10.10 Fehlersuche auf OSI-Schicht 7

OSI-Schicht 7 ist die Anwendungsschicht.

Auf dieser Schicht prüft man nicht mehr nur:

```
Kommt eine Verbindung zustande?
```

Sondern zusätzlich:

```
Funktioniert der konkrete Dienst?
Antwortet die Anwendung korrekt?
Stimmen Anmeldung, Rechte, Daten und Protokoll?
```

Typische Schicht-7-Dienste sind:

```
- HTTP / HTTPS
- DNS
- DHCP
- SMTP
- IMAP
- POP3
- FTP
- SFTP
- SMB
- LDAP
- SNMP
- NTP
- SSH
- RDP
- APIs
```

Merksatz:

```
Schicht 7 prüft den Dienst,
nicht nur die Verbindung.
```

Grundidee der Schicht-7-Fehlersuche

Bei Schicht 7 geht es um die konkrete Anwendungskommunikation.

Ein Port kann erreichbar sein, aber der Dienst kann trotzdem nicht richtig funktionieren.

Beispiel:

```
TCP 443 ist offen,
aber die Webseite zeigt HTTP 500.
```

Oder:

```
DNS-Server ist erreichbar,
aber der Name wird falsch aufgelöst.
```

Oder:

```
SMB-Port 445 ist erreichbar,
aber der Benutzer hat keine Berechtigung.
```

Merksatz:

```
Offener Port bedeutet nicht automatisch:
Anwendung funktioniert.
```

Schicht 7 erst prüfen, wenn die unteren Schichten passen

Vor der Schicht-7-Fehlersuche sollte man prüfen:

```
Schicht 1:
physische Verbindung vorhanden?

Schicht 2:
richtige MAC-Kommunikation, VLAN, Switch?

Schicht 3:
IP-Adresse, Subnetz, Gateway, Routing?
```

Schicht 4:
TCP- oder UDP-Port erreichbar?

Erst danach prüft man genauer:

Dienst,
Protokoll,
Anmeldung,
Antwort,
Daten,
Rechte,
Logs.

Merksatz:

Erst unten prüfen,
dann oben analysieren.

Typische Abgrenzung nach Schichten

Fehlerbild	wahrscheinliche Schicht
Kein Link	1
Falsches VLAN	2
Kein Gateway erreichbar	3
Port nicht erreichbar	4
Zertifikatswarnung	6
HTTP 404 oder 500	7
Login funktioniert nicht	7
Zugriff verweigert	7
DNS löst falsch auf	7
Mail landet im Spam	7
API lehnt Anfrage ab	7

Merksatz:

```
Schicht-7-Fehler betreffen Inhalt,
Dienst,
Anmeldung
oder Berechtigung.
```

Wichtige Prüffragen auf Schicht 7

Bei Anwendungsschichtproblemen stellt man Fragen wie:

```
Läuft der Dienst?
Antwortet der Dienst korrekt?
Wird das richtige Protokoll verwendet?
Wird der richtige Hostname verwendet?
Ist die URL korrekt?
Ist die Anmeldung korrekt?
Hat der Benutzer die nötigen Rechte?
Sind Zertifikate gültig?
Stimmen Header, Methode und Datenformat?
Gibt es Logs?
Gibt es eine Fehlermeldung?
Betrifft es alle Benutzer oder nur einzelne?
```

Merksatz:

```
Schicht 7 fragt:
Was macht der Dienst genau?
```

Dienst läuft oder läuft nicht

Ein häufiger Fehler ist:

```
Netzwerk funktioniert,
aber Dienst läuft nicht.
```

Beispiele:

```
Webserver gestoppt
Datenbank nicht erreichbar
SSH-Dienst deaktiviert
Maildienst gestört
DNS-Dienst nicht gestartet
Backend-Container nicht aktiv
Anwendung abgestürzt
```

Typisches Fehlerbild:

```
Host erreichbar,
aber Dienst antwortet nicht richtig.
```

Merksatz:

```
Erreichbarer Server heißt nicht:
Dienst läuft.
```

Falsches Protokoll

Manchmal wird das falsche Protokoll verwendet.

