

Diese Kopfleiste bitte unbedingt ausfüllen!

Familienname, Vorname (bitte durch eine Leerspalte trennen)

Bereich	Berufsnummer			IHK-Nummer	Prüflingsnummer		
5 5	1 1	9 7					
Sp. 1-2	Sp. 3-6	Sp. 7-9		Sp. 10-14			

Termin: Mittwoch, 8. Mai 2019

IHK

Abschlussprüfung Sommer 2019

1197

1

Ganzheitliche Aufgabe I
Fachqualifikationen

Fachinformatiker
Fachinformatikerin
Systemintegration

5 Handlungsschritte
90 Minuten Prüfungszeit
100 Punkte

Bearbeitungshinweise

- Der vorliegende Aufgabensatz besteht aus insgesamt 5 Handlungsschritten zu je 25 Punkten.

In der Prüfung zu bearbeiten sind 4 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 5. Handlungsschritt als nicht bearbeitet.

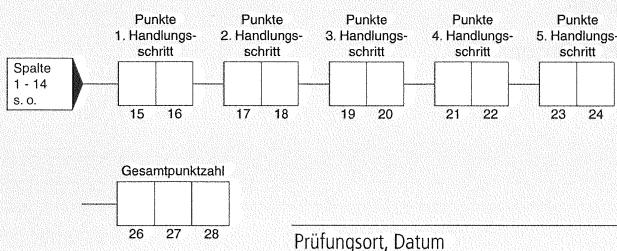
- Füllen Sie zuerst die **Kopfzeile** aus. Tragen Sie Ihren Familiennamen, Ihren Vornamen und Ihre Prüflings-Nr. in die oben stehenden Felder ein.
- Lesen Sie bitte den **Text** der Aufgaben ganz durch, bevor Sie mit der Bearbeitung beginnen.
- Halten Sie sich bei der Bearbeitung der Aufgaben genau an 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.
- 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.
- Sofern nicht ausdrücklich ein Brief oder eine Formulierung in ganzen Sätzen gefordert werden, ist eine **stichwortartige Beantwortung** zulässig.
- Verwenden Sie nur einen Kugelschreiber und schreiben Sie deutlich und gut lesbar. Ein nicht eindeutig zuzuordnendes oder **unleserliches Ergebnis** wird als **falsch** gewertet.
- Zur Lösung der Rechenaufgaben darf ein nicht programmierter, netzunabhängiger **Taschenrechner** ohne Kommunikationsmöglichkeit mit Dritten verwendet werden.
- Wenn Sie ein **gerundetes Ergebnis** eintragen und damit weiterrechnen müssen, rechnen Sie (auch im Taschenrechner) nur mit diesem gerundeten Ergebnis weiter.
- 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.



Prüfungsort, Datum

Prüfungszeit
25
Die entsprechende Ziffer (1, 2 oder 3) finden Sie in der Abfrage nach der Prüfungszeit im Anschluss an die letzte Aufgabe.

Unterschrift

Die Handlungsschritte 1 bis 5 beziehen sich auf die folgende Ausgangssituation:

Die Futur GmbH ist Dienstleister im Bereich beruflicher Weiterbildung mit der Zentrale in Frankfurt und mehreren überregionalen Außenstellen bundesweit. Die I-Net GmbH ist Internet-Provider der Futur GmbH.

Die bestehende IT-Infrastruktur der Futur GmbH soll überprüft werden. Dabei soll die Sicherheit erhöht und eine Datensicherung geplant werden.

Im Rahmen dieses Projekts sollen Sie vier der folgenden fünf Aufgaben bearbeiten:

1. Analyse der Netzwerkstruktur, Absicherung des WLANs und Einrichtung des Routings
2. Einrichtung von VLANs, Erläutern und Aufstellen von Firewall-Regeln
3. Entwicklung eines Passwortgenerators, Verbesserung der Passwortsicherheit
4. Absicherung von PC-Arbeitsplätzen, Einrichtung eines VPNs
5. Härtung von Serversystemen und der Planung eines Sicherungskonzepts

1. Handlungsschritt (25 Punkte)

Das Netzwerk der Futur GmbH besteht aus drei Schulungsräumen, einem Verwaltungsnetz und einem WLAN. Es weist die Struktur gemäß der Abbildung auf der perforierten Anlage auf.

