

Familienname, Vorname (bitte durch eine Leerspalte trennen, ä = ae etc.)

[illegible]

Berufsnummer

Prüflingsnummer

5	5
---	---

1	1	9	7
---	---	---	---

--	--	--

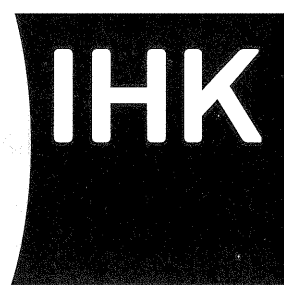
--	--	--	--	--

**Termin: Mittwoch, 13. Mai 2009**

Sp. 1-2

Sp. 3-6

Sp. 7-14



# Fachinformatiker/Fachinformatikerin Systemintegration

1197

1

## Ganzheitliche Aufgabe I Fachqualifikationen

6 Handlungsschritte  
90 Minuten Prüfungszeit  
100 Punkte

## Bearbeitungshinweise

1. Der vorliegende Aufgabensatz besteht aus insgesamt 6 Handlungsschritten zu je 20 Punkten.

In der Prüfung zu bearbeiten sind 5 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 6. Handlungsschritt als nicht bearbeitet.

2. Füllen Sie zuerst die **Kopfzeile** aus. Tragen Sie Ihren Familiennamen, Ihren Vornamen und Ihre Prüflings-Nr. in die oben stehenden Felder ein.
3. Lesen Sie bitte den **Text** der Aufgaben ganz durch, bevor Sie mit der Bearbeitung beginnen.
4. 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.
5. 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.
6. Sofern nicht ausdrücklich ein Brief oder eine Formulierung in ganzen Sätzen gefordert werden, ist eine **stichwortartige Beantwortung** zulässig.
7. Schreiben Sie deutlich und gut lesbar. Ein nicht eindeutig zuzuordnendes oder **unleserliches Ergebnis** wird als **falsch** gewertet.
8. Zur Lösung der Rechenaufgaben darf ein nicht programmierter, netzunabhängiger **Taschenrechner** ohne Kommunikationsmöglichkeit mit Dritten verwendet werden.
9. Wenn Sie ein **gerundetes Ergebnis** eintragen und damit weiterrechnen müssen, rechnen Sie (auch im Taschenrechner) nur mit diesem gerundeten Ergebnis weiter.
10. Ein **Tabellenbuch** oder ein **IT-Handbuch** oder eine **Formelsammlung** ist als Hilfsmittel zugelassen.
11. 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.

The diagram illustrates the structure of the assessment. It consists of six sequential steps, each labeled 'Punkte' (Points) and 'Handlungsschritt' (Action Step). Each step is represented by a box divided into two columns, numbered 15 to 26. The steps are connected by dashed lines. Below the steps, there is a box labeled 'Gesamtpunktzahl' (Total Score) with three columns numbered 28, 29, and 30. A line connects the 'Gesamtpunktzahl' box to the 'Spalte 1 - 14 s. o.' box.

Spalte 1 - 14 s. o.	Punkte 1. Handlungsschritt	Punkte 2. Handlungsschritt	Punkte 3. Handlungsschritt	Punkte 4. Handlungsschritt	Punkte 5. Handlungsschritt	Punkte 6. Handlungsschritt	Gesamtpunktzahl
	15 16	17 18	19 20	21 22	23 24	25 26	28 29 30

Prüfungszeit

27

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

Unterschrift

Gemeinsame Prüfungsaufgaben der Industrie- und Handelskammern. Dieser Aufgabensatz wurde von einem überregionalen Ausschuss, der entsprechend § 40 Berufsbildungsgesetz zusammengesetzt ist, beschlossen.

Die Vervielfältigung, Verbreitung und öffentliche Wiedergabe der Prüfungsaufgaben und Lösungen ist nicht gestattet. Zuwiderhandlungen werden zivil- und strafrechtlich (§§ 97 ff., 106 ff. UrhG) verfolgt. – © ZPA Nord-West 2009 – Alle Rechte vorbehalten!

