Abschlussprüfung Winter 2019/20
Lösungshinweise

Fachinformatiker/Fachinformatikerin
Systemintegration
1197

1 Ganzheitliche Aufgabe I
Fachqualifikationen

Allgemeine Korrekturhinweise

Die Lösungs- und Bewertungshinweise zu den einzelnen Handlungsschritten sind als Korrekturhilfen zu verstehen und erheben nicht in jedem Fall Anspruch auf Vollständigkeit und Ausschließlichkeit. Neben hier beispielhaft angeführten Lösungsmöglichkeiten sind auch andere sach- und fachgerechte Lösungsalternativen bzw. Darstellungsformen mit der vorgesehenen Punktzahl zu bewerten. Der Bewertungsspielraum des Korrektors (z. B. hinsichtlich der Berücksichtigung regionaler oder branchenspezifischer Gegebenheiten) bleibt unberührt.

Zu beachten ist die unterschiedliche Dimension der Aufgabenstellung (nennen – erklären – beschreiben – erläutern usw.). Wird eine bestimmte Anzahl verlangt (z. B. „Nennen Sie fünf Merkmale …“), so ist bei Aufzählung von fünf richtigen Merkmalen die volle vorgesehene Punktzahl zu geben, auch wenn im Lösungshinweis mehr als fünf Merkmale genannt sind. Bei Angabe von Teilpunkten in den Lösungshinweisen sind diese auch für richtig erbrachte Teilleistungen zu geben.

In den Fällen, in denen vom Prüfungsteilnehmer

- keiner der fünf Handlungsschritte ausdrücklich als „nicht bearbeitet“ gekennzeichnet wurde,
- der 5. Handlungsschritt bearbeitet wurde,
- einer der Handlungsschritte 1 bis 4 deutlich erkennbar nicht bearbeitet wurde,

ist der tatsächlich nicht bearbeitete Handlungsschritt von der Bewertung auszuschließen.

Ein weiterer Punktabzug für den bearbeiteten 5. Handlungsschritt soll in diesen Fällen allein wegen des Verstoßes gegen die Formvorschrift nicht erfolgen!

Für die Bewertung gilt folgender Punkte-Noten-Schlüssel:

Note 1	=	100 – 92 Punkte	Note 2	= unter	92 – 81 Punkte
Note 3	= unter	81 – 67 Punkte	Note 4	= unter	67 – 50 Punkte
Note 5	= unter	50 – 30 Punkte	Note 6	= unter	30 – 0 Punkte

1. Handlungsschritt (25 Punkte)

aa) 4 Punkte
- Flexiblere Nutzung der physischen Infrastruktur
- Begrenzung von Datenverkehr durch Verkleinerung der Broadcastdomänen
- Priorisierung von Datenverkehr (QoS, z. B. VoIP)
- Erhöhte Sicherheit durch Zugriffsregeln zwischen den VLANs
- u. a.

ab) 3 Punkte
12 Bit für die VLAN-ID → $2^{12} = 4.096$ VLANs

ac) 4 Punkte
VLAN-Tags sind notwendig, damit der nächste Switch erkennt, welchem VLAN er die ankommenden Frames zuordnen muss.

b) 6 Punkte

VLAN	Netz-ID	Anzahl Hosts	Subnetzmaske	Default-Gateway
Verwaltung	192.168.10.0	54	**255.255.255.192**	**192.168.10.62**
Entwicklung	192.168.20.0	28	**255.255.255.224**	**192.168.20.30**
Management	192.168.40.0	5	**255.255.255.248**	**192.168.40.6**

ca) 4 Punkte
Die Default-Route ins Internet fehlt. Eintrag von
```
0.0.0.0 0.0.0.0 172.16.31.1
oder 0.0.0.0 0.0.0.0 FastEthernet0/8
```

cb) 4 Punkte
192.168.0.0/19 deckt als Superroute nur den IP-Bereich von 192.168.0.0 – 192.168.31.255 ab. Darin ist aber das Netz 192.168.40.0 für das VLAN 40 (Management) nicht enthalten.

2. Handlungsschritt (25 Punkte)

a) 4 Punkte
Hinweis: Der Lösungsvorschlag enthält mehr Markierungen als gefordert, da zum Teil mehrere Hilfsprogramme geeignet sind.

