10.8 Remotezugriff und Fernadministration: SSH, RDP und Telnet

Remotezugriff gehört zur OSI-Schicht 7.

Remotezugriff bedeutet:

```
Ein Benutzer oder Administrator greift aus der Ferne auf ein anderes System zu.
```

Typische Protokolle sind:

```
- SSH
- RDP
- Telnet
```

Sie dienen dazu, entfernte Systeme zu bedienen, zu verwalten oder zu konfigurieren.

Merksatz:

```
Remotezugriff = entfernte Systeme über das Netzwerk bedienen.
```

Grundidee von Remotezugriff

Bei Remotezugriff sitzt der Benutzer nicht direkt vor dem Zielsystem.

Stattdessen erfolgt der Zugriff über das Netzwerk.

Beispiele:

```
Administrator verbindet sich per SSH auf einen Linux-Server.
Benutzer verbindet sich per RDP auf einen Windows-Rechner.
Techniker greift auf eine Firewall-Konsole zu.
Support meldet sich auf einem Terminalserver an.
Ein Server wird aus der Ferne konfiguriert.
```

Merksatz:

Remotezugriff ermöglicht Administration ohne direkten physischen Zugriff.

Remotezugriff im OSI-Modell

Remotezugriffsprotokolle gehören zur Anwendungsschicht.

Thema	Schicht
SSH	7
RDP	7
Telnet	7
TCP-Port	4
IP-Adresse	3
Verschlüsselung	6 / Sicherheitsbezug
Benutzeranmeldung	7 / Authentifizierung

Wichtig:

SSH, RDP und Telnet sind Anwendungsschicht-Protokolle.
Die verwendeten Ports gehören zur Transportschicht.

Merksatz:

Protokoll = Schicht 7.
Port = Schicht 4.

SSH

SSH steht für:

Secure Shell

SSH wird für sicheren Fernzugriff auf Kommandozeilen verwendet.

Typischer Port:

TCP 22

SSH wird häufig genutzt bei:

- Linux-Servern
- Netzwerkgeräten
- Firewalls
- NAS-Systemen
- Routern
- Switches
- Automatisierung
- Dateiübertragung über SFTP

Merksatz:

SSH = sicherer Fernzugriff auf die Shell.

Warum ist SSH wichtig?

SSH ermöglicht sichere Administration über ein Netzwerk.

SSH bietet:

- verschlüsselte Verbindung
- Authentifizierung
- Integritätsschutz
- sichere Befehlsausführung
- sichere Dateiübertragung über SFTP
- Portweiterleitungen und Tunnel

Im Gegensatz zu Telnet überträgt SSH Daten nicht einfach im Klartext.

Merksatz:

SSH schützt Fernadministration durch Verschlüsselung.

SSH-Verbindung vereinfacht

Ablauf vereinfacht:

1. Client verbindet sich mit Server auf TCP 22.
2. Server präsentiert seinen Host-Key.
3. Client prüft den Host-Key.
4. Verschlüsselung wird ausgehandelt.
5. Benutzer authentifiziert sich.
6. Shell oder Dienst wird bereitgestellt.

Merksatz:

SSH prüft Server,
verschlüsselt Verbindung
und authentifiziert Benutzer.

SSH-Client und SSH-Server

SSH-Client:

Programm, das die Verbindung startet.

SSH-Server:

Dienst auf dem Zielsystem,
der SSH-Verbindungen annimmt.

Beispiele:

Client:
Terminal, PuTTY, OpenSSH-Client

Server:
OpenSSH-Server auf Linux,
SSH-Dienst auf Netzwerkgerät

Merksatz:

SSH-Client verbindet sich zum SSH-Server.

SSH-Host-Key

Der SSH-Host-Key identifiziert den SSH-Server.

Beim ersten Verbindungsaufbau speichert der Client häufig den Host-Key.

Bei späteren Verbindungen prüft der Client:

```
Ist es derselbe Server wie vorher?
```

Wenn sich der Host-Key plötzlich ändert, erscheint eine Warnung.