- a) Die Clients im Netz sollen nach den folgenden Vorgaben konfiguriert werden. Client 1 erhält immer die erste IP-Adresse im jeweiligen IP-Netz, die Schnittstelle am Core-Switch die letzte IP-Adresse im jeweiligen IP-Netz. 7 Punkte

Die Subnetzmaske ist in Dezimalpunktschreibweise anzugeben.

	Verwaltung Client 1	Schulung-1 Client 1	WLAN Client 1
IP-Adresse			
Subnetzmaske			
Standardgateway			

- b) Das WLAN soll vor unberechtigten Zugriffen geschützt werden.

- ba) Beurteilen Sie die Schutzwirkung der folgenden WLAN-Sicherungsmaßnahmen (siehe Beispiel). 6 Punkte

Sicherungsmaßnahme	Beurteilung der Schutzwirkung
SSID Broadcast ausschalten	Bietet wenig Sicherheit, da die SSID mit geeigneten Tools gescannt werden kann.
MAC-Adressfilter	
WEP	
WPA2-Personal	

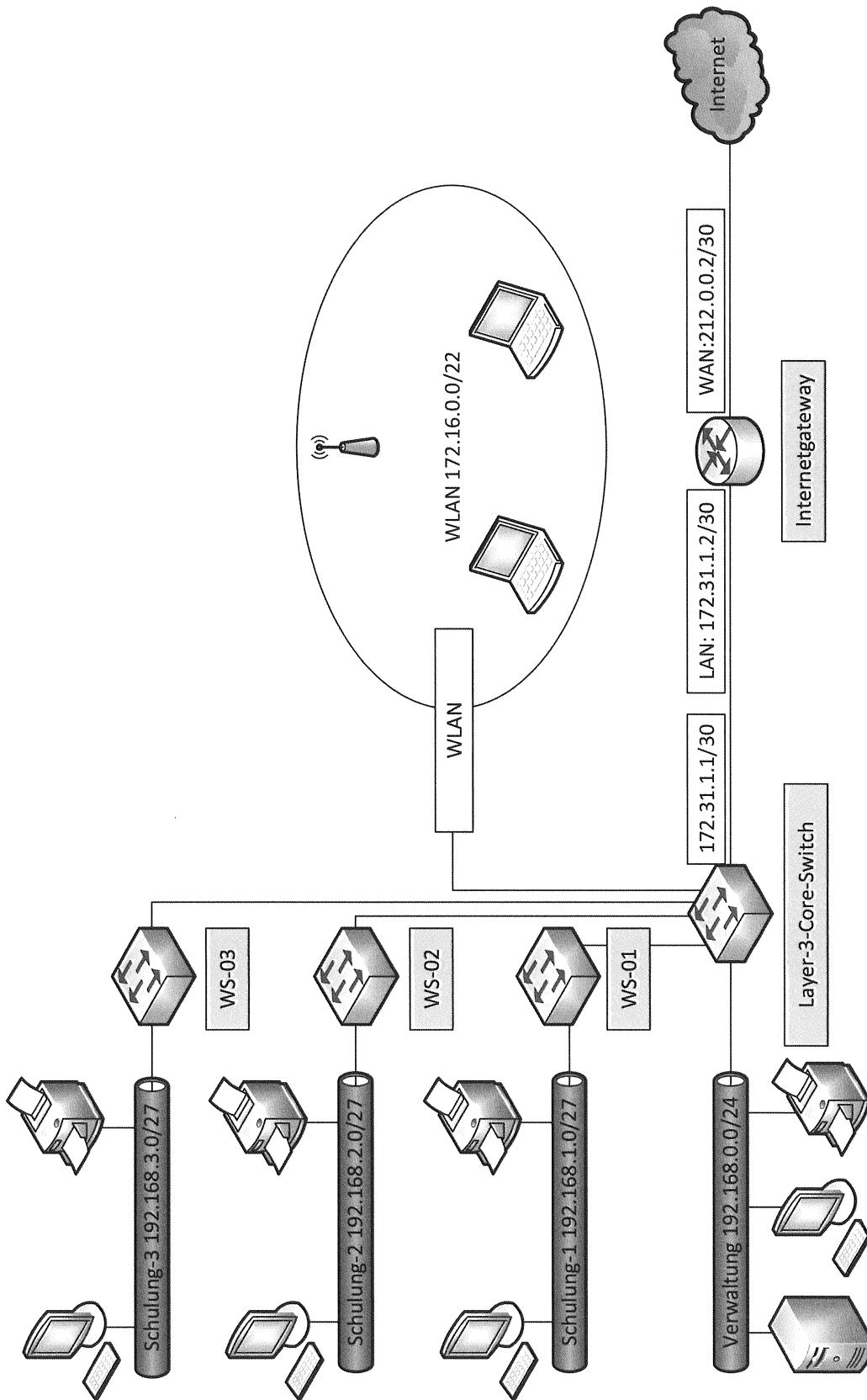
- bb) Es wird beschlossen, WPA2-Enterprise zur Absicherung des WLANs einzusetzen.

