KAPITEL 1

# Microsoft 365-Dienste entwerfen und implementieren

Auch wenn es möglich ist, einfach mit der Bereitstellung von Microsoft 365 zu beginnen, nachdem Ihr Unternehmen die Entscheidung getroffen hat, diese Technologie einzusetzen, können Sie mehr aus einer Microsoft 365-Bereitstellung herausholen, wenn Sie einige Planungs- und Entwurfsarbeiten durchführen, bevor Sie Microsoft 365-Dienste konfigurieren. In diesem Kapitel erfahren Sie mehr über die Planung einer Microsoft 365-Architektur, über die Bereitstellung eines Microsoft 365-Mandanten und über die Konfiguration dieses Mandanten und der Abonnements. Außerdem lernen Sie die Schritte kennen, die Sie unternehmen müssen, um die Migration von Benutzern und Daten aus einer herkömmlichen lokalen Umgebung in eine Microsoft 365-Umgebung zu planen.

**In diesem Kapitel abgedeckte Prüfungsziele:**

- Prüfungsziel 1.1: Planen der Architektur
- Prüfungsziel 1.2: Bereitstellen eines Microsoft 365-Mandanten
- Prüfungsziel 1.3: Verwalten des Microsoft 365-Abonnements und des Mandantenstatus
- Prüfungsziel 1.4: Planen der Migration von Benutzern und Daten

## Prüfungsziel 1.1: Planen der Architektur

Dieser Abschnitt befasst sich mit der Planung Ihrer Microsoft 365-Architektur. Um diese Qualifikation zu beherrschen, müssen Sie verstehen, wie Sie die Integration Ihrer bestehenden lokalen Umgebung mit Microsoft 365 planen, Ihr Bereitstellungsteam identifizieren, die zu verwendende Identitäts- und Authentifizierungslösung bestimmen und die Modernisierung Ihrer Unternehmensanwendung planen.

**Dieser Abschnitt behandelt die folgenden Themen:**

- Planen der Integration von Microsoft 365 und von lokalen Umgebungen
- Ermitteln des Teams für die Bereitstellung von Workloads
- Planen einer Identitäts- und Authentifizierungslösung
- Planen der Modernisierung von Unternehmensanwendungen

## Planen der Integration von Microsoft 365 und von lokalen Umgebungen

Wenn Sie eine Migration zu Microsoft 365 planen oder von Grund auf neu mit einer Bereitstellung beginnen, müssen Sie sicherstellen, dass bestimmte Voraussetzungen für die lokale Infrastruktur erfüllt sind. Diese Anforderungen an die lokale Infrastruktur beziehen sich auf die Netzwerkkonfiguration, Identitätsabhängigkeiten, Clientbetriebssysteme und die Bereitstellung von Microsoft 365 Apps for Enterprise. Außerdem müssen Sie Entscheidungen bezüglich der Strategie für die Verwaltung mobiler Geräte und den Datenschutz treffen.

### Netzwerke

Herkömmliche Netzwerke bieten Benutzern Zugriff auf Daten und Anwendungen, die in Rechenzentren gehostet werden, die sich im Besitz des Unternehmens befinden und von diesem betrieben werden und die durch starke Schutzmechanismen wie Firewalls geschützt sind. In diesem traditionellen Modell greifen die Benutzer in erster Linie über geschützte interne Netzwerke von Zweigstellen aus über WAN-Verbindungen oder aus der Ferne über VPN-Verbindungen auf Ressourcen zu.

Die Modelle Microsoft 365 und Office 365 verlagern einige (wenn nicht sogar alle) Anwendungen und Daten von geschützten internen Netzwerken an Standorte, die außerhalb des Umkreisnetzwerkes in der öffentlichen Cloud gehostet werden. Beim Wechsel von einer Umgebung, in der alle Ressourcen vor Ort gehostet werden, zu einer Umgebung, in der sich ein erheblicher Teil der Infrastruktur in der Cloud befindet, muss die Netzwerkumgebung vor Ort so konfiguriert sein, dass Microsoft 365 effektiv und effizient arbeiten kann. Wenn keine Schritte unternommen werden, um den Datenverkehr zwischen Benutzern und den Microsoft 365- oder Office 365-Diensten zu optimieren, wird dieser Datenverkehr erhöhten Latenzzeiten ausgesetzt sein, die durch Paketprüfung, Netzwerk-Hairpinning und mögliche unbeabsichtigte Verbindungen zu geografisch weit entfernten Microsoft 365- und Office 365-Dienst-Endpunkten verursacht werden.

Wenn Sie die Netzwerkanforderungen für Microsoft 365 verstehen, können Sie auch beurteilen, ob Microsoft 365 für eine bestimmte Organisation geeignet ist. So wäre es beispielsweise eine Herausforderung, Microsoft 365 in einer wissenschaftlichen Basis in der Antarktis bereitzustellen, wo nur eine begrenzte Internetverbindung mit geringer Bandbreite zur Verfügung steht.

## Internetverbindungen für Clients

Um Microsoft 365 nutzen zu können, müssen die Clients in der Lage sein, über die Ports 80 und 443 nicht authentifizierte Verbindungen zu den Office 365- und Microsoft 365-Servern im Internet herzustellen. Bei manchen Netzwerken, insbesondere denen kleinerer Unternehmen, können die folgenden Nerzwerkverbindungsprobleme auftreten:

- **Clients sind mit APIPA-Adressen konfiguriert** Falls Clients mit IP-Adressen aus dem APIPA-Adressbereich (169.254.0.0/16) (Automatic Private IP Addressing) konfiguriert sind, können diese sehr wahrscheinlich keine Internetverbindungen herstellen und daher auch nicht auf Office 365- und Microsoft 365-Ressourcen zugreifen. Sie sollten daher IP-Adressen aus dem privaten Adressbereich verwenden und ein geeignetes Standardgateway konfigurieren, über das sich die Clients entweder direkt oder indirekt mit dem Internet verbinden können.
- **Kein Standardgateway** Clients müssen mit der Standardgatewayadresse eines Geräts konfiguriert sein, das Datenverkehr in das Internet routen kann. Das Gerät, das als Standardgateway dient, muss nicht direkt mit dem Internet verbunden sein, jedoch muss es den Datenverkehr an ein Gerät weiterleiten können, das dann wohl mit dem Internet verbunden ist. Clients, denen kein Standardgateway zugewiesen ist, sind nicht in der Lage, auf Office 365- und Microsoft 365-Ressourcen zuzugreifen.
- **Firewall-Konfiguration** Clients benötigen Zugriff auf bestimmte Endpunkte, die von Microsoft 365 und Office 365 verwendet werden. Details zu diesen Endpunkten werden weiter hinten in diesem Kapitel behandelt.
- **Proxyserver-Authentifizierung** Microsoft 365 und Office 365 funktionieren nicht, wenn ein dazwischen liegender Proxyserver für Verbindungen Authentifizierung erfordert. Sie müssen entweder für die Microsoft 365- und Office 365-Endpunkte die Authentifizierung deaktivieren oder die Proxyserver-Authentifizierung komplett abschalten.

## Verwaltung von Microsoft 365-Endpunkten

Ein Microsoft 365- oder Office 365-Endpunkt ist eine URL oder IP-Adresse, die einen bestimmten Microsoft 365- oder Office 365-Dienst hostet. Beispiele sind die Adressen, die verwendet werden, wenn ein Outlook-Client mit Exchange Online oder ein mobiles Gerät mit einem Endpunkt zur Geräteregistrierung verbunden wird. Organisationen mit einem oder mehreren Bürostandorten muss ihr Netzwerk so konfiguriert sein, dass der Zugriff auf diese Endpunkte möglich ist.

