17.9 Merksätze und Prüfungswissen zu Netzwerkadministration und Systemzugriff

Diese Seite fasst die wichtigsten Inhalte aus dem Kapitel Praxis, Netzwerkadministration und Systemzugriff zusammen.

In diesem Kapitel ging es um praktische Aufgaben der Systemintegration:

- sichere Fernadministration
- SSH und RDP
- Benutzer und Rechte
- Gruppen und Rollen
- Logging und Monitoring
- Dienstprüfung
- Netzwerkbefehle
- Dateiübertragung und Freigaben
- Backup und Restore
- Dokumentation
- Change Management

Merksatz:

Netzwerkadministration verbindet Technik,
Sicherheit,
Betrieb
und Dokumentation.

Grundidee der Netzwerkadministration

Netzwerkadministration bedeutet:

Systeme,
Netzwerke,
Dienste,
Benutzer,
Zugriffe
und Konfigurationen verwalten.

Typische Aufgaben:

```
Server prüfen
Benutzer anlegen
Rechte vergeben
Netzwerkfehler suchen
Remotezugriff absichern
Logs auswerten
Backups kontrollieren
Dienste überwachen
Änderungen dokumentieren
```

Merksatz:

```
Administration ist nicht nur Einrichten,
sondern laufender sicherer Betrieb.
```

Systemzugriff

Systemzugriff bedeutet:

```
Zugriff auf ein IT-System zur Nutzung,
Verwaltung
oder Fehlerbehebung.
```

Arten:

```
lokaler Zugriff
Remotezugriff
Weboberfläche
SSH
RDP
VPN
Bastion Host
Managementnetz
Cloud-Portal
API
```

Merksatz:

```
Je mächtiger der Zugriff,
desto stärker muss er abgesichert werden.
```

Lokaler Zugriff

Lokaler Zugriff erfolgt direkt am Gerät.

Beispiele:

```
Serverkonsole
lokale Anmeldung
Tastatur und Monitor
physische Konsole im Serverraum
```

Vorteil:

```
funktioniert oft auch bei Netzwerkproblemen
```

Nachteil:

```
physischer Zugang nötig
```

Merksatz:

```
Lokaler Zugriff ist direkter Zugriff am System.
```

Remotezugriff

Remotezugriff bedeutet:

```
Zugriff aus der Ferne.
```

Beispiele:

SSH
RDP
VPN
Weboberfläche
Remote-Support-Tool
Cloud-Konsole

Risiko:

Remotezugänge sind häufige Angriffsziele.

Merksatz:

Remotezugriff ist praktisch,
aber sicherheitskritisch.

SSH

SSH steht für:

Secure Shell

SSH dient dem verschlüsselten Fernzugriff auf eine Kommandozeile.

Typische Nutzung:

Linux-Server
Unix-Systeme
Netzwerkgeräte
Firewalls
Switches
Router
NAS-Systeme
Dateiübertragung mit SFTP oder SCP

Standardport:

```
TCP 22
```

Merksatz:

```
SSH = verschlüsselter Kommandozeilenzugriff.
```

SSH-Sicherheit

SSH sollte sicher betrieben werden.

Wichtige Maßnahmen:

```
Schlüssel statt Passwort nutzen
privaten Schlüssel schützen
Passphrase verwenden
Root-Login vermeiden
sudo nutzen
Zugriff per Firewall begrenzen
MFA prüfen
alte Schlüssel entfernen
Logs überwachen
Host-Key-Warnungen ernst nehmen
```

Merksatz:

```
SSH ist verschlüsselt,
aber nur mit sicherer Konfiguration wirklich sicher.
```

Privater und öffentlicher SSH-Schlüssel

SSH-Schlüsselpaar:

```
privater Schlüssel

und

öffentlicher Schlüssel
```

Privater Schlüssel:

```
bleibt geheim beim Benutzer
```

Öffentlicher Schlüssel:

```
wird auf Zielsystemen hinterlegt
```

Merksatz:

```
Öffentlicher Schlüssel auf Server,
privater Schlüssel bleibt geheim.
```

SSH Host Key

Der SSH Host Key identifiziert den Server.

