17.10 Prüfungsvorbereitung und Wiederholung

Prüfungsvorbereitung und Wiederholung

Dieses Kapitel dient zur gezielten Wiederholung vor der Prüfung.

Es verbindet die wichtigsten Themen aus:

- Netzwerktechnik
- OSI-Modell
- TCP/IP
- IP-Adressierung
- Subnetting
- Routing
- Switching
- VLAN
- DNS
- DHCP
- Firewalls
- NAT
- VPN
- Cloud
- Sicherheit
- Administration
- Fehlersuche

Merksatz:

> Prüfungsvorbereitung bedeutet nicht nur Auswendiglernen,
> sondern Zusammenhänge erkennen.

Warum Wiederholung wichtig ist

Viele Prüfungsthemen hängen zusammen.

Beispiel:

> Ein Client kommt nicht ins Internet.

Dafür können mehrere Themen relevant sein:

```
IP-Adresse
Subnetzmaske
Gateway
DNS
DHCP
Routing
Firewall
NAT
VLAN
WLAN
Proxy
VPN
Dienstverfügbarkeit
```

Merksatz:

```
In der Prüfung wird selten nur ein einzelnes Thema isoliert geprüft.
```

Typische Prüfungslogik

Prüfungsaufgaben fragen oft nicht direkt:

```
Was ist DNS?
```

Sondern eher:

```
Ein Client kann eine Webseite nicht über den Namen erreichen,
aber die IP-Adresse funktioniert.
Welche Ursache ist wahrscheinlich?
```

Gesuchte Antwort:

```
DNS-Problem
```

Merksatz:

Prüfungen testen Anwendung von Wissen,
nicht nur Definitionen.

Wichtigste Grundregel bei Netzwerkfehlern

Immer systematisch prüfen:

1. Physische Verbindung
2. IP-Konfiguration
3. Gateway
4. DNS
5. Routing
6. Firewall
7. Dienst
8. Anwendung
9. Logs
10. Änderungen

Merksatz:

Erst Grundlagen,
dann Spezialfälle.

OSI-Modell als Prüfungswerkzeug

Das OSI-Modell hilft, Fehler schichtweise einzugrenzen.

OSI-Schicht	Name	Typische Prüfung
1	Bitübertragung	Kabel, Signal, Link
2	Sicherung	MAC, Switch, VLAN, ARP
3	Vermittlung	IP, Routing, ICMP
4	Transport	TCP, UDP, Ports
5	Sitzung	Session, Verbindungssitzung
6	Darstellung	TLS, Codierung, Verschlüsselung
7	Anwendung	DNS, DHCP, HTTP, SMTP, SMB

Merksatz:

OSI hilft,
Fehler strukturiert zu suchen.

TCP/IP-Modell wiederholen

Das TCP/IP-Modell ist praxisnaher als das OSI-Modell.

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

Merksatz:

TCP/IP ist das praktische Internetmodell.

Kapselung wiederholen

Beim Senden werden Daten schrittweise verpackt.

Beispiel:

Anwendung erzeugt Daten.
TCP ergänzt Portinformationen.
IP ergänzt IP-Adressen.
Ethernet ergänzt MAC-Adressen.
Bits werden übertragen.

Beim Empfangen wird alles wieder entpackt.

Merksatz:

Kapselung bedeutet:
Jede Schicht ergänzt eigene Steuerinformationen.

PDU-Begriffe wiederholen

Schicht	Einheit
Anwendung	Daten
Transport	Segment oder Datagramm
Internet / Netzwerk	Paket
Sicherung	Frame
Bitübertragung	Bits

Merksatz:

> Daten werden zu Segmenten,
> Paketen,
> Frames
> und Bits.

MAC-Adresse wiederholen

Eine MAC-Adresse arbeitet auf Schicht 2.

Sie dient der lokalen Zustellung im selben Netzwerksegment.

Wichtig:

> MAC-Adressen werden von Switches genutzt.
> MAC-Adressen ändern sich an jedem Router-Hop.
> MAC-Adressen sind nicht für Routing über Netze hinweg zuständig.