Microsoft empfiehlt, dass Unternehmen den Datenverkehr für Microsoft 365- und Office 365-Endpunkte optimieren, indem sie den gesamten Datenverkehr direkt durch die Perimeter-Firewall leiten und diesen Datenverkehr von der Prüfung und Verarbeitung auf Paketebene ausnehmen. Auf diese Weise wird die Latenz bei der Verbindung mit Microsoft 365- und Office 365-Ressourcenendpunkten reduziert. Außerdem werden die Auswirkungen auf diese Perimeter-Geräte reduziert, die den Datenverkehr zu bekannten vertrauenswürdigen Standorten ignorieren.

Microsoft teilt jeden Microsoft 365- und Office 365-Endpunkt in eine von drei Kategorien ein. Anhand dieser Kategorien können Sie bestimmen, wie Sie den Datenverkehr zu Microsoft 365- und Office 365-Endpunkten am besten behandeln. Die Endpunkte der Kategorien sind wie folgt:

- **Optimieren** Endpunkte mit dieser Klassifizierung sind für die Konnektivität für jeden Microsoft 365- und Office 365-Dienst erforderlich. Auf Endpunkte dieser Kategorie entfallen ca. 75 % der Bandbreite, des Datenvolumens und der einzelnen Verbindungen. Diese Endpunkte verursachen die meisten Probleme, wenn es zu Unterbrechungen der Netzwerkleistung, Latenz oder Verfügbarkeit kommt.
- **Zulassen** Endpunkte mit dieser Klassifizierung sind für die Konnektivität zu speziellen Microsoft 365- sowie Office 365-Diensten und -Funktionen erforderlich, verursachen aber bei Störungen der Netzwerkleistung, der Latenz oder der Verfügbarkeit weniger Probleme als Endpunkte der Kategorie *Optimieren*.
- **Standard** Endpunkte mit dieser Klassifizierung erfordern keine spezielle Optimierung und können wie anderer Datenverkehr behandelt werden, der für Standorte im Internet bestimmt ist.

Microsoft gibt Empfehlungen für die Konfiguration des Verkehrsflusses zu Endpunkten. Diese Empfehlungen sind in Tabelle 1–1 aufgeführt.

| Endpunktkategorie(n) | Empfehlung |
|---|---|
| Optimieren<br>Zulassen | Umgehung von Optimieren-Endpunkten auf Netzwerkgeräten und Diensten, die Abfangen von Datenverkehr, SSL-Entschlüsselung, umfassende Paketüberprüfung (Deep Packet Inspection) und Inhaltsfilterung ausführen. |
| Optimieren | Umgehen Sie firmeninterne und cloudbasierte Proxy-Geräte oder -Dienste, die für das allgemeine Surfen im Internet verwendet werden. |
| Optimieren<br>Zulassen | Priorisieren Sie die Auswertung dieser Endpunkte als vollständig vertrauenswürdig durch Ihre Netzwerkinfrastruktur und Perimetersysteme. |
| Optimieren<br>Zulassen | Reduzieren oder eliminieren Sie das WAN-Backhauling. Erleichterung des direkten verteilten Internetzugangs für Endpunkte von Zweigstellen aus. |
| Optimieren | Konfigurieren Sie getrennte Tunnel für VPN-Benutzer, um direkte Konnektivität zu diesen Cloud-Endpunkten zu ermöglichen. |
| Optimieren<br>Zulassen | Konfigurieren Sie die Priorisierung für Endpunkte bei der Konfiguration von softwaredefinierten Wide Area (SD-WAN), um Latenzzeiten und Routing zu minimieren. |
| Optimieren<br>Zulassen | Stellen Sie sicher, dass die durch die DNS-Namensauflösung (Domain Name System) zurückgegebenen IP-Adressen dem Routing-Ausgangspfad für diese Endpunkte entsprechen. |

**Tab. 1–1** Optimierungsmethoden für Endpunkte

***HINWEIS***

**In der Vergangenheit hat Microsoft andere Endpunktkategorien als die hier aufgeführten verwendet, und zwar *erforderlich* und *optional*. Einige Dokumentationen beziehen sich immer noch auf diese früher verwendeten Endpunktkategorien.**

***WEITERE INFORMATIONEN*** **Endpunktkategorien**

**Weitere Informationen über die verschiedenen Microsoft 365- und Office 365-Endpunktkategorien finden Sie unter folgender Adresse: *https://docs.microsoft.com/microsoft-365/enterprise/urls-and-ip-address-ranges?view=o365-worldwide*.**

### Ausgehende Firewall-Ports

Clients, wie beispielsweise Computer, auf denen Windows 10 ausgeführt wird, müssen in der Lage sein, über bestimmte Protokolle und Ports Verbindungen zu Office 365-Servern im Internet herzustellen. Falls bestimmte Ports und Protokolle durch eine Perimeter-Firewall blockiert werden, können die Clients bestimmte Microsoft 365- und Office 365-Dienste nicht nutzen. Tabelle 1–2 führt die Protokolle und Ports auf, die für Clients in einem internen Netzwerk geöffnet sein müssen, damit sie Verbindungen zu den Hosts im Internet herstellen können.

| Protokoll | Port | Verwendet von |
|---|---|---|
| TCP | 443 | Microsoft 365 Admin Portal<br>Outlook<br>Outlook Web App<br>SharePoint Online<br>Skype for Business-Client<br>ADFS-Verbund<br>ADFS-Proxy |
| TCP | 25 | Mail-Routing |
| TCP | 587 | SMTP-Relay |
| TCP | 143/993 | IMAP Simple Migration Tool |
| TCP | 80/443 | Microsoft Azure Active Directory Synchronisierungstool<br>Exchange Verwaltungskonsole<br>Exchange Verwaltungsshell |
| TCP | 995 | Sicheres POP3 |
| PSOM/TLS | 443 | Skype for Business Online: Ausgehende Datenfreigabe |
| STUN/TCP | 443 | Skype for Business Online: Ausgehende Video-, Audio- und Anwendungsfreigabesitzungen |
| STUN/UDP | 3478 | Skype for Business Online: Ausgehende Video- und Audiositzungen |

→

| Protokoll | Port | Verwendet von |
|---|---|---|
| UDP | 3478–3481 | Teams |
| TCP | 5223 | Skype for Business Online: Push-Benachrichtigungen für mobile Clients |
| UDP | 20000–45000 | Skype for Business Online: Ausgehende Telefonate |
| RTC/UDP | 50000–59000 | Skype for Business Online: Ausgehende Video- und Audiositzungen |

**Tab. 1–2** Ausgehende Portanforderungen von Office 365

Die Anzahl der IP-Adressen und URLs, die Sie für den Ausschluss konfigurieren müssen, ist erheblich, und eine vollständige Liste würde den Rahmen dieses Buches sprengen. Die URLs und IP-Adressbereiche, die mit Microsoft 365 und Office 365 verbunden sind, ändern sich ständig. Sie können einen REST-basierten Webdienst abonnieren, der eine Liste der Endpunkte bereitstellt, einschließlich der aktuellen Version der Liste und der Änderungen, die an der Liste vorgenommen wurden, um sie für die Konfiguration von Netzwerk-Perimeter-Geräten, einschließlich Firewalls und Proxyservern, zu verwenden.