Beispiele:

```
http:// statt https://

FTP statt SFTP

LDAP statt LDAPS

IMAP statt POP3

SMB-Pfad statt SFTP-Zugriff

HTTPS zum Backend,
obwohl Backend nur HTTP spricht
```

Merksatz:

Falsches Protokoll kann wie ein Verbindungsfehler aussehen.

Falscher Port

Ein Dienst kann auf einem anderen Port laufen als erwartet.

Beispiele:

Webserver läuft auf TCP 8080 statt TCP 80.

Adminoberfläche läuft auf TCP 8443 statt TCP 443.

SSH läuft auf anderem Port als TCP 22.

Anwendung läuft intern auf Port 3000,
extern aber über Reverse Proxy auf 443.

Merksatz:

Immer prüfen:
Welcher Dienst lauscht auf welchem Port?

Falscher Hostname

Bei vielen Diensten ist der Hostname wichtig.

Beispiele:

HTTPS-Zertifikat muss zum Hostnamen passen.

Reverse Proxy entscheidet über Host-Header.

Virtuelle Hosts liefern je nach Hostname andere Inhalte.

DNS kann intern und extern unterschiedlich auflösen.

Fehlerbild:

IP ist erreichbar,
aber falsche Webseite oder falsches Zertifikat erscheint.

Merksatz:

Hostname ist auf Schicht 7 oft entscheidend.

DNS-Fehler auf Schicht 7

DNS-Probleme sind typische Schicht-7-Probleme.

Fehlerbilder:

Name löst nicht auf.
Name löst auf falsche IP auf.
Interne und externe Antwort unterscheiden sich.
DNS-Cache ist veraltet.
MX-Record fehlt.
CNAME zeigt falsch.
AAAA-Record zeigt auf nicht erreichbares IPv6-Ziel.

Prüffragen:

Welcher DNS-Server wird gefragt?
Welche Antwort liefert er?
Ist die Antwort intern und extern gleich?
Ist der Cache noch aktiv?
Stimmt die TTL?

Merksatz:

IP geht,
Name nicht:
DNS prüfen.

HTTP-Fehler auf Schicht 7

Bei Webdiensten sind HTTP-Statuscodes sehr hilfreich.

Wichtige Beispiele:

Statuscode	Bedeutung
200	OK
301 / 302	Weiterleitung
400	fehlerhafte Anfrage
401	nicht authentifiziert
403	verboten
404	nicht gefunden
405	Methode nicht erlaubt
429	zu viele Anfragen
500	interner Serverfehler
502	Bad Gateway
503	Dienst nicht verfügbar
504	Gateway Timeout

Merksatz:

```
HTTP-Statuscodes sind wichtige Schicht-7-Hinweise.
```

---

401 und 403 bei der Fehlersuche

401 bedeutet:

```
Benutzer ist nicht authentifiziert.
```

Typische Ursachen:

```
- nicht angemeldet
- Token fehlt
- Token ungültig
- Session abgelaufen
- falsche Zugangsdaten
```

403 bedeutet:

```
Benutzer ist bekannt,
aber nicht berechtigt.
```

Typische Ursachen:

```
- Rolle fehlt
- Gruppe fehlt
- Zugriff verboten
- Richtlinie blockiert
- Ressource nicht erlaubt
```

Merksatz:

```
401 = Anmeldung fehlt.
403 = Rechte fehlen.
```

---

404 bei der Fehlersuche

404 bedeutet:

```
Ressource nicht gefunden.
```

Mögliche Ursachen:

```
- falscher Pfad
- falsche URL
- Route fehlt
- Datei existiert nicht
- Reverse Proxy leitet falsch weiter
- Anwendung erwartet anderen Basis-Pfad
- Tippfehler im Link
```

Merksatz:

```
404 heißt:
Unter diesem Pfad wurde nichts gefunden.
```

---

500 bei der Fehlersuche

500 bedeutet:

```
interner Serverfehler.
```

Mögliche Ursachen:

```
- Fehler in der Anwendung
- Datenbank nicht erreichbar
- Konfigurationsfehler
- fehlende Rechte
- Programmfehler
- Speicherproblem
- Abhängigkeit nicht verfügbar
```

Merksatz:

```
500 ist meist ein Problem der Anwendung oder des Servers.
```

502, 503 und 504 bei Reverse Proxys

Diese Fehler treten häufig bei Reverse Proxys auf.