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

b) 5 Punkte (3 Punkte für die Erläuterung, 2 Punkte für das Beispiel)
Durch Setzen des Parameters –f verhindern, dass fragmentiert wird. Nun werden die Werte für den Parameter –l solange erhöht bzw. vermindert, bis der Ping-Befehl die Meldung zurückgibt, dass das Paket fragmentiert werden müsste bzw. ohne diese Meldung durchläuft.

Beispiel: `ping -f -l 1470 www.future-gmbh.de`

c) 4 Punkte (3 x 1 Punkt je Begriff, 1 Punkt für den Gesamtzusammenhang)
Jedes SNMP-fähige Gerät (Router, Switch, Drucker, Server usw.) speichert lokal wichtige Informationen über seinen Betriebszustand in der „Management Information Base (MIB)".

Der Administrator kann von seinem Rechner aus mit dem Befehl „Get-Request" auf die MIB der Geräte zugreifen. Zur Authentifizierung dient der sogenannte „Community-String".

d) 5 Punkte
2 % von 10 Mbit/s = 200.000 bit/s und entsprechen 25.000 Byte/s
Die Komponenten 1 benötigen 10 * 1.000 Byte/s = 10.000 Byte/s
Somit verbleiben 25.000 Byte/s – 10.000 Byte/s = 15.000 Byte/s für die Komponenten 2.
15.000 Byte/s geteilt durch 500 Byte/s ergibt 30

Es können noch **30 Geräte** der Kategorie 2 überwacht werden.

ea) 4 Punkte
AnteilTCP = ((AnzEndeTCP – AnzStartTCP) / (AnzEndeIP – AnzStartIP)) * 100;
2 Punkte 2 Punkte

eb) 3 Punkte
KOPIEREN AnzEndeTCP nach AnzStartTCP;
KOPIEREN AnzEndeUDP nach AnzStartUDP;
KOPIEREN AnzEndeIP nach AnzStartIP;

Hinweis: Die Reihenfolge der Anweisungen ist beliebig!

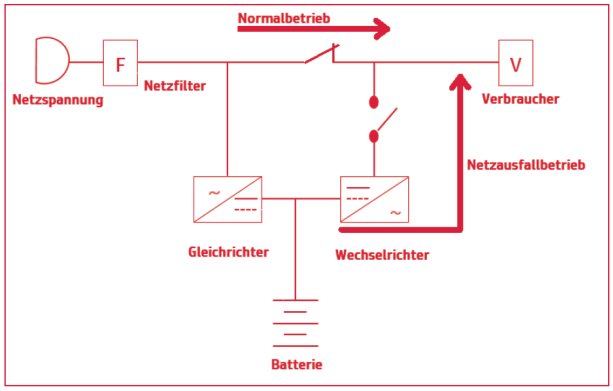
3. Handlungsschritt (25 Punkte)

a) 3 Punkte
- Server auf einer Steckkarte, die Prozessoren, Speicher, integrierte Netzwerk-Controller, optional einen Fiber Channel Host Bus Adapter (HBA) und andere Input/Output-(IO-)Ports umfasst
- Ermöglichen eine höhere Verarbeitungsleistung auf einer geringeren Rack-Standfläche
- Vereinfachte Verkabelung
- Reduzierter Stromverbrauch
- u. a.

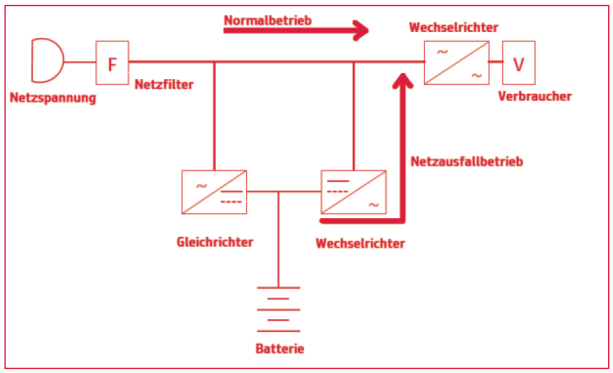
b) 3 Punkte
- LTS (Long Term Support)
- Eine über das übliche Maß hinausgehende Versorgung des Betriebssystems mit Aktualisierungen, die üblicherweise zur Behebung von sicherheitskritischen Programmfehlern gedacht sind.
- Aktualisierungen werden auch bei Erscheinen eines neueren Versionszweiges noch weiterhin entwickelt und angeboten.
- u. a.

