KAPITEL 1

Moderne Gerätedienste implementieren

Dieses Kapitel befasst sich mit cloudbasierten Diensten innerhalb von Microsoft 365, die für die Bereitstellung, die Absicherung und die Verwaltung von Geräten im Unternehmen entworfen wurden. Im Laufe dieses Buches werden Sie mit verschiedenen Microsoft-Technologien arbeiten, die in der Enterprise Mobility + Security (EMS)-Lizenzierungssuite enthalten sind. Ein Großteil der Dienste wird über das Microsoft Endpoint Manager Admin Center verwaltet, aber es gibt auch weitere Portale wie das Azure Portal und das Portal Microsoft Store für Unternehmen. Im Laufe des Kurses werden mehrere Beispiele und Komplettlösungen vorgestellt, die die Verwaltung dieser Tools veranschaulichen. Für die Demonstrationen empfehlen wir, dass Sie diese in Ihrem eigenen Labor nachzuvollziehen. Hier finden Sie einige Links, die Ihnen den Einstieg erleichtern:

- **Enterprise Mobility + Security 90-Tage-Testversion (enthält Azure Active Directory Premium P2)** ***https://www.microsoft.com/cloud-platform/enterprise-mobility-security-trial***
- **Office 365 Business Premium 30-Tage-Testversion** ***https://products.office.com/business/office-365-business-premium***

In diesem Kapitel abgedeckte Prüfungsziele:

- Prüfungsziel 1.1: Planung der Geräteverwaltung
- Prüfungsziel 1.2: Verwaltung der Gerätekonformität
- Prüfungsziel 1.3: Planung von Apps
- Prüfungsziel 1.4: Planung der Windows 10-Bereitstellung
- Prüfungsziel 1.5: Registrierung von Geräten

Prüfungsziel 1.1: Planung der Geräteverwaltung

Die Geräteverwaltung ist einer der Kerndienste von Microsoft Intune, der über das Microsoft Endpoint Manager Admin Center verwaltet wird. Die Geräteverwaltung setzt voraus, dass der Microsoft Endpoint Manager konfiguriert ist und dass im Mandanten die entsprechenden Lizenzen verfügbar sind. Sie weisen diese Lizenzen den Benutzern zu, die wiederum die im Mandanten registrierten Geräte verwenden können. Nachdem die Geräte registriert sind, können Sie diese über das Microsoft Endpoint Manager Admin Center verwalten und überwachen.

Dieser Abschnitt behandelt die folgenden Themen:

- Planen der Geräteüberwachung
- Planung der Implementierung von Microsoft Endpoint Manager
- Planung von Konfigurationsprofilen

Planen der Geräteüberwachung

In diesem Abschnitt werden die Optionen für die Geräte- oder Endpunktüberwachung in Microsoft 365 Defender vorgestellt. Diese Angebote ermöglichen es Unternehmen, den Zustand und die Compliance der Geräte und Anwendungen in ihrer Umgebung zu überwachen. Die beiden wichtigsten Tools für die Überwachung von Endpunkten werden über das Microsoft 365 Security Center und das Microsoft Endpoint Manager Admin Center bereitgestellt.

Das Microsoft 365 Security Center ist eine zentrale Anlaufstelle, die Defender für Endpunkt, Defender for Office 365, Microsoft 365 Defender und andere Tools in einer Oberfläche zusammenfasst.

Über das Security Center können Sie viele Überwachungsaktionen durchführen:

- **Anzeigen Ihrer Microsoft-Sicherheitsbewertung** Die Sicherheitsbewertung empfiehlt Ihnen auf der Grundlage der aktuellen Konfiguration Ihrer Umgebung Verbesserungsmaßnahmen.
- **Anzeigen der Gerätekonformität** Bestimmen Sie die Anzahl, den Typ und die Namen der Geräte, die konform sind, nicht konform sind, sich in einer Toleranzperiode befinden oder nicht bewertet werden.
- **Anzeigen der gefährdeten Geräte** Zeigen Sie die Anzahl der Geräte und deren Risikostufe auf der Grundlage der aktuellen Konfiguration an.
- **Geräte mit aktiver Malware anzeigen** Verfolgen Sie die Sicherheitsereignisse und erzwingen Sie die Konfiguration, Konformität und Behebung über die Intune-Geräteverwaltung.

Um Microsoft 365 Defender zu aktivieren, müssen Sie entweder die Rolle des globalen Administrators oder des Sicherheitsadministrators von Azure Active Directory haben. Wenn Sie Microsoft 365 Defender aktivieren, müssen einige Einstellungen für den Mandanten konfiguriert werden, darunter die folgenden:

- **Datenspeicherort** Der primäre Geschäftssitz der Organisation, an dem die Daten aufbewahrt werden sollen.
- **Datenaufbewahrung** Der Standardaufbewahrungszeitraum beträgt sechs Monate, kann aber geändert werden.
- **Vorschaufunktionen** Die Vorschaufunktionen sind standardmäßig aktiviert.

Das Microsoft Endpoint Manager Admin Center bietet ein All-in-One-Administrationszentrum für die Geräteanmeldung, Geräte- und Konfigurationskonformität, Endpunktsicherheit und für weitere Berichtsfunktionen. Die integrierten Berichte sind in vier Schwerpunktbereiche eingeteilt.

- **Operative Berichte** Gezielte und handlungsorientierte Daten
- **Organisationsberichte** Zusammenfassende Übersichten auf hoher Ebene für eine Organisation
- **Trendberichte** Zeigt Muster und Trends über einen bestimmten Zeitraum an.
- **Erweiterte Berichte** Ermöglicht es Ihnen, die zugrunde liegenden Daten zu verwenden, um Ihre eigenen benutzerdefinierten Berichte zu erstellen.

Abbildung 1–1 zeigt die Standard-Startseite des Microsoft Endpoint Manager Admin Center mit Berichten zum Status gesunder und aktiver Geräte.

HINWEIS

Um die Protokolle, die als Teil der Berichte verwendet werden, zu überprüfen, müssen Sie entweder die Rolle des globalen Administrators oder des Intune-Dienstadministrators oder die Rolle des Intune-Administrators mit Leserechten besitzen.

