20.14 Trainer – Gemischte Prüfungsaufgaben AP1/AP2 Netzwerktechnik

Diese Trainer-Seite ist eine gemischte Wiederholung über die wichtigsten Themen der Netzwerktechnik.

Sie verbindet:

- OSI-Modell
- TCP/IP
- IPv4 und Subnetting
- DNS und DHCP
- Switching und VLAN
- Routing und Gateway
- TCP, UDP und Ports
- Firewall, NAT und DMZ
- VPN und Cloud
- Sicherheit
- Backup und Fehlersuche

Ziel ist, prüfungsnah zu üben und Themen nicht isoliert, sondern im Zusammenhang zu erkennen.

Merksatz:

In der Prüfung steht selten nur ein Fachbegriff.
Meist musst du aus einem Fehlerbild das richtige Thema ableiten.

Lernziele

Nach dieser Seite solltest du sicher können:

- gemischte Netzwerkaufgaben einordnen
- Fehlerbilder fachlich erkennen
- passende Begriffe verwenden
- kurze IHK-sichere Antworten formulieren
- typische Prüfungsfallen vermeiden
- technische Ursache und passende Maßnahme verbinden

Aufgabe 1

Ein Client hat folgende Konfiguration:

```
IPv4-Adresse:
192.168.10.50

Subnetzmaske:
255.255.255.0

Gateway:
192.168.20.1
```

Der Client erreicht lokale Geräte, aber keine externen Netze.

Was ist falsch?

Antwort anzeigen

Das Gateway ist falsch.

Begründung:

```
Der Client liegt im Netz:

192.168.10.0/24

Das Gateway liegt im Netz:

192.168.20.0/24
```

Das Standardgateway muss im lokalen Subnetz des Clients liegen.

IHK-sichere Antwort:

```
Das Gateway befindet sich nicht im gleichen Subnetz wie der Client.
Dadurch kann der Client das Gateway lokal nicht erreichen
und keine Pakete in andere Netze senden.
```

Aufgabe 2

Ein Client hat die Adresse:

```
169.254.44.12
```

Was bedeutet das?

Antwort anzeigen

Das ist eine APIPA-Adresse.

Bedeutung:

```
Der Client hat wahrscheinlich keine gültige IP-Adresse per DHCP erhalten.
```

Mögliche Ursachen:

```
DHCP-Server nicht erreichbar

falsches VLAN

DHCP-Scope erschöpft

DHCP-Relay fehlt

Netzwerkverbindung fehlerhaft
```

Merksatz:

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

Aufgabe 3

Ein Benutzer kann eine interne Webseite per IP-Adresse öffnen, aber nicht über den Namen.

Welches Thema ist wahrscheinlich betroffen?

Antwort anzeigen

Wahrscheinlich betroffen:

```
DNS
```

Begründung:

```
Die IP-Kommunikation funktioniert.
Nur die Namensauflösung funktioniert nicht.
```

IHK-sichere Antwort:

```
Da der Zugriff per IP-Adresse funktioniert,
aber der Name nicht aufgelöst wird,
sollte die DNS-Konfiguration geprüft werden.
```

Aufgabe 4

Ein Server ist per ping erreichbar, aber HTTPS funktioniert nicht.

Nenne drei mögliche Ursachen.

Antwort anzeigen

Mögliche Ursachen:

```
TCP 443 wird durch eine Firewall blockiert

Webserver-Dienst läuft nicht

Dienst lauscht nicht auf TCP 443

TLS-Zertifikat fehlerhaft

Reverse Proxy falsch konfiguriert
```

Anwendung fehlerhaft

Merksatz:

ping prüft ICMP,
nicht HTTPS.

Aufgabe 5

Ein Switchport ist als Access-Port im falschen VLAN konfiguriert.

Welche Folge kann das haben?

Antwort anzeigen

Mögliche Folgen:

Client landet im falschen Netz

Client erhält falsche DHCP-Adresse

lokale Dienste sind nicht erreichbar

Gateway passt nicht

Sicherheitszonen werden umgangen

IHK-sichere Antwort:

Der Client wird logisch dem falschen Layer-2-Netz zugeordnet.
Dadurch kann er eine falsche IP-Konfiguration erhalten
oder nicht mit den vorgesehenen Systemen kommunizieren.