Wenn sich der Host Key unerwartet ändert, kann das bedeuten:

```
Server wurde neu installiert
falscher Server wird erreicht
Man-in-the-Middle-Angriff möglich
```

Merksatz:

```
SSH-Host-Key-Warnungen nicht blind ignorieren.
```

RDP

RDP steht für:

```
Remote Desktop Protocol
```

RDP ermöglicht grafischen Fernzugriff auf Windows-Systeme.

Standardport:

```
TCP 3389
```

Merksatz:

```
RDP = grafischer Windows-Fernzugriff.
```

RDP-Sicherheit

RDP sollte nicht breit direkt im Internet erreichbar sein.

Schutzmaßnahmen:

```
VPN nutzen
RDP Gateway nutzen
MFA aktivieren
Network Level Authentication nutzen
Quell-IP einschränken
starke Passwörter
Account Lockout
Updates einspielen
Logs überwachen
```

Merksatz:

```
RDP offen im Internet ist ein hohes Risiko.
```

VPN

VPN ermöglicht verschlüsselten Zugriff auf ein internes Netzwerk.

Vorteile:

```
Adminports müssen nicht öffentlich sein
Zugriff zentral steuerbar
MFA möglich
interne Dienste bleiben privat
bessere Protokollierung möglich
```

Wichtig:

```
VPN ersetzt keine Rechteverwaltung.
```

Merksatz:

```
VPN schützt den Zugang,
aber nicht automatisch das Zielsystem.
```

Bastion Host und Jump Server

Ein Bastion Host oder Jump Server ist ein geschützter Sprungserver.

Prinzip:

```
Administrator
verbindet sich zum Sprungserver

und von dort

zum Zielsystem
```

Vorteile:

```
weniger direkte Adminzugänge
zentrale Protokollierung
kontrollierter Zugriff
interne Systeme bleiben besser geschützt
```

Merksatz:

```
Bastion Host bündelt und schützt Adminzugriffe.
```

Managementnetz

Ein Managementnetz trennt administrative Zugriffe vom normalen Benutzernetz.

Darin liegen zum Beispiel:

```
Switch-Management
Firewall-Management
Server-Management
Storage-Management
Backup-Management
Hypervisor-Management
```

Merksatz:

```
Managementschnittstellen gehören nicht ins normale Clientnetz.
```

Out-of-Band-Management

Out-of-Band-Management nutzt einen getrennten Verwaltungsweg.

Beispiele:

```
iLO
iDRAC
IPMI
serielle Konsole
```

Vorteil:

```
Zugriff auch bei Störungen möglich
```

Risiko:

```
sehr mächtiger Zugriff
```

Merksatz:

```
Out-of-Band-Management besonders stark schützen.
```

Benutzerkonto

Ein Benutzerkonto ist eine digitale Identität.

Es enthält typischerweise:

```
Benutzername
Anmeldedaten
Gruppenmitgliedschaften
Rollen
Berechtigungen
Status
```

Merksatz:

```
Benutzerkonto = digitale Identität.
```

Persönliche Konten

Jeder Benutzer sollte ein eigenes persönliches Konto haben.

Vorteile:

```
Aktionen nachvollziehbar
Rechte gezielt verwaltbar
Offboarding einfacher
keine Passwortweitergabe
bessere Sicherheitsanalyse
```

Merksatz:

```
Ein Benutzer,
ein Konto.
```

Sammelkonten

Sammelkonten werden von mehreren Personen genutzt.

Probleme:

```
keine eindeutige Nachvollziehbarkeit
Passwortweitergabe
```

schwieriges Offboarding
höheres Missbrauchsrisiko
schlechte Protokollierung

Merksatz:

Sammelkonten vermeiden,
besonders bei Adminzugängen.

Gruppen und Rollen

Gruppen fassen Benutzer technisch zusammen.

Rollen beschreiben Aufgaben oder Funktionen.

Beispiele:

Helpdesk
Netzwerkadministrator
Serveradministrator
Backup-Operator
Standardbenutzer
Leser
Bearbeiter

Merksatz:

Gruppen vereinfachen Rechtevergabe.
Rollen beschreiben Aufgaben.