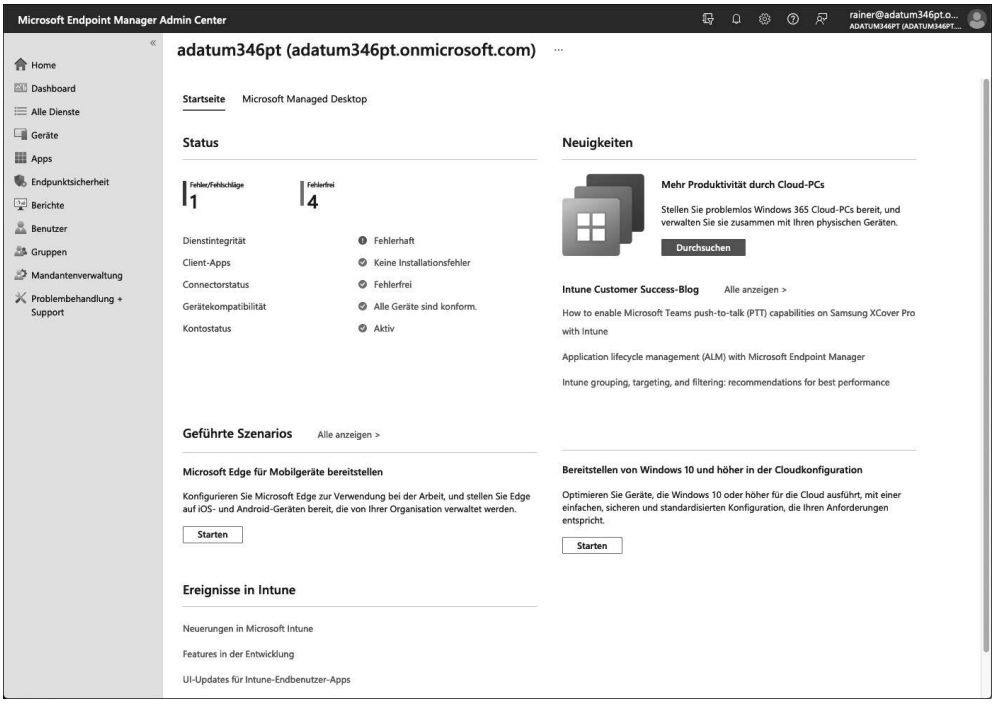

Abb. 1–1 Microsoft Endpoint Manager Admin Center

Microsoft Endpoint Manager-Implementierung planen

Microsoft bietet eine Kombination von Endpunktlösungen an, die über das Microsoft Endpoint Manager Admin Center verwaltet werden. Diese Angebote haben sich im Laufe der Jahre verändert, wobei stark in Clouddienste und die Integration mit Azure investiert wurde. Die Einführung von Windows 10 hat auch die Art und Weise beeinflusst, wie Sie Geräte mit einer Reihe von nativen MDM-Protokollen (Mobile Device Management) innerhalb des Betriebssystems verwalten, wodurch die Notwendigkeit entfällt, auf Ihren Endpunkten einen weiteren Agenten zu installieren. Welche Lösung Sie wählen sollten, hängt von den Bereitstellungszielen Ihres Unternehmens ab. Die beiden wichtigsten Geräteverwaltungslösungen von Microsoft sind:

- **Microsoft Intune** Diese Lösung eignet sich am besten für Kunden, die moderne Verwaltungsfunktionen für Windows 10-Geräte benötigen, aber gleichzeitig auch ihre lokale Serverinfrastruktur einschränken müssen. Microsoft Intune ist eine cloudbasierte Verwaltungslösung, die keine zusätzliche Serverinfrastruktur erfordert. Die Plattformunterstützung für Intune umfasst Verwaltungsfunktionen für Windows 10 und macOS. Sie haben außerdem Zugriff auf Funktionen wie Autopilot, die dazu beitragen können, die Anforderungen für die Bereitstellung herkömmlicher Betriebssysteme zu reduzieren.
- **Co-Management zwischen Microsoft Intune und ConfigMgr** Diese Lösung stellt eine Brücke zwischen Microsoft Intune und ConfigMgr dar und ermöglicht Kunden die gemeinsame Verwaltung von Geräten auf der Grundlage ihrer Anforderungen. ConfigMgr ist eine Vor-Ort-Verwaltungslösung mit zusätzlicher Plattformunterstützung, z.B. für Windows Server. Sie umfasst auch eine Reihe einzigartiger Technologien, wie z.B. Tasksequenzen und Image-Bereitstellung. Umgebungen mit Co-Management können Workloads für ihre Windows 10-Geräte und mobilen Geräte in die Cloud verlagern und gleichzeitig die traditionelle Infrastruktur unterstützen.

Intune einrichten

Zur Einrichtung von Intune sind mehrere Schritte erforderlich, bevor Sie Geräte verwalten können. Diese Schritte sind wie folgt:

1. **Verstehen der unterstützten Konfigurationen** Dazu gehören das unterstützte Gerätebetriebssystem, die Netzwerkanforderungen und die Unterschiede zwischen der kommerziellen und der speziell auf Behörden ausgerichteten Cloud.
2. **Erstellen Sie ein Abonnement** Fügen Sie Intune zu Ihrem Mandanten hinzu und berücksichtigen Sie dabei, ob Sie ein Microsoft Online Services-Konto, ein Enterprise Agreement oder einen Volumenlizenzvertrag haben.
3. **Konfigurieren Sie einen benutzerdefinierten Domänennamen** Konfigurieren Sie einen benutzerdefinierten Domänennamen oder einen Vanity-Domänennamen zur Verwendung mit Ihrem Mandanten. Es wird empfohlen, dies vor dem Hinzufügen von Benutzerkonten zu tun, um die Kontoverwaltung zu vereinfachen.

4. **Benutzer und Gruppen hinzufügen** Fügen Sie einzelne Benutzer und Gruppen zu Intune hinzu. Alternativ können Sie eine Verbindung zu Active Directory mit Intune für die Synchronisierung herstellen.
5. **Lizenzen zuweisen** Verknüpfen Sie erworbene Intune- oder Enterprise Mobility + Security-Lizenzen mit Benutzerkonten.
6. **Legen Sie die MDM-Autorität fest** Dies gilt nur für Mandanten mit einem Service-Release vor 1911. Mandanten, die 1911 oder später verwenden, werden automatisch für Intune konfiguriert.
7. **Apps zuweisen** Apps können Gruppen zur automatischen oder optionalen Installation zugewiesen werden.
8. **Geräte konfigurieren** Konfigurieren Sie die Profile, die die Geräteeinstellungen und Gerätefeatures verwalten.
9. **Anpassen der Portale** Fügen Sie den verschiedenen Portalen Ihr Firmenbranding hinzu.
10. **Aktivieren Sie die Geräteregistrierung** Aktivieren Sie bestimmte Geräte, die für die Verwaltung durch Intune registriert werden sollen.
11. **Anwendungsrichtlinien konfigurieren** Konfigurieren Sie spezifische Anwendungsschutzrichtlinien für von Intune geschützte Anwendungen.

PRÜFUNGSTIPP

Bei einigen Prüfungsaufgaben müssen Sie die Reihenfolge der Schritte zur Konfiguration einer Lösung verstehen. So müssen beispielsweise Lizenzen und die MDM-Autorität konfiguriert werden, bevor Sie die Geräteregistrierung konfigurieren können.

WEITERE INFORMATIONEN **Microsoft Intune einrichten**

Eine ausführliche Schritt-für-Schritt-Anleitung für die Einrichtung von Intune finden Sie unter *https://docs.microsoft.com/de-de/mem/intune/fundamentals/setup-steps*.

Lizenzen zuweisen

Sie können Benutzern Intune-Lizenzen sowohl über das Microsoft Endpoint Manager Admin Center als auch über das Azure-Portal in Azure Active Directory zuweisen. Gehen Sie folgendermaßen vor, um eine Lizenz über das Admin Center zuzuweisen:

1. Melden Sie sich beim Microsoft Endpoint Manager Admin Center unter *https://endpoint.microsoft.com* an.
2. Klicken Sie auf **Benutzer**.
3. Klicken Sie auf **Alle Benutzer** und dann auf den Benutzer, für den Sie die Lizenzzuweisungen ändern möchten.
4. Klicken Sie auf **Lizenzen** und dann auf **Zuweisungen**.

5. Aktivieren Sie das Kontrollkästchen **Microsoft Intune** und klicken Sie auf **Speichern**. (Die Position des Kontrollkästchens hängt von der Art der erworbenen Lizenz ab.)

Abbildung 1–2 zeigt die Microsoft Intune-Lizenz, die als Teil der Enterprise Mobility + Security E5-Lizenzsuite aktiviert ist. Jeder lizenzierte Benutzer kann auf die in seinen Profilen definierten Dienste für bis zu 15 verwaltete Geräte zugreifen und diese nutzen.

