Abschlussprüfung Sommer 2015
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) 3 Punkte

Erläuterung des Fehlers:
- Falscher DNS-Server
- Namensauflösung funktioniert nicht

Beseitigung des Fehlers:
Ändern der DNS-Adresse in 10.0.0.200

ab) 3 Punkte

Erläuterung des Fehlers:
- Falscher Standardgateway
- Aktueller Standardgateway ist die Netz-ID des nächsten Netzes

Beseitigung des Fehlers:
Ändern z. B. in 192.168.2.30 (Richtig sind alle Adressen im Bereich 192.168.2.1 – 30.)

ac) 4 Punkte

Erläuterung des Fehlers:
- Falsche Subnetzmaske
- Drucker liegt bei dieser Subnetzmaske in einem anderen Netz

Beseitigung des Fehlers:
Ändern der Subnetzmaske in 255.255.255.192

ba) 12 Punkte

Router Köln

Netzwerk	Subnetzmaske	Next Hop/Schnittstelle
10.0.0.0	255.255.252.0	ETH0
172.16.10.0	255.255.255.252	ETH1
172.16.30.0	255.255.255.252	172.16.10.2
0.0.0.0	0.0.0.0	200.10.10.2
192.168.1.0	255.255.255.192	172.16.10.2 bzw. ETH1
192.168.2.0	255.255.255.224	172.16.10.2 bzw. ETH1

Router Hamburg

Netzwerk	Subnetzmaske	Next Hop/Schnittstelle
172.16.10.0	255.255.255.252	ETH2
172.16.30.0	255.255.255.252	ETH1
192.168.1.0	255.255.255.192	ETH0
0.0.0.0	0.0.0.0	172.16.10.1
192.168.2.0	255.255.255.224	172.16.30.2 bzw. ETH1

Router Frankfurt

Netzwerk	Subnetzmaske	Next Hop/Schnittstelle
172.16.30.0	255.255.255.252	ETH1
192.168.2.0	255.255.255.224	ETH0
0.0.0.0	0.0.0.0	172.16.30.2 bzw. ETH1

bb) 3 Punkte

Ja, Routingprotokoll ist in diesem Fall sinnvoll. Über das Routingprotokoll würde automatisch eine Ersatzroute eingesetzt werden.

Andere Lösungen sind möglich.

2. Handlungsschritt (25 Punkte)

a) 4 Punkte, 2 x 2 Punkte

Webserver (http)	Port 80
Öffentliche Daten (ftp)	Port 20 + 21
VPN – Gateway (ssl)	Port 443
VPN – Gateway (PPTP)	Port 1723
Mailserver (smtp)	Port 25
Mailserver (pop3)	Port 110
Mailserver (smtp ssl)	Port 465
Mailserver (SMTP tls)	Port 587

Andere Lösungen sind möglich.

ba) 4 Punkte, 2 x 2 Punkte

Regel 1:
Von allen internen Rechnern im Netz 10.0.0.0/22 kann nur der Proxyserver (172.16.100.4/32) mit der Portnummer 3128 erreicht werden.

Regel n:
Verbieten des übrigen Datenverkehrs

Andere Lösungen sind möglich.

bb) 4 Punkte, 8 x 0,5 Punkte je Feld

Nr	Aktion	Protokoll	Quelle	Ziel	Quell-Port	Ziel-Port	Von Interface	Nach Interface
1	ACCEPT	TCP	172.16.100.4/32	ANY	ANY	80	DMZ-EXT	WAN
2	ACCEPT	TCP	172.16.100.4/32	ANY	ANY	443	DMZ-EXT	WAN
3	ACCEPT	UDP	172.16.100.4/32	ANY	ANY	53	DMZ-EXT	WAN
4	DENY	IP	ANY	ANY	-	-	ANY	ANY

Andere sinnvolle Regelungen, z. B. für die Namensauflösung, sind möglich.

c) 6 Punkte

- Ein Blacklist-Filter sperrt alle Domänen, die in der Liste aufgeführt sind.
  Alle anderen Domains sind erreichbar. Bei neuen unerwünschten Domänen müssen diese zusätzlich in die Liste eingetragen werden. 3 Punkte
- Ein Whitelist-Filter lässt nur Internetdomänen zu, die in der Liste aufgeführt sind.
  Weitere gewünschte Domänen müssen zusätzlich in die Liste eingetragen werden. 3 Punkte

Andere Lösungen sind möglich.

da) 3 Punkte

Bei einfachen Schüsselwörtern wie „shop" könnten eventuell Einkaufsseiten von Zulieferern nicht angezeigt werden.

