Funktionale Segmentierung von Enterprise IT Netzwerken

1 Ziele

Die Auszubildenden implementieren eine Kundenanforderung für die Realisierung einer IT-Infrastruktur, eruieren Risiken für den Betrieb des IT-Systems und definieren den Schutzbedarf zum störungsfreien Betrieb einer Web-App mit Datenbackend.
Sie segmentieren die IT-Infrastruktur, installieren netzwerkrelevante Dienste, eine Web-App-Lösung und implementieren Sicherheitsfunktionen.

Im Einzelnen sind die Auszubildenden in der Lage

(1) IT-Infrastruktur bedarfsgerecht zu analysieren, zu planen und Netzwerke funktional zu segmentieren.

(2) Endsysteme und Dienste in verschiedenen Netzsegmenten zu installieren, einzurichten und zu testen.

(3) Die Systemintegration der Endsysteme und Dienste mit rollenbasierten User-Stories durchzuführen und die Auftragsanforderungen zu validieren.

(4) Die Vertraulichkeit, Verfügbarkeit und Integrität der Daten und ihrer Übertragung zwischen Endsystemen sicherzustellen und nachzuweisen.

2 Lernsituation

2.1 Ausgangslage

Die Gaming-Plattform „Doubtful-Joy SE“ hat eine existierende Support-Infrastruktur, die über Mails und Telefon kontaktierbar ist.

Die schnell wachsende Kundenzahl erfordert eine Neustrukturierung des Supports.
Die Geschäftsleitung hat beschlossen, den Kundensupport auf ein Ticketsystem umzustellen und damit den Support-Prozess zu vereinheitlichen.
Tickets können direkt vom Kunden über ein Web-Interface oder durch Mitarbeiter aus einer E-Mail heraus manuell eröffnet werden. Den Tickets können beliebig viele Attachements beigefügt werden.

Sie arbeiten im IT-Unternehmen „High-Secure GmbH“, welches den Auftrag von Doubtful-Joy SE zur Einführung des Ticketsystems erhalten hat.

2.2 Arbeitsauftrag

Ihr Projektteam wird vom Projektmanager beauftragt, eine sichere Netzwerkinfrastruktur für die aufzubauende Support-Lösung zu planen, zu implementieren, zu testen und an die Applikationsprojektteams in Ihrer Firma zu übergeben.

Aus dem **Lastenheft** wurde weiterhin entnommen:

1. Doubtful-Joy fordert eine Segmentierung der Netzinfrastruktur mit einer sicheren Trennung von öffentlich erreichbaren Diensten und dem Intranet.
2. Die netzwerkrelevanten internen Dienste DNS und DHCP sind auf einem separaten System bereitzustellen um Abhängigkeiten von der Firewall auszuschließen.
3. Doubtful-Joy setzt im Bereich der Server ausschließlich RedHat und binärkompatible Systeme ein. Alle OS-Installationen folgen dieser System-Strategie.

2.3 Projektgliederung

In Abstimmung mit den Projektteams der Applikation wurde vereinbart, dass die Umsetzung des Auftrages in zwei Phasen erfolgt (Projekt 3 und Projekt 4).

In der ersten Phase wird die Netzinfrastruktur und Dienst-Funktionalität zügig geplant und bereitgestellt.

In der zweiten Phase sind das Netzwerk und die Dienste sicherheitstechnisch abzusichern und parallel dazu die Applikation zu implementieren und testen.

3 Projekt 3

Dauer des Projektes: 5 Wochen (UW 3-7)
Aufbau der Netzinfrastruktur und Sicherstellung der Systemerreichbarkeit und prinzipiellen Dienstverfügbarkeit ohne E2E-Verschlüsselung in der Datenkommunikation.

Nachfolgende Dienste gemäß Lastenheft sind bereitzustellen.

Dienstbezeichnung	**Öffentlich erreichbar**
Firewall-System	Nein
DNS	Nein
DHCP	Nein
Web-Server	Ja
Datenbank-Server	Nein
[Pi-Hole]	Nein
[Mailproxy für eingehende Mails]	Ja
[existierender Mailserver]	Nein

Tabelle 1: Diensterreichbarkeit

3.1 Logischer Netzwerkplan

Nutzen Sie den von Ihnen erstellten Netzwerkplan aus dem Vorprojekt „Realisierung der virtuellen Netzwerkinfrastruktur für LF9“.

Die *Individualisierung*sfestlegungen aus dieser Aufgabenstellung werden vollständig übernommen.