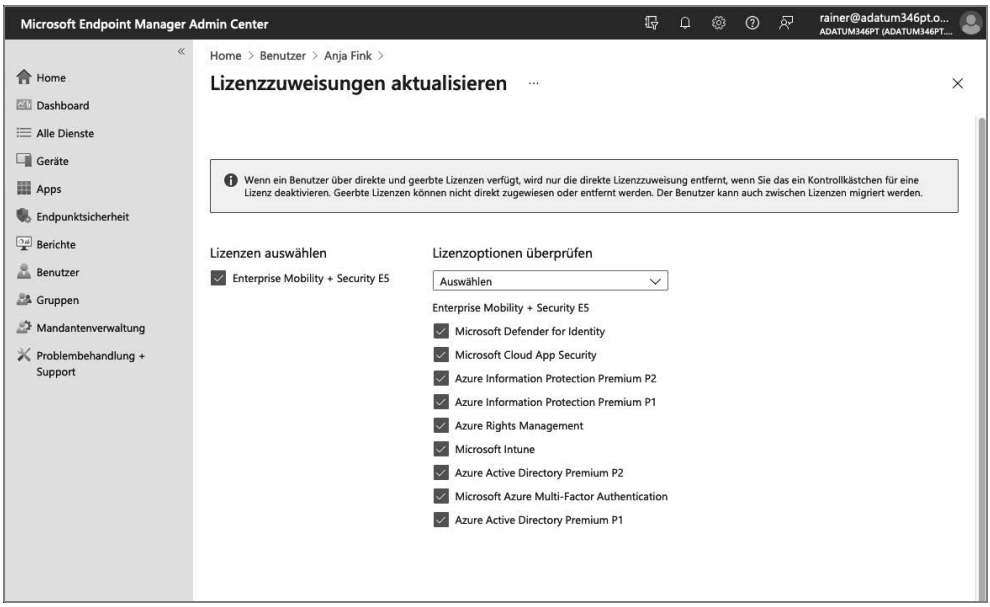

Abb. 1–2 Lizenzen an Benutzer zuweisen

Planen von Konfigurationsprofilen

In diesem Abschnitt werden Sie die verfügbaren Einstellungen für Konfigurationsprofile überprüfen. Konfigurationsprofile definieren die Einstellungen, die Sie auf den verwalteten Geräten implementieren möchten. So können Sie beispielsweise die Browsereinstellungen auf Windows-Clients anpassen oder auf mobilen Geräten den Zugriff auf Bluetooth verhindern. Konfigurationsprofile werden erstellt, um diese Einstellungen pro Plattform zu definieren.

Die vom Microsoft Endpoint Manager Admin Center unterstützten Plattformen sind:

- Android-Geräteadministrator
- Android Enterprise
- iOS/iPadOS
- macOS
- Windows 10 und höher

Nachdem Sie die Plattform ausgewählt haben, für die Sie ein Profil definieren möchten, müssen Sie einen Profiltyp auswählen. Die Profiltypen variieren je nach der von Ihnen gewählten Plattform. Für macOS- und Windows-Gerätetypen sind die Optionen entweder Einstellungskatalog oder Vorlagen. Der Einstellungskatalog ist eine Liste aller verfügbaren Einstellungen für das ausgewählte Betriebssystem. Für Windows sind das Tausende von Einstellungen.

Vorlagen sind häufig verwendete Tools, die konfiguriert werden müssen. So gibt es beispielsweise Vorlagen für den Endpunktschutz, die VPN- und WLAN-Konfiguration, Zertifikate, Gerätefunktionen und vieles mehr.

> ***WEITERE INFORMATIONEN*** **Einstellungen eines Konfigurationsprofils anwenden**
>
> **Weitere Informationen über die Anwendung der Einstellungen eines Konfigurationsprofils finden Sie unter *https://docs.microsoft.com/de-de/mem/intune/configuration/device-profiles*.**

Sie erstellen ein Konfigurationsprofil über das Microsoft Endpoint Manager Admin Center. Um ein Konfigurationsprofil zu erstellen, führen Sie die folgenden Schritte aus:

1. Melden Sie sich beim Microsoft Endpoint Manager Admin Center unter *https://endpoint.microsoft.com* an.
2. Klicken Sie auf **Geräte**.
3. Klicken Sie auf **Konfigurationsprofile**.
4. Klicken Sie auf **Profil erstellen**.
5. Wählen Sie im Dropdown-Menü **Plattform** ein Betriebssystem aus – in diesem Beispiel **Windows 10 und höher**.
6. Wählen Sie im Dropdown-Menü **Profiltyp** die Option **Vorlagen** aus.
7. Wählen Sie die Vorlage **WLAN** aus.
8. Klicken Sie auf **Erstellen**.
9. Geben Sie auf der Registerkarte **Grundlagen** einen Namen für das Profil ein, z. B. ***Erforderliches WLAN***.
10. Klicken Sie auf **Weiter**.
11. Wählen Sie im Dropdown-Menü **WLAN-Typ** die Option **Basis**.
12. Vervollständigen Sie die Konfigurationseinstellungen für das WLAN-Netzwerk, mit dem das Gerät eine Verbindung herstellen soll.

Abbildung 1–3 veranschaulicht die automatische Verbindung mit einem WLAN-Netzwerk namens *ContosoWLAN* mit WPA2-Sicherheit und dem vorinstallierten Schlüssel *Secure123!*.

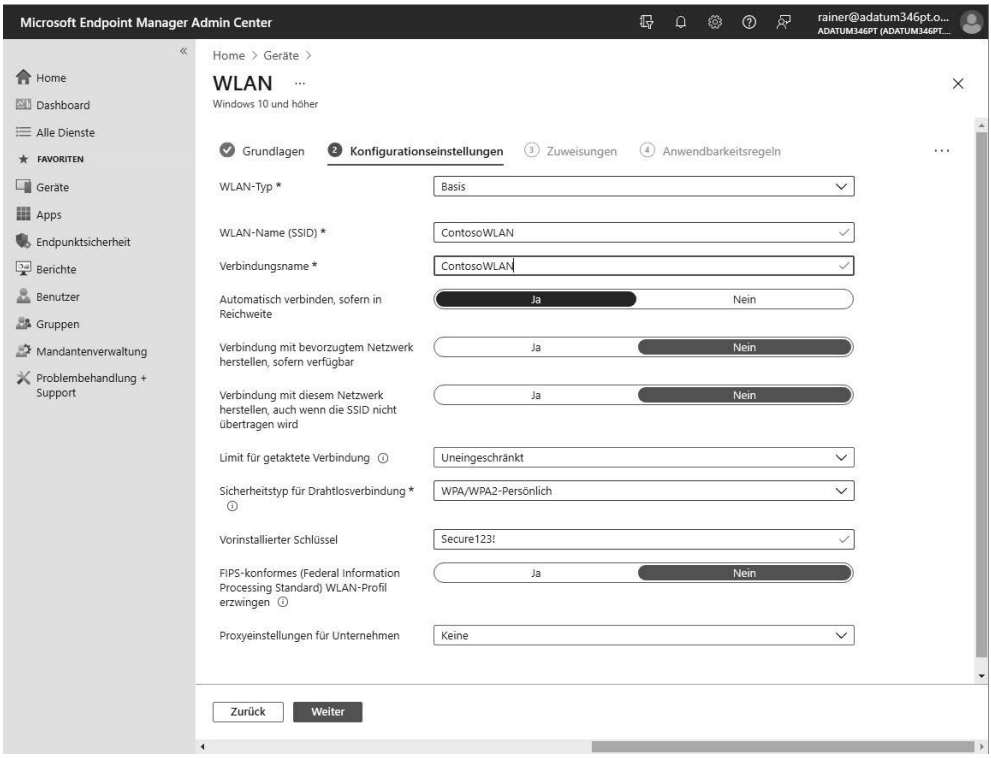

Abb. 1–3 Einstellungen des WLAN-Konfigurationsprofils

13. Klicken Sie auf **Weiter**.
14. Klicken Sie auf der Registerkarte **Zuweisungen** auf **Alle Geräte hinzufügen**. Wählen Sie alternativ die Gruppen von Geräten aus, für die das Profil gelten soll.
15. Klicken Sie auf **Weiter**.
16. Lassen Sie auf der Registerkarte **Anwendbarkeitsregeln** die Standardeinstellungen leer. Alternativ können Sie auch Regelfilter hinzufügen, um festzulegen, wann dieses Konfigurationsprofil angewendet werden soll.
17. Klicken Sie auf **Weiter** und klicken Sie dann auf **Erstellen**.

Die Konfigurationsregel wird erstellt und zu den von Ihnen ausgewählten Geräten hinzugefügt.

