

Abschlussprüfung Winter 2019/20

1197

1 Ganzheitliche Aufgabe I Fachqualifikationen

Fachinformatiker Fachinformatikerin Systemintegration

5 Handlungsschritte
90 Minuten Prüfungszeit
100 Punkte

Bearbeitungshinweise

- Der vorliegende Aufgabensatz besteht aus insgesamt 5 Handlungsschritten zu je 25 Punkten.

In der Prüfung zu bearbeiten sind 4 Handlungsschritte, die vom Prüfungsteilnehmer frei gewählt werden können.

Der nicht bearbeitete Handlungsschritt ist durch Streichung des Aufgabentextes im Aufgabensatz und unten mit dem Vermerk „Nicht bearbeiteter Handlungsschritt: Nr. ... „ an Stelle einer Lösungsniederschrift deutlich zu kennzeichnen. Erfolgt eine solche Kennzeichnung nicht oder nicht eindeutig, gilt der 5. Handlungsschritt als nicht bearbeitet.

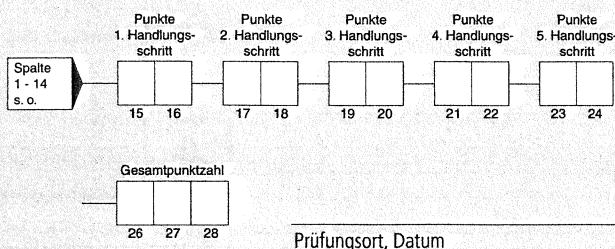
 - Füllen Sie zuerst die **Kopfzeile** aus. Tragen Sie Ihren Familiennamen, Ihren Vornamen und Ihre Prüflings-Nr. in die oben stehenden Felder ein.
 - Lesen Sie bitte den **Text** der Aufgaben ganz durch, bevor Sie mit der Bearbeitung beginnen.
 - Halten Sie sich bei der Bearbeitung der Aufgaben genau an die **Vorgaben der Aufgabenstellung** zum Umfang der Lösung. Wenn z. B. vier Angaben gefordert werden und Sie sechs Angaben anführen, werden nur die ersten vier Angaben bewertet.
 - Tragen Sie die frei zu formulierenden **Antworten dieser offenen Aufgabenstellungen** in die dafür lt. Aufgabenstellung vorgesehenen Bereiche (Lösungszeilen, Formulare, Tabellen u. a.) des Arbeitsbogens ein.
 - Sofern nicht ausdrücklich ein Brief oder eine Formulierung in ganzen Sätzen gefordert werden, ist eine **stichwortartige Beantwortung** zulässig.
 - Verwenden Sie nur einen Kugelschreiber und schreiben Sie deutlich und gut lesbar. Ein nicht eindeutig zuzuordnendes oder **unleserliches Ergebnis** wird als **falsch** gewertet.
 - Zur Lösung der Rechenaufgaben darf ein nicht programmierter, netzunabhängiger **Taschenrechner** ohne Kommunikationsmöglichkeit mit Dritten verwendet werden.
 - Wenn Sie ein **gerundetes Ergebnis** eintragen und damit weiterrechnen müssen, rechnen Sie (auch im Taschenrechner) nur mit diesem gerundeten Ergebnis weiter.
 - Für **Nebenrechnungen/Hilfsaufzeichnungen** können Sie das im Aufgabensatz enthaltene Konzeptpapier verwenden. Dieses muss vor Bearbeitung der Aufgaben herausgetrennt werden. Bewertet werden jedoch nur Ihre Eintragungen im Aufgabensatz.

Nicht bearbeiteter Handlungsschritt ist Nr.

Wird vom Korrektor ausgefüllt!

Bewertung

Für die Bewertung gilt die Vorgabe der Punkte in den Lösungshinweisen. Für den abgewählten Handlungsschritt ist anstatt der Punktzahl die Buchstabenkombination „AA“ in die Kästchen einzutragen.



Prüfungszeit
25
Die entsprechende Ziffer (1, 2 oder 3) finden Sie in der Abfrage nach der Prüfungszeit im Anschluss an die letzte Aufgabe.

Die entsprechende Ziffer (1, 2 oder 3) finden Sie in der Abfrage nach der Prüfungszeit im Anschluss an die letzte Aufgabe.

