

Familienname, Vorname (bitte durch eine Leerspalte trennen)

[illegible]

IHK

Bereich	Berufsnummer	IHK-Nummer	Prüfungsnummer
7 5	1 2 0 4		
Sp. 1-2	Sp. 3-6	Sp. 7-9	Sp. 10-14

Termin: Mittwoch, 27. November 2024

Abschlussprüfung Winter 2024/25

1204



Diagnose und Störungsbeseitigung in vernetzten Systemen

Fachinformatiker
Fachinformatikerin
Digitale Vernetzung

Teil 2 der Abschlussprüfung

4 Aufgaben

90 Minuten Prüfungszeit

100 Punkte

Bearbeitungshinweise

1. Bevor Sie mit der Bearbeitung der Aufgaben beginnen, überprüfen Sie bitte die **Vollständigkeit** dieses Aufgabensatzes. Die Anzahl der zu bearbeitenden Aufgaben ist auf dem Deckblatt links angegeben. Wenden Sie sich bei Unstimmigkeiten sofort an die Aufsicht, weil Reklamationen am Ende der Prüfung nicht anerkannt werden können.
2. Füllen Sie zuerst die **Kopfzeile** aus. Tragen Sie Ihren Familiennamen, Ihren Vornamen und Ihre Prüflings-Nr. in die oben stehenden Felder ein.
3. Lesen Sie bitte den **Text** der Aufgaben ganz durch, bevor Sie mit der Bearbeitung beginnen.
4. 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.
5. Tragen Sie die frei zu formulierenden **Antworten dieser offenen Aufgaben** in die dafür lt. Aufgabenstellung vorgesehenen Bereiche (Lösungszeilen, Formulare, Tabellen u. a.) des Arbeitsbogens ein.
6. Sofern nicht ausdrücklich ein Brief oder eine Formulierung in ganzen Sätzen gefordert werden, ist eine **stichwortartige Beantwortung** zulässig.
7. Schreiben Sie deutlich und gut lesbar. Ein nicht eindeutig zuzuordnendes oder **unleserliches Ergebnis** wird als **falsch** gewertet.
8. Zur Lösung der Rechenaufgaben darf ein nicht programmierter, netzunabhängiger **Taschenrechner** ohne Kommunikationsmöglichkeit mit Dritten verwendet werden.
9. Wenn Sie ein **gerundetes Ergebnis** eintragen und damit weiterrechnen müssen, rechnen Sie (auch im Taschenrechner) nur mit diesem gerundeten Ergebnis weiter.
10. Für **Hilfsaufzeichnungen** können Sie das in der Tasche beigelegte Konzeptpapier verwenden. Bewertet werden jedoch grundsätzlich nur Ihre Eintragungen in diesem Aufgabensatz.

Wird vom Korrektor ausgefüllt!

Bewertung

Für die Bewertung gilt die Vorgabe der Punkte in den Lösungshinweisen.

1. Aufg.

--	--

 Punkte 2. Aufg.

--	--

 Punkte 3. Aufg.

--	--

 Punkte 4. Aufg.

--	--

 Punkte

15 16 17 18 19 20 21 22

Prüfungszeit

23

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

Gesamtpunktzahl

24	25	26

Prüfungsort, Datum

Unterschrift

Gemeinsame Prüfungsaufgaben der Industrie- und Handelskammern. Dieser Aufgabensatz wurde von einem überregionalen Ausschuss, der entsprechend § 40 Berufsbildungsgesetz zusammengesetzt ist, beschlossen. Hinweis: Im Interesse einer besseren Lesbarkeit wird in der Aufgabenstellung und in den Angaben zur Aufgabenstellung nur die männliche Form (generisches Maskulinum) verwendet. Die verkürzte Sprachform beinhaltet keine Wertung und die gewählten männlichen Formulierungen gelten uneingeschränkt auch für die weiteren Geschlechter. Die Vervielfältigung, Verbreitung und öffentliche Wiedergabe der Prüfungsaufgaben und Lösungen ist nicht gestattet. Zuwiderhandlungen werden zivil- und strafrechtlich (§§ 97 ff., 106 ff. UrhG) verfolgt. – © ZPA Nord-West 2024 – Alle Rechte vorbehalten!