Merksatz:

> MAC-Adresse = lokale Zustellung im LAN.

IP-Adresse wiederholen

Eine IP-Adresse arbeitet auf Schicht 3.

Sie dient der logischen Adressierung über Netzgrenzen hinweg.

Wichtig:

IP-Adressen werden für Routing genutzt.

IP-Adressen bestehen aus Netzanteil und Hostanteil.

Subnetzmaske oder Präfix bestimmt die Aufteilung.

Merksatz:

IP-Adresse = logische Adresse für Routing.

Port wiederholen

Ports arbeiten auf Schicht 4.

Sie ordnen Netzwerkverkehr einem Dienst oder Prozess zu.

Beispiele:

TCP 80 HTTP

TCP 443 HTTPS

TCP 22 SSH

TCP 3389 RDP

TCP 25 SMTP

UDP 53 DNS

UDP 67 und 68 DHCP

Merksatz:

Port = Dienstadresse auf einem Host.

MAC, IP und Port unterscheiden

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

Merksatz:

```
MAC findet Gerät im lokalen Netz.
IP findet Netz und Host.
Port findet Dienst.
```

IPv4-Grundlagen wiederholen

IPv4-Adressen bestehen aus 32 Bit.

Sie werden meist dezimal in vier Oktetten dargestellt.

Beispiel:

```
192.168.1.10
```

Dazu gehört eine Subnetzmaske oder Präfixlänge.

Beispiel:

```
192.168.1.10/24
```

Merksatz:

```
IPv4-Adresse plus Präfix bestimmt Netz und Host.
```

Private IPv4-Adressbereiche

Wichtige private IPv4-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 IP-Adressen werden im Internet nicht direkt geroutet.
```

Subnetzmaske wiederholen

Die Subnetzmaske trennt Netzanteil und Hostanteil.

Beispiel:

```
/24 bedeutet:
24 Bit Netzanteil,
8 Bit Hostanteil
```

Bei IPv4 gilt:

```
Hostanzahl = 2 hoch Hostbits minus 2
```

Das minus 2 steht meist für:

```
Netzadresse

und

Broadcastadresse
```

Merksatz:

```
Mehr Hostbits bedeuten mehr mögliche Hosts.
```

Häufige 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:

```
Pro zusätzlichem Netzbit halbiert sich die Hostanzahl.
```

Subnetting-Grundregel

Wenn der Präfix größer wird:

```
mehr Netzbits

weniger Hostbits

kleinere Subnetze
```

Wenn der Präfix kleiner wird:

```
weniger Netzbits

mehr Hostbits

größere Subnetze
```

Merksatz:

```
/25 ist kleiner als /24.
/23 ist größer als /24.
```

Broadcast wiederholen

Die Broadcastadresse ist die letzte Adresse eines IPv4-Subnetzes.

Sie dient dazu, alle Hosts im Subnetz zu erreichen.

Beispiel bei:

```
192.168.1.0/24
```

Broadcast:

```
192.168.1.255
```

Merksatz:

```
Broadcast = letzte Adresse im IPv4-Subnetz.
```

Netzadresse wiederholen

Die Netzadresse ist die erste Adresse eines Subnetzes.

Sie beschreibt das Netzwerk selbst.

Beispiel bei:

```
192.168.1.0/24
```

Netzadresse:

```
192.168.1.0
```

Merksatz:

```
Netzadresse = erste Adresse im Subnetz.
```

Erste und letzte nutzbare Adresse

Bei einem normalen IPv4-Subnetz gilt:

```
erste nutzbare Adresse:
Netzadresse plus 1

letzte nutzbare Adresse:
Broadcastadresse minus 1
```

Beispiel:

```
Netz:
192.168.1.0/24

erste nutzbare:
192.168.1.1

letzte nutzbare:
192.168.1.254
```

Merksatz:

```
Erste nutzbare = Netzadresse + 1.
Letzte nutzbare = Broadcast - 1.
```

Gateway wiederholen

Das Standardgateway ist der Router, über den ein Host andere Netze erreicht.

Ohne Gateway funktioniert meist nur Kommunikation im eigenen Subnetz.

Merksatz:

```
Gateway = Ausgang in andere Netze.
```

DNS wiederholen

DNS übersetzt Namen in IP-Adressen.

Beispiel:

```
www.example.com
```

wird zu:

```
IP-Adresse
```

Typische Fehler:

```
falscher DNS-Server
DNS-Server nicht erreichbar
falscher DNS-Eintrag
DNS-Cache veraltet
Split-DNS bei VPN falsch
```

Merksatz:

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

DHCP wiederholen

DHCP verteilt automatisch Netzwerkkonfiguration.

Typische Informationen:

```
IP-Adresse
Subnetzmaske
Gateway
DNS-Server
Lease-Zeit
```

Merksatz:

```
DHCP nimmt Clients die manuelle IP-Konfiguration ab.
```

DHCP-Ablauf DORA

DORA steht für:

```
Discover
Offer
Request
Acknowledge
```

Ablauf:

```
Client sucht DHCP-Server.
Server bietet Adresse an.
Client fordert Adresse an.
Server bestätigt die Vergabe.
```

Merksatz:

```
DHCP-DORA = Discover,
Offer,
Request,
Acknowledge.
```

ARP wiederholen

ARP löst IPv4-Adresse in MAC-Adresse auf.

Es funktioniert im lokalen Netz.

Beispiel:

```
Wer hat 192.168.1.1?
```

Antwort:

```
MAC-Adresse des Gateways
```

Merksatz:

```
ARP verbindet IPv4 und MAC im lokalen Netz.
```

Switching wiederholen

Ein Switch arbeitet hauptsächlich auf Schicht 2.

Er lernt MAC-Adressen an Ports und leitet Frames passend weiter.

Wenn die Ziel-MAC unbekannt ist, wird geflutet.

Merksatz:

Switch lernt MAC-Adressen und baut eine MAC-Adresstabelle.

VLAN wiederholen

VLANs trennen ein physisches Netzwerk logisch in mehrere getrennte Netze.

Vorteile:

bessere Struktur
weniger Broadcastverkehr pro Segment
Sicherheitszonen
Trennung von Abteilungen
Trennung von Gastnetz und internem Netz

Merksatz:

VLAN trennt logisch auf Schicht 2.

Access-Port und Trunk-Port

Access-Port:

gehört zu einem VLAN

meist für Endgeräte

Trunk-Port:

transportiert mehrere VLANs

meist zwischen Switches,
Router
oder Firewall

Merksatz:

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

Routing wiederholen

Routing verbindet verschiedene IP-Netze.

Router entscheiden anhand der Routing-Tabelle, wohin Pakete weitergeleitet werden.

Merksatz:

```
Routing verbindet Netze.
```

Routing-Tabelle wiederholen

Eine Routing-Tabelle enthält:

```
Zielnetz
Gateway oder Next Hop
Interface
Metrik
```

Wichtig:

```
Die spezifischste passende Route gewinnt.
```

Merksatz:

```
Routing-Tabelle bestimmt den nächsten Weg.
```

ICMP wiederholen

ICMP wird für Kontroll- und Fehlermeldungen genutzt.

Typische Werkzeuge:

```
ping

traceroute
```

Merksatz:

```
ICMP hilft bei Diagnose,
ist aber kein Transportprotokoll für Anwendungen.
```

TCP wiederholen

TCP ist verbindungsorientiert und zuverlässig.

Eigenschaften:

```
Verbindungsaufbau
Reihenfolge
Bestätigung
Wiederholung verlorener Daten
Flusskontrolle
Fehlererkennung
```

Merksatz:

```
TCP = zuverlässig und verbindungsorientiert.
```

UDP wiederholen

UDP ist verbindungslos und schlanker.

Eigenschaften:

```
kein Verbindungsaufbau
keine eingebaute Zustellgarantie
wenig Overhead
schnell
```

Typische Anwendungen:

DNS
DHCP
VoIP
Streaming
Gaming

Merksatz:

UDP = schnell und verbindungslos.

TCP und UDP vergleichen

Merkmal	TCP	UDP
Verbindung	verbindungsorientiert	verbindungslos
Zuverlässigkeit	hoch	keine eingebaute Garantie
Reihenfolge	wird gesichert	nicht garantiert
Overhead	höher	geringer
Beispiele	HTTP, HTTPS, SSH, SMTP	DNS, DHCP, VoIP

Merksatz:

TCP sicherer in der Zustellung.
UDP schneller und einfacher.

NAT wiederholen

NAT steht für:

Network Address Translation

NAT übersetzt IP-Adressen.

Häufigster Fall:

private interne IP-Adressen werden beim Internetzugriff in eine öffentliche IP-Adresse übersetzt.

Merksatz:

```
NAT übersetzt Adressen.
```

PAT wiederholen

PAT steht für:

```
Port Address Translation
```

Dabei nutzen viele interne Geräte eine öffentliche IP-Adresse und werden über Ports unterschieden.

Merksatz:

```
PAT ermöglicht vielen Clients Internetzugriff über eine öffentliche IP.
```

Portweiterleitung wiederholen

Portweiterleitung leitet eingehenden Verkehr von außen an einen internen Dienst weiter.

Beispiel:

```
Extern TCP 443

wird weitergeleitet zu

internem Webserver TCP 443
```

Merksatz:

```
Portweiterleitung macht interne Dienste von außen erreichbar.
```

Firewall wiederholen

Eine Firewall filtert Netzwerkverkehr anhand von Regeln.

Typische Kriterien:

```
Quelle
Ziel
Port
Protokoll
Richtung
Zustand
Benutzer je nach System
Anwendung je nach System
```

Merksatz:

```
Firewall entscheidet,
welcher Verkehr erlaubt oder blockiert wird.
```

DMZ wiederholen

Eine DMZ ist ein getrenntes Netzwerksegment für öffentlich erreichbare Dienste.

Beispiele:

```
Webserver
Reverse Proxy
Mail-Gateway
VPN-Gateway
```

Ziel:

```
interne Netze schützen
```

Merksatz:

```
DMZ trennt öffentliche Dienste vom internen Netz.
```

VPN wiederholen

VPN stellt einen verschlüsselten Tunnel her.

Typische Arten:

Remote-Access-VPN

Site-to-Site-VPN

Merksatz:

VPN verbindet Netze oder Benutzer sicher über unsichere Netze.

Cloud-Modelle wiederholen

Modell	Bedeutung
IaaS	virtuelle Infrastruktur
PaaS	Plattform für Anwendungen
SaaS	fertige Anwendung

Merksatz:

IaaS bietet Infrastruktur.
PaaS bietet Plattform.
SaaS bietet fertige Software.

Cloud-Bereitstellungsmodelle wiederholen

Modell	Bedeutung
Public Cloud	öffentlich angebotene Cloud
Private Cloud	Cloud für eine Organisation
Hybrid Cloud	Kombination aus lokal und Cloud
Multi Cloud	mehrere Cloud-Anbieter

Merksatz:

Hybrid beschreibt Mischung der Betriebsorte.
Multi Cloud beschreibt mehrere Anbieter.

Shared Responsibility wiederholen

In der Cloud teilen sich Anbieter und Kunde Verantwortung.

Grundidee:

```
Anbieter schützt die Cloud-Infrastruktur.

