

10.6 Datei- und Freigabeprotokolle: FTP, SFTP, FTPS und SMB

Datei- und Freigabeprotokolle gehören zur OSI-Schicht 7.

Sie werden genutzt, um Dateien über ein Netzwerk bereitzustellen, zu übertragen oder gemeinsam zu verwenden.

Wichtige Protokolle sind:

- FTP
- SFTP
- FTPS
- SMB

Diese Protokolle haben unterschiedliche Aufgaben und Sicherheitsmerkmale.

Merksatz:

Dateiübertragung und Dateifreigaben gehören zur Anwendungsschicht.

Grundidee von Dateiübertragung

Bei der Dateiübertragung werden Dateien von einem System zu einem anderen übertragen.

Beispiele:

- Datei auf Server hochladen
- Datei von Server herunterladen
- Backup übertragen
- Konfigurationsdatei kopieren
- Webseite auf Webserver hochladen
- Dokumente zwischen Systemen austauschen

Dabei muss geregelt werden:

- wer zugreifen darf
- welche Dateien übertragen werden

- ob verschlüsselt wird
- welcher Port genutzt wird
- ob nur Dateiübertragung oder echte Freigabe gewünscht ist

Merksatz:

Dateiübertragung bedeutet:
Dateien gezielt zwischen Systemen bewegen.

Grundidee von Dateifreigaben

Eine Dateifreigabe stellt Dateien im Netzwerk bereit.

Dabei sieht ein Benutzer oder Client einen Ordner auf einem entfernten System.

Beispiele:

- Netzlaufwerk im Unternehmen
- gemeinsamer Projektordner
- Druckerfreigabe
- zentrale Dateiablage
- Home-Laufwerk eines Benutzers
- NAS-Freigabe

Typisch hierfür ist:

SMB

Merksatz:

Dateifreigabe bedeutet:
Dateien werden im Netzwerk gemeinsam bereitgestellt.

Dateiübertragung und Dateifreigabe unterscheiden

Thema	Dateiübertragung	Dateifreigabe
Grundidee	Datei von A nach B kopieren	Ordner im Netzwerk gemeinsam nutzen

Thema	Dateiübertragung	Dateifreigabe
typische Protokolle	FTP, SFTP, FTPS	SMB
Nutzung	Upload, Download, Transfer	Netzlaufwerk, Freigabe, gemeinsames Arbeiten
Zugriff	meist gezielte Übertragung	fortlaufender Zugriff auf entfernte Dateien
Beispiel	Datei auf Server hochladen	Laufwerk <code>\\server\share</code> öffnen

Merksatz:

FTP/SFTP/FTPS übertragen Dateien.
SMB stellt Freigaben bereit.

Einordnung im OSI-Modell

Thema	Schicht
FTP	7
SFTP	7, nutzt SSH
FTPS	7, nutzt TLS
SMB	7
TCP-Port	4
IP-Adresse	3
MAC-Adresse	2
TLS	6 mit Schicht-7-Bezug
SSH	7 mit Sicherheitsbezug

Merksatz:

Protokoll = Schicht 7.
Port = Schicht 4.

FTP

FTP steht für:

File Transfer Protocol

FTP dient zur Dateiübertragung.

Typischer Port:

TCP 21

FTP wird klassisch verwendet für:

- Dateien hochladen
- Dateien herunterladen
- Verzeichnisse auflisten
- Dateien löschen oder umbenennen
- einfache Server-Dateiverwaltung

Wichtig:

Klassisches FTP ist unverschlüsselt.

Merksatz:

FTP = Dateiübertragung über TCP 21,
aber klassisch unverschlüsselt.

FTP ist unverschlüsselt

Klassisches FTP überträgt Daten unverschlüsselt.

Das betrifft besonders:

- Benutzername
- Passwort
- Befehle
- Dateiinhalte

Wenn jemand den Netzwerkverkehr mitlesen kann, können sensible Informationen sichtbar werden.

Deshalb sollte klassisches FTP heute möglichst vermieden werden.

Merksatz:

FTP ohne Schutz ist unsicher.