Die Aufgaben 1 bis 4 beziehen sich auf die folgende Ausgangssituation:

Sie sind als Fachinformatiker der Fachrichtung Digitale Vernetzung bei der KCIK Solutions GmbH beschäftigt. Dies ist ein spezialisierter Lösungsanbieter für Industrie- und Windkraftanlagen.

Das Unternehmensportfolio umfasst Einzelmodule für Windkraftanlagen, Industrie-IT-Hardware, Zutrittssysteme, Überwachungs- und Monitoringlösungen sowie unterschiedliche modulare Sensoren.

Sie durchlaufen verschiedene Abteilungen.

Dabei bearbeiten Sie die folgenden Aufgaben:

1. Aufgabe: Leistungsverfügbarkeit klären und Orte der Leistungserbringung abgrenzen
2. Aufgabe: Ticketsysteme bedienen und erweitern
3. Aufgabe: Leistungspaket zur Anlagensicherung prüfen und Änderungen durchführen
4. Aufgabe: IT-Sicherheitsmaßnahmen im Gesamtsystem konzeptionieren

1. Aufgabe (28 Punkte)

Als Mitarbeiter der IT-Abteilung bei der KCIK Solutions GmbH sind Sie beauftragt, den Einsatz eines Monitoring-Tools zu prüfen, Cloud-Lösungen zu evaluieren und die Verfügbarkeit der Systeme zu verbessern.

aa) Verfügbarkeit und Zuverlässigkeit sind zwei wichtige Konzepte im Bereich der Informationssicherheit und des IT-Service-Managements.

Erläutern Sie die beiden Begriffe.

6 Punkte

Verfügbarkeit:

Zuverlässigkeit:

ab) Die Integrität wird in Daten- und Systemintegrität unterschieden.

Erläutern Sie die beiden Konzepte.

6 Punkte


Datenintegrität:

Systemintegrität:

Korrekturrand

4 Punkte

Der Rechenweg ist anzugeben. Das Ergebnis ist auf volle Stunden zu runden.



Wählen Sie **einen** der nachfolgend genannten Aspekte aus und erläutern Sie, inwiefern sich der von Ihnen gewählte Aspekt nach Implementierung der Cloud-Lösung positiv verändern kann. 3 Punkte

- Zeitaufwand
- Skalierbarkeit
- Kosten

Gewählter Aspekt: (siehe oben)	
Erläuterung:	

Fortsetzung 1. Aufgabe

Korrekturrand

d) Ihr Cloud-Provider bietet Ihnen verschiedene Liefermodelle für die Cloud-Dienste an, dabei fallen folgende Begriffe: SaaS, PaaS und IaaS.

Befüllen Sie die Tabelle, indem Sie die Abkürzungen ausschreiben und das jeweilige Modell beschreiben.

9 Punkte

	Abkürzung ausgeschrieben	Beschreibung
SaaS		
PaaS		
IaaS		

2. Aufgabe (22 Punkte)

Mit Abschluss eines neuen Großauftrags ist ein größeres Aufkommen von Support-Anfragen zu erwarten. Der Leiter des IT-Service-Managements überlegt daraufhin, ein Ticketsystem im Sinne des IT-Service-Managements einzuführen. Das Ticketsystem soll künftig der Kundenzugang sein, um Störungen zu melden, Unterstützung anzufragen und weitreichende Support-Antworten zu erhalten.

aa) Beschreiben Sie anhand von drei Beispielen Vorteile bzw. Erfolgsfaktoren beim Einsatz eines Ticketsystems für das Incident Management.

