

# 1 Konzeption und Administration von IT-Systemen

## 1.1 Aufgabe 1

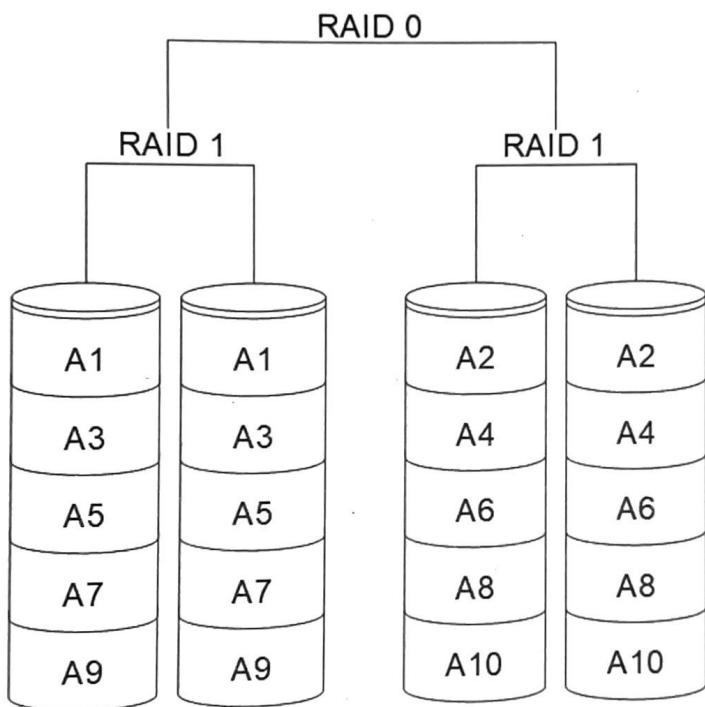
aa)

Technisches Merkmal	Möglicher Wert
Unterstützte RAID-Level	0, 1, 10, 5, 6, 50, 60
Größe des Cache	z. B. 1024 MiB
Anzahl HDD/SSD-Anschlüsse	z. B. 16 Festplatten / SSDs
Art der Schnittstelle	z. B. PCIe Gen3
Durchsatz des Controllers	z. B. 6 Gbit/s
...	...

ab) Der gesuchte RAID-Level ist **RAID 10**.

Weiterführende Informationen (für das Erreichen der beiden Punkte nicht notwendig):

### RAID 1 + 0



RAID 10 ist eine Kombination aus RAID 0 (Disk-Striping) und RAID 1 (volle Redundanz durch Spiegelung), hierdurch kann eine höchstmögliche Datenrate bei Schreiboptionen sowie ein fehlertoleranter Betrieb gewährleistet werden.

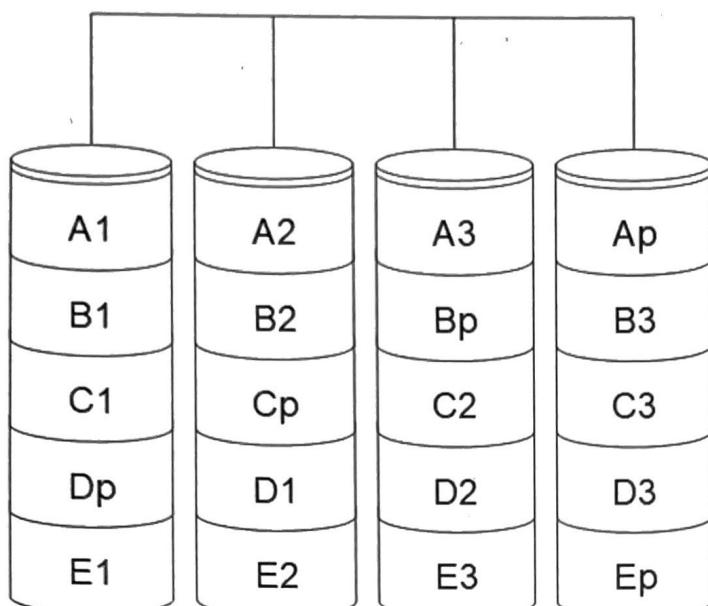
Es bietet eine hohe Redundanz bei guter Performance. Besonders geeignet ist es für Input-/Output-intensive Anwendungen, es steht eine Nettokapazität von 50 % zur Verfügung.

- ac) Der gesuchte RAID-Level ist **RAID 5**.

RAID 4 könnte auch gewählt werden. Hierbei werden die Paritäten jedoch nicht auf alle verfügbare Festplatten aufgeteilt.

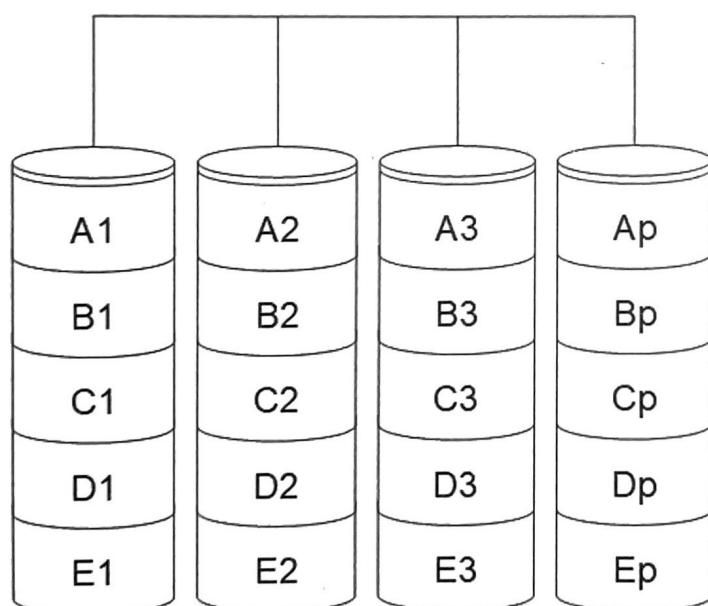
Weiterführende Informationen (für das Erreichen der beiden Punkte nicht notwendig):