Statuscode	typische Bedeutung
502	Proxy bekommt keine gültige Antwort vom Backend
503	Dienst aktuell nicht verfügbar
504	Gateway wartet zu lange auf Backend

Typische Ursachen:

```
- Backend läuft nicht
- falscher Backend-Port
- falsches Protokoll zum Backend
- Backend überlastet
- Timeout
- falscher Container-Name
- internes DNS-Problem
```

```
- Firewall blockiert intern
```

Merksatz:

```
Bei 502, 503 und 504 Proxy und Backend prüfen.
```

API-Fehler auf Schicht 7

APIs haben typische Fehlerquellen.

Prüfpunkte:

```
- richtige URL?
- richtige HTTP-Methode?
- richtiger Content-Type?
- gültiges JSON?
- Authorization-Header vorhanden?
- Token gültig?
- Berechtigung vorhanden?
- API-Version korrekt?
- Rate Limit erreicht?
- Pflichtfelder vorhanden?
```

Typische Fehler:

```
400 Bad Request
401 Unauthorized
403 Forbidden
404 Not Found
405 Method Not Allowed
429 Too Many Requests
500 Internal Server Error
```

Merksatz:

```
API-Fehler mit Methode,
Header,
Body,
```

```
Token
und Statuscode prüfen.
```

Datenformatfehler

Schicht 7 ist oft eng mit Schicht 6 verbunden.

Fehler können entstehen durch:

```
- ungültiges JSON
- ungültiges XML
- falscher Content-Type
- falsche Zeichencodierung
- fehlende Pflichtfelder
- falsches Datumsformat
- falscher Dezimaltrenner
- falsche Groß- und Kleinschreibung
- unerwartete Sonderzeichen
```

Merksatz:

```
Anwendung versteht Daten nur,
wenn Format und Inhalt passen.
```

Authentifizierungsfehler

Authentifizierung prüft:

```
Wer bist du?
```

Typische Fehler:

```
- falscher Benutzername
- falsches Passwort
- Konto gesperrt
- Konto deaktiviert
- Passwort abgelaufen
- MFA fehlt
```

- Token ungültig
- Zertifikat ungültig
- falscher Identity Provider
- Zeitabweichung

Merksatz:

Loginfehler sind nicht immer nur Passwortfehler.

Autorisierungsfehler

Autorisierung prüft:

Was darfst du?

Typische Fehler:

- Benutzer nicht in richtiger Gruppe
- Rolle fehlt
- Berechtigung fehlt
- Freigaberecht fehlt
- Dateisystemrecht fehlt
- API-Scope fehlt
- Richtlinie blockiert
- Mandant falsch
- alte Session enthält alte Rechte

Merksatz:

Zugriff verweigert bedeutet:
Rechte prüfen.

Session-Fehler

Sessions verbinden mehrere Anfragen zu einer Sitzung.

Typische Fehlerbilder:

Benutzer wird ständig ausgeloggt.

Login-Schleife.

Warenkorb wird vergessen.

Session läuft sofort ab.

Benutzer sieht falschen Zustand.

Zugriff funktioniert nur in einem Browser.

Mögliche Ursachen:

- Cookie wird blockiert
- Cookie-Domain falsch
- Cookie-Pfad falsch
- SameSite-Problem
- Secure-Flag fehlt oder passt nicht
- Zeitabweichung
- Session-Speicher gestört
- Load Balancer ohne Session-Stickiness

Merksatz:

Login-Schleifen sind oft Cookie- oder Session-Probleme.

TLS- und Zertifikatsfehler

Auch wenn TLS eher Schicht 6 zugeordnet wird, wirkt es stark auf Schicht 7.

