**Gruppe 3 NWT/ITP**

# **Pflichtenheft**

|  |  |
| --- | --- |
| **Projektbezeichnung** | Gruppe 3 NWT/ITP |
| **Projektleiter** | Julian Halbmayr |
| **Erstellt am** | 09.09.2024 |
| **Letzte Änderung am** | 14.10.2024 |
| **Status** | In Bearbeitung |
| **Aktuelle Version** | 1.2 |

**Änderungsverlauf**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Nr.** | **Datum** | **Version** | **Geänderte Kapitel** | **Art der Änderung** | **Autor** | **Status** |
| 1 | 09.09.2024 | 1.1 | Alles | Inhaltsänderung | Julian Halbmayr | Fertig |
| 2 | 07.10.2024 | 1.2 | Technische Anforderungen / Sicherheitsmaßnahmen | Inhaltsänderung | Julian Halbmayr | Fertig |
| 3 | 20.01.2025 | 1.3 | Zeitplan (Excel) | Überprüfung | Julian Halbmayr | Fertig |
| 4 |  | 1.4 |  |  |  |  |
| 5 |  | 1.5 |  |  |  |  |

Inhalt

[**Pflichtenheft** 1](#_Toc188258632)

[1 Einleitung 4](#_Toc188258633)

[1 Allgemeines 4](#_Toc188258634)

[1.1 Ziel und Zweck des Dokuments 4](#_Toc188258635)

[1.2 Teams und Schnittstellen 4](#_Toc188258636)

[2 Ziele 5](#_Toc188258637)

[2.1 Zentrale Vernetzung der Standorte 5](#_Toc188258638)

[2.2 Sicherer Remote-Zugriff 5](#_Toc188258639)

[2.3 Bereitstellung von Netzwerkdiensten 5](#_Toc188258640)

[2.4 Skalierbarkeit und Zuverlässigkeit 5](#_Toc188258641)

[2.5 Internet-Anbindung und IP-Verwaltung 5](#_Toc188258642)

[2.6 Test- und Produktivsystem 5](#_Toc188258643)

[2.7 Netzwerksicherheit 5](#_Toc188258644)

[3 Funktionale Anforderungen 6](#_Toc188258645)

[4 Nichtfunktionale Anforderungen 6](#_Toc188258646)

[5 Rahmenbedingungen 7](#_Toc188258647)

[5.1 Zeitplan (Excel) 7](#_Toc188258648)

[5.2 Technische Anforderungen 7](#_Toc188258649)

[5.1.1 Hardware 7](#_Toc188258650)

[5.1.2 Server-Hardware 8](#_Toc188258651)

[5.1.3. Netzwerkverkabelung 8](#_Toc188258652)

[5.1.4. Software 8](#_Toc188258653)

[5.1.5 Sicherheitsanforderungen 8](#_Toc188258654)

[6 Arbeitspakete und Verantwortung 9](#_Toc188258655)

[6.1 Projektmanagement und Anforderungsanalyse 9](#_Toc188258656)

[6.2 Netzwerkdesign 9](#_Toc188258657)

[6.3 Testumgebung (Packet Tracer) 9](#_Toc188258658)

[6.4 Sicherheitskonzept (Netzwerkgeräte und Server) 10](#_Toc188258659)

[6.5 Produktivumgebung 10](#_Toc188258660)

[6.6 VPN-Server 10](#_Toc188258661)

[6.7 Tests 10](#_Toc188258662)

[6.8 File Server 11](#_Toc188258663)

[6.9 DNS 11](#_Toc188258664)

[6.10 DHCP 11](#_Toc188258665)

[6.11 Netzwerkgeräte-Konfiguration 11](#_Toc188258666)

[6.12 Datenbankschema konfigurieren 11](#_Toc188258667)

[6.13 Datenbankrelationen konfigurieren 12](#_Toc188258668)

[6.14 Daten für die DB erstellen 12](#_Toc188258669)

[6.15 HTML-Seite erstellen 12](#_Toc188258670)

[6.16 Web Design erstellen 13](#_Toc188258671)

[6.17 JavaScript-Funktionen erstellen 13](#_Toc188258672)

[6.17 Web-Server aufsetzten 13](#_Toc188258673)

[6.18 HTTPS ermöglichen 14](#_Toc188258674)