c) 7 Punkte
3 x 1 Punkt für die Bezeichnungen
2 x 2 Punkte für die Schutzeigenschaften

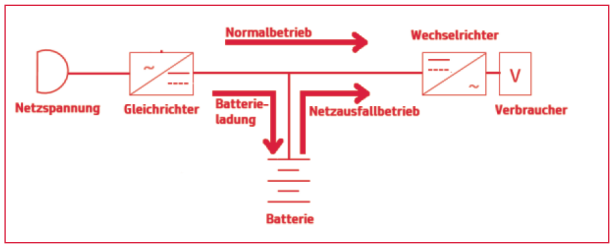
VFD (Voltage Frequency Dependent from Mains Supply); Standby- oder Offline-USV



VI (Voltage Independent from Mains Supply); Line Interactive-USV, Hybrid- oder Netzinteraktive USV



VFI (Voltage and Frequency Independent from Mains Supply) – Dauerwandler- oder Online-USV



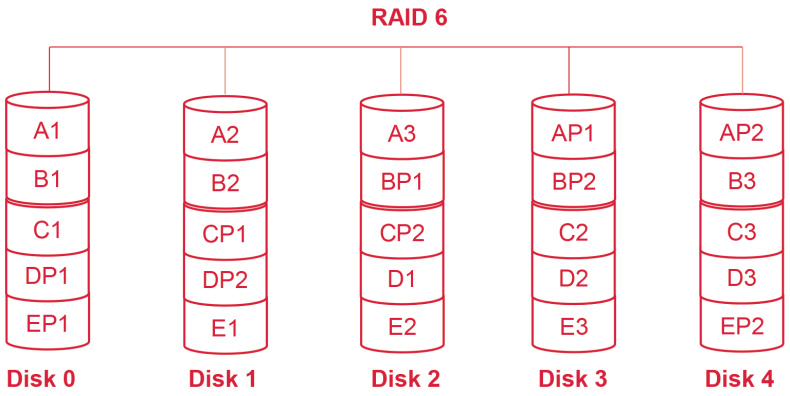
- Erzeugen ständig eine eigene Netzspannung
- Angeschlossene Verbraucher werden dauerhaft mit Netzspannung versorgt und zeitgleich werden die Akkus bzw. Batterien aufgeladen
- Keine Störspannungen, elektromagnetische Einflüsse, Frequenzstörungen und Spannungsverzerrungen

d) 4 Punkte
3 * 750 VA = 2.250 VA

t(h) = 24 *12 V * 3,6 Ah * 0,65 / 2.250 VA = 0,29952 h

Umrechnung in Minuten: 0,29952 Stunden * 60 Minuten/Stunde = 17,9712 min → 17 ganze Minuten.

ea) 5 x 1 Punkt pro korrekt beschriebener Festplatte (abweichende Darstellung möglich)



Die Verbindung und die Bezeichnung der Disks sind ebenfalls zu berücksichtigen.

Andere sinnvolle Lösungen (z. B. andere Paritätsverteilungen) sind möglich.

eb) 3 Punkte
(5 - 2) HD x 1,2 TiB/HD = 3,6 TiB

HD = Harddisk

4. Handlungsschritt (25 Punkte)

a) 6 Punkte

Aspekt	Maßnahme	Erläuterung
Logisch (Software)	Netzwerk-Firewall	Schutz vor Angriffen aus dem Netz, da nur definierte Ports/Adressen passieren können.
Logisch (Software)	**Virenscanner**	**Schadsoftware kann auf dem Rechner nicht ausgeführt werden.**
Organisatorisch (Geschäftsprozesse)	Benutzerschulung	Durchführung einer Datenschutzunterweisung. Mitarbeiter wissen, wie mit Daten umgegangen werden muss.
Organisatorisch (Geschäftsprozesse)	**Geschäftsprozess für Datensicherung erstellen**	**Es ist geklärt, wer die Datensicherung durchführt und wie zu verfahren ist.**
Physikalisch (Bauliche Maßnahme)	Backup-Server in anderen Brandabschnitt	Bei Brand im Gebäude sind die Daten noch an anderen Ort vorhanden.
Physikalisch (Bauliche Maßnahme)	**Einführung einer Zutrittskontrolle mittels Chipkarte**	**Nur berechtigte Personen können Gebäude bzw. bestimmte Räume betreten.**