- Erläutern Sie den wesentlichen Vorteil von WPA2-Enterprise gegenüber WPA2-Personal. 4 Punkte
-
-
-
-

Dieses Blatt kann an der Perforation aus dem Aufgabensatz herausgetrennt werden!

Netzwerkplan der Futur GmbH

Netzwerkplan der Futur GmbH



c) Auf dem Core-Switch (Layer 3) und auf dem Internetgateway muss das Routing eingerichtet werden.

ca) Auf dem Core-Switch soll eine Default-Route eingerichtet werden. In der Anleitung finden Sie folgendes Beispiel:

This is an example of configuring a gateway of last resort (default route) using the **ip route 0.0.0.0 0.0.0.0 <Next hop>** command:

```
Core-switch#configure terminal
```

Enter configuration commands, one per line. End with CNTL/Z.

```
Core-switch (config)#ip route 0.0.0.0 0.0.0.0 170.170.3.4
```

```
Core-switch (config)#^Z
```

Nennen Sie die den vollständigen Befehl, um die Default-Route auf dem Core-Switch der Futur GmbH einzurichten.

2 Punkte

cb) Auch auf dem Internetgateway muss das Routing eingerichtet werden. Ergänzen Sie die folgende Routingtabelle: 6 Punkte

Hinweis: Aus der Anzahl der vorgegebenen Zeilen lässt sich die Lösung nicht ableiten.

Netzwerk	Subnetzmaske	Schnittstelle	Next-Hop-Adresse
172.31.1.0	255.255.255.252	LAN	-----
212.0.0.0	255.255.255.252	WAN	-----

2. Handlungsschritt (25 Punkte)

Korrekturrand

Die Futur GmbH möchte die Sicherheit und Systemstabilität ihres Netzwerkes erhöhen.

- a) In der Futur GmbH wurden VLANs für die drei Schulungsräume (VLAN-S1, VLAN-S2, VLAN-S3) und das Verwaltungsnetz (VLAN-Verw) eingerichtet.

Erläutern Sie zwei Gründe, warum diese Maßnahme sinnvoll ist.

4 Punkte

- b) Auf dem Core-Switch wurde eine Firewall eingerichtet.

- ba) Für den Schulungsraum 1 wurde der folgende Regelsatz konfiguriert:

Nr	Aktion	Protokoll	Quell-IP	Ziel-IP	Q-Port	Z-Port	Von Interface	Nach Interface
1	Deny	IP	192.168.1.0/27	192.168.0.0/24	-	-	VLAN-S1	VLAN-Verw
2	Deny	IP	192.168.1.0/27	192.168.2.0/27	-	-	VLAN-S1	VLAN-S2
3	Deny	IP	192.168.1.0/27	192.168.3.0/27	-	-	VLAN-S1	VLAN-S3
4	Deny	IP	192.168.1.0/27	172.16.0.0/22	-	-	VLAN-S1	VLAN-WLAN
5	Permit	TCP	192.168.1.0/27	Any	>1023	80	VLAN-S1	Internet
6	Permit	TCP	192.168.1.0/27	Any	>1023	443	VLAN-S1	Internet
7	Permit	UDP	192.168.1.0/27	Any	>1023	53	VLAN-S1	Internet
8	Deny	IP	192.168.1.0/27	Any	-	-	VLAN-S1	Any

Erläutern Sie die Regeln 1 bis 8.

