Funktionale Segmentierung von Enterprise IT Netzwerken

Sebastian Spannekrebs

IT 21-1

Inhaltsverzeichnis:

1. [Logischer Netzwerkplan](#Logischer_Netzwerkplan)
2. [Analyse](#Analyse)
   1. [Analyse der zu bereitzustellenden Dienste](#Analyse_2_1)
   2. [Anwendungsfälle der Akteure](#Anwendungsfaelle_2_2)
3. [Projektplanung](#Projektplanung_3)
   1. [Analyse des Arbeits- und Projektauftrages](#drei_eins)
   2. [Pflichtenheft](#drei_zwei)
   3. Projektstrukturplan
   4. Gantt-Diagramm
4. Entscheiden und Durchführen
5. Auswertung und Reflexion
6. Logischer Netzwerkplan

Es wurde ein Repository unter GitHub, für das Projekt angelegt. Der erstellte Netzwerkplan wurde unter folgendem Link bereitgestellt.

[Netzwerkplan](https://github.com/Feyu87/Project_Ausbildung_LF9/blob/cb19be5309ab1d9c14d8e1eb762debec3bd2c2be/LogischerNetzwerkplan/Netzwerkplan_LF9_Projekt03_Spannekrebs_Neumann.pdf) (extern)

1. Analyse
   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, 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. |

* 1. 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-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)** |

1. Projektplanung
   1. Analyse des Arbeits- und Projektauftrages

|  |  |
| --- | --- |
| **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) |

* 1. Pflichtenheft

|  |  |  |
| --- | --- | --- |
| **PFLICHTENHEFT (Grobkonzept)** | | |
| Auftraggeber |  | Doubtful-Joy SE |
| Zweck des Projektes | Segmentierung der Netzinfrastruktur für die aufzubauende Support-Lösung 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 | Anlegen eines Tickets durch Mitarbeiter:  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  Anlegen eines Tickets durch User/Kunde:  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 | **SPEICHERUNG:**  Datenbankeinträge:   * Ticket-ID * Kunde/User * Kundenkontakt/Userkontakt * Ticketprotokoll * Ticketprotokolle:   + Vorgangsnummer   + Priorität   + Fehlerbewertung(Kritisch/Hoch/Mittel/Gering)   + Bearbeitungsverlauf (Datum/Uhrzeit/zuständiger Mitarbeiter) * Geschlossene oder gelöschte Tickets werden in einer separaten Datenbank archiviert   **DATENFLUSS:**   * 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 | GUI - User/Kunde:   * (Ausfüllen der Felder und über Button absenden)   GUI – Mitarbeiter:   * (Abrufen der Tickets,-bearbeiten,-löschen ,-schließen(archivieren))   GUI – Administrator:   * (Gleiche Rechte wie Mitarbeiter, zusätzlich archivierte Einträge wieder aufrufen und Datenextraktion aus archivierten Tickets für Forecast) |
| Rahmenbedingungen | Software:   * Eigenständige Dienstauswahl * VMware-Player * VM’s   Räumlichkeiten:   * BSZ Elektrotechnik Dresden * Remote   Hardware:   * Schul-PC’s 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. |
| Realisierungsvorschlag |  | Analyse und Projektplanung:   * bis 25.11.2022 (UW-4)   Entscheiden und Durchführen Teil 1:   * Abgabe:   + Bis 23.12.2022 * Life-Präsentation:   + Bis 03.02.2023   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. |