Andere Lösungen sind möglich.

db) 4 Punkte

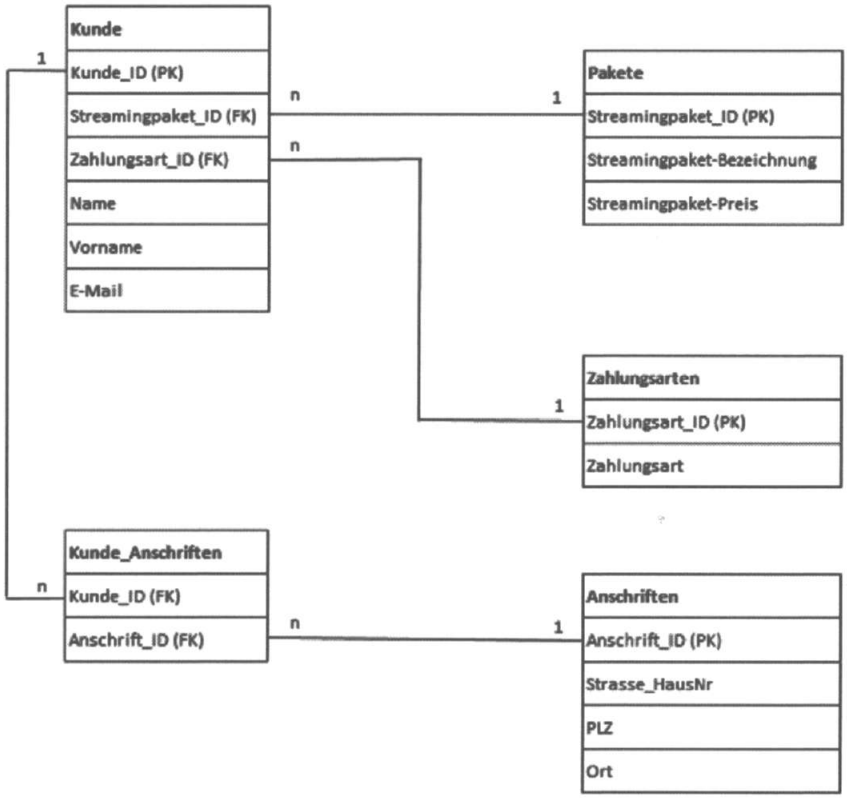
Eine Filterung kann nicht stattfinden, da der Datenverkehr verschlüsselt ist.

oder

Eine Filterung kann nur passieren, wenn der Proxy als „man in the middle" agiert und jeweils eine sichere Verbindung zum Client und eine zum Zielserver hält. Im Browserfenster würde aber ein ungültiges Zertifikat angezeigt.

3. Handlungsschritt (25 Punkte)

a) 18 Punkte
4 Punkte, 4 x 1 Punkt je Beziehung
4 Punkte, 4 x 1 Punkt je Primärschlüssel
4 Punkte, 4 x 1 Punkt je Fremdschlüssel
6 Punkte, 6 x 1 Punkt je Nichtschlüsselattribut



b) 3 Punkte

- Attribut zur eindeutigen Kennzeichnung eines Datensatzes, darf daher innerhalb einer Tabelle nur einmal vorkommen — 2 Punkte
- Ermöglicht die Kombination von Tabellen über Primär-Fremdschlüssel-Beziehungen — 1 Punkt

c) 4 Punkte

Es ist sinnvoll, nur sicherheitsrelevante Daten zu verschlüsseln, da durch die Verschlüsselung die Rechenlast des Systems stark erhöht wird. Dadurch wird die Zeit für Abfragen und Einträge verlängert.

4. Handlungsschritt (25 Punkte)

a) 3 Punkte

6 h 41 min

700 GiByte * 2^{30} * 8 Bit / 250.000.000 Bit/s = 24.051,81 s ~ 24.052 s
24.052 s / 60 = 400,8 min ~ 401 min
401 min / 60 = 6,68 h
401 - 60 * 6 = 41 min

ba) 4 Punkte

Voll-Backup einer großen Datenmenge kann lange Zeit in Anspruch nehmen
Möglichkeit des Datenverlustes bzw. der Dateninkonsistenz

bb) 4 Punkte

Ist ein „Einfrieren" eines Systems bzw. von Daten zu einem bestimmten Zeitpunkt
Anwendungen können ihre Daten weiterschreiben.
Nur die Veränderungen werden auf neue Datenblöcke geschrieben.

c) 4 Punkte

Ein Snapshot ist nicht recovery-fähig. Ein Snapshot ist Teil des Speichersystems. Ein Ausfall des physischen Speichersystems führt also zum Verlust des Schnapshots. Deswegen ist ein Backup auf ein separates Speichersystem nötig.

Andere Lösungen zu ba) – bc) sind möglich.

da) 3 Punkte

Aktion	Archiv-Bit		
	wird gesetzt	wird zurückgesetzt	wird nicht geändert
Dokument erstellen	X		
Dokument mit gesetztem Archiv-Bit umbenennen			X
Dokument lesen			X
Ein Vollbackup durchführen		X	
Eine differenzielle Datensicherung durchführen			X
Eine inkrementelle Datensicherung durchführen		X	

db) 7 Punkte

Bei der differenziellen Sicherung müssen die Backups BK-01 und BK-05 zurückgespielt werden, da die differenzelle Sicherung immer die Veränderungen bis zur letzten Vollsicherung speichert.