**RAID 5**



RAID 5 kann bei mindestens 3 Festplatten eingesetzt werden. Die Lesegeschwindigkeit ist durch parallele Zugriffe sehr hoch. Die Schreibgeschwindigkeit ist leicht verringert durch die Berechnung der Parity Information. Die Nettospeicherkapazität entspricht der Bruttospeicherkapazität abzüglich der Kapazität einer Festplatte des Verbundes.

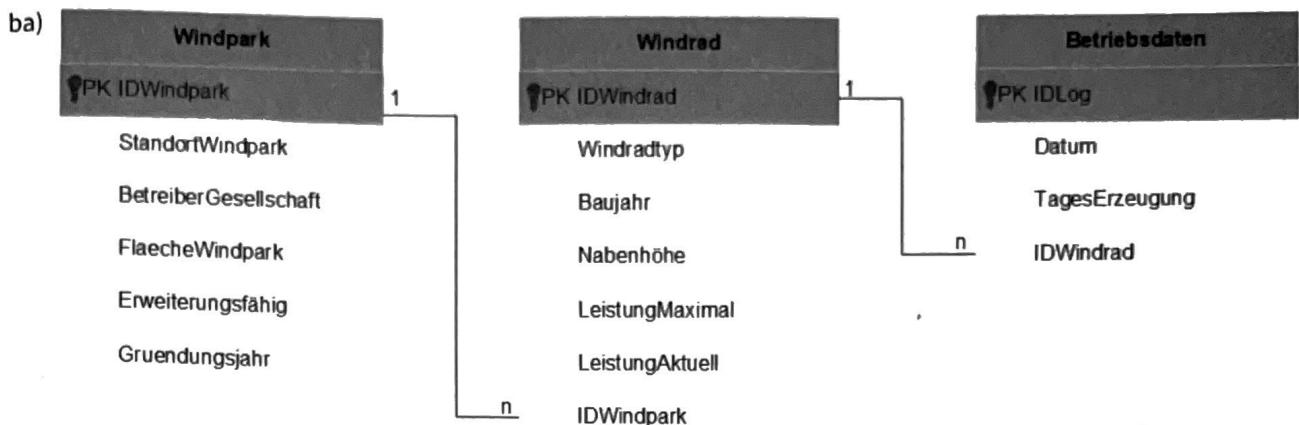
**RAID 4**



RAID 4 funktioniert analog zu RAID 5, verteilt die Paritätsinformationen jedoch nicht auf mehrere Festplatten. Im Idealfall sollte bei einer Entscheidung zwischen RAID 5 und RAID 4 immer RAID 5 bevorzugt werden – RAID 4 wird heutzutage nur noch sehr selten verwendet.

- ad) Um verfälschte Testergebnisse auszuschließen, sollte auf Folgendes geachtet werden:

- Nichtbenötigte Dienste und Programme müssen beendet werden.
- Der Test sollte in einem separaten Netzwerk / einer separaten Umgebung durchgeführt werden.
- Die Test-Umgebung sollte fehlerfrei sein.
- Der Testaufbau sollte möglichst realitätsnah erfolgen.
- Die Tests sollten so ausgewählt werden, dass sie praxisgerecht sind.



