Abschlussprüfung Sommer 2019
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)

a) 7 Punkte

	Verwaltung Client 1	Schulung-1 Client 1	WLAN Client 1
IP Adresse	192.168.0.1	192.168.1.1	172.16.0.1
Subnetzmaske	255.255.255.0	255.255.255.224	255.255.252.0
Standardgateway	192.168.0.254	192.168.1.30	172.16.3.254

IP-Adresse der 3 Clients 1 Punkt insgesamt
Subnetzmaske je Client 1 Punkt
Standardgateway je Client 1 Punkt

ba) 6 Punkte

Sicherungsmaßnahme	Beurteilung der Schutzwirkung
SSID Broadcast ausschalten	Bietet wenig Sicherheit, da die SSID mit geeigneten Tools gescannt werden kann.
MAC-Adressfilter	Geringe Sicherheit, da MAC-Adressen mitgelesen bzw. gefälscht werden können.
WEP	Keine bzw. geringe Sicherheit, da es sich um einen veralteten Verschlüsselungsstandard handelt.
WPA2 Personal	Gut geeignet, wenn ein entsprechend langes und komplexes Passwort verwendet wird.

ba) 4 Punkte
WPA2 Enterprise verwendet eine benutzerbezogene Authentifizierung mit Passwort durch einen RADIUS-Server.
Erst nach Authentifizierung durch den RADIUS-Server wird dem Benutzer Zugriff auf das WLAN erlaubt.

ca) 2 Punkte

```
ip route 0.0.0.0 0.0.0.0 172.31.1.2
```

cb) 6 Punkte

Netzwerk	Subnetzmaske	Schnittstelle	Next-Hop-Adresse
172.31.1.0	255.255.255.252	LAN	----------
212.0.0.0	255.255.255.252	WAN	----------
192.168.0.0	255.255.255.0	----------	172.31.1.1
192.168.1.0	255.255.255.224	----------	172.31.1.1
192.168.2.0	255.255.255.224	----------	172.31.1.1
192.168.3.0	255.255.255.224	----------	172.31.1.1
172.16.0.0	255.255.252.0	----------	172.31.1.1
0.0.0.0	0.0.0.0	----------	212.0.0.1

Hinweis:
Für die Angabe einer zutreffenden Super-Route (z. B. 192.168.0.0/22) sind die anteiligen Punkte ebenfalls zu geben.

2. Handlungsschritt (25 Punkte)

a) 4 Punkte

Die Aufspaltung in VLANs ist aus folgenden Gründen sinnvoll:

- Reduzierung von Broadcasts
- Erhöhung der Sicherheit, z. B. durch entsprechende Firewall-Regeln zwischen den VLANs

Und andere sinnvolle Lösungen

ba) 10 Punkte

(je Erläuterung 2 Punkte)

Regel	Erläuterung
1 - 4	Verbietet den Zugriff vom VLAN-S1 zum Verwaltungs-VLAN, auf die beiden anderen Schulungsräume und auf das WLAN
5	Erlaubt http-Datenverkehr für VLAN-S1
6	Erlaubt https-Datenverkehr für VLAN-S1
7	Erlaubt DNS für VLAN-S1
8	Verbietet den übrigen Datenverkehr

bb) 3 Punkte

Firewall-Regel 8 verbietet den Ping.

bc) 4 Punkte

je Feld 0,5 Punkte,

Quell-IP nur mit richtiger Angabe der Netzmaske (/32) als richtig werten.

Aktion	Protokoll	Quell-IP	Ziel-IP	Q-Port	Z-Port	Von Interface	Nach Interface
Permit	TCP	192.168.1.29/32	Any	> 1023	25	VLAN-S1	Internet

c) 4 Punkte

Eine Sandbox ist ein vom System getrennter Bereich. In diesem Bereich laufen meist virtuelle Maschinen, die eine reale Systemumgebung nachbilden. In diesem Bereich wird die unbekannte Datei geöffnet oder installiert. So kann man das Verhalten der Dateien bzw. Software beobachten bzw. auf unerwünschtes Verhalten überprüfen.

3. Handlungsschritt (25 Punkte)

aa) 15 Punkte

Lösungsvorschläge:

Programm	Punkte
int zahl = 0; int zaehler = 0; string passwort = ""; (bzw. Deklaration der Variablen)	2
while zaehler <= 7	2
zahl = Random(127);	2
if (zahl > 32) && (zahl < 127) then	2
passwort = passwort + ChangeChar(zahl);	2
zaehler = zaehler + 1	2
End if	1
End while	1
Ausgabe passwort;	1

Andere, sinnvolle Lösungen möglich

ab) 2 Punkte

- Erhöhung der Komplexität
- Ausschluss von Wörterbuchattacken
- u. a.

b) 4 Punkte

Durch jede zusätzliche Passwortstelle verlängert sich die Rechenzeit um das 94-fache:
30 Sekunden * 94 * 94 = 265.080 Sekunden bzw. 73,63 Stunden bzw. 3,07 Tage
Die 10-stelligen Passwörter können innerhalb der Gültigkeitsdauer erraten werden.

c) 4 Punkte

- Smartcard und PIN
- Benutzername/Passwort und SMS
- Benutzername/Passwort und Token
- u. a.