Bei der inkrementellen Sicherung müssen die Backups BK-01 bis BK-05 zurückgespielt werden, da die inkrementelle Sicherung immer die Veränderungen zum Vortag speichert.

5. Handlungsschritt (25 Punkte)

aa) 2 Punkte

Durch **Verschlüsselung der Daten** sind diese geschützt. Der berechtigte Zugriff ist nur mit Kenntnis des Schlüssels möglich.

ab) 2 Punkte

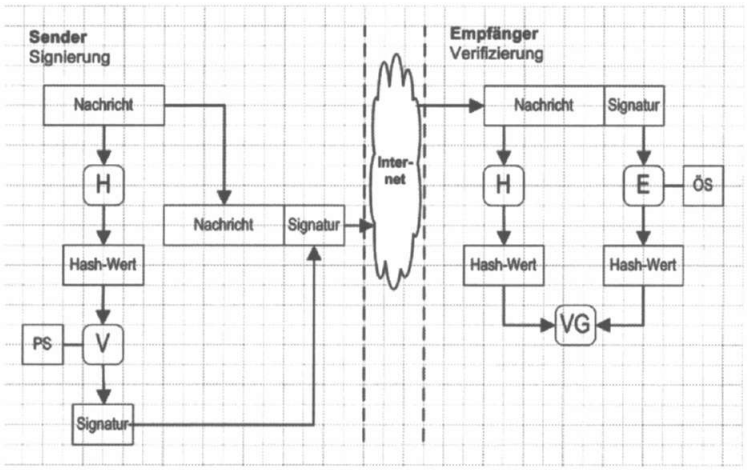
Durch eine **digitale Signatur** kann geprüft werden, ob die Nachricht vom erwarteten Absender stammt. Der Absender stellt zur Überprüfung der Signatur seinen öffentlichen Schlüssel bereit.

Eine schwächere Alternative ist die Verwendung eines **Preshared Keys (PSK)**.

ac) 2 Punkte

Durch das zusätzliche Bereitstellen einer **Prüfsumme** zur Nachricht (**Hashwert**) kann der Empfänger prüfen, ob die Nachricht verändert wurde.

b) 6 Punkte



Erläuterungen

H	Hashwert erzeugen
V	Verschlüsselung des Hashwerts mit privatem Schlüssel
E	Enstschlüsselung des Schlüssels mit öffentlichem Schlüssel
VG	Vergleich der beiden Hashwerte
PS	Privater Schlüssel
ÖS	Öffentlicher Schlüssel

Andere Lösungen sind möglich.

c) 4 Punkte, 2 x 2 Punkte

- Bei kleinsten Änderungen im Quelltext soll sich der Hashwert stark ändern.
- Es soll zu verschiedenen Quelltexten nicht den gleichen Hashwert geben.
- Der Hashwert soll vom Empfänger schnell überprüft werden können.
- Eine Rückrechnung vom Hashwert auf den Klartext darf nicht möglich sein.
- u. a.

d) 5 Punkte

Eine Public-Key-Infrastruktur (PKI) besteht aus entsprechenden Hardware- und Softwarekomponenten, die einen umfassenden Schutz innerhalb einer Organisation bei der digitalen Kommunikation und der Datenspeicherung auf Zertifikatsbasis bietet.

Somit besteht eine PKI aus Einheiten, welche die Generierung, Prüfung, Löschung usw. von Zertifikaten sicherstellt. Typischerweise ist eine PKI hierarchisch aufgebaut, untergeordnete Stellen vertrauen den übergeordneten Stellen.

Andere Lösungen sind möglich.

e) 4 Punkte

Bei WPA2-Enterprise vergibt der Administrator persönliche Zugangsdaten an diejenigen Mitarbeiter, die Zugang zum WLAN erhalten sollen. Jeder Nutzer besitzt einen eigenen Zugangscode, der von einem zentralen System validiert wird. Der administrative Aufwand ist gering, wenn es darum geht, bei einem Ausscheiden den Zugang zu sperren.

oder

Bei WPA2-Personal erhalten alle Mitarbeiter der TeNi GmbH den gleichen Zugangscode (Netzwerkschlüssel) zum WLAN. Der Administrator muss den Netzwerkschlüssel in jeden Zugangspunkt (Access Point) zum WLAN eintragen.

Eine Änderung des Netzwerkschlüssels ist bei vielen Geräten aufwendig. Jedes Gerät im WLAN muss neu konfiguriert werden.

Hinweis an den Korrektor:
- Vom Prüfling wird nur eine Erläuterung, WPA2-Personal oder WPA2-Enterprise, erwartet.
- Andere Lösungen sind möglich.