Mögliche Ursachen:

```
- Server wurde neu installiert
- Host-Key wurde geändert
- DNS zeigt auf anderen Server
- IP-Adresse wurde neu vergeben
- möglicher Man-in-the-Middle-Angriff
```

Merksatz:

```
SSH-Host-Key schützt vor unbemerktem Serverwechsel.
```

SSH-Authentifizierung mit Passwort

Bei Passwortauthentifizierung meldet sich der Benutzer mit Benutzername und Passwort an.

Vorteil:

```
einfach einzurichten
```

Nachteile:

```
- anfällig gegen schwache Passwörter
- Brute-Force-Angriffe möglich
- Passwort kann bei schlechter Verwaltung kompromittiert werden
```

Merksatz:

```
Passwortlogin ist einfach,
aber stärker abzusichern.
```

SSH-Authentifizierung mit Schlüssel

Bei Schlüsselanmeldung wird ein Schlüsselpaar verwendet.

Es besteht aus:

```
privatem Schlüssel
öffentlichem Schlüssel
```

Der öffentliche Schlüssel liegt auf dem Server.

Der private Schlüssel bleibt beim Benutzer.

Wichtig:

```
Der private Schlüssel darf nicht weitergegeben werden.
```

Merksatz:

```
SSH-Schlüssel bestehen aus öffentlichem und privatem Schlüssel.
```

Vorteile von SSH-Schlüsseln

SSH-Schlüssel haben mehrere Vorteile:

```
- keine Passwortübertragung
- gut für Automatisierung
- stärker als einfache Passwörter
- Zugriff kann pro Schlüssel verwaltet werden
- private Schlüssel können zusätzlich mit Passphrase geschützt werden
```

Merksatz:

```
SSH-Schlüssel sind für sichere Administration sehr wichtig.
```

SSH-Passphrase

Eine Passphrase schützt den privaten SSH-Schlüssel.

Wenn jemand die Schlüsseldatei kopiert, kann er sie ohne Passphrase nicht sofort verwenden.

Merksatz:

```
Passphrase schützt den privaten Schlüssel zusätzlich.
```

SSH-Agent

Ein SSH-Agent kann private Schlüssel temporär im Speicher verwalten.

Vorteil:

```
Benutzer muss die Passphrase nicht bei jeder Verbindung neu eingeben.
```

Wichtig:

```
SSH-Agent-Weiterleitung muss vorsichtig verwendet werden,
weil sie Sicherheitsrisiken erzeugen kann.
```

Merksatz:

```
SSH-Agent erleichtert Schlüsselanmeldung,
muss aber sicher genutzt werden.
```

Root-Login über SSH

Direkter Root-Login über SSH sollte in vielen Umgebungen deaktiviert werden.

Besser:

```
normaler Benutzer meldet sich an
und nutzt bei Bedarf sudo oder administrative Rechte.
```

Vorteile:

```
- bessere Nachvollziehbarkeit
- weniger Risiko bei Brute-Force-Angriffen
- gezieltere Rechtevergabe
```

Merksatz:

```
Direktes Root-Login möglichst vermeiden.
```

SSH und SFTP

SFTP steht für:

```
SSH File Transfer Protocol
```

SFTP nutzt SSH als Grundlage.

Typischer Port:

```
TCP 22
```

SFTP ist nicht FTP mit Verschlüsselung, sondern ein eigenes Dateiübertragungsprotokoll über SSH.

Merksatz:

```
SFTP läuft über SSH.
```

SSH-Tunnel

Mit SSH können Tunnel aufgebaut werden.

Ein SSH-Tunnel leitet Netzwerkverkehr sicher durch eine SSH-Verbindung.

