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.