20.15 Trainer – Abschlussprüfung Netzwerktechnik Gesamtwiederholung

Diese Seite ist die Abschlussseite des Netzwerktechnik-Trainers.

Sie dient als letzte Gesamtwiederholung vor einer Klassenarbeit, AP1, AP2 oder vor dem Eintragen eigener Lernnotizen.

Ziel ist, alle Kernbereiche noch einmal kompakt, prüfungsnah und mit typischen Antwortmustern zu wiederholen.

Merksatz:

> Am Ende zählt nicht,
> ob man Begriffe kennt,
> sondern ob man sie im Fehlerbild richtig anwendet.

Lernziele

Nach dieser Abschlussseite solltest du sicher können:

- Netzwerkprobleme nach OSI-Schichten einordnen
- Standardbegriffe kurz erklären
- typische Fehlerbilder erkennen
- passende Prüfungen nennen
- Sicherheitsrisiken bewerten
- technische Maßnahmen begründen
- kurze prüfungssichere Antworten formulieren

Abschluss-Checkliste: OSI-Modell

Schicht	Name	Kernthema	Typische Begriffe
7	Anwendung	Netzwerkdienste	HTTP, DNS, DHCP, SMTP, SMB
6	Darstellung	Format und Verschlüsselung	TLS, Zertifikate, Codierung
5	Sitzung	Sitzungen	Session, Cookie, Token, Timeout

Schicht	Name	Kernthema	Typische Begriffe
4	Transport	Ports und Transport	TCP, UDP, Port
3	Vermittlung	IP und Routing	IP, Subnetz, Gateway, ICMP
2	Sicherung	lokale Zustellung	MAC, Ethernet, VLAN, Switch
1	Bitübertragung	physische Übertragung	Kabel, Funk, Link, Signal

Merksatz:

1 Kabel.
2 MAC.
3 IP.
4 Port.
5 Sitzung.
6 TLS.
7 Anwendung.

Abschluss-Checkliste: Fehlerbilder

Fehlerbild	Wahrscheinlichstes Thema
keine Link-LED	Kabel, Port, Schicht 1
falsches Netz	VLAN oder DHCP
169.254.x.x	DHCP nicht erreicht
lokal erreichbar, extern nicht	Gateway, Routing, NAT, Firewall
IP erreichbar, Name nicht	DNS
ping funktioniert, Dienst nicht	Port, Dienst oder Firewall
HTTPS-Warnung	TLS-Zertifikat
HTTP 401	Authentifizierung
HTTP 403	Autorisierung
HTTP 404	Ressource nicht gefunden
HTTP 500	Server oder Anwendung
HTTP 502	Proxy, Gateway oder Backend
VPN verbunden, Name geht nicht	VPN-DNS
Login geht, Datei nicht	Rechteproblem
Backup vorhanden, Restore geht nicht	Restore-Test oder Backup defekt

Abschluss-Checkliste: Standardports

Dienst	Protokoll und Port
FTP	TCP 21
SSH	TCP 22
SFTP	TCP 22
SMTP	TCP 25
DNS	UDP/TCP 53
DHCP Server	UDP 67
DHCP Client	UDP 68
HTTP	TCP 80
POP3	TCP 110
NTP	UDP 123
IMAP	TCP 143
SNMP	UDP 161
HTTPS	TCP 443
SMB	TCP 445
SMTPS	TCP 465
IMAPS	TCP 993
POP3S	TCP 995
RDP	TCP 3389

Merksatz:

> Portnummer immer mit TCP oder UDP lernen.

Abschluss-Checkliste: IPv4 und Subnetting

Präfix	Subnetzmaske	nutzbare Hosts
/24	255.255.255.0	254
/25	255.255.255.128	126
/26	255.255.255.192	62
/27	255.255.255.224	30
/28	255.255.255.240	14

Präfix	Subnetzmaske	nutzbare Hosts
/29	255.255.255.248	6
/30	255.255.255.252	2

Merksätze:

Hostbits = 32 minus Präfix.

Nutzbare Hosts = 2 hoch Hostbits minus 2.

Netzadresse = erste Adresse.

Broadcastadresse = letzte Adresse.

Erste und letzte Adresse sind im normalen IPv4-Subnetz nicht für Hosts.

Abschluss-Checkliste: 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 IPv4-Adressen werden im Internet nicht direkt geroutet.