Aufgabe 6

Was ist der Unterschied zwischen VLAN und Subnetz?

Antwort anzeigen

VLAN:

```
logische Trennung auf OSI-Schicht 2
```

Subnetz:

```
logische IP-Aufteilung auf OSI-Schicht 3
```

Wichtig:

```
In der Praxis bekommt ein VLAN oft ein eigenes Subnetz.
Fachlich sind VLAN und Subnetz aber nicht dasselbe.
```

Merksatz:

```
VLAN = Layer 2.
Subnetz = Layer 3.
```

Aufgabe 7

Warum braucht Kommunikation zwischen VLANs Routing?

Antwort anzeigen

VLANs sind getrennte Layer-2-Bereiche.

Damit Geräte aus unterschiedlichen VLANs miteinander kommunizieren können, muss Verkehr zwischen den jeweiligen IP-Netzen geroutet werden.

Möglich über:

```
Router
```

Layer-3-Switch

Firewall

Merksatz:

VLANs trennen.
Routing verbindet gezielt.

Aufgabe 8

Ein Client möchte ein Ziel außerhalb seines Subnetzes erreichen.

Welche MAC-Adresse wird im Ethernet-Frame verwendet?

Antwort anzeigen

Verwendet wird:

die MAC-Adresse des Standardgateways

Begründung:

Das IP-Ziel bleibt der entfernte Zielhost.
Lokal wird das Frame aber an den nächsten Hop gesendet,
also an das Gateway.

Merksatz:

IP zeigt zum Endziel.
MAC zeigt zum nächsten lokalen Hop.

Aufgabe 9

Was macht ARP?

Antwort anzeigen

ARP löst im lokalen IPv4-Netz eine IP-Adresse in eine MAC-Adresse auf.

Beispiel:

```
Der Client kennt die IP-Adresse des Gateways,
braucht aber die MAC-Adresse,
um ein Ethernet-Frame senden zu können.
```

Merksatz:

```
ARP findet MAC-Adressen im lokalen IPv4-Netz.
```

Aufgabe 10

Bestimme für:

```
192.168.5.130/25
```

Wert	Ergebnis
Netzadresse	?
erste nutzbare Adresse	?
letzte nutzbare Adresse	?
Broadcastadresse	?
nutzbare Hosts	?

Antwort anzeigen

Bei /25 gilt:

```
Blockgröße 128
```

Bereiche:

192.168.5.0 bis 192.168.5.127

192.168.5.128 bis 192.168.5.255

192.168.5.130 liegt im zweiten Bereich.

Wert	Ergebnis
Netzadresse	192.168.5.128
erste nutzbare Adresse	192.168.5.129
letzte nutzbare Adresse	192.168.5.254
Broadcastadresse	192.168.5.255
nutzbare Hosts	126

Aufgabe 11

Bestimme für:

10.10.10.77/26

Wert	Ergebnis
Netzadresse	?
erste nutzbare Adresse	?
letzte nutzbare Adresse	?
Broadcastadresse	?

Antwort anzeigen

Bei /26 gilt:

Blockgröße 64

Bereiche:

```
0 bis 63

64 bis 127

128 bis 191

192 bis 255
```

77 liegt im Bereich 64 bis 127.

Wert	Ergebnis
Netzadresse	10.10.10.64
erste nutzbare Adresse	10.10.10.65
letzte nutzbare Adresse	10.10.10.126
Broadcastadresse	10.10.10.127

Aufgabe 12

Welche kleinste Netzgröße reicht für mindestens 60 Hosts?

Antwort anzeigen

Benötigt:

```
mindestens 60 nutzbare Hosts
```

Prüfung:

```
/27 = 30 nutzbare Hosts

/26 = 62 nutzbare Hosts
```

Antwort:

```
/26
```

Begründung:

```
/26 ist das kleinste der genannten passenden Netze,
weil es 62 nutzbare Hostadressen bietet.
```

Aufgabe 13

Welche kleinste Netzgröße reicht für mindestens 120 Hosts?

Antwort anzeigen

Prüfung:

```
/26 = 62 nutzbare Hosts

/25 = 126 nutzbare Hosts
```

Antwort:

```
/25
```

Merksatz:

```
Bedarf prüfen,
dann kleinstes passendes Netz wählen.
```

Aufgabe 14

Warum ist die Broadcastadresse nicht als Hostadresse nutzbar?

