

18.1 Prüfungsstrategie: Aufgaben richtig lesen und sicher beantworten

In Prüfungen reicht Fachwissen allein nicht aus.

Wichtig ist auch, Aufgaben richtig zu lesen, Signalwörter zu erkennen und Antworten fachlich passend zu formulieren.

Viele Fehler entstehen nicht, weil das Thema unbekannt ist, sondern weil die Aufgabenstellung falsch verstanden wird.

Merksatz:

Erst verstehen,
dann antworten.

Warum Aufgabenlesen so wichtig ist

Prüfungsaufgaben enthalten oft Hinweise, die direkt zur Lösung führen.

Diese Hinweise stehen zum Beispiel in:

Fehlerbeschreibung
IP-Konfiguration
Netzplan
Tabellen
Protokollausgabe
Logmeldung
Benutzerbeschreibung
Rahmenbedingungen
Einschränkungen
Formulierung der Frage

Merksatz:

Die Lösung steht oft indirekt schon in der Aufgabe.

Typischer Fehler: zu schnell antworten

Ein häufiger Prüfungsfehler ist:

Man erkennt ein bekanntes Stichwort
und antwortet sofort aus dem Gedächtnis.

Problem:

Die Aufgabe fragt vielleicht etwas anderes.

Beispiel:

In der Aufgabe steht DNS,
aber gefragt ist nicht:
Was ist DNS?

Sondern:
Warum funktioniert die Namensauflösung nur im VPN?

Dann geht es wahrscheinlich um:

Split-DNS
DNS-Server
VPN-Konfiguration
interne und externe Namensauflösung

Merksatz:

Nicht auf das erste bekannte Wort springen.

Drei-Schritte-Methode

Bei jeder Prüfungsaufgabe hilft eine einfache Methode:

1. Aufgabenstellung genau lesen.
2. Gegebene Informationen markieren.
3. Antwort direkt auf die Frage formulieren.

Merksatz:

Frage,
Hinweise,
Antwort.

Schritt 1: Aufgabenstellung genau lesen

Wichtige Fragen:

Was wird wirklich gefragt?

Soll ich erklären?

Soll ich berechnen?

Soll ich vergleichen?

Soll ich begründen?

Soll ich eine Maßnahme nennen?

Soll ich einen Fehler finden?

Soll ich eine Konfiguration bewerten?

Merksatz:

Die Operatoren bestimmen,
wie ausführlich die Antwort sein muss.

Operatoren in Prüfungsaufgaben

Operatoren sind Arbeitsaufträge.

Typische Operatoren:

Operator	Bedeutung
----------	-----------

nennen	kurze Stichpunkte oder Begriffe
beschreiben	sachlich darstellen
erklären	Zusammenhang verständlich machen
begründen	warum etwas so ist
vergleichen	Gemeinsamkeiten und Unterschiede
berechnen	rechnerisch ermitteln
ermitteln	aus Angaben ableiten
bewerten	fachlich einschätzen
erläutern	ausführlicher erklären
zuordnen	Begriffe passend einordnen

Merksatz:

Operator beachten,
sonst ist die Antwort schnell zu kurz oder zu lang.

Nennen

Wenn die Aufgabe „nennen“ verlangt, reichen meist kurze Begriffe.

Beispiel:

Nennen Sie zwei Vorteile von VLANs.

Mögliche Antwort:

Trennung von Broadcast-Domänen

bessere Segmentierung

erhöhte Sicherheit durch logische Netztrennung

Merksatz:

Nennen = kurz und direkt.

Beschreiben

Bei „beschreiben“ soll ein Sachverhalt dargestellt werden.

Beispiel:

Beschreiben Sie die Aufgabe eines DHCP-Servers.

Mögliche Antwort:

Ein DHCP-Server weist Clients automatisch Netzwerkkonfigurationen wie IP-Adresse, Subnetzmaske, Standardgateway und DNS-Server zu.

Merksatz:

Beschreiben = was passiert?

Erklären

Bei „erklären“ soll der Zusammenhang klar werden.

Beispiel:

Erklären Sie, warum ein Client ohne Standardgateway keine Internetverbindung hat.

Mögliche Antwort:

Das Standardgateway ist der Router in andere Netze. Ohne Standardgateway kann der Client nur Ziele im eigenen Subnetz erreichen, aber keine externen Netze wie das Internet.

