Abschlussprüfung Sommer 2009
Lösungshinweise

IHK

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 sechs Handlungsschritte ausdrücklich als „nicht bearbeitet" gekennzeichnet wurde,
- der 6. Handlungsschritt bearbeitet wurde,
- einer der Handlungsschritte 1 bis 5 deutlich erkennbar nicht bearbeitet wurde,

ist der tatsächlich nicht bearbeitete Handlungsschritt von der Bewertung auszuschließen.

Ein weiterer Punktabzug für den bearbeiteten 6. 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 (20 Punkte)

a) 9 Punkte

Schnittstelle	IP-Adresse	Erläuterung/Rechenweg
ETH0	192.168.1.94	/27 lässt noch 5 Bit im Hostbereich, damit ergeben sich 2^5 = 32er Sprünge bis zur nächsten Netz-ID. Berücksichtigt man den BC, ergibt sich .94 als letzte Host-IP.
ETH1	192.168.1.62	/26 lässt noch 6 Bit im Hostbereich, damit ergeben sich 2^6 = 64er Sprünge bis zur nächsten Netz ID. Berücksichtigt man den BC, ergibt sich .62 als letzte Host-IP.
ETH2	217.15.45.14	/29 lässt noch 3 Bit im Hostbereich, damit ergeben sich 2^3 = 8er Sprünge bis zur nächsten Netz-ID. Berücksichtigt man den BC, ergibt sich .14 als letzte Host-IP.

ba) 2 Punkte

217.40.40.7

bb) 7 Punkte, 7 x 1 Punkt (je Zeile)

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
Permit	TCP	Any	217.15.45.9	Any	25	S0	IN
Permit	TCP	217.15.45.9	Any	25	Any	S0	OUT
Permit	TCP	Any	217.15.45.9	Any	110	S0	IN
Permit	TCP	217.15.45.9	Any	110	Any	S0	OUT
Permit	TCP	Any	217.15.45.10	Any	443	S0	IN
Permit	TCP	217.15.45.10	Any	443	Any	S0	OUT
Deny	IP						

c) 2 Punkte, 2 x 1 Punkt

- Proxyserver übernimmt die Filterung des angeforderten http-Verkehrs nach Inhalt
- Caching des Datenverkehrs
- Namensauflösung für die Clients

2. Handlungsschritt (20 Punkte)

a) 9 Punkte, 3 x (2 + 1) Punkte

Angriff	**Beschreibung** (je 2 Punkte)	**Schutz** (je 1 Punkt)
Phishing	Offiziell wirkende E-Mail bzw. Internetseite, die das Opfer auffordert, vertrauliche Daten, z. B. PINs, TANs, Passwörter etc. weiterzugeben.	Aufklärung/Schulung der Mitarbeiter/-innen Einsatz von Contentfiltern
DNS-Spoofing	Vortäuschen falscher DNS-Einträge, um Namen in IP-Adressen des Angreifers aufzulösen. Datenverkehr des Opfers wird umgeleitet. Abhörung ist möglich.	Feste Einträge in der HOST-Datei für wichtige Hostnamen Einsatz von DNS-Servern, die Authentifizierung voraussetzen
ARP-Spoofing	Senden von gefälschten ARP-Nachrichten, um die ARP-Tabelle (Zuordnung IP-MAC-Adresse) zu manipulieren. Daten werden dann an die falsche MAC-Adresse geleitet.	Verwenden statischer ARP-Einträge (z. B. im Loginskript)

b) 2 Punkte

Andere Dateitypen, Archive, komprimierte Formate etc. können schädliche Inhalte transportieren und werden nicht gescannt.

c) 3 Punkte

Im Kernelmode lässt sich der Dienst durch den Anwender nicht beenden.