**Die Handlungsschritte 1 bis 6 beziehen sich auf folgende Ausgangssituation:**

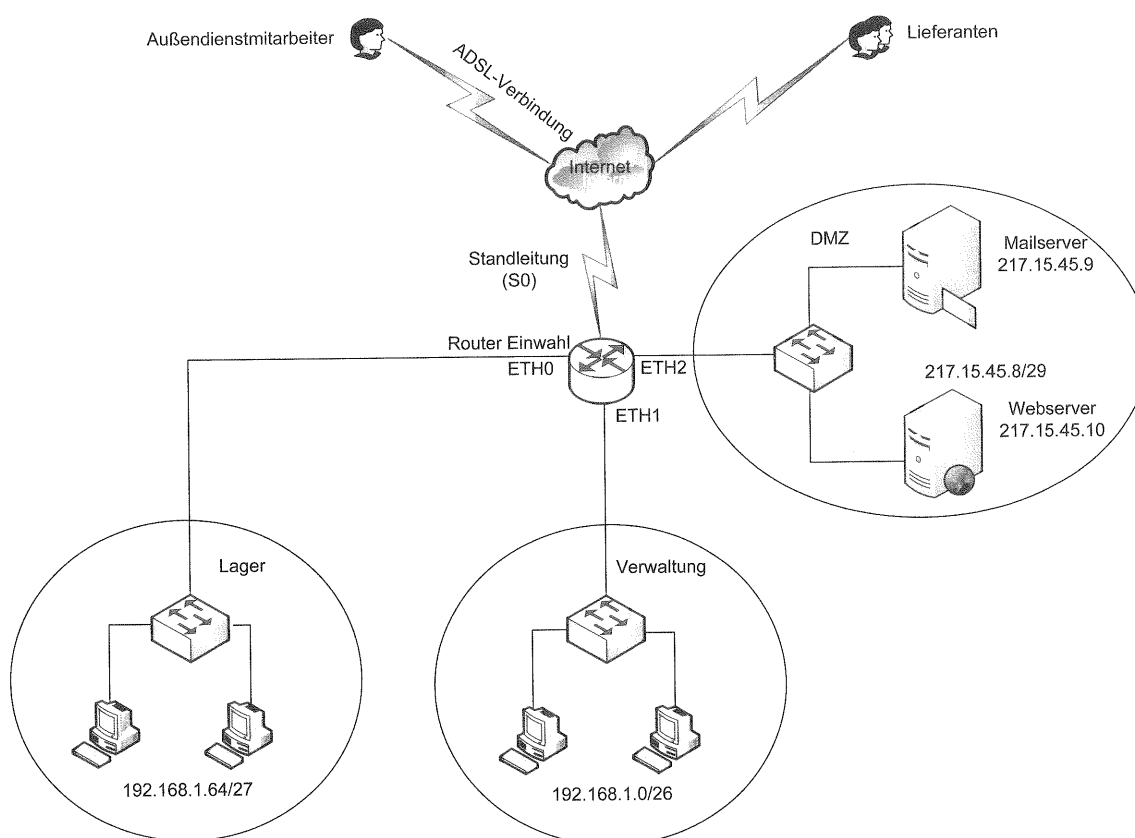
Sie sind Mitarbeiter/-in der Blackbox AG, Friedberg.

Als Systemadministrator/-in sollen Sie folgende Aufgaben erledigen:

1. Einen Router und eine Firewall konfigurieren
2. Sicherheitsaspekte erläutern und Risiken ausschließen
3. Eine VPN-Verbindung mit IPSec einrichten
4. Die Umstellung auf Thin Clients planen und die günstigere Softwarelizenz ermitteln
5. Die Migration auf IPv6 vorbereiten
6. Einen Vorgang in einem Sequenzdiagramm darstellen und Fehler eines Implementierungsdiagramms erläutern

**1. Handlungsschritt (20 Punkte)**

Die folgende Darstellung zeigt in vereinfachter Form das Netzwerk der Blackbox AG.