Merksatz:

Erklären = Zusammenhang zeigen.

Begründen

Bei „begründen“ muss ein Warum enthalten sein.

Beispiel:

Begründen Sie,
warum RDP nicht direkt aus dem Internet erreichbar sein sollte.

Mögliche Antwort:

RDP ist ein häufiges Angriffsziel für Brute-Force-Angriffe,
Credential Stuffing
und Exploits.
Deshalb sollte RDP über VPN,
Gateway,
MFA
und Firewall-Beschränkungen abgesichert werden.

Merksatz:

Begründen = Aussage plus Warum.

Vergleichen

Bei „vergleichen“ sollten mindestens zwei Dinge gegenübergestellt werden.

Beispiel:

Vergleichen Sie TCP und UDP.

Mögliche Antwort:

Merkmal	TCP	UDP
Verbindung	verbindungsorientiert	verbindungslos
Zuverlässigkeit	bestätigt und wiederholt Daten	keine eingebaute Zustellgarantie
Overhead	höher	geringer
Beispiele	HTTP, HTTPS, SSH	DNS, DHCP, VoIP

Merksatz:

Vergleichen = Unterschiede und Gemeinsamkeiten sichtbar machen.

Berechnen

Bei „berechnen“ muss ein Ergebnis aus Zahlen abgeleitet werden.

Typische Themen:

Subnetting
Hostanzahl
Netzadresse
Broadcastadresse
Übertragungszeit
Speicherbedarf
Verfügbarkeit
RPO/RTO
Datenrate
Kosten

Merksatz:

Berechnen = Einheit,
Formel
und Ergebnis sauber beachten.

Bewerten

Bei „bewerten“ soll fachlich eingeschätzt werden.

Beispiel:

Bewerten Sie,
ob eine öffentliche SMB-Freigabe im Internet sinnvoll ist.

Mögliche Antwort:

Eine öffentliche SMB-Freigabe ist aus Sicherheitsgründen kritisch,
da SMB ein häufig angegriffenes Protokoll ist und Dateifreigaben sensible Daten enthalten können.
Besser wäre ein Zugriff über VPN,
SFTP
oder eine abgesicherte Plattform mit Authentifizierung,
Protokollierung
und Rechtebegrenzung.

Merksatz:

Bewerten = fachliche Einschätzung mit Begründung.

Aufgabentext markieren

Beim Lesen sollten wichtige Informationen gedanklich markiert werden.

Besonders wichtig:

IP-Adressen
Subnetzmasken
Gateways
DNS-Server
Ports
Protokolle
Fehlermeldungen
betroffene Systeme
Zeitpunkt
letzte Änderung
Benutzerrechte
Sicherheitsanforderungen

Merksatz:

Zahlen,
Fehler
und Einschränkungen sind meistens prüfungsrelevant.

Signalwörter erkennen

Viele Aufgaben enthalten typische Signalwörter.

Signalwort oder Fehlerbild	Wahrscheinliche Richtung
IP erreichbar, Name nicht	DNS
lokales Netz erreichbar, Internet nicht	Gateway, NAT oder Firewall
nur bestimmter Port geht nicht	Firewall, Dienst oder Port
alle Benutzer betroffen	zentraler Dienst oder Netzwerk
nur ein Benutzer betroffen	Konto, Rechte oder Client
nach Update	Änderung, Version oder Kompatibilität
Zertifikatswarnung	Zertifikat, Hostname, Zeit
Zugriff verweigert	Autorisierung, ACL, Gruppe
Anmeldung fehlgeschlagen	Authentifizierung
falsche IP automatisch erhalten	DHCP
IP 169.254.x.x	keine gültige DHCP-Adresse
nur ein VLAN betroffen	VLAN, Routing oder Firewall
Verbindung langsam	Last, Latenz, Paketverlust oder DNS

Merksatz:

Signalwörter zeigen,
wo die Fehlersuche beginnen sollte.

Aufgaben mit Netzplan

Bei Aufgaben mit Netzplan zuerst prüfen:

Welche Netze gibt es?

Welche Subnetze sind eingetragen?

Wo ist das Gateway?

Welche VLANs gibt es?

Wo steht die Firewall?

Wo findet NAT statt?

Welche Dienste stehen in der DMZ?

Welche Verbindung ist erlaubt?

Welche Verbindung ist blockiert?