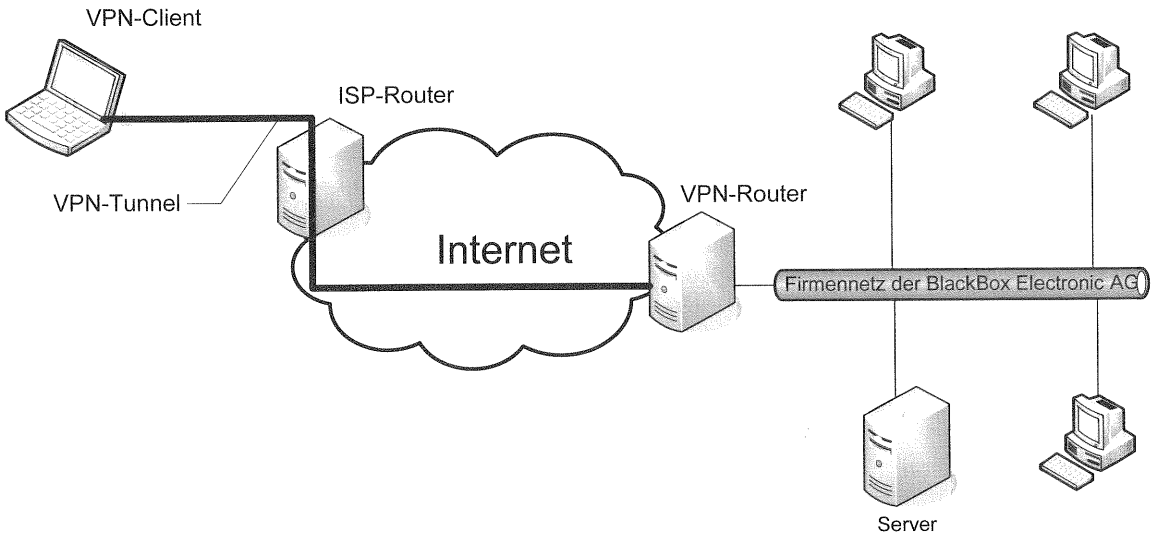
d) 6 Punkte, 3 x 2 Punkte

- Der Betriebsrat/die Personalvertretung sollte im Vorfeld der Überwachung informiert werden.
- Das Monitoring sollte anonymisiert erfolgen, d. h. es können keine Rückschlüsse auf die Identität des jeweiligen Anwenders getroffen werden.
- Die Ergebnisse des Monitorings können keine arbeitsrechtlichen Konsequenzen nach sich ziehen (Verweis, Abmahnung, Kündigung).
- Die Ergebnisse des Monitorings dürfen nicht zur Leistungsmessung verwendet werden.
- Der Schutz personenbezogener Daten muss gewährleistet sein, d. h. persönliche Angaben, die ein Anwender im Internet macht, dürfen nicht von Dritten eingesehen oder an Dritte weitergegeben werden.
- Die Geschäftsleitung darf während des Monitorings straftatsrealisierende Seiten sperren lassen. Dies stellt keine Verletzung des Persönlichkeitsrechts dar.

Weitere Punkte können aufgeführt werden.

3. Handlungsschritt (20 Punkte)

a) 1 Punkt



b) 2 Punkte

End-to-Site-Verbindung (Client-Server-Verbindung)

c) 6 Punkte, 3 x 2 Punkte

- Integrität: Daten können nicht verfälscht werden.
- Authentizität: Die Partner sind diejenigen, die sie vorgeben zu sein.
- Verschlüsselung: Daten sind gegen Ausspähen durch Dritte geschützt.

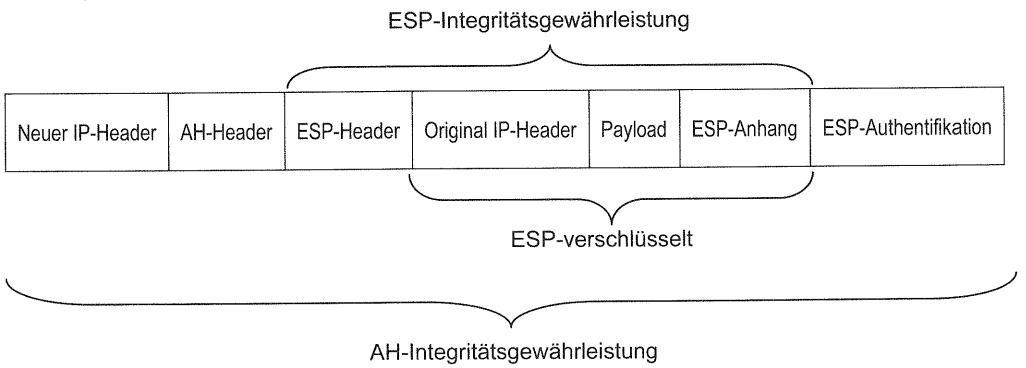
da) 2 Punkte

- AH (Authentification Header)
- Prüfsumme, die durch ein Hashing-Verfahren aus dem originalen IP-Paket und dem hinzugefügten IP-Header gebildet wird.
- Zur Überprüfung von Authentizität und Integrität