RBAC

RBAC steht für:

Role-Based Access Control

Dabei werden Rechte anhand von Rollen vergeben.

Beispiel:

```
Rolle Helpdesk darf Passwörter zurücksetzen.
```

Merksatz:

```
RBAC vergibt Rechte nach Rollen.
```

ABAC

ABAC steht für:

```
Attribute-Based Access Control
```

Dabei werden Zugriffe anhand von Eigenschaften entschieden.

Beispiele:

```
Standort
Gerätetyp
Uhrzeit
Sicherheitsstatus des Geräts
Abteilung
Datenklassifizierung
```

Merksatz:

```
ABAC entscheidet nach Eigenschaften und Bedingungen.
```

Authentifizierung und Autorisierung

Authentifizierung:

```
Wer bist du?
```

Autorisierung:

```
Was darfst du?
```

Beispiel:

```
Benutzer meldet sich an.
Danach wird geprüft,
ob er Datei lesen darf.
```

Merksatz:

```
Erst Identität prüfen,
dann Berechtigung prüfen.
```

Least Privilege

Least Privilege bedeutet:

```
nur notwendige Rechte vergeben.
```

Beispiele:

```
Benutzer ohne lokale Adminrechte
Dienstkonto nur mit benötigten Datenbankrechten
Support nur mit passenden Supportrechten
Adminrechte nur bei Bedarf
```

Merksatz:

```
So wenig Rechte wie möglich,
so viele wie nötig.
```

Need to Know

Need to Know bedeutet:

```
Zugriff nur auf Informationen,
die für die Aufgabe benötigt werden.
```

Merksatz:

Nicht jeder muss alles sehen können.

Admin- und Alltagskonto trennen

Administratoren sollten zwei Konten nutzen:

normales Benutzerkonto

und

separates Adminkonto

Vorteile:

weniger Risiko durch Phishing
weniger Malware-Schaden
bessere Nachvollziehbarkeit
weniger dauerhafte Rechte

Merksatz:

Nicht dauerhaft mit Adminrechten arbeiten.

Dienstkonto

Ein Dienstkonto ist eine technische Identität für Dienste, Anwendungen oder automatisierte Prozesse.

Beispiele:

Backupdienst
Monitoring-Agent
Webanwendung mit Datenbankzugriff
API-Integration
geplante Aufgabe

Merksatz:

Dienstkonten sind technische Identitäten und müssen rechtearm sein.

Offboarding

Offboarding bedeutet:

Zugänge werden entfernt,
wenn Benutzer ausscheiden
oder keinen Zugriff mehr benötigen.

Zu prüfen:

Benutzerkonto
Gruppen
VPN
SSH-Schlüssel
Cloud-Zugänge
API-Tokens
lokale Adminrechte
Geräte
E-Mail-Weiterleitungen

Merksatz:

Alte Zugänge sind ein Sicherheitsrisiko.

Regelmäßige Rechteprüfung

Rechte sollten regelmäßig geprüft werden.

Besonders wichtig:

Adminrechte
lokale Administratoren
Dienstkonten
externe Dienstleister
Gruppenmitgliedschaften

```
Cloud-Rollen
Freigaben
SSH-Schlüssel
```

Merksatz:

```
Rechte altern und müssen gepflegt werden.
```

Logs

Logs sind protokollierte Ereignisse.

Beispiele:

```
Anmeldung
Fehlanmeldung
Dienststart
Dienstfehler
Firewall-Block
VPN-Verbindung
Backup-Fehler
Adminänderung
```

Merksatz:

```
Logs zeigen,
was passiert ist.
```

Monitoring

Monitoring überwacht Zustände und Metriken.

Beispiele:

```
Verfügbarkeit
CPU-Auslastung
RAM-Nutzung
Speicherplatz
```

Antwortzeit

Backup-Erfolg

Zertifikatslaufzeit

Dienststatus

Merksatz:

Monitoring zeigt,
was gerade passiert oder sich anbahnt.

