

# Intranet-Deployment

## Netzwerk-Infrastruktur dokumentieren

### Wichtig fürs Pflichtenheft!

Da die Portainer-Umgebung nur aus dem Schulungs-WLAN erreichbar ist, musst du das im Pflichtenheft klar dokumentieren. Das ist KEIN Nachteil, sondern zeigt professionelles Denken über Netzwerk-Sicherheit!

### So dokumentierst du es im Pflichtenheft:

#### Im Kapitel "Systemarchitektur / Netzwerk-Konzept":

##### Deployment-Umgebung

Die Anwendung wird in der bestehenden Docker-Infrastruktur (Portainer) des Schulungszentrums deployed. Diese Umgebung ist aus Sicherheitsgründen ausschließlich aus dem internen Schulungs-WLAN erreichbar und nicht über das öffentliche Internet zugänglich.

##### Netzwerk-Architektur

Die Anwendung besteht aus drei Docker-Containern, die in einem gemeinsamen Docker-Netzwerk kommunizieren:

1. Webserver-Container (php:8.2-apache)
  - Erreichbar über Port 8080 im Schulungs-WLAN
  - Zugriff: `http://[server-ip]:8080`
2. Datenbank-Container (MariaDB)
  - Nur intern über Docker-Netzwerk erreichbar
  - Keine externe Port-Freigabe (Sicherheit!)
3. phpMyAdmin-Container
  - Verwaltungsoberfläche über Port 8081
  - Nur für Administratoren im Schulungs-WLAN

##### Sicherheitskonzept - Netzwerk-Isolation

Die Beschränkung auf das Schulungs-WLAN bietet folgende Sicherheitsvorteile:

- Kein Zugriff aus dem Internet → Schutz vor externen Angriffen
- Datenbank nur intern erreichbar → zusätzliche Sicherheitsebene
- Kontrollierter Nutzerkreis → nur Schulungsteilnehmer
- Vereinfachte Firewall-Konfiguration
- Compliance mit internen IT-Sicherheitsrichtlinien

##### Zugriffsszenario

Besucher im Empfangsbereich verbinden sich mit dem Schulungs-WLAN (Gast-WLAN oder dediziertes Gästebuch-WLAN) und rufen die Anwendung über die

bereitgestellte URL auf. Ein QR-Code am Empfang kann den Zugriff zusätzlich vereinfachen.

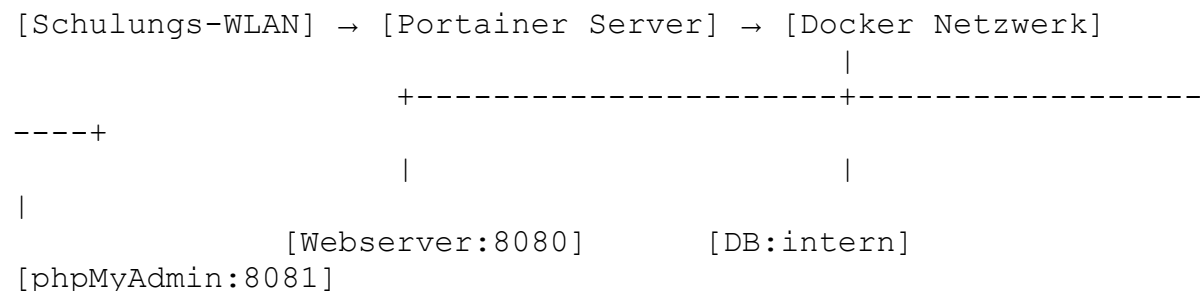
## Vorteile für die IHK-Bewertung

**Diese Einschränkung ist ein PLUS für dein Projekt:**

- ✓ Zeigt Verständnis für Netzwerk-Sicherheit
- ✓ Realistische Unternehmensumgebung (nicht alles ins Internet!)
- ✓ Dokumentiert Rahmenbedingungen professionell
- ✓ Begründet technische Entscheidungen
- ✓ Entspricht Best Practices (Defense in Depth)

### Optional: Netzwerk-Diagramm

Erstelle ein einfaches Diagramm (kann auch mit Paint gemacht werden):



Beschrifte das Diagramm mit:

- Port-Nummern
- Container-Namen
- Zugriffsbeschränkungen ("nur intern", "WLAN-Zugriff")

## Häufige Fragen

**Frage: "Ist das nicht ein Nachteil, dass man nur im WLAN darauf zugreifen kann?"**

Antwort: NEIN! Das ist sogar ein Vorteil. Erkläre es so: "Die Anwendung ist für den internen Gebrauch konzipiert. Eine Internet-Anbindung würde zusätzliche Sicherheitsmaßnahmen (HTTPS, Firewall-Regeln, DDoS-Schutz) erfordern, die für einen Intranet-Service nicht notwendig sind. Dies entspricht dem Prinzip der minimalen Angriffsfläche."

**Frage: "Wie testen Prüfer der IHK die Anwendung?"**

Antwort: Du dokumentierst:

1. Ausführliche Screenshots der laufenden Anwendung
2. Die docker-compose.yml zum Nachbauen
3. Eine Installations-Anleitung
4. Optional: Video-Demo der Funktionen

**Frage: "Soll ich trotzdem über Internet-Deployment schreiben?"**

Antwort: Du kannst optional ein Kapitel "Ausblick / Mögliche Erweiterungen" einfügen:

"Für eine zukünftige Internet-Anbindung wären folgende Anpassungen notwendig: HTTPS-Verschlüsselung, Reverse Proxy (nginx), Rate Limiting, erweiterte Eingabe-Validierung, CAPTCHA gegen Spam."

Das zeigt, dass du weiterdenkst! Aber betone: Das ist nicht Teil des aktuellen Projekts, da Intranet-Betrieb die Anforderung ist.

**Intranet ist nicht "schlechter" - es ist eine bewusste, sichere Entscheidung!**