Nachdem Sie das Profil erstellt haben, können Sie seinen Status auf Geräte- und Benutzerebene sehen. Beachten Sie jedoch, dass es je nach Anzahl der Geräte und deren Verbindungstyp einige Minuten dauern kann, bis das Profil bereitgestellt und auf die Geräte angewendet wird. Abbildung 1–4 zeigt den Status des neu erstellten Profils, das auf ein Windows 10-Gerät angewendet wird.

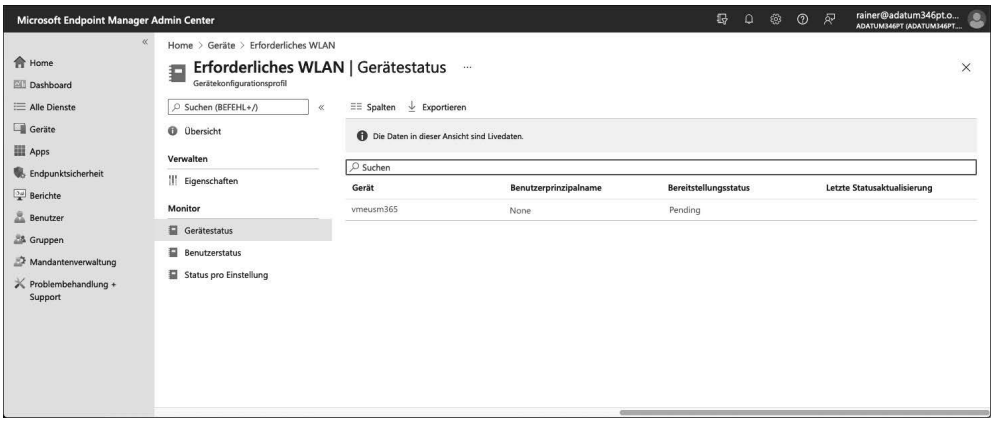

Abb. 1–4 Ausstehende Profilbereitstellung

Prüfungsziel 1.2: Verwaltung der Gerätekonformität

Mit der Gerätekonformität wird sichergestellt, dass die Geräte, die auf Ihre Umgebung zugreifen, bestimmte Anforderungen erfüllen. Diese Anforderungen werden meistens von den IT- und Cybersicherheitsteams in Ihrem Unternehmen festgelegt. Im Rahmen dieser Prüfung wird die Gerätekonformität auch als eine Funktion in Microsoft Intune bezeichnet. Diese Funktion wird bereitgestellt, um Administratoren bei der Definition ihrer Compliance-Anforderungen zu unterstützen und den Zugriff auf Daten und Dienste zu delegieren. Als Administrator ist es Ihre Aufgabe, die Anwendungsfälle für die Gerätekonformität zu verstehen und zu wissen, wie sie zu implementieren sind.

Die von Ihnen definierten Konformitätsrichtlinien bilden das Bindegewebe für verschiedene andere Aktionen in der Plattform. So kann beispielsweise der Konformitätsstatus eines Geräts als entscheidender Faktor für die Gewährung des Zugriffs auf Exchange Online genutzt werden. Dies wird mithilfe von Richtlinien für den bedingten Zugriff erreicht, einer weiteren wichtigen Funktion, die in diesem Kapitel behandelt wird. Richtlinien für den bedingten Zugriff sind eine andere Art von Richtlinie, die in Azure Active Directory (Azure AD) verwaltet wird, um den Zugriff auf Daten und Dienste zu erlauben oder zu verweigern.

Dieser Abschnitt behandelt die folgenden Themen:

- Planung der Gerätekonformität
- Reduzierung der Angriffsfläche planen
- Konfigurieren von Sicherheits-Baselines
- Konfigurieren von Richtlinien zur Gerätekonformität

Planung der Gerätekonformität

In diesem Abschnitt werden Überlegungen zur Planung der Gerätekonformität behandelt. Dazu gehören Themen wie Voraussetzungen vor der Implementierung, Konformitäts-Workflows und mögliche Anwendungsfälle für Ihr Unternehmen. Später in diesem Kapitel werden Sie mit Richtlinien zur Zugriffskontrolle arbeiten. Eine der Abhängigkeiten für den bedingten Zugriff ist der Konformitätsstatus des Endbenutzergeräts. Die MS-101-Prüfung enthält Szenarien, die sich mit der Intune-Registrierung, der Gerätekonformität und dem bedingten Zugriff befassen. Nehmen Sie sich bei der Vorbereitung Zeit, um mit diesen Technologien im Azure-Portal zu arbeiten und die Abhängigkeiten zu erkennen.

Die Voraussetzungen für die Gerätekonformität verstehen

Bevor Sie mit der Erstellung von Richtlinien zur Gerätekonformität beginnen, müssen Sie einige technische Voraussetzungen berücksichtigen. Im Verlauf dieses Buches werden Sie einige der wichtigsten Voraussetzungen für jede der Cloud-Technologien finden, insbesondere im Zusammenhang mit den erforderlichen Abonnements. Achten Sie bei der Prüfung auf diese Voraussetzungen und nehmen Sie sich etwas mehr Zeit, um zu verstehen, welche Funktionen in den verschiedenen Abonnementmodellen enthalten sind.

Dies sind die Voraussetzungen für die Gerätekonformität:

- **Abonnements** Die Technologie für die Gerätekonformität stützt sich auf Azure AD und Microsoft Intune. Das Gerät muss in Intune registriert werden, um eine Konformitätsrichtlinie zu erhalten. Das Konformitätskennzeichen wird in Azure AD gespeichert und auch für andere Funktionen, wie z.B. bedingten Zugriff, genutzt. Sie benötigen mindestens ein eigenständiges Intune-Abonnement sowie ein Azure AD Premium P1-Abonnement. Die höherstufigen Abonnements, wie Azure AD Premium P2, enthalten keine zusätzlichen Funktionen, die auf die Gerätekonformität ausgerichtet sind.
- **Plattformunterstützung** Richtlinien zur Gerätekonformität unterstützen eine Vielzahl von Plattformen. (Zur Klarstellung: Der Begriff *Plattform* bezieht sich auf das Betriebssystem, nicht auf die physische Hardware.)

  Die Plattformunterstützung ist eine wichtige Voraussetzung, wenn Sie planen, Geräte zu verwalten, die nicht unterstützt werden. Zum Zeitpunkt der Erstellung dieses Dokuments werden die folgenden Plattformen unterstützt:

  - Android
  - Android Enterprise
  - iOS/iPadOS
  - macOS
  - Windows 8.1
  - Windows 10

- **Registrierung** Geräte können erst dann die Konformität melden, wenn sie in Microsoft Intune registriert sind.

WEITERE INFORMATIONEN **Ein Abonnement auswählen**

Weitere Informationen zu den verschiedenen Editionen von Azure AD und der entsprechenden Abonnementstufe finden Sie unter *https://azure.microsoft.com/de-de/pricing/details/active-directory*.

Weitere Informationen zu Abonnements für Microsoft Intune finden Sie unter *https://www.microsoft.com/de-de/security/business/Microsoft-endpoint-manager*.

Den Prozessablauf für die Gerätekonformität verstehen

Sowohl Gerätekonformität als auch bedingter Zugriff sind richtlinienbasierte Technologien. Sie konfigurieren die Richtlinie, um Ihre Anforderungen zu erfüllen, und weisen diese Richtlinie dann in Microsoft Intune den gewünschten Ressourcen zu. Die Geräte werten die Richtlinie aus und melden zurück, ob sie die Anforderungen erfüllen oder nicht. Der Konformitätsstatus wird dann als benutzerdefiniertes Attribut in das Geräteobjekt in Azure AD geschrieben. Der Status dieses Attributs bestimmt, ob das Gerät für den Zugriff auf Daten und Dienste zugelassen ist. An dieser Stelle kommt der bedingte Zugriff ins Spiel, der später in diesem Kapitel ausführlicher behandelt wird.

Abbildung 1–5 veranschaulicht den Ablauf der Gerätekonformität. In diesem Beispiel wird die Standardkonfiguration für die Gerätekonformität verwendet. Als Administrator haben Sie einige wenige Möglichkeiten, diesen Ablauf an Ihre Anforderungen anzupassen.

