10.5 E-Mail-Protokolle: SMTP, POP3 und IMAP

E-Mail-Kommunikation gehört zur OSI-Schicht 7.

Dabei arbeiten mehrere Protokolle zusammen.

Die wichtigsten E-Mail-Protokolle sind:

- SMTP
- POP3
- IMAP

Sie haben unterschiedliche Aufgaben.

SMTP wird verwendet für:

E-Mails senden und transportieren.

POP3 und IMAP werden verwendet für:

E-Mails abrufen.

Merksatz:

SMTP sendet.
POP3 und IMAP empfangen.

Grundidee von E-Mail-Kommunikation

E-Mail ist kein einzelner einfacher Vorgang.

Beim Senden und Empfangen arbeiten mehrere Bestandteile zusammen:

- E-Mail-Client
- Mailserver
- DNS
- SMTP
- POP3 oder IMAP

- Authentifizierung
- TLS
- Spam- und Sicherheitsprüfungen

Beispiel:

Benutzer schreibt E-Mail im Mailprogramm.
Mailprogramm sendet E-Mail an Mailserver.
Mailserver transportiert E-Mail weiter.
Empfänger ruft E-Mail vom eigenen Mailserver ab.

Merksatz:

E-Mail nutzt mehrere Protokolle und Dienste zusammen.

E-Mail im OSI-Modell

E-Mail-Protokolle gehören zur Anwendungsschicht.

Thema	Schicht
SMTP	7
POP3	7
IMAP	7
DNS MX-Record	7
TLS	6 mit Schicht-7-Bezug
TCP-Port	4
IP-Adresse	3

Wichtig:

Die Protokolle SMTP, POP3 und IMAP gehören zu Schicht 7.
Die zugehörigen Ports gehören zu Schicht 4.

Merksatz:

Mailprotokoll = Schicht 7.
Mailport = Schicht 4.

SMTP

SMTP steht für:

```
Simple Mail Transfer Protocol
```

SMTP wird verwendet für:

```
- E-Mails senden
- E-Mails zwischen Mailservern transportieren
- E-Mails an den nächsten Mailserver weitergeben
```

Typischer Port:

```
TCP 25
```

Weitere häufige Ports:

```
TCP 587
TCP 465
```

Merksatz:

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

SMTP zwischen Mailservern

Wenn ein Mailserver eine E-Mail an eine andere Domain zustellen möchte, nutzt er SMTP.

Beispiel:

```
absender@firma-a.de
sendet an
empfaenger@firma-b.de
```

Der Mailserver von firma-a.de fragt per DNS, welcher Mailserver für firma-b.de zuständig ist.

Danach wird die E-Mail per SMTP an diesen Mailserver übertragen.

Merksatz:

```
Mailserver transportieren E-Mails untereinander mit SMTP.
```

SMTP Submission

SMTP Submission bedeutet:

```
Ein Mailclient übergibt eine ausgehende E-Mail an den eigenen Mailserver.
```

Typischer Port:

```
TCP 587
```

Dabei wird normalerweise Authentifizierung verwendet.

Beispiel:

```
Mailprogramm meldet sich am Mailserver an
und sendet die E-Mail über Port 587.
```

Merksatz:

```
Port 587 ist typisch für authentifiziertes Senden durch Clients.
```

SMTPS

SMTPS bezeichnet SMTP mit direkter TLS-Verschlüsselung.

Typischer Port:

```
TCP 465
```

Wichtig:

```
TCP 465 startet normalerweise direkt mit TLS.
```

Bei STARTTLS dagegen beginnt die Verbindung zunächst unverschlüsselt und wird dann auf TLS umgestellt.

Merksatz:

> SMTPS = SMTP direkt über TLS.

SMTP-Port 25, 587 und 465 unterscheiden

Port	Zweck	Kurz erklärt
25	SMTP	Mailserver zu Mailserver
587	Submission	Client sendet authentifiziert an Mailserver
465	SMTPS	SMTP direkt über TLS

Prüfungsfalle:

> Port 25 ist nicht der typische Port,
> über den moderne Mailclients ihre E-Mails authentifiziert einreichen.

Merksatz:

> 25 Servertransport,
> 587 Client-Abgabe,
> 465 SMTP über TLS.

POP3

POP3 steht für:

> Post Office Protocol Version 3

POP3 wird verwendet zum:

> Abrufen von E-Mails vom Mailserver.

Typischer Port:

```
TCP 110
```

Verschlüsselte Variante:

```
POP3S:
TCP 995
```

POP3 lädt E-Mails häufig vom Server herunter.

Je nach Einstellung können sie danach vom Server gelöscht werden.

Merksatz:

```
POP3 = E-Mails einfach abrufen.
```

POP3-Grundidee

POP3 ist eher einfach aufgebaut.

Typischer Ablauf:

```
Client verbindet sich mit Mailserver.
Client meldet sich an.
Client ruft E-Mails ab.
E-Mails werden lokal gespeichert.
E-Mails können vom Server gelöscht werden.
```

POP3 eignet sich weniger gut, wenn mehrere Geräte dieselbe Mailbox synchron nutzen sollen.

Merksatz:

```
POP3 ist einfach,
aber weniger gut für moderne Mehrgeräte-Synchronisation.
```

IMAP

IMAP steht für:

```
Internet Message Access Protocol
```

IMAP wird verwendet zum:

```
Abrufen und Verwalten von E-Mails auf dem Server.
```

Typischer Port:

```
TCP 143
```

Verschlüsselte Variante:

```
IMAPS:
TCP 993
```

IMAP lässt E-Mails normalerweise auf dem Server und synchronisiert den Zustand zwischen mehreren Geräten.

Merksatz:

```
IMAP = E-Mails auf dem Server verwalten und synchronisieren.
```

IMAP-Grundidee

Bei IMAP bleiben E-Mails meist auf dem Mailserver.

Der Client synchronisiert:

```
- Posteingang
- Ordner
- gelesen / ungelesen
- gelöscht
- verschoben
- gesendet
- Markierungen
```

Das ist praktisch bei mehreren Geräten.

Beispiel:

E-Mail auf dem Smartphone gelesen.
Am Notebook ist sie ebenfalls als gelesen markiert.

Merksatz:

IMAP eignet sich gut für mehrere Geräte.

POP3 und IMAP vergleichen

Merkmal	POP3	IMAP
Hauptzweck	E-Mails abrufen	E-Mails abrufen und verwalten
Speicherort	oft lokal beim Client	meist auf dem Server
Synchronisation	eingeschränkt	gut
mehrere Geräte	weniger geeignet	gut geeignet
Ordnerverwaltung	begrenzt	umfangreicher
typischer Port	TCP 110	TCP 143
verschlüsselt	TCP 995	TCP 993

Merksatz:

POP3 lädt eher herunter.
IMAP synchronisiert mit dem Server.

SMTP, POP3 und IMAP direkt vergleichen

Protokoll	Aufgabe	typischer Port
SMTP	E-Mail senden / transportieren	TCP 25
Submission	E-Mail vom Client einreichen	TCP 587
SMTPS	SMTP direkt über TLS	TCP 465
POP3	E-Mail abrufen	TCP 110
POP3S	POP3 über TLS	TCP 995
IMAP	E-Mail abrufen und verwalten	TCP 143
IMAPS	IMAP über TLS	TCP 993

Merksatz:

```
SMTP raus.
POP3/IMAP rein.
```

E-Mail-Client

Ein E-Mail-Client ist ein Programm oder eine App, mit der Benutzer E-Mails senden und empfangen.

Beispiele:

```
- Outlook
- Thunderbird
- Apple Mail
- Smartphone-Mail-App
- Webmail im Browser
```

Der Client nutzt je nach Einrichtung:

```
SMTP zum Senden
IMAP oder POP3 zum Empfangen
```

Merksatz:

```
Mailclient nutzt SMTP zum Senden und IMAP/POP3 zum Empfangen.
```

Mailserver

Ein Mailserver nimmt E-Mails an, speichert sie und leitet sie weiter.

Typische Aufgaben:

```
- E-Mails von Clients annehmen
- E-Mails von anderen Mailservern empfangen
- E-Mails an andere Mailserver weiterleiten
- Postfächer bereitstellen
- Spamprüfung durchführen
- Virenprüfung durchführen
```

- TLS und Authentifizierung nutzen

Merksatz:

Mailserver transportiert und verwaltet E-Mails.

Webmail

Webmail bedeutet:

E-Mails werden über eine Webseite genutzt.

Beispiel:

Benutzer öffnet Mailbox im Browser.

Dabei nutzt der Browser:

HTTP oder HTTPS

Der Webmail-Server selbst kann intern trotzdem mit Maildiensten, Datenbanken oder IMAP arbeiten.

Merksatz:

Webmail nutzt im Browser HTTP/HTTPS,
Mailserver dahinter nutzen Mailprotokolle.

DNS und E-Mail

DNS ist für E-Mail sehr wichtig.

Wichtige DNS-Records:

Record	Zweck
MX	zuständiger Mailserver einer Domain
A / AAAA	IP-Adresse des Mailservers
PTR	Reverse-DNS

Record	Zweck
TXT	SPF, DKIM, DMARC

Ohne korrekte DNS-Einträge kann E-Mail-Zustellung scheitern.

Merksatz:

```
E-Mail-Zustellung hängt stark von DNS ab.
```

MX-Record

MX steht für:

```
Mail Exchanger
```

Ein MX-Record sagt, welcher Mailserver für eine Domain zuständig ist.

Beispiel:

```
firma.de
MX 10 mail.firma.de
```

Die Zahl ist die Priorität.

Kleinere Zahl bedeutet:

```
höhere Priorität
```

Merksatz:

```
MX zeigt auf zuständigen Mailserver.
```

Mailzustellung mit MX vereinfacht

Ablauf:

```
1. Absender-Mailserver erhält E-Mail an benutzer@firma.de.
2. Er fragt DNS nach MX-Record für firma.de.
```

3. DNS liefert zuständigen Mailserver.
4. Absender-Mailserver verbindet sich per SMTP.
5. Empfänger-Mailserver nimmt E-Mail an.
6. Empfänger ruft E-Mail per IMAP, POP3 oder Webmail ab.

Merksatz:

MX sagt,
wohin E-Mail für eine Domain geliefert werden soll.

PTR und Reverse DNS bei E-Mail

PTR-Records sind bei Mailservern wichtig.

Ein PTR-Record ordnet eine IP-Adresse einem Namen zu.

Viele empfangende Mailserver prüfen, ob der sendende Mailserver einen sinnvollen Reverse-DNS-Eintrag hat.

Fehlender oder falscher PTR kann die Zustellbarkeit verschlechtern.

Merksatz:

Reverse DNS ist bei Mailservern wichtig für Vertrauenswürdigkeit.

SPF

SPF steht für:

Sender Policy Framework

SPF wird als TXT-Record im DNS veröffentlicht.

SPF legt fest, welche Server für eine Domain E-Mails senden dürfen.

Beispiel sinngemäß:

Nur diese Mailserver dürfen E-Mails für firma.de senden.

Merksatz:

```
SPF sagt,
welche Server für eine Domain senden dürfen.
```

DKIM

DKIM steht für:

```
DomainKeys Identified Mail
```

DKIM signiert E-Mails kryptografisch.

Der öffentliche Schlüssel wird im DNS als TXT-Record veröffentlicht.

Empfangende Mailserver können prüfen:

```
Wurde die E-Mail wirklich passend signiert?
Wurde sie unterwegs verändert?
```

Merksatz:

```
DKIM signiert E-Mails und hilft bei Integritätsprüfung.
```

DMARC

DMARC steht für:

```
Domain-based Message Authentication, Reporting and Conformance
```

DMARC baut auf SPF und DKIM auf.

DMARC legt fest, wie Empfänger mit E-Mails umgehen sollen, wenn SPF oder DKIM nicht passen.

Mögliche Richtlinien:

```
- nur berichten
- Quarantäne
- ablehnen
```

Merksatz:

```
DMARC steuert den Umgang mit SPF-/DKIM-Fehlern.
```

SPF, DKIM und DMARC unterscheiden

Verfahren	Hauptaufgabe
SPF	erlaubt sendende Server
DKIM	signiert E-Mails
DMARC	legt Umgang mit Prüfungsfehlern fest

Merksatz:

```
SPF erlaubt.
DKIM signiert.
DMARC entscheidet.
```

STARTTLS bei E-Mail

STARTTLS bedeutet:

```
Eine Verbindung beginnt zunächst unverschlüsselt
und wird dann auf TLS umgestellt.
```

STARTTLS wird häufig bei Mailprotokollen verwendet.

Beispiele:

```
- SMTP
- IMAP
- POP3
```

Wichtig:

```
STARTTLS ist nicht dasselbe wie ein von Anfang an verschlüsselter eigener TLS-Port.
```

Merksatz:

STARTTLS startet unverschlüsselt und schaltet dann auf TLS um.

E-Mail und TLS

TLS schützt E-Mail-Verbindungen beim Transport.

Beispiele:

- SMTP mit STARTTLS
- SMTPS
- IMAPS
- POP3S

Wichtig:

TLS schützt die Verbindung zwischen zwei Kommunikationspunkten.
Das ist nicht automatisch Ende-zu-Ende-Verschlüsselung des E-Mail-Inhalts.

Merksatz:

TLS schützt die Mailverbindung,
aber nicht automatisch den Inhalt bis zum endgültigen Empfänger.

Ende-zu-Ende-Verschlüsselung bei E-Mail

Ende-zu-Ende-Verschlüsselung bedeutet:

Der Inhalt bleibt vom Absender bis zum Empfänger geschützt.

Beispiele:

- S/MIME
- OpenPGP

Dabei können Zwischenserver die Inhalte nicht einfach lesen.

Unterschied zu TLS:

TLS schützt die Verbindung.
Ende-zu-Ende-Verschlüsselung schützt den Inhalt selbst.

Merksatz:

TLS ist Transportverschlüsselung.
S/MIME oder OpenPGP schützen den Mailinhalt Ende-zu-Ende.

E-Mail-Adresse

Eine E-Mail-Adresse besteht aus:

lokaler Teil
@
Domain

Beispiel:

felix@firma.de

Dabei ist:

felix = lokaler Teil
firma.de = Domain

Für die Domain wird per DNS der zuständige Mailserver gesucht.

Merksatz:

Rechts vom @ steht die Maildomain.

Postfach und Alias

Ein Postfach ist ein echter Speicherbereich für E-Mails.

Ein Alias ist eine zusätzliche Adresse, die auf ein Postfach oder eine Gruppe zeigen kann.

Beispiel:

```
Postfach:
felix@firma.de

Alias:
support@firma.de
```

E-Mails an support@firma.de landen im Postfach oder bei einer Gruppe.

Merksatz:

```
Postfach speichert.
Alias leitet zu.
```

Verteilergruppe

Eine Verteilergruppe sendet eine E-Mail an mehrere Empfänger weiter.

Beispiel:

```
it-team@firma.de
```

geht an:

```
admin1@firma.de
admin2@firma.de
support@firma.de
```

Merksatz:

```
Verteilergruppe verteilt an mehrere Empfänger.
```

Shared Mailbox

Eine Shared Mailbox ist ein gemeinsames Postfach.

Beispiel:

```
support@firma.de
```

Mehrere Benutzer können Zugriff haben.

Typische Nutzung:

```
- Support
- Info-Adresse
- Team-Postfach
- Bewerbungen
- Rechnungen
```

Merksatz:

```
Shared Mailbox = gemeinsames Postfach für mehrere Benutzer.
```

Postfachgröße

Ein Postfach kann eine Größenbegrenzung haben.

Wenn das Postfach voll ist, können Probleme auftreten.

Mögliche Folgen:

```
- neue E-Mails werden abgewiesen
- Benutzer kann nicht senden
- Synchronisation schlägt fehl
- Warnungen im Mailclient
```

Merksatz:

```
Volles Postfach kann Mailprobleme verursachen.
```

Spamfilter

Spamfilter prüfen eingehende E-Mails auf unerwünschte oder gefährliche Inhalte.

Kriterien können sein:

- Absenderreputation
- Inhalt
- Links
- Anhänge
- SPF
- DKIM
- DMARC
- bekannte Schadsoftware
- ungewöhnliches Verhalten

Merksatz:

Spamfilter entscheiden,
ob E-Mails zugestellt, markiert oder blockiert werden.

Quarantäne

Quarantäne bedeutet:

Eine E-Mail wird nicht direkt zugestellt,
sondern zurückgehalten.

Gründe:

- Spamverdacht
- Malwareverdacht
- gefährlicher Anhang
- Phishingverdacht
- Richtlinienverstoß

Administrator oder Benutzer können je nach System prüfen, ob die Mail freigegeben werden soll.

Merksatz:

Quarantäne hält verdächtige Mails zurück.

Phishing

Phishing ist der Versuch, Benutzer zur Preisgabe sensibler Informationen zu bringen.

Beispiele:

```
- gefälschte Login-Seite
- angebliche Paketbenachrichtigung
- falsche Rechnung
- gefälschte Bank-Mail
- angeblicher IT-Support
```

Ziel:

```
Zugangsdaten,
Zahlungsdaten
oder Zugriff auf Systeme
```

Merksatz:

```
Phishing täuscht Benutzer,
um Daten oder Zugriff zu erhalten.
```

Anhänge und Sicherheit

E-Mail-Anhänge können gefährlich sein.

Risiken:

```
- Schadsoftware
- Makros
- manipulierte Dokumente
- Archive mit Malware
- ausführbare Dateien
- Phishing-Dokumente
```

Schutzmaßnahmen:

```
- Anhänge prüfen
- Makros einschränken
```

- Antivirus
- Sandboxing
- Schulung der Benutzer
- Dateitypen filtern

Merksatz:

E-Mail-Anhänge sind ein häufiger Angriffsweg.

E-Mail-Header

E-Mail-Header enthalten technische Informationen.

Beispiele:

- Absender
- Empfänger
- Betreff
- Versandzeit
- Mailserver-Wege
- Message-ID
- SPF/DKIM/DMARC-Ergebnisse
- Received-Zeilen

Header helfen bei der Fehlersuche und Sicherheitsanalyse.

Merksatz:

Mail-Header zeigen technische Zustellinformationen.

Received-Header

Received-Header zeigen, über welche Mailserver eine E-Mail gelaufen ist.

Jeder Mailserver fügt typischerweise eine Received-Zeile hinzu.

Damit kann man den Weg einer E-Mail nachvollziehen.

Merksatz:

```
Received-Header zeigen den Mailtransportweg.
```

Bounce-Mail

Eine Bounce-Mail ist eine automatische Fehlermeldung, wenn eine E-Mail nicht zugestellt werden konnte.

Mögliche Gründe:

```
- Empfänger existiert nicht
- Postfach voll
- Domain existiert nicht
- Mailserver nicht erreichbar
- Nachricht wurde abgelehnt
- Spamprüfung fehlgeschlagen
```

Merksatz:

```
Bounce-Mail informiert über Zustellfehler.
```

NDR

NDR steht für:

```
Non-Delivery Report
```

Das ist eine Nichtzustellbarkeitsmeldung.

Sie enthält häufig:

```
- Fehlercode
- Grund der Ablehnung
- Zieladresse
- Zeit
- beteiligter Mailserver
```

Merksatz:

NDR = Meldung über nicht zugestellte E-Mail.

Typische SMTP-Fehlercodes

SMTP nutzt Antwortcodes.

Grobe Einordnung:

Bereich	Bedeutung
2xx	Erfolg
4xx	temporärer Fehler
5xx	dauerhafter Fehler

Beispiele:

Code	Bedeutung
250	OK
421	Dienst nicht verfügbar
450	Mailbox vorübergehend nicht verfügbar
550	Mailbox nicht gefunden oder abgelehnt
554	Nachricht abgelehnt

Merksatz:

4xx kann später erneut versucht werden.
5xx ist meist dauerhaft.

E-Mail-Fehlersuche: Senden

Wenn E-Mail-Senden nicht funktioniert, prüft man:

- SMTP-Server korrekt?
- richtiger Port?
- Authentifizierung korrekt?
- TLS erforderlich?
- Benutzer darf senden?
- Absenderadresse erlaubt?

- DNS korrekt?
- Firewall blockiert?
- Mailserver-Logs?
- Fehlermeldung oder NDR?

Merksatz:

Beim Senden SMTP, Authentifizierung, TLS und DNS prüfen.

E-Mail-Fehlersuche: Empfangen

Wenn E-Mail-Empfang nicht funktioniert, prüft man:

- MX-Record korrekt?
- Mailserver erreichbar?
- Postfach vorhanden?
- Postfach voll?
- Spamfilter oder Quarantäne?
- POP3/IMAP erreichbar?
- Client korrekt konfiguriert?
- TLS und Anmeldung korrekt?
- Mailserver-Logs?

Merksatz:

Beim Empfangen MX, Postfach, Spamfilter und Abrufprotokoll prüfen.

Fehlerbild: Mail kommt nicht an

Mögliche Ursachen:

- falsche Empfängeradresse
- MX-Record falsch
- Mailserver nicht erreichbar
- Spamfilter blockiert
- Quarantäne
- Postfach voll

- SPF/DKIM/DMARC-Fehler
- Absender blockiert
- Domain falsch
- NDR beachten

Merksatz:

Nicht zugestellte Mail immer mit NDR und Logs prüfen.

Fehlerbild: Mail landet im Spam

Mögliche Ursachen:

- schlechter Absender-Ruf
- SPF fehlt oder falsch
- DKIM fehlt oder falsch
- DMARC fehlt oder streng
- Inhalt wirkt verdächtig
- Links sind auffällig
- Anhänge sind verdächtig
- fehlender PTR-Record
- neue oder schlecht bewertete Domain

Merksatz:

Spamprobleme oft mit DNS-Authentifizierung und Inhalt prüfen.

Fehlerbild: Mailclient kann nicht senden

Mögliche Ursachen:

- falscher SMTP-Server
- falscher Port
- Authentifizierung falsch
- TLS-Einstellung falsch
- Passwort falsch
- Benutzer darf nicht senden

- Firewall blockiert
- Provider blockiert Port 25
- Konto gesperrt

Merksatz:

Sendeprobleme am Client betreffen oft SMTP, Port, TLS und Login.

Fehlerbild: Mailclient kann nicht empfangen

Mögliche Ursachen:

- falscher IMAP- oder POP3-Server
- falscher Port
- falsches Passwort
- TLS-Einstellung falsch
- Postfach voll
- Konto gesperrt
- Firewall blockiert
- Serverdienst gestört
- Zertifikatsfehler

Merksatz:

Empfangsprobleme am Client betreffen IMAP/POP3, Port, TLS und Login.

Fehlerbild: Zertifikatswarnung im Mailclient

Mögliche Ursachen:

- Zertifikat abgelaufen
- Name passt nicht zum Zertifikat
- falscher Mailserver eingetragen
- interne CA nicht vertraut
- Zwischenzertifikat fehlt
- falsche Systemzeit
- Proxy oder Sicherheitssoftware greift ein

Merksatz:

> Mail-Zertifikatsfehler wie HTTPS-Zertifikatsfehler prüfen.

Fehlerbild: E-Mail verzögert

Mögliche Ursachen:

- Greylisting
- temporärer SMTP-Fehler
- überlasteter Mailserver
- DNS-Probleme
- Spamprüfung dauert
- Zielserver nicht erreichbar
- Warteschlange auf Mailserver
- Rate Limits

Merksatz:

> Verzögerte Mail kann durch temporäre Fehler oder Warteschlangen entstehen.

Greylisting

Greylisting ist eine Anti-Spam-Technik.

Dabei lehnt der empfangende Server eine Mail zunächst temporär ab.

Ein seriöser Mailserver versucht später erneut zuzustellen.

Viele Spam-Systeme versuchen das nicht.

Merksatz:

> Greylisting verzögert E-Mails absichtlich zur Spamabwehr.

Was E-Mail-Protokolle nicht machen

E-Mail-Protokolle machen nicht automatisch:

- DNS korrekt konfigurieren
- Benutzer sicher schulen
- Phishing vollständig verhindern
- Anhänge automatisch ungefährlich machen
- Postfachgrößen unbegrenzt machen
- Ende-zu-Ende-Verschlüsselung erzwingen
- SPF/DKIM/DMARC automatisch korrekt setzen

Merksatz:

E-Mail braucht Protokolle,
DNS,
Sicherheit
und Administration zusammen.

Einordnung in das OSI-Modell

Thema	Schicht
SMTP	7
POP3	7
IMAP	7
DNS MX	7
SPF/DKIM/DMARC	7 mit Sicherheitsbezug
TLS bei Mail	6 mit Schicht-7-Bezug
TCP-Port 25/587/465/110/143/993/995	4
IP-Adresse des Mailservers	3
MAC-Adresse	2

Merksatz:

Mailprotokolle gehören zu Schicht 7,
ihre Ports zu Schicht 4.

Typische IHK-Fragen

In AP1 und AP2 kann zum Beispiel gefragt werden:

- Welche Protokolle werden für E-Mail verwendet?
- Wofür wird SMTP genutzt?
- Wofür wird POP3 genutzt?
- Wofür wird IMAP genutzt?
- Was ist der Unterschied zwischen POP3 und IMAP?
- Welche Ports nutzen SMTP, POP3 und IMAP?
- Was ist SMTP Submission?
- Was ist STARTTLS?
- Was ist ein MX-Record?
- Warum ist DNS für E-Mail wichtig?
- Was machen SPF, DKIM und DMARC?
- Was ist ein NDR?
- Warum landet eine Mail im Spam?
- Warum ist TLS bei Mail nicht automatisch Ende-zu-Ende-Verschlüsselung?

Typische Prüfungsfallen

SMTP sendet E-Mails.

POP3 ruft E-Mails ab.

IMAP ruft E-Mails ab und verwaltet sie auf dem Server.

SMTP zwischen Mailservern nutzt häufig TCP 25.

SMTP Submission nutzt häufig TCP 587.

SMTPS nutzt häufig TCP 465.

POP3 nutzt TCP 110.

POP3S nutzt TCP 995.

IMAP nutzt TCP 143.

IMAPS nutzt TCP 993.

SMTP ist nicht zum Abrufen von E-Mails gedacht.

POP3 ist weniger gut für mehrere Geräte.

IMAP ist besser für Synchronisation.

MX-Record zeigt zuständigen Mailserver.

SPF erlaubt sendende Server.

DKIM signiert E-Mails.

DMARC legt Umgang mit Fehlern fest.

TLS schützt Verbindung,
aber nicht automatisch Ende-zu-Ende den Inhalt.

Mailprobleme können DNS-, TLS-, Spamfilter- oder Postfachprobleme sein.

Wichtige Begriffe kurz erklärt

Begriff	Kurze Erklärung
SMTP	Protokoll zum Senden und Weiterleiten von E-Mails
POP3	Protokoll zum einfachen Abrufen von E-Mails
IMAP	Protokoll zum Abrufen und Verwalten von E-Mails
Submission	authentifiziertes Einreichen von E-Mails
SMTPS	SMTP direkt über TLS
POP3S	POP3 über TLS
IMAPS	IMAP über TLS
MX	DNS-Eintrag für zuständigen Mailserver
PTR	Reverse-DNS-Eintrag
SPF	legt erlaubte sendende Server fest
DKIM	kryptografische Signatur für E-Mails
DMARC	Richtlinie für SPF-/DKIM-Auswertung
STARTTLS	Umschalten auf TLS innerhalb einer Verbindung
S/MIME	Ende-zu-Ende-Verschlüsselung und Signatur für E-Mail
OpenPGP	Ende-zu-Ende-Verschlüsselung für E-Mail

Begriff	Kurze Erklärung
Postfach	Speicherbereich für E-Mails
Alias	zusätzliche Adresse für ein Postfach
Shared Mailbox	gemeinsames Postfach
Spamfilter	Filter gegen unerwünschte E-Mails
Quarantäne	zurückgehaltene verdächtige E-Mail
NDR	Nichtzustellbarkeitsmeldung
Bounce	automatische Fehlermeldung bei Zustellproblem

IHK-sichere Kurzformulierung

E-Mail-Kommunikation gehört zur Anwendungsschicht des OSI-Modells und nutzt mehrere Protokolle. SMTP dient dem Senden und Weiterleiten von E-Mails, POP3 und IMAP dienen dem Abrufen von E-Mails. POP3 lädt E-Mails eher einfach ab, während IMAP E-Mails auf dem Server verwaltet und zwischen mehreren Geräten synchronisiert. DNS ist für E-Mail wichtig, insbesondere durch MX-Records für zuständige Mailserver sowie TXT-Records für SPF, DKIM und DMARC. TLS kann Mailverbindungen schützen, ist aber nicht automatisch Ende-zu-Ende-Verschlüsselung des Mailinhalts.

Merksätze

E-Mail gehört zu Schicht 7.

SMTP sendet E-Mails.

POP3 ruft E-Mails ab.

IMAP ruft E-Mails ab und verwaltet sie.

SMTP = Simple Mail Transfer Protocol.

POP3 = Post Office Protocol Version 3.

IMAP = Internet Message Access Protocol.

SMTP Port 25 = Mailserver zu Mailserver.

Submission Port 587 = Client sendet authentifiziert.

SMTPS Port 465 = SMTP direkt über TLS.

POP3 Port 110 = Abruf unverschlüsselt.

POP3S Port 995 = POP3 über TLS.

IMAP Port 143 = Abruf und Verwaltung.

IMAPS Port 993 = IMAP über TLS.

MX = zuständiger Mailserver.

PTR = Reverse DNS.

SPF sagt,
wer senden darf.

DKIM signiert E-Mails.

DMARC legt Umgang mit Prüfungsfehlern fest.

POP3 lädt eher herunter.

IMAP synchronisiert besser.

STARTTLS schaltet auf TLS um.

TLS schützt Mailverbindung,
aber nicht automatisch Ende-zu-Ende den Inhalt.

S/MIME und OpenPGP schützen Inhalte Ende-zu-Ende.

NDR = Nichtzustellbarkeitsmeldung.

Mailprobleme mit DNS,
Ports,
TLS,
Authentifizierung,
Spamfilter
und Logs prüfen.