***WEITERE INFORMATIONEN*** **Microsoft 365-Endpunkte verwalten**

**Weitere Informationen über die Verwaltung von Microsoft 365-Endpunkten finden Sie unter folgender Adresse: *https://docs.microsoft.com/de-de/microsoft-365/enterprise/managing-office-365-endpoints?view=o365-worldwide*.**

### Lokale ausgehende Netzwerkverbindungen

Eine Möglichkeit, die Verbindungslatenz zu verringern, besteht darin, die Netzwerke der Zweigstellen für lokale DNS- und ausgehende Internetverbindungen zu konfigurieren, anstatt den gesamten DNS- und ausgehenden Internetverkehr über eine WAN-Verbindung zur Hauptniederlassung zu leiten, bevor er in das Internet geleitet wird. Das Routing des internetgebundenen Datenverkehrs von Zweigstellen über ein WAN, bevor er wieder ins Internet gelangt, wird als WAN-Backhauling bezeichnet. Es ist besonders wichtig, dies beim Microsoft 365- und Office 365-Datenverkehr in der Kategorie *Optimieren* zu vermeiden.

Microsoft 365- und Office 365-Dienste werden im globalen Microsoft-Netzwerk ausgeführt. Dieses Netzwerk ist mit Servern auf der ganzen Welt konfiguriert. Daher gibt es höchstwahrscheinlich in der Nähe jeder Zweigstelle einen Front-End-Server. Wird der Datenverkehr über ein WAN geleitet, anstatt ihn direkt von der Zweigstelle ausgehen zu lassen, führt dies zu unnötigen Latenzzeiten.

Der DNS-Verkehr zu Microsoft 365- und Office 365-Endpunkten sollte ebenfalls in der Zweigstelle abgewickelt werden. Dadurch wird sichergestellt, dass DNS-Server mit dem nächstgelegenen lokalen Front-End-Server antworten. Wenn DNS-Anfragen über WAN-Verbindungen weitergeleitet werden und nur über einen einzigen Standort der Hauptniederlassung laufen, werden die Clients zu den Front-End-Servern geleitet, die dem Standort der Hauptniederlassung am nächsten sind, und nicht zu der Niederlassung, von der die DNS-Anfrage stammt.

### Netzwerk-Hairpins vermeiden

Netzwerk-Hairpins treten auf, wenn VPN- oder WAN-Verkehr, der für einen bestimmten Endpunkt bestimmt ist, zunächst einen Zwischenstandort passieren muss, z. B. ein Sicherheitsgerät, ein cloudbasiertes Web-Gateway oder einen Cloud-Access-Broker, was zu einer Umleitung an einen geografisch entfernten Standort führen kann. Nehmen wir zum Beispiel an, ein Unternehmen namens Tailwind Traders hat eine australische Niederlassung, der gesamte Datenverkehr zu Microsoft 365- und Office 365-Endpunkten muss jedoch über ein cloudbasiertes Sicherheitsgerät in einem Rechenzentrum in Kanada laufen. Diese Konfiguration wird höchstwahrscheinlich zu unnötigen Latenzen führen. Selbst wenn der Datenverkehr der Zweigstelle lokal abgewickelt wird, wirkt sich dies negativ auf die Leistung aus, wenn er über einen geografisch weit entfernten Zwischenstandort geleitet wird.

Zu den Möglichkeiten, das Risiko von Netzwerk-Hairpins zu minimieren, gehören die folgenden:

- Sicherstellen, dass der ISP, der den Internet-Egress-Datenverkehr für die Zweigstelle bereitstellt, eine direkte Peering-Beziehung mit dem globalen Microsoft-Netzwerk in der Nähe des Standorts unterhält
- Konfigurieren des Egress-Routings, um vertrauenswürdigen Microsoft 365- und Office 365-Datenverkehr direkt an Microsoft 365- und Office 365-Endpunkte zu senden, anstatt ihn über zwischengeschaltete Dienste oder Geräte verarbeiten zu lassen

### SD-WAN-Geräte bereitstellen

SD-WAN-Geräte (Software-defined Wide Area Network) sind Netzwerkgeräte, die automatisch so konfiguriert werden können, dass der Datenverkehr am effizientesten an Microsoft 365- und Office 365-Endpunkte in den Kategorien *Optimieren* und *Zulassen* weitergeleitet wird. Wenn sie konfiguriert sind, kann der übrige Netzwerkverkehr – einschließlich des Datenverkehrs zu lokalen Workloads, des allgemeinen Internetverkehrs und des Datenverkehrs zu Microsoft 365- und Office 365-Standardendpunkten – an geeignete Stellen weitergeleitet werden, einschließlich Netzwerksicherheitsgeräten. Microsoft hat ein Partnerprogramm für SD-WAN-Anbieter, um die automatische Konfiguration von Geräten zu ermöglichen.

> ***WEITERE INFORMATIONEN*** **Prinzipien von Microsoft 365-Netzwerkverbindungen**
>
> **Weitere Informationen über die Prinzipien von Microsoft 365-Netzwerkverbindungen finden Sie unter folgender Adresse: *https://docs.microsoft.com/microsoft-365/enterprise/microsoft-365-network-connectivity-principles*.**

### Empfohlene Bandbreite

Zahlreiche Faktoren beeinflussen die Netzwerkbandbreite, die ein Unternehmen für den erfolgreichen Einsatz von Microsoft 365 benötigt. Zu diesen Faktoren gehören:

- Die Microsoft 365-Dienste, die das Unternehmen abonniert hat

- Die Anzahl der Clients, die sich zu einem beliebigen Zeitpunkt von einem Standardort aus mit Microsoft 365 verbindet
- Die Art der Interaktion (welche Dienste werden wie oft genutzt) zwischen Client und Microsoft 365
- Die Performance des Internetbrowsers auf den einzelnen Clientcomputern
- Die Kapazität der Netzwerkverbindung, die den einzelnen Clientcomputern zur Verfügung steht
- Die Netzwerktopologie des Unternehmens

***WEITERE INFORMATIONEN*** **Ermitteln der Bandbreitenanforderungen**

**Weitere Informationen über die Bandbreitenplanung für Microsoft 365 finden Sie unter folgender Adresse: *https://docs.microsoft.com/microsoft-365/enterprise/network-and-migration-planning*.**

### ExpressRoute

ExpressRoute für Office 365 bietet eine private Hochgeschwindigkeitsverbindung zwischen dem lokalen Netzwerk eines Unternehmens und den Rechenzentren von Microsoft. Clients, die das lokale Netzwerk einer Organisation nutzen, in dem ExpressRoute für Office 365 vorhanden ist, werden automatisch über die ExpressRoute geleitet; dieser Datenverkehr läuft dann nicht über das Internet. Wenn eine Organisation bereits über eine Azure ExpressRoute-Schaltung verfügt, kann sie den Zugriff auf Office 365 aktivieren, indem sie Routenfilter konfiguriert, um sicherzustellen, dass Microsoft 365-Dienste verfügbar sind.

***WEITERE INFORMATIONEN*** **ExpressRoute für Office 365**

**Weitere Informationen über ExpressRoute für Office 365 finden Sie unter folgender Adresse: *https://docs.microsoft.com/microsoft-365/enterprise/network-planning-with-expressroute*.**

## Windows 10 Enterprise Edition

Eine Microsoft 365 Enterprise-Lizenz umfasst eine Lizenz für das Betriebssystem Windows 10 Enterprise Edition. Im Rahmen der Einführung von Microsoft 365 muss sichergestellt werden, dass auf allen Windows-Client-Computern diese Edition des Windows 10-Betriebssystems ausgeführt wird.

Organisationen, die über eine bestehende Windows-Client-Bereitstellung verfügen, sollten ein In-Place-Upgrade mit Microsoft Endpoint Configuration Manager (früher System Center Configuration Manager) oder Microsoft Deployment Toolkit durchführen. Configuration Manager (Current Branch) bietet Organisationen die am besten automatisierte Methode für das Upgrade und die Migration bestehender Computer von früheren Versionen des Windows-Client-Betriebssystems auf Windows 10.

