https://learn.microsoft.com/de-de/training/modules/describe-azure-identity-access-security/

Identität, Zugriff und Sicherheit in Azure

Einführung in Verzeichnisdienste, Authentifizierung und Sicherheitskonzepte 1

Lernziele

- **Verzeichnisdienste in Azure**:
  - Microsoft Entra ID und Domain Services
  - Verwaltung von Identitäten und Zugriffen
- **Authentifizierungsmethoden**:
  - Single Sign-On (SSO)
  - Multi-Faktor-Authentifizierung (MFA)
  - Kennwortlose Authentifizierung

2

Lernziele

- **Externe Identitäten und Gastzugriff**:
  - Zusammenarbeit mit Partnern und Kunden sichern
- **Bedingter Zugriff und Azure RBAC**:
  - Schutz sensibler Daten durch Rollen und Richtlinien
- **Sicherheitskonzepte**:

Zero-Trust-Modell
Defense-in-Depth-Modell

Microsoft Defender für Cloud:

Sicherheitsbewertungen und Bedrohungserkennung

Microsoft Entra ID

Was ist Microsoft Entra ID?

Ein cloudbasierter Verzeichnisdienst, der Benutzer und Ressourcen verwaltet. Zentral für die Identitäts- und Zugriffsverwaltung in Azure.

Funktionen:

Benutzer- und Gruppenverwaltung.
Unterstützung von SSO für alle Azure- und Drittanbieteranwendungen. Integration mit lokalen Active Directory-Diensten.

Microsoft Entra ID

Wichtig für AZ-900: Identitätsprüfung

Die **Identitätsprüfung** ist ein zentraler Bestandteil jeder Sicherheitsstrategie. **Sicherheit und Kontrolle:**

Nur Benutzer mit bestätigter Identität können auf Ressourcen zugreifen. Unbefugte Zugriffe werden verhindert.

Erster Schritt im Zero-Trust-Modell:

Jede Anfrage wird unabhängig vom Netzwerk überprüft.

Praxisbeispiel:

Ein Mitarbeiter meldet sich mit seiner Microsoft Entra ID an.

Azure überprüft die Identität (z. B. mit MFA) und gewährt basierend darauf Zugriff.

5

Microsoft Entra Domain Services

Was sind Domain Services?

Domain Services ermöglichen es, Benutzer, Geräte und Ressourcen zentral zu verwalten und sicherzustellen, dass nur autorisierte Benutzer Zugriff auf die richtigen Ressourcen haben.

Funktion:

Sie dienen als zentrale Steuerung für Authentifizierung und Zugriffskontrolle in einem Netzwerk.

6

Microsoft Entra Domain Services

Vergleich mit AWS:

AWS Directory Service bietet ähnliche Funktionen, ist jedoch oft komplexer in der Integration.

7

Authentifizierungsmethoden

Single Sign-On (SSO):

Ermöglicht Benutzern den Zugriff auf mehrere Anwendungen mit einem einzigen Login.
Beispiel: Zugriff auf Microsoft 365-Dienste.

Multi-Faktor-Authentifizierung (MFA):
Fügt eine zusätzliche Sicherheitsebene hinzu.
Beispiele: Authentifizierungs-Apps, SMS-Codes.

8

Authentifizierungsmethoden

Kennwortlose Authentifizierung:
Methoden wie FIDO2-Schlüssel oder biometrische Verfahren.
Vorteile: Vermeidung von schwachen Passwörtern.

Parallele zu AWS:
AWS IAM bietet ähnliche Authentifizierungsmethoden, jedoch weniger integriert mit Apps.

9

Externe Identitäten und Gastzugriff

Externe Identitäten:
Ermöglichen, dass Partner und Kunden mit ihren eigenen Anmeldeinformationen auf Ressourcen zugreifen.

Gastzugriff:

Bietet eine schnelle und einfache Möglichkeit, Gästen eingeschränkten Zugriff auf spezifische Ressourcen wie Teams oder SharePoint zu geben.

10

Externe Identitäten und Gastzugriff

Beispiel:

Ein Partner wird eingeladen, auf gemeinsame Dokumente im SharePoint zuzugreifen.

Wichtig für AZ-900:

Verstehen, wie Gastzugriff die Zusammenarbeit sicher gestaltet.

11

Bedingter Zugriff

Was ist bedingter Zugriff?

Richtlinien, die den Zugriff basierend auf Benutzerstandort, Gerät oder Rolle regeln.

Beispiele für Richtlinien:

Blockieren von unsicheren Ländern.

Erzwingen von MFA für sensible Ressourcen.

12

Bedingter Zugriff

Wichtig für AZ-900:

Kenntnis der zentralen Rolle des bedingten Zugriffs für die Sicherheit in Azure. 13

Azure RBAC

Was ist RBAC?

Rollenbasierte Zugriffssteuerung: Verwalten von Berechtigungen basierend auf Rollen.
In AWS nutzen wir dafür IAM.

Beispiele für Standardrollen:

Leser: Nur Leseberechtigungen.
Mitwirkender: Erstellen und Bearbeiten von Ressourcen.
Besitzer: Vollzugriff.

14

Azure RBAC

Prinzip des minimalen Zugriffs:

Benutzern nur die Berechtigungen geben, die sie wirklich benötigen.

15

Zero-Trust-Modell

Was ist Zero-Trust?

Ansatz: „Nie vertrauen, immer überprüfen.“

Kernelemente:

Überprüfung jeder Identität und jedes Geräts.
Minimale Rechtevergabe.
Kontinuierliches Monitoring.

16

Defense-in-Depth-Modell

Was ist Defense-in-Depth?

Konzept der mehrschichtigen Sicherheit.

Schichten:

Physische Sicherheit.
Netzwerksicherheit.
Identitäts- und Zugriffskontrolle.
Anwendungssicherheit.

17

Microsoft Defender für Cloud

Funktionen:

Bedrohungserkennung.
Sicherheitsbewertungen.
Schutz für Workloads wie VMs, Datenbanken und Kubernetes.

18

Microsoft Defender für Cloud

Wichtig für AZ-900:

Verständnis, wie Defender Sicherheitsprobleme erkennt und behebt.

19