6 Punkte

Vorteile:

-

-

-

ab) Beschreiben Sie den Unterschied zwischen einem Service-Request und einem Incident. 2 Punkte

Korrekturrand

b) Um die Mitarbeiter der Supportabteilung zu entlasten, soll eine neue und für Kunden zugängliche Webapplikation erstellt werden. Diese Applikation soll als schwarzes Brett dienen und mehrfach gemeldete tagesaktuelle Störungen transparent darstellen. Für den Datenaustausch des Ticketsystems zur neuen Webapplikation können unterschiedliche Formate verwendet werden.

ba) Nennen Sie jeweils zwei Merkmale der folgenden Datenformate. 4 Punkte

XML	
JSON	

bb) Die notwendigen Daten für die neue Webapplikation können über **REST**- oder **SOAP**-Schnittstellen vom Ticketsystem abgefragt werden.

Entscheiden Sie sich anhand von zwei Argumenten für eine der beiden Schnittstellenarten. 5 Punkte

Argument 1:

Argument 2:

Zu verwendende Schnittstellenart:

c) In Zukunft möchte die KCIK Solutions GmbH für die interne IT auch Methoden zur frühzeitigen bzw. vorausschauenden Wartung einsetzen (Predictive Maintenance). Ziel ist ein möglichst unterbrechungsfreier IT-Betrieb. Hierfür sind geeignete Parameter heranzuziehen.

Nennen Sie fünf Daten, die hierfür aus einem Monitoringsystem abgefragt und berücksichtigt werden können. 5 Punkte

3. Aufgabe (26 Punkte)

Korrekturrand

Die von der KCIK Solutions GmbH betreuten Windanlagen gehören zum Energieversorgungssystem und müssen deswegen als Teil der kritischen Infrastruktur besonders geschützt werden.

Sie sind beauftragt, das **Leistungspaket** der KCIK Solutions GmbH in einem PDCA-Zyklus zu überprüfen, das Windkraftanlagenbetreibern angeboten wird. Neben der Sicherung der Anlage sind bei der Lösung auch datenschutzrechtliche Anforderungen zu erfüllen.

Bestandteile des **Leistungspakets** sind ...

- 1) ein Industrie-WLAN-Router.
- 2) eine Firewall.
- 3) drei Sicherheitskameras, im Außenbereich der Windkraftanlage, am Zugang zur zentralen Steuerungseinheit und am Zugang zum Turmaufzug.

aa) Im Folgenden sind Sie damit beauftragt, zu einem exemplarischen Szenario zu 3) (= Sicherheitskameras) einen PDCA-Zyklus zur Funktionsprüfung darzustellen. Ziel ist es, alle sicherheitsrelevanten Sichtbereiche mit Kameras abzudecken.

Beschreiben Sie hierfür pro Abschnitt eine Tätigkeit.

8 Punkte

P(lan)	D(o)
C(heck)	A(ct)

ab) Ihnen liegt ein Datenblatt zu dem Router vor, der bisher im Leistungspaket verwendet wird.

Beschreiben Sie anhand von zwei Merkmalen, dass dieses Gerät nicht mehr dem Stand der Technik entspricht.

4 Punkte

Datenblatt des bisherigen Standardrouters im Leistungspaket:

WLAN Router Modell PaulBox 23.5	
Physische WAN-Schnittstelle	RJ-45
WLAN-Band	Einzelband (2,4GHz)
Top WLAN-Standard	Wi-Fi 4 (802.11n)
WLAN Datentransferrate (max.)	80 Mbit/s
Schnittstellentyp Ethernet-LAN	Fast Ethernet
Ethernet LAN Datentransferraten	10/100 Mbit/s
Verkabelungstechnologie	10/100 Base-T(X)
Unterstützte Sicherheitsalgorithmen	WEP, WPA, WPA-Enterprise, WPA2, WPA2-Enterprise
Firewall	Paketfilter
Unterstützte Netzwerkprotokolle	IPv4, TCP, UDP

Merkmal 1:

Merkmal 2:

ac) Beschreiben Sie zwei weitere Arbeitsschritte, die notwendig sind, wenn der Router im Leistungspaket ausgetauscht wird.

