demselben Gerät verknüpfen. Melden Sie sich bei dem geänderten Konto an und richten Sie dort den zweiten Fingerabdruck ein. Wenn Sie das Gerät neu starten, können Sie Ihr Konto auswählen, indem Sie den Fingerabdruck verwenden, der mit diesem Konto verknüpft ist.