Abschlussprüfung Sommer 2024
Lösungshinweise

Fachinformatiker/Fachinformatikerin
Systemintegration
1202

1 Konzeption und Administration von IT-Systemen

Teil 2 der Abschlussprüfung

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.).

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. Aufgabe (24 Punkte)

aa) 8 Punkte

Vorteile (je 2 Punkte):

- **Skalierbarkeit**
  Cloud-Lösungen ermöglichen es Unternehmen, ihre Ressourcen bei Bedarf schnell zu skalieren. (Dies bedeutet, dass sie zusätzliche Rechenleistung, Speicherplatz oder andere Ressourcen hinzufügen können, wenn ihr Bedarf steigt, ohne physische Hardware kaufen oder installieren zu müssen. Mehr Flexibilität und Kosteneffizienz.)
- **Zugang zu Daten**
  Flexibler, weltweiter Zugang zu Daten gewährleistet 24 h Zugriff und von allen Standorten der Welt (Flexibilität der eigenen Mitarbeiter)
- **Kostensicht**
  Einsparung von Kosten hinsichtlich eigener Hardware und Mitarbeiterkosten (Einsparpotenzial)
- u. a.

Nachteile (je 2 Punkte):

- **Sicherheitsbedenken**
  Provider müssen sicherstellen, dass die Daten wie vereinbart gespeichert werden. Datensicherheit bei Ausfall sorgt ggf. für Ängste der Kunden.
- **Zuverlässigkeit**
  Provider müssen sicherstellen, dass Zugang, Betrieb und Ausfallsicherheit lt. Vertrag gegeben sind – entspricht ggf. nicht den Kundenanforderungen
- **Ausfallsicherheit**
  Provider müssen Ausfallsicherheit und Reaktionszeiten einhalten, sonst verstoßen diese ggf. gegen gültige Verträge.
- u. a.

ab) 6 Punkte

- **Flexibilität**
  Der Provider sollte skalierbare Ressourcen und Dienste anbieten, die es ermöglichen, die Infrastruktur je nach Bedarf zu erweitern oder zu reduzieren.
- **Bezahlmöglichkeiten des Angebots**
  Ein Anbieter mit flexiblen Abrechnungsmodellen ermöglicht, Ressourcen nach Bedarf hinzuzufügen oder zu entfernen.
- **Sicherheit und Compliance**
  Der Provider sollte strenge Sicherheitsmaßnahmen und Compliance-Standards, wie etwa ISO 27001 implementiert haben. Möglichkeiten zur Verschlüsselung und Authentifizierung bieten, um die Daten vor unbefugtem Zugriff zu schützen. Eine umfassende Datenschutzregelung muss vorhanden sein, insbesondere, wenn personenbezogene Daten auf der Website verarbeitet werden.
- **Unterstützung und SLAs (Service Level Agreements)**
  Der Provider sollte einen zuverlässigen Support und klare Service Level Agreements (SLAs) bieten. Umfasst die Verfügbarkeit der Dienste, Reaktionszeiten bei Problemen sowie die allgemeine Unterstützung bei der Konfiguration und Verwaltung der Cloud-Infrastruktur. Verfügbarkeit des Supports sollte rund um die Uhr erreichbar sein und ein effektives Ticketing-System für Supportanfragen sollte bereitstehen.
- u. a.

ba) 4 Punkte

- Verantwortliche Stelle für den Datenschutz im Bankhaus
- Nennung des Datenschutzbeauftragten
- Verzeichnis der Verarbeitungstätigkeiten
- Maßnahmen zur Gewährleistung der IT-Sicherheit, wie beispielsweise regelmäßige Updates, die Nutzung von Firewalls und Antivirenprogrammen sowie die Verschlüsselung von Datenübertragungen.
- Erstellung eines Notfallplans für den Fall von Datenschutzverletzungen, der eine schnelle Reaktion und Begrenzung des Schadens ermöglicht.
- Löschfristen müssen eingehalten werden.
- u. a.

bb) 6 Punkte

- Benachrichtigung der zuständigen Datenschutzbehörde
- Kontaktaufnahme zum Empfänger mit der Aufforderung zur Löschung der Daten
- Interne Kontrolle des Vorfalls und ggf. Maßnahmen ergreifen (Datenschutzschulungen etc.)
- Information an die betroffenen Bankkunden über den Vorfall
- Dokumentationspflicht
- Maßnahmen müssen unverzüglich ergriffen werden
- u. a.

2. Aufgabe (25 Punkte)

aa) 5 Punkte

TOM	Zutrittskontrolle	Zugangskontrolle	Zugriffskontrolle
RFID-Karten, um ins Firmengebäude zu gelangen	X		
Biometrische Benutzeridentifikation am PC		X	
Berechtigungskonzept auf Dateiebene			X
Verschlüsselung von Datenträgern			X
Alarmanlage außerhalb der Geschäftszeiten	X		

ab) 6 Punkte

Confidentiality:
Vertrauliche Informationen werden vor unberechtigtem Zugriff bzw. vor Weitergabe geschützt.

Integrity:
Informationen werden vor absichtlicher oder versehentlicher Änderung geschützt.

Availability:
Dienste oder Daten müssen in der zugesicherten Zeit verfügbar sein.