Korrekturrand

4 Punkte

Beispiel: Suche nach einem neuen Router

ad) Als nächsten Prüfschritt untersuchen Sie die eingesetzte Firewall-Lösung. Die Policy-Regeln einer Firewall arbeiten entweder eine Allow-Liste (white list) oder eine Block-Liste (black list) ab.

Beschreiben Sie die beiden Methoden. Entscheiden Sie sich dann für eine der beiden Policy-Regeln im Anwendungsfall mit einer nachvollziehbaren Begründung.

6 Punkte

Beschreibung Allow-Liste:

Beschreibung Block-Liste:

Begründung für die verwendete Policy-Regel:

b) Betritt autorisiertes Wartungspersonal die Windkraftanlage, geraten diese Mitarbeiter in den Sichtbereich der Kameras zur Anlagenüberwachung. Diese Bilder der Überwachungskameras stellen personenbezogene Daten dar, die besonders schützenswert sind.

Nennen Sie die gesetzliche Grundlage, die den Datenschutz in der EU regelt, und nennen Sie drei Grundsätze, die entsprechend der gesetzlichen Grundlage beachtet werden müssen.

4 Punkte

Gesetzliche Grundlage	
Grundsatz	
Grundsatz	
Grundsatz	

4. Aufgabe (24 Punkte)

Korrekturrand

Als Teil der internen IT-Abteilung werden Sie mit der Konzeptionierung von IT-Sicherheitsmaßnahmen innerhalb der KCIK Solutions GmbH beauftragt.

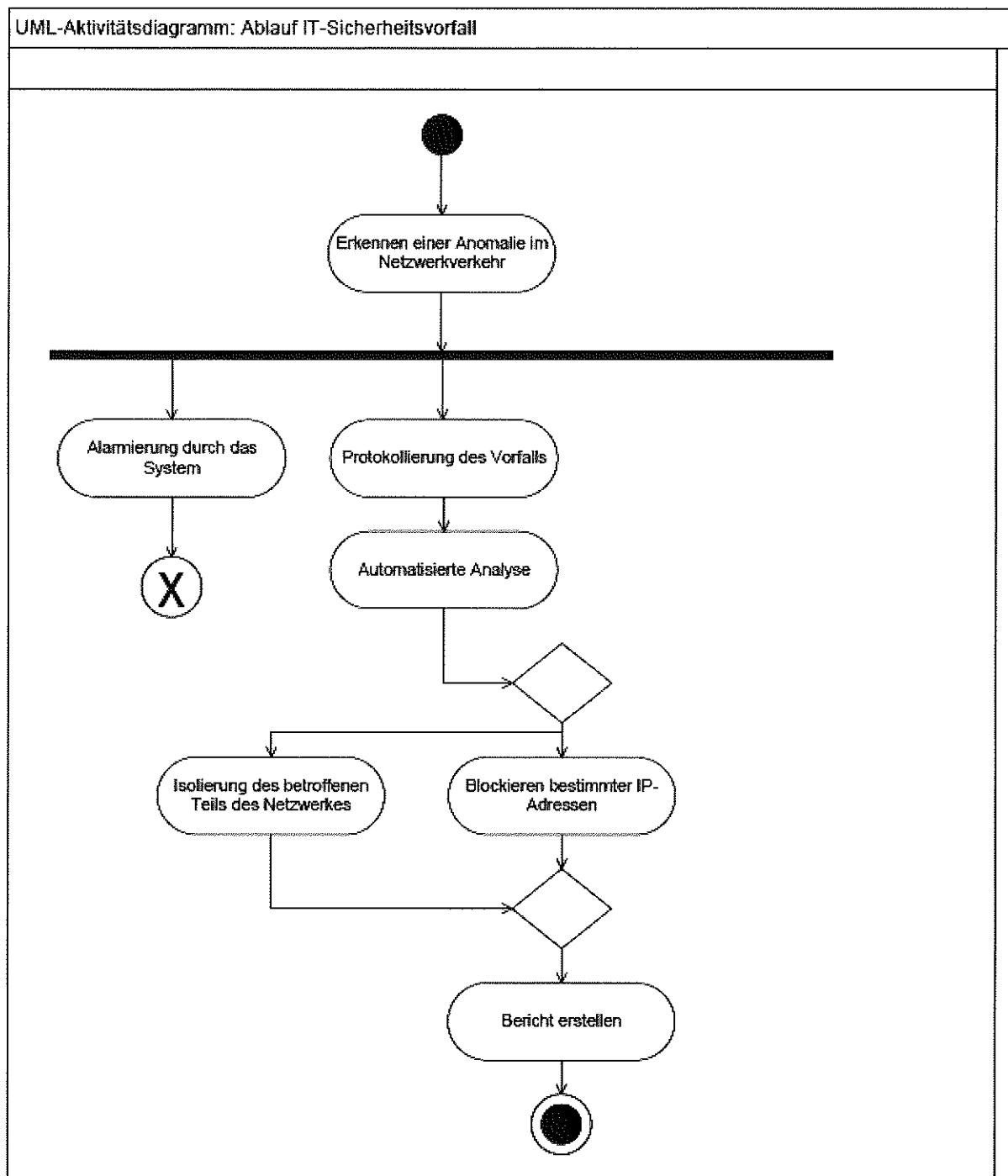
- a) Nach den letzten Sicherheitsvorfällen ist eine zusätzliche Sicherheitsmaßnahme beschlossen worden. Der Prozess zur Anomalie-Erkennung und -Behandlung in den Systemen ist zur besseren Übersicht mit einem UML-Aktivitätsdiagramm veranschaulicht.