Es sind die jeweiligen Anwendungen bzw. Dienste anzugeben.

10 Punkte

Regel	Erläuterung
1 - 4	
5	
6	
7	
8	

- bb) Nach der Aktivierung der Firewall-Regeln führt ein Teilnehmer im Schulungsraum 1 an einem Rechner den Befehl ping 8.8.8.8 durch und erhält die folgende Fehlermeldung:

Korrekturrand

Ping wird ausgeführt für 8.8.8.8 mit 32 Bytes Daten:
Zeitüberschreitung der Anforderung.
Zeitüberschreitung der Anforderung.
Zeitüberschreitung der Anforderung.
Zeitüberschreitung der Anforderung.

Ping-Statistik für 8.8.8.8:

Pakete: Gesendet = 4, Empfangen = 0, Verloren = 4
(100% Verlust),

Erläutern Sie, warum es zu diesem Fehler kommt.

3 Punkte

- bc) Der Drucker im VLAN-S1 soll seinen Toner selbstständig per E-Mail beim Lieferanten bestellen. Der Drucker hat die vorletzte IP-Adresse im Subnetz.

Erstellen Sie die notwendige Firewall-Regel.

4 Punkte

Aktion	Protokoll	Quell-IP	Ziel-IP	Q-Port	Z-Port	Von Interface	Nach Interface

- c) Das Internetgateway verfügt über eine integrierte Firewall-Appliance mit Sandbox-Funktionalität.

Beschreiben Sie den Zweck der Sandbox-Funktionalität.

4 Punkte

3. Handlungsschritt (25 Punkte)

Korrekturrand

Für die Generierung von Passwörtern soll ein Programm entwickelt werden. Die Sicherheit von Passwörtern soll beurteilt werden.

- a) Die firmeninterne Passwort-Richtlinie sieht vor, dass jeder Benutzer ein 8-stelliges Passwort verwendet, welches Groß- und Kleinbuchstaben sowie Ziffern und Sonderzeichen enthält.

- aa) Das Passwort besteht aus acht zufällig gewählten Zeichen des ASCII-Codes gemäß der Passwort-Richtlinie.

Beispiel: Y9\$£4R?a

Erstellen Sie in Pseudocode (Anlehnung an eine gängige Programmiersprache) einen Algorithmus für die Passwort-Generierung.