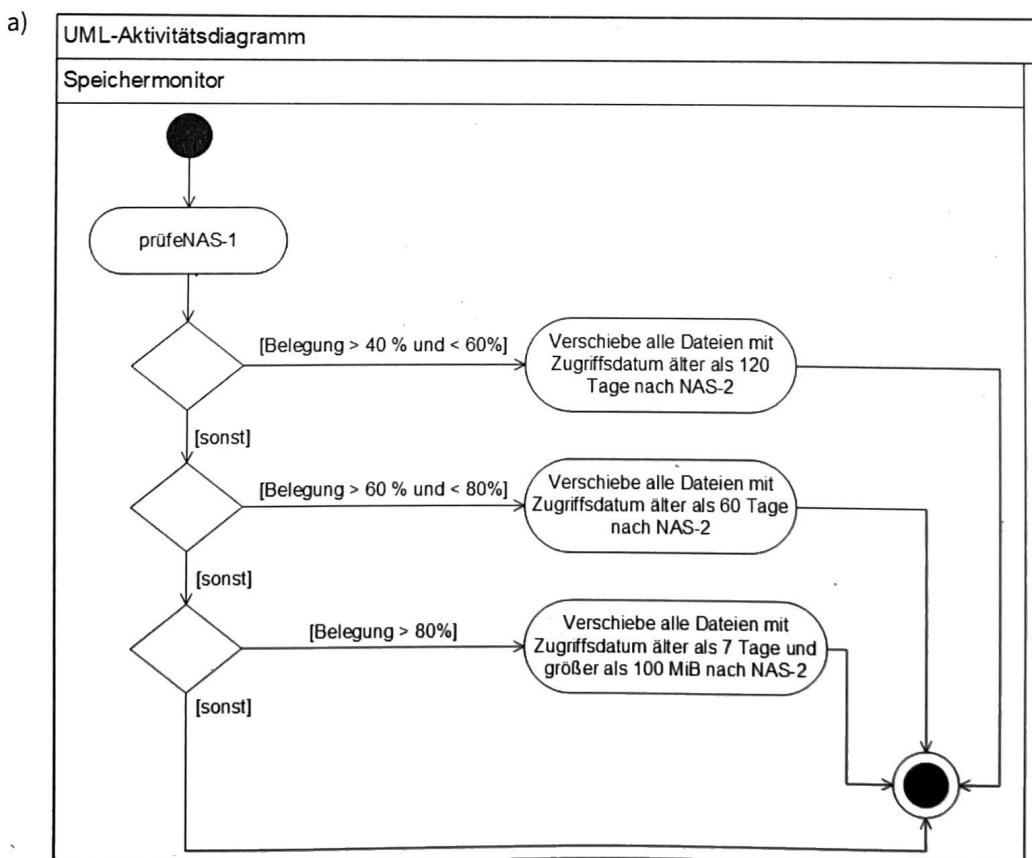
Schreibweise: 1 : n oder 1 :  $\infty$

- bb) Die Aktivierung der Check-Box „Mit referentieller Integrität“ erfolgt, um inkonsistente Zustände der Datenbank möglichst zu verhindern. Dazu zählen sogenannte Einfüge-, Lösch- und Änderungsanomalien. Die referentielle Integrität trägt somit zur Sicherstellung der Datenintegrität bei relationalen Datenbanken bei.
- bc) 

```
SELECT count(*)
FROM Windrad
WHERE IDWindpark = 102;
```
- bd) 

```
SELECT top 3
IDWindrad
FROM Betriebsdaten
WHERE IDWindpark = 102
AND Datum = „2022.05.03“
ORDER BY TagesErzeugung DESC;
```

## 1.2 Aufgabe 2



b)	Zeile 1	int [] werte = { 30, 24, 12, 50, 11, 49, 11 }; //Beispielwerte
	Zeile 2	int temp; //Variable zum Zwischenspeichern
	Zeile 3	len = werte.Length; // len entspricht der Länge des Arrays
	Zeile 4	for (int p = 0; p <= len - 2; p++) { // äußere Schleife
	Zeile 5	<b>for (int i = 0; i &lt;= len - 2 - p; i++) {</b> // innere Schleife
	Zeile 6	<b>if (werte[i] &gt; werte[i + 1]) {</b> // Vergleich der Elemente
	Zeile 7	<b>temp = werte[i + 1];</b> // Tausch der Elemente
	Zeile 8	<b>werte[i + 1] = werte[i];</b> // Tausch der Elemente
	Zeile 9	<b>werte[i] = temp;</b> // Tausch der Elemente
	Zeile 10	}
	Zeile 11	}
	Zeile 12	// Ende innere Schleife
		// Ende äußere Schleife

### 1.3 Aufgabe 3

- a) Vorteile für die Anbindung über WLAN:
- Kabellose Verbindungsart
  - Flexible Positionierung der Webcams möglich
  - Schnelle und einfache Installation
  - Einfache Zuweisung an Accesspoints
  - Günstige Implementierung
  - ...

ba)	Einsatzzweck	Webcam	Begründung
	24-stündige Überwachung des Außengeländes mit Publikumsverkehr	Neocam BVR	<ul style="list-style-type: none"> <li>- Nachtsichtmodus (Infrarot)</li> <li>- Schutz vor Vandalismus</li> <li>- Bewegungserkennung</li> </ul>
	Webkonferenzen bei höchster Bildqualität	XoCam z1	<ul style="list-style-type: none"> <li>- Höchste Qualität (Auflösung 4K)</li> </ul>
	Überwachung des Serverraums bei sicherster Verschlüsselungsmethode	CamHD-Sec	<ul style="list-style-type: none"> <li>- Passwortgeschützter Zugriff</li> <li>- Neuste Verschlüsselungsmethode (WPA3)</li> </ul>

- bb) Berechnung der Gesamtpixel:  
 $1.920 \text{ Pixel} \cdot 1.080 \text{ Pixel} = 2.073.600 \text{ Pixel}$
- Berechnung der Gesamtbit:  
 $2.073.600 \text{ Pixel} \cdot 16 \text{ Bit/Pixel} = 33.177.600 \text{ Bit}$
- Berechnung der Bit pro Sekunde:  
 $33.177.600 \text{ Bit} \cdot 10 \text{ Bilder/s} = 331.776.000 \text{ Bit/s}$

Berechnung der MiB pro Sekunde:  
 $331.776.000 \text{ Bit/s} : 8 = 41.472.000 \text{ Byte/s}$   
 $41.472.000 \text{ Byte/s} : 1.024 = 40.500 \text{ KiB/s}$   
 $40.500 \text{ KiB/s} : 1.024 = 39.5507 \text{ MiB/s}$

Berechnung der MiB pro Minute:  
 $39.5507 \text{ MiB/s} \cdot 60 \text{ s} = 2.373,04 \text{ MiB} \rightarrow \mathbf{2.374 \text{ MiB}}$

Die Angaben zur Überwachungszeit pro Tag und die Anzahl der Webcams kann vernachlässigt werden und ist für diese Aufgabe nicht relevant. Es soll lediglich die anfallende Datenmenge für eine Webcam pro Minute in MiB berechnet werden.

