18. Prüfungsvorbereitung und Wiederholung

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:

nutzbare Hosts = 2 hoch Hostbits minus 2

Beispiel:

/26

Hostbits:

32 - 26 = 6

Adressen:

2 hoch 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.

18.2 Typische Prüfungsaufgaben und Musterantworten

Diese Seite enthält typische Aufgabenformen, wie sie in Prüfungen zur Netzwerktechnik, Administration und IT-Sicherheit vorkommen können.

Ziel ist nicht, Antworten auswendig zu lernen.

Ziel ist, zu erkennen:

- Was fragt die Aufgabe?
- Welche Hinweise stehen im Text?
- Welches Thema ist betroffen?
- Welche Antwort ist fachlich passend?
- Wie formuliere ich kurz und prüfungssicher?

Merksatz:

Gute Prüfungsantworten sind kurz,
fachlich
und direkt auf die Aufgabe bezogen.

Aufgabe 1: DNS-Fehler erkennen

Aufgabe:

Ein Client kann eine Webseite über die IP-Adresse erreichen,
aber nicht über den Domainnamen.
Nennen Sie eine wahrscheinliche Ursache.

Musterantwort:

Wahrscheinlich liegt ein DNS-Problem vor.
Da die IP-Adresse erreichbar ist,
funktioniert die grundsätzliche Netzwerkverbindung.
Der Name wird aber nicht korrekt in eine IP-Adresse aufgelöst.

Prüfung:

```
DNS-Server prüfen.
DNS-Eintrag prüfen.
nslookup oder dig verwenden.
DNS-Cache prüfen.
```

Merksatz:

```
IP funktioniert,
Name nicht:
DNS prüfen.
```

Aufgabe 2: Gateway-Fehler erkennen

Aufgabe:

```
Ein Client erreicht andere Geräte im gleichen Subnetz,
aber keine Systeme im Internet.
Welche Einstellung ist wahrscheinlich falsch oder fehlt?
```

Musterantwort:

```
Wahrscheinlich fehlt das Standardgateway
oder es ist falsch konfiguriert.
Das Gateway wird benötigt,
um Ziele außerhalb des eigenen Subnetzes zu erreichen.
```

Prüfung:

```
IP-Konfiguration prüfen.
Gateway-Adresse prüfen.
Routing-Tabelle prüfen.
Gateway anpingen.
```

Merksatz:

Lokal erreichbar,
extern nicht:
Gateway prüfen.

Aufgabe 3: DHCP-Problem erkennen

Aufgabe:

Ein Windows-Client hat die IP-Adresse 169.254.23.18.
Was bedeutet das?

Musterantwort:

Die Adresse liegt im APIPA-Bereich 169.254.0.0/16.
Der Client hat wahrscheinlich keine gültige Adresse von einem DHCP-Server erhalten.

Prüfung:

DHCP-Server prüfen.
Netzwerkverbindung prüfen.
VLAN prüfen.
DHCP-Scope prüfen.
DHCP-Relay prüfen.

Merksatz:

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

Aufgabe 4: Subnetz prüfen

Aufgabe:

Ein Client hat die Adresse 192.168.10.50/24.
Als Gateway ist 192.168.20.1 eingetragen.
Warum funktioniert der Zugriff in andere Netze nicht?

Musterantwort:

Das Gateway liegt nicht im gleichen Subnetz wie der Client.
Bei /24 gehört der Client zum Netz 192.168.10.0/24.
Das Gateway 192.168.20.1 liegt im Netz 192.168.20.0/24
und ist daher lokal nicht erreichbar.

Merksatz:

Das Standardgateway muss im lokalen Subnetz erreichbar sein.

Aufgabe 5: Netzadresse berechnen

Aufgabe:

Ermitteln Sie die Netzadresse zu 192.168.1.70/26.

Lösung:

/26 bedeutet:
64 Adressen pro Subnetz.

Subnetzbereiche:

192.168.1.0 bis 192.168.1.63
192.168.1.64 bis 192.168.1.127
192.168.1.128 bis 192.168.1.191
192.168.1.192 bis 192.168.1.255

Die Adresse 192.168.1.70 liegt im Bereich:

192.168.1.64 bis 192.168.1.127

Netzadresse:

192.168.1.64

Broadcastadresse:

```
192.168.1.127
```

Nutzbare Hosts:

```
192.168.1.65 bis 192.168.1.126
```

Merksatz:

```
Erst Blockgröße bestimmen,
dann Bereich finden.
```

Aufgabe 6: Hostanzahl berechnen

Aufgabe:

```
Wie viele nutzbare Hosts sind in einem /27-Netz möglich?
```

Lösung:

```
IPv4 hat 32 Bit.
/27 bedeutet 27 Netzbits.
```

Hostbits:

```
32 - 27 = 5
```

Adressen:

```
2 hoch 5 = 32
```

Nutzbare Hosts:

```
32 - 2 = 30
```

Antwort:

30 nutzbare Hosts

Merksatz:

Nutzbare Hosts = 2 hoch Hostbits minus 2.

Aufgabe 7: TCP und UDP vergleichen

Aufgabe:

Vergleichen Sie TCP und UDP.

Musterantwort:

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

Kurzform:

TCP ist verbindungsorientiert und zuverlässig.
UDP ist verbindungslos,
schneller
und hat weniger Overhead.

Merksatz:

TCP = zuverlässig.
UDP = schlank.

Aufgabe 8: Port einem Dienst zuordnen

Aufgabe:

Ordnen Sie den Port TCP 443 einem Dienst zu.

Antwort:

TCP 443 gehört zu HTTPS.

Erklärung:

HTTPS ist HTTP über TLS
und wird für verschlüsselte Webkommunikation genutzt.

Merksatz:

HTTPS nutzt TCP 443.

Aufgabe 9: SSH-Port nennen

Aufgabe:

Welchen Standardport nutzt SSH?

Antwort:

SSH nutzt standardmäßig TCP 22.

Zusatz:

SSH dient dem verschlüsselten Fernzugriff auf die Kommandozeile
und kann auch für SFTP oder SCP genutzt werden.

Merksatz:

SSH = TCP 22.

Aufgabe 10: RDP absichern

Aufgabe:

Ein Unternehmen betreibt RDP direkt erreichbar aus dem Internet.
Nennen Sie zwei Sicherheitsmaßnahmen.

Musterantwort:

1. RDP nur über VPN oder RDP-Gateway erreichbar machen,
   damit der Dienst nicht direkt aus dem Internet angreifbar ist.

2. MFA aktivieren,
   damit ein gestohlenes Passwort allein nicht für den Zugriff ausreicht.

Weitere mögliche Maßnahmen:

Quell-IP einschränken
Network Level Authentication aktivieren
Account Lockout einrichten
starke Passwörter erzwingen
Logs überwachen
Systeme patchen

Merksatz:

RDP nicht direkt und breit ins Internet öffnen.

Aufgabe 11: VLAN erklären

Aufgabe:

Erklären Sie den Zweck von VLANs.

Musterantwort:

VLANs teilen ein physisches Netzwerk logisch in mehrere getrennte Netzbereiche auf.
Dadurch können zum Beispiel Abteilungen,
Gäste,

Server
oder Managementschnittstellen voneinander getrennt werden.
VLANs reduzieren Broadcastbereiche
und verbessern Struktur und Sicherheit.

Merksatz:

VLAN trennt logisch auf Schicht 2.

Aufgabe 12: Access-Port und Trunk-Port unterscheiden

Aufgabe:

Unterscheiden Sie Access-Port und Trunk-Port.

Musterantwort:

Porttyp	Bedeutung
Access-Port	gehört normalerweise zu genau einem VLAN und wird meist für Endgeräte genutzt
Trunk-Port	transportiert mehrere VLANs und wird meist zwischen Switches, Routern oder Firewalls genutzt

Merksatz:

Access = ein VLAN.
Trunk = mehrere VLANs.

Aufgabe 13: ARP erklären

Aufgabe:

Wofür wird ARP verwendet?

Musterantwort:

ARP löst im lokalen IPv4-Netz eine IP-Adresse in eine MAC-Adresse auf.
Ein Host nutzt ARP,

um die MAC-Adresse des Zielsystems oder des Gateways zu ermitteln.

Merksatz:

ARP verbindet IPv4-Adresse und MAC-Adresse im lokalen Netz.

Aufgabe 14: MAC, IP und Port zuordnen

Aufgabe:

Ordnen Sie MAC-Adresse,
IP-Adresse
und Port den passenden OSI-Schichten zu.

Antwort:

Begriff	OSI-Schicht	Aufgabe
MAC-Adresse	Schicht 2	lokale Zustellung im LAN
IP-Adresse	Schicht 3	logische Adressierung und Routing
Port	Schicht 4	Zuordnung zu Dienst oder Anwendung

Merksatz:

MAC lokal,
IP logisch,
Port Dienst.

Aufgabe 15: NAT und PAT unterscheiden

Aufgabe:

Unterscheiden Sie NAT und PAT.

Musterantwort:

NAT übersetzt IP-Adressen.
PAT ist eine spezielle Form von NAT,

bei der zusätzlich Ports verwendet werden,
damit mehrere interne Geräte über eine öffentliche IP-Adresse kommunizieren können.

Merksatz:

NAT übersetzt Adressen.
PAT nutzt zusätzlich Ports.

Aufgabe 16: Portweiterleitung erklären

Aufgabe:

Was ist eine Portweiterleitung?