Antwort anzeigen

Die Broadcastadresse ist die letzte Adresse eines IPv4-Subnetzes.

Sie adressiert alle Hosts in diesem Subnetz und wird daher nicht einem einzelnen Host zugewiesen.

Merksatz:

```
Erste Adresse = Netz.
Letzte Adresse = Broadcast.
```

Aufgabe 15

Was ist der Unterschied zwischen TCP und UDP?

Antwort anzeigen

TCP:

```
verbindungsorientiert

zuverlässig

bestätigt Daten

stellt Reihenfolge sicher
```

UDP:

```
verbindungslos

schlank

schnell

keine eingebaute Zustellgarantie
```

Merksatz:

```
TCP = zuverlässig.
UDP = schnell und schlank.
```

Aufgabe 16

Ordne Ports zu.

Dienst	Protokoll und Port
SSH	?
HTTP	?
HTTPS	?
DNS	?
DHCP	?
SMB	?
RDP	?

Antwort anzeigen

Dienst	Protokoll und Port
SSH	TCP 22
HTTP	TCP 80
HTTPS	TCP 443
DNS	UDP/TCP 53
DHCP	UDP 67/68
SMB	TCP 445
RDP	TCP 3389

Merksatz:

> Portnummer immer mit TCP oder UDP lernen.

Aufgabe 17

Warum ist die Aussage „Port 53 freigeben“ ungenau?

Antwort anzeigen

Die Aussage ist ungenau, weil nicht klar ist, ob TCP 53, UDP 53 oder beides gemeint ist.

DNS nutzt meistens UDP 53, kann aber auch TCP 53 verwenden.

IHK-sichere Antwort:

```
Bei Firewall-Regeln müssen Port und Transportprotokoll angegeben werden,
da TCP und UDP getrennte Protokolle sind.
```

Aufgabe 18

Was bedeutet LISTEN bei TCP?

Antwort anzeigen

LISTEN bedeutet:

```
Ein Dienst wartet auf eingehende Verbindungen.
```

Beispiel:

```
Ein Webserver lauscht auf TCP 443.
```

Merksatz:

```
LISTEN = Dienst wartet.
```

Aufgabe 19

Was bedeutet ESTABLISHED bei TCP?

Antwort anzeigen

ESTABLISHED bedeutet:

```
Eine TCP-Verbindung besteht.
```

Merksatz:

```
ESTABLISHED = Verbindung aktiv.
```

Aufgabe 20

Was ist der Unterschied zwischen NAT und Firewall?

Antwort anzeigen

NAT:

```
übersetzt IP-Adressen
```

Firewall:

```
erlaubt oder blockiert Verkehr anhand von Regeln
```

Wichtig:

```
Viele Geräte kombinieren beide Funktionen.
Fachlich bleiben sie aber unterschiedlich.
```

Merksatz:

```
NAT übersetzt.
Firewall filtert.
```

Aufgabe 21

Was ist PAT?

Antwort anzeigen

PAT steht für:

```
Port Address Translation
```

PAT ist eine Form von NAT, bei der zusätzlich Ports genutzt werden, um mehrere interne Verbindungen über eine öffentliche IP-Adresse zu unterscheiden.

Merksatz:

```
PAT nutzt Ports zur Zuordnung mehrerer Verbindungen.
```

Aufgabe 22

Was ist Portweiterleitung?

Antwort anzeigen

Portweiterleitung bedeutet:

```
Eingehender Verkehr auf einem externen Port
wird an einen internen Dienst weitergeleitet.
```

Beispiel:

```
öffentliche IP TCP 443

zu

interner Webserver 192.168.10.20 TCP 443
```

Merksatz:

```
Portweiterleitung veröffentlicht einen internen Dienst.
```

Aufgabe 23

Warum ist eine Any-to-Any-Firewall-Regel kritisch?

Antwort anzeigen

Any-to-Any erlaubt Verkehr von jeder Quelle zu jedem Ziel.

Risiken:

```
große Angriffsfläche

schlechte Nachvollziehbarkeit

Sicherheitszonen werden umgangen

unnötige Freigaben
```

Besser:

```
genaue Regeln mit Quelle,
Ziel,
Port,
Protokoll
und Zweck.
```

Merksatz:

```
Je genauer die Regel,
desto sicherer und nachvollziehbarer.
```

Aufgabe 24

Was ist eine DMZ?

