Abschlussprüfung Winter 2024/25
Lösungshinweise

IHK

Fachinformatiker/Fachinformatikerin
Digitale Vernetzung
1204

1 Diagnose und Störungsbeseitigung in vernetzten 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 (28 Punkte)

aa) 6 Punkte

Verfügbarkeit bezieht sich darauf, wie zugänglich und einsatzbereit ein IT-System oder eine IT-Dienstleistung ist. Es misst, in welchen Maßen ein System oder eine Dienstleistung für autorisierte Benutzer verfügbar ist, wenn sie darauf zugreifen müssen. Hohe Verfügbarkeit bedeutet, dass das System oder der Dienst weitgehend ohne Unterbrechungen oder Ausfälle zur Verfügung steht.

Zuverlässigkeit bezieht sich auf die Fähigkeit eines IT-Systems, die beabsichtigten Funktionen unter angegebenen Bedingungen im vorhersehbaren Zeitrahmen zu erfüllen.

ab) 6 Punkte

Datenintegrität – Datenintegrität bezieht sich darauf, sicherzustellen, dass die gespeicherten Daten korrekt und unverändert bleiben.

Die **Systemintegrität** stellt sicher, dass das IT-System in einem ordnungsgemäßen und vertrauenswürdigen Zustand bleibt. Die Integrität reicht von der einzelnen Komponente bis zum Gesamtsystem.

Ähnliche Lösungen sind möglich.

b) 4 Punkte

360 Tage * 24 Stunden = 8.640 Stunden/Jahr

100 % = 8.640 Stunden/Jahr; 1 % = 86,4 Stunden/Jahr; 0,1 % = 8,64 Stunden/Jahr

Die Systeme dürfen maximal 8 Stunden/Jahr ausfallen.

Punkteabzug bei Aufrundung des Ergebnisses.

c) 3 Punkte

Zeitaufwand: Schnelle Änderungen und Konfigurationen sind möglich (als Reaktion auf veränderte Bedarfe und Leistungsanforderungen) sowie Automatisierung von Prozessen einfach umsetzbar.

Skalierbarkeit: Ressourcen können je nach Bedarf angepasst und skaliert werden, dadurch ist es möglich, agiler zu sein und auf veränderten Ressourcenbedarf zu reagieren.

Kosten: Kosten können gespart werden, indem die Ressourcenzuteilung bedarfsorientiert erfolgt.

In der Aufgabe muss nur eine Auswahloption ausgeführt werden. Ähnliche Lösungen sind möglich.

d) 9 Punkte

SaaS (Software as a Service): Dem Nutzer wird eine Cloud-Anwendung mit all ihren zugrundeliegenden IT-Infrastrukturen und -Plattformen zur Verfügung gestellt. Software muss so nicht lokal installiert sein.

PaaS (Platform as a Service): Bereitstellung von Entwicklungsumgebung und Tools für die Entwicklung von neuen Anwendungen.

IaaS (Infrastructure as a Service): Nutzer erhalten über das Internet Zugriff auf eine sofort nutzbare, hochgradig skalierbare IT-Infrastruktur. Die Lagerung, Verwaltung und Instandhaltung der zugrundeliegenden Hardware übernimmt der Anbieter.

2. Aufgabe (22 Punkte)

aa) 6 Punkte

Vorteile eines Ticketsystems:

Zeitersparnis durch standardisierte Prozessabläufe, Feldwert-Prüfungen und transparent einsehbare Tätigkeitsschritte. Hierdurch werden Fehler schneller gefunden und Probleme zuverlässiger analysiert. Durch Feldwert-Prüfungen wird das Fehlerpotenzial im Ticketsystem selbst minimiert.

Bearbeitung von Anfragen mittels hinterlegter Systematik: Hierfür werden Prozesse und Workflows definiert. Der Support bearbeitet Anfragen je nach hinterlegter Priorität. Die Anfrager und ihre Anfragen werden z. B. in Kritikalitätsklassen eingeteilt.