Typische Nutzung:

```
- internen Dienst sicher erreichen
- temporäre Portweiterleitung
- Administration über abgesicherte Verbindung
- Zugriff auf Datenbank oder Webdienst über SSH
```

Merksatz:

```
SSH-Tunnel leitet Verkehr verschlüsselt weiter.
```

SSH-Portforwarding

SSH-Portforwarding bedeutet:

```
Ein lokaler oder entfernter Port wird über SSH weitergeleitet.
```

Beispiel sinngemäß:

```
lokaler Port 8080
→ durch SSH
→ interner Webdienst auf Server
```

Das kann nützlich sein, muss aber kontrolliert werden, weil dadurch Sicherheitsgrenzen umgangen werden können.

Merksatz:

```
SSH-Portforwarding kann hilfreich,
aber sicherheitskritisch sein.
```

SSH-Sicherheitsmaßnahmen

Wichtige Maßnahmen:

```
- starke Passwörter oder Schlüssel verwenden
- Root-Login deaktivieren
- Passwortlogin nach Möglichkeit einschränken
- nur notwendige Benutzer erlauben
- Firewall-Regeln setzen
- Zugriff per VPN begrenzen
- Fail2ban oder ähnliche Schutzmechanismen nutzen
- Logs prüfen
- alte Schlüssel entfernen
- Schlüssel mit Passphrase schützen
```

Merksatz:

```
SSH muss trotz Verschlüsselung sauber abgesichert werden.
```

Typische SSH-Fehler

Typische Fehler sind:

```
- TCP 22 blockiert
- SSH-Dienst läuft nicht
- falscher Hostname
- falsche IP-Adresse
- falscher Benutzername
- falsches Passwort
- falscher privater Schlüssel
- Rechte auf Schlüsseldatei falsch
- Benutzer nicht erlaubt
- Host-Key-Warnung
- Firewall blockiert Zugriff
```

Merksatz:

```
SSH-Fehler mit Port,
Dienst,
Benutzer,
Schlüssel
und Firewall prüfen.
```

Fehlerbild: SSH-Verbindung Timeout

Mögliche Ursachen:

```
- Zielhost nicht erreichbar
- TCP 22 durch Firewall blockiert
- Routingproblem
- falsche IP-Adresse
- SSH-Dienst lauscht auf anderem Port
- NAT oder Portweiterleitung falsch
```

```
- Server offline
```

Merksatz:

```
SSH-Timeout deutet oft auf Netzwerk,
Firewall
oder falschen Port hin.
```

Fehlerbild: SSH Connection Refused

Connection refused bedeutet:

```
Zielsystem ist erreichbar,
aber der Dienst auf dem Zielport nimmt keine Verbindung an.
```

Mögliche Ursachen:

```
- SSH-Dienst läuft nicht
- SSH lauscht nicht auf diesem Port
- Port falsch
- Dienst nur auf bestimmter IP gebunden
- lokale Firewall lehnt aktiv ab
```

Merksatz:

```
Connection refused heißt:
Host erreichbar,
Dienst nimmt nicht an.
```

Fehlerbild: SSH Permission Denied

Permission denied bedeutet:

```
Anmeldung wurde abgelehnt.
```

Mögliche Ursachen:

```
- falscher Benutzer
- falsches Passwort
- falscher Schlüssel
- öffentlicher Schlüssel fehlt auf Server
- Benutzer darf sich nicht anmelden
- Konto gesperrt
- Schlüsselrechte falsch
- Loginmethode deaktiviert
```

Merksatz:

```
Permission denied = Authentifizierung oder Berechtigung prüfen.
```

Fehlerbild: SSH Host-Key-Warnung

Eine Host-Key-Warnung bedeutet:

```
Der Server-Schlüssel passt nicht zu dem,
was der Client gespeichert hat.
```

Mögliche Ursachen:

```
- Server neu installiert
- anderer Server unter gleicher IP
- DNS zeigt auf anderes Ziel
- Load Balancer oder Proxy
- möglicher Angriff
```

Wichtig:

```
Warnung nicht blind ignorieren.
```

Merksatz:

```
Host-Key-Warnung immer prüfen.
```

RDP

RDP steht für:

```
Remote Desktop Protocol
```

RDP wird für grafischen Fernzugriff verwendet.