Der Prozess soll folgendermaßen erweitert werden:

Die interne IT-Abteilung führt zeitgleich mit der automatischen Analyse eine detaillierte manuelle Analyse durch. Hierzu sendet das System eine Benachrichtigung an die Abteilung, damit sie die Schwere des Vorfalls bewerten kann. Wenn es zum manuellen Eingreifen durch die interne IT-Abteilung kommt, können vordefinierte Maßnahmen, aber auch eine manuell umgesetzte Maßnahme zum Einsatz kommen, um den Angriff zu stoppen.

Ergänzen Sie das vorliegende Aktivitätsdiagramm entsprechend.

12 Punkte



Aktivitätsdiagramm

Startknoten



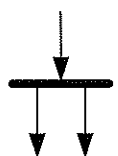
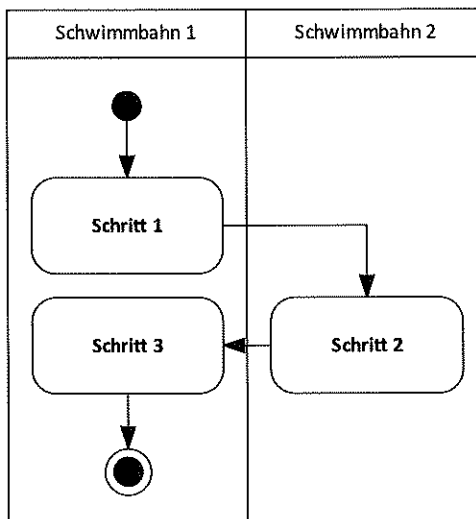
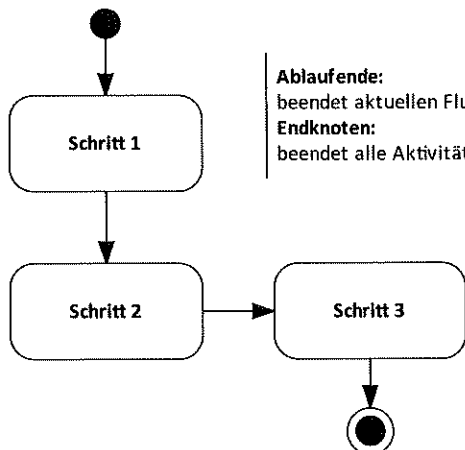
Endknoten