Mögliche Hinterlegung einer Wissensdatenbank: Viele Ticketsysteme bieten eine Wissensdatenbank für die Lösung von bereits gemeldeten Problemfällen. Die Mitarbeiter im Support können diese Wissensdatenbank pflegen und um neue Known-Errors ergänzen. Hierdurch wird die Bearbeitungszeit von Tickets beschleunigt.

Verbesserung der Servicequalität: Verbesserte Transparenz des Bearbeitungsstandes. Abruf des Ticketstatus jederzeit durch alle Mitglieder des Serviceteams und den Anwender möglich. Geringere Durchlaufzeit des Tickets, weil das gesamte Serviceteam Zugriff auf die eingegangenen Fälle hat.

Eine kurze Beschreibung ist ausreichend, zwei Punkte je korrekter Beschreibung. Ähnliche Lösungen sind möglich.

ab) 2 Punkte

Ein Service-Request ist eine Anfrage nach einem bestehenden Service (z. B. Benutzerzugriffsverwaltung), während ein Incident ein unerwartetes Ereignis ist, das den Service beeinträchtigt.

Zwei Punkte für eine zutreffende Beschreibung. Ähnliche Lösungen sind möglich.

ba) 4 Punkte

XML	– Textbasiertes hierarchisches Datenformat – Elemente des Strukturbaums können Text oder weitere Elemente enthalten. – Die Elemente sind durch Start- und Endtag ausgezeichnet. – Wird häufig bei SOAP-Webservices eingesetzt
JSON	– Textbasiertes hierarchisches Datenformat, bei dem Elemente des Strukturbaums Werte oder weitere Elemente enthalten können – Die Elemente sind in geschweiften Klammern zusammengefasst. – Wird häufig bei REST-Webservices eingesetzt

Ein Punkt je korrekter Nennung eines Merkmals.

bb) 5 Punkte

Mögliche Argumente für die Wahl von SOAP:
- Integrierte Sicherheits- und Transaktionskonformität
- Komplexere ACID-Transaktionen werden unterstützt

Mögliche Argumente für die Wahl von REST:
- Einfacher zu verwenden, da keine besonderen Anforderungen wie XML gestellt werden
- Verbraucht weniger Ressourcen und bietet eine gute Performance
- Einfacher zu implementieren als SOAP

Ein Punkt für die abschließende Entscheidung und zwei Punkte je Beschreibung eines Argumentes.

c) 5 Punkte
- Häufigkeiten je Störungsart
- Zeitpunkt der Störungen
- Lösungen und deren Häufigkeit
- Wiederkehrende Muster
- Betriebszeiten und Ausfallzeiten

Ähnliche Lösungen sind möglich.

3. Aufgabe (26 Punkte)

aa) 8 Punkte

P Kamera-Anforderungen festlegen, Erkennungsbereich festlegen, Angebote einholen, theoretische Ausleuchtung bezogen auf alle kritischen Zugänge etc.	**D** Anbringen der Kameras, Einbindung in das lokale Netzwerk etc.
C Überprüfen der Sichtfelder der Kameras für 24 h, um Aussetzer ausschließen zu können etc.	**A** Vergleich des Ergebnisses mit dem Anforderungsprofil, Kundenerfahrung auswerten, Fehlersituation analysieren, Verbesserungen planen etc.

ab) 4 Punkte

Mögliche zu beschreibende Merkmale (2 erforderlich):

- WLAN-Datentransferrate: Die WLAN-Datentransferrate (80 Mbit/s) ist gering im Vergleich mit einem aktuellen Standard von mindestens 300 Mbit/s.
- Firewall: Ein Paketfilter erfüllt nicht alle Funktionalitäten, die eine neue Firewall beherrschen sollte.
- Netzwerkprotokolle: Eine Unterstützung lediglich des IPv4-Standards ist technisch veraltet. Die Unterstützung des IPv6-Standards ist notwendig.
- Unterstützte Sicherheitsalgorithmen: WPA3 fehlt und könnte im Sinne der kritischen Infrastruktur aus Sicherheitsgründen Sinn machen.