Typischer Port:

```
TCP 3389
```

RDP ist besonders verbreitet bei Windows-Systemen.

Typische Nutzung:

```
- Windows-Server administrieren
- Terminalserver nutzen
- Remote-Arbeitsplatz
- grafische Programme aus der Ferne bedienen
```

Merksatz:

```
RDP = grafischer Fernzugriff.
```

RDP-Grundidee

Bei RDP wird eine grafische Sitzung über das Netzwerk übertragen.

Der Benutzer sieht:

```
Desktop
Fenster
Programme
Mauszeiger
Tastatureingaben
```

Die Anwendung läuft auf dem entfernten System.

Der Benutzer bedient sie aus der Ferne.

Merksatz:

```
RDP überträgt eine entfernte Benutzeroberfläche.
```

RDP-Client und RDP-Server

RDP-Client:

```
startet die Verbindung
```

RDP-Server:

```
nimmt Remote-Desktop-Verbindungen an
```

Beispiel:

```
Benutzer startet Remote Desktop Client.
Client verbindet sich zu Windows-Server.
Server zeigt grafische Sitzung.
```

Merksatz:

```
RDP-Client verbindet sich zum RDP-Server.
```

RDP und Benutzeranmeldung

Für RDP wird normalerweise ein Benutzerkonto benötigt.

Dabei können relevant sein:

```
- Benutzername
- Passwort
- Domänenkonto
- lokale Benutzergruppe
- Remote-Desktop-Berechtigung
- Multi-Faktor-Authentifizierung
- Richtlinien
```

Nicht jeder Benutzer darf sich automatisch per RDP anmelden.

Merksatz:

```
RDP braucht Anmeldung und passende Berechtigung.
```

RDP und Sicherheit

RDP sollte besonders sorgfältig abgesichert werden.

Warum?

```
RDP ist ein beliebtes Ziel für Angriffe,
besonders wenn es direkt aus dem Internet erreichbar ist.
```

Risiken:

```
- Brute-Force-Angriffe
- gestohlene Zugangsdaten
- ungepatchte Schwachstellen
- Ransomware-Angriffe
- unberechtigter Zugriff
```

Merksatz:

```
RDP niemals leichtfertig ins Internet öffnen.
```

RDP sicher betreiben

Sinnvolle Maßnahmen:

```
- Zugriff nur über VPN
- Remote Desktop Gateway nutzen
- starke Passwörter
- Multi-Faktor-Authentifizierung
- Network Level Authentication aktivieren
- Firewall-Regeln einschränken
- nur notwendige Benutzer erlauben
```

- Logs überwachen
- Systeme aktuell halten
- Kontosperrungsrichtlinien nutzen

Merksatz:

RDP nur geschützt und kontrolliert bereitstellen.

Network Level Authentication

Network Level Authentication wird kurz genannt:

NLA

NLA verlangt, dass sich der Benutzer bereits vor dem vollständigen Aufbau der grafischen Sitzung authentifiziert.

Vorteil:

weniger Angriffsfläche
bessere Absicherung vor unerwünschten Sitzungsaufbauten

Merksatz:

NLA verbessert die Sicherheit bei RDP.

Remote Desktop Gateway

Ein Remote Desktop Gateway stellt RDP nicht direkt offen bereit, sondern vermittelt den Zugriff über einen Gateway-Dienst.

Vorteile:

- zentraler Zugriffspunkt
- bessere Kontrolle
- Authentifizierung
- Protokollierung
- Zugriff über HTTPS möglich

```
- weniger direkte RDP-Exposition
```

Merksatz:

```
RD Gateway schützt und bündelt RDP-Zugriffe.
```

RDP und VPN

Ein VPN kann verwendet werden, damit RDP nur intern erreichbar ist.