Prüfungsort, Datum

Unterschrift

Die Handlungsschritte 1 bis 5 beziehen sich auf die folgende Ausgangssituation:

Sie sind bei Event GmbH in der IT-Abteilung beschäftigt. Die Event GmbH ist Dienstleister im Bereich der Planung und Durchführung von Fachmessen mit Schwerpunkt Smart Factory. Sie hat ihre Zentrale in Stuttgart.

Die Event GmbH arbeitet im WAN-Bereich mit dem Internet-Provider iKomP zusammen.

Die bestehende IT-Infrastruktur der Event GmbH soll technisch und organisatorisch aktualisiert werden. Dabei wird besonderer Wert auf die IT-Sicherheit gelegt.

Sie arbeiten in diesem Projekt mit.

Bearbeiten Sie vier der folgenden fünf Handlungsschritte:

1. Die Netzwerkstruktur analysieren und das Routing einrichten
2. Das Netzwerk-Monitoring einrichten
3. Den Serverbetrieb sicherstellen
4. Die IT-Sicherheit verbessern
5. Die Benutzeranlage erläutern

Hinweis:

Es werden die folgenden Einheiten verwendet:

Speicherkapazität (z. B. Festplatten) in MiB $1.024 * 1.024$ Byte

Transferrate (z. B. PCI-Bus) in MB/s $1.000 * 1.000$ Byte/s

Transferrate (z. B. Ethernet, DSL) in Mbit/s $1.000 * 1.000$ bit/s

1. Handlungsschritt (25 Punkte)

a) Das Netzwerk der Event GmbH soll neu strukturiert werden.

aa) Die Administratoren wollen VLANs für die Abteilungen Verwaltung, Entwicklung und Management einrichten.

Erläutern Sie zwei Gründe, die für die Einrichtung von VLANs sprechen.

4 Punkte

ab) VLANs werden mit einem „Tag“ in Netzwerken identifiziert:

16 bits	3 bits	1 bit	12 bits
TPID	TCI		
	PCP	DEI	VID

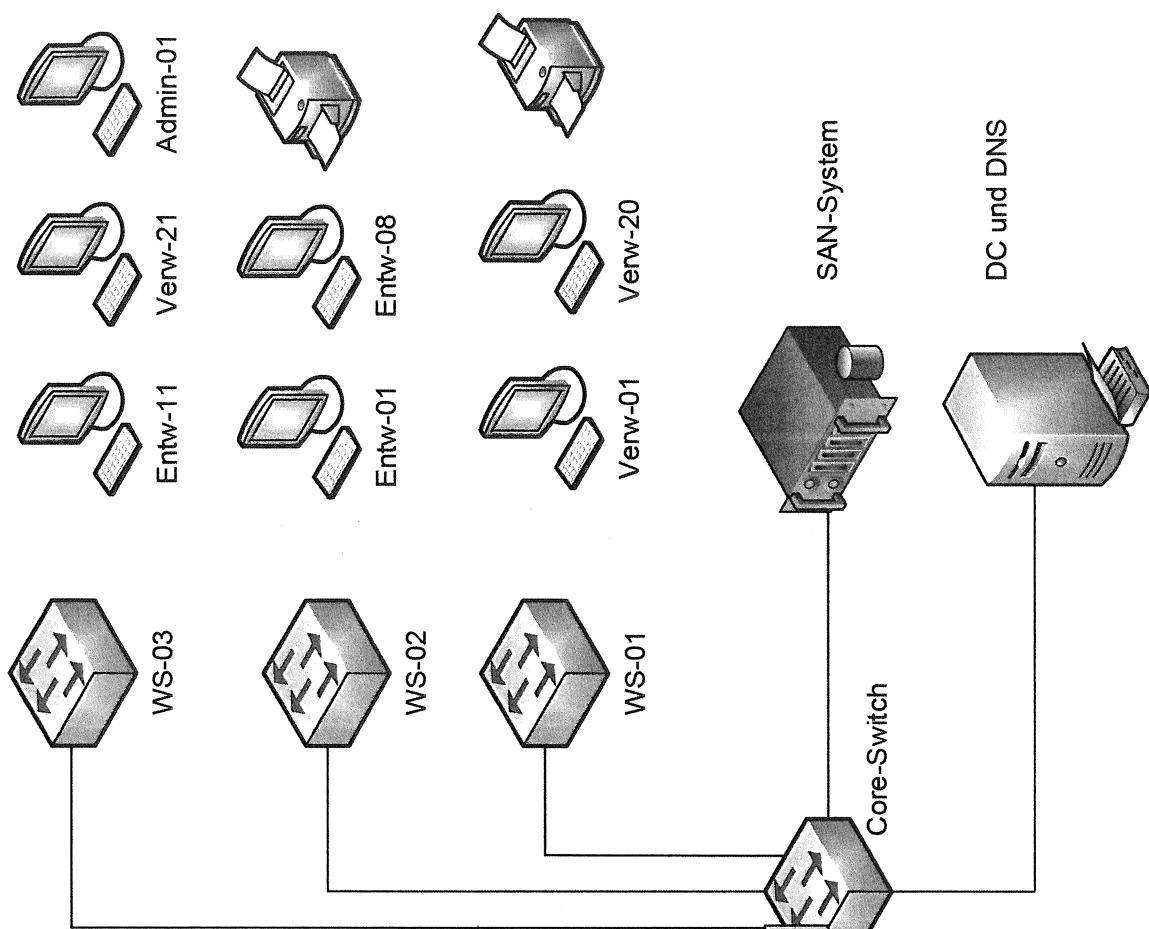
- **TPID** – Tag Protocol Identifier: Fester Wert 8100_{hex}.
- **TCI** – Tag Control Information:
 - **PCP** – Priority Code Point: Benutzer-Prioritätsinformationen.
 - **DEI** – Drop Eligible Indicator: Kann separat oder in Verbindung mit PCP verwendet werden, um anzugeben, dass Frames in der Gegenwart von Staus fallen gelassen werden können.
 - **VID** – VLAN-Identifier: Identifizierung des VLANs, zu dem der Frame gehört.