Logging, Monitoring und Alerting unterscheiden

Begriff	Zweck
Logging	Ereignisse aufzeichnen
Monitoring	Zustände überwachen
Alerting	bei kritischen Zuständen alarmieren
Reporting	Verlauf auswerten

Merksatz:

Logs erklären Ereignisse.
Monitoring beobachtet Zustände.
Alerting meldet Probleme.

Wichtige Logquellen

Typische Logquellen:

Betriebssystemlogs

Anwendungslogs

Authentifizierungslogs

Firewall-Logs

VPN-Logs

DNS-Logs

DHCP-Logs

Webserverlogs

Backup-Logs

Cloud-Audit-Logs
EDR-Logs

Merksatz:

Wichtige Systeme brauchen nachvollziehbare Logs.

Zentrale Logsammlung

Zentrale Logsammlung bedeutet:

Logs mehrerer Systeme werden zentral gesammelt.

Vorteile:

bessere Suche
bessere Korrelation
Schutz vor lokaler Manipulation
bessere Sicherheitsanalyse
Grundlage für SIEM

Merksatz:

Zentrale Logs helfen,
Zusammenhänge systemübergreifend zu erkennen.

NTP und Logs

NTP synchronisiert Systemzeiten.

Warum wichtig?

Logs verschiedener Systeme müssen zeitlich vergleichbar sein.

Merksatz:

Gemeinsame Zeitbasis ist wichtig für Loganalyse und Forensik.

Dienstprüfung

Dienstprüfung bedeutet:

> prüfen,
> ob ein Dienst läuft,
> erreichbar ist
> und korrekt arbeitet.

Zu prüfen:

> Dienststatus
> Port
> Firewall
> DNS
> Routing
> Logs
> Ressourcen
> Abhängigkeiten
> Berechtigungen

Merksatz:

> Dienst läuft nicht automatisch gleich Dienst funktioniert.

Netzwerkbefehle

Wichtige Befehle und Werkzeuge:

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

Aufgabe	Windows	Linux/macOS
Logs prüfen	Ereignisanzeige	journalctl

Merksatz:

```
Gleiche Aufgabe,
anderes Werkzeug je nach Betriebssystem.
```

---

ping

ping testet Erreichbarkeit per ICMP.

Wichtig:

```
fehlgeschlagener ping beweist nicht automatisch,
dass ein Ziel offline ist.
```

Mögliche Ursachen:

```
ICMP blockiert
Firewall
Routingproblem
DNS-Problem
Ziel offline
Paketverlust
```

Merksatz:

```
ping ist ein Hinweis,
aber kein vollständiger Diensttest.
```

DNS-Prüfung

DNS wird geprüft mit:

```
nslookup
```

```
oder

dig
```

Typische Regel:

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

Merksatz:

```
DNS-Probleme sind häufige Ursachen für Verbindungsfehler.
```

---

tracert und traceroute

tracert oder traceroute zeigen den Weg zum Ziel über Zwischenstationen.

Wichtig:

```
Nicht jeder Hop muss antworten.
Sternchen bedeuten nicht automatisch Ausfall.
```

Merksatz:

```
Traceroute-Ausgaben müssen interpretiert werden.
```

---

netstat und ss

netstat und ss zeigen Netzwerkverbindungen und lauschende Ports.

Wichtige Zustände:

```
LISTEN:
Dienst wartet auf Verbindungen.

ESTABLISHED:
Verbindung besteht.
```

Merksatz:

```
Offene Ports zeigen mögliche Dienstzugänge.
```

---

localhost und 0.0.0.0

127.0.0.1:

```
nur lokal auf demselben System erreichbar
```

0.0.0.0:

```
Dienst lauscht auf allen IPv4-Schnittstellen
```

Merksatz:

```
127.0.0.1 ist lokal.
0.0.0.0 ist überall auf dem Host.
```

---

curl

curl testet Webdienste und APIs.

Nützlich für:

```
HTTP-Statuscode
Header
Weiterleitungen
HTTPS
API-Antwort
Erreichbarkeit
```

Merksatz:

```
curl prüft Webdienste direkter als ein Browser.
```

---

systemctl und journalctl

systemctl:

```
Dienste prüfen und verwalten
```

journalctl:

```
systemd-Logs anzeigen
```

Merksatz:

```
systemctl zeigt Dienststatus.
journalctl zeigt passende Logs.
```

Dateiübertragung und Freigaben

Dateiübertragung und Freigaben müssen sicher geplant werden.