Abschluss-Checkliste: Begriffe kurz erklären

Begriff	Kurzantwort
MAC-Adresse	lokale Adresse einer Netzwerkschnittstelle
IP-Adresse	logische Adresse eines Hosts
Port	Dienst- oder Prozesszuordnung
Gateway	Router in andere Netze
DNS	löst Namen in IP-Adressen auf
DHCP	verteilt IP-Konfiguration automatisch

Begriff	Kurzantwort
ARP	löst IPv4-Adresse in MAC-Adresse auf
VLAN	logische Trennung auf Schicht 2
Subnetz	logische IP-Aufteilung auf Schicht 3
NAT	übersetzt IP-Adressen
PAT	übersetzt IP-Adressen und Ports
DMZ	getrennte Zone für öffentliche Dienste
VPN	verschlüsselter Tunnel über unsicheres Netz
IAM	Identitäts- und Rechteverwaltung
MFA	Authentifizierung mit mehreren Faktoren
Backup	Sicherung
Restore	Wiederherstellung

Abschluss-Checkliste: Sicherheit

Risiko	passende Maßnahme
gestohlenes Passwort	MFA
zu viele Rechte	Least Privilege
bekannte Sicherheitslücke	Patchmanagement
unnötige Dienste	Hardening
Ransomware	Offline- oder Immutable-Backup
Phishing	Awareness, Mailfilter, MFA
SQL Injection	Prepared Statements
XSS	Output Encoding, CSP, HttpOnly
CSRF	CSRF-Token, SameSite-Cookies
Man-in-the-Middle	TLS, Zertifikatsprüfung, VPN
DDoS	DDoS-Schutz, Rate Limiting, CDN
unklare Vorfälle	Logging, SIEM, Monitoring

Merksatz:

```
Risiko,
Maßnahme,
Wirkung.
```

Abschluss-Checkliste: Backup

Begriff	Bedeutung
Backup	Sicherung
Restore	Wiederherstellung
RPO	maximal akzeptabler Datenverlust
RTO	maximal akzeptable Wiederherstellungszeit
Retention	Aufbewahrungsregel
Vollbackup	sichert alle ausgewählten Daten
inkrementelles Backup	Änderungen seit letztem Backup
differenzielles Backup	Änderungen seit letztem Vollbackup
Snapshot	Momentaufnahme
Offline-Backup	nicht dauerhaft verbunden
Immutable Backup	unveränderliches Backup
Restore-Test	Prüfung der Wiederherstellung

Merksatz:

> Backup ohne Restore-Test ist unsicher.

Prüfungssimulation 1

Ein Client meldet:

> „Ich komme nicht ins Internet.“

Du stellst fest:

> - IP-Adresse ist 192.168.10.55/24
> - Gateway ist 192.168.10.1
> - Ping auf 192.168.10.1 funktioniert
> - Ping auf 8.8.8.8 funktioniert
> - Aufruf von Webseiten per Domain funktioniert nicht

Was ist wahrscheinlich?

Antwort anzeigen

Wahrscheinlich:

```
DNS-Problem
```

Begründung:

```
Gateway und externe IP-Adresse sind erreichbar.
Der Weg ins Internet funktioniert also grundsätzlich.
Wenn nur Domains nicht funktionieren,
ist die Namensauflösung wahrscheinlich gestört.
```

IHK-sichere Antwort:

```
Da externe IP-Adressen erreichbar sind,
aber Domainnamen nicht funktionieren,
sollte die DNS-Konfiguration geprüft werden,
insbesondere DNS-Server,
DNS-Erreichbarkeit
und DNS-Cache.
```

Prüfungssimulation 2

Ein Client meldet:

```
„Ich bekomme keine Netzwerkverbindung.“
```

Du stellst fest:

```
- keine Link-LED
- keine IP-Adresse
- andere Clients am Switch funktionieren
```

Was prüfst du zuerst?

Antwort anzeigen

Zuerst prüfen:

```
Schicht 1
```

Konkret:

```
Kabel

Stecker

Netzwerkdose

Switchport

Netzwerkkarte

anderes Patchkabel

anderen Port
```

Begründung:

```
Keine Link-LED deutet zuerst auf ein physisches Problem hin.
```

IHK-sichere Antwort:

```
Zuerst wird die physische Verbindung geprüft,
weil ohne Link keine höhere Netzwerkschicht zuverlässig funktionieren kann.
```

Prüfungssimulation 3

Ein Benutzer kann sich anmelden, aber nicht auf eine Freigabe zugreifen.

