Lernfeld:	LF9 Netzwerke und Dienste bereitstellen
Gruppe:	Spannekrebs Sebastian (Group Leader)
Klasse/Kurs	IT21-1

Funktionale Segmentierung von Enterprise IT Netzwerken

Sebastian Spannekrebs

IT 21-1

<< Zum Anfang >>

Lernfeld:	LF9 Netzwerke und Dienste bereitstellen
Gruppe:	Spannekrebs Sebastian (Group Leader)
Klasse/Kurs	IT21-1

Inhaltsverzeichnis:

<< Zum Anfang >>

1. Logischer Netzwerkplan

Version 1:

Es wurde ein Repository unter GitHub, für das Projekt angelegt. Der erstellte Netzwerkplan wurde unter folgendem Link bereitgestellt.
Dokument wurde als Anhang unter Abschnitt 6 eingefügt.

Netzwerkplan (extern)

Version 1.1:

Aktualisierte Fassung (23.11.2022). Hinzugefügt zum Repository und als Anlage zur Bewertungs-Planungs-Phase.
Dokument wurde als Anhang unter Abschnitt 6 eingefügt.

Netzwerkplan (extern)

<< Zum Anfang >>

2. Analyse

2.1 Analyse der zu bereitzustellenden Dienste:

Dienstbezeichnung	Öffentlich erreichbar	Begründung der Entscheidung
Firewall-System	Nein	- System sollte nur intern über den Admin-Rechner konfigurierbar sein. - Anfragen außerhalb des grünen Netzes prüfen und ggf. Datenverkehr blockieren. - Keine Manipulation von außen möglich.
DNS	Nein	- Es sollten nur Netzinterne Komponenten den Dienst abrufen können, ansonsten besteht Manipulationsgefahr der Nummer- bzw. Namensadressenauflösung
DHCP	Nein	- Dynamische Zuweisung der IP-Adressen nur Intern. - Dadurch keine Manipulation der IP-Adressen damit möglich und somit ein Konflikt zu verursachen, der Dienste unerreichbar macht.
Web-Server	Ja	- Stakeholder sollten von außen auf den Webserver zur Darstellung von Informationen zugreifen können. - Manipulation von Daten, nur durch Nutzerauthentifizierung,

<< Zum Anfang >>

		mit einher gehenden Nutzerechten möglich.
Datenbank-Server	Nein	- Sollte nur mit anderen Systemen Netzintern kommunizieren. - Z.B Client <-> Webserver <-> Datenbankserver - Sensible Nutzerdaten müssen geschützt werden nach Richtlinie der DSGVO
[Pi-Hole]	Nein	- Zur Filtrierung des Datenverkehrs von Trackern/Werbetreibende soll der Dienst nur intern administrierbar sein, da dieser den DNS/DHCP-Server ersetzt. Diese sensiblen Systeme sollten nicht von außen einsehbar sein.
[Mailproxy für eingehende Mails]	Ja	- Mail-Proxy sollte als Anlaufpunkt für, von aus dem Internet eingehende Mails verfügbar sein. - Weiterleitung des Datenpaketes an entsprechenden Mailserver - Proxy dient hier zur Verschleierung der Mailserveradresse. - Im Falle eines Angriffes z.B Overflow-anfragen, wird der Mailserver nicht kompromittiert.
[Existierender Mailserver]	Nein	- Mailserver sollte nicht direkt über das Internet erreichbar sein, sondern nur über den Mail-Proxy-Server. - Verschleierung der Mailserver-Adresse - Kein Angriff auf den Mailserver und somit keine Kompromittierung.

<< Zum Anfang >>

2.2 Anwendungsfälle der Akteure:

Akteure	Kommunikationsweg
Ticket erstellen und in DB speichern:	- **Client** -> Internet -> Proxy-Server (Schulnetz) -> DNS-/DHCP-Server (Schulnetz) -> Router (Schulnetz) -> Router (VMnet8/rot) -> FW -> Router (VMnet2/orange/DMZ) -> Webserver -> Router (VMnet2/orange/DMZ) -> **DB**
Administration von: FW: DNS- Server: DHCP-Server:	 - **Admin-Rechne**r (VMNet1/grün) -> Router (VMne1/grün) -> **FW** - **Admin-Rechne**r (VMNet1/grün) -> Router (VMne1/grün) -> FW -> Router (VMnet2/orange/DMZ) -> **DNS-Server** - **Admin-Rechne**r (VMNet1/grün) -> Router (VMne1/grün) -> FW -> Router (VMnet2/orange/DMZ) -> **DHCP-Server**
Administration des Web-Servers:	- **Admin-Rechne**r (VMNet1/grün) -> Router (VMne1/grün) -> FW -> Router (VMnet2/orange/DMZ) -> **Web-Server**
Datenbankabfrage zur Supportsteuerung:	- **Client** (VMNet1/grün) -> Router (VMne1/grün) -> FW -> Router (VMnet2/orange/DMZ) -> Webserver -> Router (VMnet2/orange/DMZ) -> DB **->** Router (VMnet2/orange/DMZ) -> **Webserver**
[Pi-Hole]:	- **Internet** -> Proxy-Server (Schulnetz) -> DNS-/DHCP-Server (Schulnetz) -> Router (Schulnetz) -> Router (VMnet8/rot) -> FW -> Router (VMnet2/orange/DMZ) -> Pi-Hole (DNS-/DHCP-Content-Filterung) -> Router (VMnet2/orange/DMZ) -> FW -> Router (VMne1/grün) -> **Client** (VMNet1/grün)
[Mailkommunikation]:	- **Client (Sender)**(VMNet1/grün) -> Router (VMne1/grün) -> FW -> Router (VMnet2/orange/DMZ) -> Mail-Proxy-

<< Zum Anfang >>

	Server (VMnet2/orange/DMZ) -> **Mail-Server (SMTP)**(VMnet2/orange/DMZ) - **Mail-Server (SMTP)**(VMnet2/orange/DMZ) -> Mail-Proxy-Server (VMnet2/orange/DMZ) -> Router (VMnet2/orange/DMZ) -> FW -> Router (VMnet8/rot) -> Router (Schulnetz) -> Proxy-Server (Schulnetz) -> Internet -> Mail-Proxy-Server (Empfänger) -> **Mailserver (Empfänger)(IMAP/POP3)**

3. Projektplanung

3.1 Analyse des Arbeits- und Projektauftrages

<< Zum Anfang >>

Arbeitsauftrag	Projektauftrag
- Aufbau einer sicheren Netzinfrastruktur - Planung, Implementierung, Tests - Übergabe nach Fertigstellung an Applikation-Projektteam (Betriebsintern)	- Aufbau der Netzinfrastruktur - Sicherstellung der Systemerreichbarkeit - Dienstverfügbarkeit einer Supportinfrastruktur - Erreichbarkeit aus dem Internet - Starttermin: UW-3 - Abgabe: UW-8 - Zeitumfang (72h)

3.2 Pflichtenheft

PFLICHTENHEFT (Grob- & Feinkonzept)