15 Punkte

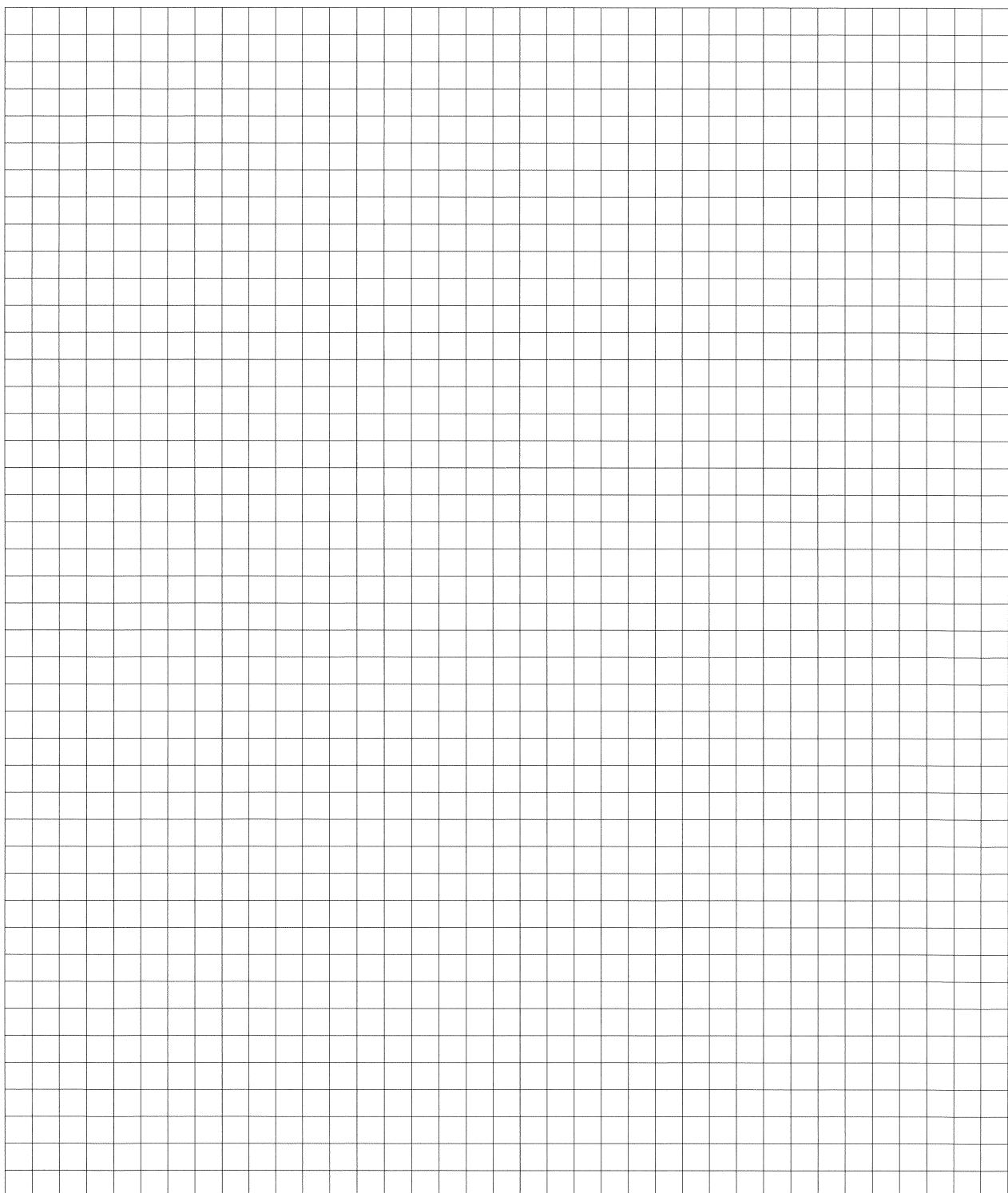
Hinweise:

Auf Seite 9 steht Ihnen die ASCII-Tabelle zur Verfügung.

Mit der Funktion Random(127) kann eine positive Ganzzahl im Bereich 0 bis 127 erzeugt werden.

Die Funktion ChangeChar(zahl) wandelt eine Zahl in das entsprechende ASCII-Zeichen um.

Das Passwort soll zur Überprüfung auf dem Bildschirm angezeigt werden.



ASCII-Tabelle

Korrekturrand

ASCII	Zeichen	ASCII	Zeichen	ASCII	Zeichen	ASCII	Zeichen
0	NUL	32	SP	64	@	96	`
1	SOH	33	!	65	A	97	a
2	STX	34	"	66	B	98	b
3	ETX	35	#	67	C	99	c
4	EOT	36	\$	68	D	100	d
5	ENQ	37	%	69	E	101	e
6	ACK	38	&	70	F	102	f
7	BEL	39	,	71	G	103	g
8	BS	40	(72	H	104	h
9	TAB	41)	73	I	105	i
10	LF	42	*	74	J	106	j
11	VT	43	+	75	K	107	k
12	FF	44	,	76	L	108	l
13	CR	45	-	77	M	109	m
14	SO	46	.	78	N	110	n
15	SI	47	/	79	O	111	o
16	DLE	48	0	80	P	112	p
17	DC1	49	1	81	Q	113	q
18	DC2	50	2	82	R	114	r
19	DC3	51	3	83	S	115	s
20	DC4	52	4	84	T	116	t
21	NAK	53	5	85	U	117	u
22	SYN	54	6	86	V	118	v
23	ETB	55	7	87	W	119	w
24	CAN	56	8	88	X	120	x
25	EM	57	9	89	Y	121	y
26	SUB	58	:	90	Z	122	z
27	Esc	59	;	91	[123	{
28	FS	60	<	92	\	124	
29	GS	61	=	93]	125	}
30	RS	62	>	94	^	126	~
31	US	63	?	95	_	127	DEL

Fortsetzung 3. Handlungsschritt

Korrekturrand

- ab) Erläutern Sie einen Grund, warum Sonderzeichen und Ziffern in Passwörtern sinnvoll sind. 2 Punkte

- b) 8-stellige Passwörter können mit einer Brute-Force-Attacke innerhalb von 30 Sekunden erraten werden. Daher wurde beschlossen, die Passwortlänge auf 10 Zeichen zu erhöhen. Jede Stelle des Passwortes besteht aus einem von 94 möglichen Zeichen. Die firmeninterne Passwortrichtlinie gibt vor, dass jedes Passwort nach spätestens 30 Tagen zu ändern ist.