Antwort anzeigen

Eine DMZ ist ein getrenntes Netzwerk für Dienste, die von außen erreichbar sein müssen.

Beispiele:

```
Webserver

Reverse Proxy

Mail-Gateway

VPN-Gateway
```

Ziel:

```
öffentliche Dienste vom internen Netz trennen.
```

Merksatz:

```
DMZ begrenzt Schaden bei öffentlichen Diensten.
```

Aufgabe 25

Warum sollte eine Datenbank nicht direkt aus dem Internet erreichbar sein?

Antwort anzeigen

Eine Datenbank enthält oft sensible Daten und ist ein attraktives Angriffsziel.

Risiken:

```
Brute Force

Exploits

Datenabfluss

Manipulation
```

Besser:

Zugriff nur vom Anwendungsserver

Firewall-Beschränkung

privates Netz oder DMZ-Konzept

starke Authentifizierung

Monitoring

Merksatz:

Datenbankports gehören nicht offen ins Internet.

Aufgabe 26

Was ist der Unterschied zwischen Remote-Access-VPN und Site-to-Site-VPN?

Antwort anzeigen

Remote-Access-VPN:

einzelner Benutzer verbindet sich ins Firmennetz

Site-to-Site-VPN:

zwei Netze oder Standorte werden verbunden

Merksatz:

Remote Access = Benutzer.
Site-to-Site = Standort oder Netz.

Aufgabe 27

VPN ist verbunden, aber interne Namen funktionieren nicht.

Was ist wahrscheinlich?

Antwort anzeigen

Wahrscheinlich:

```
VPN-DNS-Problem
```

Prüfen:

```
interner DNS-Server

DNS-Suffix

Split-DNS

Erreichbarkeit des DNS-Servers

DNS-Cache
```

Merksatz:

```
VPN-IP ja,
VPN-Name nein:
VPN-DNS prüfen.
```

Aufgabe 28

VPN ist verbunden, aber interne IP-Ziele sind nicht erreichbar.

Was ist wahrscheinlich?

Antwort anzeigen

Mögliche Ursachen:

VPN-Route fehlt

Zielnetz nicht erlaubt

Firewall blockiert

Rückroute fehlt

IP-Adresskonflikt

Benutzergruppe hat keine Berechtigung

Merksatz:

VPN verbunden heißt nicht automatisch:
Routing und Regeln stimmen.

Aufgabe 29

Was bedeutet Shared Responsibility in der Cloud?

Antwort anzeigen

Shared Responsibility bedeutet:

Cloud-Anbieter und Kunde teilen sich die Verantwortung.

Anbieter:

schützt Infrastruktur,
Rechenzentrum
und Plattform je nach Modell.

Kunde:

bleibt verantwortlich für Daten,
Benutzer,
Rechte,
Konfigurationen
und Anwendungen je nach Modell.

Merksatz:

Anbieter schützt die Cloud.
Kunde schützt seine Nutzung der Cloud.

Aufgabe 30

Ordne Cloud-Modelle zu.

Modell	Bedeutung
IaaS	?
PaaS	?
SaaS	?

Antwort anzeigen

Modell	Bedeutung
IaaS	virtuelle Infrastruktur
PaaS	verwaltete Plattform
SaaS	fertige Anwendung

Merksatz:

IaaS = Infrastruktur.
PaaS = Plattform.
SaaS = Software.

Aufgabe 31

Was ist der Unterschied zwischen Hybrid Cloud und Multi Cloud?

Antwort anzeigen

Hybrid Cloud:

```
Kombination aus lokaler oder privater IT und Public Cloud
```

Multi Cloud:

```
Nutzung mehrerer Cloud-Anbieter
```

Merksatz:

```
Hybrid beschreibt Kombination von Umgebungen.
Multi beschreibt mehrere Anbieter.
```

Aufgabe 32

Warum ist IAM in der Cloud besonders wichtig?

Antwort anzeigen

Cloud-Ressourcen sind oft schnell erreichbar, skalierbar und über Netzwerke zugänglich.