Zu klären:

```
Wer braucht Zugriff?
Welche Daten?
Welche Rechte?
Wie lange?
Intern oder extern?
Wird protokolliert?
Wird verschlüsselt übertragen?
```

Merksatz:

```
Keine Freigabe ohne Zweck und Berechtigung.
```

SMB

SMB steht für:

```
Server Message Block
```

Typische Nutzung:

```
Windows-Dateifreigaben
Netzlaufwerke
Druckerfreigaben
```

Standardport:

```
TCP 445
```

Merksatz:

```
SMB ist typisch für Windows-Dateifreigaben.
```

NFS

NFS steht für:

```
Network File System
```

Typische Nutzung:

```
Unix- und Linux-Freigaben
Serverfreigaben
Virtualisierungsspeicher
Backup-Ziele
```

Merksatz:

```
NFS ist typisch für Unix- und Linux-Umgebungen.
```

FTP, FTPS, SFTP und SCP

Protokoll	Grundlage	Verschlüsselung
FTP	FTP	nein
FTPS	FTP plus TLS	ja

Protokoll	Grundlage	Verschlüsselung
SFTP	SSH	ja
SCP	SSH	ja

Merksatz:

```
FTP ist unverschlüsselt.
FTPS ist FTP mit TLS.
SFTP ist Dateiübertragung über SSH.
SCP kopiert über SSH.
```

Synchronisation ist kein Backup

Synchronisation hält Daten an mehreren Orten gleich.

Problem:

```
Löschung,
Fehler
oder Ransomware-Verschlüsselung
können mitsynchronisiert werden.
```

Merksatz:

```
Synchronisation ist kein Backup.
```

Backup

Backup bedeutet:

```
Sicherung von Daten,
Systemen
oder Konfigurationen.
```

Restore bedeutet:

```
Wiederherstellung aus einer Sicherung.
```

Merksatz:

> Backup ist die Sicherung.
> Restore ist die Wiederherstellung.

Restore-Test

Ein Restore-Test prüft, ob Wiederherstellung wirklich funktioniert.

Zu prüfen:

> Daten vollständig?
> Anwendung startet?
> Rechte korrekt?
> Datenbank konsistent?
> Schlüssel vorhanden?
> Zeit akzeptabel?

Merksatz:

> Nur getestete Backups sind verlässlich.

Backup-Arten

Backup-Art	Bedeutung
Vollbackup	sichert alles
inkrementell	Änderungen seit letztem Backup
differenziell	Änderungen seit letztem Vollbackup
Snapshot	Momentaufnahme
Image-Backup	vollständiges Systemabbild
dateibasiert	ausgewählte Dateien und Ordner

Merksatz:

> Backup-Art nach Wiederherstellungsziel wählen.

RPO und RTO

RPO:

```
Recovery Point Objective

maximal akzeptabler Datenverlust
```

RTO:

```
Recovery Time Objective

maximal akzeptable Wiederherstellungszeit
```

Merksatz:

```
RPO = Datenverlust.
RTO = Wiederherstellungszeit.
```

3-2-1-Regel

Die 3-2-1-Regel lautet:

```
3 Kopien

2 unterschiedliche Speicherarten

1 Kopie extern oder getrennt
```

Merksatz:

```
3-2-1 reduziert das Risiko,
dass alle Kopien gleichzeitig verloren gehen.
```

Immutable und Offline Backup

Immutable Backup:

kann für eine festgelegte Zeit nicht verändert oder gelöscht werden

Offline Backup:

ist nicht dauerhaft verbunden

Vorteil:

besserer Schutz gegen Ransomware und Manipulation

Merksatz:

Backups müssen vor Angreifern geschützt werden.

Redundanz, Replikation und Backup unterscheiden

Begriff	Ziel
Backup	Wiederherstellung alter Zustände
Redundanz	Ausfall abfedern
Replikation	Daten aktuell auf zweites System kopieren

Merksatz:

Redundanz und Replikation ersetzen kein Backup.