Musterantwort:

Eine Portweiterleitung leitet eingehenden Verkehr auf einem bestimmten Port
von einer öffentlichen Adresse
an einen internen Dienst weiter.
Dadurch kann ein interner Server von außen erreichbar gemacht werden.

Beispiel:

extern TCP 443
wird weitergeleitet
auf internen Webserver TCP 443

Merksatz:

Portweiterleitung macht interne Dienste von außen erreichbar.

Aufgabe 17: Firewall-Regel bewerten

Aufgabe:

Eine Firewall-Regel erlaubt Any to Any.
Bewerten Sie diese Regel.

Musterantwort:

> Die Regel ist sicherheitskritisch,
> weil sie Verkehr von jeder Quelle zu jedem Ziel erlaubt.
> Dadurch wird die Angriffsfläche stark vergrößert.
> Besser ist eine möglichst genaue Regel mit definierter Quelle,
> definiertem Ziel,
> benötigtem Port,
> Protokoll
> und dokumentiertem Zweck.

Merksatz:

> Firewall-Regeln so eng wie möglich formulieren.

Aufgabe 18: DMZ erklären

Aufgabe:

> Was ist eine DMZ?

Musterantwort:

> Eine DMZ ist ein getrenntes Netzwerksegment für öffentlich erreichbare Dienste,
> zum Beispiel Webserver,
> Reverse Proxy
> oder Mail-Gateway.
> Sie trennt diese Systeme vom internen Netz,
> damit ein kompromittierter öffentlicher Dienst nicht direkt Zugriff auf interne Systeme erhält.

Merksatz:

> DMZ trennt öffentliche Dienste vom internen Netz.

Aufgabe 19: VPN-Arten unterscheiden

Aufgabe:

Unterscheiden Sie Remote-Access-VPN und Site-to-Site-VPN.

Musterantwort:

VPN-Art	Bedeutung
Remote-Access-VPN	einzelner Benutzer verbindet sich aus der Ferne mit einem Netzwerk
Site-to-Site-VPN	zwei Netzwerke oder Standorte werden miteinander verbunden

Merksatz:

Remote-Access verbindet Benutzer.

Site-to-Site verbindet Standorte.

Aufgabe 20: IaaS, PaaS und SaaS unterscheiden

Aufgabe:

Unterscheiden Sie IaaS,

PaaS

und SaaS.

Musterantwort:

Modell	Bedeutung	Beispiel
IaaS	virtuelle Infrastruktur	virtuelle Maschine
PaaS	Plattform für Anwendungen	verwaltete Datenbank oder App-Plattform
SaaS	fertige Anwendung	E-Mail-Dienst oder CRM im Browser

Merksatz:

IaaS = Infrastruktur.

PaaS = Plattform.

SaaS = Software.

Aufgabe 21: Shared Responsibility erklären

Aufgabe:

Erklären Sie das Shared-Responsibility-Modell in der Cloud.

Musterantwort:

Beim Shared-Responsibility-Modell teilen sich Cloud-Anbieter und Kunde die Verantwortung.
Der Anbieter schützt die Cloud-Infrastruktur.
Der Kunde bleibt verantwortlich für seine Daten,
Identitäten,
Zugriffsrechte,
Konfigurationen
und Nutzung der Dienste.

Merksatz:

Cloud bedeutet nicht,
dass der Anbieter alles absichert.

Aufgabe 22: Schutzziel zuordnen

Aufgabe:

Ein Angreifer verändert unbemerkt eine Konfigurationsdatei.
Welches Schutzziel ist betroffen?

Antwort:

Integrität

Begründung:

Integrität bedeutet,
dass Daten nicht unbemerkt verändert werden dürfen.

Merksatz:

Unbemerkte Veränderung betrifft Integrität.

Aufgabe 23: Ransomware-Schutzziel zuordnen

Aufgabe:

Ransomware verschlüsselt Firmendaten.
Welches Schutzziel ist hauptsächlich betroffen?

Antwort:

Verfügbarkeit

Begründung:

Die Daten sind nicht mehr nutzbar.
Wenn zusätzlich Daten gestohlen und veröffentlicht werden,
ist auch Vertraulichkeit betroffen.

Merksatz:

Ransomware betrifft Verfügbarkeit,
bei Datenabfluss auch Vertraulichkeit.

Aufgabe 24: Phishing-Maßnahmen nennen

Aufgabe:

Nennen Sie zwei Maßnahmen gegen Phishing.

Musterantwort:

1. MFA einsetzen,
   damit gestohlene Passwörter allein nicht ausreichen.

2. Benutzer schulen,

damit verdächtige E-Mails,
Links
und Anhänge besser erkannt werden.

Weitere mögliche Maßnahmen:

E-Mail-Filter
SPF,
DKIM
und DMARC
Passwortmanager
Meldeprozess
sichere Browserkonfiguration

Merksatz:

Gegen Phishing helfen Technik und Schulung zusammen.

Aufgabe 25: IDS und IPS unterscheiden

Aufgabe:

Was ist der Unterschied zwischen IDS und IPS?

Musterantwort:

Ein IDS erkennt verdächtige Aktivitäten und meldet sie.
Ein IPS erkennt verdächtige Aktivitäten ebenfalls,
kann sie aber zusätzlich aktiv blockieren.

Merksatz:

IDS meldet.
IPS blockiert zusätzlich.

Aufgabe 26: SIEM erklären

Aufgabe:

> Was ist die Aufgabe eines SIEM?

Musterantwort:

> Ein SIEM sammelt,
> speichert
> und korreliert Sicherheitslogs aus verschiedenen Systemen.
> Dadurch können sicherheitsrelevante Zusammenhänge erkannt
> und Alarme erzeugt werden.

Merksatz:

> SIEM sammelt und verbindet Sicherheitsereignisse.

Aufgabe 27: Authentifizierung und Autorisierung unterscheiden

Aufgabe:

> Unterscheiden Sie Authentifizierung und Autorisierung.

Musterantwort:

Begriff	Frage	Beispiel
Authentifizierung	Wer bist du?	Benutzer meldet sich mit Passwort und MFA an
Autorisierung	Was darfst du?	Benutzer darf eine Datei lesen

Merksatz:

> Authentifizierung prüft Identität.
> Autorisierung prüft Rechte.

Aufgabe 28: Least Privilege erklären

Aufgabe:

Erklären Sie das Prinzip Least Privilege.

Musterantwort:

Least Privilege bedeutet,
dass Benutzer,
Dienste
und Prozesse nur die Rechte erhalten,
die sie für ihre Aufgabe wirklich benötigen.
Dadurch wird der mögliche Schaden bei Fehlern oder Angriffen begrenzt.

Merksatz:

So wenig Rechte wie möglich,
so viele wie nötig.

Aufgabe 29: Dienstkonto erklären

Aufgabe:

Was ist ein Dienstkonto?

Musterantwort:

Ein Dienstkonto ist eine technische Identität,
die von einem Dienst,
einer Anwendung
oder einem automatisierten Prozess genutzt wird.
Es sollte nur die Rechte besitzen,
die für den jeweiligen Zweck erforderlich sind.

Merksatz:

Dienstkonten sind technische Identitäten und müssen rechtearm sein.

Aufgabe 30: Offboarding begründen

Aufgabe:

Warum ist Offboarding sicherheitsrelevant?

Musterantwort:

Beim Offboarding werden nicht mehr benötigte Zugänge entfernt.
Wenn alte Benutzerkonten,
VPN-Zugänge,
SSH-Schlüssel
oder Cloud-Rollen aktiv bleiben,
können sie später missbraucht werden.

Merksatz:

Alte Zugänge sind Sicherheitsrisiken.

Aufgabe 31: Logs und Monitoring unterscheiden

Aufgabe:

Unterscheiden Sie Logging und Monitoring.

Musterantwort:

Begriff	Bedeutung
Logging	Ereignisse werden protokolliert
Monitoring	Zustände und Metriken werden überwacht

Beispiel:

Log:
Benutzeranmeldung fehlgeschlagen.

Monitoring:
CPU-Auslastung dauerhaft über 90 Prozent.

Merksatz:

Logs zeigen Ereignisse.
Monitoring zeigt Zustände.

Aufgabe 32: NTP bei Logs erklären

Aufgabe:

Warum ist NTP für die Logauswertung wichtig?

Musterantwort:

NTP synchronisiert die Systemzeit.
Bei der Analyse von Logs müssen Ereignisse verschiedener Systeme zeitlich korrekt zugeordnet werden können.
Ohne gemeinsame Zeitbasis wird die Fehlersuche und Sicherheitsanalyse erschwert.

Merksatz:

Gleiche Zeitbasis macht Logs vergleichbar.

Aufgabe 33: HTTP-Statuscode einordnen

Aufgabe:

Ein Webserver liefert den Statuscode 403.
Was bedeutet das?

Antwort:

403 bedeutet verboten.
Der Client ist zwar grundsätzlich am Server,
darf aber auf die angeforderte Ressource nicht zugreifen.

Merksatz:

403 = verboten.

Aufgabe 34: HTTP 500 einordnen

Aufgabe:

```
Eine Webanwendung liefert HTTP 500.
Wo liegt das Problem wahrscheinlich?
```

Musterantwort:

```
HTTP 500 weist auf einen internen Serverfehler hin.
Die Ursache liegt wahrscheinlich in der Anwendung,
im Backend,
in einer Abhängigkeit
oder in der Serverkonfiguration.
```

Merksatz:

```
5xx deutet eher auf Server oder Backend.
```

Aufgabe 35: SMB erklären

Aufgabe:

```
Wofür wird SMB verwendet und welchen Standardport nutzt es?
```

Musterantwort:

```
SMB wird für Datei- und Druckerfreigaben genutzt,
besonders in Windows-Netzwerken.
Der Standardport ist TCP 445.
```

Merksatz:

```
SMB = Dateifreigaben,
TCP 445.
```

Aufgabe 36: FTP und SFTP unterscheiden

Aufgabe:

Warum ist FTP unsicher und was ist der Vorteil von SFTP?