Kunde schützt seine Daten,
Identitäten,
Konfigurationen
und Zugriffe.
```

Merksatz:

```
Cloud-Anbieter übernimmt nicht automatisch alle Sicherheitsaufgaben.
```

Informationssicherheit wiederholen

Wichtige Schutzziele:

```
Vertraulichkeit
Integrität
Verfügbarkeit
```

Zusätzlich wichtig:

```
Authentizität
Nichtabstreitbarkeit
```

Merksatz:

```
CIA-Triade = Vertraulichkeit,
Integrität,
Verfügbarkeit.
```

Typische Angriffe wiederholen

Wichtige Angriffe:

Malware
Ransomware
Phishing
Social Engineering
DoS
DDoS
Man-in-the-Middle
Spoofing
SQL Injection
XSS
CSRF
Brute Force
Credential Stuffing

Merksatz:

Angriff immer dem betroffenen Schutzziel zuordnen.

Typische Schutzmaßnahmen wiederholen

Wichtige Schutzmaßnahmen:

Patchmanagement
Hardening
Firewall
IDS
IPS
EDR
SIEM
MFA
Backup
Netzwerksegmentierung
Least Privilege
Monitoring
Logging
Schulung
Incident Response

Merksatz:

> Sicherheit entsteht durch mehrere Schutzschichten.

Backup wiederholen

Backup bedeutet:

> Sicherung von Daten,
> Systemen
> oder Konfigurationen.

Restore bedeutet:

> Wiederherstellung aus Backup.

Wichtig:

> Backup ohne Restore-Test ist unsicher.

Merksatz:

> Backup ist erst sicher,
> wenn Restore getestet wurde.

RPO und RTO wiederholen

RPO:

> maximal akzeptabler Datenverlust

RTO:

> maximal akzeptable Wiederherstellungszeit

Merksatz:

RPO = Datenverlust.
RTO = Wiederherstellungszeit.

Prüfungsvorgehen bei Rechenaufgaben

Bei Rechenaufgaben wichtig:

Einheiten beachten.
Bits und Bytes unterscheiden.
Mbit/s und MB/s nicht verwechseln.
Netzadresse und Broadcast prüfen.
Hostanzahl mit Hostbits berechnen.
Zwischenschritte sauber notieren.
Ergebnis auf Plausibilität prüfen.

Merksatz:

Viele Fehler entstehen durch Einheiten und Präfixe.

Bit und Byte wiederholen

1 Byte besteht aus:

8 Bit

Beispiele:

100 Mbit/s

ist nicht dasselbe wie:

100 MB/s

Umrechnung:

Bit durch 8 = Byte

Byte mal 8 = Bit

Merksatz:

Bit ist klein b.
Byte ist großes B.

Typische Einheitenfallen

Schreibweise	Bedeutung
b	Bit
B	Byte
kbit	Kilobit
kB	Kilobyte
Mbit	Megabit
MB	Megabyte
Gbit	Gigabit
GB	Gigabyte

Merksatz:

Großes B ist Byte.
Kleines b ist Bit.

Prüfungsstrategie bei Fehlersuche

Bei Fehlersuche:

Problem genau lesen.
Symptome markieren.
Betroffene Systeme erkennen.
Funktioniert IP?
Funktioniert DNS?

Ist Gateway korrekt?

Ist Dienst erreichbar?

Ist Port offen?

Gibt es Firewall-Regeln?

Gab es Änderungen?

Was ist die wahrscheinlichste Ursache?

Merksatz:

Symptome zuerst,
Lösung danach.

Signalwörter in Prüfungsaufgaben

Typische Signalwörter:

Signalwort	Hinweis
IP geht, Name nicht	DNS
lokal geht, Internet nicht	Gateway oder NAT
nur ein VLAN betroffen	VLAN oder Routing
nur ein Dienst betroffen	Port, Dienst, Firewall
alle Dienste langsam	Netzwerk, Last, DNS oder Speicher
Anmeldung schlägt fehl	Authentifizierung oder Konto
Zugriff verweigert	Autorisierung oder Rechte
Zertifikatswarnung	Zertifikat, Hostname oder Zeit
nach Update defekt	Änderung, Version, Kompatibilität
nur extern nicht erreichbar	Firewall, NAT, DNS, Provider

Merksatz:

Signalwörter zeigen die Richtung der Fehlersuche.

Typische IHK-Prüfungsfallen

OSI-Schichten verwechseln.

TCP und UDP verwechseln.

MAC,
IP
und Port verwechseln.

DNS und DHCP verwechseln.

NAT und Portweiterleitung verwechseln.

Firewall und Router verwechseln.

VLAN trennt Schicht 2,
Routing verbindet Netze.

ping prüft ICMP,
nicht jeden Dienst.

Kein ping bedeutet nicht automatisch Ziel offline.

IP funktioniert,
Name nicht:
DNS prüfen.

RDP nutzt TCP 3389.

SSH nutzt TCP 22.

SMB nutzt TCP 445.

HTTPS nutzt TCP 443.

DHCP nutzt UDP 67 und 68.

DNS nutzt häufig UDP 53,
je nach Fall auch TCP 53.

FTP ist unverschlüsselt.

SFTP ist nicht FTPS.

Backup,
Replikation
und Synchronisation unterscheiden.

RPO und RTO unterscheiden.

Authentifizierung und Autorisierung unterscheiden.

Least Privilege nicht mit Need to Know verwechseln.

Prüfungsantworten kurz und fachlich formulieren

Eine gute Prüfungsantwort ist:

fachlich korrekt
kurz
begründet
auf die Aufgabe bezogen
ohne unnötiges Ausschweifen

Schlechtes Beispiel:

Vielleicht liegt es am Internet.

Besser:

Da die Verbindung zur IP-Adresse funktioniert,
aber die Namensauflösung fehlschlägt,
liegt wahrscheinlich ein DNS-Problem vor.

Merksatz:

Antwort immer aus dem Fehlerbild begründen.

Beispiel: DNS-Fehler erkennen

Fehlerbild:

```
Webseite ist per IP erreichbar,
aber nicht per Namen.
```

Wahrscheinliche Ursache:

```
DNS-Problem
```

Prüfung:

```
DNS-Server prüfen
nslookup oder dig nutzen
DNS-Cache prüfen
richtigen DNS-Server konfigurieren
```

Merksatz:

```
IP ja,
Name nein:
DNS.
```

Beispiel: Gateway-Fehler erkennen

Fehlerbild:

```
Client erreicht lokale Systeme,
aber keine externen Netze.
```

Wahrscheinliche Ursache:

```
Standardgateway fehlt oder ist falsch.
```

Prüfung:

```
IP-Konfiguration prüfen
Gateway prüfen
Routing-Tabelle prüfen
```

Gateway anpingen

Merksatz:

Lokal ja,
extern nein:
Gateway prüfen.

Beispiel: Firewall-Fehler erkennen

Fehlerbild:

Server ist erreichbar,
aber bestimmter Dienst nicht.

Mögliche Ursache:

Port wird blockiert
Dienst läuft nicht
Firewall-Regel fehlt

Prüfung:

Dienststatus prüfen
Port prüfen
Firewall-Regeln prüfen
Logs prüfen

Merksatz:

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

Beispiel: Rechteproblem erkennen

Fehlerbild:

```
Benutzer kann sich anmelden,
aber Datei nicht öffnen.
```

Wahrscheinliche Ursache:

```
Autorisierungs- oder Berechtigungsproblem
```

Prüfung:

```
Gruppenmitgliedschaft
Freigaberechte
Dateisystemrechte
ACL
Deny-Regeln
```

Merksatz:

```
Anmeldung erfolgreich,
Zugriff verweigert:
Rechte prüfen.
```

Beispiel: Zertifikatsproblem erkennen

Fehlerbild:

```
Browser meldet Zertifikatswarnung.
```

Mögliche Ursachen:

```
Zertifikat abgelaufen
Hostname passt nicht
Zertifikatskette unvollständig
Systemzeit falsch
falsches Zertifikat installiert
```

Merksatz:

```
Zertifikatsfehler:
Ablauf,
Name,
Kette
und Zeit prüfen.
```

Checkliste: letzte Wiederholung vor der Prüfung