Dokumentation

Dokumentation beschreibt Systeme, Netzwerke, Dienste, Rechte, Änderungen und Notfallmaßnahmen.

Typische Inhalte:

Systeme
IP-Adressen
Hostnamen
Dienste

Ports
Firewall-Regeln
VLANs
DNS-Einträge
Zertifikate
Backups
Verantwortliche
Runbooks

Merksatz:

Gute Dokumentation macht Betrieb nachvollziehbar.

Netzplan

Ein Netzplan zeigt die Netzwerkstruktur.

Physischer Netzplan:

Geräte,
Kabel,
Ports,
Racks,
Standorte

Logischer Netzplan:

VLANs,
Subnetze,
Routing,
Firewall-Zonen,
Dienste

Merksatz:

Physisch zeigt Verkabelung.
Logisch zeigt Kommunikationsstruktur.

IPAM

IPAM steht für:

```
IP Address Management
```

IPAM verwaltet IP-Adressen, Subnetze und Zuordnungen.

Merksatz:

```
IPAM verhindert IP-Chaos und IP-Konflikte.
```

Runbook und SOP

Runbook:

```
Schritt-für-Schritt-Anleitung für konkrete Aufgaben oder Störungen
```

SOP:

```
Standard Operating Procedure,
standardisierter Ablauf
```

Merksatz:

```
Runbook hilft bei konkreter Ausführung.
SOP beschreibt standardisierte Vorgehensweise.
```

Change Management

Change Management bedeutet:

```
Änderungen werden geplant,
bewertet,
freigegeben,
umgesetzt,
getestet
```

und dokumentiert.

Merksatz:

Change Management verhindert unkontrollierte Änderungen.

Change-Arten

Change-Art	Bedeutung
Standard Change	bekannte risikoarme Routineänderung
Normal Change	geplante Änderung mit Prüfung
Emergency Change	dringende Änderung

Merksatz:

Emergency Change ist dringend,
aber nicht dokumentationsfrei.

Change Request

Ein Change Request ist ein Änderungsantrag.

Typische Inhalte:

Beschreibung
Grund
betroffene Systeme
Risiko
Zeitpunkt
Testplan
Rollback-Plan
Freigabe
Kommunikation

Merksatz:

```
Change Request beschreibt,
was geändert werden soll und warum.
```

Rollback-Plan

Ein Rollback-Plan beschreibt, wie eine Änderung zurückgenommen wird.

Beispiele:

```
Backup zurückspielen
Snapshot zurücksetzen
alte Konfiguration wiederherstellen
alte Version installieren
DNS zurücksetzen
Firewall-Regel entfernen
```

Merksatz:

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

CMDB

CMDB steht für:

```
Configuration Management Database
```

Sie enthält Informationen über verwaltete IT-Elemente und deren Beziehungen.

Beispiele:

```
Server
Anwendung
Datenbank
Firewall
Zertifikat
Lizenz
Dienst
```

Merksatz:

```
CMDB zeigt,
welche IT-Elemente zusammenhängen.
```

Typische IHK-Fragen

In AP1 und AP2 kann zum Beispiel gefragt werden:

```
- Was ist Netzwerkadministration?
- Was ist Remotezugriff?
- Was ist SSH?
- Welchen Port nutzt SSH?
- Was ist RDP?
- Welchen Port nutzt RDP?
- Warum sollte RDP nicht offen im Internet stehen?
- Was ist ein Bastion Host?
- Was ist ein Managementnetz?
- Was ist Out-of-Band-Management?
- Warum sind persönliche Konten wichtig?
- Warum sind Sammelkonten problematisch?
- Was ist RBAC?
- Was ist ABAC?
- Was ist der Unterschied zwischen Authentifizierung und Autorisierung?
- Was bedeutet Least Privilege?
- Was ist ein Dienstkonto?
- Was ist Offboarding?
- Warum sind Logs wichtig?
- Was ist der Unterschied zwischen Logging und Monitoring?
- Warum ist NTP für Logs wichtig?
- Was macht ping?
- Was prüft nslookup?
- Was prüft traceroute?
- Was zeigen netstat oder ss?
- Was ist SMB?
- Was ist SFTP?
- Warum ist FTP unsicher?
- Warum ist Synchronisation kein Backup?
- Was ist Backup?
```

- Was ist Restore?
- Was bedeutet RPO?
- Was bedeutet RTO?
- Was ist die 3-2-1-Regel?
- Was ist ein Netzplan?
- Was ist IPAM?
- Was ist Change Management?
- Was ist ein Rollback-Plan?
- Was ist eine CMDB?