Musterantwort:

Klassisches FTP überträgt Daten und Zugangsdaten unverschlüsselt.
SFTP nutzt SSH und überträgt Dateien verschlüsselt.
Dadurch sind Zugangsdaten und Dateiinhalt besser geschützt.

Merksatz:

FTP unverschlüsselt.
SFTP über SSH verschlüsselt.

Aufgabe 37: SFTP und FTPS unterscheiden

Aufgabe:

Unterscheiden Sie SFTP und FTPS.

Musterantwort:

SFTP ist Dateiübertragung über SSH.
FTPS ist FTP mit TLS-Verschlüsselung.
Beide übertragen verschlüsselt,
basieren aber auf unterschiedlichen Protokollen.

Merksatz:

SFTP ist nicht FTPS.

Aufgabe 38: Synchronisation und Backup unterscheiden

Aufgabe:

Warum ist Synchronisation kein Backup?

Musterantwort:

Synchronisation hält Daten an mehreren Orten gleich.
Wenn eine Datei gelöscht,
beschädigt
oder durch Ransomware verschlüsselt wird,
kann diese Änderung mitsynchronisiert werden.
Ein Backup speichert dagegen wiederherstellbare ältere Stände.

Merksatz:

Sync hält gleich.
Backup stellt wieder her.

Aufgabe 39: RPO und RTO unterscheiden

Aufgabe:

Unterscheiden Sie RPO und RTO.

Musterantwort:

Begriff	Bedeutung
RPO	maximal akzeptabler Datenverlust
RTO	maximal akzeptable Wiederherstellungszeit

Beispiel:

RPO 1 Stunde:
maximal Datenverlust von 1 Stunde.

RTO 4 Stunden:
System soll spätestens nach 4 Stunden wieder laufen.

Merksatz:

RPO = Datenverlust.
RTO = Zeit bis Wiederherstellung.

Aufgabe 40: Restore-Test begründen

Aufgabe:

Warum sind Restore-Tests wichtig?

Musterantwort:

Restore-Tests prüfen,
ob Backups tatsächlich wiederhergestellt werden können.
Ohne Restore-Test ist unklar,
ob Daten vollständig,
lesbar,
konsistent
und rechtzeitig wiederherstellbar sind.

Merksatz:

Backup ohne Restore-Test ist unsicher.

Aufgabe 41: Snapshot bewerten

Aufgabe:

Warum ersetzt ein Snapshot kein Backup?

Musterantwort:

Ein Snapshot liegt oft auf demselben System oder Speicher wie die Produktivdaten.
Bei Speicherdefekt,
Ransomware,
versehentlicher Löschung
oder Standortausfall kann auch der Snapshot betroffen sein.

Ein Backup sollte getrennt,
geschützt
und wiederherstellbar sein.

Merksatz:

Snapshot ist Momentaufnahme,
aber kein vollständiges Backup-Konzept.

Aufgabe 42: 3-2-1-Regel erklären

Aufgabe:

Erklären Sie die 3-2-1-Regel.

Musterantwort:

Die 3-2-1-Regel bedeutet:
Es gibt drei Kopien der Daten,
auf zwei unterschiedlichen Speicherarten,
davon eine Kopie extern oder getrennt vom Hauptsystem.

Merksatz:

3 Kopien,
2 Medien,
1 externe Kopie.

Aufgabe 43: Dokumentation begründen

Aufgabe:

Warum ist IT-Dokumentation wichtig?

Musterantwort:

IT-Dokumentation macht Systeme,
IP-Adressen,
Dienste,
Rechte,
Firewall-Regeln,
Backups
und Abhängigkeiten nachvollziehbar.
Sie hilft bei Fehlersuche,
Vertretung,
Notfällen,
Audits
und sicheren Änderungen.

Merksatz:

Dokumentation macht Betrieb nachvollziehbar.

Aufgabe 44: Change Management erklären

Aufgabe:

Was ist Change Management?

Musterantwort:

Change Management ist ein kontrollierter Prozess für Änderungen an IT-Systemen.
Änderungen werden geplant,
bewertet,
freigegeben,
umgesetzt,
getestet
und dokumentiert.

Merksatz:

Change Management verhindert unkontrollierte Änderungen.

Aufgabe 45: Rollback-Plan erklären

Aufgabe:

```
Warum ist ein Rollback-Plan wichtig?
```

Musterantwort:

```
Ein Rollback-Plan beschreibt,
wie eine Änderung rückgängig gemacht werden kann,
falls sie fehlschlägt.
Dadurch können Ausfallzeiten und Folgeschäden reduziert werden.
```

Merksatz:

```
Vor Änderung wissen,
wie man zurückkommt.
```

Aufgabe 46: Emergency Change bewerten

Aufgabe:

```
Muss ein Emergency Change dokumentiert werden?
```

Antwort:

```
Ja.
Ein Emergency Change ist zwar dringend,
muss aber spätestens nachträglich dokumentiert werden.
Sonst sind Ursache,
Wirkung,
Risiko
und geänderte Konfiguration später nicht nachvollziehbar.
```

Merksatz:

```
Dringend heißt nicht dokumentationsfrei.
```

Aufgabe 47: Runbook erklären

Aufgabe:

```
Was ist ein Runbook?
```

Musterantwort:

```
Ein Runbook ist eine Schritt-für-Schritt-Anleitung für wiederkehrende Aufgaben oder Störungen.
Es beschreibt,
wie eine bestimmte administrative Aufgabe oder Fehlerbehebung durchgeführt wird.
```

Merksatz:

```
Runbook = konkrete Schritt-für-Schritt-Anleitung.
```

Aufgabe 48: CMDB erklären

Aufgabe:

```
Was ist eine CMDB?
```

Musterantwort:

```
Eine CMDB ist eine Configuration Management Database.
Sie enthält Informationen über verwaltete IT-Elemente,
sogenannte Configuration Items,
und deren Beziehungen.
```

Beispiele:

```
Server
Anwendungen
Datenbanken
Firewalls
Zertifikate
Lizenzen
```

Merksatz:

CMDB zeigt IT-Elemente und ihre Beziehungen.

Aufgabe 49: Fehlersuche strukturieren

Aufgabe:

Ein Benutzer meldet,
dass er eine interne Anwendung nicht erreichen kann.
Nennen Sie eine sinnvolle Prüfungsreihenfolge.

Musterantwort:

1. Prüfen,
   ob nur ein Benutzer oder mehrere betroffen sind.

2. IP-Konfiguration des Clients prüfen.

3. DNS-Auflösung prüfen.

4. Erreichbarkeit des Servers per IP prüfen.

5. Port und Dienst prüfen.

6. Firewall-Regeln prüfen.

7. Logs der Anwendung und des Servers prüfen.

8. Letzte Änderungen prüfen.

Merksatz:

Fehlersuche systematisch eingrenzen.

Aufgabe 50: Sicherheitsmaßnahme passend auswählen

Aufgabe:

Ein Unternehmen möchte verhindern,
dass ein gestohlenes Passwort allein für den Zugriff auf Cloud-Dienste reicht.
Welche Maßnahme ist passend?

Antwort:

Multi-Faktor-Authentifizierung

Begründung:

MFA fordert zusätzlich zum Passwort einen weiteren Faktor,
zum Beispiel einen Token,
eine App-Bestätigung
oder eine Smartcard.
Dadurch reicht ein gestohlenes Passwort allein nicht aus.

Merksatz:

Gestohlenes Passwort allein verhindern:
MFA.

Musterformulierung für Fehlerdiagnose

Gute Antwortform:

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

Struktur:

Ursache
plus
Begründung
plus
Prüfung

Merksatz:

```
Ursache,
Begründung,
Prüfung.
```

Musterformulierung für Sicherheitsmaßnahmen

Gute Antwortform:

```
Das Risiko besteht im unberechtigten Zugriff durch gestohlene Zugangsdaten.
Als Maßnahme sollte MFA aktiviert werden.
Dadurch reicht ein Passwort allein nicht mehr aus,
um Zugriff zu erhalten.
```

Struktur:

```
Risiko
plus
Maßnahme
plus
Wirkung
```

Merksatz:

```
Risiko,
Maßnahme,
Wirkung.
```

Musterformulierung für Vergleiche

Gute Antwortform:

```
TCP und UDP sind Transportprotokolle.
TCP ist verbindungsorientiert und zuverlässig,
UDP ist verbindungslos und hat weniger Overhead.
TCP eignet sich für vollständige Datenübertragung,
```

UDP für zeitkritische Anwendungen wie VoIP.

Struktur:

Gemeinsamkeit
plus
Unterschied
plus
Beispiel

Merksatz:

Gemeinsamkeit,
Unterschied,
Beispiel.

Musterformulierung für Bewertungen

Gute Antwortform:

Die Lösung ist kritisch,
weil der Administrationsdienst direkt aus dem Internet erreichbar ist.
Dadurch steigt das Risiko für Brute-Force-Angriffe und Exploits.
Sicherer wäre ein Zugriff über VPN oder Bastion Host mit MFA und Protokollierung.

Struktur:

Einschätzung
plus
Risiko
plus
bessere Maßnahme

Merksatz:

Bewertung braucht fachliche Begründung.