Überprüfen Sie mithilfe einer Rechnung, ob jedes 10-stellige Passwort innerhalb der Gültigkeitsdauer von 30 Tagen durch eine Brute-Force-Attacke erraten werden kann. 4 Punkte

Der Rechenweg ist anzugeben.

- c) Die Sicherheit gegen unberechtigtes Anmelden soll durch eine 2-Faktor-Authentifizierung erhöht werden.

Geben Sie hierfür zwei Beispiele. 4 Punkte

4. Handlungsschritt (25 Punkte)

Korrekturrand

Sie sollen durch geeignete Maßnahmen für die IT-Sicherheit an den PC-Arbeitsplätzen sorgen.

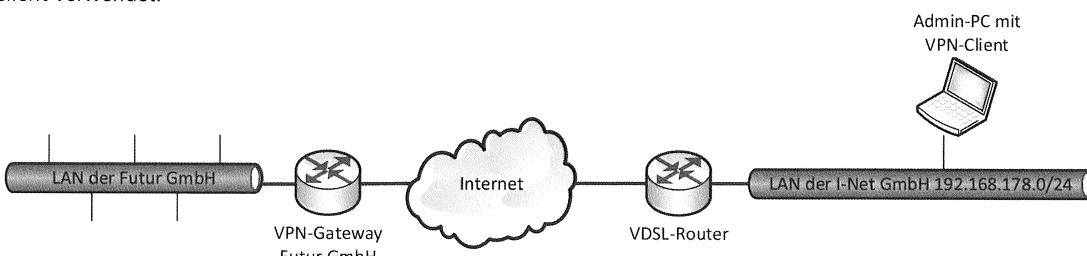
- a) Es soll verhindert werden, dass sich Unbefugte an den Arbeitsplätzen anmelden können und Zugriff auf Daten bekommen.

Nennen Sie vier mögliche Sicherheitsanpassungen, die Sie dazu an den Arbeitsplatzrechnern vornehmen. 4 Punkte

- b) Der First-Level-Support für die PC-Arbeitsplätze in der Verwaltung erfolgt über Fernwartung durch die I-Net GmbH.

Erläutern Sie zwei Maßnahmen, mit denen sowohl der Datenschutz als auch die Datensicherheit bei der Fernwartung gewährleistet werden können. 4 Punkte

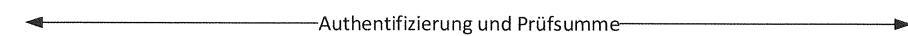
- c) Die Administratoren der I-Net GmbH sollen sich von extern mit dem LAN der Futur GmbH verbinden können. Dazu können sich die Administratoren über eine VPN-Verbindung an das Unternehmensnetz anbinden. Für die VPN-Verbindung wird ein IPSec-Client verwendet.



- ca) Nennen Sie die Art des VPNs und die Bezeichnung der Schicht im OSI-Modell, auf dem die Verbindung initiiert wird.

2 Punkte

- cb) Für die Authentifizierung und Integrität wird AH eingesetzt. AH bildet eine Prüfsumme für die Integrität über das gesamte IP-Paket. Am Router der I-Net GmbH findet ein NAT statt.



Erläutern Sie, warum der Einsatz von IPSec in diesem Fall problematisch sein könnte. 4 Punkte

Fortsetzung 4. Handlungsschritt

Korrekturrand

- cc) Die VPN-Verbindung wird über einen PSK abgesichert.

Erläutern Sie, wie ein PSK zur Authentifizierung eingesetzt wird.