**bc) Löschfristen:**

Gespeicherte Daten müssen gelöscht werden, sobald die Verarbeitung nicht mehr zur Zweckerfüllung notwendig ist, etwa wenn die Rechtsgrundlage entfällt (z. B. durch Widerruf der Einwilligung oder wenn der Vertragszweck erfüllt ist).

Näheres regelt Art. 17 DSGVO mit dem Recht auf Löschung, auch als „Recht auf Vergessenwerden“ bezeichnet. Der Verantwortliche soll sich auch im Vorfeld der Datenverarbeitung Gedanken über den „Lebenszyklus“ der Daten machen und in einem Verarbeitungsverzeichnis auch die vorgesehene Frist für die Löschung der verschiedenen Kategorien der Daten festlegen.

*Andere Erläuterungen sind möglich.*

**Persönlichkeitsrecht:**

Bilder, Fotos und Videoaufnahmen von Personen dürfen grundsätzlich nur mit Einwilligung des Abgebildeten verarbeitet oder zugänglich gemacht werden. Das gilt auch für das beschäftigte Personal. Die Datenschutzerklärung des Personals erfolgt im „Opt-in“-Verfahren. Es muss sichergestellt werden, dass die Einwilligung durch eine eindeutige Handlung (elektrisch, in Papierform oder über eine schlüssige Handlung) abgegeben wurde.

*Andere Erläuterungen sind möglich.*

**Zweckbindung:**

Die Aufnahmen der Webcams dürfen für festgelegte, eindeutige und legitime Zwecke erhoben werden. Solange die weitere Verarbeitung der Daten zur Erfüllung einer rechtlichen Verpflichtung erforderlich ist, besteht das Recht der Verarbeitung. Ist der Verarbeitungszweck erfüllt oder erreicht, so besteht die Pflicht zur Löschung (Speicherbegrenzung).

*Andere Erläuterungen sind möglich.*

**1.4 Aufgabe 4**

a)

Sicherheitsmerkmal	Erläuterung
Betriebssystem-Firewall	Schutz des Rechners vor netzinternen Angriffen, [...]
Dateisystem-/Zugriffs-berechtigungen	Schutz der Daten vor unbefugten Zugriffen, auch im laufenden Betrieb; Least-Privilege-Prinzip: Aufgabengerechte Vergabe von Berechtigungen
Laufwerksverschlüsselung	Schutz der Daten vor unberechtigten Zugriffen, z. B. bei Diebstahl oder sonstigem Verlust des Geräts
Sicheres bzw. zuverlässiges Löschen von Datenträgern	Statt einer normalen Formatierung: Daten durch mehrfaches Überschreiben löschen
Snapshots/Timeshift bzw. Wiederherstellungspunkte	Bereitstellung von Recoverymaßnahmen zum Sichern und Wiederherstellen
Logs	Verschiedene Systemlogs zur Überwachung von Zugriffen und Dokumentation von Änderungen

b) Eine Betriebssystemhärtung könnte zum Beispiel erfolgen durch...

- die Deaktivierung nicht benötigter Softwarekomponenten (z. B. Remotezugriff, FTP, Webzugriff),
- die Deaktivierung von unsicheren oder veralteten Schnittstellen, Autostart-Mechanismen und Hintergrunddiensten,
- die Beschränkung der laufenden Dienste auf einen Betrieb unter minimalen Rechten,
- die Nutzung von Verschlüsselung,
- die Anpassung der Dateisystemrechte und ihrer Vererbung (insbesondere für Konfigurationsdateien des Betriebssystems),
- ...

c)

	<b>Hypervisor Typ-1</b>	<b>Hypervisor Typ-2</b>
Erläuterung	<b>Nativer / Bare-metal Hypervisor</b> <ul style="list-style-type: none"> <li>- Virtualisierungssoftware, die direkt auf der Hardware-Ebene aufsetzt</li> </ul>	<b>Gehosteter Hypervisor</b> <ul style="list-style-type: none"> <li>- setzt auf einem bereits installierten Betriebssystem auf</li> </ul>
Einsatzbeispiel	<ul style="list-style-type: none"> <li>- mehrheitlich in Rechenzentren zur Bereitstellung von Servern verwendet</li> </ul>	<ul style="list-style-type: none"> <li>- Einsatz größtenteils im Bereich von Arbeitsplätzen und im privaten Umfeld zum Test und zur Entwicklung von Software</li> </ul>
Bsp. für marktgängige Produkte	<ul style="list-style-type: none"> <li>- KVM</li> <li>- VMware vSphere</li> <li>- Microsoft Hyper-V</li> <li>- Xen</li> </ul>	<ul style="list-style-type: none"> <li>- Parallels</li> <li>- VMware Workstation (Player / Pro)</li> <li>- VirtualBox (Oracle)</li> <li>- VMware Fusion</li> </ul>

d) Zwei Lösungen möglich:

```
copy *2022040?.log X:\debug
oder
copy *2022040*.log X:\debug
```

ea) Beim **differentiellen** Backup werden zunächst alle Daten vollständig kopiert (Voll-Backup). Anschließend erfolgt eine zusätzliche Sicherung aller Daten, die **seit dem letzten Voll-Backup** geändert wurden. Neu erstellte Dateien, aktualisierte sowie anderweitig veränderte Daten werden hierdurch berücksichtigt. Zyklisch wird das Voll-Backup erneuert. Die Größe der differentiellen Sicherungen wächst mit jeder zusätzlichen Sicherung an.