Typische Prüfungsfallen auf dieser Seite

Antwort nicht auf die Frage bezogen.

Operator übersehen.

Nur Begriff genannt,
obwohl Erklärung verlangt war.

Keine Begründung gegeben.

Maßnahme genannt,
aber Wirkung nicht erklärt.

DNS und DHCP verwechselt.

Authentifizierung und Autorisierung verwechselt.

NAT und PAT verwechselt.

SFTP und FTPS verwechselt.

RPO und RTO verwechselt.

Backup und Synchronisation verwechselt.

VLAN und Subnetz gleichgesetzt.

Firewallproblem behauptet,
ohne Port oder Dienst zu prüfen.

Ping als vollständigen Diensttest verstanden.

Snapshot als vollständiges Backup bezeichnet.

Merksatz:

Viele Fehler entstehen durch ungenaue Begriffe.

Checkliste: Musterantwort prüfen

Vor Abgabe prüfen:

```
Habe ich die Frage beantwortet?

Habe ich die geforderte Anzahl genannt?

Habe ich den Operator beachtet?

Habe ich Fachbegriffe korrekt verwendet?

Habe ich kurz begründet?

Habe ich bei Berechnungen eine Einheit angegeben?

Habe ich bei Fehlersuche Ursache und Prüfung genannt?

Habe ich bei Sicherheit Risiko und Maßnahme verbunden?
```

Merksatz:

```
Eine kurze richtige Antwort ist besser als eine lange ungenaue Antwort.
```

IHK-sichere Kurzformulierung

Typische Prüfungsaufgaben prüfen nicht nur Definitionen, sondern die Anwendung von Wissen auf Fehlerbilder, Sicherheitsrisiken und technische Szenarien. Gute Antworten nennen die wahrscheinliche Ursache, begründen sie mit den Angaben aus der Aufgabe und nennen eine passende Prüfung oder Maßnahme. Bei Sicherheitsfragen sollten Risiko, Schutzmaßnahme und Wirkung verbunden werden. Bei Vergleichen sollten Unterschiede klar gegenübergestellt werden. Bei Berechnungen müssen Einheit, Präfix, Formel und Ergebnis stimmen. Fachbegriffe wie DNS, DHCP, Authentifizierung, Autorisierung, NAT, PAT, SFTP, FTPS, Backup, Replikation, RPO und RTO müssen sauber unterschieden werden.

Merksätze

```
Musterantworten zeigen Struktur,
nicht Auswendiglernen.
```

Gute Antworten sind kurz und fachlich.

Ursache aus Fehlerbild ableiten.

Maßnahme passend zum Risiko wählen.

IP geht,
Name nicht:
DNS.

Lokal geht,
extern nicht:
Gateway.

169.254.x.x:
DHCP-Problem.

Host erreichbar,
Dienst nicht:
Port,
Dienst,
Firewall.

Login geht,
Zugriff nicht:
Rechte.

SSH nutzt TCP 22.

RDP nutzt TCP 3389.

SMB nutzt TCP 445.

HTTPS nutzt TCP 443.

VLAN trennt logisch.

Routing verbindet Netze.

NAT übersetzt Adressen.

PAT nutzt Ports.

IDS meldet.

IPS blockiert zusätzlich.

MFA schützt gegen Passwortmissbrauch.

SIEM sammelt und korreliert Logs.

Backup ohne Restore-Test ist unsicher.

Sync ist kein Backup.

Replikation ist kein Backup.

RPO ist Datenverlust.

RTO ist Wiederherstellungszeit.

Dokumentation macht Betrieb nachvollziehbar.

Change Management kontrolliert Änderungen.

Rollback vor Änderung planen.

Dringend heißt nicht dokumentationsfrei.

Fachbegriffe sauber verwenden.

Antwort immer zur Aufgabe passend formulieren.

18.3 Prüfungschecklisten nach Themen

Diese Seite dient als kompakte Wiederholung, um kurz vor der Prüfung die wichtigsten Themen systematisch zu prüfen.

Sie ist nach Themenbereichen aufgebaut.

Ziel ist:

- Lücken erkennen
- Begriffe sauber unterscheiden
- typische Fehler vermeiden
- prüfungssichere Kurzantworten vorbereiten
- Zusammenhänge wiederholen

Merksatz:

Eine Checkliste hilft,
Wissen geordnet zu wiederholen.

Checkliste: OSI-Modell

Das solltest du sicher können:

OSI-Schichten 1 bis 7 benennen.
Aufgabe jeder Schicht erklären.
typische Protokolle und Geräte zuordnen.
Fehlerbilder passenden Schichten zuordnen.
Kapselung erklären.
PDUs zuordnen.

Schicht	Name	Typische Begriffe
7	Anwendung	HTTP, DNS, DHCP, SMTP
6	Darstellung	TLS, Verschlüsselung, Codierung
5	Sitzung	Session, Sitzungsaufbau
4	Transport	TCP, UDP, Ports
3	Vermittlung	IP, Routing, ICMP

Schicht	Name	Typische Begriffe
2	Sicherung	MAC, Ethernet, Switch, VLAN, ARP
1	Bitübertragung	Kabel, Signal, Stecker, Funk

Merksatz:

OSI ist ein Denkmodell für Kommunikation und Fehlersuche.

Checkliste: TCP/IP-Modell

Das solltest du sicher können:

TCP/IP-Schichten benennen.
TCP/IP-Schichten grob OSI zuordnen.
Protokolle passend einordnen.
Unterschied zwischen OSI und TCP/IP erklären.

TCP/IP-Schicht	Entspricht grob OSI	Beispiele
Anwendung	5 bis 7	HTTP, DNS, DHCP, SMTP
Transport	4	TCP, UDP
Internet	3	IP, ICMP
Netzzugang	1 bis 2	Ethernet, WLAN, MAC

Merksatz:

TCP/IP ist praxisnäher,
OSI ist feiner aufgeteilt.

Checkliste: Kapselung

Das solltest du sicher können:

Daten werden beim Senden schrittweise verpackt.
Jede Schicht ergänzt eigene Steuerinformationen.
Beim Empfangen wird entkapselt.
MAC,

IP
und Port gehören zu unterschiedlichen Schichten.

Reihenfolge beim Senden:

Anwendungsdaten
Segment oder Datagramm
Paket
Frame
Bits

Merksatz:

Kapselung bedeutet:
jede Schicht ergänzt ihren eigenen Header.

Checkliste: MAC, IP und Port

Begriff	Schicht	Aufgabe
MAC-Adresse	2	lokale Zustellung im LAN
IP-Adresse	3	logische Adressierung und Routing
Port	4	Zuordnung zu Dienst oder Anwendung

Typische Prüfungsfalle:

MAC-Adresse wird nicht über Router hinweg weiterverwendet.
IP-Adresse bleibt für Routing relevant.
Port zeigt den Dienst auf dem Zielhost.

Merksatz:

MAC lokal,
IP über Netze,
Port zum Dienst.

Checkliste: IPv4

Das solltest du sicher können:

IPv4 besteht aus 32 Bit.
Darstellung in vier Oktetten.
Netzanteil und Hostanteil unterscheiden.
Präfixschreibweise verstehen.
private IPv4-Bereiche kennen.
Netzadresse,
Broadcast
und nutzbare Hosts bestimmen.

Private Bereiche:

Bereich	CIDR
10.0.0.0 bis 10.255.255.255	10.0.0.0/8
172.16.0.0 bis 172.31.255.255	172.16.0.0/12
192.168.0.0 bis 192.168.255.255	192.168.0.0/16

Merksatz:

Private IPv4-Adressen werden im Internet nicht direkt geroutet.

Checkliste: Subnetting

Das solltest du sicher können:

Präfix in Netzbits und Hostbits zerlegen.
Hostanzahl berechnen.
Blockgröße bestimmen.
Netzadresse finden.
Broadcastadresse finden.
erste und letzte nutzbare Adresse bestimmen.
größere und kleinere Präfixe richtig einordnen.

Formel:

nutzbare Hosts = 2 hoch Hostbits minus 2

Beispiel:

```
/26
```

Hostbits:

```
32 - 26 = 6
```

Adressen:

```
64
```

Nutzbare Hosts:

```
62
```

Merksatz:

```
Mehr Hostbits bedeuten mehr Hosts.
Mehr Netzbits bedeuten kleinere Subnetze.
```

Checkliste: häufige IPv4-Präfixe

Präfix	Maske	Adressen	nutzbare Hosts
/24	255.255.255.0	256	254
/25	255.255.255.128	128	126
/26	255.255.255.192	64	62
/27	255.255.255.224	32	30
/28	255.255.255.240	16	14
/29	255.255.255.248	8	6
/30	255.255.255.252	4	2

Merksatz:

```
Von /24 zu /25 halbiert sich die Anzahl der Adressen.
Von /25 zu /24 verdoppelt sie sich.
```

Checkliste: IPv6

Das solltest du sicher können:

- IPv6 hat 128 Bit.
- Schreibweise in hexadezimalen Blöcken.
- führende Nullen können weggelassen werden.
- einmalige Kürzung mit doppeltem Doppelpunkt möglich.
- kein klassischer IPv4-Broadcast.
- SLAAC und DHCPv6 grob einordnen.
- Link-Local-Adressen erkennen.

Wichtige Begriffe:

- Global Unicast
- Link-Local
- Multicast
- SLAAC
- DHCPv6
- Präfix

Merksatz:

- IPv6 ist nicht einfach nur längeres IPv4.