3 Punkte

- cd) Die Administratoren ersetzen die PSK-Authentifizierung durch die Authentifizierung mit einem digitalen Zertifikat:

Aussteller	Futur GmbH
Signaturhashalgorithmus	SHA
Gültig von	01.01.2019
Gültig bis	31.12.2029
Inhaber	HomeOffice
Öffentlicher Schlüssel	RSA (2048 Bit)
	30 82 01 0a 02 82 01 01 00 b3 04 13 1b 80 0f a1 .. .
Fingerabdruck	dcd447f7315fcc9f0e905a2d3c55a07660f4ee7c

Digitale Zertifikate stellen Vertraulichkeit, Authentizität und Integrität sicher.

Ergänzen Sie die folgende Tabelle um den jeweiligen Zertifikatsbestandteil.

4 Punkte

Anforderung	Zertifikatsbestandteil
Vertraulichkeit	
Authentizität	

- ce) Erläutern Sie zwei Vorteile der Authentifizierung mit einem digitalen Zertifikat gegenüber der Authentifizierung mit einem PSK.

4 Punkte

5. Handlungsschritt (25 Punkte)

Korrekturrand

Sie arbeiten an dem Projekt „IT-Sicherheit 2020“ in der Futur GmbH mit. In diesem Zusammenhang sollen Sie folgende Aufgaben bearbeiten.

- a) Server-Betriebssysteme laufen nach der Installation zunächst mit Default-Einstellungen. Zur Erhöhung der Systemsicherheit wird eine Betriebssystemhärtung durchgeführt, bei der verschiedene Einstellungen entsprechend geändert werden.

Erläutern Sie zwei in diesem Zusammenhang stehende Änderungen an der Konfiguration des Server-Betriebssystems. 6 Punkte

- b) Bestimmte Dateien des Betriebssystems sollen auf Veränderungen hin überwacht werden. Dazu wird das Kommandozeilen-Programm *hof.exe* (Hash-of-File) eingesetzt, welches zu einer Datei oder einem Ordner einen Hashwert berechnet.

Von allen Dateien im Ordner „c:\bs\system“ und dortigen Unterordnern sollen Hashwerte berechnet werden. Die Hashwerte sollen in der Datei hashconf.xml im Verzeichnis d:\sys\ gespeichert werden. Es soll das Hash-Verfahren mit dem höheren Sicherheitslevel benutzt werden.

Der Syntax des Programms „*hof.exe*“ ist wie folgt:

hof.exe [parameter]

Parameterliste:

Pfad	Pfadangabe zur Datei oder zum Ordner
-r	rekursive Bearbeitung von Ordnern
-v	Hashwerte berechnen und vergleichen
-sha3	Hashalgorithmus sha256 verwenden
-md5	Hashalgorithmus md5 verwenden
-csv	Speichern der Hashwerte im csv-Format (default)
-xml	Speichern der Hashwerte im xml-Format
File	Platzhalter für die Bezeichnung der Datei, die zum Speichern oder Lesen der Hashwerte dient
-?	Hilfeaufruf

Erstellen Sie den entsprechenden Befehlsaufruf.

4 Punkte

- c) Der Download einer 75 MiB großen Update-Datei erfolgt über eine Internetverbindung mit folgenden Eigenschaften:

- Minimale Übertragungsrate: 16.000.000 bit/s
- MTU (Maximum Transmission Unit): 1.450 Byte
- Latenz pro Frame: 0,4 ms

Berechnen Sie die Zeit in Sekunden, die für den Download mindestens benötigt wird.

4 Punkte

Hinweis: Der Protokoll-Overhead soll nicht berücksichtigt werden.

Fortsetzung 5. Handlungsschritt

- d) Im Rahmen des Projekts „IT-Sicherheit 2020“ sollen die Verfahren zur Datensicherung, zur Datenarchivierung und zur Datenwiederherstellung neu konzipiert werden.

In dem Konzept sollen u. a. folgende Techniken zum Einsatz kommen:

- Backup-as-a-Service
- Deduplizierung der Daten
- Replikation der Daten
- Speichern der Daten auf WORM-Hard-Disk-Drives (Write Once Read Many)

- da) Erläutern Sie im Rahmen des Projektes **drei** der genannten Techniken.

9 Punkte

- db) In dem Konzept wird zwischen geschäftskritischen und sonstigen Daten unterschieden.

Nennen Sie zwei Aspekte, die in dem Konzept besonders für die geschäftskritischen Daten beachtet werden sollten.

2 Punkte

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.