FTP-Steuerverbindung und Datenverbindung

FTP arbeitet mit zwei Verbindungsarten:

Steuerverbindung

Datenverbindung

Steuerverbindung:

Befehle und Anmeldung

Datenverbindung:

Dateiinhalt und Verzeichnislisten

Typisch:

TCP 21 für Steuerverbindung

Die Datenverbindung hängt vom Modus ab.

Merksatz:

FTP nutzt Steuerverbindung und Datenverbindung.

Aktiver FTP-Modus

Beim aktiven FTP-Modus baut der Server eine Datenverbindung zurück zum Client auf.

Problem:

Firewalls und NAT können das erschweren,
weil der Server von außen zum Client verbinden möchte.

Typische Schwierigkeit:

Client sitzt hinter NAT oder Firewall.

Merksatz:

Aktives FTP kann mit NAT und Firewalls Probleme machen.

Passiver FTP-Modus

Beim passiven FTP-Modus baut der Client beide Verbindungen zum Server auf.

Das ist heute häufig praktischer, weil Clients oft hinter NAT oder Firewalls sitzen.

Der Server teilt dem Client einen Datenport mit, zu dem der Client sich verbindet.

Wichtig:

Die passiven Portbereiche müssen auf Firewall und Server korrekt erlaubt sein.

Merksatz:

Passives FTP ist NAT-freundlicher,
braucht aber passende Firewall-Regeln.

FTP und Firewall-Probleme

FTP kann bei Firewalls schwieriger sein als einfache Protokolle.

Warum?

FTP nutzt nicht nur eine einzelne Verbindung.

Typische Fehler:

- Login funktioniert,
aber Verzeichnisliste lädt nicht

- Verbindung funktioniert,
aber Dateiübertragung schlägt fehl
- passiver Portbereich nicht freigegeben
- NAT übersetzt falsche Adresse

Merksatz:

Bei FTP müssen Steuer- und Datenverbindung funktionieren.

SFTP

SFTP steht für:

SSH File Transfer Protocol

SFTP ist Dateiübertragung über SSH.

Typischer Port:

TCP 22

SFTP ist nicht dasselbe wie FTP.

SFTP nutzt SSH als sichere Grundlage.

Dadurch werden Anmeldung und Daten verschlüsselt übertragen.

Merksatz:

SFTP = Dateiübertragung über SSH.

SFTP und SSH

SFTP läuft über SSH.

SSH bietet:

- Verschlüsselung
- Authentifizierung
- sichere Verbindung
- Zugriff über Benutzerkonto oder Schlüssel

SFTP nutzt diese sichere Verbindung, um Dateien zu übertragen.

Typische Nutzung:

- Serveradministration
- Datei-Upload auf Server
- sichere Dateiübertragung
- Automatisierung mit Schlüsseln

Merksatz:

Wer SFTP nutzt,
nutzt technisch SSH als Grundlage.

SFTP ist nicht FTP über TLS

Ein häufiger Fehler ist:

SFTP = sicheres FTP

Besser:

SFTP ist ein eigenes Protokoll über SSH.

Es ist nicht:

klassisches FTP mit Verschlüsselung

Das wäre eher:

FTPS

Merksatz:

SFTP ist nicht FTPS.

FTPS

FTPS bedeutet:

FTP mit TLS-Schutz

FTPS basiert auf FTP, nutzt aber TLS zur Verschlüsselung.

Es gibt zwei typische Varianten:

explizites FTPS

implizites FTPS

Merksatz:

FTPS = FTP mit TLS.

Explizites FTPS

Explizites FTPS startet zunächst auf dem klassischen FTP-Port.

Typischer Port:

TCP 21

Dann wird mit einem Befehl auf TLS umgestellt.

Das ist ähnlich zur Idee von STARTTLS.

Merksatz:

Explizites FTPS startet auf TCP 21
und schaltet auf TLS um.

Implizites FTPS

Implizites FTPS startet direkt mit TLS.

Typischer Port:

TCP 990

Dabei wird von Beginn an verschlüsselt kommuniziert.

