10.1 OSI-Schicht 7 – Anwendungsschicht

Die Anwendungsschicht ist Schicht 7 des OSI-Modells.

Sie ist die oberste Schicht.

Die Hauptaufgabe von Schicht 7 ist:

```
Netzwerkdienste für Anwendungen bereitstellen.
```

Dabei geht es vor allem um Protokolle und Dienste, die direkt von Anwendungen genutzt werden.

Typische Beispiele:

```
- HTTP
- HTTPS
- DNS
- DHCP
- SMTP
- IMAP
- POP3
- FTP
- SSH
- SMB
- LDAP
- SNMP
- NTP
```

Merksatz:

```
Schicht 7 = Netzwerkdienste für Anwendungen.
```

Grundidee von Schicht 7

Schicht 7 ist die Schicht, mit der Anwendungen direkt arbeiten.

Beispiele:

Webbrowser nutzt HTTP oder HTTPS.
Mailprogramm nutzt SMTP, IMAP oder POP3.
Betriebssystem nutzt DNS zur Namensauflösung.
Client nutzt DHCP zur automatischen IP-Konfiguration.
Administrator nutzt SSH zur Fernverwaltung.

Wichtig:

Die Anwendungsschicht ist nicht die Anwendung selbst,
sondern die Netzwerkschnittstelle beziehungsweise das Protokoll,
das die Anwendung nutzt.

Merksatz:

Schicht 7 beschreibt Dienste und Protokolle,
die Anwendungen für Netzwerkkommunikation verwenden.

Einordnung im OSI-Modell

OSI-Schicht	Name	Aufgabe
7	Anwendungsschicht	Netzwerkdienste für Anwendungen
6	Darstellungsschicht	Darstellung, Codierung, Verschlüsselung
5	Sitzungsschicht	Sitzungen aufbauen, verwalten und beenden
4	Transportschicht	TCP, UDP, Ports
3	Vermittlungsschicht / Netzwerkschicht	IP, Routing
2	Sicherungsschicht	Frames, MAC, VLAN
1	Bitübertragungsschicht	Bits, Signale

Merksatz:

Schicht 7 ist die oberste OSI-Schicht.

Schicht 7 ist nicht einfach „das Programm“

Ein häufiger Fehler ist:

```
Browser = Schicht 7
```

Besser formuliert:

```
Der Browser ist eine Anwendung.
Der Browser nutzt Protokolle der Anwendungsschicht,
zum Beispiel HTTP oder HTTPS.
```

Beispiel:

```
Firefox, Chrome oder Safari
= Anwendung

HTTP, HTTPS
= Protokolle der Anwendungsschicht
```

Merksatz:

```
Programm nutzt Schicht 7,
ist aber nicht automatisch selbst die Schicht.
```

Was macht die Anwendungsschicht?

Die Anwendungsschicht stellt Funktionen bereit wie:

```
- Webseiten abrufen
- Namen in IP-Adressen auflösen
- E-Mails senden und empfangen
- Dateien übertragen
- Zeit synchronisieren
- Netzwerkgeräte überwachen
- Verzeichnisdienste abfragen
- automatische IP-Konfiguration anstoßen
- entfernte Systeme verwalten
```

Merksatz:

Schicht 7 stellt konkrete Netzwerkdienste bereit.

Schicht 7 und Ports

Viele Anwendungsschicht-Protokolle nutzen Ports auf Schicht 4.

Beispiele:

Anwendungsschicht-Protokoll	Transport	typischer Port
HTTP	TCP	80
HTTPS	TCP	443
DNS	UDP / TCP	53
DHCP	UDP	67 / 68
SSH	TCP	22
SMTP	TCP	25
IMAP	TCP	143
POP3	TCP	110
NTP	UDP	123

Wichtig:

Port gehört zu Schicht 4.
Dienstprotokoll gehört zu Schicht 7.

Merksatz:

Port = Schicht 4.
Protokoll/Dienst = Schicht 7.