Fehlerhafte Rechte können führen zu:

```
Datenabfluss

unberechtigtem Zugriff

Manipulation

Kostenexplosion

Löschung von Ressourcen
```

Merksatz:

> In der Cloud sind Identitäten oft der wichtigste Sicherheitsperimeter.

Aufgabe 33

Ordne Schutzziele zu.

Ereignis	Schutzziel
Daten werden gelesen	?
Datei wird manipuliert	?
Dienst fällt aus	?
Absender wird gefälscht	?

Antwort anzeigen

Ereignis	Schutzziel
Daten werden gelesen	Vertraulichkeit
Datei wird manipuliert	Integrität
Dienst fällt aus	Verfügbarkeit
Absender wird gefälscht	Authentizität

Merksatz:

> Lesen = Vertraulichkeit.
> Verändern = Integrität.
> Ausfall = Verfügbarkeit.
> Echtheit = Authentizität.

Aufgabe 34

Was ist der Unterschied zwischen Brute Force, Password Spraying und Credential Stuffing?

Antwort anzeigen

Brute Force:

> viele Passwortversuche

Password Spraying:

> ein häufiges Passwort gegen viele Konten

Credential Stuffing:

> geleakte Zugangsdaten werden bei anderen Diensten getestet

Merksatz:

> Brute Force = viele Versuche.
> Spraying = ein Passwort gegen viele Konten.
> Stuffing = geleakte Zugangsdaten.

Aufgabe 35

Ordne Webangriffe zu.

Angriff	Beschreibung
SQL Injection	?
XSS	?
CSRF	?

Antwort anzeigen

Angriff	Beschreibung
SQL Injection	SQL-Code in Eingaben einschleusen
XSS	Skriptcode im Browser anderer Benutzer ausführen
CSRF	gültige Sitzung für ungewollte Aktion missbrauchen

Merksatz:

SQLi betrifft Datenbankabfragen.

XSS betrifft Browser.

CSRF betrifft Sitzungen.

Aufgabe 36

Welche Maßnahme passt zu welchem Risiko?

Risiko	Maßnahme
gestohlenes Passwort	?
ungepatchter Server	?
zu viele Rechte	?
unnötige Dienste	?
Ransomware	?

Antwort anzeigen

Risiko	Maßnahme
gestohlenes Passwort	MFA
ungepatchter Server	Patchmanagement
zu viele Rechte	Least Privilege
unnötige Dienste	Hardening
Ransomware	Offline- oder Immutable-Backups und Restore-Test

Merksatz:

Maßnahme muss zum Risiko passen.

Aufgabe 37

Was ist der Unterschied zwischen IDS und IPS?

Antwort anzeigen

IDS:

erkennt und meldet Angriffe

IPS:

erkennt und blockiert Angriffe zusätzlich

Merksatz:

IDS meldet.
IPS blockiert.

Aufgabe 38

Was ist der Unterschied zwischen Backup, Replikation und Synchronisation?

Antwort anzeigen

Backup:

sichert Daten zur Wiederherstellung alter Zustände

Replikation:

erzeugt eine möglichst aktuelle Kopie auf anderem System

Synchronisation:

gleicht Daten zwischen Speicherorten ab

Wichtig:

Replikation und Synchronisation ersetzen kein Backup,
weil Fehler,

Löschungen
oder Ransomware mit übertragen werden können.

Merksatz:

Backup stellt wieder her.
Replikation hält aktuell.
Synchronisation gleicht ab.

Aufgabe 39

Was bedeuten RPO und RTO?

Antwort anzeigen

RPO:

Recovery Point Objective

maximal akzeptabler Datenverlust

RTO:

Recovery Time Objective

maximal akzeptable Wiederherstellungszeit

Merksatz:

RPO = Datenverlust.
RTO = Zeit bis Wiederherstellung.

Aufgabe 40

Warum ist ein Restore-Test wichtig?

Antwort anzeigen

Ein Restore-Test prüft, ob Backups wirklich wiederherstellbar sind.

Ohne Restore-Test ist unklar:

```
ob Daten vollständig sind

ob Daten lesbar sind

ob Schlüssel vorhanden sind

ob Rechte stimmen

ob die Wiederherstellungszeit passt
```

Merksatz:

```
Backup ohne Restore-Test ist unsicher.
```

Aufgabe 41

Welche Antwort ist besser?