Ermitteln Sie die maximale Anzahl an VLANs, die in einem Netzwerk eingerichtet werden können. Der Rechenweg ist anzugeben.

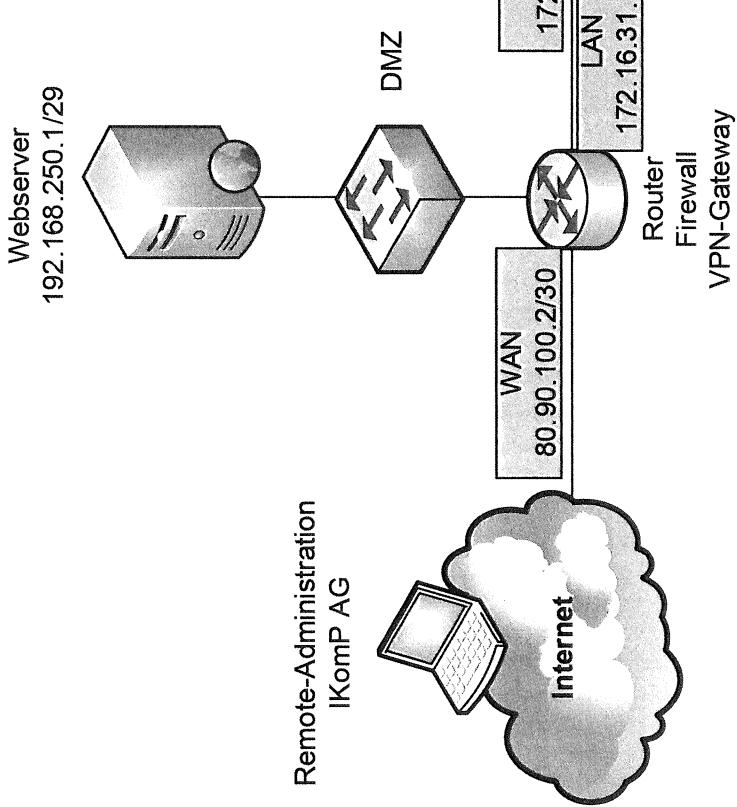
3 Punkte

Dieses Blatt kann an der Perforation aus dem Aufgabensatz herausgetrennt werden!

Netzwerkplan der Event GmbH



Netzwerkplan der Event GmbH



- ac) Auf den Verbindungen zwischen den Switchen (z. B. Core-Switch ↔ WS-03) wird VLAN-Tagging eingerichtet.

Erläutern Sie, warum VLAN-Tagging auf diesen Verbindungen zwingend notwendig ist.

4 Punkte

Korrekturrand

- b) Im Netzwerk der Event GmbH sollen für jede(n) Abteilung/Zweck ein eigenes VLAN eingerichtet werden. Die Anzahl der maximal möglichen IP-Adressen soll dabei auf ein Minimum anhand der Subnetzmaske beschränkt werden. Die Administratoren haben bereits die Hostzahlen ermittelt.