# Einleitung

*Das vorliegende Projekt befasst sich mit der Planung und Implementierung eines Intranetzwerks für ein Unternehmen mit drei verteilten Standorten. Der Hauptsitz des Unternehmens befindet sich in Salzburg und beherbergt das zentrale Serversystem, das für die Bereitstellung der kritischen Netzwerkdienste verantwortlich ist. Die beiden weiteren Standorte sind über Gigabit-Ethernet-Verbindungen mit der Firmenzentrale vernetzt. Da auch Mitarbeiter von außerhalb, wie z. B. Home-Office-Nutzer, auf das Netzwerk zugreifen müssen, soll ein sicheres VPN-System integriert werden, das verschlüsselten und kontrollierten Zugriff ermöglicht.*

*Neben der Vernetzung der Standorte ist es eine wesentliche Anforderung, mehrere zentrale Dienste sicher und effizient bereitzustellen. Dies umfasst unter anderem einen Webserver, der für den öffentlichen Zugriff über das Internet zur Verfügung steht, sowie interne Server, die unter anderem File-Sharing-Dienste und Datenbankzugriff ermöglichen. Ein besonders hoher Stellenwert wird auf die Sicherheit der Netzwerkinfrastruktur gelegt, um sowohl unautorisierten internen Zugriff als auch Angriffe aus dem Internet abzuwehren. Hierfür ist ein durchdachtes Firewall-Konzept sowie der Einsatz moderner Sicherheitsstandards erforderlich.*

# Allgemeines

## Ziel und Zweck des Dokuments

*Dieses Pflichtenheft beschreibt die technischen Anforderungen und das Design für die Implementierung des Netzwerks sowohl in einer Testumgebung (Packet Tracer) als auch im produktiven Einsatz mit Cisco-Hardware. Das Ziel ist es, eine leistungsfähige, skalierbare und sichere Netzwerklösung zu entwickeln, die den heutigen Anforderungen an Datensicherheit, Verfügbarkeit und Flexibilität gerecht wird. Darüber hinaus wird die Netzwerkinfrastruktur so konzipiert, dass sie zukünftigen Erweiterungen oder Änderungen problemlos standhalten kann.*

## Teams und Schnittstellen

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Rolle(n)** | **Name** | **Telefon** | **E-Mail** | **Gruppe** |
| Projektleiter | Julian Halbmayr |  | julian.halbmayr@htlwy.at | 3 |
| Projektleiter  (Stellvertreter) | Laurenz Berchtold |  | laurenz.berchtold@htlwy.at | 3 |
| Mitarbeiter | Gabriel Deaic |  | gabriel.deaic@htwly.at | 3 |
| Auftraggeber | Andreas Schatz |  | sz.@htlwy.at |  |

# Ziele

## 2.1 Zentrale Vernetzung der Standorte

* *Gigabit-Ethernet-Verbindungen zwischen den drei Standorten sicherstellen.*
* *Zentrale Verwaltung und Bereitstellung von Netzwerkdiensten von der Firmenzentrale (Salzburg) aus.*

## 2.2 Sicherer Remote-Zugriff

* *Bereitstellung eines sicheren VPN-Zugangs für Home-Office-Nutzer, um remote auf das Netzwerk zugreifen zu können.*
* *Firewall- und Sicherheitskonzept zum Schutz vor unerwünschten Zugriffen und Datenverkehr.*

## 2.3 Bereitstellung von Netzwerkdiensten

* *Web-Server für sicheren öffentlichen Zugriff.*
* *VPN-Server für sicheren Zugriff auf das Netzwerk.*
* *File-Server sowohl für öffentliche als auch interne Nutzung.*
* *Datenbank-Server für Zugriff innerhalb des Server-Netzwerks.*
* *DNS- und DHCP-Server für die Verwaltung des Intranets.*
* *SSH-Zugriff für das Inband-Management der Geräte.*

## 2.4 Skalierbarkeit und Zuverlässigkeit

* *Sicherstellung, dass das Netzwerk skalierbar ist, um zukünftiges Wachstum zu unterstützen.*
* *Hohe Verfügbarkeit und Ausfallsicherheit durch redundante Verbindungen und Geräte.*

## 2.5 Internet-Anbindung und IP-Verwaltung

* *Verwendung der vier verfügbaren öffentlichen IP-Adressen effizient verwalten.*
* *Gigabit-Ethernet für den Internet-Zugang über den ISP-Router sicherstellen.*

## 2.6 Test- und Produktivsystem

* *Testimplementierung des Netzwerks im Cisco Packet Tracer zur Überprüfung der Funktionalität.*
* *Produktion des Netzwerks auf Cisco-Hardware für den realen Einsatz.*