<< Zum Anfang >>

Auftraggeber	Doubtful-Joy SE
Zweck des Projektes	Segmentierung der Netzinfrastruktur für die aufzubauende Support-Lösung und Erweiterung des Ökosystems um eine weitere Komponente in Form eines Ticketsystems.
Analyse der Ausgangssituation	Bereits existierende Supportinfrastruktur via Mails und Telefon. Bis zu 100 Tickets pro Tag, Tendenz stark steigend (100%), erfordert eine Entlastung des Supports mithilfe eines Ticketsystems. Es wird eine Segmentierung der Infrastruktur gefordert. Dienste sollen strikt von öffentlich Erreichbar, zu intern Erreichbar getrennt werden. Es besteht eine klare Vorstellung der System-Strategie hinsichtlich der Server-Betriebssysteme. Begründete Empfehlungen/Beratungen zur technischen Bereitstellung der IT-Infrastruktur sowie zukunftssicheren Systembetrieb garantieren nach der Devise „make or buy“:
Funktionsspezifikation	<u>Anlegen eines Tickets durch Mitarbeiter:</u> Mitarbeiter-Clients befinden sich nach dem Netzwerkplan im gesicherten Intranet(grün/VMnet1). Das Anlegen eines Tickets erfolgt über den Webbrowser (Darstellungsschicht). Die Einträge werden vom Webserver (Applikationsschicht) an den Datenbankserver (Data-Source) weitergegeben und festgehalten. Das Abrufen erfolgt mit Eingabe der Ticket-ID/Kunde/Nutzer (durch Kontaktdaten). Mitarbeiter kann Tickets anlegen, bearbeiten und löschen oder schließen <u>Anlegen eines Tickets durch User/Kunde:</u> Der Kunde/User kann über die Internetseite der Firma „Doubful-Joy“ ein Support-Ticket eröffnen. Kontaktdaten (z.B E-Mailadresse) sind Pflicht, sowie Kurzbeschreibung des Problems. Über Die Darstellungsschicht->Applikationsschicht->Data-Source wird ein Ticket angelegt. Wurde ein Ticket angelegt, erfolgt eine Benachrichtigung, welche vom Support-Mitarbeiter abgerufen werden kann. Der User/Kunde kann ein Ticket anlegen. Löschen oder bearbeiten ist nur durch einen Mitarbeiter der Doubtful-Joy möglich.

Datenspezifikation	Ticket:
	- Attribute:
	  ○ Ticket-ID
	  ○ User/Kunden – ID (ID oder Benutzername etc.)
	  ○ User/Kunden – Vorname
	  ○ User/Kunden - Name

<< Zum Anfang >>

<table>
<tr><td></td><td></td><td>

User/Kunden – E-Mailadresse
User/Kunden - Vorname
Dropdown Auswahl (Problemeingrenzung-Bereich)
Dropdown Auswahl (Problemeingrenzung)
Dropdown Auswahl (Problemeingrenzung)
Textfeld: (Fehlercode eintragen, der ausgelöst wurde (optional))
Textfeld – Umschreibung des Problems (wenn in der Dropdown Auswahl „Sonstiges“ ausgewählt wurde, wird die Fläche freigeschaltet)

- Bei Versand des Tickets erhält der Nutzer/Kunde, eine Kopie des Tickets als Nachweis per E-Mail.

<u>SPEICHERUNG:</u>

<u>Datenbankeinträge:</u>
- Ticket-ID
- Kunde/User
- Kundenkontakt/Userkontakt
- Ticketprotokoll
- <u>Ticketprotokolle:</u>
○ Vorgangsnummer
○ Priorität
○ Fehlerbewertung (Kritisch/Hoch/Mittel/Gering)
○ Bearbeitungsverlauf (Datum/Uhrzeit/zuständiger Mitarbeiter)
- Geschlossene oder gelöschte Tickets werden in einer separaten Datenbank archiviert
- Backup der Datenbanken zur Sicherung

<u>Webserver:</u>

- Umstellung des Clients & Backend durch Module, Services, Komponenten
- Backup der Daten

<u>DATENFLUSS:</u>
- Mitarbeiter mit internen Datenaustausch zum Webserver/Datenbankserver/Mailserver zum Anlegen, Bearbeiten oder Löschen bzw. schließen eines Tickets
- Anlegen eines Tickets durch den Nutzer/Kunden (Attribute siehe Datenbankeinträge)
</td></tr>
<tr><td>Schnittstellenspezifikation</td><td></td><td>GUI - User/Kunde:
- Ausfüllen der Felder und über Button absenden

GUI – Mitarbeiter:</td></tr>
</table>

<< Zum Anfang >>

		- Abrufen der Tickets,-bearbeiten,-löschen,-schließen(archivieren) GUI – Administrator: - Gleiche Rechte wie Mitarbeiter, zusätzlich archivierte Einträge wieder aufrufen und Datensammlungen aus archivierten Tickets für Forecast und Kennzahlenerfassung. - Wartung über Terminal/Shell
Rahmenbedingungen		Software: - Eigenständige Dienstauswahl - VMware-Player - VMs Räumlichkeiten: - BSZ Elektrotechnik Dresden - Remote Hardware: - Schul-PCs oder vergleichbare Ausstattung wird bereitgestellt Dokumente: - Vorlagen siehe Lernsax Projektordner LF9
Qualitätsbetrachtung		Einteilung der Arbeitspakete und Verantwortlichkeiten führen zur genauen Dokumentation der Arbeitsabläufe und des Arbeitsstandes. Protokollierung der Prozesse und Life-Präsentation der Prototypen und schlussendlich des fertiggestellten Projektes durch eine Abnahme. Exakte Terminvorgaben der einzelnen Arbeitsschritte zeigen Zwischenstände und dadurch den Fortschritt des Projektes. Jegliche Projektentwicklung werden in GitHub-Branches protokolliert und können somit nachvollzogen werden.

Realisierungsvorschlag		<u>Analyse und Projektplanung:</u>
		
		- bis 25.11.2022 (UW-4)
		
		<u>Entscheiden und Durchführen Teil 1</u>:
		
		- Abgabe:
		  ○ Bis 23.12.2022
		- Life-Präsentation:
		  ○ Bis 03.02.2023

<< Zum Anfang >>

		Entscheiden und Durchführen Teil 2(Auswertung und Reflektion):
		- Abgabe:
		  ○ Bis 10.02.2023
		- Life-Präsentation und Auswertung:
		  ○ 27.03.2023 bis 05.04.2023

Projektplanung		Das Projekt lässt sich in dem geforderten Rahmen umsetzen. Bedenken gibt es nur hinsichtlich der Arbeitsverteilung/Arbeitspakete der Gruppenmitglieder. Da es nur eine Person umsetzen wird.
Kosten-Nutzen-Analyse		Kosten-Nutzen-Analyse wird nachgereicht. Es wird durch Betriebsinterne Stellen bearbeitet.

<< Zum Anfang >>

3.3 Projektstrukturplan:

Version 1:

Projektstrukturplan erstellt.
Dokument wurde als Anhang unter Abschnitt 6 eingefügt.

Projektstrukturplan (extern)

<< Zum Anfang >>

3.4 Gantt-Diagramm

Version 1:

Gantt-Diagramm erstellt.
Dokument wurde als Anhang unter Abschnitt 6 eingefügt.