Checkliste: Gateway und Routing

Das solltest du sicher können:

- Gateway ist Router in andere Netze.
- Ohne Gateway meist nur lokales Netz erreichbar.
- Routing-Tabelle enthält Zielnetz,
- Gateway,
- Interface
- und Metrik.
- spezifischste Route gewinnt.
- Standardroute ist Weg für unbekannte Ziele.

Typisches Fehlerbild:

```
lokal erreichbar,
Internet nicht erreichbar
```

Wahrscheinlich:

```
Gateway,
NAT
oder Firewall
```

Merksatz:

```
Gateway führt aus dem eigenen Netz heraus.
```

Checkliste: DNS

Das solltest du sicher können:

```
DNS löst Namen in IP-Adressen auf.
DNS kann auch Reverse Lookup liefern.
wichtige Recordtypen kennen.
DNS-Probleme von IP-Problemen unterscheiden.
nslookup oder dig als Prüfwerkzeuge kennen.
```

Wichtige Records:

Record	Bedeutung
A	Name zu IPv4
AAAA	Name zu IPv6
CNAME	Alias
MX	Mailserver
TXT	Textinformationen
NS	Nameserver
PTR	Reverse DNS

Merksatz:

```
IP funktioniert,
Name nicht:
DNS prüfen.
```

Checkliste: DHCP

Das solltest du sicher können:

```
DHCP verteilt IP-Konfiguration automatisch.
DHCP vergibt IP-Adresse,
Maske,
Gateway,
DNS
und Lease-Zeit.
DORA-Ablauf kennen.
APIPA erkennen.
DHCP-Relay grob verstehen.
```

DORA:

```
Discover
Offer
Request
Acknowledge
```

APIPA:

```
169.254.0.0/16
```

Merksatz:

```
169.254.x.x bedeutet häufig:
kein DHCP erhalten.
```

Checkliste: ARP

Das solltest du sicher können:

ARP löst IPv4-Adresse in MAC-Adresse auf.
ARP funktioniert im lokalen Netz.
ARP wird benötigt,
um Frames an das lokale Ziel oder Gateway zu senden.
ARP-Spoofing als Angriff kennen.

Merksatz:

ARP verbindet IPv4 und MAC im lokalen Netz.

Checkliste: Switching

Das solltest du sicher können:

Switch arbeitet hauptsächlich auf Schicht 2.
Switch lernt MAC-Adressen.
MAC-Adresstabelle ordnet MACs Ports zu.
unbekannte Ziel-MAC führt zu Flooding.
Broadcasts werden im VLAN verteilt.
Schleifen können Broadcast-Stürme verursachen.

Merksatz:

Switches leiten Frames anhand von MAC-Adressen weiter.

Checkliste: VLAN

Das solltest du sicher können:

VLAN trennt logisch auf Schicht 2.
VLANs bilden getrennte Broadcast-Domänen.
Access-Port und Trunk-Port unterscheiden.
Inter-VLAN-Routing benötigt Router oder Layer-3-Switch.
VLANs verbessern Struktur und Sicherheit,
ersetzen aber keine Firewall.

Porttyp	Bedeutung

Access-Port	ein VLAN, meistens Endgerät
Trunk-Port	mehrere VLANs, meistens Verbindung zwischen Netzwerkgeräten

Merksatz:

```
Access = ein VLAN.
Trunk = mehrere VLANs.
```

Checkliste: STP

Das solltest du sicher können:

```
STP verhindert Schleifen auf Schicht 2.
Schleifen können Broadcast-Stürme verursachen.
STP blockiert redundante Pfade logisch.
Redundanz ist möglich,
ohne Schleife aktiv zu nutzen.
```

Merksatz:

```
STP schützt vor Layer-2-Schleifen.
```

Checkliste: TCP

Das solltest du sicher können:

```
TCP ist verbindungsorientiert.
TCP ist zuverlässig.
TCP nutzt Bestätigungen.
TCP kann verlorene Daten erneut übertragen.
TCP stellt Reihenfolge sicher.
TCP nutzt Ports.
TCP hat mehr Overhead als UDP.
```

Typische Dienste:

HTTP
HTTPS
SSH
SMTP
IMAP
POP3
RDP

Merksatz:

TCP = zuverlässig und verbindungsorientiert.

Checkliste: UDP

Das solltest du sicher können:

UDP ist verbindungslos.
UDP hat wenig Overhead.
UDP garantiert keine Zustellung.
UDP garantiert keine Reihenfolge.
UDP ist gut für schnelle oder zeitkritische Kommunikation.

Typische Dienste:

DNS
DHCP
VoIP
Streaming
Gaming

Merksatz:

UDP = schnell,
schlank
und verbindungslos.

Checkliste: Standardports

Dienst	Protokoll	Port
FTP	TCP	21
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 mit Dienst,
> Protokoll
> und Zweck lernen.

Checkliste: NAT, PAT und Portweiterleitung

Das solltest du sicher können:

> NAT übersetzt IP-Adressen.
> PAT nutzt zusätzlich Ports.
> PAT ermöglicht vielen Clients eine öffentliche IP.
> Portweiterleitung macht internen Dienst extern erreichbar.
> NAT ist keine vollwertige Firewall.
> Portweiterleitung erhöht Angriffsfläche.

Merksatz:

> NAT übersetzt Adressen.
> PAT unterscheidet über Ports.
> Portweiterleitung veröffentlicht Dienste.

Checkliste: Firewall

Das solltest du sicher können:

> Firewall filtert Verkehr.
> Regeln enthalten Quelle,
> Ziel,
> Port,
> Protokoll,
> Richtung
> und Aktion.
> Default Deny ist sicherer.
> Any-to-Any ist kritisch.
> Stateful Firewall kennt Verbindungszustände.
> Firewall-Logs helfen bei Fehlersuche.

Merksatz:

> Firewall-Regeln so eng wie möglich formulieren.

Checkliste: DMZ

Das solltest du sicher können:

> DMZ ist getrenntes Netz für öffentlich erreichbare Dienste.
> DMZ schützt internes Netz.
> DMZ-Systeme dürfen nur notwendige Verbindungen haben.
> typische Systeme sind Webserver,
> Reverse Proxy,
> Mail-Gateway
> und VPN-Gateway.

Merksatz:

> DMZ trennt öffentliche Dienste vom internen Netz.

Checkliste: VPN

Das solltest du sicher können:

> VPN verschlüsselt Verbindung über unsichere Netze.
> Remote-Access-VPN verbindet Benutzer.
> Site-to-Site-VPN verbindet Standorte.
> VPN ersetzt keine Rechteverwaltung.
> VPN braucht Authentifizierung,
> Routing,
> DNS
> und Firewall-Regeln.

Merksatz:

> VPN schützt den Transportweg,
> aber nicht automatisch alle Zugriffe.

Checkliste: Cloud

Das solltest du sicher können:

> IaaS,
> PaaS
> und SaaS unterscheiden.
> Public,
> Private,
> Hybrid
> und Multi Cloud unterscheiden.
> Shared Responsibility erklären.
> IAM als Zugriffskontrolle verstehen.
> Security Groups grob einordnen.
> Kostenkontrolle und Monitoring beachten.

Modell	Bedeutung
IaaS	Infrastruktur
PaaS	Plattform
SaaS	fertige Anwendung

Merksatz:

> Cloud bedeutet geteilte Verantwortung.

Checkliste: IT-Sicherheit

Das solltest du sicher können:

> Vertraulichkeit,
> Integrität
> und Verfügbarkeit unterscheiden.
> Authentizität und Nichtabstreitbarkeit kennen.
> Schwachstelle,
> Bedrohung
> und Risiko unterscheiden.
> technische,
> organisatorische,
> personelle
> und physische Maßnahmen unterscheiden.

Merksatz:

> Schutzmaßnahme immer zum Risiko und Schutzziel passend wählen.

Checkliste: typische Angriffe

Angriff	Kurzbeschreibung
Malware	Schadsoftware
Ransomware	verschlüsselt oder sperrt Daten
Phishing	Täuschung zur Datenpreisgabe
Social Engineering	Manipulation von Menschen

Angriff	Kurzbeschreibung
DoS	Dienstüberlastung
DDoS	verteilter DoS
MitM	Angreifer zwischen Kommunikationspartnern
Spoofing	Identität oder Herkunft vortäuschen
SQL Injection	SQL-Code einschleusen
XSS	Skript im Browser ausführen
CSRF	gültige Sitzung missbrauchen
Brute Force	systematisches Ausprobieren

Merksatz:

> Angriff erkennen,
> Schutzziel zuordnen,
> Maßnahme nennen.

Checkliste: Schutzmaßnahmen

Risiko	Maßnahme
Passwortdiebstahl	MFA
Malware	EDR, Patchmanagement
Ransomware	Backup, Segmentierung
DDoS	DDoS-Schutz, CDN
Datenabfluss	DLP, Verschlüsselung
unsichere Rechte	Least Privilege
alte Software	Patchmanagement
Fehlkonfiguration	Change Management
unklare Vorfälle	Logging, SIEM
Phishing	Schulung, MFA, Mailfilter

Merksatz:

> Gute Sicherheit besteht aus mehreren Schutzschichten.

Checkliste: Benutzer und Rechte

Das solltest du sicher können:

Benutzerkonto als digitale Identität erklären.
persönliche Konten statt Sammelkonten.
Gruppen und Rollen unterscheiden.
RBAC und ABAC grob erklären.
Authentifizierung und Autorisierung unterscheiden.
Least Privilege erklären.
Admin- und Alltagskonto trennen.
Dienstkonten rechtearm betreiben.
Offboarding konsequent durchführen.