## 2.7 Netzwerksicherheit

* *Implementierung einer Firewall zur Abwehr von Bedrohungen aus dem Internet und dem internen Netzwerk.*
* *Sicherstellung, dass alle Systeme sicher konfiguriert sind und regelmäßige Updates erhalten.*

# Funktionale Anforderungen

***Anforderung 1: Zugriff auf Netzwerkdienste***

* ***Web-Server****: Muss sicheren öffentlichen Zugriff ermöglichen.*
* ***VPN-Server****: Muss sicheren Zugriff für Home-Office-User ermöglichen.*
* ***File-Server****: Muss sowohl öffentlichen Zugriff als auch Zugriff aus dem Intranet bieten.*
* ***Datenbank-Server****: Muss nur aus dem Server-Netzwerk zugänglich sein.*
* ***DNS und DHCP-Server****: Muss für das Intranet funktionsfähig sein.*
* ***SSH-Zugang****: Muss für das Management der intermediären Geräte im Intranet verfügbar sein.*

***Anforderung 2: Netzwerkverbindung und Infrastruktur***

* ***Gigabit-Ethernet****: Verbindung zwischen den drei Standorten muss über Gigabit-Ethernet laufen.*
* ***VPN-Zugriff****: Home-Office-User müssen über VPN sicher auf die Firmenzentrale zugreifen können.*
* ***Internet-Zugang****: Die Firmenzentrale muss über den ISP-Router mit vier öffentlichen IP-Adressen Zugang zum Internet haben.*

***Anforderung 3: Sicherheitsmaßnahmen***

* ***Firewall-Konzept****: Muss sowohl unerwünschten Datenverkehr innerhalb des Firmennetzwerks als auch aus dem Internet verhindern.*
* ***Zugriffssteuerung****: Zugang zu verschiedenen Servern muss gemäß den definierten Regeln und Rollen kontrolliert werden.*

# Nichtfunktionale Anforderungen

***Allgemeine Anforderungen***

* ***Verfügbarkeit****: Das Netzwerk und alle Serverdienste müssen rund um die Uhr verfügbar sein.*
* ***Skalierbarkeit****: Die Netzwerkinfrastruktur muss skalierbar sein, um zukünftige Erweiterungen zu ermöglichen.*

***Gesetzliche Anforderungen***

* ***Datenschutz****: Alle Datenübertragungen müssen den geltenden Datenschutzgesetzen entsprechen, insbesondere in Bezug auf die Sicherheit von personenbezogenen Daten.*

***Technische Anforderungen***

* ***Performance****: Die Reaktionszeiten der Serverdienste müssen den Erwartungen entsprechen, z. B. minimale Latenzzeiten bei Web- und File-Servern.*
* ***Wartbarkeit****: Das System muss wartungsfreundlich sein, mit klaren Dokumentationen und einfachen Aktualisierungen.*
* ***Testbarkeit****: Das System muss umfassend in Packet Tracer getestet werden können, um sicherzustellen, dass alle Anforderungen erfüllt sind, bevor es auf Cisco-Hardware umgesetzt wird.*

# Rahmenbedingungen

## Zeitplan (Excel)Ein Bild, das Screenshot, Text, Diagramm, Schrift enthält. Automatisch generierte BeschreibungEin Bild, das Text, Screenshot, Diagramm, Reihe enthält. Automatisch generierte Beschreibung

## Technische Anforderungen

### 5.1.1 Hardware

* Router (Cisco-Hardware):
  + Modell: Router 2901 (Salzburg), Router 2911 (Wels), Router 2911 (Linz)
* Switches (Cisco Catalyst Series):
  + Modell: Switch 2960 (Salzburg), Switch 2960 (Wels), Switch 2960 (Linz)
* ISP-Router:
  + Funktionen: Verbindung zum Internet

### 5.1.2 Server-Hardware

Server für zentrale Dienste (Raspberry Pi):

* + Prozessor: Quad-Core Cortex-A72, 1,5 GHz
  + Speicherkapazität: microSD-Karte (128 GB)
* Server-Funktionen:
  + Web-Server: XAMPP (Apache)
  + VPN-Server: OPEN VPN
  + File-Server: Samba
  + Datenbank-Server: MySQL
  + DNS- und DHCP-Server: BIND9 DNS und ISC-DHCP Server

### 5.1.3. Netzwerkverkabelung

* Gigabit-Ethernet-Kabel (Cat 6a):

### 5.1.4. Software

* Packet Tracer: Cisco Packet Tracer für das Testsystem zur Netzwerksimulation und -analyse.
* Betriebssysteme:
  + Linux (Ubuntu)
* Netzwerkmanagement-Software:
  + SSH-Client (z.B. Tera-Term) für remote Zugriff und Inband-Management der Geräte.
* Firewall-Management-Software:
  + Cisco Firewall

### 5.1.5 Sicherheitsanforderungen

* VPN: IPSec oder SSL-VPN für sichere Verbindungen von Home-Office-Mitarbeitern zur Firmenzentrale.
* Firewall-Regeln: Einrichtung von Regeln zur Überwachung und Steuerung des Datenverkehrs, sowohl intern als auch von externen Quellen.

