

Lernfeld:
Gruppe:
Klasse/Kurs

LF9 Netzwerke und Dienste bereitstellen
Spannekrebs Sebastian(Groupleader)
IT21-1

Funktionale Segmentierung von Enterprise IT Netzwerken

Sebastian Spannekrebs

IT 21-1

<< [Zum Anfang](#) >>

Lernfeld:
Gruppe:
Klasse/Kurs

LF9 Netzwerke und Dienste bereitstellen
Spannekrebs Sebastian(Groupleader)
IT21-1

Inhaltsverzeichnis:

1. [Logischer Netzwerkplan](#)
2. [Analyse](#)
 - 2.1. [Analyse der zu bereitzustellenden Dienste](#)
 - 2.2. [Anwendungsfälle der Akteure](#)
3. [Projektplanung](#)
 - 3.1. [Analyse des Arbeits- und Projektauftrages](#)
 - 3.2. [Pflichtenheft](#)
 - 3.3. [Projektstrukturplan](#)
 - 3.4. [Gantt-Diagramm](#)
4. Entscheiden und Durchführen
5. Auswertung und Reflexion
6. [Dokumentenanhänge](#)

<< [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)

2. Analyse

2.1 Analyse der zu bereitzustellenden Dienste:

Dienstbezeichnung	Öffentlich erreichbar	Begründung der Entscheidung
Firewall-System	Nein	<ul style="list-style-type: none">- 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	<ul style="list-style-type: none">- Es sollten nur Netzinterne Komponenten den Dienst abrufen können ansonsten besteht Manipulationsgefahr der Nummer- bzw. Namensadressenauflösung
DHCP	Nein	<ul style="list-style-type: none">- 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	<ul style="list-style-type: none">- Stakeholder sollten von außen auf den Webserver zur Darstellung von Informationen zugreifen können.- Manipulation von Daten, nur durch Nutzerauthentifizierung,

		mit einher gehenden Nutzerechten möglich.
Datenbank-Server	Nein	<ul style="list-style-type: none"> - Sollte nur mit anderen Systemen Netzzintern kommunizieren. - Z.B. Client <-> Webserver <-> Datenbankserver - Sensible Nutzerdaten müssen geschützt werden nach Richtlinie der DSGVO
[Pi-Hole]	Nein	<ul style="list-style-type: none"> - 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	<ul style="list-style-type: none"> - 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	<ul style="list-style-type: none"> - 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.

2.2 Anwendungsfälle der Akteure:

Akteure	Kommunikationsweg
Ticket erstellen und in DB speichern:	<ul style="list-style-type: none"> - 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:	<ul style="list-style-type: none"> - Admin-Rechner(VMNet1/grün) -> Router(VMne1/grün) -> FW - Admin-Rechner(VMNet1/grün) -> Router(VMne1/grün) -> FW -> Router(VMnet2/orange/DMZ) -> DNS-Server - Admin-Rechner(VMNet1/grün) -> Router(VMne1/grün) -> FW -> Router(VMnet2/orange/DMZ) -> DHCP-Server
Administration des Web-Servers:	<ul style="list-style-type: none"> - Admin-Rechner(VMNet1/grün) -> Router(VMne1/grün) -> FW -> Router(VMnet2/orange/DMZ) -> Web-Server
Datenbankabfrage zur Supportsteuerung:	<ul style="list-style-type: none"> - Client(VMNet1/grün) -> Router(VMne1/grün) -> FW -> Router(VMnet2/orange/DMZ) -> Webserver -> Router(VMnet2/orange/DMZ) -> DB -> Router(VMnet2/orange/DMZ) -> Webserver
[Pi-Hole]:	<ul style="list-style-type: none"> - 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 ->

Lernfeld:
Gruppe:
Klasse/Kurs

LF9 Netzwerke und Dienste bereitstellen
Spannekrebs Sebastian(Groupleader)
IT21-1

	Router(VMne1/grün) -> Client (VMNet1/grün)
[Mailkommunikation]:	<ul style="list-style-type: none">- Client(Sender)(VMNet1/grün) -> Router(VMne1/grün) -> FW -> Router(VMnet2/orange/DMZ) -> Mail- Proxy-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