Ergänzen Sie die entsprechende Subnetzmaske (Dezimal-Punkt-Schreibweise) und die IP-Adresse des Default-Gateways.

Die IP-Adresse des Default-Gateways soll immer die letzte IP sein.

6 Punkte

VLAN	Netz-ID	Anzahl Hosts	Subnetzmaske	Default-Gateway
Verwaltung	192.168.10.0	54		
Entwicklung	192.168.20.0	28		
Management	192.168.40.0	5		

- c) Nach der Einrichtung der VLANs überprüfen Sie die Kommunikation im Netzwerk.

- ca) Clients in den VLANs haben keinen Zugriff auf den Webserver in der DMZ oder Webserver im Internet.

Sie lassen sich die Routingtabelle auf dem Layer 3-Core-Switch anzeigen:

```
172.16.31.0/30 is directly connected, FastEthernet0/8
192.168.10.0/26 is directly connected, Vlan10
192.168.20.0/27 is directly connected, Vlan20
192.168.40.0/29 is directly connected, Vlan199
```

Erläutern Sie, welcher Fehler in der Routingtabelle vorliegt und wie Sie diesen Fehler beheben.

4 Punkte

- cb) Auch nach der Behebung des Fehlers funktioniert die Kommunikation mit dem Internet aus dem Management-VLAN noch nicht. Aus den anderen VLANs ist ein Internetzugriff möglich. Sie überprüfen daraufhin die Routing-Tabelle des Routers:

```
80.90.100.0/30, is directly connected, FastEthernet0/1
172.16.31.0/30 is directly connected, FastEthernet0/0
192.168.0.0/19 [1/0] via 172.16.31.2
192.168.250.0/29 is directly connected, FastEthernet1/0
0.0.0.0/0 [1/0] via 80.90.100.1
```

Erläutern Sie, welcher Fehler in diesem Fall vorliegt.

4 Punkte

2. Handlungsschritt (25 Punkte)

Korrekturrand

Sie arbeiten an dem Projekt „Netzwerk-Monitoring“ mit und sollen in diesem Zusammenhang folgende Aufgaben bearbeiten.

- a) Bei der Überprüfung der Netzwerkfunktionalität am Client Verw-01 benutzen Sie verschiedene, im Betriebssystem integrierte Hilfsprogramme.

Geben Sie zu jeder der folgenden Situationen jeweils **ein** geeignetes Hilfsprogramm an, indem Sie das entsprechende Feld in der Tabelle mit „X“ markieren. 4 Punkte

Situation	ping	tracert/ traceroute	arp	ipconfig/ ifconfig	nslookup
Die MAC-Adresse des eigenen Rechners ermitteln.					
Den Host-Namen des eigenen Rechners überprüfen.					
Die IP-Adresse des Gateways für den eigenen Rechner anzeigen lassen.					
Die MAC-Adresse des Gateways für den eigenen Rechner anzeigen lassen.					
Feststellen, ob der Host www.ihk.de IPv6 unterstützt.					
Die IPv6 Netz-ID des eigenen LAN ermitteln.					
Die Anzahl Hops (Router) zu einem externen Server ermitteln.					
Die Erreichbarkeit des Webservers in der DMZ fortlaufend kontrollieren.					

- b) Zur Analyse und Optimierung der Netzwerkverbindung zu dem Server www.future-gmbh.de soll der MTU-Wert (Maximum Transmission Unit) für diese Verbindung ermittelt werden.

Erläutern Sie eine mögliche Vorgehensweise, um den MTU-Wert einer Netzwerkverbindung mithilfe des Ping-Befehls zu ermitteln. Geben Sie dabei auch **ein Beispiel** für einen entsprechenden Ping-Befehl einschließlich der erforderlichen Parameter an. 5 Punkte

Syntax: ping [-t] [-a] [-n Anzahl] [-l Größe] [-f] [-i TTL Gültigkeitsdauer]
 [-v Diensttyp] [-r Anzahl] [-s Anzahl] [[-j Hostliste] |
 [-k Hostliste]] [-w Zeitlimit] Zielname

Optionen:

- t Pingt den angegebenen Host bis zur Beendigung des Vorgangs.
 Drücken Sie STRG+UNTBR, um die Statistik anzuzeigen und den Vorgang fortzusetzen.
 Drücken Sie STRG+C, um den Vorgang abzubrechen.
 - a Löst Adressen zu Hostnamen auf.
 - n Anzahl Die Anzahl der zu sendenden Echoanforderungen.
 - l Größe Die Größe des Sendepuffers.
 - f Legt das Kennzeichen für „Nicht fragmentieren“ im Paket fest.
 - i TTL Die Lebensdauer des Datenpaketes.
 - v TOS Der Diensttyp (Type of Service).
 - r Anzahl Datensatzroute für Anzahl von Hops (nur IPv4).
 - s Anzahl Zeitstempel für Anzahl von Hops (nur IPv4).
 - j Hostliste „Loose Source Route“ gemäß Hostliste (nur IPv4).
 - k Hostliste „Strict Source Route“ gemäß Hostliste (nur IPv4).
 - w Zeitlimit Zeitlimit in Millisekunden für eine Rückmeldung
-
-
-
-
-

- c) Der Betriebszustand bestimmter Netzwerkergeräte soll mithilfe von SNMP (Simple Network Management Protocol) überwacht werden.

Korrekturrand

Erläutern Sie in diesem Zusammenhang die grundlegende Arbeitsweise von SNMP.

4 Punkte

Bearbeitungshinweis: Verwenden Sie in Ihrer Erläuterung folgende Begriffe:

- MIB (Management-Information-Base)
 - GetRequest;
 - Community-String

- d) Sie planen das Remote-Netzwerk-Management. Der externe Zugriff auf das Netzwerk erfolgt über ein VPN-Gateway. Das VPN-Gateway hat eine ADSL 50/10 Mbit/s Internetanbindung.

Das Remote-Netzwerk-Management soll maximal 2 % Übertragungskapazität der Verbindung beanspruchen.

Jede der zehn Komponenten der Kategorie 1 (z. B. Router) überträgt 1.000 Byte je Abfrage.

Komponenten der Kategorie 2 übertragen 500 Byte je Abfrage. Die Abfragen erfolgen einmal pro Sekunde.

Berechnen Sie die Anzahl der Komponenten der Kategorie 2 (z. B. Drucker), die noch überwacht werden können, ohne dass mehr als 2 % der Übertragungskapazität des VPN-Gateway benötigt werden. 5 Pu

Fortsetzung 2. Handlungsschritt

Korrekturrand

- e) An der Management-Station soll fortlaufend der jeweilige Anteil von UDP- und TCP-Paketen am IP-Traffic der vergangenen Sekunde in Prozent angezeigt werden. Dazu werden die entsprechenden Werte einmal pro Sekunde beim Internet-Gateway abgefragt. Ein entsprechendes Skript liegt als unvollständiger Entwurf im Pseudocode vor.

Zeile 1 STARTSKRIPT

Zeile 2 LESEN Anzahl TCP-Pakete vom Internet-GW und SPEICHERN in AnzStartTCP;

Zeile 3 LESEN Anzahl UDP-Pakete vom Internet-GW und SPEICHERN in AnzStartUDP;

Zeile 4 LESEN Anzahl IP-Pakete vom Internet-GW und SPEICHERN in AnzStartIP;

Zeile 5 WIEDERHOLE

Zeile 6 VERZÖGERN 1s

Zeile 7 LESEN Anzahl TCP-Pakete vom Internet-GW und SPEICHERN in AnzEndeTCP;

Zeile 8 LESEN Anzahl UDP-Pakete vom Internet-GW und SPEICHERN in AnzEndeUDP;

Zeile 9 LESEN Anzahl Pakete vom Internet-GW insgesamt SPEICHERN in AnzEndelP;

Zeile 10 BERECHNE AnteilTCP;

Zeile 11 BERECHNE AnteilUDP;

Zeile 12 ANZEIGEN von AnteilTCP und AnteilUDP;

Zeile 13 _____

Zeile 14 _____

Zeile 15 _____

Zeile 16 SOLANGE das Programm nicht beendet wird;

Zeile 17 ENDESKRIPT

- ea) Erstellen Sie für den Programmschritt in Zeile 10 den entsprechenden Code (in Pseudocode oder in einer Ihnen vertrauten Programmiersprache). 4 Punkte

- eb) Ergänzen Sie die Zeilen 13 bis 15 so, dass die Variablen „AnzStartTCP, AnzStartUDP und AnzStartIP“ die erforderlichen Werte für den nächsten Schleifendurchgang zugewiesen bekommen. 3 Punkte

3. Handlungsschritt (25 Punkte)

Korrekturrand

Die Event GmbH will ihre Serverlandschaft modernisieren und absichern.