Merksatz:

Implizites FTPS nutzt typischerweise TCP 990.

SFTP und FTPS vergleichen

Merkmal	SFTP	FTPS
Grundlage	SSH	FTP + TLS
typischer Port	TCP 22	TCP 21 oder TCP 990
Protokollfamilie	SSH-basiert	FTP-basiert
Verschlüsselung	durch SSH	durch TLS
Firewall-Aufwand	meist einfacher	oft aufwendiger wegen FTP-Datenkanälen
nicht verwechseln mit	FTPS	SFTP

Merksatz:

SFTP = SSH.

FTPS = FTP mit TLS.

FTP, SFTP und FTPS vergleichen

Protokoll	Verschlüsselung	typischer Port	Kurzidee
FTP	nein	TCP 21	klassische Dateiübertragung
SFTP	ja, SSH	TCP 22	Dateiübertragung über SSH
FTPS explizit	ja, TLS	TCP 21	FTP startet und schaltet auf TLS

Protokoll	Verschlüsselung	typischer Port	Kurzidee
FTPS implizit	ja, TLS	TCP 990	FTP direkt über TLS

Merksatz:

FTP unverschlüsselt.
SFTP über SSH.
FTPS über TLS.

SMB

SMB steht für:

Server Message Block

SMB wird für Datei- und Druckerfreigaben verwendet.

Typischer Port:

TCP 445

Typische Nutzung:

- Windows-Dateifreigaben
- Netzlaufwerke
- Druckerfreigaben
- zentrale Dateiablagen
- Zugriff auf NAS-Freigaben
- Freigaben in Unternehmensnetzen

Merksatz:

SMB = Datei- und Druckerfreigaben im Netzwerk.

SMB-Freigabe

Eine SMB-Freigabe ist ein freigegebener Ordner im Netzwerk.

Beispiel Windows-Schreibweise:

```
\\server01\daten
```

Dabei ist:

server01 = Servername

daten = Freigabename

Benutzer können diese Freigabe als Netzlaufwerk verbinden.

Merksatz:

SMB-Freigabe = Netzwerkordner.

UNC-Pfad

UNC steht für:

Universal Naming Convention

Ein UNC-Pfad beschreibt eine Netzwerkfreigabe.

Beispiel:

```
\\server01\freigabe\ordner\datei.txt
```

Bestandteile:

Servername

Freigabename

Pfad innerhalb der Freigabe

Merksatz:

UNC-Pfad zeigt auf eine Netzwerkfreigabe.

Netzlaufwerk

Ein Netzlaufwerk ist eine eingebundene Netzwerkfreigabe.

Beispiel:

Laufwerk Z:
zeigt auf
\\server01\projekte

Vorteil:

Benutzer kann die Freigabe wie ein Laufwerk verwenden.

Merksatz:

Netzlaufwerk = eingebundene SMB-Freigabe.

SMB und Berechtigungen

Bei SMB gibt es meist zwei Berechtigungsebenen:

Freigabeberechtigungen
Dateisystemberechtigungen

In Windows-Umgebungen sind Dateisystemberechtigungen oft NTFS-Berechtigungen.

Wichtig:

Es gilt am Ende die wirksam einschränkende Berechtigung.

Merksatz:

SMB-Zugriff hängt von Freigabe- und Dateisystemrechten ab.

Freigabeberechtigungen

Freigabeberechtigungen gelten auf Ebene der Netzwerkfreigabe.

Beispiele:

Lesen
Ändern
Vollzugriff

Sie steuern, was Benutzer über die Freigabe grundsätzlich dürfen.

Merksatz:

Freigaberechte gelten am Netzwerkzugriffspunkt.

Dateisystemberechtigungen

Dateisystemberechtigungen gelten auf dem Dateisystem selbst.

Beispiele:

Lesen
Schreiben
Ändern
Löschen
Ausführen
Vollzugriff

Sie gelten oft auch lokal auf dem Server, nicht nur über das Netzwerk.

Merksatz:

Dateisystemrechte schützen Dateien und Ordner direkt.