Organisationen, die neue Computer mit Windows 10 Enterprise Edition Version 1703 oder höher bereitstellen, können Windows Autopilot verwenden, um den Bereitstellungs- und Konfigurationsprozess auszulösen, indem sie sich mit ihren Schul- oder Arbeitskonto anmelden. Organisationen, die die Pro-Edition verwenden, können Windows Autopilot auch dazu nutzen, um diese Computer automatisch auf die Enterprise-Edition zu aktualisieren.

***WEITERE INFORMATIONEN*** **Microsoft 365 und Windows 10 Enterprise**

**Weitere Informationen über den Zusammenhang zwischen Microsoft 365 und Windows 10 Enterprise Edition finden Sie unter folgender Adresse: *https://docs.microsoft.com/windows/deployment/deploy-m365*.**

## Datenschutz

Bei der Planung der Datenschutzstrategie Ihres Unternehmens für Microsoft 365 ist der erste und vielleicht wichtigste Schritt, sich mit den Rechts- und Compliance-Teams Ihres Unternehmens in Verbindung zu setzen, um festzustellen, welchen Compliance-Standards das Unternehmen unterliegt, z. B. der General Data Protection Regulation (GDPR) oder dem Health Insurance Portability and Accountability Act (HIPAA). Nachdem Sie die spezifischen Compliance-Standards oder -Vorschriften ermittelt haben, an die sich Ihr Unternehmen halten muss, müssen Sie die folgenden Fragen beantworten:

- Welches sind die angemessenen Sicherheits- und Informationsschutzniveaus für unsere Organisation?
- Welches Klassifizierungsschema für Dokumente ist für unsere Organisation angemessen?
- Welche Schritte müssen unternommen werden, damit die angemessene Sicherheitsstufe innerhalb von Microsoft 365 und Office 365 konfiguriert ist?
- Ist es notwendig, für Microsoft 365 und Office 365 die Verwaltung privilegierter Zugriffe zu konfigurieren?

### Sicherheits- und Informationsschutzstufen

Microsoft 365 ermöglicht es Unternehmen, ihre eigenen Sicherheits- und Schutzstufen zu entwickeln. Auch wenn es möglich ist, eine verwirrende Anzahl von Sicherheitsstufen für den Informationsschutz zu erstellen, erhöht dies die Komplexität für Endbenutzer, die versuchen zu verstehen, welche Stufe angemessen ist, und für Compliance-Mitarbeiter, die feststellen müssen, ob die angemessene Stufe ausgewählt wurde.

Microsoft empfiehlt, dass Unternehmen mindestens drei verschiedene Sicherheitsstufen für den Informationsschutz vorsehen. Je höher die Sicherheitsstufen für den Informationsschutz, desto besser sind die Daten geschützt, aber desto schwieriger wird es für die Benutzer, mit diesen Daten zu interagieren. Nur für den Zugriff auf die vertraulichsten Daten sollte ein Benutzer bei jedem Öffnen eines Dokuments eine mehrstufige Authentifizierung (MFA) durchlaufen müssen. Microsoft schlägt die folgenden Stufen vor:

- **Baseline** Ein Mindeststandard für den Schutz von Daten, Identitäten und den Geräten, die für die Interaktion mit Unternehmensdaten verwendet werden.
- **Vertraulich** Ein Zwischenstandard für Daten, die als vertraulich gelten, für die aber nicht die strengsten Sicherheitskontrollen erforderlich sind.
- **Hochgradig reguliert** Erfordert die strengsten Sicherheitskontrollen. Dieser Standard ist wahrscheinlich nur für einen kleinen Teil der Daten einer Organisation geeignet. Sie könnten z. B. verlangen, dass der Zugriff auf Daten von einem verwalteten Gerät nur für eine begrenzte Zeit möglich ist, nachdem ein Benutzer die mehrstufige Authentifizierung durchgeführt hat.

### Klassifizierungsschemata

Klassifizierungsschemata ermöglichen es Ihnen, bestimmten Informationen, wie z. B. einem Dokument oder einer E-Mail-Nachricht, eine Informationsschutzstufe zuzuweisen. Microsoft 365 enthält die folgenden Klassifizierungsschemata:

- **Typen vertraulicher Informationen für Office 365** Office 365 erkennt automatisch bestimmte Informationstypen, wie z. B. Kreditkarten- oder Reisepassnummern. Sie können die Typen vertraulicher Informationen von Office 365 nutzen, um automatisch Regeln und Richtlinien zur Verhinderung von Datenverlusten anzuwenden, damit diese Daten das angemessene Schutzniveau haben.
- **Office 365-Aufbewahrungsbezeichnungen** Mit Office 365-Aufbewahrungsbezeichnungen können Sie festlegen, wie lange bestimmte Daten in Exchange, SharePoint Online und OneDrive gespeichert werden sollen. Office 365-Aufbewahrungsbezeichnungen können die zuvor beschriebenen Sicherheits- und Informationsschutzstufen verwenden: Baseline, vertraulich, stark reguliert. Sie können auch benutzerdefinierte Informationsschutzstufen verwenden, die von der Organisation festgelegt wurden.
- **Azure Information Protection (AIP)-Bezeichnungen und -Schutz** AIP bietet eine weitere Reihe von Optionen für die Klassifizierung und den Schutz von Dokumenten und E-Mail-Nachrichten. Ein Vorteil von AIP ist, dass es mit Dokumenten verwendet werden kann, die außerhalb von Office 365-Standorten wie Exchange Online, SharePoint Online und OneDrive gespeichert sind. AIP-Bezeichnungen und -Schutz können automatisch auf der Grundlage von Regeln und Bedingungen, die von einem Administrator definiert wurden, manuell von Benutzern oder in Verbindung mit automatischen Empfehlungen, die den Benutzern angezeigt werden, angewendet werden.

### Verbesserung des Sicherheitsniveaus

Bei der Planung Ihrer Microsoft 365-Informationsschutzstrategie müssen Sie über die Informationsklassifizierung, die Aufbewahrungsrichtlinien und den Informationsschutz hinausgehen. Sie müssen außerdem zusätzliche Microsoft 365-Sicherheitstechnologien aktivieren. Zu diesen Technologien gehören die folgenden:

- **Richtlinien für das Bedrohungsmanagement** Sie können im Security & Compliance Center Richtlinien für das Bedrohungsmanagement konfigurieren. Zu den Richtlinien gehören Advanced Threat Protection (ATP), Antiphishing, Antischadsoftware, ATP Sichere Anlagen, ATP Sichere Links, Antispam (Mail-Filterung) und E-Mail-Authentifizierung.
- **Mandantenweite Einstellungen in Exchange Online** Sie können die Sicherheit verbessern, indem Sie den entsprechenden E-Mail-Fluss (auch als Transportregeln bekannt) implementieren und die moderne Authentifizierung aktivieren, die Ihnen die Verwendung der mehrstufigen Authentifizierung ermöglicht.
- **SharePoint-Einstellungen** Sie können die Sicherheit erhöhen, indem Sie Einstellungen für das externe Teilen konfigurieren. Zu den Optionen gehören die Beschränkung der Freigabe auf authentifizierte externe Benutzer, das Zulassen anonymer Zugriffslinks, die Konfiguration von Ablaufzeiten für anonyme Zugriffslinks und Standard-Linktypen.
- **Azure Active Directory-Einstellungen** Sie können die Sicherheit erhöhen, indem Sie benannte Standorte konfigurieren, die Teil des bedingten Zugriffs sind, und Apps blockieren, die keine moderne Authentifizierung unterstützen.
- **Microsoft Defender for Cloud Apps (früher Cloud App Security)** Microsoft Defender for Cloud Apps ermöglicht es Unternehmen, ihre Sicherheitslage zu verbessern, indem sie Risiken bewerten, Warnungen für verdächtige Aktivitäten ausgeben und automatisch Abhilfemaßnahmen durchführen. Für Microsoft Defender for Cloud Apps ist ein Microsoft 365-, Office 365- oder Enterprise Mobility + Security (EMS) E5-Plan erforderlich.