Arbeitsauftrag	Projektauftrag
<ul style="list-style-type: none">- Aufbau einer sicheren Netzinfrastruktur- Planung, Implementierung, Tests- Übergabe nach Fertigstellung an Applikation-Projektteam (Betriebsintern)	<ul style="list-style-type: none">- 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)	
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 zukunftsicheren Systembetrieb garantieren nach der Devise „make or buy“:
Funktionsspezifikation	<p><u>Anlegen eines Tickets durch Mitarbeiter:</u></p> <p>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</p> <p><u>Anlegen eines Tickets durch User/Kunde:</u></p> <p>Der Kunde/User kann über die Internetseite der Firma „Doubtful-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</p>

	oder bearbeiten ist nur durch einen Mitarbeiter der Doubtful-Joy möglich.
Datenspezifikation	<p>Ticket:</p> <ul style="list-style-type: none"> - Attribute: <ul style="list-style-type: none"> o Ticket-ID o User/Kunden – ID (ID oder Benutzername etc.) o User/Kunden – Vorname o User/Kunden - Name o User/Kunden – E-Mailadresse o User/Kunden - Vorname o Dropdown Auswahl (Problemeingrenzung-Bereich) o Dropdown Auswahl (Problemeingrenzung) o Dropdown Auswahl (Problemeingrenzung) o Textfeld: (Fehlercode eintragen, der ausgelöst wurde (optional)) o 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. <p><u>SPEICHERUNG:</u></p> <p><u>Datenbankeinträge:</u></p> <ul style="list-style-type: none"> - Ticket-ID - Kunde/User - Kundenkontakt/Userkontakt - Ticketprotokoll - <u>Ticketprotokolle:</u> <ul style="list-style-type: none"> o Vorgangsnummer o Priorität o Fehlerbewertung(Kritisch/Hoch/Mittel/Gering) o Bearbeitungsverlauf (Datum/Uhrzeit/zuständiger Mitarbeiter) - Geschlossene oder gelöschte Tickets werden in einer separaten Datenbank archiviert - Backup der Datenbanken zur Sicherung <p><u>Webserver:</u></p> <ul style="list-style-type: none"> - Umstellung des Clients & Backend durch Module, Services, Komponenten - Backup der Daten <p><u>DATENFLUSS:</u></p>

	<ul style="list-style-type: none"> - 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)
Schnittstellenspezifikation	<p>GUI - User/Kunde:</p> <ul style="list-style-type: none"> - Ausfüllen der Felder und über Button absenden <p>GUI – Mitarbeiter:</p> <ul style="list-style-type: none"> - Abrufen der Tickets,-bearbeiten,-löschen ,- schließen(archivieren) <p>GUI – Administrator:</p> <ul style="list-style-type: none"> - Gleiche Rechte wie Mitarbeiter, zusätzlich archivierte Einträge wieder aufrufen und Datensammlungen aus archivierten Tickets für Forecast und Kennzahlenerfassung. - Wartung über Terminal/Shell
Rahmenbedingungen	<p>Software:</p> <ul style="list-style-type: none"> - Eigenständige Dienstauswahl - VMware-Player - VM's <p>Räumlichkeiten:</p> <ul style="list-style-type: none"> - BSZ Elektrotechnik Dresden - Remote <p>Hardware:</p> <ul style="list-style-type: none"> - Schul-PC's oder vergleichbare Ausstattung wird bereitgestellt <p>Dokumente:</p> <ul style="list-style-type: none"> - Vorlagen siehe Lernsax Projektordner LF9
Qualitätsbetrachtung	<p>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-Branche Protokolliert und können somit nachvollzogen werden.</p>
Realisierungsvorschlag	<p><u>Analyse und Projektplanung:</u></p> <ul style="list-style-type: none"> - bis 25.11.2022 (UW-4)

	<p><u>Entscheiden und Durchführen Teil 1:</u></p> <ul style="list-style-type: none">- Abgabe:<ul style="list-style-type: none">o Bis 23.12.2022- Life-Präsentation:<ul style="list-style-type: none">o Bis 03.02.2023 <p><u>Entscheiden und Durchführen Teil 2(Auswertung und Reflektion):</u></p> <ul style="list-style-type: none">- Abgabe:<ul style="list-style-type: none">o Bis 10.02.2023- Life-Präsentation und Auswertung:<ul style="list-style-type: none">o 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.

Lernfeld:
Gruppe:
Klasse/Kurs

LF9 Netzwerke und Dienste bereitstellen
Spannekrebs Sebastian(Groupleader)
IT21-1

3.3 Projektstrukturplan:

Version 1:

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

[Projektstrukturplan](#) (extern)

Lernfeld:
Gruppe:
Klasse/Kurs

LF9 Netzwerke und Dienste bereitstellen
Spannekrebs Sebastian(Groupleader)
IT21-1

3.4 Gantt-Diagramm

Version 1:

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

[Gantt-Diagramm](#) (extern)

6. Dokumentenanhänge

Im folgenden Verlauf, sind alle geforderten Dokumente angehängt.