Was ist wahrscheinlich?

Antwort anzeigen

Wahrscheinlich:

```
Autorisierungs- oder Berechtigungsproblem
```

Begründung:

```
Die Authentifizierung funktioniert,
weil die Anmeldung erfolgreich ist.
Der Zugriff auf die Ressource wird aber verweigert.
```

Prüfen:

```
Gruppenmitgliedschaft

Freigaberechte

Dateisystemrechte

ACLs

Rollen
```

Merksatz:

```
Login ja,
Zugriff nein:
Rechte prüfen.
```

Prüfungssimulation 4

Ein Webserver ist per ping erreichbar, aber die Webseite öffnet nicht.

Was ist wichtig?

Antwort anzeigen

Wichtig:

> ping prüft nur ICMP.

Zu prüfen:

> TCP 80 oder TCP 443 erreichbar?
>
> Webserver-Dienst läuft?
>
> Dienst lauscht auf richtigem Port?
>
> Firewall blockiert?
>
> TLS-Zertifikat korrekt?
>
> Reverse Proxy oder Anwendung fehlerhaft?

IHK-sichere Antwort:

> Die ICMP-Erreichbarkeit zeigt nur,
> dass der Host erreichbar ist.
> Für die Webseite müssen zusätzlich Port,
> Dienst,
> Firewall
> und Anwendung geprüft werden.

Prüfungssimulation 5

Ein Server steht in der DMZ. Er soll aus dem Internet per HTTPS erreichbar sein und auf eine interne Datenbank zugreifen.

Welche Regeln sind sinnvoll?

Antwort anzeigen

Sinnvolle Regeln:

Quelle	Ziel	Protokoll	Port	Aktion	Zweck
Internet	Webserver-DMZ	TCP	443	erlauben	HTTPS-Zugriff
Webserver-DMZ	interne Datenbank	TCP	Datenbankport	erlauben	Anwendung benötigt Datenbank
Internet	interne Datenbank	TCP	Datenbankport	blockieren	Datenbank schützen
DMZ	internes Netz	any	any	blockieren, außer benötigte Regeln	Schutz des internen Netzes

IHK-sichere Antwort:

> Nur der benötigte HTTPS-Zugriff auf den Webserver wird aus dem Internet erlaubt.
>
> Der Zugriff vom Webserver zur internen Datenbank wird gezielt auf den notwendigen Port beschränkt.
>
> Direkter Zugriff aus dem Internet auf die Datenbank wird blockiert.

Prüfungssimulation 6

Ein VPN verbindet sich erfolgreich, aber interne Server sind nur per IP-Adresse erreichbar, nicht per Namen.

Was ist wahrscheinlich?

Antwort anzeigen

Wahrscheinlich:

> VPN-DNS-Problem

Prüfen:

> interner DNS-Server wird per VPN gesetzt?
>
> DNS-Server ist über VPN erreichbar?

DNS-Suffix ist korrekt?

Split-DNS funktioniert?

DNS-Cache veraltet?

IHK-sichere Antwort:

Da interne IP-Adressen erreichbar sind,
aber Namen nicht aufgelöst werden,
sollte die DNS-Konfiguration des VPN geprüft werden.

Prüfungssimulation 7

Ein Unternehmen nutzt Cloud-Speicher. Ein Benutzer teilt versehentlich einen Ordner öffentlich.

Welches Thema ist betroffen?

Antwort anzeigen

Betroffen:

Vertraulichkeit

Ursache:

falsche Freigabe oder zu breite Berechtigung

Maßnahmen:

Berechtigungen einschränken

Freigaben regelmäßig prüfen

Least Privilege

MFA

DLP

Audit-Logs

Sensibilisierung

IHK-sichere Antwort:

Durch die öffentliche Freigabe können unberechtigte Personen Daten lesen.
Damit ist die Vertraulichkeit betroffen.
Die Freigabe sollte entfernt,
die Berechtigungen geprüft
und die Zugriffe protokolliert ausgewertet werden.

Prüfungssimulation 8

Ein Server wurde durch Ransomware verschlüsselt. Die Backups liegen dauerhaft erreichbar auf einer Netzfreigabe und wurden ebenfalls verschlüsselt.