Merksatz:

Rechte müssen notwendig,
nachvollziehbar
und regelmäßig geprüft sein.

Checkliste: Logs und Monitoring

Das solltest du sicher können:

Logging und Monitoring unterscheiden.
Alerting erklären.
typische Logquellen nennen.
zentrale Logsammlung erklären.
NTP-Bedeutung für Logs kennen.
Health Checks verstehen.
Backup-Monitoring erklären.
Zertifikatsüberwachung beachten.

Begriff	Bedeutung
Logging	Ereignisse aufzeichnen
Monitoring	Zustände überwachen
Alerting	alarmieren
Reporting	auswerten

Merksatz:

> Logs zeigen Ereignisse.
> Monitoring zeigt Zustände.

Checkliste: Netzwerkbefehle

Aufgabe	Windows	Linux/macOS
IP prüfen	ipconfig	ip addr
Routing prüfen	route print	ip route
DNS prüfen	nslookup	dig
Erreichbarkeit prüfen	ping	ping
Route verfolgen	tracert	traceroute
Verbindungen prüfen	netstat	ss
Dienst prüfen	services.msc, PowerShell	systemctl
Logs prüfen	Ereignisanzeige	journalctl

Merksatz:

> Befehle liefern Fakten für die Fehlersuche.

Checkliste: Dateiübertragung

Das solltest du sicher können:

> SMB,
> NFS,
> FTP,
> FTPS,
> SFTP
> und SCP unterscheiden.
> FTP als unverschlüsselt erkennen.
> SFTP und FTPS nicht verwechseln.
> SMB-Port TCP 445 kennen.
> Freigabe- und Dateisystemrechte gemeinsam prüfen.
> Synchronisation nicht mit Backup verwechseln.

Merksatz:

SFTP nutzt SSH.
FTPS nutzt FTP mit TLS.

Checkliste: Backup und Restore

Das solltest du sicher können:

Backup und Restore unterscheiden.
Restore-Test begründen.
Vollbackup,
inkrementell
und differenziell unterscheiden.
Snapshot einordnen.
RPO und RTO unterscheiden.
3-2-1-Regel erklären.
Immutable und Offline Backup erklären.
Redundanz,
Replikation
und Synchronisation von Backup unterscheiden.

Merksatz:

Backup ohne Restore-Test ist unsicher.

Checkliste: Dokumentation und Change Management

Das solltest du sicher können:

Dokumentation als Betriebs- und Sicherheitsmaßnahme erklären.
Systemdokumentation,
Netzwerkdokumentation
und Runbook unterscheiden.
IPAM erklären.
Netzplan erklären.
Change Management erklären.
Standard Change,

Normal Change
und Emergency Change unterscheiden.
Rollback-Plan erklären.
CMDB und Configuration Item grob einordnen.

Merksatz:

Änderungen müssen geplant,
getestet,
dokumentiert
und bei Bedarf rückgängig machbar sein.

Checkliste: typische Fehlerbilder

Fehlerbild	Wahrscheinliche Richtung
IP geht, Name nicht	DNS
Lokal geht, Internet nicht	Gateway, NAT, Firewall
169.254.x.x	DHCP
Host erreichbar, Dienst nicht	Port, Dienst, Firewall
Anmeldung scheitert	Authentifizierung
Anmeldung geht, Zugriff nicht	Autorisierung, Rechte
Zertifikatswarnung	Zertifikat, Hostname, Zeit
nur ein VLAN betroffen	VLAN, Routing, Firewall
nach Update defekt	Änderung, Version, Kompatibilität
Dateiübertragung langsam	Netzwerk, Speicher, Last
Backup nicht nutzbar	Restore-Test, Konsistenz, Schlüssel

Merksatz:

Fehlerbild zuerst einordnen,
dann Maßnahme ableiten.

Checkliste: Prüfungsantwort formulieren

Eine gute Antwort enthält:

klare Ursache
Bezug zur Aufgabe
Fachbegriff
kurze Begründung
passende Prüfung oder Maßnahme
Einheit bei Berechnung
keine unnötigen Ausschweifungen

Struktur bei Fehler:

Ursache
Begründung
Prüfung

Struktur bei Sicherheit:

Risiko
Maßnahme
Wirkung

Merksatz:

Kurz,
fachlich,
begründet.

Checkliste: Rechenaufgaben

Vor Abgabe prüfen:

Bit oder Byte?
Mbit oder MB?
Präfix korrekt?
Netzbits und Hostbits korrekt?
Netzadresse korrekt?
Broadcast korrekt?
nutzbare Hosts korrekt?

Einheit angegeben?

Ergebnis plausibel?

Merksatz:

Einheitenfehler sind klassische Prüfungsfehler.

Checkliste: letzte 10 Minuten vor Abgabe

Name und Aufgabe prüfen.

Alle Teilaufgaben beantwortet?

Gefragte Anzahl eingehalten?

Einheiten ergänzt?

Rechenwege plausibel?

Fachbegriffe korrekt?

Tabellen vollständig?

Netzadresse und Broadcast geprüft?

RPO und RTO nicht verwechselt?

DNS und DHCP nicht verwechselt?

Authentifizierung und Autorisierung nicht verwechselt?

Antwort lesbar und eindeutig?

Merksatz:

Die letzten Minuten bringen oft noch sichere Punkte.

IHK-sichere Kurzformulierung

Prüfungschecklisten helfen dabei, Themen systematisch zu wiederholen und typische Fehler zu vermeiden. Besonders wichtig sind die sichere Zuordnung von OSI-Schichten, MAC-Adresse, IP-Adresse und Port, die Unterscheidung von DNS und DHCP, Gateway und Routing, TCP und UDP, NAT und PAT, Authentifizierung und Autorisierung sowie Backup, Replikation und Synchronisation. Bei Fehlerbildern sollte zuerst das Symptom eingeordnet und anschließend eine passende Prüfung oder Maßnahme genannt werden. Gute Prüfungsantworten sind kurz, fachlich korrekt, begründet und direkt auf die Aufgabenstellung bezogen.

Merksätze

Checklisten ordnen Wiederholung.

OSI hilft bei Fehlersuche.

TCP/IP ist praxisnah.

Kapselung verpackt Daten.

MAC ist Schicht 2.

IP ist Schicht 3.

Port ist Schicht 4.

IPv4 hat 32 Bit.

Private Adressen werden nicht direkt im Internet geroutet.

Subnetting immer systematisch lösen.

Mehr Hostbits bedeuten mehr Hosts.

Gateway führt in andere Netze.

DNS löst Namen auf.

DHCP verteilt Konfiguration.

ARP löst IPv4 zu MAC auf.

Switch lernt MAC-Adressen.

VLAN trennt logisch.

STP verhindert Schleifen.

TCP ist zuverlässig.

UDP ist schlank.

Ports mit Dienst und Protokoll lernen.

NAT übersetzt Adressen.

PAT nutzt Ports.

Firewall filtert Verkehr.

DMZ trennt öffentliche Dienste.

VPN verschlüsselt Verbindungen.

Cloud bedeutet geteilte Verantwortung.

Sicherheit schützt Vertraulichkeit,
Integrität
und Verfügbarkeit.

Rechte regelmäßig prüfen.

Logs zeigen Ereignisse.

Monitoring zeigt Zustände.

Befehle liefern Fakten.

FTP ist unverschlüsselt.

SFTP ist nicht FTPS.

Backup ohne Restore-Test ist unsicher.

Replikation ist kein Backup.

Dokumentation macht Betrieb nachvollziehbar.

Change Management kontrolliert Änderungen.

Fehlerbild bestimmt Prüfweg.

Prüfungsantwort:

kurz,

fachlich,

begründet.

18.4 Merksätze und Prüfungswissen zur Prüfungsvorbereitung

Diese Seite fasst die wichtigsten Punkte zur Prüfungsvorbereitung zusammen.

Sie dient als Abschluss für das Kapitel Prüfungsvorbereitung und Wiederholung.

Im Mittelpunkt stehen:

- Aufgaben richtig lesen
- Operatoren beachten
- Signalwörter erkennen
- Fehlerbilder einordnen
- Fachbegriffe sauber verwenden
- Rechenaufgaben systematisch lösen
- Antworten kurz und prüfungssicher formulieren

Merksatz:

> Prüfungsvorbereitung heißt:
> Wissen verstehen,
> anwenden
> und sauber formulieren.

Wichtigste Grundregel

Die wichtigste Regel in der Prüfung lautet:

> Erst die Aufgabe verstehen,
> dann antworten.

Nicht sofort auf bekannte Stichwörter reagieren.

Immer prüfen:

> Was wird wirklich gefragt?

Welche Informationen sind gegeben?

Welche Einschränkungen stehen in der Aufgabe?

Wie viele Antworten werden verlangt?

Soll ich nennen,
erklären,
begründen,
vergleichen
oder berechnen?

Merksatz:

Die Aufgabenstellung entscheidet,
wie die Antwort aussehen muss.

Operatoren sicher beachten

Operator	Erwartung
nennen	kurze Begriffe oder Stichpunkte
beschreiben	sachlich darstellen
erklären	Zusammenhang deutlich machen
begründen	Warum nennen
vergleichen	Unterschiede und Gemeinsamkeiten darstellen
berechnen	rechnerisch ermitteln
bewerten	fachlich einschätzen
zuordnen	passend einordnen

Merksatz:

Wer den Operator ignoriert,
beantwortet schnell die falsche Frage.