- a) Die IT-Abteilung der Event GmbH plant den Einsatz von aktuellen Blade-Serversystemen.

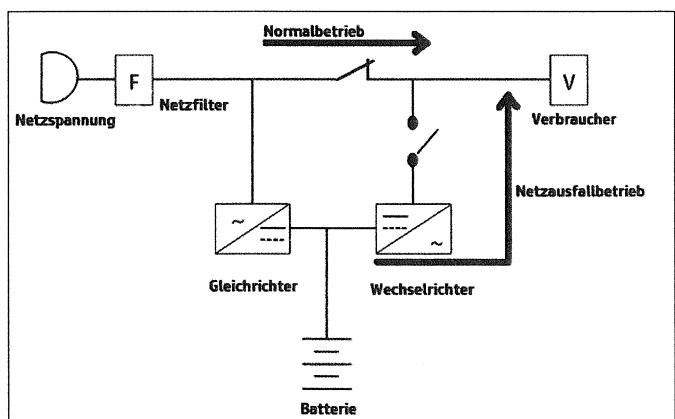
Nennen Sie drei Vorteile, die ein solches Blade-Serversystem gegenüber klassischen Serversystemen aufweist. 3 Punkte

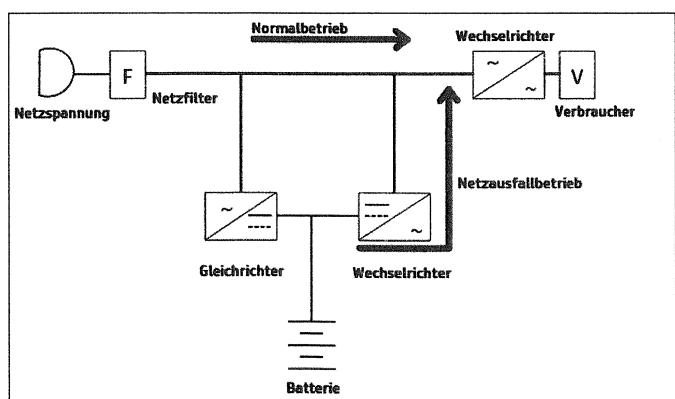
-
-
-
- b) Sie sollen ein entsprechendes Betriebssystem für die Installation des Datenbank-Servers auswählen. Bei der Recherche dazu stoßen Sie auf Betriebssysteme in der Variante „LTS“.

Erklären Sie den Begriff „LTS“ und beschreiben Sie, warum der Einsatz einer LTS-Variante für Server sinnvoll ist. 3 Punkte

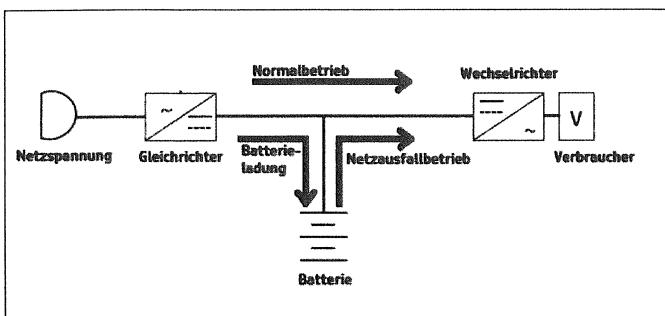
- c) Die Stromversorgung der eingesetzten Server soll durch eine USV gesichert werden. Sie stoßen bei Ihren Recherchen auf USVs mit den Betriebsmodi VFD, VI und VFI.

Ordnen Sie die Bezeichnungen den entsprechenden Blockschaltbildern zu und nennen Sie zwei spezifische Schutzeigenschaften einer VFI-USV. 7 Punkte





Fortsetzung 3. Handlungsschritt →



Spezifische Schutzeigenschaften einer VFI-USV:

- d) Die aktuell eingesetzte Unterbrechungsfreie Stromversorgung (Online-USV) ist durch drei Firmen-Server mit jeweils 750 VA belastet

Angaben zur Online-USV:

- Leistungsabgabe: max. 3.000 VA
 - Akkumulatoren: 24 Stück mit je 12 V/3,6 Ah
 - Zustand zum Zeitpunkt des Stromausfalls: zu 100 % geladen, lineare Entladung bis zum Shutdown

Bei einem Netzausfall soll die USV den Betrieb der Server solange aufrechterhalten, bis die Akkus eine Restladung von 35 % erreicht haben. Danach sollen die Server kontrolliert heruntergefahren werden.