### Verwaltung des privilegierten Zugriffs

Die Wirksamkeit einer Informationsschutzstrategie hängt davon ab, wie sicher die zur Verwaltung dieser Strategie verwendeten Verwaltungskonten sind. Wenn Konten, die zur Konfiguration und Verwaltung einer Informationsschutzstrategie verwendet werden können, nicht richtig gesichert sind, kann die Informationsschutzstrategie selbst leicht gefährdet werden.

Mit der Verwaltung des privilegierten Zugriffs können Sie Richtlinien konfigurieren, die Just-in-Time-Verwaltungsprinzipien auf vertrauliche Verwaltungsrollen anwenden. Wenn beispielsweise jemand vorübergehend Zugriff benötigt, um eine Informationsschutzrichtlinie zu konfigurieren, muss diese Person einen Genehmigungsprozess durchlaufen, um die erforderlichen Rechte zu erhalten, anstatt dass ihr dauerhaft ein Azure Active Directory (Azure AD)-Konto mit diesen Rechten zugewiesen wird.

> ***WEITERE INFORMATIONEN*** **Microsoft Information Protection-Infrastruktur**
>
> **Weitere Informationen über die Architektur von Microsoft Information Protection finden Sie unter folgender Adresse: *https://docs.microsoft.com/microsoft-365/compliance/information-protection*.**

## Ermitteln des Teams für die Bereitstellung von Workloads

Bei der Zusammenstellung eines Bereitstellungsteams müssen Sie beurteilen, welche Mitarbeiter für die Bereitstellungsaufgaben zuständig sein sollen, und sicherstellen, dass sie über die erforderliche Schulung verfügen und die entsprechenden Berechtigungen zur Ausführung dieser Aufgaben erhalten. Sie sollten vor Beginn des Rollouts festlegen, welche Mitarbeiter für welche Bereiche der Microsoft 365-Bereitstellung in Ihrem Unternehmen verantwortlich sein werden.

Sie sollten Mitarbeiter bestimmen, die die Leitung und Verantwortung für die folgenden Bereiche der Bereitstellung übernehmen:

- **Identitätsinfrastruktur** Verantwortlich für die Festlegung der Merkmale der Microsoft 365-Identität, einschließlich der Hybridanforderungen und der Authentifizierungskonfiguration.
- **Netzwerk** Verantwortlich dafür, dass das lokale Netzwerk für die Unterstützung von Microsoft 365-Diensten konfiguriert ist.
- **Client-Software und Windows 10** Verantwortlich für die Bereitstellung und Verwaltung der Client-Software, einschließlich Microsoft 365 Apps. Außerdem für die Konfiguration des Client-Betriebssystems verantwortlich.
- **Exchange** Verantwortlich für die Bereitstellung und Konfiguration von Exchange Online.
- **SharePoint** Verantwortlich für die Bereitstellung und Konfiguration von SharePoint Online.
- **Skype for Business oder Microsoft Teams** Verantwortlich für die Bereitstellung und Konfiguration von Skype for Business und/oder Microsoft Teams.
- **Sicherheit und Compliance** Verantwortlich für die Konfiguration von Microsoft 365, damit alle Complianceanforderungen vor der Bereitstellung erfüllt sind.

Ihr Team sollte für die Workloads-Bereitstellung über die erforderlichen Schulungen und Kenntnisse verfügen. Sie können das Team auch eine Pilotbereitstellung mit einem Testabonnement durchführen lassen, bevor Sie die Produktionsbereitstellung in Angriff nehmen. Auf diese Weise können sie potenzielle Blockierungsprobleme erkennen und beheben, bevor sie sich auf die Benutzer bei der tatsächlichen Bereitstellung auswirken.

> ***WEITERE INFORMATIONEN*** **Umstellung auf Microsoft 365**
>
> **Weitere Informationen zur Umstellung Ihres Unternehmens auf Microsoft 365 finden Sie unter *https://docs.microsoft.com/microsoft-365/enterprise/microsoft-365-overview*.**

## Planen einer Identitäts- und Authentifizierungslösung

Identitätsanbieter sind die primäre Autoritätsquelle und hosten Benutzer- und Gruppenkonten. Wenn Sie eine primäre Identitätsquelle auswählen, ist dies der Ort, an dem maßgebliche Änderungen an einem Konto oder einer Gruppe vorgenommen werden. Wenn Sie beispielsweise eine Kennwortänderung vornehmen, wird diese nur dann als gültig angesehen, wenn sie bei der primären Identitätsquelle vorgenommen wird.

***HINWEIS***

**In einem hybriden Szenario ist es möglich, das Kennwort eines Kontos zu ändern, das von einem lokalen Verzeichnis in ein cloudbasiertes Azure Active Directory in der Cloud repliziert wird. Diese Änderung wird jedoch möglicherweise überschrieben, wenn das replizierte Konto das nächste Mal mit der primären Identitätsquelle synchronisiert wird.**

Microsoft 365 und Office 365 verwenden Azure AD als Identitäts- und Authentifizierungsdienst für Benutzer und Gruppen. Azure AD speichert Benutzer-, Gruppen- und Gerätekontenobjekte und ist auch für die Durchführung der Microsoft 365- und Office 365-Authentifizierung verantwortlich.

Bei der Bereitstellung von Microsoft 365 und Office 365 können Sie wählen, ob die Identitätsverwaltung nur in der Cloud erfolgt oder ob eine Beziehung zwischen einem lokalen Identitätsanbieter wie Active Directory Domain Services (AD DS) und Azure AD besteht.

## Cloud-Authentifizierung

Wenn Sie sich für die Cloud-Authentifizierung entscheiden, erfolgt die Authentifizierung gegen Azure Active Directory. Wie Sie die Cloud-Authentifizierung implementieren, hängt davon ab, ob Ihr Unternehmen über eine bestehende lokale AD DS-Bereitstellung verfügt und welche Pläne Sie für diese Bereitstellung in der Zukunft haben.

### Nur Cloud

Das Modell der reinen Cloud-Authentifizierung dient der Verwaltung von Benutzer- und Gruppenkonten, die nur innerhalb von Microsoft 365 existieren. Sie können Benutzer im Microsoft 365 Admin Center (siehe Abbildung 1–1), im Azure AD-Portal oder über die entsprechenden PowerShell-Cmdlets erstellen und verwalten.