Antworten nach Operator formulieren

Beispiel „nennen“:

Zwei Vorteile von VLANs sind logische Netztrennung
und kleinere Broadcast-Domänen.

Beispiel „erklären“:

VLANs trennen ein physisches Netzwerk logisch in mehrere getrennte Netzbereiche.
Dadurch können Geräte verschiedener Abteilungen oder Sicherheitszonen getrennt werden.

Beispiel „begründen“:

VLANs erhöhen die Struktur und Sicherheit,
weil Broadcastverkehr begrenzt
und Zugriffe zwischen Netzbereichen gezielter geregelt werden können.

Merksatz:

Gleicher Begriff,
andere Antworttiefe je nach Operator.

Signalwörter erkennen

Signalwörter zeigen oft direkt die Richtung der Lösung.

Signalwort oder Fehlerbild	Wahrscheinliches Thema
IP erreichbar, Name nicht	DNS
169.254.x.x	DHCP
lokal erreichbar, extern nicht	Gateway, NAT, Firewall
Host erreichbar, Dienst nicht	Port, Dienst, Firewall
Anmeldung fehlgeschlagen	Authentifizierung
Zugriff verweigert	Autorisierung, Rechte
Zertifikatswarnung	Zertifikat, Hostname, Zeit
nur ein VLAN betroffen	VLAN, Routing, Firewall
nach Update defekt	Change, Version, Kompatibilität
viele fehlgeschlagene Logins	Brute Force, Passwortangriff
verschlüsselte Dateien	Ransomware

Signalwort oder Fehlerbild	Wahrscheinliches Thema
gestohlene Zugangsdaten	Phishing, Credential Theft
Backup nicht lesbar	Restore-Test, Konsistenz, Schlüssel

Merksatz:

> Signalwörter sind Hinweise,
> keine Zufälle.

Typische Fehlerbilder sicher zuordnen

Fehlerbild	Erste Prüfung
kein Netzwerk	Kabel, WLAN, Link, IP
kein Internet	Gateway, DNS, NAT, Firewall
Name funktioniert nicht	DNS
falsche automatische IP	DHCP
Dienst nicht erreichbar	Port, Dienststatus, Firewall
Datei nicht zugreifbar	Rechte, Gruppe, ACL
Login nicht möglich	Konto, Passwort, MFA, Verzeichnisdienst
Webseite 404	URL, Pfad, Webserver
Webseite 500	Anwendung, Backend, Logs
Zertifikatsfehler	Ablaufdatum, Hostname, Kette, Uhrzeit
langsame Verbindung	Latenz, Paketverlust, Last, DNS

Merksatz:

> Fehlerbild zuerst einordnen,
> dann gezielt prüfen.

OSI-Modell als Prüfungswerkzeug

Das OSI-Modell hilft, Fehler strukturiert einzugrenzen.

Schicht	Typische Fehler
1	Kabel defekt, kein Link, falscher Stecker
2	VLAN falsch, MAC-Problem, ARP, Switchport

Schicht	Typische Fehler
3	IP falsch, Gateway falsch, Routingfehler
4	Port blockiert, TCP/UDP-Problem
5	Sitzung abgelaufen, Sessionproblem
6	TLS, Zertifikat, Codierung
7	DNS, DHCP, HTTP, SMTP, SMB

Merksatz:

> Von unten nach oben prüfen:
> physisch,
> Netzwerk,
> Dienst,
> Anwendung.

MAC, IP und Port nicht verwechseln

Begriff	Schicht	Aufgabe
MAC-Adresse	2	lokale Zustellung im LAN
IP-Adresse	3	logische Adressierung über Netze
Port	4	Zuordnung zu einem Dienst

Merksatz:

> MAC findet lokal.
> IP findet das Zielnetz.
> Port findet den Dienst.

DNS und DHCP nicht verwechseln

DNS:

> löst Namen in IP-Adressen auf

DHCP:

verteilt IP-Konfiguration automatisch

Beispiel DNS-Problem:

IP funktioniert,
Name nicht.

Beispiel DHCP-Problem:

Client erhält 169.254.x.x
oder keine passende IP-Konfiguration.

Merksatz:

DNS beantwortet:
Wie heißt die IP?

DHCP beantwortet:
Welche IP bekomme ich?

Gateway und DNS unterscheiden

Gateway:

Weg in andere Netze

DNS:

Namensauflösung

Typisches Gateway-Problem:

lokales Netz erreichbar,
Internet nicht

Typisches DNS-Problem:

IP erreichbar,

Name nicht

Merksatz:

Gateway ist der Weg.

DNS ist das Telefonbuch.

TCP und UDP sicher unterscheiden

Merkmal	TCP	UDP
Verbindung	verbindungsorientiert	verbindungslos
Zustellung	zuverlässig	keine eingebaute Garantie
Reihenfolge	wird gesichert	nicht garantiert
Overhead	höher	geringer
Einsatz	vollständige Datenübertragung	schnelle oder zeitkritische Kommunikation

Merksatz:

TCP = zuverlässig.

UDP = schlank.

Wichtige Ports sicher können

Dienst	Port
FTP	TCP 21
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

Dienst	Port
IMAP	TCP 143
HTTPS	TCP 443
SMB	TCP 445
SMTPS	TCP 465
IMAPS	TCP 993
POP3S	TCP 995
RDP	TCP 3389

Merksatz:

> Ports immer mit Dienst und Protokoll lernen.

Subnetting-Prüfungswissen

Bei Subnetting immer gleich vorgehen:

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

Formel:

> nutzbare Hosts = 2 hoch Hostbits minus 2

Merksatz:

> Subnetting wird einfacher,
> wenn die Reihenfolge immer gleich bleibt.

Subnetting-Merksätze

IPv4 hat 32 Bit.

Präfix gibt die Netzbits an.

Hostbits = 32 minus Präfix.

Mehr Netzbits bedeuten kleinere Netze.

Mehr Hostbits bedeuten mehr Hosts.

Netzadresse ist die erste Adresse.

Broadcastadresse ist die letzte Adresse.

Erste nutzbare Adresse = Netzadresse plus 1.

Letzte nutzbare Adresse = Broadcastadresse minus 1.

Pro zusätzlichem Netzbit halbiert sich die Hostanzahl.

Pro zusätzlichem Hostbit verdoppelt sich die Hostanzahl.

Merksatz:

Präfix größer:
Netz kleiner.

Präfix kleiner:
Netz größer.

NAT, PAT und Portweiterleitung unterscheiden

NAT:

übersetzt IP-Adressen

PAT:

übersetzt zusätzlich Ports,
damit mehrere interne Clients eine öffentliche IP nutzen können

Portweiterleitung:

leitet eingehenden Verkehr auf einen internen Dienst weiter

Merksatz:

NAT übersetzt Adressen.
PAT unterscheidet über Ports.
Portweiterleitung veröffentlicht einen Dienst.

Firewall-Prüfungswissen

Eine Firewall filtert Verkehr anhand von Regeln.

Typische Regelbestandteile:

Quelle
Ziel
Port
Protokoll
Richtung
Aktion
Zustand
Zweck

Sichere Grundregel:

Default Deny

Das bedeutet:

Standardmäßig blockieren,
nur benötigten Verkehr erlauben.

Merksatz:

Firewall-Regeln so eng wie möglich formulieren.

VPN-Prüfungswissen

Remote-Access-VPN:

einzelner Benutzer verbindet sich mit einem Netzwerk

Site-to-Site-VPN:

zwei Netzwerke oder Standorte werden verbunden

Wichtig:

VPN verschlüsselt den Transportweg,
ersetzt aber keine Rechteverwaltung.

Merksatz:

VPN schützt Verbindung,
nicht automatisch jede Berechtigung.

Cloud-Prüfungswissen

IaaS:

virtuelle Infrastruktur

PaaS:

Plattform für Anwendungen

SaaS:

fertige Anwendung

Public Cloud:

öffentlich angebotene Cloud

Private Cloud:

Cloud für eine Organisation

Hybrid Cloud:

Kombination aus lokal und Cloud

Multi Cloud:

Nutzung mehrerer Cloud-Anbieter

Merksatz:

IaaS,
PaaS
und SaaS beschreiben Servicemodelle.

Public,
Private,
Hybrid
und Multi Cloud beschreiben Bereitstellungsmodelle.

Shared Responsibility

Beim Shared-Responsibility-Modell teilen sich Cloud-Anbieter und Kunde die Verantwortung.

Anbieter:

Infrastruktur der Cloud

Kunde:

Daten
Identitäten
Zugriffe
Konfigurationen
Anwendungen je nach Modell

Merksatz:

Cloud-Anbieter übernimmt nicht automatisch alles.

Sicherheitsbegriffe sicher unterscheiden

Begriff	Bedeutung
Vertraulichkeit	Schutz vor unberechtigtem Lesen
Integrität	Schutz vor unbemerkter Veränderung
Verfügbarkeit	Nutzbarkeit von Systemen und Daten
Authentizität	Echtheit einer Identität oder Nachricht
Nichtabstreitbarkeit	Nachweisbarkeit einer Handlung
Schwachstelle	ausnutzbare Lücke
Bedrohung	mögliches schädliches Ereignis
Risiko	Wahrscheinlichkeit und Auswirkung
Maßnahme	reduziert Risiko

Merksatz:

Schwachstelle ist die Lücke.
Bedrohung ist das Ereignis.
Risiko ist die bewertete Gefahr.