Ablauf:

```
Benutzer baut VPN auf.
Benutzer greift per RDP auf internes System zu.
```

Vorteil:

```
RDP-Port muss nicht direkt öffentlich erreichbar sein.
```

Merksatz:

```
RDP besser über VPN als direkt aus dem Internet.
```

Typische RDP-Fehler

Typische Fehler sind:

```
- TCP 3389 blockiert
- Remote Desktop deaktiviert
- Benutzer nicht berechtigt
- falsches Passwort
- Konto gesperrt
- NLA-Problem
- Lizenzproblem bei Terminalserver
- Firewall blockiert
- DNS-Name falsch
- Zielsystem ausgeschaltet
```

- maximale Sitzungsanzahl erreicht

Merksatz:

RDP-Fehler mit Erreichbarkeit,
Dienst,
Anmeldung
und Berechtigung prüfen.

Fehlerbild: RDP verbindet nicht

Mögliche Ursachen:

- Zielsystem offline
- falscher Hostname
- DNS falsch
- TCP 3389 blockiert
- Remote Desktop nicht aktiviert
- Firewall blockiert
- VPN nicht verbunden
- NAT oder Portweiterleitung falsch

Merksatz:

RDP-Verbindungsfehler zuerst mit Netzwerk und Port prüfen.

Fehlerbild: RDP Anmeldung wird abgelehnt

Mögliche Ursachen:

- Benutzername falsch
- Passwort falsch
- Benutzer nicht in erlaubter Gruppe
- Konto gesperrt
- Passwort abgelaufen
- Anmeldung per RDP verboten
- NLA-Kompatibilitätsproblem

```
- Domänencontroller nicht erreichbar
```

Merksatz:

```
RDP-Anmeldefehler mit Konto und Berechtigung prüfen.
```

Fehlerbild: RDP ist langsam

Mögliche Ursachen:

```
- geringe Bandbreite
- hohe Latenz
- Paketverlust
- hohe Bildschirmauflösung
- viele Grafikeffekte
- Drucker- oder Laufwerksumleitung
- Server überlastet
- VPN langsam
```

Merksatz:

```
RDP-Leistung hängt von Netzwerk,
Grafik
und Serverlast ab.
```

Telnet

Telnet ist ein älteres Protokoll für Fernzugriff auf eine Kommandozeile.

Typischer Port:

```
TCP 23
```

Problem:

```
Telnet ist unverschlüsselt.
```

Das bedeutet:

```
Benutzername,
Passwort
und Befehle
können im Klartext übertragen werden.
```

Merksatz:

```
Telnet ist unsicher,
weil es unverschlüsselt überträgt.
```

Warum Telnet heute vermeiden?

Telnet sollte für Administration möglichst nicht mehr verwendet werden.

Gründe:

```
- keine Verschlüsselung
- Passwörter im Klartext
- Befehle im Klartext
- leicht mitzulesen
- keine moderne Sicherheit
- hohes Risiko in unsicheren Netzwerken
```

Bessere Alternative:

```
SSH
```

Merksatz:

```
Telnet durch SSH ersetzen.
```

Telnet als Testwerkzeug

Obwohl Telnet als Administrationsprotokoll unsicher ist, wurde es früher oft als einfaches Testwerkzeug verwendet.

Beispiel:

Kann ich TCP-Port 25 erreichen?

Kann ich TCP-Port 80 erreichen?

Heute nutzt man dafür besser geeignete Werkzeuge.

Beispiele:

- nc
- Test-NetConnection
- openssl s_client
- curl

Merksatz:

Telnet nicht für sichere Administration verwenden.

SSH, RDP und Telnet vergleichen

Protokoll	Zweck	Port	Sicherheit
SSH	sichere Shell / Administration	TCP 22	verschlüsselt
RDP	grafischer Fernzugriff	TCP 3389	absichern, nicht offen ins Internet
Telnet	alte Shell / Fernzugriff	TCP 23	unverschlüsselt, vermeiden

Merksatz:

SSH für sichere Shell.

RDP für grafischen Zugriff.

Telnet vermeiden.

Remotezugriff und Authentifizierung

Remotezugriff braucht sichere Authentifizierung.