Weitere sinnvolle Lösungen sind möglich.

b) 3 Punkte
Das interne Netz ist durch eine Firewall zur DMZ abgetrennt. Bei einer Kompromittierung des Webservers ist durch diese Firewall eine Abgrenzung zum internen Netz gegeben. Der Angreifer hat keinen direkten Zugriff auf das interne Netz.

c) 3 Punkte
Ein Honeypot ist ein besonders präpariertes System, das einem Angreifer ein verwundbares System vorspielt. Alle Aktivitäten eines Angreifers werden aufgezeichnet. Aus den Aufzeichnungen kann die Vorgehensweise rekonstruiert werden. Dies kann genutzt werden, um Schwachstellen zu analysieren, Gegenmaßnahmen zu entwickeln oder Beweise für strafrechtliche Schritte zu sammeln.

d) 8 Punkte

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
2	**Permit**	**TCP**	**VLAN-Verw, VLAN-Entw**	**Any**	**>1024**	**443**	**LAN**	**WAN**
3	**Permit**	**UDP**	**VLAN-Verw, VLAN-Entw**	**Any**	**>1024**	**53**	**LAN**	**WAN**
4	**Permit**	**TCP**	**VLAN-Verw, VLAN-Entw**	**Any**	**>1024**	**25**	**LAN**	**WAN**
5	**Permit**	**TCP**	**VLAN-Verw, VLAN-Entw**	**Any**	**>1024**	**110**	**LAN**	**WAN**
6	**Permit**	**IP**	**VLAN-Management**	**Any**	**-**	**-**	**LAN**	**WAN**
7	**Deny**	**IP**	**Any**	**Any**	**-**	**-**	**LAN**	**WAN**

e) 5 Punkte
Code Injection:
Bei dynamisch erzeugten Webseiten werden Rückgabewerte aus Formularen oder Seitenaufrufen durch eine Skriptsprache oder Programmcode erzeugt. Wenn nun Schadcode durch präparierte Formular- oder Rückgabewerte an den Server gesendet wird, bekommt die Firewall nichts mit, da eine Paketfilterfirewall auf Schicht 3 und 4 arbeitet. Die Seiteninhalte auf höherer Schicht wird werden gültiger Inhalt betrachtet. Durch die Skriptsprache auf den Server kann der Schadcode ausgeführt werden.

SQL-Injection:
Versuch, über Eingabefelder SQL-Befehle zu übergeben, um Benutzernamen, Passwörter und andere Informationen auslesen zu können. Davon bekommt die Firewall nichts mit, da eine Paketfilter-Firewall auf Schicht 3 und 4 arbeitet.

Andere Lösungen sind möglich!

5. Handlungsschritt (25 Punkte)

aa) 10 Punkte

Schritt	Kommentar
1	Initialisierung der Variablen (1 Punkt)
2	Spaltenweises Einlesen der Importdatei anhand des Trenners „;“ in die Variable $users (2 Punkte)
3	Zeilenweises Lesen der Variablen $users und Füllen der Variablen $Vorname, $Name, $Abteilung und $Homeverzeichnis (3 Punkte)
4	Anlegen des Benutzers mit den Eigenschaften Vorname, Name und Homeverzeichnis, Setzen des Homelaufwerks auf H: (3 Punkte)
5	Anlegen des Homeverzeichnisses (1 Punkt)

ab) 3 Punkte

- Aus dem Hashwert kann nicht auf das Passwort geschlossen werden.
- Bei der Prüfung von Benutzernamen und Passwort kann der Passwort-Hashwert über das Netz übermittelt werden, der mit dem Passwort-Hashwert verglichen werden kann.

ac) 4 Punkte

- Erzwingen einer Passwortchronik
- Ablaufzeit für Passwort
- Passwort muss den Komplexitätsbedingungen entsprechen
- u. a.

ba) 6 Punkte

`dev tun`	`VPN-Modus: Tunnelmodus`
`cipher AES-256`	`Verschlüsselung mit AES`
`auth` **`SHA`**	`Authentifizierung und Integrität mit SHA`
`remote 80.90.100.2`	`IP des VPN-Partners`

bb) 2 Punkte

Maßnahme ist sinnvoll, da bei einer kleineren MTU weitere Informationen (z. B. Authentifizierung, Integrität) im Paket untergebracht werden können, ohne dass Pakete fragmentiert werden müssen.