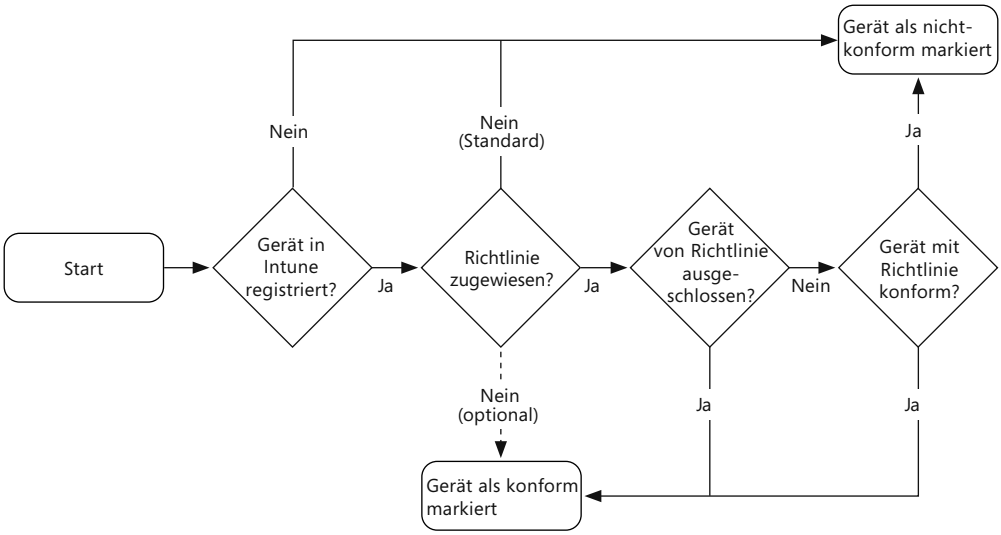

Abb. 1–5 Prozessablauf der Gerätekonformität

Die folgenden Punkte beschreiben Einstellmöglichkeiten, die Administratoren zur Verfügung stehen, um den Fluss der Gerätekonformität zu ändern.

- **Intune-Registrierung** Geräte, die nicht in Intune registriert sind, können keine Richtlinien zur Gerätekonformität erhalten. Dies gilt auch für Geräte, die mit Azure AD verbunden sind. Dies wurde bereits im Abschnitt über die Voraussetzungen behandelt. In diesem Zusammenhang kann die nicht vorhandene Intune-Registrierung auch verwendet werden, um zu verhindern, dass Konformitätsrichtlinien auf nicht verwaltete Geräte angewendet werden.
- **Richtlinienzuweisung** In den Einstellungen für Konformitätsrichtlinien für Microsoft Intune haben Sie die Möglichkeit, Geräte als konform zu markieren, denen keine Richtlinie zugewiesen ist. Standardmäßig werden alle Geräte ohne eine zugewiesene Richtlinie als nicht konform markiert. Sie haben jedoch die Möglichkeit, dieses Verhalten zu ändern und alle Geräte standardmäßig als konform zu kennzeichnen. Dies wird durch die gestrichelte Linie zwischen der zugewiesenen Richtlinie und dem als konform gekennzeichneten Gerät in der Abbildung dargestellt, die mit dem Text *optional* beschriftet ist.
- **Geräte ausschließen** Das Ausschließen von Geräten ist ein weiteres Steuerelement, das Sie konfigurieren können. Dies geschieht in den Richtlinieneinstellungen, indem Sie festlegen, für welche Geräteplattformen die Konformitätsrichtlinie gelten soll. Wenn Ihre Konformitätsrichtlinie alle Plattformen außer iOS umfasst, sind iOS-Geräte von der Ausführung dieser Richtlinie ausgenommen.

PRÜFUNGSTIPP

Während der Vorbereitung auf diese Prüfung sollten Sie sich die einzelnen Optionen für die Gerätekonformität im Intune-Portal genau ansehen. Beachten Sie die Einstellungen sowohl aus der Portal- als auch aus der PowerShell-Perspektive.

Anwendungsfälle für die Gerätekonformität kennenlernen

In diesem Abschnitt werden Sie sich einige potenzielle Anwendungsfälle für die Gerätekonformität ansehen. Machen Sie sich zunächst klar, dass Konformitätsrichtlinien eine Reihe von Regeln enthalten, die Sie definieren. Diese Regeln bestimmen, ob ein Gerät konform ist. Konformitätsrichtlinien können helfen, bestimmte Bedingungen zu beheben, aber in den meisten Fällen wird das Gerät unter Quarantäne gestellt, und die Behebung wird dem Benutzer überlassen. Angenommen, Sie verfügen über eine Richtlinie zur Gerätekonformität, die eine Sicherheitsregel enthält, die vor dem Entsperren eines Geräts ein Kennwort verlangt. Wenn ein Gerät diese Richtlinie nicht erfüllt, wird der Benutzer aufgefordert, ein Kennwort für sein nicht konformes Gerät festzulegen.

Benutzer mit Geräten, die als nicht richtlinienkonform gekennzeichnet sind, erhalten Benachrichtigungen über die nicht erfüllten Regeln. Als Administrator können Sie auch eine Richtlinie für den bedingten Zugriff erstellen, um diese Geräte zu sperren, bis sie repariert sind. In Tabelle 1–1 finden Sie eine Reihe von Konformitätsrichtlinien und entsprechende Anwendungsbeispiele.

Plattform	Einstellung(en)	Beispiel für Anwendungsfall
Windows 10	Mindestversion des Betriebssystems Gültige Betriebssystembuilds	Windows 10-Geräte, auf denen nicht das neueste kumulative Update ausgeführt wird, werden als nicht konform gekennzeichnet. Windows 10-Geräte, auf denen eine unterstützte Version ausgeführt wird, sind noch gültig, während die Upgrades ausgerollt werden.
macOS	Systemintegritätsschutz erforderlich	macOS-Geräte, auf denen der Systemintegritätsschutz nicht aktiviert ist, werden als nicht konform gekennzeichnet.
Android	Gerootete Geräte Verschlüsselung des Datenspeichers	Android-Geräte, die gerootet sind, werden als nicht konform markiert. Android-Geräte, bei denen die Verschlüsselung des Datenspeichers nicht aktiviert ist, werden als nicht konform gekennzeichnet.
iOS	Geräte mit Jailbreak Mindestversion des Betriebssystems Eingeschränkte Apps	iOS-Geräte, auf denen ein Jailbreak vorhanden ist, werden als nicht konform markiert. iOS-Geräte, auf denen nicht die neueste Hauptversion von iOS läuft, werden als nicht konform markiert. iOS-Geräte, auf denen die Dropbox-App installiert ist, werden als nicht konform markiert.

Tab. 1–1 Beispiele von Anwendungsfällen für plattformspezifische Einstellungen

Richtlinien für den bedingten Zugriff entwerfen

In diesem Abschnitt werden Sie die Designaspekte von Richtlinien für den bedingten Zugriff kennenlernen. Während Sie sich auf diese Prüfungsziele vorbereiten, sollten Sie Zeit für die Arbeit im Azure-Portal einplanen und sich die Schnittstelle und die Steuerelemente für den bedingten Zugriff ansehen.

In diesem Abschnitt wurde zunächst erläutert, was Gerätekonformität aus Perspektive des Cloud-Managements bedeutet. Jetzt werden Sie sehen, wie die Gerätekonformität verwendet wird, um Zugriffsanforderungen für Daten und Dienste in Ihrem Unternehmen einzurichten.