Möglichkeiten:

- Benutzername und Passwort
- SSH-Schlüssel
- Zertifikate
- Multi-Faktor-Authentifizierung
- Domänenkonto
- zentrale Identitätsdienste

Wichtig:

Je mächtiger der Zugriff,
desto stärker sollte die Absicherung sein.

Merksatz:

Fernzugriff braucht starke Authentifizierung.

Remotezugriff und Autorisierung

Nicht jeder angemeldete Benutzer darf automatisch alles.

Autorisierung bedeutet:

Welche Rechte hat der Benutzer?

Beispiele:

- darf sich per RDP anmelden
- darf sudo verwenden
- darf Server konfigurieren
- darf Dateien ändern
- darf Dienste neu starten

Merksatz:

Anmeldung ist nicht gleich Berechtigung.

Remotezugriff und Protokollierung

Remotezugriffe sollten protokolliert werden.

Wichtige Informationen:

- wer hat sich angemeldet
- wann wurde zugegriffen
- von welcher IP-Adresse
- welcher Dienst wurde genutzt
- war die Anmeldung erfolgreich
- welche Fehler sind aufgetreten

Logs helfen bei:

- Fehlersuche
- Sicherheitsanalyse
- Nachvollziehbarkeit
- Angriffserkennung

Merksatz:

Remotezugriffe müssen nachvollziehbar sein.

Remotezugriff und Firewall

Remotezugriffe sollten durch Firewalls eingeschränkt werden.

Beispiele:

SSH nur von Admin-Netz erlauben.
RDP nur über VPN erlauben.
Telnet blockieren.
Zugriff auf bestimmte IP-Adressen begrenzen.

Merksatz:

Remotezugriff nur für notwendige Quellen erlauben.

Remotezugriff und VPN

VPN ist eine wichtige Schutzmaßnahme für Remotezugriff.

Ablauf:

```
Benutzer verbindet sich per VPN ins interne Netz.
Danach nutzt er interne Dienste wie SSH oder RDP.
```

Vorteil:

```
Administrative Dienste müssen nicht direkt öffentlich erreichbar sein.
```

Merksatz:

```
VPN schützt interne Verwaltungszugänge.
```

Remotezugriff und Zero Trust

Zero Trust bedeutet vereinfacht:

```
keinem Zugriff automatisch vertrauen.
```

Auch interne Zugriffe werden geprüft.

Wichtige Prinzipien:

```
- Identität prüfen
- Gerät prüfen
- Rechte begrenzen
- Zugriff protokollieren
- nur notwendige Dienste freigeben
- MFA nutzen
```

Merksatz:

```
Zero Trust prüft jeden Zugriff bewusst.
```

Remotezugriff und Least Privilege

Auch beim Remotezugriff gilt:

```
nur notwendige Rechte vergeben.
```

Beispiel:

```
Ein Benutzer darf sich per SSH anmelden,
aber nicht automatisch Root-Rechte haben.
```

Oder:

```
Ein Support-Benutzer darf RDP nutzen,
aber keine Serverrollen ändern.
```

Merksatz:

```
Fernzugriff nur mit notwendigen Rechten erlauben.
```

Remotezugriff und Brute Force

Brute Force bedeutet:

```
Angreifer probiert viele Passwörter aus.
```

Besonders gefährdet:

```
öffentlich erreichbare SSH- oder RDP-Dienste.
```

Schutzmaßnahmen:

```
- starke Passwörter
- MFA
- Kontosperrung
- Fail2ban
- Rate Limiting
- VPN
- IP-Einschränkungen
```

- keine Standardbenutzer

Merksatz:

Öffentliche Remotezugänge sind Brute-Force-Ziele.

Remotezugriff und Updates

Remotezugriffsprotokolle und Zielsysteme müssen aktuell gehalten werden.

Warum?

Schwachstellen in Remotezugriffsdiensten können besonders kritisch sein.

Beispiele für Risiken:

- unautorisierter Zugriff
- Rechteausweitung
- Remote Code Execution
- Ransomware-Einstieg

Merksatz:

Remotezugriffsdienste müssen regelmäßig gepatcht werden.

Fehlersuche bei Remotezugriff

Eine sinnvolle Reihenfolge:

1. Zielname richtig?
2. DNS-Auflösung korrekt?
3. Ziel-IP erreichbar?
4. Richtiger Port erreichbar?
5. Dienst läuft?
6. Firewall erlaubt Zugriff?
7. Benutzer darf sich anmelden?
8. Authentifizierung korrekt?

9. Berechtigungen korrekt?

10. Logs prüfen.

Merksatz:

Remotezugriff nach DNS,
IP,
Port,
Dienst,
Anmeldung
und Rechten prüfen.

Typische Prüfpunkte nach Protokoll

Protokoll	Prüfpunkte
SSH	TCP 22, SSH-Dienst, Benutzer, Schlüssel, Host-Key, Firewall
RDP	TCP 3389, Remote Desktop aktiv, Benutzerrechte, NLA, VPN, Firewall
Telnet	TCP 23, Dienst aktiv, aber möglichst vermeiden
SFTP	TCP 22, SSH-Zugang, SFTP-Rechte
RD Gateway	HTTPS-Zugriff, Richtlinien, Zertifikat, Benutzerrechte

Merksatz:

Jedes Remoteprotokoll hat eigene typische Fehlerquellen.

Was Remotezugriffsprotokolle nicht machen

Remotezugriffsprotokolle machen nicht automatisch:

- Benutzer sicher berechtigen
- Angriffe verhindern
- Updates einspielen
- Logs auswerten
- MFA erzwingen
- Firewall korrekt konfigurieren
- unsichere Passwörter verhindern

- Datenschutz automatisch sicherstellen

Remotezugriff braucht immer ein Sicherheitskonzept.

Merksatz:

> Remotezugriff ist mächtig
> und muss bewusst abgesichert werden.

Einordnung in das OSI-Modell

Thema	Schicht
SSH	7
RDP	7
Telnet	7
SFTP	7 über SSH
TCP 22	4
TCP 23	4
TCP 3389	4
IP-Adresse	3
DNS-Name	7
Verschlüsselung bei SSH	Sicherheits-/Darstellungsbezug
Benutzeranmeldung	7

Merksatz:

> SSH, RDP und Telnet sind Schicht-7-Protokolle,
> ihre Ports liegen auf Schicht 4.

Typische Ports

Protokoll	Port	Zweck
SSH	TCP 22	sichere Shell / Administration
SFTP	TCP 22	Dateiübertragung über SSH
Telnet	TCP 23	alte unverschlüsselte Shell

Protokoll	Port	Zweck
RDP	TCP 3389	grafischer Fernzugriff
RD Gateway	TCP 443	RDP über Gateway / HTTPS

Merksatz:

```
SSH 22,
Telnet 23,
RDP 3389.
```

Typische IHK-Fragen

In AP1 und AP2 kann zum Beispiel gefragt werden:

```
- Wofür steht SSH?
- Wofür wird SSH verwendet?
- Welchen Port nutzt SSH typischerweise?
- Warum ist SSH sicherer als Telnet?
- Was ist ein SSH-Host-Key?
- Was ist SSH-Schlüsselauthentifizierung?
- Wofür steht RDP?
- Wofür wird RDP genutzt?
- Welchen Port nutzt RDP typischerweise?
- Warum sollte RDP nicht offen im Internet stehen?
- Was ist NLA?
- Wofür steht Telnet?
- Warum gilt Telnet als unsicher?
- Welche Sicherheitsmaßnahmen sind bei Remotezugriff sinnvoll?
- Wie grenzt man Remotezugriffsfehler systematisch ein?
```

Typische Prüfungsfallen

```
SSH gehört zu Schicht 7.

SSH nutzt typischerweise TCP 22.

SSH ist verschlüsselt.
```

SFTP läuft über SSH.

SSH-Host-Key identifiziert den Server.