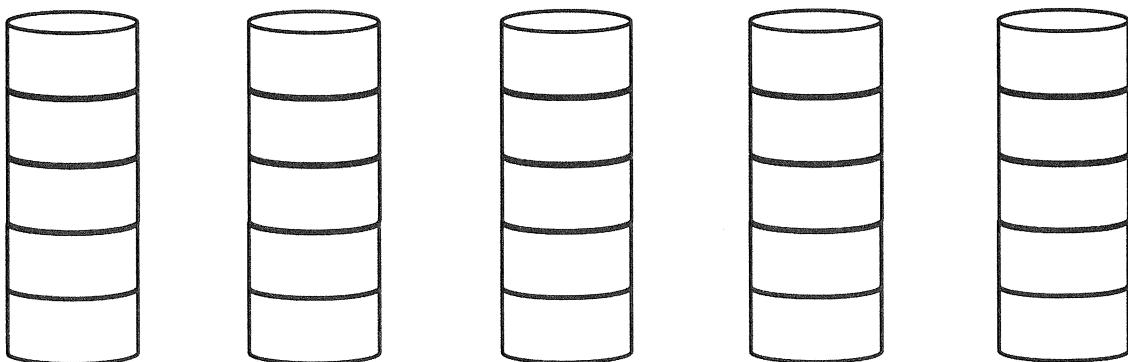
Ermitteln Sie die Zeit, in der der Server bis zum Herunterfahren mit Energie versorgt werden kann, in vollen Minuten. 4 Punkte

- e) Sie sollen in der Event GmbH ein logisches Laufwerk mit einem RAID 6-Verbund einrichten. Dazu stehen Ihnen fünf Festplatten mit je 1,2 TiB zur Verfügung.

ea) Stellen Sie das Prinzip der Datenhaltung in diesem RAID 6-Verbund schematisch dar.

Tragen Sie deutlich die Verteilung der Blöcke und den Verbund der fünf Festplatten ein.

5 Punkte



eb) Berechnen Sie die Nettospeicherkapazität dieses RAID 6-Verbunds.

3 Punkte

Korrekturrand

4. Handlungsschritt (25 Punkte)

Bei der Event GmbH soll der IT-Betrieb auf Sicherheit überprüft werden.

a) Bei der Überprüfung werden alle Maßnahmen der IT-Sicherheit betrachtet. Zusätzliche Maßnahmen sollen eingeführt werden.

Ergänzen Sie die Tabelle um jeweils eine weitere entsprechende Maßnahme.

6 Punkte

Aspekt	Maßnahme	Erläuterung
Logisch (Software)	Netzwerk-Firewall	Schutz vor Angriffen aus dem Netz, da nur definierte Ports/Adressen passieren können.
Logisch (Software)		
Organisatorisch (Geschäftsprozesse)	Benutzerschulung	Durchführung einer Datenschutzunterweisung. Mitarbeiter wissen, wie mit Daten umgegangen werden muss.
Organisatorisch (Geschäftsprozesse)		
Physikalisch (Bauliche Maßnahme)	Backup-Server in anderen Brandabschnitt	Bei Brand im Gebäude sind die Daten noch an anderen Ort vorhanden.
Physikalisch (Bauliche Maßnahme)		

b) Zur Absicherung des Datenverkehrs zum Internet wird eine DMZ eingesetzt.

Beschreiben Sie, warum es sinnvoll ist, die Homepage auf einem Webserver in der DMZ zu hosten.

3 Punkte

Fortsetzung 4. Handlungsschritt

Korrekturrand

- c) Die Event GmbH betreibt zum Aufspüren von Angriffen einen Honeypot.

Erklären Sie kurz die Funktionsweise eines Honeypot.

3 Punkte

- d) Das Netzwerk soll durch entsprechende Firewall-Regeln abgesichert werden.

Die Event GmbH schützt ihr Netz mithilfe einer DMZ, bei der eine Stateful Packet Inspection (SPI) als äußere Firewall zum Einsatz kommt.

Dazu wurde die Regel 1 aufgestellt.