Angriffe sicher zuordnen

Angriff	Typisches Ziel
Phishing	Zugangsdaten, Identitäten
Ransomware	Verfügbarkeit, oft auch Vertraulichkeit

Angriff	Typisches Ziel
DDoS	Verfügbarkeit
Man-in-the-Middle	Vertraulichkeit und Integrität
SQL Injection	Datenbank
XSS	Browser anderer Benutzer
CSRF	gültige Sitzung
Brute Force	Passwort
Credential Stuffing	wiederverwendete Zugangsdaten
Spoofing	Identität oder Herkunft

Merksatz:

> Angriff immer dem Ziel und Schutzziel zuordnen.

Schutzmaßnahmen sicher zuordnen

Risiko	passende Maßnahme
gestohlenes Passwort	MFA
zu viele Rechte	Least Privilege
Malware	EDR, Patchmanagement
Ransomware	Backup, Immutable Backup, Segmentierung
DDoS	DDoS-Schutz, CDN, Rate Limiting
unsichere Freigaben	Rechteprüfung, Ablaufdatum
fehlende Nachvollziehbarkeit	Logging, SIEM
Fehlkonfiguration	Change Management
unsichere Benutzer	Schulung, Awareness
veraltete Software	Patchmanagement

Merksatz:

> Maßnahme muss direkt zum Risiko passen.

Authentifizierung und Autorisierung

Authentifizierung:

Wer bist du?

Autorisierung:

Was darfst du?

Beispiel:

Benutzer meldet sich mit Passwort und MFA an.
Danach wird geprüft,
ob er auf einen Ordner zugreifen darf.

Merksatz:

Erst Identität,
dann Rechte.

Least Privilege und Need to Know

Least Privilege:

nur notwendige Rechte

Need to Know:

nur notwendige Informationen

Beispiel:

Ein Supportmitarbeiter braucht vielleicht Zugriff auf Gerätedaten,
aber nicht auf Gehaltsdaten.

Merksatz:

Least Privilege begrenzt Rechte.
Need to Know begrenzt Informationen.

Backup, Replikation und Synchronisation unterscheiden

Backup:

wiederherstellbare Sicherung alter Zustände

Replikation:

aktuelle Kopie auf anderem System

Synchronisation:

Abgleich zwischen Speicherorten

Risiko:

Fehler,
Löschung
oder Ransomware können bei Replikation oder Synchronisation mit übertragen werden.

Merksatz:

Sync und Replikation sind kein Backup.

RPO und RTO

RPO:

maximal akzeptabler Datenverlust

RTO:

maximal akzeptable Wiederherstellungszeit

Beispiel:

RPO 1 Stunde:
maximal 1 Stunde Datenverlust

RTO 4 Stunden:
Dienst soll spätestens nach 4 Stunden wieder laufen

Merksatz:

RPO = Datenverlust.
RTO = Zeit bis Wiederherstellung.

Logging, Monitoring und Alerting unterscheiden

Logging:

Ereignisse werden aufgezeichnet

Monitoring:

Zustände werden überwacht

Alerting:

bei kritischen Zuständen wird alarmiert

Reporting:

Zustände werden über einen Zeitraum ausgewertet

Merksatz:

Logs zeigen Ereignisse.
Monitoring zeigt Zustände.
Alerting meldet Probleme.

Wichtige Befehle sicher einordnen

Aufgabe	Werkzeug
IP-Konfiguration Windows	ipconfig
IP-Konfiguration Linux	ip addr
Routing Windows	route print
Routing Linux	ip route
DNS prüfen	nslookup, dig
Erreichbarkeit prüfen	ping
Weg verfolgen	tracert, traceroute
Verbindungen anzeigen	netstat, ss
Webdienst prüfen	curl
Linux-Dienst prüfen	systemctl
Linux-Logs prüfen	journalctl
Windows-Logs prüfen	Ereignisanzeige

Merksatz:

> Befehle liefern Fakten,
> keine Vermutungen.

Typische Prüfungsfallen

> DNS und DHCP verwechseln.
>
> Gateway und DNS verwechseln.
>
> MAC,
> IP
> und Port verwechseln.
>
> TCP und UDP verwechseln.
>
> NAT,
> PAT
> und Portweiterleitung verwechseln.
>
> VLAN und Subnetz gleichsetzen.

Firewall und Router verwechseln.

Authentifizierung und Autorisierung verwechseln.

Backup,
Replikation
und Synchronisation verwechseln.

RPO und RTO verwechseln.

SFTP und FTPS verwechseln.

IDS und IPS verwechseln.

Redundanz als Backup bezeichnen.

Snapshot als vollständiges Backup bezeichnen.

ping als vollständigen Diensttest verstehen.

Merksatz:

Prüfungsfallen sind oft Begriffsfallen.

Gute Antwortstruktur bei Fehlersuche

Struktur:

Ursache
Begründung
Prüfung

Beispiel:

Wahrscheinlich liegt ein DNS-Problem vor,
da die IP-Adresse erreichbar ist,
der Name aber nicht aufgelöst wird.

Der DNS-Server und der DNS-Eintrag sollten mit nslookup oder dig geprüft werden.

Merksatz:

Fehlerantwort:
Ursache,
Begründung,
Prüfung.

Gute Antwortstruktur bei Sicherheitsfragen

Struktur:

Risiko
Maßnahme
Wirkung

Beispiel:

Das Risiko besteht im Missbrauch gestohlener Zugangsdaten.
Durch MFA reicht ein gestohlenes Passwort allein nicht mehr aus.
Dadurch wird die Wahrscheinlichkeit eines unberechtigten Zugriffs reduziert.

Merksatz:

Sicherheitsantwort:
Risiko,
Maßnahme,
Wirkung.

Gute Antwortstruktur bei Vergleichen

Struktur:

Gemeinsamkeit
Unterschied
Beispiel

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:

```
Vergleich:
Gemeinsamkeit,
Unterschied,
Beispiel.
```

Gute Antwortstruktur bei Berechnungen

Struktur:

```
gegebene Werte
Formel oder Regel
Rechenschritt
Ergebnis mit Einheit
Plausibilitätsprüfung
```

Beispiel:

```
Bei /27 gibt es 5 Hostbits.
2 hoch 5 ergibt 32 Adressen.
Davon sind 30 nutzbar,
weil Netzadresse und Broadcastadresse nicht für Hosts genutzt werden.
```

Merksatz:

```
Berechnung immer mit Bedeutung des Ergebnisses angeben.
```

Letzte Prüfungsminute

Kurz vor Abgabe prüfen:

```
Habe ich alle Teilfragen beantwortet?

Habe ich die geforderte Anzahl genannt?

Habe ich Einheiten ergänzt?

Habe ich Fachbegriffe sauber verwendet?

Habe ich DNS und DHCP nicht verwechselt?

Habe ich RPO und RTO nicht verwechselt?

Habe ich bei Subnetting Netzadresse und Broadcast geprüft?

Habe ich bei Sicherheitsfragen die Maßnahme begründet?

Habe ich bei Fehlersuche eine Prüfung genannt?
```

Merksatz:

```
Die letzte Kontrolle verhindert einfache Punktverluste.
```

IHK-sichere Gesamtformulierung

Für die Prüfung ist entscheidend, Aufgabenstellungen genau zu lesen, Operatoren zu beachten und technische Hinweise richtig einzuordnen. Netzwerkfehler sollten systematisch nach OSI-Modell geprüft werden: physische Verbindung, IP-Konfiguration, Gateway, DNS, Routing, Firewall, Dienst und Anwendung. Wichtige Begriffe wie MAC-Adresse, IP-Adresse, Port, DNS, DHCP, TCP, UDP, NAT, PAT, Authentifizierung, Autorisierung, Backup, Replikation, RPO und RTO müssen sauber unterschieden werden. Gute Antworten sind kurz, fachlich korrekt und begründet. Bei Fehlersuche werden Ursache, Begründung und Prüfung genannt. Bei Sicherheitsfragen werden Risiko, Maßnahme und Wirkung verbunden.

Wichtigste Merksätze

```
Erst Aufgabe verstehen,
dann antworten.
```

Operator beachten.

Signalwörter erkennen.

Fehlerbild einordnen.

OSI als Fehlersuche nutzen.

MAC ist lokal.

IP ist logisch.

Port ist Dienst.

DNS löst Namen auf.

DHCP verteilt Konfiguration.

Gateway führt in andere Netze.

TCP ist zuverlässig.

UDP ist schlank.

NAT übersetzt Adressen.

PAT nutzt Ports.

Portweiterleitung veröffentlicht Dienste.

Firewall filtert Verkehr.

VPN schützt Verbindung.

Cloud bedeutet geteilte Verantwortung.

Vertraulichkeit schützt vor Mitlesen.

Integrität schützt vor Manipulation.

Verfügbarkeit schützt Nutzbarkeit.

MFA schützt gegen Passwortmissbrauch.

Least Privilege begrenzt Rechte.

Backup ist Wiederherstellungsvorsorge.

Replikation ist kein Backup.

Synchronisation ist kein Backup.

RPO ist Datenverlust.

RTO ist Wiederherstellungszeit.

Logging zeigt Ereignisse.

Monitoring zeigt Zustände.

Alerting meldet Probleme.

Befehle liefern Fakten.

Prüfungsfallen sind oft Begriffsfallen.

Fehlerantwort:
Ursache,
Begründung,
Prüfung.

Sicherheitsantwort:
Risiko,
Maßnahme,
Wirkung.

Vergleich:
Gemeinsamkeit,
Unterschied,

Beispiel.

Berechnung:
Regel,
Ergebnis,
Einheit.

Kurz,
fachlich,
begründet.