Aufgabe:

```
Ein Benutzer kann sich anmelden,
aber nicht auf eine Datei zugreifen.
Was ist wahrscheinlich?
```

Antwort A:

```
Das Netzwerk ist kaputt.
```

Antwort B:

Wahrscheinlich liegt ein Berechtigungsproblem vor,
da die Authentifizierung funktioniert,
der Zugriff auf die Ressource aber verweigert wird.

Antwort anzeigen

B ist besser.

Begründung:

Die Antwort trennt Authentifizierung und Autorisierung.

Merksatz:

Login ja,
Zugriff nein:
Rechte prüfen.

Aufgabe 42

Welche Antwort ist besser?

Aufgabe:

Warum ist MFA sinnvoll?

Antwort A:

Weil es sicherer ist.

Antwort B:

MFA verlangt zusätzlich zum Passwort einen weiteren Faktor.
Dadurch reicht ein gestohlenes Passwort allein nicht aus,
um Zugriff zu erhalten.

Antwort anzeigen

B ist besser.

Begründung:

Die Antwort erklärt die konkrete Schutzwirkung.

Merksatz:

Maßnahme mit Wirkung erklären.

Aufgabe 43

Welche Antwort ist besser?

Aufgabe:

Warum ersetzt ein Snapshot kein Backup?

Antwort A:

Weil Snapshot und Backup verschiedene Wörter sind.

Antwort B:

Snapshots liegen oft auf demselben System oder Speicher.
Bei Speicherdefekt,
Löschung
oder Ransomware können sie ebenfalls betroffen sein.
Ein Backup muss getrennt,
geschützt
und wiederherstellbar sein.

Antwort anzeigen

B ist besser.

Begründung:

Die Antwort nennt die fachliche Ursache
und Anforderungen an ein Backup.

Merksatz:

Fachbegriff plus Begründung.

Aufgabe 44

Welche Antwort ist besser?

Aufgabe:

Warum ist eine öffentlich erreichbare Datenbank kritisch?

Antwort A:

Weil Datenbanken wichtig sind.

Antwort B:

Eine öffentlich erreichbare Datenbank erhöht die Angriffsfläche.
Es drohen Brute-Force-Angriffe,
Ausnutzung von Schwachstellen,
Datenabfluss
und Manipulation.
Besser ist Zugriff nur aus benötigten Netzen oder vom Anwendungsserver.

Antwort anzeigen

B ist besser.

Begründung:

Die Antwort nennt Risiko,
Folgen
und bessere Maßnahme.

Merksatz:

Sicherheitsantwort:
Risiko,
Maßnahme,
Wirkung.

Aufgabe 45

Welche Antwort ist besser?

Aufgabe:

Warum ist systematische Fehlersuche wichtig?

Antwort A:

Weil man dann professionell wirkt.

Antwort B:

Systematische Fehlersuche grenzt den Fehler anhand von Symptomen,
Schichten
und Messwerten ein.
Dadurch werden Ursachen schneller gefunden
und unnötige Änderungen vermieden.

Antwort anzeigen

B ist besser.

Begründung:

> Die Antwort erklärt den Nutzen der systematischen Vorgehensweise.

Merksatz:

> Nicht raten,
> sondern eingrenzen.

Mini-Prüfung: Gesamtzuordnung

Fehlerbild oder Begriff	Thema
keine Link-LED	Schicht 1
MAC-Adresse	Schicht 2
IP-Adresse	Schicht 3
TCP-Port	Schicht 4
TLS-Zertifikat	Schicht 6
HTTP	Schicht 7
169.254.x.x	DHCP
IP ja, Name nein	DNS
ping ja, HTTPS nein	Port, Dienst, Firewall, TLS
falsches Netz nach DHCP	VLAN oder DHCP
RDP aus Internet offen	Sicherheitsrisiko
Datenbank öffentlich erreichbar	Sicherheitsrisiko
Backup nicht wiederherstellbar	Restore-Test fehlt
Dienst nach Update defekt	Change, Logs, Rollback
VPN verbunden, Name geht nicht	VPN-DNS

Mini-Prüfung: Begriffe kurz erklären

Begriff	Kurzantwort
VLAN	logische Trennung auf Schicht 2
Subnetz	logische IP-Aufteilung auf Schicht 3
Gateway	Router in andere Netze
DNS	Namensauflösung

