12.4 Systematische Netzwerkfehlersuche nach dem OSI-Modell

Netzwerkfehlersuche sollte nicht zufällig erfolgen.

Besser ist ein systematisches Vorgehen nach Schichten.

Das OSI-Modell hilft dabei, Fehler Schritt für Schritt einzugrenzen.

Grundidee:

```
erst einfache Grundlagen prüfen
dann höhere Schichten prüfen
Fehler sauber eingrenzen
Messergebnisse dokumentieren
nicht vorschnell raten
```

Merksatz:

```
Systematische Fehlersuche spart Zeit und verhindert falsche Vermutungen.
```

Warum nach Schichten prüfen?

Viele Fehler sehen ähnlich aus.

Beispiel:

```
Webseite öffnet nicht.
```

Mögliche Ursachen können sein:

```
Kabel defekt
WLAN getrennt
falsches VLAN
falsche IP-Adresse
Gateway fehlt
DNS falsch
Port blockiert
```

```
Zertifikat ungültig
Webserver down
Benutzer nicht berechtigt
```

Ohne Struktur sucht man schnell an der falschen Stelle.

Merksatz:

```
Ein Symptom kann viele Ursachen auf verschiedenen Schichten haben.
```

Top-Down und Bottom-Up

Es gibt zwei typische Vorgehensweisen:

```
Bottom-Up
Top-Down
```

Bottom-Up bedeutet:

```
Man beginnt unten bei Schicht 1
und arbeitet sich nach oben.
```

Top-Down bedeutet:

```
Man beginnt bei der Anwendung
und arbeitet sich nach unten.
```

Beide Methoden sind sinnvoll, je nach Fehlerbild.

Merksatz:

```
Bottom-Up beginnt beim Kabel.
Top-Down beginnt bei der Anwendung.
```

Bottom-Up-Methode

Bottom-Up prüft von unten nach oben:

```
Schicht 1:
Kabel, Link, Signal

Schicht 2:
MAC, Switch, VLAN

Schicht 3:
IP, Subnetz, Gateway, Routing

Schicht 4:
TCP, UDP, Ports

Schicht 5–7:
Sitzung, Darstellung, Anwendung
```

Vorteil:

```
grundlegende Fehler werden früh erkannt.
```

Merksatz:

```
Bottom-Up ist gut,
wenn unklar ist,
ob überhaupt Netzverbindung besteht.
```

Top-Down-Methode

Top-Down beginnt bei der Anwendung.

Beispiel:

```
Benutzer sagt:
E-Mail funktioniert nicht.
```

Dann prüft man zuerst:

```
Mailclient
Anmeldung
```

```
Fehlermeldung
Servername
Protokoll
Port
DNS
Netzwerk
```

Vorteil:

```
schneller,
wenn der Fehler klar an einem Dienst hängt.
```

Merksatz:

```
Top-Down ist gut,
wenn ein bestimmter Dienst betroffen ist.
```

Divide-and-Conquer-Methode

Divide and Conquer bedeutet:

```
Problem in der Mitte eingrenzen.
```

Man prüft zuerst eine mittlere Schicht, zum Beispiel IP-Erreichbarkeit oder Port-Erreichbarkeit.

Beispiel:

```
Ping zum Server funktioniert.
```

Dann weiß man:

```
Schicht 1 bis 3 sind wahrscheinlich grundsätzlich ok.
```

Dann prüft man weiter:

```
Port
Dienst
```

```
Anmeldung
Anwendung
```

Merksatz:

```
Divide and Conquer halbiert den Suchbereich.
```

Vergleichsmethode

Bei der Vergleichsmethode vergleicht man:

```
funktionierendes System
mit
fehlerhaftem System
```

Beispiele:

```
anderer Client funktioniert
anderer Benutzer funktioniert
anderes VLAN funktioniert
anderer Browser funktioniert
anderer DNS-Server liefert andere Antwort
```

Dadurch erkennt man Unterschiede.

Merksatz:

```
Vergleich zeigt,
was beim fehlerhaften Fall anders ist.
```

Fehler reproduzieren

Ein Fehler sollte möglichst reproduzierbar gemacht werden.

Fragen:

```
Wann tritt der Fehler auf?
Bei welchem Benutzer?
```

Bei welchem Client?
Bei welchem Dienst?
Seit wann?
Nach welcher Änderung?
Immer oder nur manchmal?
Intern oder extern?
Mit WLAN oder LAN?
Mit VPN oder ohne VPN?

Merksatz:

Nur reproduzierbare Fehler lassen sich sauber messen.

Fehlerbild genau aufnehmen

Vor der Analyse sollte man das Fehlerbild genau aufnehmen.

Nicht ausreichend:

Internet geht nicht.

Besser:

Benutzer kann https://intranet.firma.local öffnen,
aber https://portal.firma.de nicht.
Fehler im Browser:
DNS_PROBE_FINISHED_NXDOMAIN.

Noch besser:

Zeitpunkt,
Client-IP,
Benutzer,
DNS-Server,
Fehlermeldung,
betroffener Dienst.

Merksatz:

Genaue Fehlerbeschreibung ist Teil der Diagnose.

W-Fragen bei Netzwerkfehlern

Wichtige Fragen:

Wer ist betroffen?
Was funktioniert nicht?
Wann tritt der Fehler auf?
Wo tritt der Fehler auf?
Wie äußert sich der Fehler?
Seit wann besteht der Fehler?
Was wurde zuletzt geändert?
Welche Systeme funktionieren noch?

Merksatz:

Gute Fragen grenzen den Fehler ein.

Einzelner Benutzer oder alle Benutzer?

Wenn nur ein Benutzer betroffen ist, prüft man eher:

Benutzerkonto
Berechtigungen
Passwort
MFA
Clientprofil
lokale Einstellungen
Browsercache
gespeicherte Zugangsdaten

Wenn alle Benutzer betroffen sind, prüft man eher:

Dienst
Server
DNS

Netzwerk
Firewall
Zertifikat
zentrale Authentifizierung
Provider
Infrastruktur

Merksatz:

Einzelner Benutzer = Konto oder Client.
Alle Benutzer = Dienst oder Infrastruktur.

Ein Client oder mehrere Clients?

Wenn nur ein Client betroffen ist, prüft man:

Netzwerkkabel
WLAN
IP-Konfiguration
DNS-Einstellungen
lokale Firewall
Proxy
VPN
Zertifikatsspeicher
lokale Software

Wenn mehrere Clients betroffen sind, prüft man:

Switch
VLAN
DHCP
DNS
Gateway
Firewall
Server
zentrale Dienste

Merksatz:

Ein Client betroffen:
lokal prüfen.
Viele Clients betroffen:
Infrastruktur prüfen.

Intern oder extern betroffen?

Wenn intern alles funktioniert, extern aber nicht, prüft man:

externe DNS-Auflösung
öffentliche IP
NAT
Firewall WAN → DMZ
Provider
CGNAT
Zertifikat
Reverse Proxy

Wenn extern funktioniert, intern aber nicht, prüft man:

internes DNS
Split DNS
Hairpin NAT
interne Firewall
interne Route
Proxy-Einstellungen

Merksatz:

Interne und externe Sicht getrennt prüfen.

Nur WLAN oder auch LAN?

Wenn nur WLAN betroffen ist, prüft man:

WLAN-Signal
SSID

WLAN-Passwort
VLAN-Zuordnung am Access Point
DHCP im WLAN-Netz
Roaming
Störungen
Access Point
Client-Treiber

Wenn LAN auch betroffen ist, liegt die Ursache eher bei:

IP-Konfiguration
Gateway
DNS
Firewall
Dienst
zentraler Infrastruktur

Merksatz:

WLAN-Fehler nicht automatisch als Internetfehler behandeln.

Nur ein VLAN betroffen?

Wenn nur ein VLAN betroffen ist, prüft man:

VLAN-ID
Switchport-Modus
Tagged oder Untagged
Trunk
Access-Port
DHCP-Scope
Gateway für VLAN
Firewall-Regeln
Routing
ACLs

Merksatz:

```
VLAN-bezogene Fehler sind oft Schicht 2 und 3.
```

Nur ein Dienst betroffen?

Wenn nur ein Dienst betroffen ist, prüft man eher:

```
DNS-Name des Dienstes
Ziel-IP
Port
Protokoll
Firewall-Regel
Dienststatus
Zertifikat
Authentifizierung
Berechtigung
Anwendungslogs
```

Beispiel:

```
Internet funktioniert,
aber SMB-Freigabe nicht.
```

Dann ist nicht das ganze Netzwerk down, sondern ein Dienst oder Zugriffspfad gestört.

Merksatz:

```
Ein Dienst betroffen:
Dienstkette prüfen.
```

Schicht 1 prüfen

Schicht 1 ist die Bitübertragungsschicht.

Prüfpunkte:

```
Kabel steckt?
Link-LED aktiv?
richtiger Port?
```

Netzteil aktiv?
SFP-Modul korrekt?
Glasfaser richtig gesteckt?
WLAN-Signal vorhanden?
keine physische Beschädigung?
Duplex oder Speed auffällig?

Werkzeuge:

Sichtprüfung
Linkstatus
Kabeltester
Switchport-Status
WLAN-Signalprüfung

Merksatz:

Ohne funktionierende Schicht 1 funktioniert darüber nichts.

Schicht 2 prüfen

Schicht 2 ist die Sicherungsschicht.

Prüfpunkte:

MAC-Adresse sichtbar?
Switchport aktiv?
VLAN korrekt?
Access oder Trunk richtig?
MAC-Adresstabelle passend?
STP blockiert?
Broadcast-Sturm?
ARP funktioniert?
keine doppelte IP im lokalen Netz?

Werkzeuge:

```
Switch-MAC-Tabelle
ARP-Tabelle
VLAN-Konfiguration
Wireshark
Switch-Logs
```

Merksatz:

```
Schicht 2 betrifft lokale Kommunikation im richtigen Netzsegment.
```

Schicht 3 prüfen

Schicht 3 ist die Vermittlungs- oder Netzwerkschicht.

Prüfpunkte:

```
IP-Adresse korrekt?
Subnetzmaske korrekt?
Gateway korrekt?
Routing korrekt?
Zielnetz erreichbar?
keine APIPA-Adresse?
keine doppelte IP?
IPv4 oder IPv6 korrekt?
Rückweg vorhanden?
```

Werkzeuge:

```
ipconfig
ifconfig
ip addr
ping
traceroute / tracert
route print
ip route
Routingtabelle
```

Merksatz:

```
Schicht 3 beantwortet:
Komme ich zum richtigen Netz?
```

Schicht 4 prüfen

Schicht 4 ist die Transportschicht.

Prüfpunkte:

```
TCP oder UDP?
richtiger Port?
Port offen?
Dienst lauscht?
Firewall blockiert?
TCP-Handshake vollständig?
UDP-Antwort vorhanden?
NAT oder PAT beteiligt?
Rückweg korrekt?
```

Werkzeuge:

```
nc
Test-NetConnection
ss
netstat
tcpdump
Wireshark
Firewall-Logs
```

Merksatz:

```
Schicht 4 beantwortet:
Ist der Dienstport erreichbar?
```

Schicht 5 prüfen

Schicht 5 ist die Sitzungsschicht.

Prüfpunkte:

```
Session wird aufgebaut?
Session bleibt bestehen?
Benutzer wird ständig ausgeloggt?
Cookie korrekt?
Session Timeout?
Load Balancer mit Session-Stickiness?
Session-Speicher erreichbar?
```

Typische Fehler:

```
Login-Schleife
Session läuft sofort ab
Warenkorb wird vergessen
Remote-Sitzung bricht ab
```

Merksatz:

```
Schicht 5 betrifft Sitzungen und deren Verwaltung.
```

Schicht 6 prüfen

Schicht 6 ist die Darstellungsschicht.

Prüfpunkte:

```
TLS korrekt?
Zertifikat gültig?
Name passt zum Zertifikat?
CA vertrauenswürdig?
Datenformat korrekt?
Zeichencodierung korrekt?
Kompression korrekt?
JSON oder XML gültig?
```

Typische Fehler:

```
Zertifikatswarnung
falsche Umlaute
ungültiges JSON
TLS-Handshake-Fehler
falscher Content-Type
```

Merksatz:

```
Schicht 6 betrifft Darstellung,
Codierung,
Kompression
und Verschlüsselung.
```

Schicht 7 prüfen

Schicht 7 ist die Anwendungsschicht.

Prüfpunkte:

```
Dienst läuft?
richtige URL?
richtiger Hostname?
richtige Methode?
richtiger Statuscode?
Anmeldung korrekt?
Berechtigung vorhanden?
Anwendung antwortet?
API korrekt?
Logs vorhanden?
Backend erreichbar?
```

Typische Fehler:

```
HTTP 404
HTTP 500
Login fehlgeschlagen
Zugriff verweigert
DNS falsch
```

```
Mail kommt nicht an
API antwortet mit Fehler
```

Merksatz:

```
Schicht 7 betrifft den konkreten Dienst und seine Antwort.
```

DNS als häufiger Sonderfall

DNS gehört zur Anwendungsschicht, wirkt aber auf fast alle anderen Dienste.

Wenn DNS falsch ist, sucht man oft am falschen Ziel.

Typische DNS-Fehler:

```
falsche IP-Adresse
NXDOMAIN
falscher DNS-Server
Split DNS falsch
veralteter Cache
IPv6-Antwort nicht erreichbar
MX-Record falsch
```

Merksatz:

```
DNS immer früh prüfen,
wenn Namen verwendet werden.
```

DHCP als häufiger Sonderfall

DHCP gehört zur Anwendungsschicht, liefert aber Schicht-3-Konfiguration.

DHCP-Fehler führen zu:

```
keiner IP-Adresse
APIPA 169.254.x.x
falschem Gateway
falschem DNS
```

falschem VLAN
falscher Lease

Merksatz:

DHCP-Fehler wirken wie IP- oder Internetprobleme.

Firewall als häufiger Sonderfall

Firewalls können mehrere Schichten betreffen.

Je nach Firewall prüft sie:

IP-Adressen
Ports
Protokolle
Zustand
Anwendung
Benutzer
Zonen

Bei Firewall-Verdacht prüfen:

Quelle
Ziel
Port
Protokoll
Richtung
Zone
Regel
Logs
NAT
Rückweg

Merksatz:

Firewall-Fehler mit Quelle,
Ziel,

```
Port,
Richtung
und Logs prüfen.
```

NAT als häufiger Sonderfall

NAT kann IP-Adressen und Ports verändern.

Deshalb muss man wissen:

```
Welche Adresse sieht der Client?
Welche Adresse sieht der Server?
Gibt es Source NAT?
Gibt es Destination NAT?
Gibt es PAT?
Gibt es Portweiterleitung?
Stimmt der Rückweg?
```

Merksatz:

```
Bei NAT immer vor und nach der Übersetzung denken.
```

Logs immer einbeziehen

Logs liefern oft die entscheidenden Hinweise.

Wichtige Logs:

```
Client-Logs
Server-Logs
Firewall-Logs
DNS-Logs
DHCP-Logs
Webserver-Logs
Reverse-Proxy-Logs
Authentifizierungslogs
VPN-Logs
Ereignisanzeige
```

```
journalctl
```

Merksatz:

```
Logs zeigen Entscheidungen,
Mitschnitte zeigen Verkehr.
```

Paketmitschnitt gezielt einsetzen

Ein Paketmitschnitt ist besonders hilfreich, wenn unklar ist:

```
ob Pakete ankommen
ob Antworten zurückkommen
ob DNS korrekt gefragt wird
ob TCP-Handshake klappt
ob UDP-Antworten kommen
ob NAT richtig arbeitet
ob Retransmissions auftreten
ob Reset oder Timeout entsteht
```

Merksatz:

```
Mitschnitt nutzen,
wenn der echte Verkehr unklar ist.
```

Fehler nach Änderung

Viele Störungen entstehen nach Änderungen.

Beispiele:

```
Firewall-Regel geändert
DNS-Eintrag geändert
DHCP-Scope geändert
VLAN geändert
Zertifikat erneuert
Server-IP geändert
Dienst aktualisiert
```

```
Reverse Proxy angepasst
Passwort oder Rechte geändert
VPN-Konfiguration geändert
```

Merksatz:

```
Nach Änderung zuerst die Änderung prüfen.
```

Change und Rollback

Bei Änderungen sollte vorher klar sein:

```
Was wird geändert?
Warum wird es geändert?
Wer ist verantwortlich?
Wann wird getestet?
Wie wird zurückgerollt?
Welche Systeme sind betroffen?
Gibt es ein Backup?
Gibt es Dokumentation?
```

Rollback bedeutet:

```
Änderung zurücknehmen,
wenn sie Probleme verursacht.
```

Merksatz:

```
Keine kritische Änderung ohne Rückweg.
```

Dokumentation während der Fehlersuche

Während der Fehlersuche sollte man dokumentieren:

```
Fehlerbild
Zeitpunkt
betroffene Systeme
```

betroffene Benutzer
getestete Schritte
Messergebnisse
Logs
Änderungen
gefundene Ursache
Lösung
offene Punkte

Merksatz:

Gute Dokumentation verhindert doppelte Arbeit.

Hypothesen bilden

Eine Hypothese ist eine fachliche Vermutung, die getestet wird.

Beispiel:

Hypothese:
DNS zeigt auf falsche IP.

Test:

nslookup oder dig ausführen.

Ergebnis:

Wenn DNS falsch ist,
Hypothese bestätigt.

Wenn nicht:

Hypothese verwerfen
und nächste Ursache prüfen.

Merksatz:

```
Hypothesen müssen getestet,
nicht geglaubt werden.
```

Nicht mehrere Dinge gleichzeitig ändern

Wenn man mehrere Dinge gleichzeitig ändert, weiß man später nicht, welche Änderung geholfen oder geschadet hat.

Besser:

```
eine Änderung durchführen
testen
Ergebnis dokumentieren
nächste Änderung durchführen
```

Merksatz:

```
Eine Änderung pro Testschritt.
```

Workaround und Ursachenbehebung unterscheiden

Ein Workaround umgeht ein Problem vorübergehend.

Eine Ursachenbehebung beseitigt die Ursache.

Beispiel:

```
Workaround:
Benutzer nutzt IP-Adresse statt DNS-Namen.

Ursache:
DNS-Eintrag ist falsch.
```

Die Ursache muss trotzdem behoben werden.

Merksatz:

```
Workaround ist nicht automatisch Lösung.
```

Typische Fehlerbilder und erste Einordnung

Fehlerbild	erste Vermutung
Kein Link	Schicht 1
IP 169.254.x.x	DHCP-Problem
Gateway nicht erreichbar	Schicht 2 / 3
Name löst nicht auf	DNS
Ping geht, Port nicht	Schicht 4 / Firewall / Dienst
Port offen, HTTP 500	Anwendung / Backend
Zertifikatswarnung	TLS / Zeit / Name
Zugriff verweigert	Autorisierung
Login schlägt fehl	Authentifizierung
Nur extern gestört	NAT / Firewall / DNS extern
Nur intern gestört	DNS intern / Hairpin NAT / Routing

Merksatz:

> Fehlerbild gibt Hinweis,
> aber noch keinen Beweis.

Beispiel: Webseite öffnet nicht

Systematische Prüfung:

1. URL korrekt?
2. DNS löst korrekt auf?
3. Ziel-IP erreichbar?
4. TCP 443 erreichbar?
5. TLS-Zertifikat gültig?
6. HTTP-Statuscode prüfen.
7. Reverse Proxy prüfen.
8. Backend prüfen.
9. Webserver-Logs prüfen.
10. Firewall-Logs prüfen.

Merksatz:

Webfehler mit DNS,
Port,
TLS,
HTTP
und Logs prüfen.

Beispiel: Client bekommt keine IP-Adresse

Systematische Prüfung:

1. Link vorhanden?
2. VLAN korrekt?
3. DHCP Discover sichtbar?
4. DHCP Offer sichtbar?
5. DHCP-Scope frei?
6. DHCP-Relay korrekt?
7. Firewall erlaubt UDP 67/68?
8. Richtiger DHCP-Server?
9. Keine Rogue-DHCP-Antwort?
10. Client erhält Lease?

Merksatz:

DHCP-Fehler mit DORA eingrenzen.

Beispiel: Server per SSH nicht erreichbar

Systematische Prüfung:

1. Ziel-IP oder DNS prüfen.
2. Routing prüfen.
3. TCP 22 erreichbar?
4. SSH-Dienst läuft?
5. Host-Firewall erlaubt?
6. zentrale Firewall erlaubt?
7. Benutzer oder Schlüssel korrekt?
8. SSH-Logs prüfen.

9. Fail2ban oder Sperre prüfen.
10. Host-Key-Warnung prüfen.

Merksatz:

SSH-Fehler mit Netz,
Port,
Dienst,
Benutzer
und Logs prüfen.

Beispiel: SMB-Freigabe Zugriff verweigert

Systematische Prüfung:

1. Servername löst korrekt auf?
2. TCP 445 erreichbar?
3. SMB-Dienst läuft?
4. Benutzer korrekt angemeldet?
5. Freigabeberechtigung korrekt?
6. Dateisystemberechtigung korrekt?
7. Gruppenmitgliedschaft korrekt?
8. gespeicherte Anmeldedaten falsch?
9. Datei gesperrt?
10. Logs prüfen.

Merksatz:

SMB-Zugriff braucht Verbindung,
Anmeldung
und Rechte.

Beispiel: E-Mail kommt nicht an

Systematische Prüfung:

1. Absender erhält Fehlermeldung?
2. MX-Record korrekt?
3. DNS korrekt?
4. SMTP TCP 25 erreichbar?
5. Mailserver zuständig?
6. Spamfilter oder Quarantäne?
7. SPF, DKIM, DMARC korrekt?
8. Postfach voll?
9. TLS-Problem?
10. Mailserver-Logs prüfen.

Merksatz:

Mailfehler mit DNS,
SMTP,
Authentifizierung,
Spamfilter
und Logs prüfen.

Beispiel: VPN verbunden, aber interne Systeme nicht erreichbar

Systematische Prüfung:

1. VPN-Verbindung wirklich aktiv?
2. VPN-IP erhalten?
3. Route ins interne Netz vorhanden?
4. DNS für interne Namen korrekt?
5. Firewall-Regel VPN → Zielnetz korrekt?
6. Benutzergruppe berechtigt?
7. Split Tunnel korrekt?
8. Zielsystem-Firewall erlaubt?
9. Rückweg korrekt?
10. Logs prüfen.

Merksatz:

VPN braucht Tunnel,
Adresse,

```
Route,
DNS,
Firewall
und Rechte.
```

Beispiel: Nur langsam, nicht komplett kaputt

Bei Performanceproblemen prüft man zusätzlich:

```
Latenz
Paketverlust
Bandbreite
Duplex
WLAN-Signal
Retransmissions
Serverlast
DNS-Verzögerungen
MTU
Proxy
VPN
Speicher und CPU
Festplatten-I/O
```

Merksatz:

```
Langsam ist nicht dasselbe wie nicht erreichbar.
```

Latenz

Latenz ist die Verzögerung, bis Daten ihr Ziel erreichen und eine Antwort zurückkommt.

Hohe Latenz stört besonders:

```
VoIP
Videokonferenzen
Remote Desktop
Online-Anwendungen
Datenbankzugriffe
```

interaktive Anwendungen

Merksatz:

Latenz = Verzögerung.

Paketverlust

Paketverlust bedeutet:

Pakete gehen unterwegs verloren.

Folgen:

Verbindungen werden langsam.
TCP sendet erneut.
Audio oder Video stottert.
VPN wird instabil.
Webseiten laden unvollständig.

Hinweise:

Retransmissions
verlorene Ping-Antworten
Abbrüche
Timeouts

Merksatz:

Paketverlust erzeugt Wiederholungen und Instabilität.

Bandbreite

Bandbreite beschreibt, wie viele Daten pro Zeit übertragen werden können.

Geringe Bandbreite führt zu:

```
langsamen Downloads
ruckelnden Streams
langen Backups
langsamer Dateiübertragung
Engpässen bei vielen Benutzern
```

Merksatz:

```
Bandbreite = maximale Datenmenge pro Zeit.
```

Jitter

Jitter ist die Schwankung der Verzögerung.

Besonders störend bei:

```
VoIP
Videokonferenzen
Echtzeitanwendungen
Streaming
Remote-Zugriff
```

Merksatz:

```
Jitter = schwankende Latenz.
```

MTU

MTU steht für:

```
Maximum Transmission Unit
```

MTU beschreibt, wie groß ein Paket auf einem Übertragungsweg maximal sein darf.

MTU-Probleme können verursachen:

```
Webseiten laden teilweise.
VPN ist instabil.
große Downloads brechen ab.
kleine Pings funktionieren,
große Pakete nicht.
```

Merksatz:

```
MTU-Probleme zeigen sich oft erst bei größeren Paketen.
```

Fehlerklasse: Erreichbarkeit

Erreichbarkeitsfehler bedeuten:

```
Ziel ist gar nicht oder nur teilweise erreichbar.
```

Prüfen:

```
Link
IP
Gateway
Routing
Firewall
NAT
Port
Dienst
```

Merksatz:

```
Erreichbarkeit zuerst technisch eingrenzen.
```

Fehlerklasse: Namensauflösung

Namensauflösungsfehler bedeuten:

```
Name wird nicht oder falsch aufgelöst.
```

Prüfen:

```
DNS-Server
DNS-Record
DNS-Suffix
Split DNS
Cache
A/AAAA
CNAME
MX
interne und externe Antwort
```

Merksatz:

```
Name falsch bedeutet oft Ziel falsch.
```

Fehlerklasse: Authentifizierung

Authentifizierungsfehler bedeuten:

```
Identität wird nicht akzeptiert.
```

Prüfen:

```
Benutzername
Passwort
MFA
Konto gesperrt
Konto deaktiviert
Zertifikat
Token
Zeit
LDAP/AD/IdP
```

Merksatz:

```
Authentifizierung = Wer bist du?
```

Fehlerklasse: Autorisierung

Autorisierungsfehler bedeuten:

```
Identität ist bekannt,
aber Rechte fehlen.
```

Prüfen:

```
Gruppen
Rollen
Freigaberechte
Dateisystemrechte
API-Scopes
Richtlinien
Mandant
alte Session
```

Merksatz:

```
Autorisierung = Was darfst du?
```

Fehlerklasse: Anwendung

Anwendungsfehler bedeuten:

```
Netzwerkverbindung besteht,
aber der Dienst funktioniert nicht korrekt.
```

Prüfen:

```
Logs
Statuscodes
Backend
Datenbank
Konfiguration
Version
Abhängigkeiten
```

```
Speicher
CPU
Berechtigungen
Datenformat
```

Merksatz:

```
Wenn Netzwerk steht,
aber Dienst fehlerhaft antwortet,
Anwendung prüfen.
```

Fehlerklasse: Sicherheit

Sicherheitsmechanismen können Verkehr bewusst blockieren.

Beispiele:

```
Firewall
IDS/IPS
WAF
Antivirus
EDR
Spamfilter
Proxy
MFA
Conditional Access
Geoblocking
Rate Limiting
```

Merksatz:

```
Nicht jede Blockierung ist ein Fehler,
manchmal ist sie gewollt.
```

Abschluss einer Fehlersuche

Am Ende sollte klar sein:

Was war die Ursache?
Wie wurde sie nachgewiesen?
Was wurde geändert?
Welche Systeme waren betroffen?
Wie wurde getestet?
Ist die Lösung dauerhaft?
Muss dokumentiert werden?
Muss Monitoring angepasst werden?
Muss Prävention verbessert werden?

Merksatz:

Eine Fehlersuche endet mit Ursache,
Lösung
und Dokumentation.

Typische IHK-Fragen

In AP1 und AP2 kann zum Beispiel gefragt werden:

- Warum hilft das OSI-Modell bei der Fehlersuche?
- Was bedeutet Bottom-Up-Fehlersuche?
- Was bedeutet Top-Down-Fehlersuche?
- Was ist Divide and Conquer bei der Fehlersuche?
- Warum muss man Fehler genau eingrenzen?
- Warum reicht „Internet geht nicht“ nicht als Fehlerbeschreibung?
- Welche Schichten prüft man bei fehlender Verbindung?
- Warum prüft man DNS frühzeitig?
- Warum sind Logs wichtig?
- Warum sollte man nicht mehrere Dinge gleichzeitig ändern?
- Was ist ein Workaround?
- Was ist der Unterschied zwischen Authentifizierung und Autorisierung?
- Wie geht man bei einem Webfehler systematisch vor?
- Wie geht man bei DHCP-Problemen systematisch vor?
- Wie geht man bei VPN-Problemen systematisch vor?

Typische Prüfungsfallen

Nicht sofort die Firewall beschuldigen.

Nicht nur ping testen.

Nicht nur Port testen.

DNS kann viele Fehler verursachen.

DHCP gehört zu Schicht 7,
wirkt aber auf Schicht 3.

Firewall kann mehrere Schichten betreffen.

NAT verändert Adressen und Ports.

Ein einzelner Benutzer deutet oft auf Konto oder Client.

Alle Benutzer deuten eher auf zentrale Infrastruktur.

Intern und extern getrennt prüfen.

WLAN und LAN getrennt prüfen.

Authentifizierung ist nicht Autorisierung.

Workaround ist nicht Ursachenbehebung.

Eine Änderung pro Testschritt.

Nach Änderung zuerst Änderung prüfen.

Logs und Mitschnitt ergänzen sich.

Langsam ist ein anderes Fehlerbild als nicht erreichbar.

Wichtige Begriffe kurz erklärt

Begriff	Kurze Erklärung
Fehlersuche	systematisches Finden einer Ursache

Begriff	Kurze Erklärung
Bottom-Up	von Schicht 1 nach oben prüfen
Top-Down	von Anwendung nach unten prüfen
Divide and Conquer	Suchbereich durch mittlere Prüfung eingrenzen
Vergleichsmethode	funktionierenden und fehlerhaften Fall vergleichen
Fehlerbild	beobachtetes Problem
Reproduzierbarkeit	Fehler lässt sich gezielt erneut auslösen
Hypothese	testbare Vermutung
Workaround	vorübergehende Umgehung
Ursachenbehebung	eigentliche Ursache beseitigen
Rollback	Änderung zurücknehmen
Latenz	Verzögerung
Paketverlust	Pakete gehen verloren
Bandbreite	Datenmenge pro Zeit
Jitter	Schwankung der Verzögerung
MTU	maximale Paketgröße
Authentifizierung	Identität prüfen
Autorisierung	Rechte prüfen
Log	Ereignisprotokoll
Paketmitschnitt	aufgezeichneter Netzwerkverkehr

IHK-sichere Kurzformulierung

Das OSI-Modell hilft bei der Netzwerkfehlersuche, weil Fehler systematisch nach Schichten eingegrenzt werden können. Bei der Bottom-Up-Methode beginnt man bei Schicht 1 mit physischer Verbindung und arbeitet sich bis zur Anwendungsschicht hoch. Bei der Top-Down-Methode beginnt man bei der Anwendung und prüft dann nach unten. Wichtig sind eine genaue Fehlerbeschreibung, die Eingrenzung betroffener Benutzer und Systeme, die Prüfung von DNS, DHCP, IP-Konfiguration, Routing, Firewall, NAT, Ports, Diensten, Authentifizierung, Autorisierung und Logs. Messergebnisse sollten dokumentiert werden, und Änderungen sollten einzeln getestet werden. Ein Workaround kann kurzfristig helfen, ersetzt aber nicht die Beseitigung der eigentlichen Ursache.

Merksätze

OSI-Modell hilft bei Fehlersuche.

Nicht raten,
sondern schrittweise prüfen.

Bottom-Up beginnt bei Schicht 1.

Top-Down beginnt bei der Anwendung.

Divide and Conquer grenzt den Fehlerbereich ein.

Fehlerbild genau aufnehmen.

Einzelner Benutzer:
Konto oder Client prüfen.

Alle Benutzer:
Dienst oder Infrastruktur prüfen.

Intern und extern getrennt prüfen.

WLAN und LAN getrennt prüfen.

DNS früh prüfen.

DHCP mit DORA prüfen.

Firewall mit Quelle,
Ziel,
Port,
Richtung
und Logs prüfen.

NAT vor und nach Übersetzung denken.

Logs zeigen Entscheidungen.

Mitschnitte zeigen Verkehr.

Nach Änderung zuerst Änderung prüfen.

Eine Änderung pro Test.

Workaround ist nicht Ursache.

Langsam ist nicht gleich nicht erreichbar.

Latenz = Verzögerung.

Paketverlust = verlorene Pakete.

Jitter = schwankende Verzögerung.

MTU = maximale Paketgröße.

Authentifizierung = Wer bist du?

Autorisierung = Was darfst du?

Fehlersuche endet mit Ursache,
Lösung
und Dokumentation.