```
OSI-Schichten sicher können.
TCP/IP-Modell sicher können.
MAC,
IP
und Port unterscheiden.
Private IP-Bereiche kennen.
Subnetting üben.
Netzadresse und Broadcast berechnen.
Gateway,
DNS
und DHCP unterscheiden.
TCP und UDP vergleichen.
Standardports wiederholen.
NAT,
PAT
und Portweiterleitung unterscheiden.
Firewall-Regeln verstehen.
VLAN und Routing unterscheiden.
VPN-Arten wiederholen.
Cloud-Modelle unterscheiden.
Sicherheitsangriffe zuordnen.
Schutzmaßnahmen nennen können.
Backup,
Restore,
RPO
und RTO unterscheiden.
Rechte,
Rollen
```

und Gruppen verstehen.
Logging,
Monitoring
und Alerting unterscheiden.
Fehlersuche systematisch erklären.

Merksatz:

Wer sauber zuordnet,
löst viele Prüfungsaufgaben sicherer.

IHK-sichere Kurzformulierung

In der Prüfungsvorbereitung sollten Netzwerkthemen nicht isoliert, sondern im Zusammenhang wiederholt werden. Das OSI-Modell hilft bei der strukturierten Fehlersuche, während das TCP/IP-Modell die praktische Kommunikation beschreibt. MAC-Adressen arbeiten auf Schicht 2, IP-Adressen auf Schicht 3 und Ports auf Schicht 4. DNS löst Namen auf, DHCP verteilt Netzwerkkonfiguration und das Gateway verbindet einen Host mit anderen Netzen. TCP ist verbindungsorientiert und zuverlässig, UDP ist verbindungslos und schlank. Firewalls filtern Verkehr, NAT übersetzt Adressen, VPNs verschlüsseln Verbindungen und Backups ermöglichen Wiederherstellung. Bei Prüfungsaufgaben sollten Symptome genau gelesen, Signalwörter erkannt und Lösungen fachlich kurz begründet werden.

Wichtigste Merksätze

Prüfungsvorbereitung heißt Zusammenhänge verstehen.

Erst Aufgabe lesen,
dann Lösung ableiten.

OSI hilft bei Fehlersuche.

TCP/IP beschreibt praktische Kommunikation.

Kapselung verpackt Daten schichtweise.

MAC ist Schicht 2.

IP ist Schicht 3.

Port ist Schicht 4.

MAC lokal,
IP logisch,
Port Dienst.

IPv4 hat 32 Bit.

Präfix bestimmt Netz- und Hostanteil.

Pro Netzbit weniger halbiert sich die Hostanzahl.

Pro Hostbit mehr verdoppelt sich die Hostanzahl.

Netzadresse ist erste Adresse.

Broadcast ist letzte Adresse.

Gateway führt in andere Netze.

DNS löst Namen auf.

DHCP verteilt IP-Konfiguration.

ARP löst IPv4 zu MAC auf.

Switch lernt MAC-Adressen.

VLAN trennt logisch.

Routing verbindet Netze.

ICMP hilft bei Diagnose.

TCP ist zuverlässig.

UDP ist schnell und verbindungslos.

NAT übersetzt Adressen.

PAT nutzt Ports zur Zuordnung.

Firewall filtert Verkehr.

DMZ trennt öffentliche Dienste.

VPN verschlüsselt Verbindungen.

IaaS,
PaaS
und SaaS unterscheiden.

Public,
Private,
Hybrid
und Multi Cloud unterscheiden.

Vertraulichkeit,
Integrität
und Verfügbarkeit unterscheiden.

Angriff dem Schutzziel zuordnen.

Schutzmaßnahmen kombinieren.

Backup ohne Restore-Test ist unsicher.

RPO ist Datenverlust.

RTO ist Wiederherstellungszeit.

Bit und Byte unterscheiden.

IP funktioniert,
Name nicht:
DNS prüfen.

Lokal geht,
extern nicht:
Gateway prüfen.

Host geht,
Dienst nicht:
Port,
Dienst
und Firewall prüfen.

Anmeldung geht,
Zugriff nicht:
Rechte prüfen.

Zertifikatsfehler:
Ablauf,
Name,
Kette
und Zeit prüfen.

Signalwörter erkennen.

Prüfungsantwort kurz,
fachlich
und begründet formulieren.