Typische Prüfungsfallen

SSH ist verschlüsselt,
aber nicht automatisch sicher konfiguriert.

SSH nutzt TCP 22.

RDP nutzt TCP 3389.

RDP nicht direkt öffentlich bereitstellen.

VPN ersetzt keine Rechteverwaltung.

Bastion Host ist ein Sprungserver.

Managementnetz vom Clientnetz trennen.

Out-of-Band-Zugriff ist besonders kritisch.

Sammelkonten vermeiden.

Admin- und Alltagskonto trennen.

Authentifizierung und Autorisierung unterscheiden.

Least Privilege gilt auch für Administratoren.

Dienstkonten brauchen minimale Rechte.

Offboarding muss alle Zugänge entfernen.

Logs zeigen Ereignisse.

Monitoring zeigt Zustände.

Alerting meldet kritische Abweichungen.

Ohne NTP sind Logzeiten schwer vergleichbar.

Dienst läuft nicht automatisch gleich Anwendung funktioniert.

ping prüft ICMP,
nicht jeden Dienst.

Kein ping kann Firewall sein.

IP funktioniert,
Name nicht:
DNS prüfen.

Offener Port bedeutet nicht Anwendung gesund.

127.0.0.1 ist nur lokal.

FTP ist unverschlüsselt.

SFTP ist nicht FTPS.

SMB nutzt TCP 445.

Synchronisation ist kein Backup.

Replikation ist kein Backup.

Redundanz ist kein Backup.

Backup ohne Restore-Test ist unsicher.

RPO ist Datenverlust.

RTO ist Wiederherstellungszeit.

Snapshot ist nicht automatisch Backup.

Dokumentation muss aktuell sein.

Secrets gehören nicht in Klartextdokumentation.

Emergency Change muss nachträglich dokumentiert werden.

Rollback vor Änderung planen.

Wichtige Begriffe kurz erklärt

Begriff	Kurze Erklärung
Netzwerkadministration	Verwaltung von Netzwerken und Systemen
Systemzugriff	Zugriff auf ein IT-System
Remotezugriff	Zugriff aus der Ferne
SSH	verschlüsselter Kommandozeilenzugriff
RDP	grafischer Windows-Fernzugriff
VPN	verschlüsselter Zugang ins interne Netz
Bastion Host	geschützter Sprungserver
Jump Server	Zwischensystem für Administration
Managementnetz	getrenntes Verwaltungsnetz
Out-of-Band	separater Verwaltungsweg
Benutzerkonto	digitale Identität
Gruppe	Zusammenfassung von Benutzern
Rolle	Aufgabe mit Rechten
RBAC	rollenbasierte Zugriffskontrolle
ABAC	attributbasierte Zugriffskontrolle
Authentifizierung	Identität prüfen
Autorisierung	Rechte prüfen
Least Privilege	minimale notwendige Rechte
Dienstkonto	technische Identität