ac) 4 Punkte

- Auswahl eines neuen Routers
- Dokumentieren der Leistungsmerkmale des neuen Routers möglichst mit Bezug zum Anforderungskatalog für Netzwerkgeräte im Bereich kritischer Infrastruktur und ggf. Zertifikate
- Reflexion, ob damit alle Anforderungen erfüllt sind
- Implementieren der Änderungen des Leistungspakets in allen Angebotsunterlagen des Unternehmens und der Beschreibung des Leistungspakets

Weitere ähnliche Antworten sind möglich.

ad) 6 Punkte

Beschreibung Allow-Liste:
Bei der Allow-Liste werden nur bestimmte IP-Adressen, Domains, Ports oder Anwendungen als vertrauenswürdig eingestuft und der Zugriff darauf erlaubt. Alles, was nicht auf der Erlaubnisliste steht, ist standardmäßig blockiert.

Beschreibung Block-Liste:
Bei der Block-Liste werden spezifische IP-Adressen, Domains, Ports oder Anwendungen identifiziert, die als unsicher oder unerwünscht gelten, und der Zugriff auf sie wird explizit verboten. Alles, was nicht auf der Blockliste steht, ist standardmäßig erlaubt.

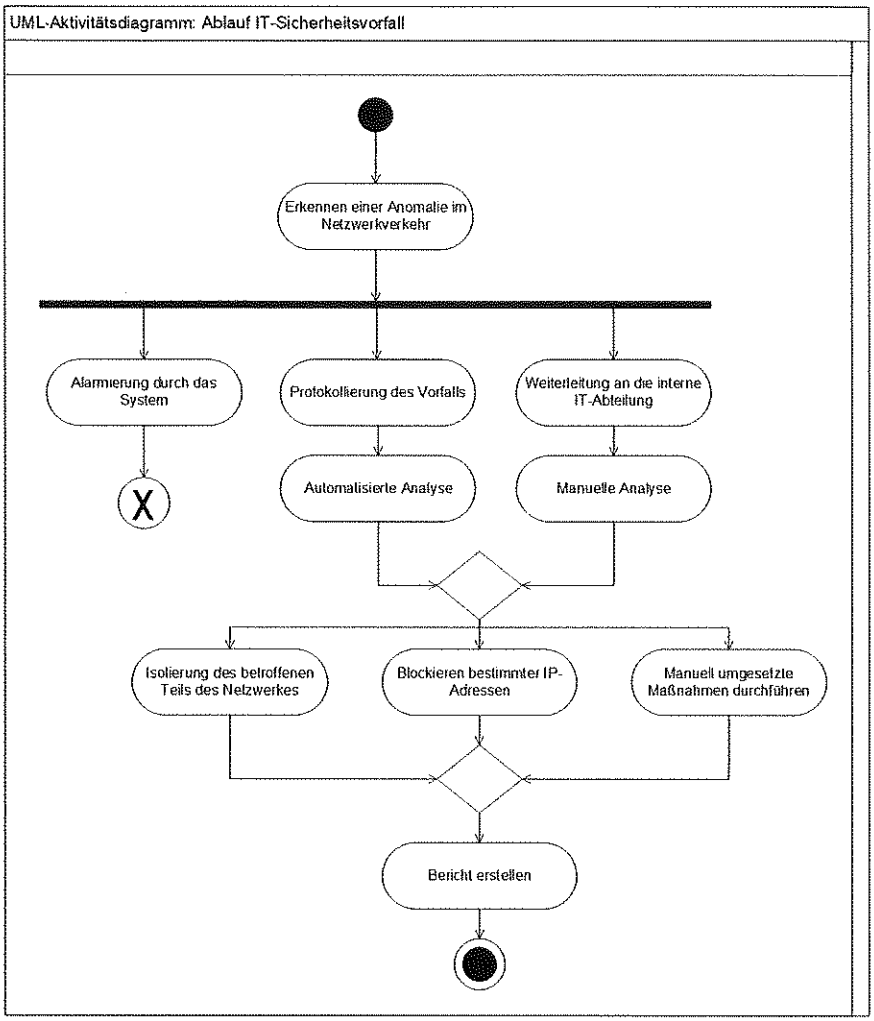
Begründung für die verwendete Policy-Regel:
Allow-Liste, da dieser Ansatz restriktiver ist und somit einen erhöhten Sicherheitsgrad bietet, der zum Umfeld der kritischen Infrastrukturen passt.