Merksatz:

Netzplan zuerst verstehen,
dann Fehler suchen.

Aufgaben mit Tabellen

Tabellen enthalten oft konkrete Hinweise.

Zu prüfen:

stimmen IP-Adressen?
passen Subnetzmasken?
ist Gateway im gleichen Netz?
sind DNS-Server plausibel?
sind Ports korrekt?
sind VLANs richtig zugeordnet?
sind Rechte korrekt?
sind Kosten oder Zeiten korrekt?

Merksatz:

Tabellen nicht überfliegen,
sondern systematisch prüfen.

Aufgaben mit Logs

Logs zeigen Ereignisse.

Bei Logaufgaben prüfen:

Zeitpunkt

Quelle

Ziel

Benutzer

Fehlermeldung

Statuscode

Port

Dienst

erfolgreiche oder fehlgeschlagene Aktion

wiederholte Muster

Merksatz:

Logs beantworten oft:

Wer,

wann,

was,

von wo,

mit welchem Ergebnis?

Aufgaben mit HTTP-Statuscodes

HTTP-Statuscodes richtig einordnen:

Statuscode	Bedeutung
200	erfolgreich
301 / 302	Weiterleitung
400	fehlerhafte Anfrage
401	nicht authentifiziert
403	verboten
404	nicht gefunden
500	interner Serverfehler
502	Fehler beim Gateway oder Backend
503	Dienst nicht verfügbar

Merksatz:

4xx deutet eher auf Client,
Anfrage
oder Rechte.
5xx deutet eher auf Server,
Anwendung
oder Backend.

Aufgaben mit IP-Konfiguration

Bei IP-Konfiguration prüfen:

IP-Adresse vorhanden?
Subnetzmaske korrekt?
Gateway im gleichen Netz?
DNS-Server korrekt?
DHCP oder statisch?
doppelte IP möglich?
APIPA-Adresse vorhanden?
IPv4 oder IPv6 relevant?

Merksatz:

IP,
Maske,
Gateway
und DNS gemeinsam prüfen.

APIPA erkennen

APIPA-Adressen liegen im Bereich:

169.254.0.0/16

Sie entstehen, wenn ein Client keine gültige DHCP-Adresse erhält.

Typisches Fehlerbild:

Client hat 169.254.x.x
und erreicht keine normalen Netzdienste.

Merksatz:

169.254.x.x deutet auf DHCP-Problem hin.

Gateway im gleichen Netz prüfen

Das Gateway muss für den Client lokal erreichbar sein.

Beispiel:

Client:
192.168.10.50/24

Gateway:
192.168.20.1

Problem:

Gateway liegt nicht im gleichen Subnetz.

Merksatz:

Standardgateway muss im erreichbaren lokalen Netz liegen.

DNS-Problem sicher erkennen

Typisches Fehlerbild:

ping auf IP-Adresse funktioniert

ping oder Zugriff per Name funktioniert nicht

Wahrscheinliche Ursache:

DNS

Prüfen:

DNS-Server

DNS-Eintrag

DNS-Suffix

Split-DNS

DNS-Cache

Merksatz:

IP ja,

Name nein:

DNS.

Firewall-Problem sicher erkennen

Typisches Fehlerbild:

Zielhost ist erreichbar,
aber bestimmter Dienst nicht.

Mögliche Ursachen:

Firewall blockiert Port

Dienst läuft nicht

Dienst lauscht auf falscher Schnittstelle

NAT oder Portweiterleitung fehlt

Prüfen:

Port

Dienststatus

Firewall-Regel

Logs

Merksatz:

Host ja,
Dienst nein:
Port,
Dienst,
Firewall.

Rechteproblem sicher erkennen

Typisches Fehlerbild:

Anmeldung funktioniert,
Zugriff auf Datei oder Anwendung aber nicht.

Wahrscheinliche Ursache:

Autorisierung oder Berechtigung

Prüfen:

Gruppe
Rolle
ACL
Freigaberecht
Dateisystemrecht
Deny-Regel
Lizenz
Anwendungseinstellung

Merksatz:

Login ja,
Zugriff nein:
Rechte.

Authentifizierungsproblem sicher erkennen

Typisches Fehlerbild:

Benutzer kann sich nicht anmelden.