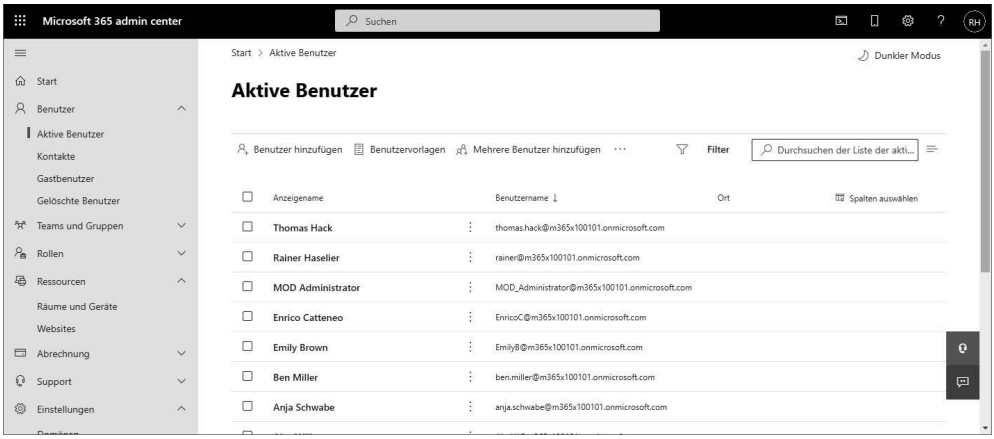


**Abb. 1–1** Erstellen und Verwalten von Microsoft 365-Benutzern

Eine reine Cloud-Identitäts- und Authentifizierungslösung ist geeignet, wenn:

- Ihre Organisation keine lokale AD DS-Umgebung implementiert hat.
- Ihre Organisation über eine sehr komplexe lokale Verzeichnislösung verfügt und den Versuch einer Integration vermeiden möchte.
- Ihre Organisation über eine lokale AD DS-Umgebung verfügt, aber eine Pilot- oder Testphase von Microsoft 365 durchführen möchte und sich erst dann um die Integration in die bestehende Umgebung kümmern will, wenn die Pilot- oder Testphase erfolgreich verläuft.

### Kennworthashsynchronisierung mit Single Sign-On (Einmaliges Anmelden)

Wenn Sie eine Identitäts- und Authentifizierungslösung mit Kennworthashsynchronisierung planen, synchronisiert Ihr Unternehmen lokale AD DS-Benutzerkonten mit dem Azure AD-Dienst, der von Microsoft 365 und Office 365 verwendet wird. Wenn Sie diese Strategie anwenden, werden kryptografische Hashes von lokalen Benutzerkennwörtern mit Azure AD synchronisiert.

Der kryptografische Hashing-Vorgang ist einseitig. Das bedeutet, dass es nicht möglich ist, eine umgekehrte kryptografische Operation mit dem Hash durchzuführen, um das Kennwort abzuleiten, aus dem er generiert wurde, obwohl es Techniken gibt, die mögliche Kennwörter durchlaufen, um zu sehen, ob sie mit einem kryptografischen Hash übereinstimmen, falls es gelingt, einen zu erfassen.

Die Verwendung von kryptografischen Hashwerten bedeutet, dass in Azure AD nicht die Benutzerkennwörter selbst gespeichert werden. Bei der Authentifizierung wird für das vom Benutzer eingegebene Kennwort dieselbe kryptografische Operation durchgeführt, und der Hash dieses Kennworts wird dann mit dem in Azure AD gespeicherten Kennwort verglichen. Wenn die Hashwerte übereinstimmen, wird der Benutzer authentifiziert. Wenn sie nicht übereinstimmen, wird der Benutzer nicht authentifiziert. Wenn ein Kennwort in der lokalen Kontodatenbank geändert wird, wird ein neuer Kennworthash berechnet, und der neue kryptografische Hash wird mit Azure AD synchronisiert und in Azure AD gespeichert.

Wählen Sie diese Methode, wenn AD DS vor Ort die Autoritätsquelle für Benutzerkonten bleiben soll und wenn die Vorschriften, denen Ihre Organisation unterliegt, die Speicherung von kryptografischen Kennworthashwerten in der Cloud zulassen. Für diese Lösung ist Azure AD Connect erforderlich, das Sie in Kapitel 2, »Benutzeridentität und Rollen verwalten«, kennenlernen werden.

### Passthrough-Authentifizierung mit Single Sign-On (Einmaliges Anmelden)

Wenn Sie die Passthrough-Authentifizierung mit Single Sign-On (SSO) implementieren, installieren Sie auf einem oder mehreren lokalen AD DS-Domänencontrollern einen Software-Agent. Wenn sich ein Benutzer gegenüber Azure AD authentifiziert, wird die Anfrage über den Agent an die lokale AD-Instanz weitergeleitet, um festzustellen, ob die Authentifizierungsanfrage gültig ist.

Diese Lösung ist geeignet, wenn Ihr Unternehmen keine Form der Kennwortsynchronisierung mit der Cloud zulassen darf. Dazu kann auch gehören, dass kryptografische Kennworthashwerte nicht in der Cloud gespeichert werden dürfen. In diesem Szenario wäre die Passthrough-Au-

thentifizierung mit SSO eine geeignete Lösung. Sie ist auch dann geeignet, wenn der lokale Kontostatus sowie lokale Kennwortrichtlinien und Anmeldezeiten durchgesetzt werden müssen. In Kapitel 2 erfahren Sie mehr über die Konfiguration der Passthrough-Authentifizierung mit SSO.

## Verbundauthentifizierung

Die Verbundauthentifizierung ist eine Alternative zur Cloud-Authentifizierung, obwohl sie oft wesentlich komplizierter zu konfigurieren und zu warten ist. Die meisten Unternehmen verwenden Azure AD Connect, um Identitätsinformationen zwischen lokalem AD DS und Azure AD zu synchronisieren. Organisationen, die zusätzliche Authentifizierungsoptionen zulassen möchten, wie z. B. Smartcard-basierte Authentifizierung oder Multifaktor-Authentifizierung von Drittanbietern, wie z. B. ein RSA-Token-Gerät, sollten die Verbundauthentifizierung implementieren.

### Verbundidentität mit Active Directory-Verbunddiensten

Wenn Sie die Verbundidentität mit Active Directory-Verbunddiensten (Active Direcoty Federation Services, AD FS) verwenden, stellen Sie Server bereit, die die AD FS-Rolle im lokalen Netzwerk und im Perimeter-Netzwerk Ihrer Organisation hosten. Anschließend müssen Sie den Verbund zwischen Ihrer lokalen AD FS-Instanz und Azure AD konfigurieren. Wenn Sie diese Identitäts- und Authentifizierungstechnologie implementieren, verwenden Benutzer die gleichen Authentifizierungsoptionen für den Zugriff auf Microsoft 365- und Office 365-Ressourcen wie für den Zugriff auf die lokalen Ressourcen. Diese Authentifizierungsmethode wird in der Regel von Unternehmen gewählt, die Authentifizierungsanforderungen haben, die von Azure AD nicht nativ unterstützt werden.

### Authentifizierungs- und Identitätsanbieter von Drittanbietern

Organisationen, die einen lokalen Identitätsanbieter verwenden, der nicht zu Active Directory gehört, können diesen Identitätsanbieter durch Föderation in Azure AD integrieren, sofern die Verbundlösung des Identitätsanbieters mit Azure AD kompatibel ist. Wenn diese Lösung implementiert ist, können Benutzer auf Microsoft 365- und Office 365-Ressourcen unter Verwendung ihres Benutzernamens und Kennworts des lokalen Identitätsanbieters zugreifen.

***WEITERE INFORMATIONEN*** **Microsoft 365- und Office 365-Identität verstehen**

**Weitere Informationen über die Microsoft 365-Identitätsmodelle finden Sie unter *https://docs.microsoft.com/microsoft-365/enterprise/about-microsoft-365-identity*.**

***PRÜFUNGSTIPP***

**Merken Sie sich den Unterschied zwischen Kennworthashsynchronisierung mit Single Sign-On und Passthrough-Authentifizierung mit Single Sign-On.**

## Planen der Modernisierung von Unternehmensanwendungen

Die Anwendungsmodernisierung kann es Unternehmen ermöglichen, ihren Fußabdruck im Rechenzentrum zu reduzieren. Ein Unternehmen, das seine gesamten Exchange- und SharePoint-Workloads auf Microsoft 365 migriert hat, wird wahrscheinlich auch möglichst viele seiner lokalen branchenspezifischen Anwendungen in die Cloud verlagern wollen.