b) 4 Punkte

Gesetzliche Grundlage	DSGVO/Datenschutz-Grundverordnung/GDPR (gleichermaßen zulässig)
Mögliche Grundsätze	– Rechtmäßigkeit – Transparenz – Zweckmäßigkeit – Datensparsamkeit – Datenpannen melden – Löschung/Speicherbegrenzung – Integrität – Vertraulichkeit

4. Aufgabe (24 Punkte)

a) 12 Punkte



In der vorgeschlagenen Lösung sind **drei** Aktivitäten à 4 Punkte zu ergänzen, bei denen folgende Aspekte korrekt sein müssen (entsprechender Punkteabzug bei Nichteinhaltung):

1. Startpunkt des Kontrollflusses
2. Endpunkt des Kontrollflusses
3. Form für die Aktivität (z. B. nicht eckig)
4. Beschriftung (Wortlaut muss nicht exakt laut Musterlösung sein)

b) 8 Punkte

Zwei der drei Abschnitte müssen erläutert sein: Funktionsweise 2 Punkte, Ziel 2 Punkte, Bezug auf Quellcode nicht klar erkennbar – 1 Punkt

Zeile 6-8: Dieser Codeabschnitt überwacht die Datenübertragung und löst einen Alarm aus, wenn ein inaktiver Benutzer eine unüblich große Menge an Daten überträgt, die den vordefinierten Schwellenwert überschreitet. Das dient dazu, verdächtige Aktivitäten von normalen Übertragungen zu unterscheiden.

Zeile 10-19: Hier wird die Anzahl der fehlgeschlagenen Zugriffsversuche auf eine besonders geschützte Ressource gezählt. Wenn diese Anzahl den vordefinierten Schwellenwert überschreitet, wird ein Alarm ausgelöst. Dies dient dazu, auf potenzielle Angriffsversuche oder Sicherheitsverletzungen hinzuweisen.

Zeile 21-25: Dieser Abschnitt analysiert den Netzwerkverkehr und löst einen Alarm aus, wenn ein Paket an einen Server gesendet wird, der nicht zu den vordefinierten Kommunikationspartnern des Unternehmens gehört. Das hilft dabei, unautorisierte Kommunikation zu erkennen, die auf mögliche Bedrohungen hinweisen könnte.

c) 4 Punkte

Automatisierte Reaktionsmaßnahmen:

- Sofortige Reaktion auf Sicherheitsvorfälle möglich
- Reaktionen auch außerhalb der regulären Arbeitszeiten möglich
- Ausbreitung von Angriffen kann schnell begrenzt werden
- Bekannte Angriffsmuster können effizient und effektiv bewältigt werden

Manuelle Eingriffe:

- Flexiblere Reaktionsmöglichkeit, bei der je nach Kontext reagiert werden kann
- Erkennen von Zusammenhängen außerhalb der Systemgrenzen
- Neue und individuelle Lösungen möglich
- Komplexen/neuartigen Angriffen kann begegnet werden

Vergleichbare Lösungen sind ebenfalls zulässig.