Effektive Berechtigung

Wenn Freigaberechte und Dateisystemrechte zusammenkommen, zählt die effektiv erlaubte Berechtigung.

Beispiel:

Freigabe:

Vollzugriff

Dateisystem:

Lesen

Ergebnis:

Benutzer kann nur lesen.

Merksatz:

Die strengere Berechtigung begrenzt den Zugriff.

Gruppen statt Einzelbenutzer

In Unternehmensnetzen vergibt man Rechte möglichst über Gruppen.

Beispiel:

Gruppe:

Projekt_A_Lesen

Gruppe:

Projekt_A_Aendern

Benutzer werden in Gruppen aufgenommen, statt direkt auf einzelne Ordner berechtigt zu werden.

Vorteile:

- bessere Übersicht
- einfachere Verwaltung
- weniger Fehler
- leichteres Entfernen von Rechten

Merksatz:

Berechtigungen über Gruppen vergeben.

Least Privilege

Least Privilege bedeutet:

Benutzer erhalten nur die Rechte,
die sie wirklich benötigen.

Beispiel:

Praktikant braucht Leserechte,
aber keine Löschrechte.

Dieses Prinzip reduziert Sicherheitsrisiken.

Merksatz:

Nur so viele Rechte wie nötig,
so wenige wie möglich.

SMB und Active Directory

In Windows-Umgebungen wird SMB häufig mit Active Directory kombiniert.

Active Directory liefert:

Benutzerkonten
Gruppen
Authentifizierung
Richtlinien

SMB nutzt diese Informationen, um Freigabezugriffe zu erlauben oder abzulehnen.

Merksatz:

SMB-Freigaben nutzen oft AD-Benutzer und Gruppen.

SMB und DNS

SMB-Zugriff nutzt häufig Servernamen.

Beispiel:

```
\\fileserver01\projekte
```

Dafür muss Namensauflösung funktionieren.

Mögliche Namensauflösung:

- DNS
- lokale Namensauflösung
- ältere NetBIOS-Mechanismen

In modernen Netzwerken ist DNS besonders wichtig.

Merksatz:

SMB-Probleme können DNS-Probleme sein.

SMB-Versionen

Es gibt verschiedene SMB-Versionen.

Wichtig:

SMBv1 ist veraltet und unsicher.

Moderne Systeme sollten SMBv2 oder SMBv3 verwenden.

SMBv3 unterstützt unter anderem bessere Sicherheitsfunktionen und kann Verschlüsselung unterstützen.

Merksatz:

SMBv1 vermeiden.
SMBv2 oder SMBv3 verwenden.

SMB und Sicherheit

SMB sollte sorgfältig abgesichert werden.

Wichtige Punkte:

- SMBv1 deaktivieren
- Zugriff nur intern oder über VPN
- keine SMB-Freigaben direkt ins Internet öffnen
- Berechtigungen sauber setzen
- Gruppen verwenden
- Protokollierung aktivieren
- Updates einspielen
- Gastzugriff vermeiden
- starke Authentifizierung nutzen

Merksatz:

SMB gehört nicht ungeschützt ins Internet.

SMB und Druckerfreigaben

SMB kann auch für Druckerfreigaben verwendet werden.

Beispiel:

\\printserver01\drucker01

Clients verbinden sich mit der Freigabe und senden Druckaufträge an den Druckserver.

Merksatz:

SMB kann Dateien und Drucker freigeben.

FTP oder SMB?

Anwendungsfall	eher passend
einzelne Datei auf Server hochladen	SFTP oder FTPS
Webseite per Dateiübertragung aktualisieren	SFTP

Anwendungsfall	eher passend
gemeinsames Netzlaufwerk im Unternehmen	SMB
NAS-Freigabe im LAN	SMB
automatisierter sicherer Dateitransfer	SFTP
klassische unverschlüsselte Übertragung	FTP vermeiden

Merksatz:

SMB für Freigaben.
SFTP/FTPS für Dateiübertragung.