Die Modernisierung von Unternehmensanwendungen ist ein weit gefasster Begriff für die Aktualisierung von branchenspezifischen Anwendungen in Unternehmen, damit sie auf modernen Plattformen laufen. Eine Herausforderung für viele Unternehmen besteht darin, dass sie branchenspezifische Anwendungen einsetzen, die von älteren Softwareversionen abhängig sind, die möglicherweise nicht mit neueren Technologien kompatibel sind. Hier ein paar Beispiele:

- Webanwendungen, die Flash verwenden, das von aktuellen Browsern nicht mehr unterstützt wird
- Anwendungen oder Plug-Ins, die für ältere Versionen von Microsoft Office geschrieben wurden, aber nicht mit Microsoft 365 Apps for Enterprise kompatibel sind
- Anwendungen, die eine ältere Version von SQL Server verwenden, wie z. B. SQL Server 2005, die nur mit nicht unterstützten Versionen von Windows Server kompatibel sind

Organisationen können eine Vielzahl von Methoden zur Modernisierung ihrer Unternehmensanwendungen einsetzen. Dazu gehören u. a. die folgenden:

- Umschreiben der Anwendung, damit sie mit unterstützter Software funktioniert. Ein Beispiel wäre die Aktualisierung einer Webanwendung, damit sie moderne Webstandards verwendet und auf einem unterstützten Browser läuft.
- Migration einer bestehenden Anwendung, sodass sie in einem Container und nicht auf einem eigenen Server für diese Anwendung läuft. Die Containerisierung einer bestehenden Anwendung vereinfacht auch den Prozess der Migration dieser Anwendung in die Cloud.
- Umschreiben oder Aktualisieren einer Anwendung oder eines Plug-Ins, die bzw. das für eine frühere Version von Microsoft Office geschrieben wurde, damit sie bzw. es mit Microsoft 365 Apps for Enterprise kompatibel ist.
- Umschreiben der Anwendung, sodass sie auf einem geeigneten Azure Platform-as-a-Service (PaaS)-Angebot gehostet werden kann, wie z. B. Web App, Azure Functions, Azure SQL oder einem serverlosen Angebot, anstatt sie in einem lokalen Rechenzentrum auf einem von Ihrem Unternehmen verwalteten Betriebssystem zu hosten.

***WEITERE INFORMATIONEN*** **Containerisierung von Unternehmensanwendungen**

**Weitere Informationen über die Containerisierung von Unternehmensanwendungen finden Sie unter *https://docs.microsoft.com/dotnet/architecture/microservices/architect-microservice-container-applications/containerize-monolithic-applications*.**

# Prüfungsziel 1.2: Bereitstellen eines Microsoft 365-Mandanten

Dieser Abschnitt befasst sich mit den Schritten, die Sie zur Bereitstellung und Konfiguration eines Microsoft 365-Mandanten durchführen müssen. Um diese Qualifikation zu beherrschen, müssen Sie verstehen, wie man Microsoft 365-Domänen verwaltet. Außerdem müssen Sie mit Organisationseinstellungen vertraut sein, wissen, wie man einen Microsoft-Partner hinzufügt oder mit FastTrack arbeitet, und lernen, wie man mandantenweite Workload-Einstellungen konfiguriert.

**Dieser Abschnitt behandelt die folgenden Themen:**

- Verwalten von Domänen
- Konfigurieren von Organisationseinstellungen
- Vervollständigen des Organisationsprofils
- Hinzuziehen eines Microsoft-Partners oder Arbeiten mit Microsoft FastTrack
- Vervollständigen des Assistenten zur Einrichtung von Abonnements
- Planen und Erstellen eines Mandanten
- Bearbeiten eines Organisationsprofils
- Planen und Erstellen von Abonnements
- Konfigurieren von mandantenweiten Workload-Einstellungen

## Verwalten von Domänen

Wenn Sie ein Microsoft 365-Abonnement erstellen, wird dem Abonnement-Mandanten automatisch eine benutzerdefinierte *onmicrosoft.com*-Domäne zugewiesen. Der Name des Mandanten hat das Format *name.onmicrosoft.com*, wobei *name* der Name ist, den Sie dem Mandanten Ihrer Organisation zuweisen möchten. Dieser Name muss eindeutig sein; es ist nicht möglich, dass zwei Organisationen denselben Mandantennamen verwenden. Beim Anlegen der Mandanten wird der vorgeschlagene Name überprüft. Wenn bereits ein Mandant mit diesem Namen existiert, müssen Sie eine Alternative auswählen.

Auch wenn es unwahrscheinlich ist, dass Sie den Domänennamen *onmicrosoft.com* tatsächlich verwenden, nachdem Sie den Mandanten Ihrer Organisation vollständig konfiguriert haben, ist es wichtig zu wissen, dass Sie den Mandantennamen nicht mehr ändern können, nachdem Sie Ihr Microsoft 365-Abonnement konfiguriert haben. Der bei der Einrichtung gewählte Name für den Mandanten bleibt während der gesamten Laufzeit des Abonnements bestehen und kann

nicht entfernt werden. Widerstehen Sie der Versuchung, einen lustigen Namen zuzuweisen, denn Ihre Organisation wird diesen Namen nicht mehr los, selbst wenn es sich nicht um den primären Domänennamen handelt.

Sie können dem Mandanten einen Domänennamen zuweisen, der Ihnen gehört, sodass Sie den Mandantennamen nicht regelmäßig verwenden müssen. Sie könnten sich beispielsweise für ein Microsoft 365-Abonnement mit dem Mandantennamen *contoso.onmicrosoft.com* anmelden. Jedes Konto, das Sie erstellen, verwendet das E-Mail-Suffix *contoso.onmicrosoft.com* für das Office 365 Exchange-Postfach des Kontos. Nach der Einrichtung von Microsoft 365 können Sie jedoch einen benutzerdefinierten Domänennamen zuweisen und diesen als primäres E-Mail-Suffix verwenden. Wenn Sie z. B. den Domänennamen *contoso.com* besitzen, können Sie Ihren Mandanten so konfigurieren, dass der benutzerdefinierte Domänenname *contoso.com* für den Mandanten *contoso.onmicrosoft.com* verwendet wird.

Microsoft 365 unterstützt das Hinzufügen von bis zu 900 Domänen zu einem einzigen Abonnement. Sie können auch unterschiedliche Domänennamen mit einem Abonnement verwenden, z. B. *contoso.com* und *tailwindtraders.com*. Sie können auch Subdomänen eines Domänennamens zuordnen, z. B. *partners.tailwindtraders.com* oder *australia.contoso.com*.

## Erwerb eines Domänennamens

Wenn Ihre Organisation einen neuen Domänennamen mit ihrem Microsoft 365-Mandanten verwenden möchte, kann sie einen solchen bei einem Registrar erwerben. Dabei können Sie wählen, ob der Registrar die Nameservereinträge für die Domäne hosten soll oder ob Sie Ihre eigenen Nameservereinträge auswählen.

