Praxisbeispiel:

1. Terraform-Aufgabe: Bereitstellung einer Azure Web App

- **Aufgabe**: Verwenden Sie Terraform, um eine Azure Web App zu erstellen. Die Web App sollte in einem neuen Resource Group und in einem definierten Azure App Service Plan bereitgestellt werden.
- **Anforderungen**:
    - Eine Resource Group muss erstellt werden.
    - Erstellen Sie einen App Service Plan im kostenfreien Tarif.
    - Erstellen Sie eine Web App, die eine einfache Webseite hosten kann.
    - Die Konfiguration der App sollte von Variablen abhängen (z.B. App Name, Region).

2. Azure DevOps Pipelines (ADO) Aufgabe: CI/CD Pipeline für Azure Web App

- **Aufgabe**: Implementieren Sie eine vollständige CI/CD-Pipeline in Azure DevOps für eine Web-App.
- **Anforderungen**:
    - Erstellen Sie eine YAML-basierte Pipeline, die den Code einer Beispiel-Web-App aus einem Git-Repository abruft.
    - Stellen Sie sicher, dass die Pipeline einen Build-Prozess durchführt und anschließend die Anwendung in einer Azure Web App bereitstellt.
    - Fügen Sie Schritte zur Durchführung von Unit-Tests und zur Bereitstellung der App im Staging und dann in der Produktionsumgebung hinzu.

3. Aufgabe zur Netzwerkkonfiguration: Implementierung eines virtuellen Netzwerks

- **Aufgabe**: Erstellen Sie ein Azure Virtual Network mit Subnets und einem Network Security Group (NSG).
- **Anforderungen**:
    - Erstellen Sie ein virtuelles Netzwerk mit mindestens zwei Subnetzen (Frontend und Backend).
    - Richten Sie eine Network Security Group ein, die den HTTP-Traffic nur zum Frontend-Subnetz zulässt.
    - Konfigurieren Sie den Backend-Traffic so, dass er nur aus dem Frontend-Subnetz zugänglich ist.
    - Stellen Sie sicher, dass keine eingehende Verbindung zu Backend-Ressourcen möglich ist.

-

4. Speicheraufgabe: Erstellung eines Storage-Accounts mit Verschlüsselung und Zugriffsrichtlinien

- **Aufgabe**: **Konfigurieren Sie einen Azure Storage Account für ein Projekt mit spezifischen Sicherheitsanforderungen.**
- **Anforderungen**:
    - Erstellen Sie einen Storage Account mit blob encryption aktiviert.
    - Richten Sie eine Shared Access Signature (SAS) ein, die nur für 1 Stunde gültig ist und nur Lesezugriff auf eine bestimmte Blob-Datei ermöglicht.
    - Erstellen Sie eine Lifecycle-Policy, die ältere Blobs automatisch archiviert.