Beim **inkrementellen** Backup werden zunächst alle Daten vollständig kopiert (Voll-Backup). Anschließend erfolgt eine zusätzliche Sicherung aller Daten, die **nach der jeweils letzten Sicherung** geändert wurden. Neu erstellte Dateien, aktualisierte sowie anderweitig veränderte Daten werden hierdurch berücksichtigt. Die letzte Sicherung kann ein Voll-Backup oder eine zusätzliche Sicherung sein. Zyklisch wird das Voll-Backup erneuert. Die Größe der inkrementellen Sicherungen bleibt bei gleichbleibenden Änderungen am Dateisystem relativ ähnlich.

eb) Beim Aufruf des Programms fehlt die entsprechende Pfadangabe zur Ausführung. Um das Problem zu lösen, sollte entweder die Pfadangabe beim Programmaufruf mit angegeben werden (C:\Backup\qbackup) oder die Umgebungsvariable %path sollte um C:\Backup ergänzt werden.

## 2 Analyse und Entwicklung von Netzwerken

### 2.1 Aufgabe 1

aa) Netz-ID:	203.0.113.160
Erste mögliche Host-IP:	203.0.113.161
Letzte mögliche Host-IP:	203.0.113.190
Broadcast:	203.0.113.191
Subnetzmaske (dezimal):	255.255.255.224

Die Werte ergeben sich aus der Kombination der gegebene IP-Adresse mit der Subnetzmaske 255.255.255.224 (203.0.113.180/27).

ab) Für das Subnetting steht der Bereich ab dem 56. Bit zur Verfügung. Die letzten 64 Bit dürfen nicht verwendet werden. 64 Bit – 56 Bit = 8 Bit

Mit 8 Bit lassen sich 28 Subnetze (also 256) bilden:

Erstes Netz: 2001:db8:ca::/64

Host-Adress-Range: 2001:db8:ca:: - 2001:db8:ca::

Letztes Netz: 2001:db8:ca:ff::/64eg

Host-Adress-Range: 2001:db8:ca:ff:: - 2001:db8:ca:ff::

Die Host-Adress-Range muss nicht angegeben werden und dient nur zur weiterführenden Erklärung.

	Öffentliche IPv4-Adresse	Private IPv4-Adresse	Global-Unicast IPv6-Adresse	Link-Local IPv6-Adresse
Herr Meier	X		X	
Frau Schmitt		X	X	
Herr Pfeiffer		X	X	

Weiterführende Erklärung:

Adressbereiche privater IP-Adressen:

- Klasse A: 10.0.0.0 – 10.255.255.255
- Klasse B: 172.16.0.0 – 172.31.255.255
- Klasse C: 192.168.0.0 – 192.168.255.255

Global-Unicast-Adressen sind weltweit einmalige Adressen, die weltweit geroutet werden. Sie werden vom Netzwerkgerät benötigt, um eine Internetverbindung aufzubauen.

Link-Local-Adressen sind immer nur innerhalb von lokalen Netzwerken gültig und beginnen mit dem Formatpräfix FE80::/10

	IPv4 only	IPv6 only	Dual Stack
Herr Meier			X
Frau Schmitt			X
Herr Pfeiffer			X

Alle Mitarbeiter haben sowohl eine IPv4- als auch eine IPv6-Adresse zugewiesen bekommen.

bc)	Herr Meier	Frau Schmitt	Herr Pfeiffer
Mobilfunk			X (LTE-Router)
Telefonkabel	X (Kabelanschluss DOCSIS)		
Koaxialkabel		X (DSL-Anschluss)	

ca) VPN steht für Virtual Private Network.

Es handelt sich hierbei um ein geschlossenes logisches Netzwerk, bei dem eine verschlüsselte Verbindung von Endgeräten bzw. Netzwerken zu anderen Endgeräten / Netzwerken hergestellt wird.

cb) Besonders für den sicheren Datenverkehr sensibler Unternehmensdaten wird häufig aufgrund der erhöhten Anforderungen an den Datenschutz sowie die Datensicherheit auf VPN-Verbindungen gesetzt. Das Risiko von Datenlecks wird so auf ein Minimum reduziert.

Für den Verbindungsaufbau über das VPN wird häufig ein separater Benutzername sowie ein zugehöriges Passwort benötigt. So kann sichergestellt werden, dass nur berechtigte Mitarbeiter Zugriff auf die Daten der Versicherung haben.

Traffic des Mitarbeiters, der für externe Netze bestimmt ist (z. B. für das Internet) kann so von der Versicherung überwacht und beispielsweise auf Schadsoftware gefiltert werden.

cc) Rechnung:

$$2^{15} = 32.768 \text{ Netze mit jeweils 2 IP-Adressen}$$

Erläuterung:

Laut dem vorliegenden Ausschnitt zum RFC 3021 können Netze der Größe /31 genutzt werden, da im Netzwerk für eine Punkt-zu-Punkt Verbindung keine eigene IP-Adresse für die Netz-ID und die Broadcast-Adresse benötigt wird.

Unter der Angabe 172.20.0.0/16 stehen somit 15 Bit für das Subnetting zur Verfügung (/31 - /16 = /15).