HTTP

HTTP steht für:

Hypertext Transfer Protocol

HTTP wird verwendet, um Webseiten und Webdaten zu übertragen.

Typischer Port:

```
TCP 80
```

HTTP ist unverschlüsselt.

Beispiele für HTTP-Kommunikation:

```
Browser ruft Webseite ab.
Webanwendung liefert HTML.
API sendet Daten.
Client lädt Dateien von einem Webserver.
```

Merksatz:

```
HTTP = Webprotokoll ohne TLS-Verschlüsselung.
```

HTTPS

HTTPS steht für:

```
Hypertext Transfer Protocol Secure
```

HTTPS ist:

```
HTTP über TLS
```

Typischer Port:

```
TCP 443
```

HTTPS schützt die Übertragung durch TLS.

Schutzziele:

```
- Vertraulichkeit
- Integrität
```

- Authentizität

Merksatz:

HTTPS = HTTP mit TLS-Schutz.

HTTP und HTTPS unterscheiden

Merkmal	HTTP	HTTPS
Verschlüsselung	nein	ja, TLS
typischer Port	TCP 80	TCP 443
Zertifikat nötig	nein	ja
Schutz vor Mitlesen	nein	ja
Schutz vor Manipulation	nein	ja

Merksatz:

HTTP ist unverschlüsselt.
HTTPS ist verschlüsselt.

DNS

DNS steht für:

Domain Name System

DNS löst Namen in IP-Adressen auf.

Beispiel:

www.example.com
→ 93.184.216.34

DNS wird benötigt, damit Benutzer und Anwendungen mit Namen arbeiten können, statt sich IP-Adressen merken zu müssen.

Typischer Port:

```
UDP 53
TCP 53
```

Merksatz:

```
DNS = Name zu IP-Adresse.
```

A-Record und AAAA-Record

DNS kann verschiedene Einträge liefern.

Wichtige Einträge:

DNS-Record	Bedeutung
A	Name zu IPv4-Adresse
AAAA	Name zu IPv6-Adresse
CNAME	Alias auf anderen Namen
MX	Mailserver einer Domain
TXT	Textinformationen, oft für Prüfungen
NS	zuständiger Nameserver

Merksatz:

```
A = IPv4.
AAAA = IPv6.
MX = Mailserver.
```

DNS und Schicht 7

DNS ist ein Anwendungsschicht-Protokoll, obwohl es UDP oder TCP auf Schicht 4 nutzt.

Wichtig:

```
DNS-Port 53 gehört zu Schicht 4.
DNS-Protokoll gehört zu Schicht 7.
```

Merksatz:

```
DNS nutzt Ports,
ist aber ein Dienst der Anwendungsschicht.
```

DHCP

DHCP steht für:

```
Dynamic Host Configuration Protocol
```

DHCP vergibt automatisch Netzwerkkonfigurationen.

Ein Client kann per DHCP erhalten:

```
- IP-Adresse
- Subnetzmaske
- Standard-Gateway
- DNS-Server
- Lease-Zeit
- weitere Optionen
```

Typische Ports:

```
DHCP-Server:
UDP 67

DHCP-Client:
UDP 68
```

Merksatz:

```
DHCP = automatische IP-Konfiguration.
```

DHCP und Schicht 7

DHCP ist ein Anwendungsschicht-Protokoll, auch wenn es IP-Konfigurationen für Schicht 3 bereitstellt.

Das ist wichtig:

```
DHCP vergibt IP-Daten,
aber das DHCP-Protokoll selbst gehört zur Anwendungsschicht.
```

Merksatz:

```
DHCP liefert Schicht-3-Konfiguration,
ist aber ein Schicht-7-Protokoll.
```

SMTP

SMTP steht für:

```
Simple Mail Transfer Protocol
```

SMTP wird für das Senden und Weiterleiten von E-Mails verwendet.

Typischer Port:

```
TCP 25
```

Weitere häufige Ports:

```
TCP 587 für Mail Submission
TCP 465 für SMTPS
```

Merksatz:

```
SMTP = E-Mail senden und transportieren.
```

POP3

POP3 steht für:

```
Post Office Protocol Version 3
```

POP3 wird zum Abrufen von E-Mails verwendet.