Ergänzen Sie die übrigen Regeln, um den VLANs Verwaltung und Entwicklung die Protokolle HTTPS, DNS, SMTP und POP3 zu erlauben. Dem Management-VLAN wird unbeschränkter Zugriff auf das Internet gegeben. Der übrige Datenverkehr wird verboten.

8 Punkte

Hinweis:

Die Anzahl der Lösungszeilen lässt keinen Rückschluss auf die benötigten Regeln zu.

Nr	Aktion	Protokoll	Quell-IP	Ziel-IP	Q-Port	Z-Port	Von Interface	Nach Interface
1	Permit	TCP	VLAN-Verw, VLAN-Entw	Any	>1024	80	LAN	WAN

- e) Der Webauftritt der Event GmbH wird dynamisch aus Datenbankinhalten und Formularen erzeugt. Der Webserver der Event GmbH ist durch eine SPI-Firewall geschützt. Trotz dieses Schutzes ist es Angreifern gelungen, Daten bzw. Schadcode einzuspielen.

Beschreiben Sie eine mögliche Angriffsmethode und warum die SPI-Firewall gegen diese keinen Schutz bietet.

5 Punkte

5. Handlungsschritt (25 Punkte)

Korrekturrand

Die Event GmbH verwaltet alle ihre Benutzer in einer zentralen Datenbank.

- a) Neue Benutzer werden per Skript aus einer csv-Datei in diese Datenbank importiert. Die csv-Datei „NeueBenutzer.csv“ hat folgenden Aufbau:

```
Vorname;Name;Abteilung
Alfred;Huber;Verwaltung
Maria;Maier;Verwaltung
Werner;Schmidt;Entwicklung
Wilhem;Thor;Administration
```

Das Anlegen der Benutzer erfolgt mit folgendem Skript:

```
#Schriftt 1:
$ImportDatei = "NeueBenutzer.csv"
$Vorname = ""
$Nachname = ""
$Abteilung = ""
$HomeDirectory = ""

#Schriftt 2:
$Users = Import-CSV -Delimiter ';' $ImportDatei

#Schriftt 3:
foreach ($User in $Users)
{
    $Vorname = $User."Vorname"
    $Nachname = $User."Nachname"
    $Abteilung = $User."Abteilung"
    $HomeDirectory = "\server\user\$Abteilung\$Nachname"

#Schriftt 4:
    New-User      -Name $Nachname -GivenName $Vorname
                  -HomeDirectory $HomeDirectory -HomeDrive "H:"

#Schriftt 5:
    mkdir $HomeDirectory
}
```

Kommentieren Sie für die Dokumentation des Codes die einzelnen Schritte:

10 Punkte

Schritt	Kommentar
1	
2	
3	
4	
5	

Fortsetzung 5. Handlungsschritt →

Fortsetzung 5. Handlungsschritt

Korrekturrand

- ab) Das Benutzerpasswort wird in der Datenbank nicht im Klartext, sondern als Hashwert abgespeichert.

Erläutern Sie, warum es sinnvoll ist, das Passwort als Hashwert zu speichern.

3 Punkte

- ac) Die Unternehmensleitung beschließt, die Passwortsicherheit zu erhöhen.

Erläutern Sie zwei Maßnahmen, mit denen die Passwortsicherheit erhöht werden kann.

4 Punkte

- b) Die Administratoren der Event GmbH möchten ihrem Provider, der iKomP AG, Remotezugriff auf den Router zu Wartungszwecken ermöglichen.

- ba) Dazu wurde auf einem Notebook der iKomP AG ein VPN-Client mit folgender Konfiguration eingerichtet.

Erläutern Sie die Bedeutung der fett markierten Begriffe (siehe Beispiel):

6 Punkte

dev tun	VPN-Modus: Tunnelmodus
cipher AES-256	
auth SHA	
remote 80.90.100.2	

- bb) Für die IPsec-VPN-Verbindung wird die MTU auf 1.400 Byte heruntergesetzt.

Erläutern Sie, warum diese Maßnahme sinnvoll ist.

2 Punkte

PRÜFUNGSZEIT – NICHT BESTANDTEIL DER PRÜFUNG!

Wie beurteilen Sie nach der Bearbeitung der Aufgaben die zur Verfügung stehende Prüfungszeit?

- [1] Sie hätte kürzer sein können. [2] Sie war angemessen. [3] Sie hätte länger sein müssen.