- a) Der Router in der Zentrale soll auf seine Ethernetschnittstellen die jeweils letzte Adresse im jeweiligen Subnetz erhalten.  
Ergänzen Sie dazu die folgende Tabelle: (9 Punkte)

Schnittstelle	IP-Adresse	Rechenweg/Erklärung
ETH0		
ETH1		
ETH2		

b) Das Firmennetz ist über eine Standleitung mit dem Internet verbunden. Der Provider hat der Blackbox AG die IP-Adresse 217.40.40.6 mit der Subnetmaske 255.255.255.252 zugewiesen. Die Routingtabelle muss um eine Defaultroute nach folgendem Muster ergänzt werden:

```
0.0.0.0 0.0.0.0 <Next Hop Address>
```

ba) Nennen Sie die Next-Hop-Adresse. (2 Punkte)

---

---

---

Auf der Firewall (reiner Paketfilter) wurden zunächst die folgenden Regeln eingetragen, um den Zugriff auf den Webserver zu gewährleisten:

Erlauben/ Verbieten	Proto- koll	Quelle	Ziel	Quell-Port	Ziel-Port	Interface	Richtung
Permit	TCP	Any	217.15.45.10	Any	80	S0	IN
Permit	TCP	217.15.45.10	Any	80	Any	S0	OUT
Deny	IP						

bb) Den Außendienstmitarbeitern soll das Senden (SMTP) und Abholen (POP3) von Mails über den Mailserver und eine gesicherte Verbindung zum Webserver ermöglicht werden.

Tragen Sie die dazu erforderlichen Regeln in folgende Tabelle ein. (7 Punkte)

Erlauben/ Verbieten	Proto- koll	Quelle	Ziel	Quell-Port	Ziel-Port	Interface	Richtung
Permit	TCP	Any	217.15.45.10	Any	80	S0	IN
Permit	TCP	217.15.45.10	Any	80	Any	S0	OUT

c) Die Firmenleitung beschließt, den Internetverkehr nur noch über einen Proxyserver zu erlauben.  
Nennen Sie zwei Aufgaben, die der Proxyserver übernimmt. (2 Punkte)

---

---

---

---

---

---

---

---

---

---

## 2. Handlungsschritt (20 Punkte)

Korrekturrand

Der Internetzugang der Blackbox AG ist derzeit nur über einen einfachen Paketfilter gesichert.

- a) Ergänzen Sie die folgende Tabelle, indem Sie den jeweiligen Angriff beschreiben und einen Schutz nennen. (9 Punkte)

Angriff	Beschreibung	Schutz
Phishing		
DNS-Spoofing		
ARP-Spoofing		

- b) Das eingesetzte Antivirenprogramm ist nur in der Lage, ausführbare Dateien und Office-Dateien zu scannen.

Erläutern Sie, warum dieser Schutz nicht ausreichend ist.

(2 Punkte)

---

---

---

---

---

---

---

---

---

---

- c) Erläutern Sie, warum das Antivirenprogramm im Kernelmodus laufen sollte.

(3 Punkte)

---

---

---

---

---

---

d) Im Unternehmen dürfen derzeit Internet und E-Mail auch privat genutzt werden. Nun besteht der Verdacht, dass einer der Mitarbeiter über den Internetzugang des Unternehmens Internetseiten mit strafbaren Inhalten aufruft. Daraufhin möchte die Geschäftsleitung ein Echtzeit-Monitoring (Online) des Internetverkehrs über alle Anwender durchführen.

Korrekturrand

Nennen Sie drei Punkte, die für ein Echtzeit-Monitoring aus technischer, organisatorischer und rechtlicher Sicht zu beachten sind.

(6 Punkte)