## 2.2 Aufgabe 2

- aa) – Frequenzband der Access-Points  
   – Anzahl und Verteilung der Access-Points  
   – Site Survey vor Ort (Messung wichtiger Parameter, Festlegung und Dokumentation)  
   – Verschlüsselungsstandard  
   – Authentifizierungslösung  
   – Unternehmensanbindung  
   – Sonstige Sicherheitsaspekte (z. B. Gastzugang)  
   – ...
- ab) Bei RADIUS handelt es sich um ein sogenanntes Triple-A-System. Hierbei kommen verschiedene Komponenten zum Einsatz.  
    Authentication / Authentifizierung: Die User-Credentials werden überprüft und abgeglichen.  
    Authorization / Autorisierung: Die individuelle User-Berechtigung wird festgelegt und angewandt.  
    Accounting / Protokollierung: Alle Aktivitäten des Users werden protokolliert und eine Log-Datei wird geschrieben.
- ac) RADIUS bietet den Vorteil, dass individuelle Zugangskennungen und -parameter für jeden User vergeben werden können. Diese Informationen lassen sich dank des Services zentral verwalten.  
    Auf einen zentralen Zugangsschlüssel bzw. ein allgemeingültiges Passwort wird verzichtet. Der Zugang zum Netzwerk wird somit weitestgehend eingeschränkt. Durch den personalisierten Zugang wird die Sicherheit im Netzwerk erhöht.  
    Die Capitol-Versicherung kann User vorübergehend sperren, dauerhaft deaktivieren oder Löschen bei Beendigung der Betriebszugehörigkeit.

Technische Voraussetzungen	Erklärung / Begründung
eigene SSID	Das Gast-WLAN ist durch einen eigenen Namen eindeutig identifizierbar und von anderen Netzwerken zu unterscheiden (SSID = Service Set Identifier).
eigener IP-Adressbereich	Durch die logische Trennung des Netzwerkes mithilfe eines eigenen IP-Adressbereiches wird die Verwaltung erleichtert und alle IP-Pakete werden getrennt geroutet.
Captive-Portal (Voucher)	Durch die vorgeschaltete Seite muss zunächst den Bedingungen des Netzwerkes zugestimmt werden. Der anschließende Traffic ist eindeutig einzelnen Nutzern zuzuordnen.

- ad)
- ba) Es werden Beschreibungen zu möglichen Vorteilen eines VLANs erwartet, z. B. zu:  
   – Verkleinerung der Broadcast-Domäne  
   – Verbesserte und erleichterte Konfiguration der logischen Gruppen im Netzwerk  
   – Unabhängigkeit von physikalischer Topologie  
   – Eindeutige Trennung des Traffics eines VLANs zu anderen VLANs  
*Weitere Vorteile sind möglich.*
- bb) Beide Switchports müssen auf VLAN-Tagging gesetzt werden (z. B. 802.1q).
- bc) – Einloggen nur für Geräte erlauben, die im RADIUS-Server in der Gerätedatenbank (z. B. anhand der MAC-Adresse)  
   freigeschaltet und konfiguriert wurden.  
   – Einloggen nur für authentifizierte Nutzer nach IEEE 802.1X bzw. RADIUS, sodass nur zugelassene Endgeräte eine Verbindung aufbauen dürfen (z. B. Cisco Identity Service Engine).  
   – Konfigurieren der Port-Security: Hierdurch kann die Anzahl der MAC-Adressen, welche pro Switchport gespeichert werden dürfen, eingeschränkt werden. Beim Erreichen des Limits erfolgt eine Deaktivierung des Ports.  
*Weitere Lösungen sind möglich.*

### 2.3 Aufgabe 3

a) Es muss sich für die Option „Entschlüsseln und scannen“ entschieden werden. Hierdurch wird der Datenverkehr inhaltlich überprüft. Bei der Option „Nur URL-Filterung“ könnte keine Überprüfung der Inhalte auf Schadsoftware erfolgen. Es handelt sich hierbei lediglich um einen Abgleich der Ziel-URLs mit einer Black- bzw. Whitelist.

b) Der Fehler „NET::ERR\_CERT\_AUTHORITY\_INVALID“ entsteht, da der Proxyserver den Datenverkehr zwischen der Capitol-Versicherung und „https://www.ihk.de“ entschlüsselt, scannt und anschließend wieder mit einem selbst-ausgestellten Zertifikat verschlüsselt (siehe Aufgabe a). Abschließend erfolgt die Weiterleitung des Traffics an den Client.

Das verwendete Zertifikat für die erneute Verschlüsselung ist dem Client nicht bekannt bzw. wurde beim Client nicht als vertrauenswürdig hinterlegt. Der Client stuft die Verbindung daher als nicht privat bzw. nicht sicher ein.

bb) Das Root-Zertifikat des Proxyservers sollte auf dem Client in die Liste der vertrauenswürdigen Stammzertifizierungsstellen aufgenommen werden. Dies kann entweder manuell oder durch eine Gruppenrichtlinie erfolgen.

Alternativ könnte das Root-Zertifikat des Proxyservers durch eine bereits vertrauenswürdige Stammzertifizierungsstelle des Clients signiert werden oder der Benutzer fügt eine dauerhafte Ausnahme für diese explizite Seite hinzu.

ca) Ein Reverse-Proxy ist eine zusätzliche Sicherheitskomponente. Anfragen aus dem Internet werden stellvertretend entgegengenommen und anschließend an einen Web-Server im Hintergrund weitergeleitet.

