# Aufgabe 1: Anwendungssicherheit

# Datenbank schützen:

• Keine direkte Verbindung zum Internet

• Zugriff nur über Backend-Server

• Starke Authentifizierung und verschlüsselte Verbindungen (TLS)

• Firewall-Regeln, um unautorisierte Zugriffe zu blockieren

• Ports absichern:

## Ports absichern:

• Nu notwendige Ports öffnen (z. B. über eine Firewall oder Security Groups)

• SSH-Zugriff auf bestimmte IP-Adressen beschränken

• Unnötige Dienste deaktivieren

• Benutzer- und Rechtemanagement:

## Benutzer- und Rechtemanagement:

• Least Privileg-Prinzip: Benutzer nur die nötigsten Rechte geben

• Multi-Faktor-Authentifizierung (MFA) nutzen

• Regelmäßige Überprüfung von Berechtigungen

• Sichere Softwareentwicklung:

## Sichere Softwareentwicklung:

• Eingaben validieren, um SQL-Injektion und XSS zu verhindern

• Regelmäßige Sicherheitsupdates und Patch-Management

• Code-Reviews und Penetrationstests durchführen

## Hardware-Schutz

• Biometrisch Zugänge

• Kameras

• Sicherheitspersonal

# Aufgabe 2: VM

Unbekannte Begriffe: VPC,

Bekannte Begriffe: Firewall, Port, Verschlüsselung, Authentifizierung, Security Group