IHK Prüfungen Praxis

IHK Fachinformatiker Prüfung 2024 Praktisch – Lösungen

Prüfungsteil I: Wirtschafts- und Sozialkunde (20 Punkte)

Aufgabe 1.1 Personalmanagement und Arbeitsrecht (10 P)
a) Vor- und Nachteile von Gleitzeitmodellen:
- Vorteile für Arbeitgeber:
  1. Erhöhte Mitarbeiterzufriedenheit und Motivation.
  2. Bessere Anpassung an betriebliche Erfordernisse.
  3. Reduzierung von Überstundenkosten.
- Nachteile für Arbeitgeber:
  1. Schwierigkeit bei der Koordination von Teams.
  2. Erhöhter Verwaltungsaufwand.
  3. Potenzielle Probleme bei der Erreichbarkeit.
- Vorteile für Mitarbeiter:
  1. Bessere Work-Life-Balance.
  2. Flexibilität bei der Arbeitszeitgestaltung.
  3. Reduzierung von Pendelzeiten.
- Nachteile für Mitarbeiter:
  1. Mögliche Isolation von Kollegen.
  2. Schwierigkeit bei der Trennung von Arbeit und Freizeit.
  3. Potenzieller Druck, mehr zu arbeiten.

b) Verfahren zur Anmeldung und Abführung der Sozialversicherungsbeiträge:
1. Anmeldung des Mitarbeiters bei der Krankenkasse.
2. Erhalt der Sozialversicherungsnummer.
3. Berechnung der Beiträge basierend auf dem Bruttogehalt.
4. Monatliche Abführung der Beiträge an die zuständigen Sozialversicherungsträger.

Aufgabe 1.2 Datenschutz und IT-Recht (10 P)
a) Verpflichtungen nach der DSGVO:
1. Durchführung einer Datenschutz-Folgenabschätzung.
2. Abschluss eines Auftragsverarbeitungsvertrags mit dem Cloud-Anbieter.
3. Sicherstellung der Datensicherheit durch technische und organisatorische Maßnahmen.
4. Information der betroffenen Personen über die Datenverarbeitung.

b) Zustimmungs- und Widerrufsprozedere:
1. Information der betroffenen Personen über die Datenverarbeitung.
2. Einholung der ausdrücklichen Zustimmung.
3. Dokumentation der Zustimmung.
4. Möglichkeit zum Widerruf der Zustimmung bereitstellen.
5. Bestätigung des Widerrufs und Einstellung der Datenverarbeitung.

Prüfungsteil II: Fachaufgabe – allgemeiner Teil (30 Punkte)

Aufgabe 2.1 Projektmanagement (15 P)
a) Projektphasen und Arbeitspakete:
1. Initiierung: Projektdefinition, Stakeholder-Analyse.
2. Planung: Ressourcenplanung, Zeitplanung.
3. Analyse: Anforderungsanalyse, Risikoanalyse.
4. Design: Systemdesign, Prototyping.
5. Implementierung: Entwicklung, Testen.

b) Gantt-Chart:
- Wochen 1-4: Analyse
- Wochen 5-8: Design
- Wochen 9-16: Implementierung

c) Netzplandiagramm:
- Projektstart
- Abnahme Design
- Go-Live
- Kritischer Weg: Initiierung -> Planung -> Analyse -> Design -> Implementierung

Aufgabe 2.2 Wirtschaftlichkeitsrechnung (15 P)
a) Amortisationsdauer:
- Gesamtkosten: 30.000 €
- Jährliche Einsparung: 12.000 €
- Amortisationsdauer: 30.000 € / 12.000 € = 2,5 Jahre

b) Gesamtbetriebskosten über fünf Jahre:
- Anschaffungskosten: 30.000 €
- Laufende Kosten: 4.000 € x 5 = 20.000 €
- Gesamt: 50.000 €

c) Return on Investment (ROI) nach einem Jahr:
- ROI = (Einsparung - Kosten) / Kosten
- ROI = (12.000 € - 30.000 €) / 30.000 € = -0,6 oder -60 %

d) Wirtschaftliche Beurteilung:
- Das Projekt lohnt sich langfristig, da die Amortisationsdauer 2,5 Jahre beträgt.
- Kurzfristig ist der ROI negativ, aber die Effizienzsteigerung rechtfertigt die Investition.

Prüfungsteil III: Fachrichtung Systemintegration (50 Punkte)

Aufgabe 3.1 Netzwerkkonzeption und -planung (20 P)
a) Logische Netzwerktopologie:
- Core-Switch verbindet Distribution-Switches.
- Distribution-Switches verbinden Access-Switches auf jeder Etage.

b) IPv4-Adressierungsschema:
- Mitarbeiter: Netzwerk 10.20.0.0, Broadcast 10.20.3.255, erste Host 10.20.0.1
- Gäste: Netzwerk 10.20.4.0, Broadcast 10.20.7.255, erste Host 10.20.4.1
- Management: Netzwerk 10.20.8.0, Broadcast 10.20.11.255, erste Host 10.20.8.1

c) Funktion des Spanning Tree Protocols:
- Verhindert Schleifen im Netzwerk.
- Sorgt für Redundanz und Ausfallsicherheit.

d) QoS-Klassen:
- VoIP: Hohe Priorität, garantierte Bandbreite.
- Daten: Mittlere Priorität, variable Bandbreite.
- Video: Hohe Priorität, reservierte Bandbreite.

Aufgabe 3.2 Sicherheit und Datenschutz im Netz (15 P)
a) VPN-Architektur:
- Site-to-Site VPN mit VPN-Gateways an beiden Standorten.
- Verschlüsselung der Datenübertragung.

b) Firewall-Regeln:
1. Webzugriff: Quelle: intern, Ziel: extern, Protokoll: HTTP/HTTPS, Port: 80/443, Aktion: erlauben
2. Mailzugriff: Quelle: intern, Ziel: extern, Protokoll: SMTP, Port: 25, Aktion: erlauben
3. SSH-Zugriff: Quelle: intern, Ziel: extern, Protokoll: SSH, Port: 22, Aktion: erlauben
4. Webzugriff: Quelle: extern, Ziel: intern, Protokoll: HTTP/HTTPS, Port: 80/443, Aktion: blockieren
5. Mailzugriff: Quelle: extern, Ziel: intern, Protokoll: SMTP, Port: 25, Aktion: blockieren

c) Zwei-Faktor-Authentifizierung:
1. Eingabe von Benutzername und Passwort.
2. Erhalt eines Einmalcodes auf das Mobilgerät.
3. Eingabe des Einmalcodes zur Bestätigung.

Aufgabe 3.3 Fehlersuche, Monitoring und Wartung (15 P)
a) Tools zur Überwachung der Latenz:
1. Ping: Überprüfung der Erreichbarkeit und Latenz.
2. SNMP: Überwachung von Netzwerkgeräten.
3. Traceroute: Analyse des Datenpfads.
4. NetFlow: Analyse des Netzwerkverkehrs.

b) Systemlog-Fehlermeldungen:
1. Fehlermeldung: Netzwerkverbindung unterbrochen. Ursache: Kabelproblem. Maßnahme: Kabel überprüfen und ersetzen.
2. Fehlermeldung: Speicherüberlastung. Ursache: Unzureichender RAM. Maßnahme: RAM aufrüsten.

c) Backup-Strategie:
- Zeitplan: Tägliche inkrementelle Backups, wöchentliche vollständige Backups.
- Aufbewahrung: Monatliche Backups für ein Jahr.
- Medium: Externe Festplatten oder Cloud-Speicher.