Design für den Schutz von Daten und Diensten mithilfe von Richtlinien für den bedingten Zugriff

Es gibt eine Vielzahl von Richtlinieneinstellungen für den bedingten Zugriff und eine Vielzahl von Konfigurationen, die Sie implementieren können. Werfen wir zunächst einen Blick auf das Blatt **Richtlinien für den bedingten Zugriff** im Azure-Portal. Dies wird Ihnen dabei helfen,

sich mit den Richtlinien für bedingten Zugriff vertraut zu machen und einige Schlüsselbegriffe kennenzulernen. Abbildung 1–6 zeigt das Blatt **Neue Richtlinie für den bedingten Zugriff**. Schauen wir uns die einzelnen verfügbaren Optionen genauer an.

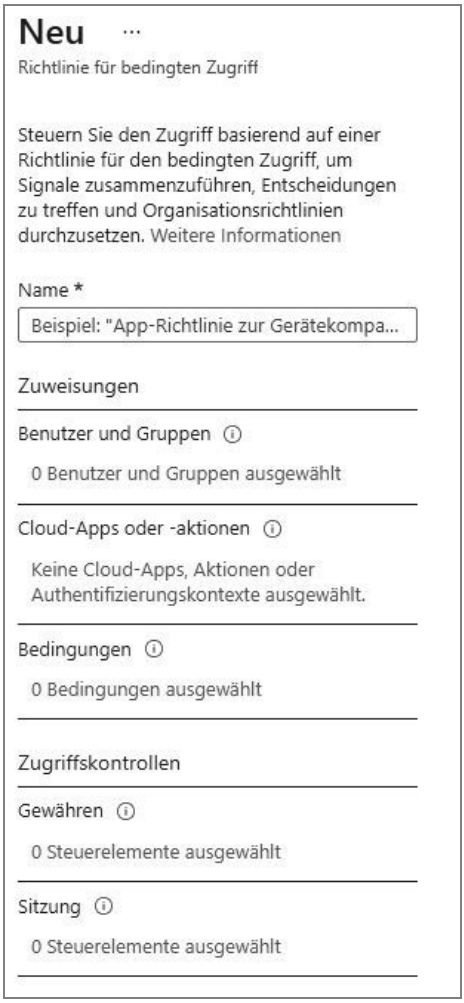

Abb. 1–6 Erstellen einer Richtlinie für bedingten Zugriff

- **Zuweisungen** Diese definieren den Umfang, die Kriterien und die Bedingungen der Richtlinie, die Sie bereitstellen. Das Blatt **Neue Richtlinie für bedingten Zugriff** enthält drei Zuweisungskategorien:
  - **Benutzer und Gruppen** Diese definieren, wer die Richtlinie erhält. Sie können Benutzer und Gruppen entweder einschließen oder ausschließen. Obwohl das Blatt **Neue Richtlinie für bedingten Zugriff** Sie nicht daran hindert, fortzufahren, benötigen alle Richtlinien für den bedingten Zugriff eine Benutzer- und Gruppenzuweisung, bevor sie angewendet werden können. Für das Einschließen können Sie alle Benutzer oder bestimmte Benutzer und Gruppen auswählen. Wenn Sie zum Beispiel eine Gruppe haben,

die nur Ihr Marketing-Team enthält, können Sie diese als Option auswählen. Als Ausschlusskriterien können Sie alle Gastbenutzer (definiert durch das Attribut userType), bestimmte Verzeichnisrollen (z. B. Anwendungsentwickler) oder bestimmte Benutzer oder Gruppen auswählen.

- **Cloud-Apps oder -aktionen** Diese definieren die Dienste, auf die Benutzer für ihre Produktivität zugreifen können. Sie haben die Wahl, Dienste aus einer vordefinierten Liste unterstützter Cloud-Apps ein- oder auszuschließen. Für Einschlüsse können Sie alle Cloud-Apps oder bestimmte Apps, wie z. B. Microsoft Teams, auswählen. Für den Ausschluss können Sie bestimmte Apps auswählen.
- **Bedingungen** Diese definieren, wann eine Richtlinie angewendet wird. In Tabelle 1–2 finden Sie eine Aufschlüsselung der einzelnen Bedingungen, die verfügbaren Optionen und einige Anwendungsbeispiele.

Bedingung	Beschreibung	Optionen	Beispiel eines Anwendungsfalls
Anmelderisiko	Azure AD bestimmt das Anmelderisiko eines Benutzers basierend auf einer konfigurierbaren Richtlinie unter Azure AD Identity Protection.	Hoch, Mittel, Niedrig oder kein Risiko	Durchsetzung der MFA-Richtlinie für Benutzer, die mit einem mittleren Anmelderisiko markiert sind.
Geräteplattformen	Azure AD ruft das Betriebssystem des eingebundenen Geräts ab, aber diese Informationen werden nicht überprüft. Diese sollte mit einer Microsoft Intune-Registrierung und Geräte-Konformitätsrichtlinie kombiniert werden.	Android, iOS, Windows Phone, Windows, macOS	Setzen Sie eine App-Beschränkungsrichtlinie nur auf iOS- und Android-Geräten durch.
Standorte	Standorte werden verwendet, um vertrauenswürdige Netzwerkstandorte zu definieren. Vertrauenswürdige Netzwerkstandorte werden in Azure AD unter **Benannte Standorte** konfiguriert.	Alle Standorte, Alle vertrauenswürdigen Standorte, Ausgewählte Standorte	Blockieren Sie den Zugang zu Exchange Online aus dem Büro in San Francisco mit dem IP-Subnetz 10.20.11.0/22.
Client-Apps	Legen Sie bedingte Einschränkungen basierend auf bestimmten Client-Anwendungen fest.	Browser, Mobile Apps und Desktopclients	Schränken Sie den Zugang zu mobilen Apps ein, wenn das Gerät nicht als konform gekennzeichnet ist.
Gerätestatus (Vorschau)	Schließen Sie unternehmenseigene oder vertrauenswürdige Geräte von bedingten Zugriffsbeschränkungen aus.	In Azure AD eingebundenes Hybridgerät, Gerät als konform markiert	Setzen Sie für nicht-konforme Geräte Einschränkungen für Office 365 Exchange Online durch.

Tab. 1–2 Optionen für den bedingten Zugriff

- **Zugriffskontrollen** Diese definieren zusätzliche Anforderungen für die Gewährung oder Verweigerung des Zugriffs sowie Sitzungssteuerelemente zur Einschränkung der Erfahrung innerhalb von Cloudanwendungen. Die folgenden Optionen sind im Abschnitt **Zugriffskontrollen** verfügbar:
  - **Gewähren** Damit können Sie den Zugriff auf der Grundlage der Bedingungen sperren, die Sie im Abschnitt **Zuweisungen** definiert haben. Alternativ dazu können Sie den Zugriff gewähren und zusätzliche Anforderungen durchsetzen. So können Sie beispielsweise MFA verlangen oder den Zugriff nur auf Geräte gewähren, die durch Richtlinien zur Gerätekonformität als konform gekennzeichnet sind.
  - **Sitzung** Mit dieser Option können Sie die Nutzung bestimmter Cloudanwendungen einschränken. Zum Zeitpunkt der Erstellung dieses Dokuments sind Office 365, SharePoint Online und Exchange Online die einzigen Cloudanwendungen, die von der App erzwungene Einschränkungen unterstützen. Wenn Sie diese Funktion aktivieren, können Sie diese Anwendungen in Echtzeit überwachen und steuern.

Nachdem Sie nun einige Zeit damit verbracht haben, die Benutzeroberfläche zu erkunden, wollen wir uns nun ansehen, wie eine Richtlinie für bedingten Zugriff aufgebaut ist. Die Richtlinie besteht aus zwei Teilen: der Bedingung und der Zugriffskontrolle. Sie können diese auch in folgendem Zusammenhang betrachten: *Wenn dies geschieht* (Bedingung), *dann mache das* (Zugriffskontrolle). Für die Prüfung sollten Sie mit dieser Formel vertraut sein und wissen, wie sie mit den Einschränkungen mithilfe des bedingten Zugriffs korrespondiert. In Tabelle 1–3 finden Sie einige Beispiele für den Aufbau von Zugriffskontrollrichtlinien.