Mögliche Ursachen:

falsches Passwort
Konto gesperrt
Konto deaktiviert
MFA-Problem
Verzeichnisdienst nicht erreichbar
Uhrzeitproblem
Zertifikatsproblem
abgelaufenes Passwort

Merksatz:

Anmeldung scheitert:
Authentifizierung prüfen.

Zeitproblem erkennen

Falsche Uhrzeit kann viele Fehler verursachen.

Typische Auswirkungen:

Zertifikatsfehler
Kerberos-Fehler
MFA-Probleme
ungültige Tokens
falsche Log-Zuordnung
geplante Aufgaben laufen falsch

Merksatz:

Bei Zertifikat,
Kerberos
und Logs immer auch Zeit prüfen.

Subnetting-Aufgaben richtig angehen

Bei Subnetting immer klären:

Welche Adresse ist gegeben?

Welcher Präfix ist gegeben?

Wie viele Hostbits gibt es?

Wie viele Adressen gibt es?

Wie viele nutzbare Hosts gibt es?

Wie groß ist die Blockgröße?

Wo beginnt das Netz?

Wo endet das Netz?

Merksatz:

Subnetting ist systematische Grenzberechnung.

Subnetting-Reihenfolge

Sinnvolle Reihenfolge:

1. Präfix bestimmen.
2. Hostbits berechnen.
3. Gesamtadressen berechnen.
4. Nutzbare Hosts berechnen.
5. Blockgröße bestimmen.
6. Netzadresse bestimmen.
7. Broadcastadresse bestimmen.
8. erste und letzte nutzbare Adresse bestimmen.

Merksatz:

Immer in derselben Reihenfolge rechnen.

Hostanzahl berechnen

Formel:

$\text{nutzbare Hosts} = 2^{\text{Hostbits}} - 2$

Beispiel:

/26

Hostbits:

$32 - 26 = 6$

Adressen:

$2^6 = 64$

Nutzbare Hosts:

$64 - 2 = 62$

Merksatz:

Hostbits bestimmen die Hostanzahl.

Blockgröße erkennen

Die Blockgröße zeigt, in welchen Schritten Subnetze springen.

Beispiel:

/26 entspricht Maske 255.255.255.192

Blockgröße:

$256 - 192 = 64$

Subnetze im letzten Oktett:

0
64
128
192

Merksatz:

Blockgröße = 256 minus interessanter Maskenwert.

Netzadresse und Broadcast finden

Beispiel:

IP:
192.168.1.70/26

Blockgröße:

64

Subnetze:

192.168.1.0
192.168.1.64
192.168.1.128
192.168.1.192

Die Adresse 70 liegt im Bereich:

192.168.1.64 bis 192.168.1.127

Netzadresse:

192.168.1.64

Broadcast:

192.168.1.127

Nutzbar:

192.168.1.65 bis 192.168.1.126

Merksatz:

IP-Adresse liegt immer in genau einem Subnetzbereich.

Standardports sicher wiederholen

Dienst	Protokoll	Port
SSH	TCP	22
Telnet	TCP	23
SMTP	TCP	25
DNS	UDP/TCP	53
DHCP Server	UDP	67
DHCP Client	UDP	68
HTTP	TCP	80
POP3	TCP	110
IMAP	TCP	143
HTTPS	TCP	443
SMB	TCP	445
SMTPS	TCP	465
IMAPS	TCP	993
POP3S	TCP	995
RDP	TCP	3389

Merksatz:

Ports nicht nur auswendig lernen,
sondern Dienst und Protokoll verstehen.

TCP oder UDP in der Prüfung

Typische Zuordnung:

TCP:
wenn zuverlässige Verbindung wichtig ist

UDP:
wenn geringe Verzögerung oder einfache Anfrage wichtig ist

Beispiele:

HTTP nutzt TCP,
weil Webseiten vollständig übertragen werden sollen.

DNS nutzt häufig UDP,
weil einzelne Anfragen schnell beantwortet werden.

VoIP nutzt häufig UDP,
weil Verzögerung schlimmer ist als einzelner Paketverlust.

Merksatz:

TCP = Zuverlässigkeit.
UDP = wenig Overhead.

Sicherheitsaufgaben richtig beantworten

Bei Sicherheitsfragen immer prüfen:

Welches Schutzziel ist betroffen?

Welche Schwachstelle wird ausgenutzt?

Welche Bedrohung liegt vor?