4. Handlungsschritt (25 Punkte)

a) 4 Punkte
- Benutzernamen vom letzten Login ausblenden
- Verhindern des automatischen Startens von Applikationen beim Systemstart
- Login-Screen ändern
- Lokalen Admin-Account deaktivieren
- Kein automatisches Anmelden beim Starten
- Regelmäßige Updates der Betriebssysteme
- Automatisches Abmelden nach einer bestimmten Zeit ohne Eingabe
- Booten von anderen Medien verbieten
- u. a.

b) 4 Punkte
- Teamviewer-Session-ID und Passwort übergeben
- Aktive Bestätigung durch Mitarbeiter …
- Warnhinweis, Rechner wird übernommen
- Sensible Daten dürfen dem Supporter nicht angezeigt werden, z. B. Trennung von Netzlaufwerken vor Verbindungsaufbau
- User muss die Aktionen auf dem Desktop mitverfolgen können
- u. a.

ca) 2 Punkte
End-to-Site und Vermittlungsschicht (Network-Layer)

cb) 4 Punkte
Der IPSec-Client am Admin-Rechner authentifiziert den kompletten IP-Header mit einem Hashwert. Dem Header wird aber die öffentliche IP hinzugefügt, damit das Paket im Internet geroutet werden kann. Somit ändert sich aber auch der Hashwert.

cc) 3 Punkte
Der PSK wird auf beiden Seiten hinterlegt und verschlüsselt/gehashed beim Verbindungsaufbau übermittelt und verglichen. Stimmen die Werte überein, sind die Partner authentifiziert.

cd) 4 Punkte

Anforderung	Zertifikatsbestandteil
Vertraulichkeit	Schlüsselpaar des Zertifikats (öffentlicher und privater Schlüssel)
Authentizität	Fingerabdruck (digitale Signatur)

ce) 4 Punkte
- Meist wesentlich höhere Passwortlänge, dadurch besserer Schutz gegen Attacken
- Zeitliche Begrenzung des Zertifikats
- Unterstützung von Token und Smartcards
- Authentifizierung beider Gegenstellen durch Dritte (z. B. CA) möglich
- u. a.

5. Handlungsschritt (25 Punkte)

a) 6 Punkte
- Einspielen der aktuellen Sicherheitsupdates bzw. Patches
- Entfernung oder Deaktivierung von für den Betrieb nicht zwingend erforderlichen Softwarekomponenten wie z. B. Remotezugriff, FTP, WEB-Zugriff oder anderer Protokolle
- Verwendung nicht privilegierter Benutzerkonten zur Ausführung von Server-Prozessen
- Anpassung von Dateisystemrechten und ihrer Vererbung
- Nutzung von Verschlüsselung für kritische Daten

Weitere sinnvolle Aspekte sind auch als richtig zu werten.

b) 4 Punkte

```
hof c:\bs\system -r -sha3 -xml d:\sys\hashconf.xml
```

Die Parameter r, sha und xml können in beliebiger Reihenfolge stehen.
Die Zieldatei muss am Ende des Befehls stehen.

c) 4 Punkte

Berechnung der Anzahl der zu übertragenen Frame:
$N_P = 75 * 1.024 * 1.024$ Byte / 1.450 Byte = 54.237 Frame

Berechnung der Gesamt-Latenzzeit:
t_{GL} = 54.237 Frame * 0,4 ms/Frame = 21,7 s

Berechnung der Übertragungszeit:
$t_Ü = (75 * 1.024 * 1.024 * 8 / 16.000.000)$ s = 39,3 s

Berechnung der Downloadzeit:
$t_D = t_{GL} + t_Ü$ = 21,7 s + 39,3 s = 61 s

Downloadzeit: 61 Sekunden

da) 9 Punkte

Bitte beachten, dass nur drei Erläuterungen verlangt sind.

Beim Backup-as-a-Service wird der Datensicherungsprozess an einen Cloud-Anbieter ausgelagert. Dieser gewährleistet eine hochverfügbare Speicherung großer Datenmengen abseits der Firmenstruktur.

Bei der Daten-Deduplizierung wird Speicherplatz eingespart, indem mögliche Kopien von Dateien vermieden werden. Bei Dateien, die ganz oder teilweise den gleichen Inhalt haben, werden die übereinstimmenden Blöcke (Dateifragmente) nur einmal physisch gespeichert. Dadurch beschleunigt sich sowohl der Backup-Prozess als auch gegebenenfalls eine Datenwiederherstellung.

Die Replikation gewährleistet Datensicherheit, in dem der Datenbestand zwischen zwei oder mehreren Servern ständig ausgetauscht wird. Dadurch kann ein Datenverlust vermieden werden, der zwischen zeitlich folgenden Backups möglich ist.

Ein WORM Hard-Disk-Array ist eine speziell auf die Datenarchivierung optimierte Festplattenstation. Nachdem sie beschrieben wurde, ist nur noch Lesezugriff möglich.

Andere sinnvolle Lösungen sind möglich.

db) 2 Punkte
- Besonders kurze Wiederherstellzeit
- Keine Beeinträchtigung der Geschäftsprozesse durch die Datensicherung
- Mehrfache Datensicherungen
- Verschlüsselte Datensicherungen
- Beschränkter Zugang zu den Datensicherungen
- u. a.