Andere Formulierungen sind möglich.

ba) 3 Punkte

- Unspezifische Anrede
- Empfänger nur im CC
- Absendermailadresse @gmail.de
- Rechtschreibfehler
- Angezeigte URL ungleich der verlinkten URL
- Keine Signatur
- Keine Logos
- Grammatikfehler
- u. a.

bb) 3 Punkte

- Erhöhte Auslastung der CPU
- Computer stürzt häufiger ab
- Abnehmende Geschwindigkeit beim Surfen
- Geänderte oder gelöschte Daten
- Auftauchen von unbekannten Programmen oder Desktop-Symbolen
- Unbekannte laufende Prozesse
- Programme, die sich selbst starten, abschalten oder neu konfigurieren
- E-Mails, die ohne Wissen verschickt werden
- u. a.

bc) 4 Punkte

	Virus	Wurm	Trojaner	Ransomware
Code, der sich selbst fortlaufend über das Netzwerk repliziert und weitere Betriebssysteme befällt.		X		
Code, der sich zusammen mit anderen Programmen installiert.	X			
Code, der die Daten verschlüsselt und zu einer Zahlung an den Angreifer auffordert.				X
Code, der offensichtlich nützlich sein soll, aber im Hintergrund Systemressourcen freigibt.			X	

c) 4 Punkte

- White-Hat-Hacker: Dringen im Auftrag des Eigentümers in dessen Netze oder Systeme ein, um Schwachstellen zu finden, damit deren IT-Sicherheit verbessert werden kann. Die Ergebnisse werden ihm mitgeteilt.
- Black-Hat-Hacker: Machen sich Schwachstellen zunutze, um in Netze oder Systeme einzudringen. Auf diese Weise versuchen sie, sich persönliche, finanzielle oder sonstige Vorteile zu verschaffen.

3. Aufgabe (26 Punkte)

aa) 10 Punkte (1 Punkt je Feld)

i	CPULoad[i] Während Schritt i	max Bei Ende von Schritt i	max2 Bei Ende von Schritt i
0	12	12	0
1	10	**10**	**0**
2	40	**40**	**10**
3	73	**73**	**40**
4	33	**73**	**40**
5	60	**60**	**40**

Folgefehler sind bei der Korrektur zu berücksichtigen.

ab) 5 Punkte
Die Variable „max" für den Höchstwert der CPU-Auslastung wird in der Abfrage CPULoad[i] > max2 fälschlicherweise mit dem zweithöchsten Wert überschrieben.

ac) 5 Punkte

Programmzeile	Anweisung
17	max2 = CPULoad [i]

ba) 3 Punkte
-2.147.483.648 bis 2.147.483.647

bb) 3 Punkte
- Der Wertebereich des Datentyps „byte" ist ausreichend groß, um die ganzzahligen Prozentwerte darzustellen.
- Da der Datentyp „byte" nur positive Werte darstellt, ist sichergestellt, dass nicht versehentlich negative Werte zu einer Fehlersituation führen.

Andere Begründungen sind möglich.

4. Aufgabe (25 Punkte)

a) 6 Punkte
User CALs (Nutzer-CALs):
Werden für jeden Nutzer, der auf den Server zugreift, um verschiedene Dienste wie das Speichern von Daten oder Druckdienste zu nutzen, eingesetzt. Der Erwerb einer Nutzer-CAL ist dann sinnvoll, wenn die Mitarbeiter des Unternehmens mit mehreren Geräten einen Roaming-Zugang zum Unternehmensnetzwerk benötigen oder wenn es einfach mehr Geräte als Nutzer im Unternehmen gibt.

Device CALs (Geräte-CALs):
Werden für jedes Gerät, welches auf den Server zugreift, eingesetzt. Die Anzahl der Nutzer, die ein Gerät für den Zugriff auf den Server verwenden, ist hiervon unabhängig. Das Teilen von Geräten durch die Mitarbeiter kann wirtschaftlich und verwaltungstechnisch sinnvoll sein.

b) 6 Punkte
- Einsatz von 2-Faktor-Authentifizierung mit biometrischer Komponente
- Einsatz eines mobilen Gerätemanagements (Rücksetzungsmöglichkeit)
- Daten werden nicht auf dem mobilen Endgerät gespeichert
- Aktivierung des TPM-Chips
- Nutzung der weltweiten Geräteerkennung (Drittanbieter)
- BIOS gehärtet (Bootoptionen eingeschränkt; SecureBoot)
- u. a.

c) 6 Punkte
- Unterbrechungsfreie Stromversorgungen (USV)
- Einsetzen von Hochverfügbarkeitsclustern
- Verwendung von Load Balancing, um Anwendungs- und Netzwerkverkehr auf andere Hardware, z. B. Server, zu verteilen.
- Implementierung von zuverlässigem Crossover oder Failover in Bezug auf die Datenspeicherung (RAID, SAN)
- u. a.

da) 6 Punkte

RAID 10:
20TiB / 4 TiB = 5 Festplatten, wegen Datamirror * 2 = **10 Festplatten**

RAID 5:
20TiB / 4 TiB = 5 Festplatten, wegen Stripeset mit einfacher Parität +1 = **6 Festplatten**

RAID 6:
20TiB / 4 TiB = 5 Festplatten, wegen Stripeset mit doppelter Parität +2 = **7 Festplatten**

db) 1 Punkt
RAID 5 (s. o.)