---

---

---

---

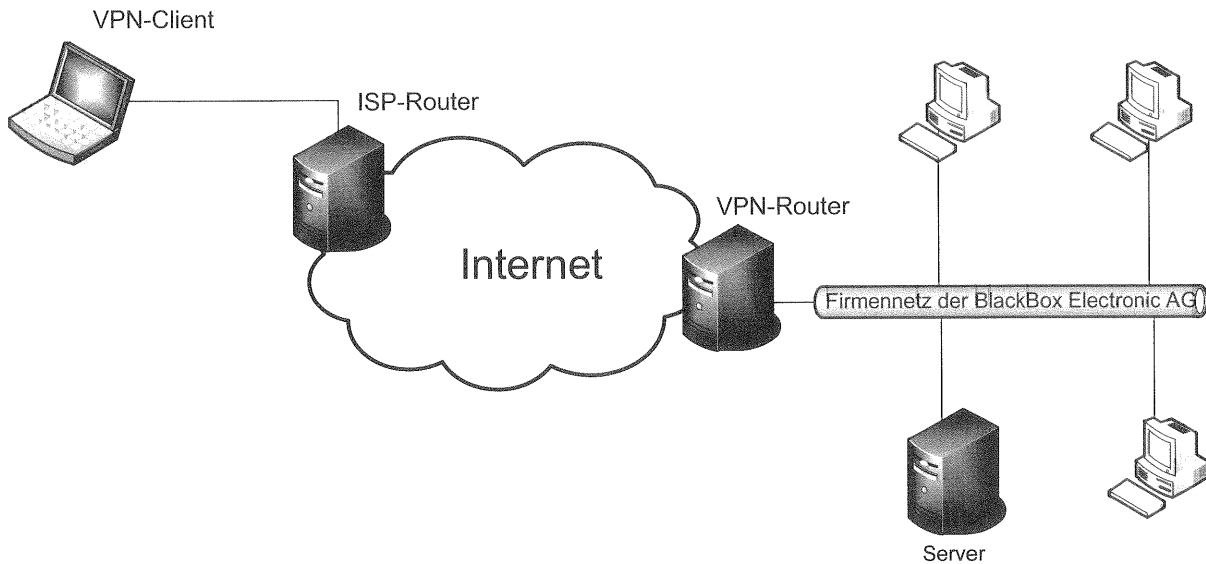
---

### 3. Handlungsschritt (20 Punkte)

Korrekturrand

Sie sollen für den Leiter der Finanzabteilung eine sichere Verbindung von seinem Laptop zum Server im Firmennetz einrichten. Sie entscheiden sich für eine VPN-Verbindung mit IPSec.

- a) Kennzeichnen Sie in folgender Skizze den „VPN-Tunnel“, sodass erkennbar ist, welche Knoten die Endpunkte des „VPN-Tunnels“ sind. (1 Punkt)



- b) Nennen Sie den Begriff für diese Verbindungsart. (2 Punkte)

- c) Erläutern Sie stichwortartig die drei Sicherheitsaspekte, die bei einer VPN-Verbindung sichergestellt werden sollen. (6 Punkte)

- d) Im Zusammenhang mit IPSec werden auch AH und ESP genannt.

Nennen Sie jeweils die Langform und erläutern Sie jeweils kurz

- da) AH. (2 Punkte)  
db) ESP. (2 Punkte)

e) Das folgende Schema zeigt die Segmente eines Datenpakets, das über eine VPN-Verbindung mittels IPSec im Tunnelmodus verschickt wird. Zum Schutz werden ESP und AH angewendet.

Kennzeichnen Sie am Schema die folgenden Bereiche des Datenpaketes:

- Verschlüsselter Bereich
- Durch ESP authentifizierter Bereich
- Durch ASP authentifizierter Bereich

(3 Punkte)

Neuer IP-Header	AH-Header	ESP-Header	Original IP-Header	Payload	ESP-Anhang	ESP-Authentifikation
-----------------	-----------	------------	--------------------	---------	------------	----------------------

f) Im LAN der Blackbox AG wird nur NAT und kein NAT-T eingesetzt.

Erläutern Sie kurz, warum daher IPSec mit AH nicht eingesetzt werden kann.

(4 Punkte)

## Korrekturrand

Es müssen 90 EDV-Arbeitsplätze mit neuen Geräten ausgestattet werden, die im Schichtbetrieb von 150 Mitarbeitern genutzt werden.

- |                                           |            |
|-------------------------------------------|------------|
| Kosten für einen PC-Arbeitsplatz:         | 700,00 €   |
| Kosten für einen Thin Client-Arbeitsplatz | 400,00 €   |
| Mehrkosten für leistungsfähigere Server   | 8.000,00 € |
| VMWare/Terminalserver Lizenzkosten        | 7.000,00 € |

A full-page sheet of white graph paper featuring a uniform grid of thin black lines. The grid consists of small squares covering the entire area of the page.

- 
- 
- 
- 
- 

- [illegible]



d) Erläutern Sie mithilfe des folgenden englischen Textes, für welche der beiden angebotenen Lizenzen sich die Blackbox AG aus Kostengründen entscheiden sollte. (4 Punkte)

Korrekturrand

To use Terminal Server, you are required to have a Computer Access License (CAL) for every Terminal Server Client. There are two types of licenses:

- Per Device CAL 17,00 €
- Per User CAL 17,00 €

<p>A <b>Per Device CAL</b> provides each client computer the right to access a terminal server.</p> <p>Per Device licensing is a good choice for:</p> <ul style="list-style-type: none"><li>• Hosting a user's primary desktop for devices the customer owns or controls.</li><li>• Thin clients or computers that connect to a terminal server for a large percentage of the working day.</li><li>• Hosting line-of-business applications that are used for the bulk of your users' work.</li></ul> <p>This type of licensing is a poor choice if you do not control the device accessing the server, for example computers in an Internet café, or if you have a business partner who connects to your terminal server from outside your network.</p>	<p>In <b>Per User CAL</b> licensing mode you must have one license for every user. With Per User licensing, one user can access a terminal server from an unlimited number of devices and only needs one CAL rather than a CAL for each device.</p> <p>Per User licensing is a good choice in the following situations:</p> <ul style="list-style-type: none"><li>• Providing access for roaming users.</li><li>• Providing access for users who use more than one computer, for example, a portable and a desktop computer.</li><li>• Providing ease of management for organizations that track access to the network by user, rather than by computer.</li></ul> <p>In general, if your organization has more computers than users, Per User licensing might be a cost-effective way to deploy Terminal Server.</p>
---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

---

---

---

---

---

---

---

## 5. Handlungsschritt (20 Punkte)

Korrekturrand

Die Blackbox AG will mit einem asiatischen Zulieferer zusammenarbeiten, der über IPv6 an das Internet angeschlossen ist. Die Blackbox AG überprüft nun, ob eine Migration auf IPv6 möglich ist.

a) Geben Sie die englischen Erläuterungen folgender Fachbegriffe sinngemäß auf Deutsch wieder.

aa) Global Unicast Address (2000/3): This address is the analogue of the IPv4 address. Identifies an unique interface. (2 Punkte)

---

---

---

---

---

---

---

---

ab) Site local address (FEC0/10): An identifier for a network or host. Can be used to build a private network, like the private network address space (10.x.x.x) in IPv4. (2 Punkte)

---

---

---

---

---

---

---

---

ac) Link local address (FE80/10): This address is found on each IPv6 interface after stateless auto-configuration. Packets using link-local addressing will never pass a router. (2 Punkte)

---

---

---

---

---

---

---

---

ad) 6to4 tunnelling: 6to4 is a mechanism that allows IPv6-hosts, -sites or -networks to communicate across the IPv4 Internet. The local node encapsulates the IPv6 traffic with an IPv4 header and sends it to another 6to4 node over the IPv4 Internet. On this site the IPv4 header will be removed and the IPv6 traffic will be send to the destination node using the IPv6 network infrastructure. (3 Punkte)

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

- b) Die Verbindung zu dem asiatischen Zulieferer wird geprüft. Mit einem Protocolanalyser wurden im lokalen LAN zwei IP-Pakete aufgezeichnet.

Korrekturrand

#### Trace 1

```
45 00 00 54 A1 1B 00 00 41 01 55 52 C0 A8 01 02
C0 A8 01 E9 00 00 9B E3 3F 1C 00 09 24 13 36 47
D5 98 0D 00 08 09 0A 0B 0C 0D 0E 0F 10 11 12 13
14 15 16 17 18 19 1A 1B 1C 1F 20 21 22 23 24 25
...
```

#### Trace 2

```
60 00 00 00 00 00 40 3A 40 FE C0 00 01 00 00 00
00 00 AF C1 00 B4 00 51 FE C0 00 03 00 00 00 00
00 00 00 BE FE 30 01 F0 81 00 A4 6B 0C 1C 00 41
52 0F 36 47 9F 89 0C 00 08 09 0A 0B 0E 0F 10 11
...
```

Next header Options:

- 0 = Hop by Hop
- 6 = TCP
- 17 = UDP
- 43 = Routing header
- 44 = Fragment header
- 50 = Encapsulation security
- 51 = Authentication header
- 58 = ICMPv6
- 59 = no next header
- 60 = Destination header

#### IPv6-Header

Version (4bit)	Traffic Class (8bit)	Flow Label (20 bit)	
Payload length (16bit)		Next Header (8bit)	Hop Limit (8bit)
Source Address (128bit)			
Destination Address (128bit)			

- ba) Ermitteln Sie den Trace mit dem IPv6 Paket.

(1 Punkt)

---



---



---

- bb) Nennen Sie die IPv6 Senderadresse.

(2 Punkte)

---



---



---

- bc) Nennen Sie die IPv6 Empfängeradresse.