Welche Maßnahme reduziert das Risiko?

Ist die Maßnahme technisch,
organisatorisch,
personell
oder physisch?

Merksatz:

Sicherheitsantworten mit Schutzziel und Maßnahme begründen.

Schutzziele zuordnen

Schutzziel	Typische Verletzung
Vertraulichkeit	unberechtigtes Lesen
Integrität	unbemerkte Veränderung
Verfügbarkeit	Dienst oder Daten nicht nutzbar
Authentizität	falsche Identität
Nichtabstreitbarkeit	Handlung nicht nachweisbar

Merksatz:

Erst Schutzziel erkennen,
dann Schutzmaßnahme nennen.

Schutzmaßnahmen zuordnen

Risiko	passende Maßnahme
Passwortdiebstahl	MFA, Passwortmanager
Malware	EDR, Patchmanagement, Rechtebegrenzung
Ransomware	Backup, Immutable Backup, Segmentierung
DDoS	DDoS-Schutz, CDN, Rate Limiting

Risiko	passende Maßnahme
Datenabfluss	DLP, Verschlüsselung, Rechtekonzept
unsichere Freigabe	Least Privilege, Ablaufdatum, Audit
veraltete Software	Patchmanagement
Fehlkonfiguration	Change Management, Vier-Augen-Prinzip
unklare Vorfälle	Logging, SIEM, Monitoring

Merksatz:

Maßnahme muss zum Risiko passen.

Antworten nicht zu allgemein formulieren

Zu allgemein:

Man sollte das sicherer machen.

Besser:

Der Zugriff sollte über VPN und MFA abgesichert werden, damit der Administrationsdienst nicht direkt aus dem Internet erreichbar ist und gestohlene Passwörter allein nicht ausreichen.

Merksatz:

Konkrete Maßnahme plus Grund nennen.

Fachbegriffe korrekt verwenden

Häufige Verwechslungen vermeiden:

Nicht verwechseln	Unterschied
Authentifizierung / Autorisierung	Identität prüfen / Rechte prüfen
DNS / DHCP	Namen auflösen / IP-Konfiguration verteilen
NAT / PAT	Adresse übersetzen / Port zur Zuordnung nutzen
IDS / IPS	erkennen / erkennen und blockieren

Nicht verwechseln	Unterschied
SFTP / FTPS	SSH-basiert / FTP mit TLS
Backup / Replikation	Wiederherstellung alter Stände / aktuelle Kopie
Redundanz / Backup	Verfügbarkeit / Wiederherstellung
RPO / RTO	Datenverlust / Wiederherstellungszeit
VLAN / Subnetz	Layer-2-Trennung / Layer-3-Netz
Switch / Router	Frames im LAN / Pakete zwischen Netzen

Merksatz:

Fachbegriffe sauber trennen bringt Punkte.

Prüfungsantwort bei Fehlersuche aufbauen

Gute Struktur:

1. Wahrscheinliche Ursache nennen.
2. Begründung aus Fehlerbild geben.
3. Prüfung oder Maßnahme nennen.

Beispiel:

Wahrscheinlich liegt ein DNS-Problem vor,
da die IP-Adresse erreichbar ist,
der Name aber nicht aufgelöst wird.
Der DNS-Server und der entsprechende DNS-Eintrag sollten mit nslookup oder dig geprüft werden.

Merksatz:

Ursache,
Begründung,
Prüfung.

Prüfungsantwort bei Sicherheitsmaßnahme aufbauen

Gute Struktur:

1. Risiko nennen.
2. Maßnahme nennen.
3. Wirkung erklären.

Beispiel:

Das Risiko besteht im Passwortdiebstahl durch Phishing.
Als Maßnahme sollte MFA eingesetzt werden.
Dadurch reicht ein gestohlenes Passwort allein nicht mehr für den Zugriff aus.

Merksatz:

Risiko,
Maßnahme,
Wirkung.

Prüfungsantwort bei Vergleich aufbauen

Gute Struktur:

1. Gemeinsamkeit nennen.
2. Unterschied nennen.
3. Einsatzbeispiel nennen.

Beispiel:

TCP und UDP sind Transportprotokolle.
TCP ist verbindungsorientiert und zuverlässig,
UDP ist verbindungslos und hat weniger Overhead.
TCP wird zum Beispiel bei HTTPS genutzt,
UDP häufig bei DNS oder VoIP.