Sicherheit: FTP vermeiden

Klassisches FTP sollte möglichst vermieden werden, weil es unverschlüsselt ist.

Bessere Alternativen:

- SFTP
- FTPS
- HTTPS-Upload
- VPN plus interne Freigabe
- sichere Cloud- oder Filesharing-Lösung

Merksatz:

FTP ohne Verschlüsselung ist nicht mehr zeitgemäß.

Sicherheit: SFTP bevorzugen

SFTP ist oft eine gute Wahl für sichere Dateiübertragung.

Vorteile:

- nur ein typischer Port
- SSH-Verschlüsselung
- Schlüsselbasierte Anmeldung möglich
- gut automatisierbar

- häufig auf Servern verfügbar

Merksatz:

SFTP ist für sichere Dateiübertragung oft einfacher als FTPS.

Dateiübertragung und Datenschutz

Bei Dateiübertragung können sensible Daten betroffen sein.

Beispiele:

- Kundendaten
- Rechnungen
- Bewerbungen
- personenbezogene Daten
- Zugangsdaten
- interne Dokumente
- Backups

Deshalb wichtig:

- verschlüsselte Übertragung
- Zugriffsschutz
- Protokollierung
- Berechtigungskonzept
- Aufbewahrungsregeln
- sichere Löschung bei Bedarf

Merksatz:

Dateiübertragung muss Datenschutz und Zugriffsschutz beachten.

Fehlerbild: FTP-Login geht, Dateiübertragung nicht

Mögliche Ursachen:

- passiver Portbereich nicht freigegeben
- aktiver Modus scheitert an NAT
- Firewall blockiert Datenverbindung
- Server gibt falsche externe IP aus
- TLS-Modus passt nicht
- Berechtigungen fehlen

Merksatz:

Bei FTP kann Login funktionieren,
obwohl Datenübertragung scheitert.

Fehlerbild: SFTP-Verbindung scheitert

Mögliche Ursachen:

- SSH-Dienst läuft nicht
- TCP 22 blockiert
- falscher Benutzer
- falscher Schlüssel
- Passwortlogin deaktiviert
- Benutzer hat keine SFTP-Berechtigung
- falscher Hostname
- Firewall blockiert
- Host-Key-Warnung

Merksatz:

SFTP-Probleme wie SSH-Probleme prüfen.

Fehlerbild: FTPS-Zertifikatsfehler

Mögliche Ursachen:

- Zertifikat abgelaufen
- Name passt nicht zum Zertifikat
- CA nicht vertrauenswürdig

- Zwischenzertifikat fehlt
- Client unterstützt TLS-Version nicht
- falscher FTPS-Modus

Merksatz:

FTPS-Zertifikatsfehler wie TLS-Probleme prüfen.

Fehlerbild: SMB-Freigabe nicht erreichbar

Mögliche Ursachen:

- Servername wird nicht aufgelöst
- TCP 445 blockiert
- Serverdienst läuft nicht
- Firewall blockiert SMB
- falscher Freigabename
- Benutzer hat keine Rechte
- falsche Domänenanmeldung
- SMB-Version nicht kompatibel
- Netzwerkprofil blockiert Freigaben

Merksatz:

SMB-Probleme mit DNS,
TCP 445,
Dienst
und Berechtigungen prüfen.

Fehlerbild: Zugriff verweigert bei SMB

Mögliche Ursachen:

- Benutzer nicht berechtigt
- Gruppe fehlt
- Freigabeberechtigung zu streng
- NTFS-Berechtigung zu streng

- Vererbung falsch
- falsches Konto verwendet
- gespeicherte alte Anmeldedaten
- Datei durch anderen Prozess gesperrt

Merksatz:

Zugriff verweigert heißt oft:
Berechtigungen oder Anmeldung prüfen.

Fehlerbild: Netzlaufwerk verbindet nicht

Mögliche Ursachen:

- Server nicht erreichbar
- DNS-Name falsch
- Freigabe existiert nicht
- Benutzer nicht berechtigt
- falsche gespeicherte Zugangsdaten
- VPN nicht verbunden
- SMB-Port blockiert
- Offline-Dateien oder Cache-Problem
- Gruppenrichtlinie greift nicht

Merksatz:

Netzlaufwerkprobleme mit Pfad,
DNS,
Port,
Anmeldung
und Rechten prüfen.