(2 Punkte)

---



---



---

- bd) Ermitteln Sie das übergeordnete Protokoll.

(2 Punkte)

---



---



---

- c) Nennen Sie zwei Gründe, die für die Einführung von IPv6 sprechen.

(4 Punkte)

---



---



---



---



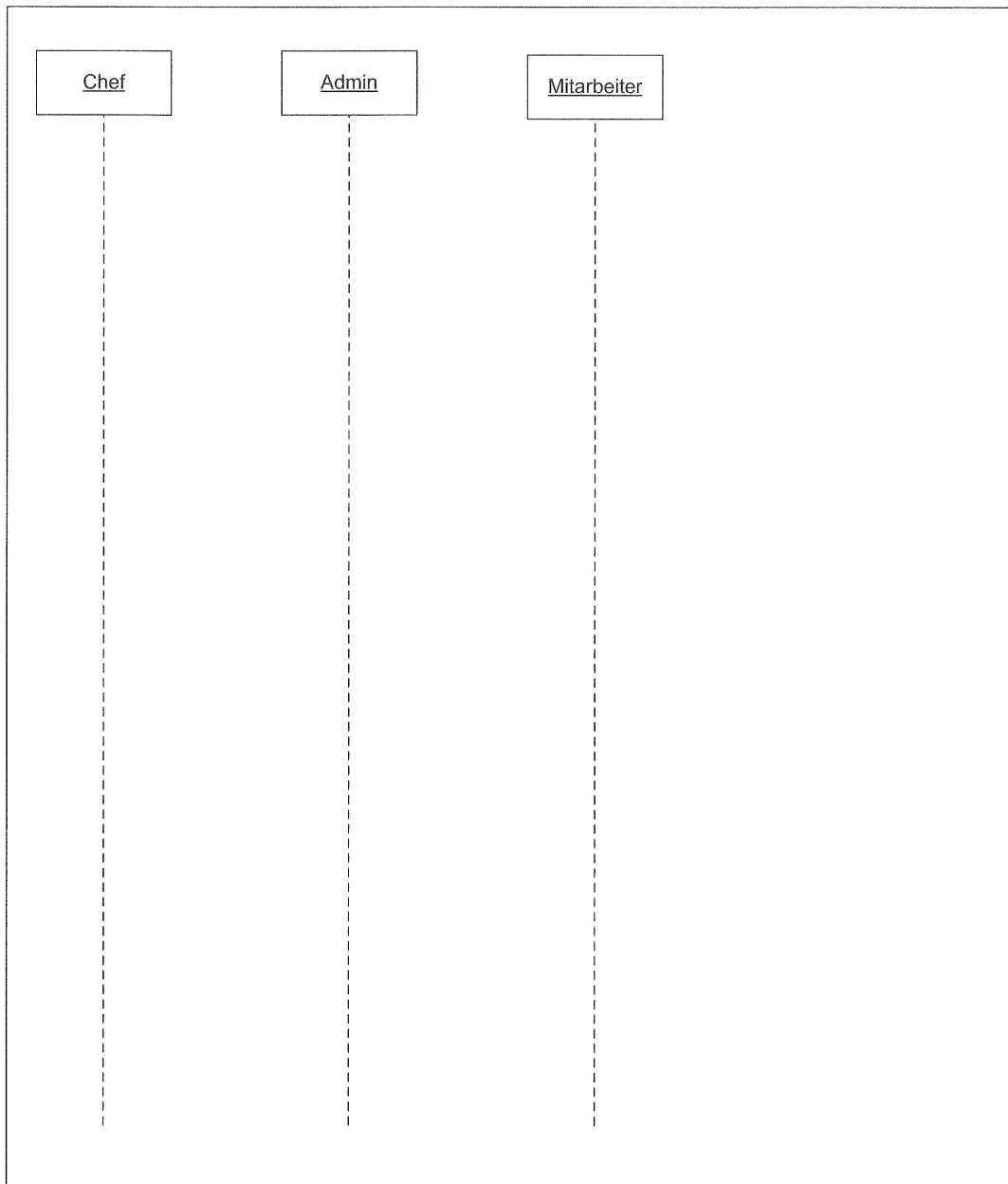
---

## 6. Handlungsschritt (20 Punkte)

Korrekturrand

Der Leiter der Vertriebsabteilung teilt Ihnen telefonisch mit, dass Sie für einen neuen Mitarbeiter ein Benutzerkonto einrichten sollen. Sie legen das Benutzerkonto an. Danach rufen Sie den neuen Mitarbeiter an und bitten ihn, sich zum Test mit seinem neuen Account im Firmennetz anzumelden. Der neue Mitarbeiter meldet sich an. Sie warten die Bestätigung des Mitarbeiters, dass die Anmeldung mit dem neuen Account erfolgreich war, ab.