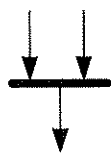
Ablaufende



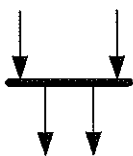
Ablaufende:
beendet aktuellen Fluss
Endknoten:
beendet alle Aktivitäten



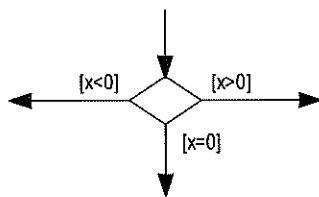
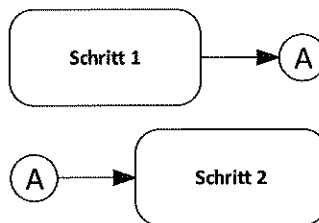
Teilung
(Splitting)



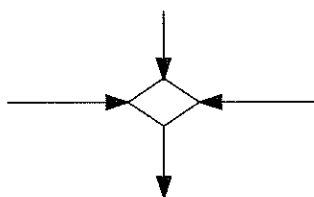
Synchronisation
(Und)



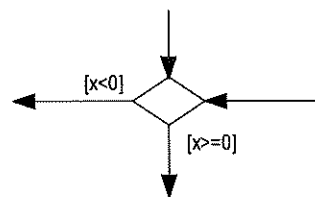
Teilung und
Synchronisation



Entscheidung



Zusammenführung
(Oder)



Entscheidung und
Zusammenführung

Fortsetzung 4. Aufgabe

Korrekturrand

b) Sie verschaffen sich einen Einblick in die Programmierlogik der Netzwerk- und Systemüberwachung. Folgender Quellcode liegt Ihnen vor.

```
1 class NetzwerkUeberwachung:
2     def __init__(self):
3         self.SW_DATENUEBERTRAGUNG = 1000
4         self.SW_FEHLGESCHLAGENE_ZUGRIFFE = 3
5
6     def code1_ueberwachung(self, benutzer, datenmenge):
7         if benutzer.inaktiv and datenmenge > self.SW_DATENUEBERTRAGUNG:
8             self.ausloese_alarm("Alarm Code 1")
9
10    def code2_ueberwachung(self, ressource, zugriffsversuche):
11        fehlgeschlagene_zugriffe_auf_geschuetzte_ressource = 0
12        for versuch in zugriffsversuche:
13            if ressource.besonders_geschuetzt and
14                versuch.fehlgeschlagen:
15                fehlgeschlagene_zugriffe_auf_geschuetzte_ressource += 1
16
17        if fehlgeschlagene_zugriffe_auf_geschuetzte_ressource >
18            self.SCHWELLENWERT_FEHLGESCHLAGENE_ZUGRIFFE:
19            self.ausloese_alarm("Alarm Code 2")
20
21    def code3_ueberwachung(self, netzwerkverkehr):
22        for paket in netzwerkverkehr:
23            if not paket.zieladresse in
24                unternehmens_kommunikationspartner:
25                self.ausloese_alarm("Alarm Code 3")
26
27    def ausloese_alarm(self, nachricht):
28        print(f"Alarm: {nachricht}")
```

Hier sind Prüfungen und Reaktionen auf verschiedene Anomalien programmiert. Eine Anomalie ist z. B. eine Manipulation, welche die Systemintegrität beeinträchtigt (nicht im Quellcode enthalten).

Erläutern Sie zwei im Quellcode erkennbare Anomalie-Prüfungen, jeweils mit ihrer Funktionsweise und ihrem Ziel. 8 Punkte

Hinweis: Für den Bezug auf die Abschnitte im Quellcode reichen die Zeilennummern.

Anomalie-Prüfung A:

Anomalie-Prüfung B:

- c) Beschreiben Sie jeweils einen spezifischen Vorteil von automatisierten Reaktionsmaßnahmen und manuellen Eingriffen bei der Bewältigung von IT-Sicherheitsvorfällen. 4 Punkte

Korrekturrand

Vorteil automatisierte Reaktionsmaßnahmen:

Vorteil manuelle Eingriffe:

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.

☐