Fehlerbild: Datei lässt sich nicht speichern

Mögliche Ursachen:

- keine Schreibrechte
- Speicherplatz voll
- Quota erreicht
- Datei gesperrt
- Pfad zu lang
- Dateiname ungültig
- Netzwerkunterbrechung
- Synchronisationsproblem
- Antivirus blockiert

Merksatz:

Speichern auf Freigaben braucht Rechte,
Platz
und stabile Verbindung.

Fehlerbild: Datei ist gesperrt

Eine Datei kann durch einen Benutzer oder Prozess gesperrt sein.

Mögliche Ursachen:

- Datei ist geöffnet
- Anwendung hält Sperre
- vorherige Sitzung nicht sauber beendet
- Synchronisationsdienst greift zu
- Backup oder Antivirus scannt Datei

Merksatz:

Dateisperren verhindern gleichzeitige unsichere Änderungen.

Fehlersuche bei Datei- und Freigabeproblemen

Eine sinnvolle Reihenfolge:

1. Name oder IP erreichbar?
2. Richtiger Port erreichbar?
3. Richtiger Dienst läuft?
4. Richtiges Protokoll verwendet?
5. Authentifizierung korrekt?
6. Berechtigungen korrekt?
7. Verschlüsselung oder Zertifikat korrekt?
8. Firewall oder NAT im Weg?
9. Serverlogs prüfen.
10. Clientlogs oder Fehlermeldung prüfen.

Merksatz:

Erst Verbindung,
dann Protokoll,
dann Anmeldung,
dann Rechte.

Nützliche Prüfpunkte

Prüffrage	Bedeutung
Ist der Server erreichbar?	Schicht 3 prüfen
Ist der Port erreichbar?	Schicht 4 prüfen
Läuft der Dienst?	Schicht 7 prüfen
Stimmt der Benutzer?	Authentifizierung prüfen
Hat der Benutzer Rechte?	Autorisierung prüfen
Ist die Verbindung verschlüsselt?	Sicherheit prüfen
Gibt es Logs?	Ursache genauer finden

Merksatz:

Datei-Probleme sauber nach Schichten eingrenzen.

Was Datei- und Freigabeprotokolle nicht machen

Sie machen nicht automatisch:

- Benutzer korrekt berechtigen
- Daten verschlüsselt speichern
- Backups erstellen
- Malware verhindern
- Datenschutz automatisch erfüllen
- Versionierung bereitstellen
- Konflikte automatisch sinnvoll lösen
- defekte Dateien reparieren

Merksatz:

Dateiübertragung ersetzt kein Berechtigungs-, Backup- oder Sicherheitskonzept.

Typische Ports

Protokoll	Port	Hinweis
FTP	TCP 21	Steuerverbindung
SFTP	TCP 22	über SSH
FTPS explizit	TCP 21	FTP mit TLS-Umschaltung
FTPS implizit	TCP 990	direkt TLS
SMB	TCP 445	Datei- und Druckerfreigaben

Merksatz:

FTP 21,
SFTP 22,
FTPS 990,
SMB 445.

Einordnung in das OSI-Modell

Thema	Schicht
FTP	7
SFTP	7

Thema	Schicht
FTPS	7 mit TLS-Bezug
SMB	7
TLS bei FTPS	6
SSH bei SFTP	7 mit Sicherheitsbezug
TCP-Port 21 / 22 / 445 / 990	4
IP-Adresse des Servers	3
DNS-Name des Servers	7
SMB-Berechtigungen	7 / Betriebssystembezug

Merksatz:

Datei- und Freigabeprotokolle sind Schicht 7,
nutzen aber Schicht 4-Ports.