Die überwiegende Mehrheit der Unternehmen besitzt bereits einen Domänennamen und hostet diesen entweder bei einer bestimmten Registrierungsstelle, ihrem Internetdienstanbieter oder sogar auf ihren eigenen DNS-Servern. Um eine Domain mit Microsoft 365 zu verwenden, müssen die DNS-Server, die als Nameserver für die Domain verwendet werden, die folgenden Eintragstypen unterstützen:

- **CNAME-Einträge** Um Skype for Business online vollständig zu unterstützen, müssen die DNS-Server in der Lage sein, mehrere CNAME-Einträge in einer DNS-Zone zu unterstützen.
- **SPF/TXT-Einträge** Mit diesen Einträgen können Sie Einträge für das Sender Protection Framework (SPF) konfigurieren, die zur Bekämpfung unerwünschter kommerzieller E-Mails verwendet werden können. TXT-Einträge sind auch eine Möglichkeit, den Besitz einer Domäne zu überprüfen.
- **SRV-Einträge** SRV-Einträge werden für die Skype for Business Online-IM und die Integration der Anwesenheitsinformationen mit der Outlook-Webanwendung verwendet. Sie werden auch für den Verbund mit Skype for Business Online-Nutzern in verschiedenen Organisationen verwendet, einschließlich für öffentliche Internetverbindungen mit Microsoft-Konten.
- **MX-Einträge** Diese Einträge werden für die Weiterleitung von E-Mails an Exchange Online-Mailserver verwendet.

## Erwerb einer Domäne über Microsoft 365

In einigen Regionen können Sie einen benutzerdefinierten Domänennamen über Microsoft 365 erwerben. In diesem Fall sind Sie auf die folgenden Top-Level-Domains beschränkt:

- .biz
- .com
- .info
- .me
- .mobi
- .net
- .org
- .tv
- .co.uk
- .org.uk

Der Erwerb einer Domäne über Microsoft 365 kann insofern von Vorteil sein, als dass die meisten DNS-bezogenen Vorgänge automatisch für Sie durchgeführt werden. Sie sollten diese Option jedoch nicht wählen, wenn Ihr Unternehmen weiterhin E-Mail-Dienste außerhalb von Microsoft 365 nutzen wird, da Sie die entsprechenden MX-Einträge nicht ändern können.

## Konfigurieren eines benutzerdefinierten Domänennamens

Um Microsoft 365 für die Verwendung eines benutzerdefinierten Domänennamens zu konfigurieren, müssen Sie den benutzerdefinierten Domänennamen zu Microsoft 365 hinzufügen. Das Konto, mit dem diese Aktion durchgeführt wird, muss ein globaler Administrator eines Business- oder Enterprise-Plans sein.

Um eine benutzerdefinierte Domäne zu Microsoft 365 hinzuzufügen, führen Sie die folgenden Schritte aus:

1. Wählen Sie im linken Bereich des Microsoft 365 Admin Centers unter *Einstellungen* die Option *Domänen* (siehe Abbildung 1–2).
2. Wenn Ihre Organisation bereits eine Domäne besitzt, wählen Sie *Domäne hinzufügen*.

   Die Seite *Domäne hinzufügen* wird geöffnet.

***HINWEIS***

**Sie können auch eine Domain über Office 365 und GoDaddy kaufen. Klicken Sie dazu auf der Seite *Domänen* auf die Schaltfläche *Domäne kaufen*. Wenn Sie eine Domäne über GoDaddy kaufen, wird der gesamte Prozess der Zuweisung einer benutzerdefinierten Domäne zu Microsoft 365 automatisch durchgeführt. Wenn die Domäne Ihrer Organisation jedoch bereits an einem anderen Ort gehostet wird, müssen Sie die Eigentümerschaft dieser Domäne bestätigen, indem Sie spezielle TXT- oder MX-Einträge konfigurieren, die im Einrichtungsprozess überprüft werden können.**

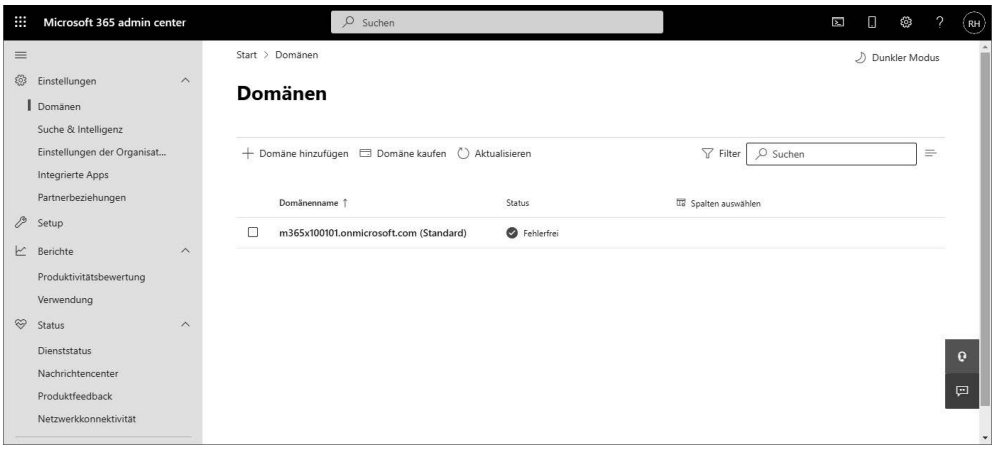


**Abb. 1–2** Die Seite *Domänen*

3. Geben Sie in das Feld *Domänenname* den Namen der bestehenden Domäne ein, die Sie konfigurieren möchten, und wählen Sie *Diese Domäne verwenden* (siehe Abbildung 1–3).

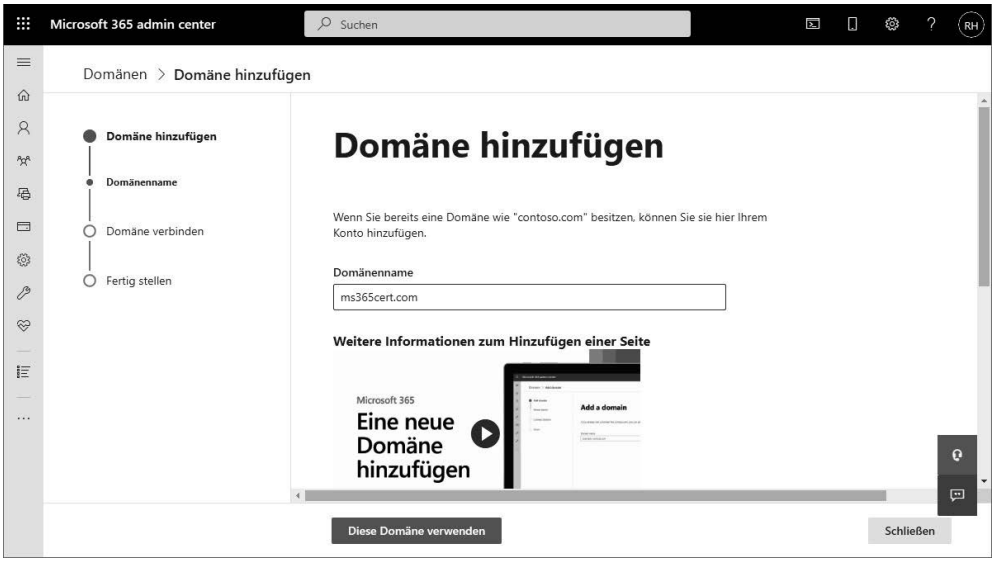


**Abb. 1–3** Hinzufügen einer bestehenden Domäne in Microsoft 365

Jetzt beginnt der Prozess des Hinzufügens der Domäne. Sie müssen deren Besitz bestätigen, bevor Sie die Domäne verwenden können. Anweisungen dazu finden Sie im nächsten Abschnitt.