Zusätzlich gilt für die öffentlich verwaltete Domäne die nachstehende Bildungsregel für den DNS-Namen

Doubtful-Joy<zweistellige[1] Klassenbuchnummer des Projektleiters>.{com|de}

3.2 Analyse

1. Begründen Sie die in der Tabelle 1 getroffenen Entscheidungen zur öffentlichen Erreichbarkeit der Dienste.

2. Beschreiben Sie die Akteure und den jeweiligen Kommunikationsweg über die Zwischensysteme zu den IT-Endsystemen für folgenden Anwendungsfälle:

   a. Ticket erstellen und in DB speichern
   b. Administration von FW, DNS- und DHCP-Server
   c. Administration des Web-Servers
   d. Datenbankabfragen zur Supportsteuerung (z.B. Anzahl offener Tickets)
   e. [Pi-Hole]
   f. [Mailkommunikation]

[1] Die Schülernummern 1-9 werden mit einer Präfixnull aufgefüllt.

3.3 Projektplanung

1. Analysieren Sie den Arbeitsauftrag und erstellen Sie ein Pflichtenheft gemäß Anlage 3 - „Anforderungen an das Pflichtenheft“ (Grob- und Feinkonzept[2]).
2. Definieren Sie Arbeitspakete, Verantwortlichkeiten und zeichnen Sie einen Projektstrukturplan.
3. Erstellen Sie ein Gantt-Diagramm auf Teilnehmer-Arbeitspaketebene, das mit dem Abnahmetermin in der 7. Unterrichtswoche endet.
4. Definieren Sie für das Ende jeder Schulwoche Meilensteine.

3.4 Entscheiden und Durchführen

1. Installation der Systeme und Dienste entsprechend Tabelle 1.
2. Einrichtung einer Test-Web-Seite zur Anzeige der Anzahl der Datensätze der einzigen Tabelle „Tickets“ des DB-Servers. (Tabelle Tickets: Ticketnummer, Datum der Erstellung, Tickettext)
3. Nachweis der Nutzbarkeit der WEB-Seite aus dem Netz des Hostrechners,
4. Start und Stopp des WEB-Servers vom Adminrechner.
5. [Installation Pi-Hole]
6. [Installation Mail-Server und Mail-Proxy]

3.5 Auswertung und Reflexion

1. Fassen Sie Ihre praktischen Arbeitsergebnisse der Durchführung als Ablaufdokumentation zusammen.
2. Erstellen Sie einen Soll-Ist-Vergleich zum erreichten Ergebnis und erläutern Sie Ursachen für Defizite.
3. Ergänzen Sie in Ihrem Zeitplan den realen Arbeitsaufwand und vergleichen Sie die Ergebnisse mit Ihrer Planung und reflektieren Sie zu möglichen Abweichungen.
4. Nennen Sie Optimierungsvorschläge zur Projektrealisierung.
5. [Führen Sie eine Schutzbedarfsanalyse für das Ticketsystem durch und unterbreiten Sie Umsetzungsvarianten]

3.6 Arbeitshinweise

In eckige Klammern gesetzte Systeme und Aufgaben sind optional.

4 Projekt 4

Härtung der Komplettlösung unter Beachtung aktueller Security-Anforderungen nach dem Stand der Technik. Die Konkretisierung erfolgt mit Projektstart.

[2] Das Feinkonzept ist die Grundlage der Projektplanung und enthält im Gegensatz zum Grobkonzept die Detailabstimmung der Anforderungen aus dem Gespräch mit dem Auftraggeber.

5 Anlage 1- Projektauftrag Projekt 3

Projektname: Phase 1 der funktionalen Segmentierung von Enterprise IT Netzwerken

Projektbeschreibung
Der Laborversuch zum Thema „Segmentierung von Enterprise IT Netzwerken“ im Rahmen der handlungsorientierten Ausbildung umfasst den Aufbau der Netzinfrastruktur und Sicherstellung der Systemerreichbarkeit und prinzipiellen Dienstverfügbarkeit einer Supportinfrastruktur mit Erreichbarkeit aus dem Internet. Jede Projektgruppe plant die Durchführung und die Zuordnung der Arbeitspakete an die Mitglieder des Teams sowie den relativen Zeitumfang der Tätigkeiten *selbständig*.