Typische Fehler:

- Zertifikat abgelaufen
- Name passt nicht
- CA nicht vertrauenswürdig
- Zwischenzertifikat fehlt
- falsche Systemzeit
- TLS-Version zu alt
- Cipher Suite passt nicht
- Reverse Proxy liefert falsches Zertifikat

Merksatz:

```
HTTPS-Probleme immer mit Zertifikat,
Name
und Zeit prüfen.
```

Mailprobleme auf Schicht 7

E-Mail nutzt mehrere Anwendungsschichtprotokolle.

Typische Fehlerbilder:

```
Mail kann nicht gesendet werden.
Mail kann nicht empfangen werden.
Mail landet im Spam.
Mail kommt verzögert an.
Mailclient kann sich nicht anmelden.
Zertifikatswarnung im Mailclient.
NDR wird erzeugt.
```

Prüfpunkte:

```
SMTP
IMAP
POP3
MX
SPF
DKIM
DMARC
TLS
Authentifizierung
Spamfilter
Postfachgröße
Mailserver-Logs
```

Merksatz:

```
Mailfehler mit Protokoll,
DNS,
Authentifizierung
```

```
und Logs prüfen.
```

SMB-Fehler auf Schicht 7

SMB wird für Datei- und Druckerfreigaben genutzt.

Typische Fehler:

```
Freigabe nicht erreichbar.
Zugriff verweigert.
Netzlaufwerk verbindet nicht.
Datei kann nicht gespeichert werden.
Datei ist gesperrt.
Benutzer sieht Freigabe nicht.
```

Prüfpunkte:

```
DNS-Name
TCP 445
SMB-Dienst
Freigabename
Benutzerkonto
Gruppe
Freigaberecht
Dateisystemrecht
gespeicherte Anmeldedaten
SMB-Version
```

Merksatz:

```
SMB-Fehler oft mit Name,
Port,
Anmeldung
und Rechten prüfen.
```

LDAP-Fehler auf Schicht 7

LDAP wird für Verzeichnisdienste genutzt.

Typische Fehler:

```
Benutzer wird nicht gefunden.
Anmeldung schlägt fehl.
Gruppen werden nicht erkannt.
Anwendung kann LDAP nicht verbinden.
LDAPS-Zertifikat wird abgelehnt.
```

Prüfpunkte:

```
LDAP-Server
Port 389 oder 636
Base-DN
Bind-Benutzer
Passwort
Suchfilter
Gruppenpfad
Zertifikat bei LDAPS
Firewall
DNS
```

Merksatz:

```
LDAP-Fehler mit Bind,
Base-DN,
Filter
und Zertifikat prüfen.
```

SNMP-Fehler auf Schicht 7

SNMP wird für Monitoring genutzt.

Typische Fehler:

```
Gerät wird als down angezeigt.
Werte werden nicht gelesen.
Interface-Daten fehlen.
Traps kommen nicht an.
```

Monitoring zeigt falsche Werte.

Prüfpunkte:

SNMP-Agent aktiv?
richtige SNMP-Version?
Community-String korrekt?
SNMPv3-Benutzer korrekt?
UDP 161 erlaubt?
UDP 162 für Traps erlaubt?
OID vorhanden?
MIB korrekt?
Zugriff vom Monitoring-Server erlaubt?

Merksatz:

SNMP-Fehler mit Version,
Zugangsdaten,
Port
und OID prüfen.

NTP-Fehler auf Schicht 7

NTP synchronisiert Zeit.

Typische Fehlerbilder:

Systemzeit falsch.
Zertifikate wirken ungültig.
Kerberos-Anmeldung schlägt fehl.
Logs passen zeitlich nicht zusammen.
Monitoring-Zeitstempel stimmen nicht.

Prüfpunkte:

NTP-Server erreichbar?
UDP 123 erlaubt?
DNS-Name des Zeitservers korrekt?

Zeitzone korrekt?
Zeitquelle vertrauenswürdig?
Zeitabweichung zu groß?
VM-Zeitquelle korrekt?

Merksatz:

Falsche Zeit kann viele scheinbar andere Fehler verursachen.

SSH-Fehler auf Schicht 7

SSH dient sicherem Fernzugriff.

Typische Fehler:

Timeout
Connection refused
Permission denied
Host-Key-Warnung
falscher Schlüssel
Benutzer darf nicht anmelden
Dienst läuft nicht

Prüfpunkte:

TCP 22 erreichbar?
SSH-Dienst aktiv?
richtiger Benutzer?
richtiger Schlüssel?
richtige Dateirechte?
Host-Key plausibel?
Firewall erlaubt Zugriff?
Loginmethode erlaubt?

Merksatz:

SSH-Fehler mit Port,
Dienst,

Benutzer,
Schlüssel
und Host-Key prüfen.

RDP-Fehler auf Schicht 7

RDP dient grafischem Fernzugriff.

Typische Fehler:

Verbindung nicht möglich.
Anmeldung abgelehnt.
RDP ist langsam.
Sitzung wird getrennt.
NLA-Fehler.
Benutzer hat keine Berechtigung.

Prüfpunkte:

TCP 3389 erreichbar?
Remote Desktop aktiviert?
Benutzer berechtigt?
NLA kompatibel?
VPN verbunden?
Firewall erlaubt Zugriff?
Konto gesperrt?
Server überlastet?

Merksatz:

RDP-Fehler mit Verbindung,
Anmeldung,
Berechtigung
und Richtlinien prüfen.

DHCP-Fehler auf Schicht 7

DHCP ist ein Anwendungsschichtprotokoll, liefert aber Schicht-3-Konfiguration.

Typische Fehler:

```
Client bekommt keine IP.
Client bekommt falsche IP.
Client bekommt 169.254.x.x.
Gateway ist falsch.
DNS ist falsch.
Manche VLANs funktionieren nicht.
```

Prüfpunkte:

```
DHCP-Server aktiv?
DHCP-Scope vorhanden?
Adressen frei?
DHCP-Relay korrekt?
VLAN korrekt?
UDP 67/68 erlaubt?
Rogue-DHCP vorhanden?
DHCP-Optionen korrekt?
```

Merksatz:

```
DHCP-Fehler mit VLAN,
Scope,
Relay
und Optionen prüfen.
```

Logs sind auf Schicht 7 besonders wichtig

Auf Schicht 7 liefern Logs oft die beste Information.

Wichtige Logs:

```
- Webserver-Logs
- Anwendungslogs
- Authentifizierungslogs
- Mailserver-Logs
- DNS-Logs
```

- DHCP-Logs
- LDAP-Logs
- Reverse-Proxy-Logs
- Firewall-Logs
- Monitoring-Logs
- Systemlogs

Logs zeigen oft:

- Statuscode
- Fehlermeldung
- Benutzer
- Zeit
- Quelle
- Ziel
- Pfad
- angefragte Ressource
- Authentifizierungsgrund
- Backend-Fehler

Merksatz:

> Ohne Logs bleibt Schicht-7-Fehlersuche oft ungenau.

Fehlermeldungen richtig lesen

Fehlermeldungen liefern wichtige Hinweise.

Beispiele:

Meldung	mögliche Bedeutung
Unauthorized	nicht angemeldet oder Token ungültig
Forbidden	keine Berechtigung
Not Found	Ressource oder Pfad fehlt
Bad Gateway	Proxy erreicht Backend nicht sauber
Connection refused	Dienst nimmt Verbindung nicht an
Timeout	keine Antwort innerhalb der Zeit
Invalid credentials	Zugangsdaten falsch

Meldung	mögliche Bedeutung
Certificate expired	Zertifikat abgelaufen
Name mismatch	Zertifikat passt nicht zum Namen

Merksatz:

> Fehlermeldung nicht ignorieren,
> sondern technisch einordnen.

Fehler nur bei einem Benutzer

Wenn ein Problem nur bei einem Benutzer auftritt, prüft man eher:

- Benutzerkonto
- Passwort
- MFA
- Gruppenmitgliedschaften
- Rollen
- Berechtigungen
- Session
- gespeicherte Anmeldedaten
- Clientprofil
- Browsercache
- lokale Einstellungen

Merksatz:

> Einzelner Benutzer betroffen:
> Konto und Rechte prüfen.

Fehler bei allen Benutzern

Wenn alle Benutzer betroffen sind, prüft man eher:

- Dienst läuft?
- Server erreichbar?
- DNS korrekt?

- Zertifikat gültig?
- Datenbank erreichbar?
- Backend verfügbar?
- zentrale Authentifizierung erreichbar?
- Reverse Proxy korrekt?
- Lizenz oder Ressourcenproblem?
- allgemeine Störung?

Merksatz:

Alle betroffen:
Dienst, Server oder zentrale Infrastruktur prüfen.

Fehler nur intern oder nur extern

Wenn ein Dienst intern funktioniert, extern aber nicht, prüft man:

- externes DNS
- Firewall
- NAT
- Reverse Proxy
- Zertifikat
- öffentliche IP
- Portweiterleitung
- Geo- oder Zugriffsbeschränkung

Wenn ein Dienst extern funktioniert, intern aber nicht, prüft man:

- internes DNS
- Split DNS
- Hairpin NAT
- interne Firewall
- Proxy-Einstellungen
- Routing intern
- Zertifikat und Hostname intern

Merksatz:

Intern und extern getrennt prüfen.

Fehler nur in einem Browser

Mögliche Ursachen:

- Browsercache
- Cookies
- gespeicherte Zugangsdaten
- Erweiterungen
- CORS-Verhalten
- alte Session
- Zertifikatsspeicher
- Proxy-Einstellungen
- HSTS-Eintrag

Merksatz:

Browserabhängige Fehler oft mit Cache,
Cookies
und Erweiterungen prüfen.

Fehler nur auf einem Client

Mögliche Ursachen:

- falsche DNS-Einstellung
- falsche Systemzeit
- veraltetes Zertifikat
- lokale Firewall
- Proxy-Einstellung
- VPN aktiv oder inaktiv
- falsche gespeicherte Anmeldedaten
- veraltete Anwendung
- defektes Profil

Merksatz:

```
Einzelner Client betroffen:
lokale Einstellungen prüfen.
```

Fehler nach Änderung

Nach Änderungen prüft man zuerst, was geändert wurde.

Beispiele:

```
DNS geändert
Zertifikat erneuert
Passwort geändert
Gruppe geändert
Firewall angepasst
Anwendung aktualisiert
Reverse Proxy geändert
Datenbank verschoben
Container neu gestartet
Port geändert
Lizenz geändert
```

Merksatz:

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

Systematische Schicht-7-Fehlersuche

Eine sinnvolle Reihenfolge:

```
1. Fehlermeldung genau lesen.
2. Betroffene Benutzer und Systeme eingrenzen.
3. Dienst und Protokoll bestimmen.
4. DNS und Hostname prüfen.
5. IP-Erreichbarkeit prüfen.
6. Port prüfen.
7. TLS oder Zertifikat prüfen.
8. Anwendung oder Dienst prüfen.
9. Anmeldung prüfen.
```

10. Berechtigung prüfen.
11. Datenformat oder Anfrage prüfen.
12. Logs prüfen.
13. letzte Änderungen prüfen.

Merksatz:

> Erst eingrenzen,
> dann Schicht für Schicht prüfen.

Typische Werkzeuge

Werkzeug	Zweck
Browser-Entwicklertools	HTTP-Status, Header, Cookies, Netzwerk
curl	HTTP/API testen
nslookup	DNS einfach prüfen
dig	DNS detailliert prüfen
ping	IP-Erreichbarkeit grob prüfen
traceroute / tracert	Weg zum Ziel prüfen
telnet / nc	TCP-Port testen
openssl s_client	TLS-Zertifikat prüfen
ssh -v	SSH-Verbindung detailliert prüfen
Ereignisanzeige	Windows-Logs prüfen
journalctl	Linux-Systemlogs prüfen
Webserver-Logs	HTTP-Anfragen prüfen
Mailserver-Logs	E-Mail-Zustellung prüfen

Merksatz:

> Das richtige Werkzeug hängt vom Dienst ab.

---

curl für Webfehler

curl kann HTTP-Antworten prüfen.

Typische Prüfpunkte:

```
- Statuscode
- Header
- Weiterleitung
- TLS-Fehler
- Antwortinhalt
- API-Antwort
```

Beispielgedanke:

```
Was antwortet der Server wirklich?
```

Merksatz:

```
curl zeigt,
was ein Webdienst tatsächlich zurückgibt.
```

Browser-Entwicklertools

Browser-Entwicklertools helfen bei Webproblemen.

Sie zeigen unter anderem:

```
- HTTP-Requests
- HTTP-Responses
- Statuscodes
- Header
- Cookies
- Ladezeiten
- CORS-Fehler
- JavaScript-Fehler
- blockierte Inhalte
```

Merksatz:

```
Browser-Entwicklertools sind wichtig für Web-Schicht-7-Fehler.
```

---

openssl s_client

Mit openssl s_client kann man TLS-Verbindungen prüfen.

Typische Informationen:

- Zertifikat
- Zertifikatskette
- TLS-Version
- Cipher
- Name und Zertifikat
- Ablaufdatum

Besonders hilfreich bei:

- HTTPS
- LDAPS
- IMAPS
- SMTPS
- POP3S

Merksatz:

TLS-Probleme mit Zertifikat und Kette prüfen.

Paketmitschnitt auf Schicht 7

Ein Paketmitschnitt kann helfen, wenn Logs nicht ausreichen.

Man kann sehen:

- DNS-Anfragen
- DHCP-DORA
- TCP-Verbindungsaufbau
- TLS-Handshake
- unverschlüsselte Protokollinhalte
- Fehlercodes
- Wiederholungen
- Timeouts

Wichtig:

Bei verschlüsselten Verbindungen sieht man Inhalte nicht einfach im Klartext.

Merksatz:

Mitschnitt zeigt Verkehr,
aber TLS schützt Inhalte.

Schicht-7-Fehler und Sicherheit

Viele Schicht-7-Fehler haben Sicherheitsbezug.

Beispiele:

- falsche Rechte
- schwache Authentifizierung
- unsichere Cookies
- offene Adminbereiche
- veraltete Webanwendung
- unsicheres FTP
- Telnet statt SSH
- fehlende MFA
- falsche CORS-Konfiguration
- Tokens in URLs
- zu genaue Fehlermeldungen

Merksatz:

Anwendungsschicht ist häufig Angriffsziel.

Was Schicht-7-Fehlersuche nicht ersetzt

Schicht-7-Fehlersuche ersetzt nicht:

- Prüfung der Verkabelung
- VLAN-Prüfung
- Routing-Prüfung
- Firewall-Prüfung

- Portprüfung
- Zertifikatsprüfung
- Berechtigungskonzept
- Sicherheitskonzept
- Backup-Konzept
- Monitoring

Sie ergänzt diese Prüfungen.

Merksatz:

> Schicht 7 ist nur ein Teil der gesamten Fehlersuche.

Typische IHK-Fragen

In AP1 und AP2 kann zum Beispiel gefragt werden:

- Warum reicht ein erfolgreicher Ping nicht aus?
- Warum reicht ein offener Port nicht aus?
- Was prüft man bei HTTP 404?
- Was prüft man bei HTTP 500?
- Was bedeutet HTTP 401?
- Was bedeutet HTTP 403?
- Warum kann ein DNS-Fehler wie ein Internetproblem wirken?
- Warum kann ein falsches Zertifikat durch DNS entstehen?
- Wie grenzt man Anmeldeprobleme ein?
- Wie grenzt man Berechtigungsprobleme ein?
- Warum sind Logs bei Schicht-7-Problemen wichtig?
- Welche Rolle spielt der Reverse Proxy bei Webfehlern?
- Warum kann ein Dienst trotz erreichbarem Server nicht funktionieren?

Typische Prüfungsfallen

> Ping prüft nicht die Anwendung.
>
> Offener Port heißt nicht,
> dass der Dienst korrekt funktioniert.

HTTP-Statuscodes gehören zur Anwendungsschicht.

401 bedeutet nicht authentifiziert.

403 bedeutet nicht berechtigt.

404 bedeutet Ressource nicht gefunden.

500 bedeutet interner Serverfehler.

502 deutet oft auf Proxy-Backend-Problem.

DNS gehört zu Schicht 7.

DHCP gehört zu Schicht 7,
auch wenn es IP-Konfiguration verteilt.

Mailprobleme sind oft DNS-, TLS- oder Spamfilterprobleme.

SMB-Probleme sind oft Rechte- oder Anmeldeprobleme.

LDAP-Probleme sind oft Base-DN-, Bind- oder Filterprobleme.

NTP-Probleme können Zertifikats- und Loginfehler verursachen.

Schicht 7 braucht Logs.

Wichtige Begriffe kurz erklärt

Begriff	Kurze Erklärung
Schicht-7-Fehler	Fehler im Dienst oder Anwendungsprotokoll
Dienst	bereitgestellte Netzwerkfunktion
Statuscode	Antwortcode eines Protokolls
HTTP 401	nicht authentifiziert
HTTP 403	nicht berechtigt
HTTP 404	Ressource nicht gefunden
HTTP 500	interner Serverfehler

Begriff	Kurze Erklärung
HTTP 502	Bad Gateway
Backend	interner Ziel-Dienst
Reverse Proxy	vorgelagerter Webserver
Authentifizierung	Identität prüfen
Autorisierung	Rechte prüfen
Session	Sitzung zwischen Client und Anwendung
Token	digitaler Zugriffsnachweis
Log	Protokolldatei mit Ereignissen
API	Schnittstelle zwischen Anwendungen
Content-Type	Datenformat im HTTP-Body
DNS-Cache	zwischengespeicherte DNS-Antwort

IHK-sichere Kurzformulierung

Fehlersuche auf OSI-Schicht 7 betrifft die Anwendungsschicht und damit konkrete Dienste und Protokolle wie HTTP, DNS, DHCP, SMTP, SMB, LDAP, SNMP, NTP, SSH, RDP und APIs. Dabei reicht es nicht aus, nur IP-Erreichbarkeit oder offene Ports zu prüfen. Ein Dienst kann trotz erreichbarem Server und offenem Port fehlerhaft antworten. Deshalb prüft man auf Schicht 7 insbesondere Dienststatus, Protokoll, Hostname, URL, HTTP-Statuscodes, Anmeldung, Berechtigungen, Datenformat, Zertifikate, Reverse Proxy, Backend und Logs. Schicht-7-Fehler zeigen sich häufig als falsche DNS-Antworten, HTTP-Fehler, Loginprobleme, Zugriff verweigert, Mailprobleme oder fehlerhafte API-Antworten.

Merksätze

```
Schicht 7 = Anwendungsschicht.

Schicht 7 prüft den konkreten Dienst.

Ping prüft nicht die Anwendung.

Offener Port heißt nicht:
Anwendung funktioniert.

Dienst läuft nicht immer,
nur weil Server erreichbar ist.
```

Falsches Protokoll erzeugt Fehler.

Falscher Hostname kann falsches Zertifikat liefern.

DNS-Probleme sind Schicht-7-Probleme.

HTTP-Statuscodes helfen bei Webfehlern.

401 = nicht authentifiziert.

403 = nicht berechtigt.

404 = nicht gefunden.

500 = interner Serverfehler.

502 = Proxy-Backend-Problem.

503 = Dienst nicht verfügbar.

504 = Gateway Timeout.

API-Fehler mit Methode,
Header,
Body
und Token prüfen.

Loginfehler = Authentifizierung prüfen.

Zugriff verweigert = Autorisierung prüfen.

Login-Schleife = Session und Cookies prüfen.

Mailfehler mit DNS,
SMTP,
IMAP,
TLS
und Spamfilter prüfen.

SMB-Fehler mit Name,

Port,
Anmeldung
und Rechten prüfen.

LDAP-Fehler mit Bind,
Base-DN
und Filter prüfen.

SNMP-Fehler mit Version,
Zugangsdaten
und OID prüfen.

NTP-Fehler können viele Folgefehler erzeugen.

Logs sind bei Schicht 7 besonders wichtig.

Erst eingrenzen,
dann Schicht für Schicht prüfen.