Merksatz:

Gemeinsamkeit,
Unterschied,
Beispiel.

Prüfungsantwort bei Berechnung aufbauen

Gute Struktur:

1. gegebene Werte nennen
2. Formel oder Regel anwenden
3. Ergebnis mit Einheit angeben
4. Plausibilität prüfen

Beispiel:

Bei /26 gibt es 6 Hostbits.
2 hoch 6 ergibt 64 Adressen.
Davon sind 62 nutzbar,
da Netzadresse und Broadcastadresse nicht für Hosts verwendet werden.

Merksatz:

Ergebnis immer mit Einheit oder Bedeutung angeben.

Wenn mehrere Antworten möglich sind

Manche Aufgaben erlauben mehrere sinnvolle Lösungen.

Dann wichtig:

Maßnahme fachlich begründen

und

zur Aufgabenstellung passend wählen

Beispiel:

RDP absichern

Mögliche Maßnahmen:

VPN
RDP Gateway
MFA
Quell-IP-Beschränkung
NLA
Account Lockout
Logging

Merksatz:

Mehrere Maßnahmen sind möglich,
aber sie müssen zum Problem passen.

Wenn eine Aufgabe nach „zwei Maßnahmen“ fragt

Dann genau zwei nennen, nicht zehn.

Besser:

1. MFA aktivieren,
damit ein gestohlenes Passwort allein nicht ausreicht.
2. Zugriff per Firewall auf VPN- oder feste Quell-IP-Adressen beschränken,
damit der Dienst nicht breit aus dem Internet erreichbar ist.

Merksatz:

Gefragte Anzahl beachten.

Wenn eine Aufgabe nach Vorteilen und Nachteilen fragt

Antwort sauber trennen.

Beispiel:

Maßnahme	Vorteil	Nachteil
Cloud-Backup	externer Standort, skalierbar	abhängig von Internet und Anbieter
lokales Backup	schneller Restore	Risiko bei Standortausfall

Merksatz:

Vorteile und Nachteile nicht vermischen.

Wenn eine Aufgabe nach Reihenfolge fragt

Reihenfolge ist besonders wichtig bei:

DHCP-Ablauf
TCP-Verbindungsaufbau
Backup-Restore
Incident Response
Fehlersuche
Change Management
Kapselung
OSI-Schichten

Merksatz:

Bei Reihenfolgeaufgaben keine Schritte vertauschen.

Typische Reihenfolgen wiederholen

DHCP:

Discover
Offer
Request
Acknowledge

Incident Response:

erkennen
bewerten
eindämmen
beseitigen
wiederherstellen

verbessern

Change Management:

planen
bewerten
freigeben
umsetzen
testen
dokumentieren

Fehlersuche:

physisch
IP
Gateway
DNS
Routing
Firewall
Dienst
Logs

Merksatz:

Reihenfolgen sind klassische Prüfungspunkte.

Wenn du unsicher bist

Bei Unsicherheit hilft:

Aufgabe nochmals lesen.
Signalwörter suchen.
OSI-Schicht zuordnen.
Schutzziel zuordnen.
Ausschlussverfahren nutzen.
Grundbegriffe sauber verwenden.
Antwort knapp begründen.

Merksatz:

Unsicherheit wird kleiner,
wenn man strukturiert bleibt.

Typische Prüfungsfehler vermeiden

Häufige Fehler:

Frage nicht genau gelesen
Operator ignoriert
zu allgemein geantwortet
falsche Anzahl genannt
Einheiten verwechselt
Bit und Byte verwechselt
IP und DNS verwechselt
Authentifizierung und Autorisierung verwechselt
Backup und Replikation verwechselt
keine Begründung gegeben
Maßnahme passt nicht zum Risiko
Fachwort falsch benutzt

Merksatz:

Viele Punkte gehen durch ungenaue Formulierung verloren.

Checkliste: Aufgabe bearbeiten

Aufgabenstellung vollständig lesen.
Operator markieren.
Zahlen und technische Angaben markieren.
Fehlerbild erkennen.
Betroffene Schicht zuordnen.
Signalwörter beachten.
Gefragte Anzahl beachten.
Antwort direkt zur Frage formulieren.
Fachbegriffe korrekt verwenden.

Kurz begründen.
Ergebnis mit Einheit angeben.
Plausibilität prüfen.