- a) Der oben beschriebene Vorgang soll in einem Sequenzdiagramm dargestellt werden. Ergänzen Sie dazu das nachfolgende Diagramm. (12 Punkte)

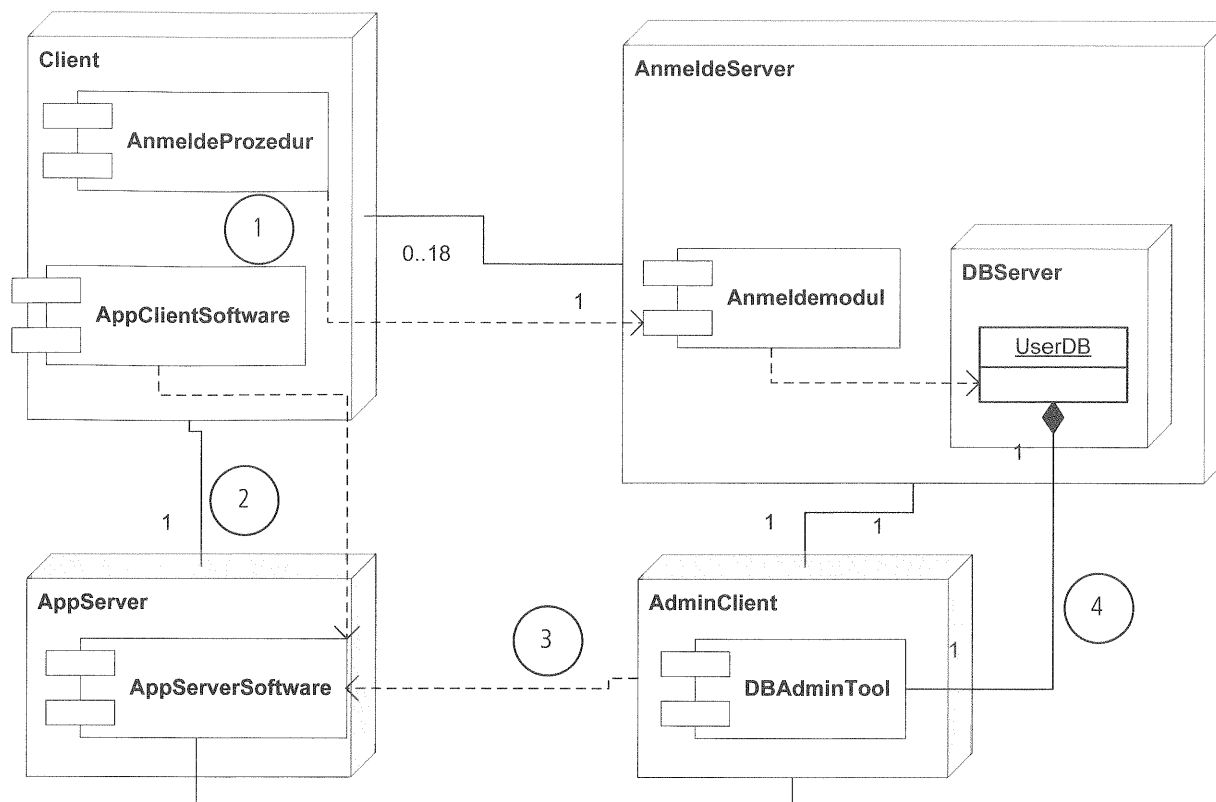


b) Für eine Präsentation wurde das folgende Implementierungsdiagramm erstellt. Ihr Abteilungsleiter hat vier Fehler festgestellt und mit 1 bis 4 markiert.

Korrekturrand

Erläutern Sie kurz die vier Fehler in unten stehender Tabelle.

(8 Punkte)



Fehler-Nr.	Erläuterung
1	
2	
3	
4	

### 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.

☐