db) 2 Punkte

- ESP (Encapsulating Security Payload))
- Je nach Modus werden nur die Nutzdaten oder zusätzlich auch die originalen IP-Header verschlüsselt.
- Schutz der Daten gegen unbefugte Einsichtnahme durch Dritte.

e) 3 Punkte, 3 x 1 Punkt



f) 4 Punkte

NAT verändert den IP-Header. Der VPN-Server verwirft die Pakete mit verändertem Header, da nach seinen Regeln zur Wahrung der Integrität diese Pakete verfälscht sind.

4. Handlungsschritt (20 Punkte)

a) 6 Punkte

$700 \cdot x = 400 \cdot x + 8.000 + 7.000$
$300 \cdot x = 15.000$
$x = 50$

Ab 51 Arbeitsplätzen sind die Anschaffungskosten für Thin Clients niedriger als die für PCs.

b) 4 Punkte, 4 x 1 Punkt

- Geringere Stromkosten
- Längere Lebensdauer
- Wirtschaftlichere Administration der Arbeitsplätze
- Geringerer Zeitaufwand für Softwareinstallationen
- Geringere Kosten für Wartung und Reparatur
- Kürzere Ausfallzeiten
- Höherer Schutz vor Viren, Sabotage und Datenkorruption
- u. a.

c) 6 Punkte

- Alle Anwendungen laufen auf einem oder mehreren Servern
- Nur die Bildschirmausgabe wird zum Thin Client übertragen
- Alle am Thin Client vorgenommenen Eingaben werden zum Server gesendet.
- Die Eingaben eines Thin Clients werden auf dem Server in einer virtuellen, geschützten Umgebung verarbeitet.

d) 4 Punkte

Die Lizenz Device CAL ist günstiger weil
- es aufgrund des Schichtdienstes mehr Mitarbeiter als Computer gibt.
- jeder Mitarbeiter nur an einem bestimmten Computer arbeitet.
- keine Außendienstmitarbeiter zu berücksichtigen sind.

5. Handlungsschritt (20 Punkte)

aa) 2 Punkte

Diese Adresse ist wie eine normale öffentliche IPv4-Adresse zu sehen. Kennzeichnet eine einzige Schnittstelle.

ab) 2 Punkte

Bezeichnet ein Netzwerk oder einen Rechner
Kann genutzt werden, um ein privates Netzwerk aufzubauen, ähnlich dem privaten Adressraum 10.x.x.x bei IPv4.

ac) 2 Punkte

Diese Adresse ist bei jeder IPv6 Schnittstelle nach der statuslosen Autokonfiguration zu finden.
Pakete, die eine Link-Local-Adresse verwenden, werden nicht vom Router weitergeleitet.

ad) 3 Punkte

6to4 ist eine Technik, die es IPv6-Rechnern oder IPv6-Netzwerken erlaubt, über ein IPv4 Netzwerk (Internet) zu kommunizieren. Ein lokaler Knoten fügt den IPv6-Netzwerkverkehr mit IPv4 Header und sendet diese zu einen anderen 6to4 Knoten über das IPv4 Internet. Auf dieser Seite wird der IPv4 Header entfernt und wird als IPv6 Netzwerkverkehr unter Nutzung der IPv6 Netzwerkinfrastruktur zum Empfänger gesendet.