Merksatz:

Jede Antwort muss zur Frage passen.

Checkliste: technische Fehlersuche in Prüfungsaufgaben

Ist das Kabel oder WLAN plausibel?
Hat der Client eine IP-Adresse?
Passt die Subnetzmaske?
Ist das Gateway korrekt?
Funktioniert lokale Kommunikation?
Funktioniert IP-Kommunikation?
Funktioniert DNS?
Ist Routing korrekt?
Blockiert eine Firewall?
Läuft der Dienst?
Lauscht der richtige Port?
Gibt es Rechteprobleme?
Gibt es Loghinweise?
Gab es Änderungen?

Merksatz:

Fehlersuche von unten nach oben denken.

Checkliste: Sicherheitsfrage beantworten

Schutzziel bestimmen.
Schwachstelle erkennen.
Bedrohung benennen.
Risiko beschreiben.
passende Maßnahme nennen.
Wirkung erklären.

technische und organisatorische Maßnahmen unterscheiden.

Least Privilege prüfen.

Logging und Monitoring beachten.

Backup und Restore berücksichtigen.

Merksatz:

Sicherheit immer mit Risiko und Wirkung begründen.

Checkliste: Rechenaufgabe prüfen

Einheit lesen.

Bit oder Byte unterscheiden.

Präfix beachten.

Formel richtig anwenden.

Zwischenschritt prüfen.

Ergebnis mit Einheit angeben.

Plausibilität prüfen.

bei Subnetting Netz und Broadcast beachten.

bei Übertragung Datenmenge und Datenrate passend umrechnen.

Merksatz:

Rechenfehler entstehen oft durch Einheitenfehler.

IHK-sichere Kurzformulierung

Bei Prüfungsaufgaben sollte zuerst die Aufgabenstellung genau gelesen und der Operator erkannt werden. Begriffe wie nennen, erklären, vergleichen, begründen oder berechnen bestimmen die Art der Antwort. Technische Hinweise wie IP-Adressen, Subnetzmasken, Ports, Fehlermeldungen, Logs und Signalwörter müssen sorgfältig ausgewertet werden. Bei Fehlersuche hilft das OSI-Modell, um systematisch von physischer Verbindung über IP, DNS, Routing, Firewall, Dienst und Anwendung zu prüfen. Gute Prüfungsantworten nennen die wahrscheinliche Ursache, begründen sie mit dem Fehlerbild und nennen eine passende Prüfung oder Maßnahme. Bei Sicherheitsfragen sollten Schutzziel, Risiko, Maßnahme und Wirkung klar verbunden werden.

Merksätze

Erst verstehen,
dann antworten.

Operator bestimmt Antwortform.

Nennen heißt kurz.

Erklären heißt Zusammenhang zeigen.

Begründen heißt Warum nennen.

Vergleichen heißt gegenüberstellen.

Berechnen heißt mit Einheit arbeiten.

Signalwörter ernst nehmen.

Netzpläne zuerst verstehen.

Tabellen systematisch prüfen.

Logs beantworten:

wer,

wann,

was,

von wo,

mit welchem Ergebnis.

4xx eher Client oder Rechte.

5xx eher Server oder Backend.

169.254.x.x deutet auf DHCP-Problem.

Gateway muss lokal erreichbar sein.

IP ja,

Name nein:

DNS.

Host ja,

Dienst nein:

Port,

Dienst,

Firewall.

Login ja,

Zugriff nein:

Rechte.

Anmeldung scheitert:

Authentifizierung.

Zertifikatsfehler:

Ablauf,

Name,

Kette,

Zeit.

Subnetting immer gleich lösen.

Hostbits bestimmen Hostanzahl.

Blockgröße hilft bei Netzgrenzen.

Ports sicher wiederholen.

TCP steht für Zuverlässigkeit.

UDP steht für wenig Overhead.

Sicherheitsfragen mit Schutzziel beantworten.

Maßnahme muss zum Risiko passen.

Fachbegriffe sauber trennen.

Gute Fehlerantwort:

Ursache,

Begründung,

Prüfung.

Gute Sicherheitsantwort:

Risiko,

Maßnahme,

Wirkung.

Gefragte Anzahl beachten.

Reihenfolgen nicht vertauschen.

Bei Unsicherheit strukturiert bleiben.

Jede Antwort muss zur Frage passen.