Ein Bild, das Diagramm, Screenshot, Text, Reihe enthält.

Automatisch generierte BeschreibungEin Bild, das Text, Screenshot, Quittung, Schrift enthält.

Automatisch generierte Beschreibung

# Arbeitspakete und Verantwortung

## 6.1 Projektmanagement und Anforderungsanalyse

**Beschreibung**: Sammlung und Analyse der Anforderungen für das Netzwerk, die Server, Datenbanken, und Webdesign.

**Aufgaben**:

* Analyse der Netzwerk- und Serveranforderungen.
* Ermittlung der Web- und Datenbankanforderungen (HTML, JavaScript, Datenbank).
* Dokumentation der benötigten Technologien und Sicherheitsmaßnahmen.

**Verantwortliche**: Julian Halbmayr

## 6.2 Netzwerkdesign

**Beschreibung**: Ausarbeitung eines detaillierten Netzwerkdesigns (Netzwerkplan, Netzwerkgeräte)

**Aufgaben**:

* Design der Netzwerkstruktur (Subnetze, VLANs, Topologie).
* Auswahl der Netzwerkgeräte.
* Konfiguration der Geräte

**Verantwortliche**: Laurenz Berchtold

## 6.3 Testumgebung (Packet Tracer)

**Beschreibung**: Simulation der geplanten Netzwerkinfrastruktur in Cisco Packet Tracer.

**Aufgaben**:

* Virtuelle Nachbildung des Netzwerks.
* Testen von Firewall-Regeln, VPN-Verbindungen und der Netzwerksicherheit.
* Optimierung des Designs basierend auf Testergebnissen.

**Verantwortliche**: Laurenz Berchtold

## 6.4 Sicherheitskonzept (Netzwerkgeräte und Server)

**Beschreibung**: Erstellung eines umfassenden Sicherheitskonzepts für die Netzwerkinfrastruktur und Server.

**Aufgaben**:

* Konfiguration der Firewall und Sicherheitsregeln.

**Verantwortliche**: Laurenz Berchtold

## 6.5 Produktivumgebung

**Beschreibung**: Implementierung der finalen Netzwerkinfrastruktur auf Cisco-Hardware.

**Aufgaben**:

* Installation der Netzwerkgeräte.
* Konfiguration von VLANs, VPN, Routing und Serverdiensten (DNS, DHCP, File-Server).
* Implementierung der Sicherheitsrichtlinien.

**Verantwortliche**: Laurenz Berchtold, Gabriel Deiac, Julian Halbmayr

## 6.6 VPN-Server

**Beschreibung**: Aufbau und Konfiguration eines VPN-Servers für sichere Remote-Zugriffe.

**Aufgaben**:

* Installation und Konfiguration des VPN-Servers.
* Testen der Verbindungen und Konfiguration der Sicherheitsprotokolle.

**Verantwortliche**: Gabriel Deiac

## 6.7 Tests

**Beschreibung**: Durchführung von Tests und Optimierungen des Netzwerks und der Serverkonfiguration.

**Aufgaben**:

* Überprüfung der Sicherheitsmaßnahmen.
* Performance-Tests der Netzwerk- und Serverdienste.

**Verantwortliche**: Gabriel Deiac

## 6.8 File Server

**Beschreibung**: Implementierung eines File-Servers zur Dateifreigabe innerhalb des Netzwerks.

**Aufgaben**:

* Konfiguration des File-Servers.
* Testen der Dateifreigabe und Zugriffsrechte.

**Verantwortliche**: Julian Halbmayr.

## 6.9 DNS

**Beschreibung**: Implementierung eines DNS-Servers zur Namensauflösung im Netzwerk.

**Aufgaben**:

* Installation und Konfiguration des DNS-Servers.
* Überprüfung und Sicherstellung der Funktionsfähigkeit.