b) 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 40 **3A** 40 **FE C0 00 01 00 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

ba) 1 Punkt

Trace 2 (ersten vier bit "6")

bb) 2 Punkte

Mögliche Lösungen:
- FE C0:00 01:00 00:00 00:00 00:AF C1:00 B4:00 51
- FE C0:1:0:0:0:AF C1:B4:51
- **FEC0:1::AFC1:B4:51**

bc) 2 Punkte

Mögliche Lösungen
- FE C0:00 03:00 00:00 00:00 00:00 BE:FE 30:01 F0
- FE C0:3:0:0:0:BE:FE 30:1F0
- FEC0:3::BE:FE30:1F0

bd) 2 Punkte

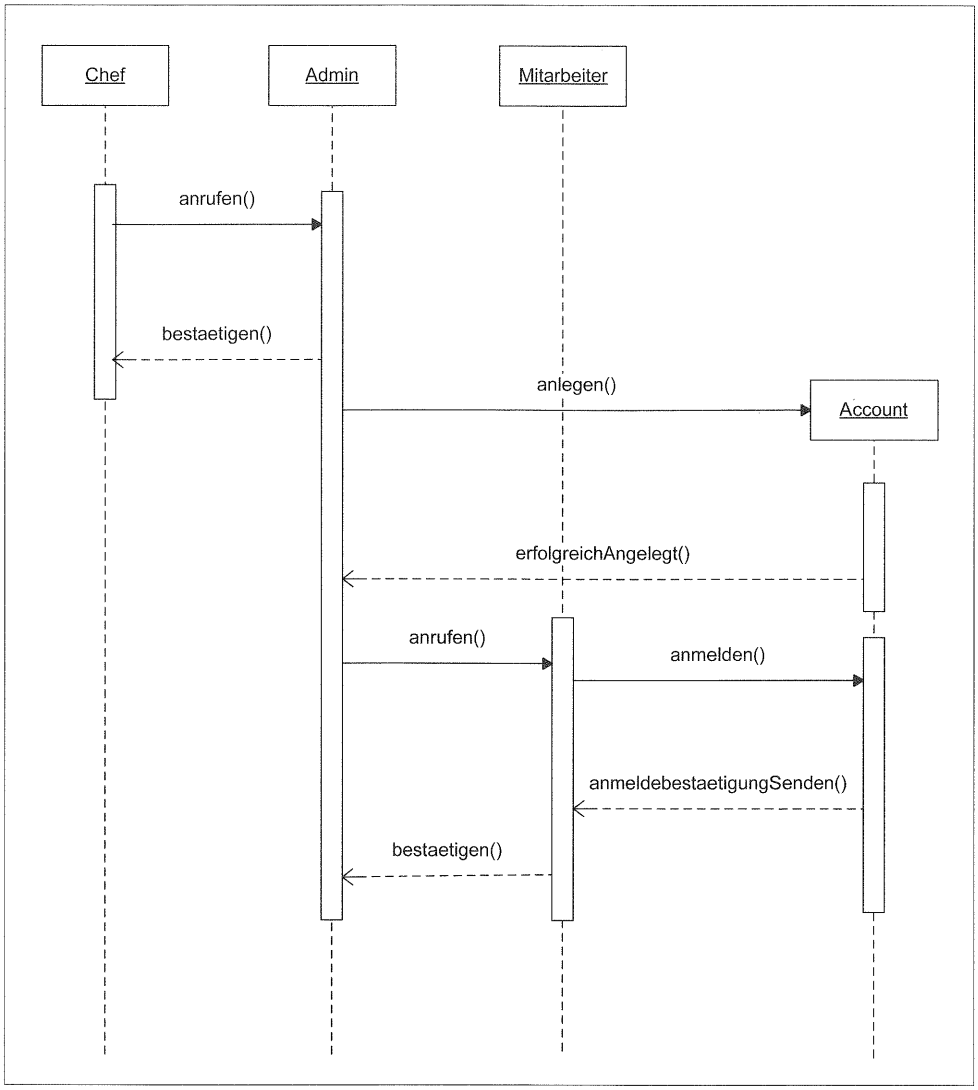
Feld Next Header 3A (hexadezimal) entspricht 58 (dezimal)
ICMPv6

c) 4 Punkte, 2 x 2 Punkte

- Steigende Zahl von internetfähigen Endgeräten
- Wenige freie Netzwerke für „neue" Firmen/Anbieter
- Begrenzte Zahl von öffentlichen IPv4 Adressen
- Steigende Internettelefonie benötigt zusätzliche IP-Adressen
- QoS (Quality of Service) bereits in IPv6 implementiert
- IPsec integriert
- IPv6-Header auf weniger Felder reduziert, dadurch können IPv6-Pakete schneller geroutet werden
- Mobiles Computing möglich
- Erweiterungsheader bietet zusätzliche Möglichkeiten
- u. a.