Gantt-Diagramm (extern)

<< Zum Anfang >>

4. Durchführen

- Siehe Virtuelle Maschinen

<< Zum Anfang >>

5. Auswertung und Reflexion

1: DNS/DHCP-Server

1.1. Installation und Konfiguration des DHCP-Servers
1.2. Installation und Konfiguration des DNS-Servers

2: Webserver

2.1. Installation des Webservers unter Apache
2.2. Installation der Programmiersprache PHP und der Datenbank MySQL
2.3. Konfiguration der Programmiersprache und der Datenbank

3: Firewall

3.1. Konfiguration der Firewall IPFire
3.2. Definition und Begründung der Regeln für den DNS/DHCP-Server, Webserver und die Datenbank

4. SOLL – IST Vergleich (Ergebnis und Zeitaufwand)

4.1 Benennung von Defiziten zur Sicherheit der Lösung
4.2 Optimierungsvorschläge

<< Zum Anfang >>

1: DNS/DHCP-Server

1.1 Installation und Konfiguration des DHCP-Servers

Voraussetzung für VM:

CPU: 1 vCore
RAM: 1024 MB
HDD: 5 GB
Lan-Adapter : RJ45 1000 MB/s
Eingebunden in: 192.168.25.0
root-Anmeldung: Benutzername: “root“, Passwort: „telekinese“

Ziel :

Es soll ein DHCP Server auf einem CentOS 9.x System installiert werden. Es sollen folgende Netze mit eingebunden werden. Die IP-Adressen sollen automatisch an die Endgeräte verteilt werden können. Alle Endgeräte sind in der gleichen Domain.

Schritt 1: Installation des dhcpd-Pakets:

- Geben sie folgende Zeile im Terminal ein

```
sudo yum install dhcpd
```

Schritt 2: Konfiguration des DHCP-Servers:

- Öffnen Sie die Konfigurationsdatei mit folgendem Befehl:

```
sudo vi /etc/dhcp/dhcpd.conf
```

<< Zum Anfang >>

- fügen Sie in die Datei folgende Zeilen am Ender der Datei ein, um das Netzwerk 192.168.25.0 und 192.168.125.0 zu konfigurieren:

```
subnet 192.168.25.0 netmask 255.255.255.0 {
  range 192.168.25.10 192.168.25.50;
  option routers 192.168.25.2;
  option domain-name-servers 192.168.25.4;
  option domain-name "doubtful-joy25.com";
}
subnet 192.168.125.0 netmask 255.255.255.0 {
  range 192.168.125.10 192.168.125.50;
  option routers 192.168.125.2;
  option domain-name-servers 192.168.25.4;
  option domain-name "doubtful-joy125.com";
}
```

Schritt 3: Starten des DHCP-Servers

- Um den DHCP-Server zu starten, geben sie folgenden Befehl ein:

```
sudo systemctl start dhcpd
```

- Um den Status des Servers zu prüfen geben Sie folgenden Befehl ein:

```
sudo systemctl status dhcpd
```

Stellen Sie sicher, dass der DHCP-Server ausgeführt wird und keine Fehler aufweist.

<< Zum Anfang >>

Schritt 4: Automatisches Starten des DHCP-Server beim Systemstart

- Damit der Server automatisch bei jedem Systemstart hochfährt, geben Sie folgenden Befehl ein:

```
sudo systemctl enable dhcpd
```

Die Installation und Konfiguration ist hiermit abgeschlossen. Der Server verteilt nun IP-Adressen an alle Geräte in den Netzwerken.

1.2 Installation und Konfiguration des DNS-Servers

Vorraussetzungen:

root-Anmeldung: Benutzername: “root“, Passwort: „telekinese
(Der DNS – Server wird auf der gleichen Maschiene wie der DHCP – Server installiert)

Ziel:

Es soll ein DNS Server im GreenNet installiert werden. Dieser Service löst Namen und IP-Adressen zueinander auf und weist diese zueinander zu. Alle Endgeräte werden mit der IP-Adresse oder dessen Hostnamen ansprechbar und abrufbar sein.

Schritt 1: Installation des DNS – Servers

- Mit dem folgenden Befehl, laden sie das Paket herunter und installieren den DNS-Server

```
```

<< Zum Anfang >>

```
sudo yum install bind bind-utils
```

Schritt 2: Konfiguration des DNS-Servers

- Öffnen Sie mit dem folgenden Befehl die Datei im Editor

```
sudo vi /etc/named.conf
```

- Kommentieren Sie folgende Zeile aus

```
#listen-on-v6 { any; };
```

- Die folgenden Zeilen werden unter die auskommentierte Zeile hinzugefügt. Es erlaubt interne und externe Anfragen auf den DNS-Server

```
listen-on port 53 { 127.0.0.1; 192.168.25.4;};
allow-query { any ; } ;
allow-query-cache { any; };
allow-recursion { localhost; 192.168.25.0/24; };
```

<< Zum Anfang >>

- Am Ende der Datei soll folgende Anweisung hinzugefügt werden. Die erlaubt die modulare unterteilung der Zonen und die Zonenauflösung der Endgeräte.

```
zone "doubtful-joy25.com" {
  type master;
  file "/etc/named/doubtful-joy25.com.zone";
};

zone "25.168.192.in-addr.arpa" {
  type master;
  file "/etc/named/25.168.192.in-addr.arpa.zone";
};

zone "125.168.192.in-addr.arpa" {
  type master;
  file "/etc/named/125.168.192.in-addr.arpa.zone";
};
```

Schritt 3. Konfiguration der Forward-Zone

- Öffnen Sie die Datei im Texteditor

```
sudo vi /etc/named/doubtful-joy25.com.zone
```

- Sollte die Datei nicht vorhanden sein, geben Sie folgenden Befehl ein

```
```

<< Zum Anfang >>

```
sudo touch /etc/named/doubtful-joy25.com.zone
sudo vi /etc/named/doubtful-joy25.com.zone
```

- Fügen Sie folgenden Eintrag hinzu. Dieser Teil löst die IP Adressen in Hostnamen auf.

```
$TTL 86400
@     IN SOA    DNSDHCP.doubtful-joy25.com. root.doubtful-joy25.com. (
            2022041201
            3600
            1800
            604800
            86400 )
   IN NS     DNSDHCP.doubtful-joy25.com.
   IN A      192.168.25.4
   IN A      192.168.25.2
   IN PTR    firewall.doubtful-joy25.com.
   IN A      192.168.25.3
   IN PTR    adminrechner.doubtful-joy25.com.
   IN A      192.168.25.5
   IN PTR    dbserver.doubtful-joy25.com.
   IN A      192.168.125.3
   IN PTR    webserver.doubtful-joy25.com.
```

- Speichern Sie die Datei und schließen den Editor.