Begriff	Kurze Erklärung
Offboarding	Entfernen alter Zugänge
Log	protokolliertes Ereignis
Monitoring	Überwachung von Zuständen
Alerting	automatische Alarmierung
NTP	Zeitsynchronisation
Health Check	Dienstgesundheitsprüfung
ping	ICMP-Erreichbarkeitstest
nslookup	DNS-Prüfung
dig	detaillierte DNS-Prüfung
tracert	Windows-Wegverfolgung
traceroute	Wegverfolgung unter Linux/macOS
netstat	Netzwerkverbindungen anzeigen
ss	Socketanzeige unter Linux
curl	Web- und API-Test
SMB	Windows-Dateifreigabeprotokoll
NFS	Network File System
FTP	unverschlüsselte Dateiübertragung
FTPS	FTP mit TLS
SFTP	Dateiübertragung über SSH
SCP	Kopieren über SSH
Backup	Sicherung
Restore	Wiederherstellung
RPO	maximaler Datenverlust
RTO	maximale Wiederherstellungszeit
Immutable Backup	unveränderliches Backup
Snapshot	Momentaufnahme
Redundanz	mehrfach vorhandene Komponenten
Replikation	Kopie aktueller Daten
Dokumentation	nachvollziehbare Beschreibung
Netzplan	grafische Netzwerkdarstellung
IPAM	IP-Adressverwaltung
Runbook	Schritt-für-Schritt-Anleitung

Begriff	Kurze Erklärung
SOP	Standardprozess
Change Management	kontrollierter Änderungsprozess
Rollback	Rücknahme einer Änderung
CMDB	Datenbank verwalteter IT-Elemente

IHK-sichere Gesamtformulierung

Netzwerkadministration umfasst den sicheren Betrieb und die Verwaltung von Systemen, Netzwerken, Diensten, Benutzern, Zugängen und Konfigurationen. Remotezugriffe wie SSH und RDP müssen durch VPN, Bastion Hosts, Managementnetze, MFA, Logging und Least Privilege abgesichert werden. Benutzer sollten persönliche Konten nutzen, Rechte sollten über Gruppen und Rollen vergeben und regelmäßig geprüft werden. Logs, Monitoring, Alerting und NTP sind wichtig für Fehlersuche, Sicherheit und Nachvollziehbarkeit. Netzwerkbefehle wie ping, nslookup, traceroute, netstat, ss, curl, ipconfig, ip addr, route print und ip route helfen bei systematischer Analyse. Dateiübertragung und Freigaben müssen verschlüsselt, berechtigt und dokumentiert erfolgen. Backups müssen geschützt, überwacht und durch Restore-Tests geprüft werden. Dokumentation und Change Management stellen sicher, dass Systeme nachvollziehbar betrieben und Änderungen kontrolliert durchgeführt werden.

Wichtigste Merksätze

Netzwerkadministration ist laufender Betrieb.

Adminzugänge besonders schützen.

Remotezugriff ist sicherheitskritisch.

SSH nutzt TCP 22.

RDP nutzt TCP 3389.

RDP nicht offen ins Internet stellen.

VPN schützt Zugang,
ersetzt aber keine Rechte.

Bastion Host schützt interne Systeme.

Managementnetz trennt Verwaltung.

Persönliche Konten statt Sammelkonten.

Admin- und Alltagskonto trennen.

RBAC arbeitet mit Rollen.

ABAC arbeitet mit Eigenschaften.

Authentifizierung fragt:
Wer bist du?

Autorisierung fragt:
Was darfst du?

Least Privilege gilt immer.

Dienstkonten rechtearm betreiben.

Offboarding entfernt alte Zugänge.

Logs zeigen Ereignisse.

Monitoring zeigt Zustände.

Alerting meldet Probleme.

NTP macht Logs vergleichbar.

Dienst läuft nicht automatisch gleich Dienst funktioniert.

ping prüft ICMP.

DNS mit nslookup oder dig prüfen.

traceroute zeigt den Weg.

netstat und ss zeigen Verbindungen.

curl prüft Webdienste.

SMB nutzt TCP 445.

FTP ist unsicher,
weil unverschlüsselt.

SFTP nutzt SSH.

FTPS nutzt FTP mit TLS.

Synchronisation ist kein Backup.

Backup ohne Restore-Test ist unsicher.

RPO ist Datenverlust.

RTO ist Wiederherstellungszeit.

Replikation ersetzt kein Backup.

Redundanz ersetzt kein Backup.

Dokumentation muss aktuell sein.

Change Management kontrolliert Änderungen.

Rollback vor Änderung planen.

Notfallzugänge streng schützen.

Sichere Administration braucht Technik,
Prozesse,
Rechte,
Logs
und Dokumentation.