6. Handlungsschritt (20 Punkte)

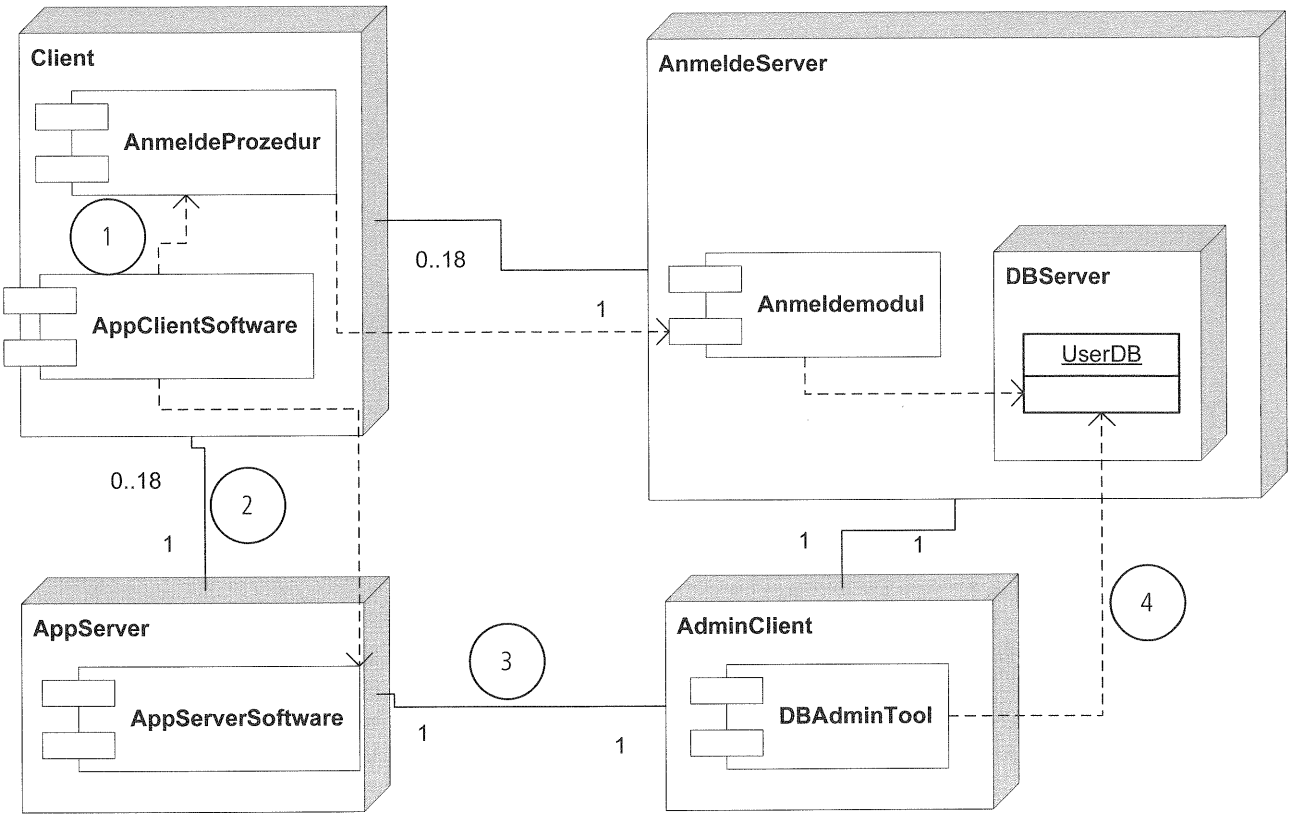
a) 12 Punkte



Fortsetzung 6. Handlungsschritt →

Fortsetzung 6. Handlungsschritt

b) 8 Punkte



(Diagramm, korrigiert)

Fehler-Nr.	Erläuterung
1	Die Abhängigkeit der Software von der Anmeldung fehlt.
2	Die Kardinalitäten fehlen.
3	Der Client des Admins ist nicht vom AppServer abhängig. Er ist höchstens mit ihm vernetzt.
4	Die Komposition ist falsch. Das Datenbank-Administrationstool ist von der Datenbank nur abhängig.