Begriff	Kurzantwort
DHCP	automatische IP-Konfiguration
NAT	Adressübersetzung
PAT	Adress- und Portübersetzung
DMZ	getrennte Zone für öffentliche Dienste
VPN	verschlüsselter Tunnel
IAM	Identitäts- und Rechteverwaltung
MFA	Anmeldung mit mehreren Faktoren
Least Privilege	nur nötige Rechte vergeben
Hardening	Angriffsfläche reduzieren
RPO	maximaler Datenverlust
RTO	maximale Wiederherstellungszeit

Mini-Prüfung: typische Prüfungsfallen

Falle	Richtig denken
ping geht, also Dienst geht	falsch, ping prüft nur ICMP
VLAN ist dasselbe wie Subnetz	falsch, VLAN Layer 2, Subnetz Layer 3
NAT ist Firewall	falsch, NAT übersetzt, Firewall filtert
Cloud-Anbieter ist für alles verantwortlich	falsch, Shared Responsibility
Snapshot ist Backup	falsch, Snapshot ersetzt kein Backup
Sync ist Backup	falsch, Sync gleicht nur ab
Portnummer ohne TCP/UDP reicht	ungenau
Loginproblem und Rechteproblem sind gleich	falsch, Authentifizierung und Autorisierung unterscheiden
Any-to-Any ist praktisch	kritisch, zu breite Freigabe
Mehr Rechte lösen Probleme	unsicher, Least Privilege beachten

IHK-sichere Kurzformulierung

Bei gemischten Netzwerkaufgaben ist entscheidend, das Fehlerbild systematisch einzuordnen. Keine Link-Anzeige deutet auf Schicht 1 hin, MAC-Adressen und VLANs auf Schicht 2, IP-Adressen und Routing auf Schicht 3, TCP, UDP und Ports auf Schicht 4. DNS-Probleme zeigen sich häufig dadurch, dass eine IP-Adresse erreichbar ist, ein Name aber nicht. DHCP-Probleme erkennt man oft an APIPA-Adressen aus 169.254.0.0/16. Firewall-Regeln müssen Quelle, Ziel, Port, Protokoll und Zweck enthalten. NAT übersetzt Adressen, während Firewalls Verkehr filtern. VPN-Verbindungen benötigen neben dem Tunnel auch passende Routen, DNS und Berechtigungen.

Sicherheitsantworten sollten Risiko, Maßnahme und Wirkung enthalten. Backup-Fragen müssen Restore, RPO, RTO und Restore-Tests berücksichtigen.

Merksätze

Erst Fehlerbild lesen,
dann Thema zuordnen.

Kein Link:
Schicht 1.

MAC:
Schicht 2.

IP:
Schicht 3.

TCP und UDP:
Schicht 4.

TLS:
Schicht 6.

HTTP und DNS:
Schicht 7.

VLAN ist Layer 2.

Subnetz ist Layer 3.

Switch arbeitet mit MAC-Adressen.

Router arbeitet mit IP-Adressen.

Gateway führt in andere Netze.

DNS löst Namen auf.

DHCP verteilt IP-Konfiguration.

169.254.x.x:
DHCP nicht erreicht.

ping ist kein Diensttest.

IP ja,
Name nein:
DNS.

Lokal ja,
extern nein:
Gateway,
Routing,
NAT
oder Firewall.

ping ja,
Port nein:
Dienst,
Port
oder Firewall.

NAT übersetzt.

Firewall filtert.

PAT nutzt Ports.

DMZ trennt öffentliche Dienste.

VPN braucht Tunnel,
Route,
DNS
und Rechte.

Cloud bedeutet geteilte Verantwortung.

IAM entscheidet,
wer was darf.

MFA schützt gegen Passwortmissbrauch.

Least Privilege begrenzt Schaden.

Patchmanagement schließt bekannte Lücken.

Hardening reduziert Angriffsfläche.

Backup ist Wiederherstellungsvorsorge.

Restore-Test beweist,
dass Backup nutzbar ist.

RPO = Datenverlust.

RTO = Wiederherstellungszeit.

Gute Prüfungsantwort:
Ursache,
Begründung,
passende Prüfung
oder Maßnahme.

Nicht raten,
sondern fachlich eingrenzen.