Privater SSH-Schlüssel muss geheim bleiben.

RDP gehört zu Schicht 7.

RDP nutzt typischerweise TCP 3389.

RDP ist grafischer Fernzugriff.

RDP sollte nicht direkt offen ins Internet.

VPN oder RD Gateway sind bessere Schutzmaßnahmen.

NLA verbessert RDP-Sicherheit.

Telnet gehört zu Schicht 7.

Telnet nutzt typischerweise TCP 23.

Telnet ist unverschlüsselt.

Telnet sollte durch SSH ersetzt werden.

Port erreichbar heißt nicht automatisch:
Anmeldung erlaubt.

Anmeldung erfolgreich heißt nicht automatisch:
ausreichende Rechte vorhanden.

Wichtige Begriffe kurz erklärt

Begriff	Kurze Erklärung
Remotezugriff	Zugriff auf ein entferntes System
Fernadministration	Verwaltung eines Systems aus der Ferne
SSH	Secure Shell

Begriff	Kurze Erklärung
SSH-Client	startet SSH-Verbindung
SSH-Server	nimmt SSH-Verbindung an
Host-Key	identifiziert SSH-Server
SSH-Schlüssel	Schlüsselpaar zur Anmeldung
privater Schlüssel	geheimer Teil des Schlüssels
öffentlicher Schlüssel	Teil, der auf dem Server liegen darf
Passphrase	Schutz für privaten Schlüssel
SSH-Tunnel	verschlüsselte Weiterleitung über SSH
SFTP	Dateiübertragung über SSH
RDP	Remote Desktop Protocol
NLA	Network Level Authentication
RD Gateway	Gateway für RDP-Zugriffe
Telnet	altes unverschlüsseltes Fernzugriffsprotokoll
Brute Force	massenhaftes Ausprobieren von Passwörtern
Least Privilege	nur notwendige Rechte vergeben
MFA	Multi-Faktor-Authentifizierung

IHK-sichere Kurzformulierung

SSH, RDP und Telnet sind Protokolle der Anwendungsschicht für Remotezugriff und Fernadministration. SSH steht für Secure Shell, nutzt typischerweise TCP-Port 22 und ermöglicht verschlüsselten Zugriff auf eine Kommandozeile sowie Dateiübertragung über SFTP. RDP steht für Remote Desktop Protocol, nutzt typischerweise TCP-Port 3389 und ermöglicht grafischen Fernzugriff, besonders auf Windows-Systeme. Telnet nutzt typischerweise TCP-Port 23, überträgt Daten unverschlüsselt und sollte für Administration durch SSH ersetzt werden. Remotezugriffe müssen durch starke Authentifizierung, passende Berechtigungen, Firewall-Regeln, VPN oder Gateway-Lösungen und Protokollierung abgesichert werden.

Merksätze

```
Remotezugriff gehört zu Schicht 7.

SSH = Secure Shell.

SSH nutzt typischerweise TCP 22.
```

SSH ist verschlüsselt.

SSH dient sicherer Fernadministration.

SFTP läuft über SSH.

SSH-Host-Key identifiziert den Server.

Privater SSH-Schlüssel bleibt geheim.

RDP = Remote Desktop Protocol.

RDP nutzt typischerweise TCP 3389.

RDP = grafischer Fernzugriff.

RDP nicht direkt ungeschützt ins Internet öffnen.

RDP besser über VPN oder Gateway nutzen.

NLA verbessert RDP-Sicherheit.

Telnet nutzt typischerweise TCP 23.

Telnet ist unverschlüsselt.

Telnet durch SSH ersetzen.

Port offen heißt nicht:
Anmeldung erfolgreich.

Anmeldung erfolgreich heißt nicht:
ausreichende Rechte.

Remotezugriff braucht starke Authentifizierung.

Remotezugriff braucht Least Privilege.

Remotezugriff braucht Logs.

Remotezugriff braucht Firewall-Regeln.

Remotezugriff ist mächtig

und sicherheitskritisch.v