Funktionen eines Reverse-Proxyservers:

#### Schutz und Verschlüsselung:

Reverse-Proxyserver können Kontrollsystme wie VirensScanner oder Paketfilter beinhalten. Außerdem können Reverse-Proxyserver zur Verschlüsselung des weitergeleiteten Traffics verwendet werden.

#### Anonymisierung:

Der Zugang zum internen Netzwerk kann nur über den Reverse-Proxy aufgebaut werden. Dieser leitet alle Anfragen an die eigentlichen Zielsysteme weiter und agiert nach außen hin so, als ob eine direkte Verbindung mit dem Zielsystem aufgebaut wird.

#### Caching:

Durch den Reverse-Proxy können Serverantworten zwischengespeichert werden. Statische Inhalte wie Bilder oder häufig aufgerufene dynamische Webseiten werden somit im Cache-Speicher des Proxys vorgehalten und bei eventuellen Anfragen schneller an die Clients verteilt. Die Geschwindigkeit der Serverdienste wird hierdurch beschleunigt.

#### Loadbalancing:

Eine einzige URL kann durch einen Reverse-Proxy an mehrere Server im Netzwerk gekoppelt werden. Da ohnehin alle Anfragen über den Reverse-Proxy geleitet werden, kann hier ein Loadbalancing auf die verschiedenen hinterlegten Server erfolgen. Bei einzelnen Ausfällen kann so die Verfügbarkeit der URL weiterhin sichergestellt werden.

#### Kompression:

Eingehende und ausgehende Daten werden durch entsprechende Komprimierungsmethoden (wie z. B. GZIP) komprimiert und die Dateigrößen werden verringert. Hierdurch wird Speicherplatz gespart und die Datenübertragung im Netzwerk wird zusätzlich beschleunigt.

cb) Bei einem DMZ (demilitarisierte Zone) handelt es sich um einen speziell kontrollierten Netzwerkbereich, der zwischen dem internen und dem externen Netzwerk liegt. Die DMZ stellt eine Pufferzone dar, die Netze voneinander trennt und durch erweiterte Firewall- sowie Kommunikationsregeln schützt. Dienste, die von außen erreichbar sein müssen, liegen meistens in der DMZ.

Die DMZ verhindert durch Ihre Pufferfunktion des Weiteren den direkten Durchgriff auf das interne Netzwerk.

**cc) Server, die in die geplante DMZ verschoben werden sollten, sind:**

- Mailserver
- Webserver
- Reverse-Proxy

Begründung: Diese Dienste müssen sowohl aus dem Internet als auch von innen erreicht werden können. Es ist daher sicherer, wenn diese in die DMZ verschoben werden und somit vom internen Netzwerk abgetrennt werden.

**Server, die im internen Netzwerk verbleiben sollten, sind:**

- Datenbankserver
- Active-Directory-Server
- Druckserver
- Applikationsserver

Begründung: Die genannten Dienste müssen nicht von außen erreichbar sein. Sie können daher im internen Netz verbleiben.

**2.4 Aufgabe 4**

- aa) Das „A“ innerhalb von ADSL steht für asymmetric. Hierdurch wird spezifiziert, dass die Bandbreite zwischen Up- und Download unterschiedlich ist. In der Regel steht hierdurch viel mehr Bandbreite für den Download als für den Upload zur Verfügung.

Es ist davon auszugehen, dass bei einer 16 Mbit/s ADSL-Anbindung zwar 16 Mbit/s für den Download, aber nur ca. 1 – 2,4 Mbit/s für den Upload, zur Verfügung stehen.

Die Bandbreite reicht daher – insbesondere, wenn noch weiterer Datenverkehr in Richtung Internet geht – nicht für eine gute Bild- und/oder Tonqualität aus.

- ab) 1.634 MiB in Bit:

$$1.634 \text{ MiB} * 8 \text{ Bit} = 13.072 \text{ MiBit}$$

$$13.072 \text{ MiBit} * 1.024 * 1.024 = 13.706.985.472 \text{ Bit}$$

$$13.706.985.472 \text{ Bit} / 16.000.000 \text{ Bit/s} = 856,6865 \text{ Sekunden}$$

$$856,6865 \text{ Sekunden} / 60 = \mathbf{14,28 \text{ Minuten}}$$

(14 Minuten und 17 Sekunden)

- ba) Mögliche weitere Regeln für einen Spamfilter:

- Absender steht auf der White-List
  - Unerwünschte Begriffe im Betreff (siehe Blacklist der Begriffe)
  - Im E-Mail-Text kommen unerwünschte Links vor (siehe Blacklist der Begriffe)
  - Absender-Domain und angezeigter Absender-Name stimmen nicht überein
  - Anhänge haben Datei-Formate, die unbekannt oder unerwünscht sind (z. B. ausführbare Dateien)
- Weitere Nennungen sind möglich.*

- bb) Die Mitarbeiter des Unternehmens sollten vorab nachweislich über die Kontrolle durch Spamfilter oder Administratoren informiert werden. Im bestens Fall sollte die ausdrückliche Einwilligung eingeholt werden.

Alternativ sollte privater E-Mail-Verkehr untersagt werden, da das Unternehmen bei rein geschäftlichen Inhalten den Mailverkehr ohnehin einsehen darf.