Was war das Problem?

Antwort anzeigen

Problem:

Backups waren dauerhaft online und beschreibbar erreichbar.

Dadurch konnte Ransomware auch die Backups verschlüsseln.

Bessere Maßnahmen:

Offline-Backup

Immutable Backup

getrennte Backup-Rechte

MFA für Backup-Administration

Restore-Tests

Monitoring

IHK-sichere Antwort:

Backups müssen gegen Manipulation und Verschlüsselung geschützt werden.
Offline- oder Immutable-Backups verhindern,
dass Ransomware alle Sicherungen gleichzeitig zerstört.

Prüfungssimulation 9

Ein Administrator soll erklären, warum ein Snapshot kein vollständiges Backup ersetzt.

Formuliere eine gute Antwort.

Antwort anzeigen

Gute Antwort:

Ein Snapshot ist eine Momentaufnahme,
liegt aber häufig auf demselben System oder Speicher wie die Produktivdaten.
Bei Speicherdefekt,
Löschung,
Ransomware
oder beschädigter Snapshot-Kette kann er ebenfalls betroffen sein.
Ein Backup muss getrennt,
geschützt
wiederherstellbar
und regelmäßig getestet sein.

Merksatz:

Snapshot ist hilfreich,
aber kein vollständiges Backup-Konzept.

Prüfungssimulation 10

Ein Cloud-Anbieter stellt eine SaaS-Anwendung bereit. Ein Kunde vergibt allen Benutzern Adminrechte.

Wer ist für dieses Problem verantwortlich?

Antwort anzeigen

Verantwortlich ist typischerweise:

der Kunde

Begründung:

Bei SaaS betreibt der Anbieter die Anwendung.
Der Kunde bleibt aber für Benutzer,
Rollen,
Daten,
Berechtigungen
und Konfigurationen verantwortlich.

IHK-sichere Antwort:

Nach dem Shared-Responsibility-Modell ist der Kunde für die korrekte Rechtevergabe verantwortlich.
Der Anbieter stellt die SaaS-Anwendung bereit,
aber Benutzer- und Berechtigungsverwaltung bleiben Aufgabe des Kunden.

Prüfungssimulation 11

Ein Dienstleister benötigt Zugriff auf einen Server. Er bekommt VPN-Zugriff auf das gesamte interne Netz.

Bewerte das.

Antwort anzeigen

Bewertung:

Das ist kritisch.

Grund:

Der Dienstleister erhält mehr Zugriff als notwendig.

Besser:

Least Privilege

Zugriff nur auf benötigten Server

nur benötigte Ports

zeitlich begrenzter Zugriff

MFA

Logging

separate Rolle oder Gruppe

IHK-sichere Antwort:

Der Zugriff sollte nach dem Least-Privilege-Prinzip eingeschränkt werden.
Ein Dienstleister sollte nur auf die Systeme und Dienste zugreifen können,
die er für seine Aufgabe benötigt.
Dadurch wird das Risiko bei Missbrauch oder kompromittierten Zugangsdaten reduziert.

Prüfungssimulation 12

Ein Unternehmen öffnet RDP direkt ins Internet, damit Administratoren leichter zugreifen können.

Bewerte das.

Antwort anzeigen

Bewertung:

Das ist ein hohes Sicherheitsrisiko.

Risiken:

Brute Force

Credential Stuffing

Exploits

unberechtigter Fernzugriff

Besser:

VPN

RDP-Gateway

MFA

Firewall-Beschränkung auf bekannte Quellnetze

Logging

IHK-sichere Antwort:

RDP sollte nicht direkt aus dem Internet erreichbar sein.
Sicherer ist ein Zugriff über VPN oder RDP-Gateway mit MFA,
Zugriffsbeschränkung und Protokollierung.