Wenn dies geschieht (Bedingung)	Dann mache das (Zugriffskontrolle)
Besitzer von Windows- und macOS-Geräten greifen auf SharePoint Online von einem nicht vertrauenswürdigen Netzwerk aus zu. Es sind zusätzliche Sicherheitsmaßnahmen erforderlich.	Gewähren Sie Windows- und macOS-Geräten Zugriff auf SharePoint Online. Erfordern Sie eine Multi-Faktor-Authentifizierung und ein konformes Gerät, wenn der Zugriff von einem nicht vertrauenswürdigen Netzwerk aus erfolgt.
Das Vertriebsteam greift von ihren iOS- und Android-Geräten auf Exchange Online zu. Diese Geräte müssen konform sein, bevor der Zugriff gewährt wird.	Gewähren Sie der Gruppe Vertrieb Zugriff auf Exchange Online. Verlangen Sie, dass alle Besitzer von Geräten des Vertriebsteams in Intune registriert und als konform gekennzeichnet sein müssen.
Alle Benutzer greifen auf Microsoft Teams von vertrauenswürdigen und nicht vertrauenswürdigen Netzwerken zu. Für Benutzer, die sich in einem nicht vertrauenswürdigen Netzwerk befinden, sind zusätzliche Sicherheitsmaßnahmen erforderlich.	Gewähren Sie allen Benutzern Zugriff auf Microsoft Teams. Fordern Sie Multi-Faktor-Authentifizierung, wenn der Zugriff von einem nicht vertrauenswürdigen Netzwerk aus erfolgt.
BYOD-Geräte greifen über ihre Browser auf Exchange Online zu. Der Zugriff muss auf genehmigte Anwendungen beschränkt werden.	Gewähren Sie allen Benutzern Zugriff auf Exchange Online. Schränken Sie den Zugriff nur auf vertrauenswürdige Client-Anwendungen ein.

Tab. 1–3 Bedingungen und Zugriffskontrollen

Die folgende Liste enthält Voraussetzungen, mit denen Sie vertraut sein müssen. Einige davon sind feste Anforderungen und andere sind strategische Fragen, die Sie dabei unterstützen, sich auf den Entwurf von Richtlinien vorzubereiten.

- **Abonnements** Die grundlegenden Funktionen der Zugriffskontrolle sind mit einem Azure AD Premium-Abonnement verfügbar. Es gibt jedoch zusätzliche Funktionen, die erst verfügbar sind, wenn Sie Ihr Abonnement aktualisieren. Dazu gehören die folgenden:
  - **Azure AD Premium P1** Das P1-Abonnement bietet Ihnen die grundlegenden Funktionen für Richtlinien für bedingten Zugriff.
  - **Azure AD Premium P2** Das P2-Abonnement ermöglicht Identitätsschutz, der erforderlich ist, wenn Sie das Anmelderisiko nutzen möchten. Das Anmelderisiko ist eine Funktion, die feststellt, ob eine Benutzeranmeldung böswillig ist, und den Risikograd misst. Diese Funktion kann als Teil Ihrer Richtlinienbedingungen genutzt werden.
  - **Microsoft Intune** Intune kann als Einzelprodukt oder über ein Enterprise Mobility + Security E3- oder E5-Abonnement erworben werden. Richtliniendefinitionen, die ein konformes Gerät erfordern, hängen davon ab, dass das Gerät in Intune registriert ist.

> ***WEITERE INFORMATIONEN*** **Details zu Abonnements**
>
> **Weitere Informationen über Azure AD-Abonnements finden Sie unter *https://azure.microsoft.com/de-de/pricing/details/active-directory*. Weitere Informationen über Microsoft Intune-Abonnements finden Sie unter *https://www.microsoft.com/de-de/security/business/Microsoft-endpoint-manager*.**

- **Berechtigungen** Bevor Sie mit dem Erstellen und Verwalten von Richtlinien für bedingten Zugriff beginnen können, müssen Sie Ihrem Konto die entsprechenden Berechtigungen zuweisen. Der Administrator für bedingten Zugriff ist eine vordefinierte Rolle, die die erforderlichen Berechtigungen enthält.
- **Zu erfüllende Anforderungen** Welche Anforderungen haben Sie an die Gerätekonformität und den bedingten Zugriff? Dies ist etwas, das Sie von Anfang an definieren sollten. Legen Sie fest, ob es sich um ein einfaches Ziel handelt (z. B. die Erzwingung der Multi-Faktor-Authentifizierung für Benutzer) oder um etwas Komplexeres (z. B. die Einschränkung des Zugriffs auf SharePoint Online von Windows-Geräten, wenn diese mit einem nicht vertrauenswürdigen Netzwerk verbunden sind).
- **Geräteverwaltung** Welche Lösung für die Geräteverwaltung setzen Sie aktuell ein? Der volle Funktionsumfang des bedingten Zugriffs hängt von Microsoft Intune ab. Wenn Sie jedoch ConfigMgr verwenden, können Sie Co-Management aktivieren und die Richtlinien für bedingten Zugriff früher nutzen.
- **Geräteplattformen** Welche Arten von Geräten und Betriebssystemen müssen Sie unterstützen? Richtlinien für bedingten Zugriff unterstützen eine Vielzahl von Betriebssystemen. Zum Zeitpunkt der Erstellung dieses Dokuments sind die einzigen Ausreißer Geräte, die unter Linux laufen. Überlegen Sie, welche Geräte in Ihrer Umgebung vorhanden sind und welche Arten von Beschränkungen Sie erzwingen müssen.

- **E-Mail-Anforderungen** Welche Anforderungen stellen Sie an den Zugriff auf E-Mails? E-Mail wird häufig als einer der ersten Dienste für die Durchsetzung von bedingten Zugriffsbeschränkungen verwendet. Wenn Ihr Ziel darin besteht, bedingte Zugriffsbeschränkungen für Exchange Online zu aktivieren, ist die Auswahl der Cloud-App aus der Standardliste der Zuweisungen einfach und wird später in diesem Kapitel behandelt. Wenn Ihr Ziel darin besteht, Zugriffsbeschränkungen für einen lokalen Exchange-Server zu aktivieren, müssen Sie zusätzliche Voraussetzungen einplanen, z.B. die Installation und Konfiguration des lokalen Exchange-Connectors.

Design von geräte- und App-basierten Richtlinien für den bedingten Zugriff

Zunächst sollten Sie verstanden haben, dass eine Richtlinie für den bedingten Zugriff eine beliebige Kombination von Optionen enthalten kann, einschließlich gerätebasierter und App-basierter Einschränkungen. Die Unterscheidung zwischen gerätebasierten und App-basierten Beschränkungen hängt von den von Ihnen ausgewählten Zugriffskontrollen und der Struktur Ihrer Richtlinien ab. Abgesehen davon können geräte- und App-basierte Richtlinien unterschiedliche Anforderungen haben und unabhängig voneinander funktionieren, wenn Sie dies wünschen.

Sehen wir uns ein paar Beispiele an:

- **Gerätebasiert** Diese erste Richtlinie konzentriert sich auf gerätebasierte Steuerung. Hier verlangt die Richtlinie für iOS-Geräte in nicht vertrauenswürdigen Netzwerken die Multi-Faktor-Authentifizierung. Die Richtlinie wird allen Benutzern zugewiesen. In diesem Beispiel haben wir keine App-basierten Beschränkungen definiert, um den Fokus auf die Plattform und das Netzwerk zu legen.
- **App-basiert** Diese zweite Richtlinie konzentriert sich auf App-basierte Zugriffskontrollen. Hier erfordert die Richtlinie genehmigte Client-Apps beim Zugriff auf Exchange Online. Diese Richtlinie wird allen Benutzern zugewiesen. In diesem Beispiel haben wir keine gerätebasierten Beschränkungen definiert, sondern den Schwerpunkt auf Anwendungskontrollen gelegt.
- **Gemischt** Diese dritte Richtlinie enthält eine Mischung von Zugriffskontrollen. Hier verlangt die Richtlinie, dass alle Plattformen in Intune registriert und als konform gekennzeichnet werden, bevor sie von zugelassenen Client-Apps auf Exchange Online zugreifen können. In diesem Beispiel werden gerätebasierte und App-basierte Einschränkungen festgelegt, um das gewünschte Ergebnis zu erzielen.