- bc) Bei einer Sandbox handelt es sich um eine abgeschottete virtuelle Maschine mit verschiedensten Betriebssystemen überprüft werden. Eine Kommunikation aus der Sandbox hinaus kann nicht stattfinden – die übrigen Systeme und Umgebungen sind somit von eventuellen Aktionen der Dateianhänge geschützt.

### 3 Wirtschafts- und Sozialkunde

- | Aufgabe | Lösung  |
|---------|---|
| 1.      | <b>4</b> Das individuell vereinbarte Arbeitsentgelt darf jederzeit über dem tariflich geregelten Arbeitsentgelt liegen.   |
| 2.      | <b>1;5</b> Bei Arbeitnehmern kann eine Probezeit von null bis sechs Monate vereinbart werden.<br>Bei Auszubildenden wäre eine minimale Probezeit von einem Monat und eine maximale Probezeit von vier Monaten möglich.  |
| 3.      | <b>06:00</b> Siehe Auszug des Gesetzestextes  |
| 4.      | <b>1</b> Siehe § 15 Fünf-Tage-Woche - Jugendarbeitsschutzgesetz (JArbSchG)  |
| 5.      | <b>30</b> Die höchste Regelung findet Anwendung. Daher gelten die in § 42 Erholungsurlaub definierten Urlaubstage.  |
| 6.      | <b>2</b> Alle übrigen Anforderungen sind optional.  |
| 7.      | <b>3</b> Siehe § 102 Abs. 1 Betriebsverfassungsgesetz (BetrVG)  |
| 8.      | <b>4</b> Unter 18 Jahren gilt die beschränkte Geschäftsfähigkeit – daher ist eine Unterschrift der Erziehungsberechtigten notwendig.  |
| 9.      | <b>4</b> Ein qualifiziertes Arbeitszeugnis enthält Ausführungen über die Leistungen und das Verhalten.  |
| 10.     | <b>5</b> Siehe § 87 Mitbestimmungsrechte (Betriebsverfassungsgesetz)  |
| 11.     | <b>3</b> Gemäß §§ 60 und 61 (Betriebsverfassungsgesetz) sind alle Arbeitnehmer wahlberechtigt, die das 18. Lebensjahr noch nicht vollendet haben oder zu ihrer Berufsausbildung beschäftigt sind. Wahlbar sind alle Arbeitnehmer des Betriebs, die das 25. Lebensjahr noch nicht vollendet haben oder die zu ihrer Berufsausbildung beschäftigt sind. [...] |
|         | Ein JAV-Mitglied, das das 25. Lebensjahr vollendet oder die Ausbildung beendet, bleibt dennoch Mitglied der JAV. Siehe § 64 Zeitpunkt der Wahlen und Amtszeit (Betriebsverfassungsgesetz).  |
| 12.     | <b>2</b> Tarifparteien können eine absolute Friedenspflicht vereinbaren, während der Laufzeit eines Tarifvertrages wird also der Arbeitskampf verboten.   |
| 13.     | <b>1;3</b> (Siehe auch Aufgabe 1)   |
| 14.     | <b>3</b> Ein Mantel- oder Rahmentarifvertrag regelt die langfristigen sowie allgemeinen Bedingungen des Arbeitsverhältnisses.   |
| 15.     | <b>3;6</b> Lebensversicherungen sind privat abzuschließen und nicht in den Abgaben zur Sozialversicherung enthalten.<br><br>Die Beträge zur gesetzlichen Unfallversicherung trägt der Arbeitgeber allein.   |
| 16.     | <b>2</b>  |
| 17. a)  | <b>2</b>  |
| 17. b)  | <b>1</b>  |
| 17. c)  | <b>2</b>  |
| 17. d)  | <b>3</b>  |
| 17. e)  | <b>3</b>  |
|         | Primärer Sektor: Gewinnung von Rohstoffen<br>Sekundärer Sektor: Verarbeitung von Rohstoffen<br>Tertiärer Sektor: Dienstleistungen   |
| 18.     | <b>5</b> Gehälter werden jedoch vor einer Gewinnausschüttung ausbezahlt. Anschließend werden die überschüssigen Gelder entsprechend der Geschäftsanteile verteilt, wenn im Gesellschaftervertrag nichts Abweichendes vereinbart wurde.  |

19. **3** Formel:  
Wirtschaftlichkeit = Ertrag / Aufwand  
1.  $180.000 / 150.000 = 1,2$   
2.  $50.000 / 40.000 = 1,25$   
**3.  $52.000 / 40.000 = 1,3$**   
4.  $62.000 / 50.000 = 1,24$
20. **5** Die rechtliche Selbstständigkeit der beiden GmbHs bleibt erhalten.
21. **2** Es handelt sich hierbei um eine überlappende Organisationsform mit mehreren beteiligten Dimensionen.
22. **2**
23. a) **2**
23. b) **6**
23. c) **1**
23. d) **5**
- Die übrigen Symbole:
- 3: Warnung vor gefährlicher elektrischer Spannung  
4: Zutritt für Unbefugte verboten  
7: Sammelplatz / Sammelstelle
24. **4**
25. **3** Tropf- und Fließbrände sind von oben nach unten zu löschen.
26. a) **3**
26. b) **2**
26. c) **4**
26. d) **5**
26. e) **1**
27. **2**
28. **3**
29. **4** Der Ausbildungsstand bzw. die Art des Abschlusses zählt zur fachlichen sowie objektiven Qualifikation. Deshalb werden diese Punkte von der Charta der Vielfalt nicht berücksichtigt.
30. **5**