Mitarbeiter (Name, Vorname: Kommunikation)[3]	**Lernfeld** LF9 Netze und Dienste bereitstellen
_____ _____ _____	**Klasse / Kurs** IT20/__ **Gruppen-Nr.** _____

Termine	**Betreuende(r) Fachlehrer**
Beginn der Arbeit: Beginn UW3 Abnahme der Arbeit: in UW7 **Zeitumfang (UStd)** 30 Ustd je Schüler	Name: _____ Telefon: (03 51) 47 35 – _____ email: _____ Postanschrift: BSZ für Elektrotechnik Dresden Strehlener Platz 2 01219 Dresden

Auftragsbedingungen (Hilfsmittel, SW, HW, Arbeitsorte)
Dokumente und Vorlagen: siehe Lernsax Projektordner LF9 Hardware: Schul-PC‘s im Medios-Netz oder vergleichbare Ausstattung Software: VMware-Player und eingeführte VMs, Dienstauswahl eigenständig Arbeitsort: BSZ Elektrotechnik Dresden

3 Projektleiter **an erster Stelle** der Nennung

Lernfeld 9: Netzwerke und Dienste bereitstellen

Technische Vorgaben für die Laborumgebung

1. Alle virtuellen Maschinen sind **ausschließlich** in einem Netzwerk eines virtuellen Switches mit **NAT, Host-Only oder Custom** des VMware Workstation Players zu betreiben.
2. Die **DNS Weiterleitung (upstream)** aus allen virtuellen Netzen ist **ausschließlich** über den **DNS-Resolver der Firewall**-Lösung (z.B. IP-Fire im roten Netzwerk) zu realisieren**.**

   Hinweise zu IP-Fire

   Damit der unbound-DNS-Resolver in IP-Fire den Stub-Resolver in VMnet8 (default: 192.168.72.2) akzeptiert, ist die Datei *unbound.conf* in das Verzeichnis */etc/unbound/* der IP-Fire-VM zu kopieren (z.B. mit scp). Die Konfigurationsdatei stellt der betreuende Fachlehrer zur Verfügung.

   Anschießend ist im Webinterface des IP-Fire in: *Netzwerk →Domain-Name-System* der Stub-Resolver von VMnet8 als DNS-upstream-Adresse einzutragen und ggf. auf das TCP-Protokoll zu wechseln (dns).

Projektziele (Sachziele, Kostenziele/Bewertung, Terminziele)

Sachziel: Herstellen der Dienstverfügbarkeit in einem Enterprise-Netzwerk mit Firewall und DMZ

Kostenziel: entfällt

Bewertung: nach schulischem Maßstab gemäß Ausbildungsverordnung
Pflichtenheft und Projektgrobplanung, Funktionalitätsnachweis des Auftrages (Abnahme)

5. UW: Projektgespräch je Gruppe 15-20‘ / Präsentation der Planung (Analyse & Projektplanung)

7. UW: Projektabschluss je Gruppe 15-20‘ / Life-Präsentation der Dienst-Funktionalität ab 8.UW

Terminziel: Abschluss Projekt 3 am Ende der 7.UW

Geforderte Dokumentationen zur Projektarbeit

1. Pflichtenheft und Projektgrobplanung (bis Ende 4. UW)
2. Projektabschlussdokumentation (bis Ende 7. UW)

Benennen Sie Dokumente eindeutig und geben Sie im Dokument formale Informationen zum Projekt. Laden Sie Arbeitsergebnisse als PDF-Dokument in den Unterordner „Schülerlösungen“ im Lernsax Projektordner LF9.

Projektleiter	**Bestätigung des betreuenden Fachlehrers**
Dresden, _____ 2021	Dresden, _____ 2021
.....	.....
Unterschrift	*Unterschrift*

6 Anlage 2: Anforderungen an das Pflichtenheft

Auftraggeber	Siehe Lernsituation
Zweck des Projektes	Siehe Lernsituation
Analyse der Ausgangssituation	Erläutern Sie die Ausgangslage und die Zielsetzung in eigenen Worten.
Funktionsspezifikation	Beschreiben Sie die betroffenen Geschäftsprozesse, Dienste und Anwender auf der Grundlage des Schichtenmodells eines IT-Systems (Orgware, Manware, Software, Hardware)
Datenspezifikation	Analysieren Sie die vermuteten Datenmengen, die Art der Daten und den Datenfluss.
Schnittstellenspezifikation	Definieren Sie die Schnittstellen und die Bedienoberfläche Ihrer Lösung.
Rahmenbedingungen	Beschreiben Sie die Ressourcen und Mitwirkungspflichten des AG, die Sie für die Umsetzung und Testung benötigen.
Qualitätsbetrachtung	Beschreiben Sie, wie Sie die Qualität und Zeitplanung während der Entwicklung sicherstellen wollen. Benennen Sie den Aufwand für den Support Ihrer Lösung.
Realisierungsvorschlag	Es ist ein Lösungsvorschlag basierend auf den Vorgaben des Lastenheftes und der Akzeptanzanalyse vorzulegen.
Projektplanung	Bestätigen Sie, dass sich das Projekt in der gewünschten Zeit umsetzen lässt. Wenn Sie Bedenken haben, benennen und begründen Sie diese.
Kosten-Nutzen-Analyse	Begründen Sie, dass eine monetäre Kosten-Nutzenanalyse für diesen Projektauftrag nachgeordnet ist.