Zu diesem Zeitpunkt sollten Sie die Unterschiede zwischen gerätebasierten und App-basierten Richtlinien gut verstehen. Als Nächstes werden wir die einzelnen Steuerelemente für die verschiedenen Richtlinientypen untersuchen. Die folgenden Punkte beziehen sich auf die Anforderungen gerätebasierter Richtlinien:

- **In Azure AD eingebundenes Gerät** Diese Anforderung ist sowohl als Bedingung als auch als Zugriffskontrolle verfügbar. Wenn Sie eine Bedingung definieren, haben Sie die Möglichkeit, Geräte auszuschließen, die in Azure AD eingebunden sind. Dies ist über das Blatt **Gerätestatus** möglich. Sie können dies in einem Szenario verwenden, in dem Sie den Zugriff sperren, aber in Azure AD eingebundene Geräte ignorieren möchten. Alternativ ha-

ben Sie bei der Definition der Steuerelemente für die Zugriffsgewährung die Möglichkeit, Azure AD-eingebundene Geräte zu verlangen. Dies ist über das Blatt **Gewähren** im Bereich **Zugriffskontrollen** verfügbar und kann als eine von vielen erforderlichen Kontrollen vor der Freigabe des Zugriffs auf Cloud-Anwendungen verwendet werden.

- **Gerätekonformität** Diese Anforderung ist sowohl als Bedingung als auch als Zugriffskontrolle verfügbar, ähnlich wie die im vorherigen Punkt erwähnte Anforderung für Geräte, die in Azure AD eingebunden sind. Geräte müssen in Microsoft Intune registriert und als konform gekennzeichnet sein, damit diese Anforderung erfüllt wird. Wenn Sie eine Bedingung definieren, haben Sie die Möglichkeit, Geräte auszuschließen, die als konform gekennzeichnet sind. Dies ist über das Blatt **Gerätestatus** möglich. Dies könnte in einem Szenario verwendet werden, in dem Sie den Zugriff sperren, aber registrierte Geräte, die die Anforderungen erfüllen, ignorieren möchten. Alternativ haben Sie bei der Definition für die Zugriffsgewährung die Möglichkeit, registrierte und konforme Geräte zu verlangen. Dies ist über das Blatt **Gewähren** für die Zugriffskontrolle verfügbar und kann als eine von vielen erforderlichen Kontrollen vor der Freigabe des Zugriffs auf Cloud-Anwendungen verwendet werden.
- **Geräteregistrierung** Diese Anforderung wird nicht direkt durch eine Richtlinie für bedingten Zugriff definiert, ist aber eine Voraussetzung für die Identifizierung der Gerätekonformität.
- **Geräteplattformen** Diese Anforderung ist als Bedingungselement verfügbar. Wenn Sie eine Bedingung definieren, haben Sie die Möglichkeit, die folgenden Betriebssysteme ein- oder auszuschließen: Android, iOS, Windows Phone, Windows und macOS. Diese Option ist über das Blatt **Geräteplattformen** verfügbar. Dies könnte in einem Szenario verwendet werden, in dem Sie den Zugriff auf eine Cloud-App einschränken und bestimmte Plattformen ausschließen möchten.

Als Nächstes wollen wir die App-basierten Anforderungen untersuchen. Wir haben im Abschnitt zu diesem Prüfungsziel bereits Sitzungssteuerelemente vorgestellt, mit denen Sie das Erlebnis in Cloud-Apps einschränken können. Zwei der Anforderungen, die wir abdecken werden, werden durch Sitzungssteuerelemente aktiviert. Die folgenden Punkte beziehen sich auf App-basierte Richtlinienanforderungen.

- **Von der App erzwungene Einschränkungen verwenden** Diese Anforderung ist als Element der Zugriffskontrolle verfügbar. Bei der Definition von Zugriffskontrollen haben Sie die Möglichkeit, von der App erzwungene Einschränkungen zu aktivieren. Diese Option wird auf dem Blatt **Sitzung** definiert. Sie kann in einem Szenario verwendet werden, in dem Sie nicht konformen Geräten eingeschränkten Zugriff auf Office 365 Exchange Online oder SharePoint Online gewähren müssen.
- **App-Steuerung für bedingten Zugriff verwenden** Diese Anforderung ist als Zugriffskontrollelement verfügbar. Wenn Sie Zugriffskontrollen definieren, haben Sie die Möglichkeit, die App-Steuerung für bedingten Zugriff zu aktivieren. Dies wird im Blatt **Sitzung** definiert. Dies kann in einem Szenario verwendet werden, in dem Sie den Anwendungszugriff in Echtzeit überwachen und kontrollieren müssen. Zugriffs- und Sitzungsrichtlinien kön-

nen dann über das Portal Microsoft Defender for Cloud Apps (früher Cloud App Security-Portal genannt) konfiguriert werden, das eine granulare Kontrolle des Benutzerzugriffs erlaubt.

- **Verfügbare Richtlinien** Dazu gehören Zugriffs-, Aktivitäts-, App-Erkennungs-, App-Berechtigungs-, Cloud Discovery-Anomalieerkennungs-, Datei- und Sitzungsrichtlinien. Einige dieser Richtlinien sind für die Überwachung und Alarmierung vorgesehen, während für andere automatische Aktionen aktiviert werden können.
- **Genehmigte Client-App erforderlich** Diese Anforderung ist als Zugriffskontrollelement verfügbar. Bei der Definition von Zugriffskontrollen haben Sie die Möglichkeit, die Anforderung für genehmigte Client-Apps zu aktivieren. Dies wird auf dem Blatt **Gewähren** definiert. Sie kann in einem Szenario verwendet werden, in dem Sie sicherstellen müssen, dass der Zugriff auf Dienste nur von genehmigten Clientanwendungen erfolgt.

> ***HINWEIS*** **Genehmigte Client-Apps**
>
> **Wenn Sie die Anforderung für genehmigte Client-Apps aktivieren, wird verhindert, dass Benutzer von nativen Anwendungen oder Anwendungen von Drittanbietern, die von Microsoft nicht genehmigt wurden, auf Dienste zugreifen. Eine Liste der zugelassenen Clientanwendungen finden Sie unter *https://docs.microsoft.com/azure/active-directory/conditional-access/technical-reference#approved-client-app-requirement*.**

Plan zur Reduzierung der Angriffsfläche

Die Reduzierung der Angriffsfläche ist eine Methode, um die Anzahl der Schwachstellen und Bedrohungen zu verringern, denen das Unternehmen durch die Verwendung dieser Geräte ausgesetzt sein könnte. Dieser Abschnitt beschreibt, wie Sie die Angriffsfläche reduzieren können, indem Sie Intune zur Erhöhung der Endpunktsicherheit verwenden. Nachdem Sie Geräte mit Windows 10 (oder höher) in Intune registriert haben, können Sie Endpunktsicherheitsrichtlinien und die Antivirensoftware von Windows Defender verwenden, um die Sicherheitseinstellungen des Geräts zu konfigurieren und Angriffe zu entschärfen.

> ***HINWEIS***
>
> **Um in Intune Sicherheitsrichtlinien zur Verringerung der Angriffsfläche zu verwenden, müssen Sie als Gerätebetriebssystem Windows 10 oder höher verwenden. Außerdem muss die Windows Defender-Virenschutzsoftware die primäre Virenschutzsoftware auf dem Gerät sein.**

Profile für die Endpunktsicherheit

Um die Angriffsfläche eines Geräts zu reduzieren, können Sie in Intune Profile für die Endpunktsicherheit verwenden. Wenn Sie ein neues Profil erstellen, wird als Betriebssystem Windows 10 oder höher unterstützt. Die verfügbaren Profileinstellungen sind wie folgt: