19.3 Standardports-Spickzettel

Dieser Spickzettel fasst wichtige Standardports kompakt zusammen.

Er ist besonders wichtig für:

```
- Firewall-Regeln
- Fehlersuche
- Protokollzuordnung
- Sicherheitsfragen
- Prüfungsaufgaben
- Netzwerkdokumentation
```

Merksatz:

```
Ports zeigen,
welcher Dienst auf einem Host angesprochen wird.
```

Grundidee: Was ist ein Port?

Ein Port ist eine logische Nummer, mit der ein Dienst oder Prozess auf einem System angesprochen wird.

Beispiel:

```
IP-Adresse:
Welcher Host?

Port:
Welcher Dienst auf diesem Host?
```

Beispiel:

```
192.168.1.10:443
```

Bedeutung:

```
Host 192.168.1.10

Dienst auf Port 443
```

Merksatz:

```
IP findet den Host.
Port findet den Dienst.
```

Port und OSI-Schicht

Ports gehören zur Transportschicht.

OSI-Schicht:

```
Schicht 4
```

Protokolle:

```
TCP

UDP
```

Merksatz:

```
Ports sind Schicht 4.
```

TCP und UDP bei Ports

Ein Port allein reicht nicht immer aus.

Wichtig ist auch, ob TCP oder UDP verwendet wird.

Beispiel:

```
TCP 53
```

```
und

UDP 53
```

sind nicht dasselbe, auch wenn die Portnummer gleich ist.

Merksatz:

```
Portnummer immer zusammen mit TCP oder UDP betrachten.
```

Well-Known Ports

Well-Known Ports sind bekannte Standardports.

Bereich:

```
0 bis 1023
```

Beispiele:

```
TCP 22 SSH

TCP 80 HTTP

TCP 443 HTTPS

UDP 53 DNS
```

Merksatz:

```
Well-Known Ports sind bekannte Dienstports.
```

Registered Ports

Registered Ports liegen im Bereich:

```
1024 bis 49151
```

Sie werden häufig von Anwendungen, Diensten oder Herstellern genutzt.

Beispiele:

```
TCP 3306 MySQL

TCP 5432 PostgreSQL

TCP 8080 alternativer HTTP-Port
```

Merksatz:

```
Registered Ports werden oft von Anwendungen genutzt.
```

Dynamic oder Ephemeral Ports

Dynamische Ports werden häufig für Clientverbindungen genutzt.

Bereich:

```
49152 bis 65535
```

Beispiel:

```
Client verbindet sich von zufälligem hohen Quellport
zu Server TCP 443.
```

Merksatz:

```
Server lauscht meist auf bekanntem Port.
Client nutzt oft dynamischen Quellport.
```

Quellport und Zielport

Bei einer Verbindung gibt es:

Quell-IP

Quellport

Ziel-IP

Zielport

Beispiel:

Client:
192.168.1.50:52344

Server:
93.184.216.34:443

Bedeutung:

Client nutzt dynamischen Quellport.
Server nutzt Zielport HTTPS.

Merksatz:

Zielport zeigt meist den angesprochenen Dienst.

Wichtige Standardports Gesamtübersicht

Dienst	Protokoll	Port	Zweck
FTP Control	TCP	21	klassische FTP-Steuerverbindung
FTP Data	TCP	20	klassische FTP-Datenverbindung im aktiven Modus
SSH	TCP	22	verschlüsselter Kommandozeilenzugriff
Telnet	TCP	23	unverschlüsselter Fernzugriff

Dienst	Protokoll	Port	Zweck
SMTP	TCP	25	E-Mail-Versand zwischen Mailservern
DNS	UDP/TCP	53	Namensauflösung
DHCP Server	UDP	67	DHCP-Server
DHCP Client	UDP	68	DHCP-Client
HTTP	TCP	80	unverschlüsselte Webkommunikation
POP3	TCP	110	E-Mail-Abruf
NTP	UDP	123	Zeitsynchronisation
IMAP	TCP	143	E-Mail-Abruf und Synchronisation
SNMP	UDP	161	Netzwerkmanagement
SNMP Trap	UDP	162	SNMP-Ereignismeldungen
LDAP	TCP/UDP	389	Verzeichnisdienst
HTTPS	TCP	443	verschlüsselte Webkommunikation
SMB	TCP	445	Datei- und Druckfreigaben
SMTPS	TCP	465	SMTP über TLS
Syslog	UDP	514	Logübertragung
LDAPS	TCP	636	LDAP über TLS
IMAPS	TCP	993	IMAP über TLS
POP3S	TCP	995	POP3 über TLS
RDP	TCP	3389	Remote Desktop
PostgreSQL	TCP	5432	Datenbankdienst
HTTP Alternate	TCP	8080	alternativer Webport

Merksatz:

> Port,
> Protokoll
> und Dienst zusammen lernen.

Webports

Dienst	Protokoll	Port	Bedeutung

HTTP	TCP	80	unverschlüsselte Webseite
HTTPS	TCP	443	verschlüsselte Webseite
HTTP Alternate	TCP	8080	alternativer Webdienst
HTTPS Alternate	TCP	8443	alternativer verschlüsselter Webdienst

Merksatz:

> HTTP ist unverschlüsselt.
> HTTPS ist verschlüsselt.

HTTP und HTTPS unterscheiden

HTTP:

> Hypertext Transfer Protocol
>
> nutzt meist TCP 80
>
> keine Transportverschlüsselung

HTTPS:

> HTTP über TLS
>
> nutzt meist TCP 443
>
> verschlüsselte Verbindung

Merksatz:

> HTTPS = HTTP plus TLS.

E-Mail-Ports

Dienst	Protokoll	Port	Zweck
SMTP	TCP	25	Mailserver zu Mailserver

Dienst	Protokoll	Port	Zweck
Submission	TCP	587	E-Mail-Versand durch Clients mit Authentifizierung
SMTPS	TCP	465	SMTP über TLS
POP3	TCP	110	E-Mail abrufen
POP3S	TCP	995	POP3 verschlüsselt
IMAP	TCP	143	E-Mail synchronisieren
IMAPS	TCP	993	IMAP verschlüsselt

Merksatz:

> SMTP sendet.
> POP3 und IMAP empfangen.

SMTP, POP3 und IMAP unterscheiden

SMTP:

> E-Mails senden

POP3:

> E-Mails abrufen,
> eher einfaches Herunterladen

IMAP:

> E-Mails auf Server synchron verwalten

Merksatz:

> SMTP raus.
> POP3 und IMAP rein.

DNS-Ports

Dienst	Protokoll	Port	Zweck
DNS	UDP	53	normale DNS-Abfragen
DNS	TCP	53	große Antworten, Zonentransfers, bestimmte Spezialfälle

Merksatz:

```
DNS nutzt häufig UDP 53,
kann aber auch TCP 53 nutzen.
```

DHCP-Ports

Dienst	Protokoll	Port	Bedeutung
DHCP Server	UDP	67	Server empfängt Anfragen
DHCP Client	UDP	68	Client empfängt Antworten

Merksatz:

```
DHCP nutzt UDP 67 und 68.
```

DHCP und Broadcast

DHCP nutzt am Anfang Broadcast, weil der Client noch keine vollständige IP-Konfiguration hat.

Ablauf:

```
Discover

Offer

Request

Acknowledge
```

Merksatz:

```
DHCP-DORA gehört zu UDP 67 und 68.
```

Fernadministration-Ports

Dienst	Protokoll	Port	Sicherheit
SSH	TCP	22	verschlüsselt
Telnet	TCP	23	unverschlüsselt, unsicher
RDP	TCP	3389	verschlüsselt möglich, stark absichern

Merksatz:

SSH statt Telnet.
RDP nicht offen ins Internet stellen.

SSH

SSH steht für:

Secure Shell

Standardport:

TCP 22

Nutzung:

sichere Kommandozeile
SFTP
SCP
Administration von Servern und Netzwerkgeräten

Merksatz:

SSH = sicherer Fernzugriff über TCP 22.

Telnet

Telnet nutzt:

TCP 23

Problem:

unverschlüsselte Übertragung

Risiko:

Zugangsdaten können mitgelesen werden.

Merksatz:

Telnet ist unsicher und sollte vermieden werden.

RDP

RDP steht für:

Remote Desktop Protocol

Standardport:

TCP 3389

Nutzung:

grafischer Fernzugriff auf Windows-Systeme

Sicherheit:

möglichst über VPN,
RDP-Gateway,
MFA
und Firewall-Beschränkung

Merksatz:

RDP = TCP 3389,

aber nicht offen ins Internet.

Dateiübertragungs- und Freigabeports

Dienst	Protokoll	Port	Zweck
FTP Data	TCP	20	FTP-Datenkanal aktiv
FTP Control	TCP	21	FTP-Steuerkanal
SFTP	TCP	22	Dateiübertragung über SSH
FTPS	TCP	21 oder 990	FTP mit TLS
SMB	TCP	445	Datei- und Druckfreigaben
NFS	TCP/UDP	2049	Unix-/Linux-Dateifreigaben

Merksatz:

SFTP nutzt SSH.

SMB nutzt TCP 445.

FTP, FTPS und SFTP

FTP:

klassisches File Transfer Protocol

meist TCP 21

unverschlüsselt

FTPS:

FTP mit TLS-Verschlüsselung

nutzt FTP-Grundlage

SFTP:

Dateiübertragung über SSH

nutzt TCP 22

Merksatz:

FTPS ist FTP mit TLS.
SFTP ist Dateiübertragung über SSH.

SMB

SMB steht für:

Server Message Block

Standardport:

TCP 445

Nutzung:

Windows-Dateifreigaben
Druckerfreigaben
Netzlaufwerke

Merksatz:

SMB = Dateifreigaben über TCP 445.

NFS

NFS steht für:

Network File System

Standardport:

TCP/UDP 2049

Nutzung:

Unix- und Linux-Dateifreigaben
Serverfreigaben
Virtualisierungsspeicher
Backupziele

Merksatz:

NFS ist typisch für Unix- und Linux-Umgebungen.

Verzeichnisdienst-Ports

Dienst	Protokoll	Port	Zweck
LDAP	TCP/UDP	389	Verzeichnisdienst
LDAPS	TCP	636	LDAP über TLS
Kerberos	TCP/UDP	88	Authentifizierungsprotokoll

Merksatz:

LDAP fragt Verzeichnisinformationen ab.
Kerberos dient der Authentifizierung.

LDAP und LDAPS

LDAP:

Lightweight Directory Access Protocol

nutzt meist TCP/UDP 389

LDAPS:

LDAP über TLS

nutzt meist TCP 636

Merksatz:

LDAPS = LDAP verschlüsselt.

Kerberos

Kerberos ist ein Authentifizierungsprotokoll.

Standardport:

TCP/UDP 88

Wichtig:

Zeitabweichungen können Kerberos-Probleme verursachen.

Merksatz:

Kerberos braucht korrekte Zeit.

Zeit und Management

Dienst	Protokoll	Port	Zweck
NTP	UDP	123	Zeitsynchronisation
SNMP	UDP	161	Netzwerkmanagement
SNMP Trap	UDP	162	Ereignismeldung vom Gerät
Syslog	UDP	514	Logübertragung

Merksatz:

NTP sorgt für gleiche Zeit.
SNMP überwacht Geräte.

Syslog sammelt Logs.

NTP

NTP steht für:

Network Time Protocol

Standardport:

UDP 123

Wichtig für:

Logs
Zertifikate
Kerberos
Tickets
Zeitstempel
geplante Aufgaben

Merksatz:

Ohne korrekte Zeit wird Fehlersuche schwerer.

SNMP

SNMP steht für:

Simple Network Management Protocol

Standardports:

UDP 161 für Abfragen

UDP 162 für Traps

Nutzung:

```
Netzwerkgeräte überwachen
Status abfragen
Messwerte erfassen
Ereignisse melden
```

Merksatz:

```
SNMP fragt ab,
SNMP Trap meldet Ereignisse.
```

Syslog

Syslog dient zur Übertragung von Logmeldungen.

Standardport:

```
UDP 514
```

Nutzung:

```
zentrale Logsammlung
Firewall-Logs
Switch-Logs
Router-Logs
Server-Logs
```

Merksatz:

```
Syslog transportiert Logmeldungen.
```

Datenbankports

Dienst	Protokoll	Port	Zweck
MySQL / MariaDB	TCP	3306	Datenbankdienst
PostgreSQL	TCP	5432	Datenbankdienst

Dienst	Protokoll	Port	Zweck
Microsoft SQL Server	TCP	1433	Datenbankdienst
MongoDB	TCP	27017	Datenbankdienst

Merksatz:

> Datenbankports sollten nicht unnötig öffentlich erreichbar sein.

Sicherheitsregel für Datenbankports

Datenbanken sollten normalerweise nur erreichbar sein für:

> Anwendungserver
>
> Adminnetz
>
> Backupsysteme
>
> Monitoring

Nicht sinnvoll:

> Datenbank direkt öffentlich ins Internet stellen.

Merksatz:

> Datenbankports gehören nicht offen ins Internet.

Typische Proxy- und Alternativports

Dienst	Protokoll	Port	Zweck
HTTP Alternate	TCP	8080	alternativer Webdienst
HTTPS Alternate	TCP	8443	alternativer HTTPS-Dienst
Proxy	TCP	3128	häufig genutzter Proxy-Port
SOCKS Proxy	TCP	1080	SOCKS-Proxy

Merksatz:

8080 und 8443 werden oft für Weboberflächen oder Testdienste genutzt.

Portbereiche kompakt

Bereich	Name	Bedeutung
0 bis 1023	Well-Known Ports	bekannte Systemdienste
1024 bis 49151	Registered Ports	registrierte Anwendungsports
49152 bis 65535	Dynamic / Ephemeral Ports	dynamische Clientports

Merksatz:

Niedrige Ports sind oft Serverdienste.
Hohe Ports sind oft Client-Quellports.

Ports in Firewall-Regeln

Firewall-Regeln sollten enthalten:

Quelle

Ziel

Protokoll

Zielport

Aktion

Richtung

Zweck

Beispiel:

Quelle	Ziel	Protokoll	Port	Aktion	Zweck
Client-Netz	Webserver	TCP	443	erlauben	HTTPS-Zugriff

Quelle	Ziel	Protokoll	Port	Aktion	Zweck
Adminnetz	Server	TCP	22	erlauben	SSH-Administration
Internet	Datenbank	TCP	5432	blockieren	Datenbank schützen

Merksatz:

> Firewall-Regeln immer so genau wie möglich formulieren.

Any-to-Any-Regeln

Any-to-Any bedeutet:

> jede Quelle
>
> zu
>
> jedem Ziel

Problem:

> sehr große Angriffsfläche
> schlechte Nachvollziehbarkeit
> unnötige Freigaben
> hohes Sicherheitsrisiko

Merksatz:

> Any-to-Any ist fast immer kritisch.

Ports bei Fehlersuche

Wenn ein Dienst nicht erreichbar ist, prüfen:

> Läuft der Dienst?

Lauscht der Dienst auf dem richtigen Port?

Lauscht der Dienst auf der richtigen Schnittstelle?

Blockiert die lokale Firewall?

Blockiert eine Netzwerkfirewall?

Ist NAT oder Portweiterleitung korrekt?

Stimmt TCP oder UDP?

Zeigen Logs Fehler?

Merksatz:

> Host erreichbar heißt nicht,
> dass der Port erreichbar ist.

Typische Fehlerbilder mit Ports

Fehlerbild	Mögliche Ursache
Ping funktioniert, Webseite nicht	TCP 80 oder 443, Webdienst oder Firewall
SSH nicht erreichbar	TCP 22 blockiert, Dienst aus, falscher Port
RDP nicht erreichbar	TCP 3389 blockiert, RDP deaktiviert, VPN fehlt
DNS funktioniert nicht	UDP/TCP 53 blockiert oder DNS-Server falsch
DHCP funktioniert nicht	UDP 67/68, VLAN oder DHCP-Relay
SMB-Freigabe nicht erreichbar	TCP 445 blockiert oder Rechteproblem
Mailversand schlägt fehl	SMTP-Port, Authentifizierung oder Mailserver
Datenbank nicht erreichbar	Datenbankport, Firewall oder Dienststatus

Merksatz:

> Bei Dienstproblemen immer Port,
> Protokoll
> und Dienststatus prüfen.

TCP-Status kurz einordnen

Status	Bedeutung
LISTEN	Dienst wartet auf eingehende Verbindung
ESTABLISHED	Verbindung besteht
SYN_SENT	Verbindungsaufbau gestartet
TIME_WAIT	Verbindung wurde beendet, Wartephase
CLOSE_WAIT	Gegenseite hat beendet, lokale Anwendung noch nicht

Merksatz:

```
LISTEN zeigt:
Ein Dienst wartet auf Verbindungen.
```

Portscanner fachlich einordnen

Ein Portscanner prüft, welche Ports auf einem Ziel erreichbar sind.

Nutzung:

```
Sicherheitsprüfung
Fehlersuche
Inventarisierung
Prüfung von Firewall-Regeln
```

Wichtig:

```
Nur mit Erlaubnis einsetzen.
```

Merksatz:

```
Portscan zeigt erreichbare Dienste,
aber nicht automatisch deren Sicherheit.
```

Ports und Sicherheit

Offene Ports bedeuten:

ein Dienst ist erreichbar

Risiko:

Angriffsfläche steigt

Sicherheitsmaßnahmen:

nur notwendige Ports öffnen
Dienste patchen
starke Authentifizierung
Firewall einschränken
Logging aktivieren
nicht benötigte Dienste deaktivieren
keine Adminports öffentlich bereitstellen

Merksatz:

Jeder offene Port ist eine mögliche Angriffsfläche.

Besonders kritische Ports

Kritisch bei direkter Internet-Erreichbarkeit:

TCP 22 SSH

TCP 3389 RDP

TCP 445 SMB

TCP 3306 MySQL

TCP 5432 PostgreSQL

TCP 1433 Microsoft SQL Server

TCP 23 Telnet

Warum kritisch?

```
Adminzugänge
Dateifreigaben
Datenbanken
unverschlüsselte Protokolle
häufige Angriffsziele
```

Merksatz:

```
Admin-,
Datei-
und Datenbankports nicht frei ins Internet stellen.
```

Prüfungsfalle: Port offen bedeutet nicht Zugriff erlaubt

Ein offener Port bedeutet:

```
Dienst ist grundsätzlich erreichbar.
```

Aber Zugriff kann trotzdem scheitern durch:

```
falsche Zugangsdaten
fehlende Rechte
Anwendungskonfiguration
Zertifikatsproblem
IP-Beschränkung
MFA
Lizenz
interne Fehlermeldung
```

Merksatz:

```
Port offen heißt nicht automatisch:
Anwendung funktioniert vollständig.
```

Prüfungsfalle: Ping ersetzt keinen Porttest

Ping prüft ICMP.

Ping prüft nicht automatisch, ob ein TCP- oder UDP-Dienst erreichbar ist.

Beispiel:

```
ping auf Webserver funktioniert

aber

TCP 443 ist blockiert
```

Ergebnis:

```
Webseite trotzdem nicht erreichbar.
```

Merksatz:

```
Ping prüft Host-Erreichbarkeit,
nicht den Dienst.
```

Prüfungsfalle: gleicher Port, anderes Protokoll

Beispiel:

```
DNS nutzt UDP 53

und

DNS kann TCP 53 nutzen.
```

Eine Firewall-Regel nur für TCP 53 reicht nicht immer aus.

Merksatz:

```
TCP und UDP getrennt beachten.
```

Typische IHK-Fragen

In AP1 und AP2 kann zum Beispiel gefragt werden:

- Welchen Port nutzt SSH?
- Welchen Port nutzt HTTPS?
- Welchen Port nutzt RDP?
- Welchen Port nutzt SMB?
- Welche Ports nutzt DHCP?
- Warum nutzt DNS UDP und TCP 53?
- Warum ist Telnet unsicher?
- Warum sollte RDP nicht direkt im Internet erreichbar sein?
- Was ist der Unterschied zwischen Quellport und Zielport?
- Was ist ein Well-Known Port?
- Warum ist ein offener Datenbankport kritisch?
- Warum ersetzt ping keinen Porttest?
- Welche Angaben gehören in eine Firewall-Regel?

Typische Prüfungsfallen

TCP und UDP nicht angegeben.

Portnummer richtig,
aber falsches Protokoll.

DNS nur als UDP betrachten,
TCP 53 vergessen.

DHCP-Ports 67 und 68 verwechseln.

SSH und Telnet verwechseln.

SFTP und FTPS verwechseln.

SMTP,
POP3
und IMAP verwechseln.

RDP öffentlich erlauben.

SMB öffentlich erlauben.

Datenbankport öffentlich erlauben.

Ping als Diensttest verstehen.

Offenen Port mit erfolgreicher Anmeldung verwechseln.

Merksatz:

Portwissen muss immer mit Dienst,
Protokoll
und Sicherheitswirkung verbunden werden.

IHK-sichere Kurzformulierung

Ports dienen auf der Transportschicht zur Zuordnung von Netzwerkverkehr zu Diensten oder Prozessen. Ein Zielport zeigt meist den angesprochenen Dienst, zum Beispiel TCP 22 für SSH, TCP 443 für HTTPS, TCP 445 für SMB oder TCP 3389 für RDP. Dabei muss immer zwischen TCP und UDP unterschieden werden. DNS nutzt häufig UDP 53, kann aber auch TCP 53 verwenden. DHCP nutzt UDP 67 für den Server und UDP 68 für den Client. Offene Ports vergrößern die Angriffsfläche und sollten über Firewall-Regeln nur gezielt freigegeben werden. Besonders Admin-, Datei- und Datenbankports sollten nicht unnötig öffentlich erreichbar sein.

Merksätze

Port = Dienstadresse auf einem Host.

Ports gehören zu OSI-Schicht 4.

Port immer mit TCP oder UDP nennen.

Zielport zeigt meist den Dienst.

Quellport ist beim Client oft dynamisch.

Well-Known Ports liegen bei 0 bis 1023.

SSH nutzt TCP 22.

Telnet nutzt TCP 23 und ist unsicher.

HTTP nutzt TCP 80.

HTTPS nutzt TCP 443.

DNS nutzt UDP und TCP 53.

DHCP nutzt UDP 67 und 68.

SMTP nutzt TCP 25.

Submission nutzt TCP 587.

POP3 nutzt TCP 110.

IMAP nutzt TCP 143.

SMB nutzt TCP 445.

RDP nutzt TCP 3389.

NTP nutzt UDP 123.

SNMP nutzt UDP 161 und 162.

LDAP nutzt 389.

LDAPS nutzt 636.

Kerberos nutzt 88.

MySQL nutzt TCP 3306.

PostgreSQL nutzt TCP 5432.

SFTP nutzt SSH und damit TCP 22.

FTPS ist FTP mit TLS.

FTP ist unverschlüsselt.

Jeder offene Port ist Angriffsfläche.

Ping ersetzt keinen Porttest.

Port offen heißt nicht automatisch Anwendung funktioniert.

Datenbankports nicht öffentlich freigeben.

Adminports stark absichern.

Firewall-Regeln genau formulieren.

Any-to-Any ist kritisch.