Schritt 4. Konfiguration der Reverse-Zone

- Diese Konfiguration erlaubt wes nun in der umgekehrten Variante die Hostnamen in IP Adressen aufzulösen. Dabei werden einzelne Zonen in separate Dateien gespeichert.
- Öffnen Sie mit diesem Befehl die Datei für die GreenNet-Reverse-Zone

```
```

<< Zum Anfang >>

```
sudo vi /etc/named/25.168.192.in-addr.arpa.zone
```

- Sollte die Datei nicht vorhanden sein geben Sie diesen Befehl ein

```
sudo touch /etc/named/25.168.192.in-addr.arpa.zone
sudo vi /etc/named/25.168.192.in-addr.arpa.zone
```

- Fügen Sie folgenden Block in die Datei ein um die Reverse-Zone für das GreenNet zu konfigurieren.

```
$TTL 86400
@     IN SOA    DNSDHCP.doubtful-joy25.com. root.doubtful-joy25.com. (
            2022041201
            3600
            1800
            604800
            86400 )
   IN NS     DNSDHCP.doubtful-joy25.com.
   IN PTR    DNSDHCP.doubtful-joy25.com.
   IN PTR    firewall.doubtful-joy25.com.
   IN PTR    adminrechner.doubtful-joy25.com.
   IN PTR    dbserver.doubtful-joy25.com.
   IN PTR    webserver.doubtful-joy25.com.
```

- Speichern und schließen Sie die Datei anschließend.

Schritt 5: Konfiguration der Reverse-Zone für DMZ (OrangeNet)

- Öffnen Sie folgende Datei im Text-Editor

<< Zum Anfang >>

```
sudo vi /etc/named/125.168.192.in-addr.arpa.zone
```

- Sollte die Datei nicht vorhanden sein, führen sie bitte folgende Befehle aus.

```
sudo touch /etc/named/125.168.192.in-addr.arpa.zone
sudo vi /etc/named/125.168.192.in-addr.arpa.zone
```

- Fügen Sie zu guter Letzt den Textblock in die Textdatei ein.

```
$TTL 86400
@     IN SOA    DNSDHCP.doubtful-joy25.com. root.doubtful-joy25.com. (
            2022041201
            3600
            1800
            604800
            86400 )
   IN NS     DNSDHCP.doubtful-joy25.com.
   IN PTR    DNSDHCP.doubtful-joy25.com.
   IN PTR    webserver.doubtful-joy25.com.
```

- Speichern und schließen Sie die Datei

Schritt 6: Firewall-Konfiguration

- Um den Datenverkehr von den anfragenden Endgeräten aus dem Netzen zum DNS Server zu gewähren, müssen die Firewallregeln der DNSDHCP-VM angepasst werden. Aus diesem Grund, öffnen Sie die Datei:

```
sudo vi /etc/sysconfig/iptables
```

<< Zum Anfang >>

- Fügen Sie nun folgende Zeilen hinzu.

```
-A INPUT -s 192.168.25.0/24 -m state --state NEW -p udp --dport 53 -j ACCEPT
-A INPUT -s 192.168.25.0/24 -m state --state NEW -p tcp --dport 53 -j ACCEPT
-A INPUT -s 192.168.125.0/24 -m state --state NEW -p udp --dport 53 -j ACCEPT
-A INPUT -s 192.168.125.0/24 -m state --state NEW -p tcp --dport 53 -j ACCEPT
```

- Speichern und schließen Sie die Datei
- Starten Sie nun die Firewall neu, um die Änderungen zu übernehmen

```
sudo systemctl restart iptables
```

Schritt 7: DNS-Server starten und Autostart einschalten

- Um den DNS-Server bei einem Systemstart automatisch zu laden geben Sie folgende Befehlszeile ein.

```
sudo systemctl enable named
```

- Schlussendlich soll der Server noch gestartet werden

<< Zum Anfang >>

```
sudo systemctl restart named
```

Wenn keine Fehlermeldung angezeigt wurden, ist die Konfiguration des DNS-Server unter Bind9 abgeschlossen und der Server ist für Sie nun einsatzbereit.

2: Webserver

2.1 Installation und Konfiguration Webservers unter Apache

Voraussetzung für VM:

CPU: 1 vCore
RAM: 1024 MB
HDD: 5 GB
Lan-Adapter : RJ45 1000 MB/s
Eingebunden in: 192.168.25.0
root-Anmeldung: Benutzername: “root“, Passwort: „telekinese“

Ziel :

Es soll ein Webserver mit dem Apache Package installiert und konfiguriert werden. Er soll als standalone server seinen Dienst verrichten. Der Webserver wird auf das OS: CentOS 9.x aufgesetzt.

<< Zum Anfang >>

Schritt 1: **Installation von Apache**

- Um das Package des Apache-Webservers herunterzuladen und zu installieren benötigen sie folgende Anweisungen:

```
sudo yum install httpd
```

- Sobald der Download beendet, Sie der Installation des Webservers zugestimmt haben und dieser installiert wurde, müssen zunächst die Firewall-Regeln des Webservers angepasst werden um den Datenverkehr zu gewährleisten.
- Geben Sie nun folgende Befehle ein:

```
sudo firewall-cmd --zone=public --add-port=80/tcp --permanent
sudo firewall-cmd --reload
```

Sie haben Erfolgreich den Apache Webserver auf ihrer Maschiene installiert. Zum Testen, rufen Sie im Browser ihrer wahl den Webserver über die IP-Adresse der VM auf, oder direkt über den Hostname in der Browser Suchleiste.

2.2 Installation von PHP und MySQL

Schritt 1: **Installation von PHP (Datenbankserver und Webserver**)

- Führen Sie folgenden Befehl aus um die neuste PHP Version zu installieren. Sollten Sie diesen Installationsschritt bereits in der Vergangenheit gemacht haben können Sie mit diesem Befehlssatz auch eine Aktualisierung auf beiden Servern vornehmen.

<< Zum Anfang >>

```
sudo apt-get update
sudo apt-get install -y software-properties-common
sudo add-apt-repository ppa:ondrej/php
sudo apt-get update
sudo apt-get install -y php
```

- Mit dem nachfolgendem Befehl, können Sie die installierte Version überprüfen.

```
php -v
```

Die Einrichtung von PHP ist nun abgeschlossen. Sie können entweder beide Server einem optionalen reboot unterziehen, oder mit dem nächsten Schritt fortfahren.

Schritt 2: Installation von MySQL (Datenbankserver)

- Beginnen Sie mit folgendem Befehlssatz um den MySQL Server herunterzuladen und zu installieren. Eventuelle Systemupdates/Updates sollten mitgenommen werden.

```
sudo apt-get update
sudo apt-get install -y mysql-server
```

- Für der Start und den automatischen Start des MySQL Servers , verwenden Sie folgende Befehle:

```
sudo systemctl start mysql
```

<< Zum Anfang >>

```
sudo systemctl enable mysql
```

Die MySQL Installation für den Datenbankserver ist hiermit abgeschlossen.

Schritt 3 : Installation des MySQL – Clients (Webserver)

- Starten Sie die Installtaion des Clients auf dem Webserver mit folgenden Befehlen:

```
sudo apt-get update
sudo apt-get install -y mysql-client
```

Damit ist die Installation auf dem Webserver abgeschlossen und im nächsten Schritt geht es um die Konfiguration der beiden Server um eine Verbindung herzustellen.

Schritt 4: Verbinden und Konfigurieren des Webservers mit der Datenbank

- Auf dem Datenbankserver führen Sie folgenden Befehl aus, um sich in MySQL einzuloggen.

```
sudo mysql -u root -p
```

- Angemeldet, geben Sie folgende Befehle nacheinander ein, um die Datenbank einzurichten

<< Zum Anfang >>

```
CREATE DATABASE ticketsystem;

USE ticketsystem;

CREATE TABLE tickets (
   id INT AUTO_INCREMENT PRIMARY KEY,
   name VARCHAR(255) NOT NULL,
   email VARCHAR(255) NOT NULL,
   subject VARCHAR(255) NOT NULL,
   message TEXT NOT NULL
);

CREATE USER 'webserver'@'%' IDENTIFIED BY 'telekinese';

GRANT ALL PRIVILEGES ON ticketsystem.tickets TO 'webserver'@'%';

FLUSH PRIVILEGES;

EXIT;
```

Sie haben nun die Datenbank erstellt und können mit den Festgelegten Konfigurationen ihren Datenbankserver modifizieren.

3. Firewall

3.1 . Definition und Begründung der Regeln für den DNS/DHCP-Server, Webserver und die Datenbank

<< Zum Anfang >>

- Im folgenden Screenshots sind die notwendigsten Firewallregeln angegeben, um eine Kommunikation auf ein mindestmaß zu begrenzen. Insofern dient dies zur optimierung des Sicherheitsaspektes, dass nur die notwendigsten ports an die notwendigsten protokolle geöffnet wurden.

Firewallregeln

#	Protokoll:	Quelle	Log	Ziel	Aktion
1	TCP	ROT	☑	Firewall : 443 ->192.168.125.3: HTTPS	☑
2	TCP	ROT	☑	Firewall : 80 ->192.168.125.3: HTTP	☑
3	TCP	192.168.125.3	☑	192.168.25.5: 3306	☑
4	TCP, UDP	192.168.125.3	☑	192.168.25.4: DNS	☑

GRÜN ORANGE	Internet (Zugelassen) Internet (Zugelassen)	ORANGE (Zugelassen) GRÜN (Blockiert)

Richtlinie: Zugelassen

Begründung

Firewallregel	Begründung
#1 und #2	- Um Zugang zu dem Webserver aus externen Netzen zu bekommen um das Ticketsystem zu nutzen werden die Kommunikationsprotokolle http(Port 80) und https(443) zur DMZ hin geöffnet. Dies reicht um Webseiten zum Klienten darzustellen und nutzbar zu machen
#3	- Die Kommunikation vom Webserver zum Datenbank-Server ist nur auf das Protokoll TCP zur Übertragung beschränkt, da MySQL Kommunikation meist über dieses Protokoll läuft. Der angegeben Port ist der Standardport zur MySQL Befehlsübertragung
#4	- Die Freischlatung dieses Kommunikationsweges gewährleistet die Namens- und Adressauflösung für

<< Zum Anfang >>

	den DNS-Server zum Webserver über den port 53. Die Standardprotokolle sind TCP oder UDP. Der Webserver kann somit intern über webserver.doubtful-joy25.com aufgerufen werden.

4. SOLL- IST -Vergleich: Ergebnis und Zeitaufwand

Soll-Zeitaufwand	Ist-Zeitaufwand	Soll-Ergebnis	Ist-Ergebnis
- 0.5 PT - 0.5 PT - 1 PT - 2 PT - 10 min	- 1 PT - 1 PT - 1 PT - 2 PT - 30 min	- Inbetriebnahme des Datenbankservers - Inbetriebnahme des Webservers - Nutzereinstellungen auf DB-Server und Web-Server - Software installieren und Konfigurieren - Anpassen der Firewall	- Datenbankserver in Betrieb - Webserver in Betrieb - Nutzer Angelegt und Datenbank mit Table eingerichtet - Software installiert nach Vorgabe - Firewall angepasst

Begründung:

- Aufgrund von Unerfahrenheit und Komplikationen in der Kommunikation der Server, mussten beide Server anfangs neu aufgesetzt werden. Das gewünschte Ergebnis bei der Inbetriebnahme wurde Erreicht, jedoch unter doppelt so hohem Zeitaufwand.
- Die Festgelegte Projektzeit von Rund 4 PT zur Durchführung musste daher auf rund 1 PT verlängert werden um das gewünschte Ergebnis zu erhalten.

<< Zum Anfang >>

4.1 Aufälligkeiten von Defiziten bezüglich der Sicherheit

1. Es Existiert keine TLS oder SSL Zertifizierung.

   - Das System ist nicht sicher in der Kommunikation über bestimmte Protokolle z.B. http (port: 80)

   - **L Lösung/Optimierungsvorschlag**
     Eine SSL-Zertifizierung des Servers zur Echtheitsbestätigung des Endknotens kann die Sicherheit in diesem Punkt erhöhen. Durch openssl lässt sich ein Zertifikat, selbst signiert erstellen und auf dem Webserver integrieren

2. Es Existiert kein Sicherheitsassisten für die MySQL Datenbank.

   - Evenetuelle Attacken auf den Datenbankserver können nicht abgewehrt werden. Mögliches Sicherheitsrisiko der Kundendaten

   - **Lösung/Optimierungsvorschlag**
     Die erweiterte Instalaltion eines Sicherheitsassistenten könnte Abhilfe verschaffen. Mit der Installationsanweisung auf dem Datenbankserver:

     ```
     sudo mysql_secure_installation
     ```

     Könnte das Risiko , Zugriff auf sensible Kundendaten zu bekommen miniert werden.-

3. Token-Anmeldeverfahren löst unsichere Kennwörter ab

   - Alle vergeben Kennwörter sind leicht zu korrumpieren und bieten eine offene Tür für Angreifer.

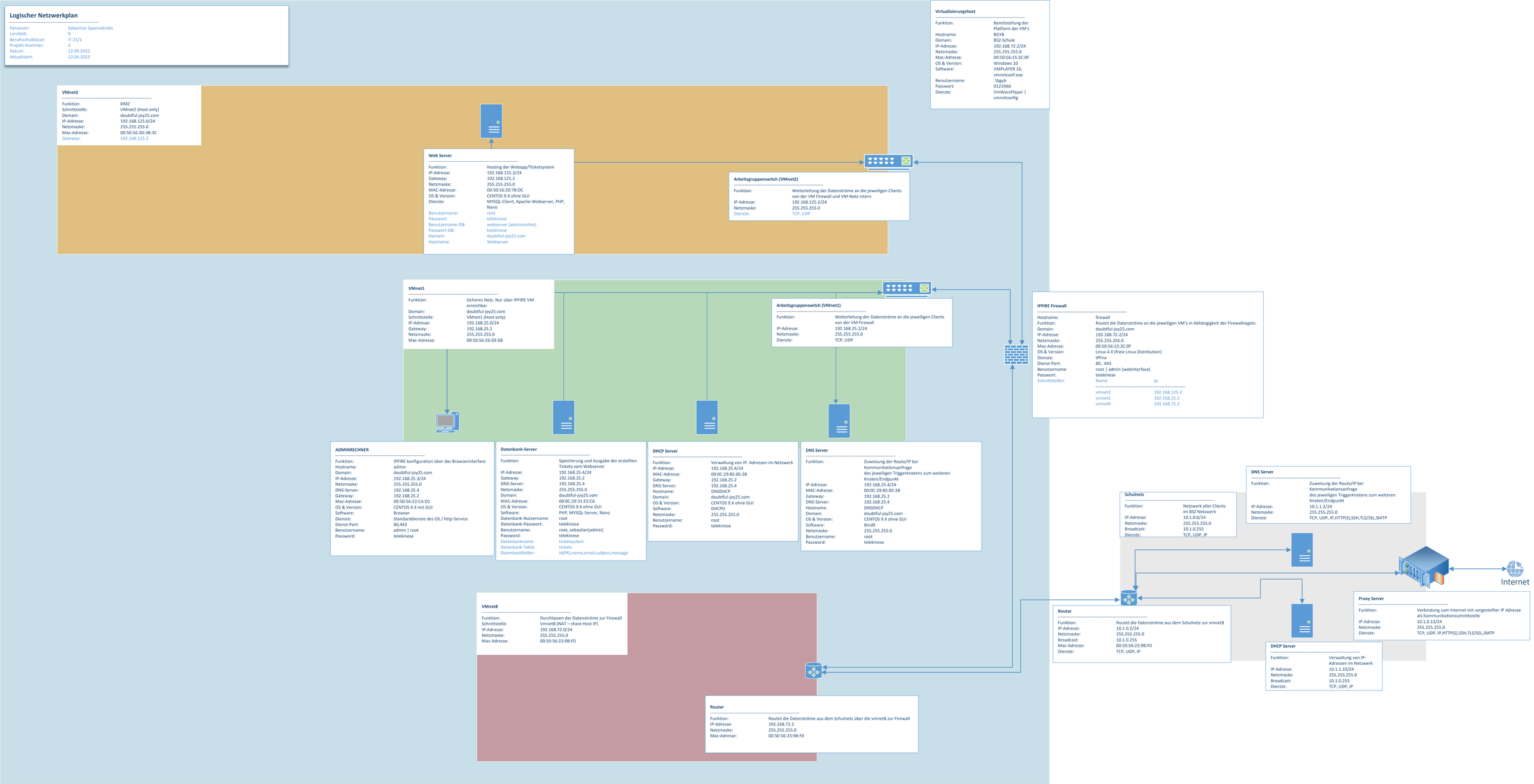
   - **Lösung/Optimierungsvorschlag:**
     Um das System maximal sicher zu gestalte, könnte eine zwei-Faktor-Autenthisierung oder durch Anmelde-Schlüssel/Token eines jeden Nutzers

<< Zum Anfang >>

6. Dokumentenanhänge

Im folgenden Verlauf sind alle geforderten Dokumente angehängt.

<< Zum Anfang >>


Logischer Netzwerkplan
Personen: Sebastian Spannekrebs
Lernfeld: 9
Berufsschulklasse: IT 21/1
Projekt-Nummer: 3
Datum: 12.09.2022
Aktualisiert: 12.04.2023
Virtualisierungshost
Funktion: Bereitstellung der Platform der VM's
Hostname: BGYB
Domain: BSZ-Schule
IP-Adresse: 192.168.72.2/24
Netzmaske: 255.255.255.0
Mac-Adresse: 00:50:56:15:3C:0F
OS & Version: Windows 10
Software: VMPLAYER 16, vmnetconf.exe
Benutzername: .\bgyb
Passwort: 01219dd
Dienste: VmWarePlayer | vmnetconfig
VMnet2
Funktion: DMZ
Schnittstelle: VMnet2 (Host-only)
Domain: doubtful-joy25.com
IP-Adresse: 192.168.125.0/24
Netzmaske: 255.255.255.0
Mac-Adresse: 00:50:56:3D:38:3C
Gateway: 192.168.125.2
Web Server
Funktion: Hosting der Webapp/Ticketsystem
IP-Adresse: 192.168.125.3/24
Gateway: 192.168.125.2
Netzmaske: 255.255.255.0
MAC-Adresse: 00:50:56:20:7B:DC
OS & Version: CENTOS 9.X ohne GUI
Dienste: MYSQL-Client, Apache-Webserver, PHP, Nano
Benutzername: root
Passwort: telekinese
Benutzername-DB: webserver (adminrechte)
Passwort-DB: telekinese
Domain: doubtful-joy25.com
Hostname: Webserver
Arbeitsgruppenswitch (VMnet2)
Funktion: Weiterleitung der Datenströme an die jeweiligen Clients von der VM Firewall und VM-Netz intern
IP-Adresse: 192.168.125.2/24
Netzmaske: 255.255.255.0
Dienste: TCP, UDP
VMnet1
Funktion: Sicheres Netz. Nur über IPFIRE VM erreichbar
Domain: doubtful-joy25.com
Schnittstelle: VMnet1 (Host-only)
IP-Adresse: 192.168.25.0/24
Gateway: 192.168.25.2
Netzmaske: 255.255.255.0
Mac-Adresse: 00:50:56:26:DE:68
Arbeitsgruppenswitch (VMnet1)
Funktion: Weiterleitung der Datenströme an die jeweiligen Clients von der VM Firewall
IP-Adresse: 192.168.25.2/24
Netzmaske: 255.255.255.0
Dienste: TCP, UDP
IPFIRE Firewall
Hostname: firewall
Funktion: Routet die Datenströme an die jeweiligen VM's in Abhängigkeit der Firewallregeln.
Domain: doubtful-joy25.com
IP-Adresse: 192.168.72.2/24
Netzmaske: 255.255.255.0
Mac-Adresse: 00:50:56:15:3C:0F
OS & Version: Linux 4.X (freie Linux Distribution)
Dienste: IPFire
Dienst-Port: 80 , 443
Benutzername: root | admin (webinterface)
Passwort: telekinese
Schnittstellen:
Name: ip:
vmnet2 192.168.125.2
vmnet1 192.168.25.2
vmnet8 192.168.72.2
ADMINRECHNER
Funktion: IPFIRE konfiguration über das Browserinterface
Hostname: admin
Domain: doubtful-joy25.com
IP-Adresse: 192.168.25.3/24
Netzmaske: 255.255.255.0
DNS-Server: 192.168.25.4
Gateway: 192.168.25.2
Mac-Adresse: 00:50:56:22:CA:D1
OS & Version: CENTOS 9.X mit GUI
Software: Browser
Dienste: Standarddienste des OS / http-Service
Dienst-Port: 80,443
Benutzername: admin | root
Password: telekinese
Datenbank-Server
Funktion: Speicherung und Ausgabe der erstellten Tickets vom Webserver
IP-Adresse: 192.168.25.4/24
Gateway: 192.168.25.2
DNS-Server: 192.168.25.4
Netzmaske: 255.255.255.0
Domain: doubtful-joy25.com
MAC-Adresse: 00:0C:29:31:E5:C6
OS & Version: CENTOS 9.X ohne GUI
Software: PHP, MYSQL-Server, Nano
Datenbank-Nutzername: root
Datenbank-Passwort: telekinese
Benutzername: root, sebastian(admin)
Password: telekinese
Datenbankname: ticketsystem
Datenbank-Table: tickets
Datenbankfelder: id(PK),name,email,subject,message
DHCP Server
Funktion: Verwaltung von IP- Adressen im Netzwerk
IP-Adresse: 192.168.25.4/24
MAC-Adresse: 00:0C:29:B5:85:3B
Gateway: 192.168.25.2
DNS-Server: 192.168.25.4
Hostname: DNSDHCP
Domain: doubtful-joy25.com
OS & Version: CENTOS 9.X ohne GUI
Software: DHCPD
Netzmaske: 255.255.255.0
Benutzername: root
Password: telekinese
DNS Server
Funktion: Zuweisung der Route/IP bei Kommunikationsanfrage des jeweiligen Triggerknotens zum weiteren Knoten/Endpunkt
IP-Adresse: 192.168.25.4/24
MAC-Adresse: 00:0C:29:B5:85:3B
Gateway: 192.168.25.2
DNS-Server: 192.168.25.4
Hostname: DNSDHCP
Domain: doubtful-joy25.com
OS & Version: CENTOS 9.X ohne GUI
Software: Bind9
Netzmaske: 255.255.255.0
Benutzername: root
Password: telekinese
VMnet8
Funktion: Durchlassen der Datenströme zur Firewall
Schnittstelle: Vmnet8 (NAT – share Host IP)
IP-Adresse: 192.168.72.0/24
Netzmaske: 255.255.255.0
Mac-Adresse: 00:50:56:23:9B:F0
Router
Funktion: Routet die Datenströme aus dem Schulnetz über die vmnet8 zur Firewall
IP-Adresse: 192.168.72.2
Netzmaske: 255.255.255.0
Mac-Adresse: 00:50:56:23:9B:F0
Schulnetz
Funktion: Netzwerk aller Clients im BSZ Netzwerk
IP-Adresse: 10.1.0.0/24
Netzmaske: 255.255.255.0
Broadcast: 10.1.0.255
Dienste: TCP, UDP, IP
DNS Server
Funktion: Zuweisung der Route/IP bei Kommunikationsanfrage des jeweiligen Triggerknotens zum weiteren Knoten/Endpunkt
IP-Adresse: 10.1.1.2/24
Netzmaske: 255.255.255.0
Dienste: TCP, UDP, IP,HTTP(S),SSH,TLS/SSL,SMTP
Internet
Router
Funktion: Routet die Datenströme aus dem Schulnetz zur vmnet8
IP-Adresse: 10.1.0.2/24
Netzmaske: 255.255.255.0
Broadcast: 10.1.0.255
Mac-Adresse: 00:50:56:23:9B:F0
Dienste: TCP, UDP, IP
Proxy Server
Funktion: Verbindung zum Internet mit vorgestellter IP Adresse als Kommunikationsschnittstelle
IP-Adresse: 10.1.0.13/24
Netzmaske: 255.255.255.0
Dienste: TCP, UDP, IP,HTTP(S),SSH,TLS/SSL,SMTP
DHCP Server
Funktion: Verwaltung von IP-Adressen im Netzwerk
IP-Adresse: 10.1.1.10/24
Netzmaske: 255.255.255.0
Broadcast: 10.1.0.255
Dienste: TCP, UDP, IP

Projektstrukturplan

Personen:	Sebastian Spannekrebs
Lernfeld:	9
Berufsschulklasse:	IT 21/1
Projekt-Nummer:	3
Gesamtbudget-PT:	19 PT (152h bei 8h-Tag)
Datum:	23.11.2022
Aktualisiert:	23.11.2022

Phase: 1.1 Projekt 3

Logischer Netzwerkplan
Budget: 4 PT

Dokumente zusammentragen und Überprüfung der Vollständigkeit der Projektinformationen

Verantwortung:	Sebastian Spannekrebs
Dauer:	2.00 h.
Deadline:	02.09.2022
Status:	Abgeschlossen

Korrekturlesen und ggf. korrigieren von Inhalten sowie logischen Fehlern

Verantwortung:	Sebastian Spannekrebs
Dauer:	2 PT
Deadline:	02.09.2022
Status:	Abgeschlossen

Beschriftung aller Komponenten

Verantwortung:	Sebastian Spannekrebs
Dauer:	1 PT
Deadline:	02.09.2022
Status:	Abgeschlossen

Planerstellung und logische Anordnung der Komponenten

Verantwortung:	Sebastian Spannekrebs
Dauer:	1 PT
Deadline:	02.09.2022
Status:	Abgeschlossen

Präsentation und Auswertung

Verantwortung:	Sebastian Spannekrebs
Dauer:	30 min.
Deadline:	11.11.2022
Status:	Abgeschlossen

Phase: 1.2 Projekt 3

Analyse und Projektplanung
Budget: 3.5 PT

Dokumente zusammentragen und Überprüfung der Vollständigkeit der Projektinformationen

Verantwortung:	Sebastian Spannekrebs
Dauer:	2.00 h.
Deadline:	23.11.2022
Status:	Abgeschlossen

Netzwerkplan

Verantwortung:	Sebastian Spannekrebs
Dauer:	0.5 PT
Deadline:	23.11.2022
Status:	Abgeschlossen

Hinzufügen der geplanten Komponenten und Beschriftungen

Verantwortung:	Sebastian Spannekrebs
Dauer:	4 h
Deadline:	23.11.2022
Status:	Abgeschlossen

Korrekturlesen und ggf. Fehlerberichtigung

Verantwortung:	Sebastian Spannekrebs
Dauer:	2 h
Deadline:	23.11.2022
Status:	Abgeschlossen

Analyse

Verantwortung:	Sebastian Spannekrebs
Dauer:	1 PT
Deadline:	22.11.2022
Status:	Abgeschlossen

Analyse der Serviceerreichbarkeiten

Verantwortung:	Sebastian Spannekrebs
Dauer:	3 h
Deadline:	22.11.2022
Status:	Abgeschlossen

Analyse der Akteure und deren Kommunikationswege

Verantwortung:	Sebastian Spannekrebs
Dauer:	3 h
Deadline:	22.11.2022
Status:	Abgeschlossen

Korrekturlesen und ggf. Fehlerberichtigung

Verantwortung:	Sebastian Spannekrebs
Dauer:	2 h
Deadline:	22.11.2022
Status:	Abgeschlossen

Planung

Verantwortung:	Sebastian Spannekrebs
Dauer:	1.5 PT
Deadline:	23.11.2022
Status:	Abgeschlossen

Erstellung Pflichtenheft

Verantwortung:	Sebastian Spannekrebs
Dauer:	0.5 PT
Deadline:	22.11.2022
Status:	Abgeschlossen

Erstellung Projektstrukturplan

Verantwortung:	Sebastian Spannekrebs
Dauer:	3 h
Deadline:	23.11.2022
Status:	Abgeschlossen

Erstellung Gantt-Diagramm

Verantwortung:	Sebastian Spannekrebs
Dauer:	3 h
Deadline:	23.11.2022
Status:	Abgeschlossen

Korrekturlesen und ggf. Fehlerberichtigung

Verantwortung:	Sebastian Spannekrebs
Dauer:	2 h
Deadline:	23.09.2022
Status:	Abgeschlossen

Präsentation und Auswertung

Verantwortung:	Sebastian Spannekrebs
Dauer:	30 min.
Deadline:	16.12.2023
Status:	offen

Phase: 1.3 Projekt 3

Entscheiden und Durchführen Teil 1:
Budget: 7 PT

Dokumente zusammentragen und Überprüfung der Vollständigkeit der Projektinformationen. Präsentationsvorbereitungen

Verantwortung:	Sebastian Spannekrebs
Dauer:	0.5 PT
Deadline:	21.12.2022
Status:	offen

Durchführung Teil 1:

Verantwortung:	Sebastian Spannekrebs
Dauer:	6 PT
Deadline:	21.12.2022
Status:	offen

Einrichten, Verbinden aller Komponenten laut Netzwerkplan

Verantwortung:	Sebastian Spannekrebs
Dauer:	3 PT
Deadline:	21.12.2022
Status:	offen

Testen aller Komponenten und ggf. konfigurieren

Verantwortung:	Sebastian Spannekrebs
Dauer:	3 PT
Deadline:	21.12.2022
Status:	offen

Life - Präsentation und Gespräch

Verantwortung:	Sebastian Spannekrebs
Dauer:	30 min.
Deadline:	03.02.2023
Status:	offen

Phase: 1.4 Projekt 3

Entscheiden und Durchführen Teil 2:
Budget: 4.5 PT

Dokumente zusammentragen und Überprüfung der Vollständigkeit der Projektinformationen. Präsentationsvorbereitungen

Verantwortung:	Sebastian Spannekrebs
Dauer:	0.5 PT
Deadline:	10.02.2023
Status:	offen

Durchführung Teil 2:

Verantwortung:	Sebastian Spannekrebs
Dauer:	4 PT
Deadline:	10.02.2023
Status:	offen

Inbetriebnahme aller Server

Verantwortung:	Sebastian Spannekrebs
Dauer:	2 PT
Deadline:	10.02.2023
Status:	offen

Testen aller Komponenten und ggf. konfigurieren

Verantwortung:	Sebastian Spannekrebs
Dauer:	2 PT
Deadline:	10.02.2023
Status:	offen

Life - Präsentation und Gespräch

Verantwortung:	Sebastian Spannekrebs
Dauer:	30 min.
Deadline:	05.04.2023
Status:	offen

Phase: 2 Projekt 4

Entscheiden und Durchführen Teil 2:
Budget:

Absichern der Netzwerke

Verantwortung:	-
Dauer:	-
Deadline:	-
Status:	offen

Absichern der Dienste

Verantwortung:	-
Dauer:	-
Deadline:	-
Status:	offen

Implementierung der Applikation

Verantwortung:	-
Dauer:	-
Deadline:	-
Status:	offen

Testen der Applikation

Verantwortung:	-
Dauer:	-
Deadline:	-
Status:	offen

Gantt-Diagramm

Personen:	Sebastian Spannebrötz
Abteilung:	IT
Berufsqualifikation:	IT 13.1
Projekt-Nummer:	1
Start:	24.10.2022
Aktualisiert:	23.11.2022

ID	Phase & Meilensteine	Aufgabe	Unteraufgabe	Verantwortung	Anfang	Abschluss	Dauer
1	**Phase 1.1 - Logischer Netzwerkplan**	**Powerpflichtig und logische Anordnung der Komponenten**		Sebastian Spannebrötz	29.08.2022	29.08.2022	1T
2		**Diskussion zusammenfassen und Überprüfung der Vollständigkeit der Projektinformationen**		Sebastian Spannebrötz	30.08.2022	30.08.2022	2h
3		**Beschriftung aller Komponenten**		Sebastian Spannebrötz	31.08.2022	01.09.2022	1T
4		**Kontrollieren und ggf. korrigieren von Inhalten sowie logisches Fließen**		Sebastian Spannebrötz	01.09.2022	02.09.2022	2T
5	Meilenstein Fertigstellung Netzwerkplan				02.09.2022	02.09.2022	0T
6		**Präsentation und Auswertung**		Sebastian Spannebrötz	11.11.2022	11.11.2022	1T
7	Meilenstein Präsentation Tag				11.11.2022	11.11.2022	0T
8	**Phase 1.2 - Analyse und Projektplanung**	**Diskussion zusammenfassen und Überprüfung der Vollständigkeit der Projektinformationen**		Sebastian Spannebrötz	02.11.2022	02.11.2022	2h
9		**Netzwerkplan**	**Anzeigen der gelisteten Komponenten und Beschriftungen**	Sebastian Spannebrötz	02.11.2022	02.11.2022	4h
10			**Kontrollieren und ggf. Fehlerbeseitigung**	Sebastian Spannebrötz	02.11.2022	02.11.2022	2h
11	Meilenstein Netzwerkplan v1.1				02.11.2022	02.11.2022	0T
12		**Analyse**	**Analyse der Hardwarevoraussetzungen**	Sebastian Spannebrötz	02.11.2022	02.11.2022	2h
13			**Analyse der Akkuzeit und deren Kommunikationsmanagement**	Sebastian Spannebrötz	09.11.2022	09.11.2022	3h
14			**Kontrollieren und ggf. Fehlerbeseitigung**	Sebastian Spannebrötz	09.11.2022	09.11.2022	2h
15	Meilenstein Abschluss der Analysen				09.11.2022	09.11.2022	0T
16		**Planung**	**Erarbeitung Pflichtenheft**	Sebastian Spannebrötz	09.11.2022	09.11.2022	6h
17			**Erarbeitung Projektstrukturplan**	Sebastian Spannebrötz	09.11.2022	09.11.2022	3h
18			**Erstellung Gantt Diagramm**	Sebastian Spannebrötz	11.11.2022	11.11.2022	3h
19			**Kontrollieren und ggf. Fehlerbeseitigung**	Sebastian Spannebrötz	11.11.2022	11.11.2022	2h
20	Meilenstein Abschluss der Planung				11.11.2022	11.11.2022	0T
21		**Präsentation und Auswertung**		Sebastian Spannebrötz	16.12.2022	16.12.2022	2h
22	Meilenstein Phase 1 abgeschlossen				16.12.2022	16.12.2022	0T
23	**Phase 1.3 - Entscheiden und durchführen Teil 1**	**Diskussion zusammenfassen und Überprüfung der Vollständigkeit der Projektinformationen**		Sebastian Spannebrötz	13.12.2022	13.12.2022	6h
24		**Durchführung Teil 1**	**Vorarbeiten, Verbinden aller Komponenten laut Netzwerkplan**	Sebastian Spannebrötz	13.12.2022	15.12.2022	3T
25			**Testen aller Komponenten und ggf. Verfügbarkeit**	Sebastian Spannebrötz	16.12.2022	18.12.2022	3T
26	Meilenstein Durchführung Teil 1 abgeschlossen				18.12.2022	18.12.2022	0T
27		**Ufo - Präsentation und Gespräch**		Sebastian Spannebrötz	03.02.2023	03.02.2023	2h
28	Meilenstein Ufo - Präsentation abgeschlossen				03.02.2023	03.02.2023	0T
29	**Phase 1.4 - Entscheiden und durchführen Teil 2**	**Diskussion zusammenfassen und Überprüfung der Vollständigkeit der Projektinformationen**		Sebastian Spannebrötz	31.01.2023	31.01.2023	6h
30		**Durchführung Teil 2**	**Internetzugriff über Server**	Sebastian Spannebrötz	07.02.2023	08.02.2023	2T
31			**Testen aller Komponenten und ggf. Verfügbarkeit**	Sebastian Spannebrötz	28.03.2023	29.03.2023	2T
32	Meilenstein Durchführung Teil 2 abgeschlossen				29.03.2023	29.03.2023	0T
33		**Ufo - Präsentation und Gespräch**		Sebastian Spannebrötz	05.04.2023	05.04.2023	2h
34	Meilenstein Ufo - Präsentation abgeschlossen				05.04.2023	05.04.2023	0T