Abschluss: typische IHK-Antwortmuster

Fehlersuche

```
Wahrscheinlich liegt ein Problem bei [Thema] vor,
weil [Symptom] funktioniert,
aber [Symptom] nicht funktioniert.
Daher sollte [konkrete Prüfung] geprüft werden.
```

Beispiel:

```
Wahrscheinlich liegt ein DNS-Problem vor,
weil die IP-Adresse erreichbar ist,
der Name aber nicht aufgelöst wird.
Daher sollten DNS-Server,
DNS-Eintrag
und DNS-Cache geprüft werden.
```

Sicherheitsbewertung

```
Das ist kritisch,
weil [Risiko].
Eine geeignete Maßnahme ist [Maßnahme],
weil dadurch [Wirkung] erreicht wird.
```

Beispiel:

```
Eine öffentlich erreichbare Datenbank ist kritisch,
weil sie direkt aus dem Internet angegriffen werden kann.
Besser ist,
den Zugriff nur aus dem Anwendungsserver-Netz zu erlauben
und die Datenbank in einem privaten Netz zu betreiben.
```

Vergleich

```
[Begriff A] bedeutet [Erklärung].
[Begriff B] bedeutet [Erklärung].
```

Der wesentliche Unterschied ist [Unterschied].

Beispiel:

NAT übersetzt IP-Adressen.
Eine Firewall erlaubt oder blockiert Verkehr anhand von Regeln.
Der wesentliche Unterschied ist,
dass NAT Adressen übersetzt,
während die Firewall Verkehr filtert.

Backup-Frage

RPO beschreibt den maximal akzeptablen Datenverlust.
RTO beschreibt die maximal akzeptable Wiederherstellungszeit.
Die Backup-Frequenz muss zum RPO passen,
der Restore-Prozess zum RTO.
Zusätzlich müssen Restore-Tests durchgeführt werden.

Cloud-Frage

Beim Shared-Responsibility-Modell teilen sich Anbieter und Kunde die Verantwortung.
Der Anbieter schützt die Cloud-Infrastruktur.
Der Kunde bleibt je nach Modell für Daten,
Benutzer,
Rechte,
Konfigurationen
und Anwendungen verantwortlich.

Letzte Wiederholung: 30 Sekunden

OSI 1:
Kabel,
Link,
Signal.

OSI 2:

MAC,
Switch,
VLAN.

OSI 3:
IP,
Gateway,
Routing.

OSI 4:
TCP,
UDP,
Ports.

OSI 5:
Session,
Cookie,
Token.

OSI 6:
TLS,
Zertifikat,
Verschlüsselung.

OSI 7:
HTTP,
DNS,
DHCP,
SMB.

DNS:
Name zu IP.

DHCP:
IP-Konfiguration automatisch.

ARP:
IPv4 zu MAC.

NAT:
Adresse übersetzen.

Firewall:
Verkehr filtern.

VPN:
verschlüsselter Tunnel.

Backup:
Sicherung.

Restore:
Wiederherstellung.

RPO:
Datenverlust.

RTO:
Wiederherstellungszeit.

MFA:
Passwort allein reicht nicht.

Least Privilege:
nur nötige Rechte.

Hardening:
Angriffsfläche reduzieren.

Patchmanagement:
bekannte Lücken schließen.

Abschluss-Merksätze

Fehlerbild zuerst lesen.

Nicht raten,

sondern eingrenzen.

IP ja,
Name nein:
DNS.

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

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

Login ja,
Zugriff nein:
Rechte.

Anmeldung scheitert:
Authentifizierung.

169.254.x.x:
DHCP nicht erreicht.

VLAN ist Layer 2.

Subnetz ist Layer 3.

NAT ist nicht Firewall.

Snapshot ist nicht Backup.

Sync ist nicht Backup.

```
Cloud ist geteilte Verantwortung.

Portnummer ohne TCP oder UDP ist unvollständig.

Sicherheitsantworten brauchen Risiko,
Maßnahme
und Wirkung.

Gute Prüfungsantworten sind kurz,
fachlich
und begründet.
```

Stand dieses Trainers

Mit dieser Seite ist der gemischte Netzwerktechnik-Trainer inhaltlich abgeschlossen.

Weitere sinnvolle Ergänzungen wären nur noch separate Spezialtrainer, zum Beispiel:

```
- reiner Subnetting-Rechentrainer
- reiner Ports-Trainer
- reiner Firewall-Regel-Trainer
- reiner Fehlersuche-Trainer mit Fällen
- reiner Sicherheitsmaßnahmen-Trainer
- AP1-Simulation mit Zeitdruck
- AP2-Simulation mit komplexem Szenario
```

Diese wären eigene zusätzliche Trainerseiten und keine notwendige Fortsetzung dieses Kapitels.