**Verantwortliche**: Julian Halbmayr

## 6.10 DHCP

**Beschreibung**: Einrichtung eines DHCP-Servers zur automatischen IP-Adressvergabe.

**Aufgaben**:

* Konfiguration des DHCP-Servers.
* Test der automatischen IP-Vergabe im Netzwerk.

**Verantwortliche**: Gabriel Deiac

## 6.11 Netzwerkgeräte-Konfiguration

**Beschreibung**: Konfiguration der Netzwerkgeräte (Router, Switches) nach dem finalen Design.

**Aufgaben**:

* Konfiguration der Netzwerkgeräte gemäß dem Design.
* Sicherstellung der korrekten VLAN- und Routing-Einstellungen.

**Verantwortliche**: Laurenz Berchtold.

## 6.12 Datenbankschema konfigurieren

**Beschreibung**: Erstellung und Implementierung des Datenbankschemas für das Projekt.

**Aufgaben**:

* Design und Implementierung des Schemas.
* Definition der Relationen und Constraints.

**Verantwortliche**: Gabriel Deiac.

## 6.13 Datenbankrelationen konfigurieren

**Beschreibung**: Konfiguration der Relationen zwischen den Datenbanktabellen.

**Aufgaben**:

* Definition von Primär- und Fremdschlüsseln.
* Sicherstellen der Datenintegrität und Relationen.

**Verantwortliche**: Gabriel Deiac.

## 6.14 Daten für die DB erstellen

**Beschreibung**: Erstellung und Integration der erforderlichen Daten in die Datenbank.

**Aufgaben**:

* Datenimport und -einfügung.
* Testen der Datenbankabfragen und -integrität.

**Verantwortliche**: Gabriel Deiac.

## 6.15 HTML-Seite erstellen

**Beschreibung**: Erstellung einer benutzerfreundlichen HTML-Seite für den Webauftritt.

**Aufgaben**:

* Design und Entwicklung der HTML-Seite.
* Sicherstellung der responsiven Darstellung.

**Verantwortliche**: Julian Halbmayr.

## 6.16 Web Design erstellen

**Beschreibung**: Design und Umsetzung der Benutzeroberfläche und des Layouts.

**Aufgaben**:

* Entwicklung eines Designs, das zur Marke passt.
* Implementierung von CSS zur Gestaltung.

**Verantwortliche**: Julian Halbmayr.

## 6.17 JavaScript-Funktionen erstellen

**Beschreibung**: Entwicklung von JavaScript-Funktionen für interaktive Features auf der Webseite.

**Aufgaben**:

* Programmierung und Integration von JavaScript-Funktionen.
* Sicherstellen der Benutzerinteraktionen und reibungslosen Funktionalität.

**Verantwortliche**: Julian Halbmayr.

## 6.17 Web-Server aufsetzten

**Beschreibung**: Installation und Konfiguration eines Webservers für die Bereitstellung der HTML-Seiten und Webanwendungen.

**Aufgaben**:

* Auswahl des Webservers (z.B. Apache, Nginx).
* Installation und Konfiguration des Webservers auf einem Server.
* Sicherstellen der Erreichbarkeit der Webanwendungen und HTML-Seiten.
* Konfiguration von Sicherheitsmaßnahmen (z.B. SSL/TLS für HTTPS).

**Verantwortliche**: Julian Halbmayr

## 6.18 HTTPS ermöglichen

**Beschreibung**: Implementierung von HTTPS, um sichere Kommunikation zwischen Clients und dem Webserver zu gewährleisten.

**Aufgaben**:

* **SSL/TLS-Zertifikat auswählen**
* **Zertifikate erstellen und installieren**: Erstellung eines SSL-Zertifikats und Konfiguration auf dem Webserver.
* **HTTPS konfigurieren**: Die Webserver-Konfiguration (Apache) anpassen, um HTTPS-Anfragen zu unterstützen.
* **Automatische HTTP-zu-HTTPS-Weiterleitung einrichten**: Sicherstellen, dass alle HTTP-Anfragen automatisch auf HTTPS umgeleitet werden.
* **Regelmäßige Zertifikatsaktualisierungen sicherstellen**: Automatisierte Tools (z.B. Certbot für Let's Encrypt) verwenden, um Zertifikate regelmäßig zu erneuern.
* **Testen und sicherstellen, dass HTTPS korrekt funktioniert**: Überprüfen der HTTPS-Verbindung und der Gültigkeit des Zertifikats mit Tools wie SSL Labs.

**Verantwortliche**: Julian Halbmayr