Typischer Port:

```
TCP 110
```

Verschlüsselte Variante:

```
POP3S über TCP 995
```

POP3 lädt E-Mails häufig vom Server herunter.

Merksatz:

```
POP3 = E-Mail abrufen.
```

IMAP

IMAP steht für:

```
Internet Message Access Protocol
```

IMAP wird zum Abrufen und Verwalten von E-Mails verwendet.

Typischer Port:

```
TCP 143
```

Verschlüsselte Variante:

```
IMAPS über TCP 993
```

IMAP lässt E-Mails häufig auf dem Server und synchronisiert sie zwischen Geräten.

Merksatz:

```
IMAP = E-Mail verwalten und synchronisieren.
```

SMTP, POP3 und IMAP unterscheiden

Protokoll	Hauptaufgabe	typischer Port
SMTP	E-Mail senden / transportieren	TCP 25
POP3	E-Mail abrufen	TCP 110
IMAP	E-Mail abrufen und verwalten	TCP 143

Merksatz:

```
SMTP sendet.
POP3 und IMAP empfangen.
```

FTP

FTP steht für:

```
File Transfer Protocol
```

FTP dient zur Dateiübertragung.

Typischer Port:

```
TCP 21
```

Wichtig:

```
Klassisches FTP ist unverschlüsselt.
```

Sicherere Alternativen sind zum Beispiel:

```
- SFTP
- FTPS
```

Merksatz:

```
FTP = Dateiübertragung,
klassisch unverschlüsselt.
```

SFTP und FTPS unterscheiden

SFTP und FTPS werden oft verwechselt.

Begriff	Bedeutung
SFTP	Dateiübertragung über SSH
FTPS	FTP mit TLS-Schutz

Typische Einordnung:

```
SFTP nutzt SSH.
FTPS nutzt TLS.
```

Merksatz:

```
SFTP ist nicht dasselbe wie FTPS.
```

SSH

SSH steht für:

```
Secure Shell
```

SSH dient zur sicheren Fernverwaltung.

Typischer Port:

```
TCP 22
```

SSH wird genutzt für:

```
- sichere Shell
- Serveradministration
- SFTP
- Tunnel
- sichere Befehlsausführung
```

Merksatz:

```
SSH = sicherer Fernzugriff.
```

Telnet

Telnet ist ein älteres Fernzugriffsprotokoll.

Typischer Port:

```
TCP 23
```

Problem:

```
Telnet ist unverschlüsselt.
```

Benutzernamen, Passwörter und Eingaben können mitgelesen werden.

Heute sollte man für Administration SSH verwenden.

Merksatz:

```
Telnet ist unsicher,
SSH ist die sichere Alternative.
```

SMB

SMB steht für:

```
Server Message Block
```

SMB wird häufig für Datei- und Druckerfreigaben verwendet.

Typischer Port:

```
TCP 445
```

Typische Nutzung:

```
- Windows-Dateifreigaben
- Netzlaufwerke
- Druckerfreigaben
- Dateiablage im LAN
```

Merksatz:

```
SMB = Datei- und Freigabedienst.
```

LDAP

LDAP steht für:

```
Lightweight Directory Access Protocol
```

LDAP dient zur Abfrage und Verwaltung von Verzeichnisdiensten.

Typische Nutzung:

```
- Benutzerverzeichnisse
- Gruppen
- Authentifizierungsinformationen
- zentrale Identitätsverwaltung
```

Typische Ports:

```
LDAP:
TCP/UDP 389

LDAPS:
TCP 636
```

Merksatz:

```
LDAP = Zugriff auf Verzeichnisdienste.
```

SNMP

SNMP steht für:

```
Simple Network Management Protocol
```

SNMP wird für Überwachung und Verwaltung von Netzwerkgeräten genutzt.

Typische Nutzung:

```
- Switches überwachen
- Router überwachen
- Drucker überwachen
- Serverwerte abfragen
- Monitoring-Systeme anbinden
```

Typische Ports:

```
UDP 161 für Abfragen
UDP 162 für Traps
```

Merksatz:

```
SNMP = Netzwerkgeräte überwachen.
```

NTP

NTP steht für:

```
Network Time Protocol
```

NTP synchronisiert die Uhrzeit von Systemen.

Typischer Port:

```
UDP 123
```

Korrekte Zeit ist wichtig für:

```
- Zertifikate
- Kerberos
- Logs
- Monitoring
- Fehlersuche
- Authentifizierung
```

Merksatz:

```
NTP = Zeitsynchronisation.
```

RDP

RDP steht für:

```
Remote Desktop Protocol
```

RDP wird für grafischen Fernzugriff verwendet, besonders bei Windows-Systemen.

Typischer Port:

```
TCP 3389
```

Wichtig:

```
RDP sollte nicht ungeschützt direkt ins Internet geöffnet werden.
```

Besser:

```
- VPN
- Zugriffsbeschränkung
- Multi-Faktor-Authentifizierung
- Remote Desktop Gateway
- starke Passwörter
```

Merksatz:

```
RDP = grafischer Fernzugriff,
sorgfältig absichern.
```

Anwendungsschicht und Benutzer

Schicht 7 ist die OSI-Schicht, die am nächsten an der Benutzeranwendung liegt.

Beispiele:

```
Browser lädt Webseite.
Mailprogramm ruft E-Mails ab.
Datei-Explorer öffnet Netzfreigabe.
Monitoring fragt Gerätedaten ab.
Admin verbindet sich per SSH.
```

Wichtig:

```
Der Benutzer sieht oft nur die Anwendung.
Technisch arbeitet die Anwendung mit Schicht-7-Protokollen.
```

Merksatz:

```
Schicht 7 ist die benutzernahe Netzwerkschicht.
```

Client und Server

Viele Anwendungsschicht-Protokolle arbeiten nach dem Client-Server-Prinzip.

Client:

```
stellt Anfrage
```

Server:

```
liefert Antwort oder Dienst
```

Beispiel HTTP:

```
Browser = Client
Webserver = Server
```

Beispiel DNS:

```
DNS-Resolver = Client
DNS-Server = Server
```

Merksatz:

```
Client fragt an,
Server antwortet.
```

Request und Response

Viele Anwendungsschicht-Protokolle arbeiten mit Anfrage und Antwort.

Beispiel HTTP:

```
Request:
Client fordert eine Webseite an.

Response:
Server liefert die Webseite zurück.
```

Beispiel DNS:

```
Request:
Client fragt nach IP-Adresse.

Response:
DNS-Server liefert Adresse zurück.
```

Merksatz:

```
Request = Anfrage.
Response = Antwort.
```

HTTP-Methoden

HTTP nutzt Methoden, um die Art einer Anfrage zu beschreiben.

Wichtige Methoden:

Methode	Bedeutung
GET	Daten abrufen
POST	Daten senden / erstellen
PUT	Daten ersetzen
PATCH	Daten teilweise ändern
DELETE	Daten löschen
HEAD	nur Kopfzeilen abrufen

Merksatz:

> GET liest.
> POST sendet.
> DELETE löscht.

HTTP-Statuscodes

HTTP-Statuscodes zeigen das Ergebnis einer Anfrage.

Wichtige Bereiche:

Bereich	Bedeutung
1xx	Information
2xx	Erfolg
3xx	Weiterleitung
4xx	Clientfehler
5xx	Serverfehler

Beispiele:

Statuscode	Bedeutung
200	OK
301	dauerhaft weitergeleitet

Statuscode	Bedeutung
302	vorübergehend weitergeleitet
400	fehlerhafte Anfrage
401	nicht authentifiziert
403	verboten
404	nicht gefunden
500	interner Serverfehler
502	Bad Gateway
503	Dienst nicht verfügbar

Merksatz:

```
2xx gut,
4xx Clientproblem,
5xx Serverproblem.
```

API

API steht für:

```
Application Programming Interface
```

Eine API ist eine Schnittstelle, über die Anwendungen miteinander kommunizieren.

Im Netzwerkumfeld sind Web-APIs häufig.

Sie nutzen oft:

```
- HTTP oder HTTPS
- JSON
- XML
- Tokens
- Statuscodes
```

Merksatz:

```
API = Schnittstelle zwischen Anwendungen.
```

REST kurz erklärt

REST ist ein Architekturstil für Web-APIs.

Typisch:

```
Ressourcen werden über URLs angesprochen.
HTTP-Methoden beschreiben die Aktion.
Daten werden häufig als JSON übertragen.
```

Beispiel:

```
GET /users
```

bedeutet sinngemäß:

```
Benutzerliste abrufen.
```

Merksatz:

```
REST nutzt HTTP-Ideen für APIs.
```

Anwendungsschicht und Authentifizierung

Viele Dienste müssen prüfen:

```
Wer bist du?
```

Das nennt man:

```
Authentifizierung
```

Beispiele:

```
- Benutzername und Passwort
- SSH-Schlüssel
- Zertifikat
```

```
- Token
- Multi-Faktor-Authentifizierung
```

Merksatz:

```
Authentifizierung prüft Identität.
```

Anwendungsschicht und Autorisierung

Autorisierung bedeutet:

```
Was darfst du?
```

Beispiel:

```
Benutzer ist angemeldet,
darf aber keine Adminseite öffnen.
```

Authentifizierung und Autorisierung unterscheiden:

```
Authentifizierung:
Wer bist du?

Autorisierung:
Was darfst du?
```

Merksatz:

```
Authentifizierung = Identität.
Autorisierung = Rechte.
```

Cookies und Sessions

Webanwendungen nutzen oft Cookies, um Sitzungen wiederzuerkennen.

Beispiel:

```
Benutzer meldet sich an.
Server setzt Session-Cookie.
Browser sendet Cookie bei weiteren Anfragen mit.
Server erkennt Benutzer wieder.
```

Schichtbezug:

```
Session = Schicht 5 / 7-Bezug
Cookie = Anwendungsschicht
HTTP = Anwendungsschicht
```

Merksatz:

```
Cookies helfen Webanwendungen,
Sitzungen wiederzuerkennen.
```

Anwendungsschicht und Datenformate

Schicht 7 arbeitet oft mit Datenformaten aus Schicht 6.

Beispiele:

```
HTTP überträgt HTML.
API überträgt JSON.
Mail enthält MIME-Strukturen.
Webserver liefert CSS, JavaScript, Bilder.
```

Darum sind Schicht 6 und 7 in der Praxis eng verbunden.

Merksatz:

```
Schicht 7 nutzt häufig Datenformate aus Schicht 6.
```

Anwendungsschicht und DNS-Probleme

DNS-Probleme wirken oft wie Internetprobleme.

Beispiel:

```
ping 8.8.8.8 funktioniert.
ping www.example.com funktioniert nicht.
```

Dann ist IP-Kommunikation grundsätzlich möglich, aber Namensauflösung funktioniert nicht.

Mögliche Ursachen:

```
- falscher DNS-Server
- DNS-Server nicht erreichbar
- falscher DNS-Eintrag
- DNS-Cache fehlerhaft
- Firewall blockiert DNS
- Domain nicht vorhanden
```

Merksatz:

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

Anwendungsschicht und HTTP-Fehler

Wenn TCP 443 erreichbar ist, aber die Webseite Fehler zeigt, liegt das Problem oft höher als Schicht 4.

Beispiele:

```
404 Not Found:
Ressource nicht gefunden.

500 Internal Server Error:
Anwendung oder Serverfehler.

502 Bad Gateway:
Proxy oder Gateway bekommt keine passende Antwort.

503 Service Unavailable:
Dienst nicht verfügbar.
```

Merksatz:

```
HTTP-Statuscodes helfen bei Schicht-7-Fehlersuche.
```

Anwendungsschicht und E-Mail-Fehler

E-Mail-Probleme können viele Ursachen haben.

Mögliche Prüfpunkte:

```
- SMTP-Server erreichbar?
- IMAP/POP3 erreichbar?
- Benutzer angemeldet?
- DNS MX-Record korrekt?
- Spamfilter blockiert?
- TLS korrekt?
- Authentifizierung korrekt?
- Mailbox voll?
- Sender oder Empfänger falsch?
```

Merksatz:

```
E-Mail-Fehler betreffen oft DNS, Authentifizierung, TLS und Mailprotokolle.
```

Anwendungsschicht und DHCP-Fehler

Wenn ein Client keine IP-Adresse erhält, denkt man oft zuerst an Schicht 3.

Aber DHCP selbst ist ein Anwendungsschicht-Protokoll.

Mögliche Ursachen:

```
- DHCP-Server nicht aktiv
- DHCP-Bereich erschöpft
- DHCP-Relay fehlt
- falsches VLAN
- Firewall blockiert UDP 67/68
- falsche DHCP-Optionen
- Dienstfehler am DHCP-Server
```

Merksatz:

```
DHCP vergibt IP-Daten,
ist aber ein Dienstprotokoll.
```

Anwendungsschicht und Sicherheit

Schicht 7 ist besonders wichtig für Sicherheit, weil dort konkrete Dienste und Benutzerinteraktion stattfinden.

Typische Risiken:

```
- schwache Passwörter
- fehlende MFA
- unsichere Webanwendungen
- fehlerhafte API-Berechtigungen
- unsichere Dateifreigaben
- veraltete Dienste
- Standardpasswörter
- offene Verwaltungsdienste
```

Merksatz:

```
Viele Angriffe zielen direkt auf Anwendungsschicht-Dienste.
```

Typische Schutzmaßnahmen auf Schicht 7

Beispiele:

```
- starke Authentifizierung
- Multi-Faktor-Authentifizierung
- sichere Passwörter
- Rechte nach Minimalprinzip
- Updates
- sichere Konfiguration
- Protokollierung
- Eingabevalidierung
- Web Application Firewall
```

- sichere API-Tokens
- nicht benötigte Dienste deaktivieren

Merksatz:

> Schicht-7-Sicherheit schützt konkrete Dienste und Anwendungen.

Was Schicht 7 nicht macht

Schicht 7 macht nicht:

- Bits als elektrische oder optische Signale übertragen
- MAC-Adressen im LAN verwenden
- IP-Pakete routen
- TCP-Verbindungen aufbauen
- Ports bereitstellen
- reine Verschlüsselungsschicht ersetzen

Diese Aufgaben liegen auf unteren Schichten.

Merksatz:

> Schicht 7 nutzt die unteren Schichten,
> ersetzt sie aber nicht.

Einordnung typischer Begriffe

Begriff	Schicht
HTTP	7
HTTPS	7 mit TLS-Bezug
DNS	7
DHCP	7
SMTP	7
IMAP	7
POP3	7
FTP	7

Begriff	Schicht
SSH	7
SMB	7
LDAP	7
SNMP	7
NTP	7
TCP-Port	4
IP-Adresse	3
MAC-Adresse	2

Merksatz:

> Dienstprotokolle wie HTTP, DNS und SMTP gehören zu Schicht 7.

Schicht 7 und Fehlersuche

Typische Fragen bei Schicht-7-Problemen:

> Funktioniert IP-Erreichbarkeit?
> Ist der Port erreichbar?
> Läuft der Dienst?
> Stimmt der DNS-Name?
> Antwortet die Anwendung?
> Gibt es HTTP-Statuscodes?
> Funktioniert die Anmeldung?
> Sind Rechte korrekt?
> Ist TLS gültig?
> Stimmen Datenformat und API-Anfrage?
> Gibt es Fehlermeldungen in Logs?

Merksatz:

> Bei Schicht 7 prüft man Dienst, Inhalt, Anmeldung und Anwendung.

Fehlerbild: Webseite öffnet nicht

Mögliche Ursachen auf verschiedenen Schichten:

Schicht 3:
keine Route, falsches Gateway

Schicht 4:
TCP 80 oder 443 blockiert

Schicht 6:
TLS-Zertifikat fehlerhaft

Schicht 7:
Webserverfehler, falscher Pfad, HTTP 500

Merksatz:

Webfehler können mehrere Schichten betreffen.

Fehlerbild: Login funktioniert nicht

Mögliche Ursachen:

- falscher Benutzername
- falsches Passwort
- Konto gesperrt
- MFA fehlt
- Session-Cookie blockiert
- Zeitproblem bei Tokens
- Berechtigung fehlt
- Authentifizierungsdienst nicht erreichbar
- LDAP oder Verzeichnisdienst gestört

Merksatz:

Loginfehler sind meist Anwendung, Authentifizierung oder Sitzung.

Fehlerbild: API antwortet mit Fehler

Mögliche Ursachen:

```
- falsche URL
- falsche HTTP-Methode
- fehlender Token
- falsche Berechtigung
- ungültiges JSON
- falscher Content-Type
- Serverfehler
- Rate Limit
- falsche API-Version
```

Merksatz:

```
API-Fehler betreffen oft Methode, Datenformat, Token oder Rechte.
```

Fehlerbild: DNS löst falsch auf

Mögliche Ursachen:

```
- falscher A-Record
- falscher AAAA-Record
- alter DNS-Cache
- falscher DNS-Server
- Split-DNS-Konfiguration
- Tippfehler im Namen
- Zone nicht aktualisiert
- TTL noch nicht abgelaufen
```

Merksatz:

```
Falscher DNS-Eintrag kann zum falschen Server führen.
```

Fehlerbild: E-Mail kommt nicht an

Mögliche Ursachen:

```
- falscher MX-Record
- SMTP blockiert
```

- Spamfilter
- SPF, DKIM oder DMARC fehlerhaft
- Mailbox voll
- Empfängeradresse falsch
- TLS-Problem
- Authentifizierung fehlerhaft
- Blacklisting

Merksatz:

Mailzustellung hängt stark von DNS, SMTP und Sicherheitsprüfungen ab.

Schicht 7 und Logs

Logs sind bei Schicht-7-Fehlern besonders wichtig.

Typische Logs:

- Webserver-Log
- Anwendungslog
- Authentifizierungslog
- Mailserver-Log
- DNS-Log
- Proxy-Log
- API-Log
- Firewall-Log

Logs zeigen oft:

- konkrete Fehlermeldungen
- Statuscodes
- Benutzer
- Zeitpunkt
- Quelle
- Anfragepfad
- Antwortcode

Merksatz:

Schicht-7-Fehler findet man oft in Anwendungs- und Dienstlogs.

Typische IHK-Fragen

In AP1 und AP2 kann zum Beispiel gefragt werden:

- Welche Aufgabe hat die Anwendungsschicht?
- Welche Protokolle gehören zur Anwendungsschicht?
- Was ist der Unterschied zwischen HTTP und HTTPS?
- Was macht DNS?
- Was ist der Unterschied zwischen A- und AAAA-Record?
- Was macht DHCP?
- Warum ist DHCP trotz IP-Bezug ein Anwendungsschicht-Protokoll?
- Welche Mailprotokolle gibt es?
- Was ist der Unterschied zwischen SMTP, POP3 und IMAP?
- Was macht SMB?
- Was macht LDAP?
- Was macht SNMP?
- Was bedeuten HTTP-Statuscodes?
- Warum reicht ein erfolgreicher Ping nicht für einen funktionierenden Dienst?
- Warum können Schicht-7-Fehler trotz offener Ports auftreten?

Typische Prüfungsfallen

Schicht 7 heißt Anwendungsschicht.

Schicht 7 ist nicht einfach das Programm selbst.

Anwendungen nutzen Schicht-7-Protokolle.

HTTP gehört zu Schicht 7.

HTTPS gehört zu Schicht 7,
nutzt aber TLS.

DNS gehört zu Schicht 7.

DHCP gehört zu Schicht 7,
obwohl es IP-Konfiguration vergibt.

Port gehört zu Schicht 4.

Dienstprotokoll gehört zu Schicht 7.

TCP 443 offen bedeutet nicht automatisch,
dass die Webseite funktioniert.

HTTP-Statuscode 404 ist ein Anwendungsschicht-Hinweis.

HTTP-Statuscode 500 deutet auf Server- oder Anwendungsproblem hin.

SMTP sendet E-Mails.

POP3 und IMAP empfangen E-Mails.

SFTP ist nicht FTPS.

Telnet ist unverschlüsselt.

SSH ist sicherer als Telnet.

Wichtige Begriffe kurz erklärt

Begriff	Kurze Erklärung
Anwendungsschicht	OSI-Schicht 7
HTTP	Webprotokoll
HTTPS	HTTP über TLS
DNS	Namensauflösung
DHCP	automatische IP-Konfiguration
SMTP	E-Mail senden
POP3	E-Mail abrufen
IMAP	E-Mail abrufen und verwalten
FTP	Dateiübertragung
SFTP	Dateiübertragung über SSH

Begriff	Kurze Erklärung
FTPS	FTP mit TLS
SSH	sicherer Fernzugriff
SMB	Datei- und Druckerfreigaben
LDAP	Verzeichnisdienstzugriff
SNMP	Netzwerkmanagement
NTP	Zeitsynchronisation
API	Schnittstelle zwischen Anwendungen
REST	Architekturstil für Web-APIs
Request	Anfrage
Response	Antwort
Statuscode	Ergebnis einer HTTP-Anfrage
Authentifizierung	Identität prüfen
Autorisierung	Rechte prüfen

IHK-sichere Kurzformulierung

Die Anwendungsschicht ist Schicht 7 des OSI-Modells. Sie stellt Netzwerkdienste für Anwendungen bereit. Typische Protokolle der Anwendungsschicht sind HTTP, HTTPS, DNS, DHCP, SMTP, POP3, IMAP, FTP, SSH, SMB, LDAP, SNMP und NTP. Die Anwendungsschicht ist nicht einfach das Programm selbst, sondern umfasst die Protokolle und Dienste, die Anwendungen für die Netzwerkkommunikation verwenden. Ports gehören zur Transportschicht, während die eigentlichen Dienstprotokolle zur Anwendungsschicht gehören. Fehler auf Schicht 7 betreffen häufig Dienste, Anmeldungen, DNS, HTTP-Statuscodes, APIs, Datenformate oder Berechtigungen.

Merksätze

```
Schicht 7 = Anwendungsschicht.

Schicht 7 = Netzwerkdienste für Anwendungen.

Anwendung nutzt Schicht-7-Protokoll.

Browser ist Anwendung,
HTTP ist Protokoll.

Port gehört zu Schicht 4.
```

Dienstprotokoll gehört zu Schicht 7.

HTTP = Webprotokoll.

HTTPS = HTTP über TLS.

DNS = Name zu IP-Adresse.

A-Record = IPv4.

AAAA-Record = IPv6.

MX = Mailserver.

DHCP = automatische IP-Konfiguration.

DHCP ist trotz IP-Bezug Schicht 7.

SMTP sendet E-Mails.

POP3 ruft E-Mails ab.

IMAP verwaltet E-Mails auf dem Server.

FTP ist klassische Dateiübertragung.

SFTP ist Dateiübertragung über SSH.

FTPS ist FTP mit TLS.

SSH = sicherer Fernzugriff.

SMB = Datei- und Druckerfreigaben.

LDAP = Verzeichnisdienst.

SNMP = Netzwerküberwachung.

NTP = Zeitsynchronisation.

2xx = Erfolg.

4xx = Clientfehler.

5xx = Serverfehler.

Offener Port heißt nicht automatisch:
Anwendung funktioniert.

Schicht 7 prüft Dienst,
Inhalt,
Anmeldung
und Berechtigung.