Typische IHK-Fragen

In AP1 und AP2 kann zum Beispiel gefragt werden:

- Wofür wird FTP genutzt?
- Warum ist klassisches FTP unsicher?
- Was ist der Unterschied zwischen FTP, SFTP und FTPS?
- Welcher Port wird typischerweise für SFTP genutzt?
- Was ist SMB?
- Wofür wird SMB verwendet?
- Welcher Port wird für SMB verwendet?
- Was ist eine SMB-Freigabe?
- Was ist ein UNC-Pfad?
- Was ist der Unterschied zwischen Dateiübertragung und Dateifreigabe?
- Warum sollte SMB nicht direkt ins Internet geöffnet werden?
- Warum kann FTP trotz erfolgreichem Login bei der Dateiübertragung scheitern?
- Welche Rolle spielen Berechtigungen bei SMB?
- Warum sollte man Berechtigungen über Gruppen vergeben?

Typische Prüfungsfallen

FTP ist klassisch unverschlüsselt.

FTP nutzt typischerweise TCP 21.

FTP kann Steuer- und Datenverbindung nutzen.

FTP kann mit NAT und Firewall schwierig sein.

SFTP ist Dateiübertragung über SSH.

SFTP nutzt typischerweise TCP 22.

SFTP ist nicht FTPS.

FTPS ist FTP mit TLS.

Implizites FTPS nutzt häufig TCP 990.

SMB nutzt typischerweise TCP 445.

SMB ist für Datei- und Druckerfreigaben.

SMBv1 ist veraltet und unsicher.

UNC-Pfad sieht aus wie `\\server\freigabe`.

Freigaberechte und Dateisystemrechte zusammen beachten.

Strengere Berechtigung begrenzt den Zugriff.

Berechtigungen möglichst über Gruppen vergeben.

SMB gehört nicht ungeschützt ins Internet.

Wichtige Begriffe kurz erklärt

Begriff	Kurze Erklärung
FTP	klassisches Dateiübertragungsprotokoll

Begriff	Kurze Erklärung
SFTP	Dateiübertragung über SSH
FTPS	FTP mit TLS
SMB	Datei- und Druckerfreigabeprotokoll
Steuerverbindung	FTP-Verbindung für Befehle
Datenverbindung	FTP-Verbindung für Dateinhalt
aktiver FTP-Modus	Server baut Datenverbindung zum Client auf
passiver FTP-Modus	Client baut Datenverbindung zum Server auf
SMB-Freigabe	freigegebener Netzwerkordner
UNC-Pfad	Pfad zu einer Netzwerkfreigabe
Netzlaufwerk	eingebundene Netzwerkfreigabe
Freigabeberechtigung	Recht auf Netzwerkfreigabeebene
Dateisystemberechtigung	Recht auf Datei- oder Ordnebene
effektive Berechtigung	tatsächlich wirkendes Recht
Least Privilege	nur notwendige Rechte vergeben
SMBv1	veraltete unsichere SMB-Version

IHK-sichere Kurzformulierung

FTP, SFTP, FTPS und SMB sind Protokolle der Anwendungsschicht. FTP dient der klassischen Dateiübertragung, ist ohne Zusatzschutz jedoch unverschlüsselt und nutzt typischerweise TCP-Port 21. SFTP ist Dateiübertragung über SSH und nutzt typischerweise TCP-Port 22. FTPS ist FTP mit TLS-Schutz und nutzt je nach Variante TCP-Port 21 oder 990. SMB wird für Datei- und Druckerfreigaben verwendet und nutzt typischerweise TCP-Port 445. Bei SMB sind Freigabeberechtigungen und Dateisystemberechtigungen zu unterscheiden. Moderne Systeme sollten SMBv1 vermeiden und SMB-Freigaben nicht ungeschützt aus dem Internet erreichbar machen.

Merksätze

Dateiübertragung und Freigaben gehören zu Schicht 7.

FTP = File Transfer Protocol.

FTP nutzt typischerweise TCP 21.

FTP ist klassisch unverschlüsselt.

FTP nutzt Steuer- und Datenverbindung.

Passives FTP ist NAT-freundlicher.

SFTP = SSH File Transfer Protocol.

SFTP nutzt typischerweise TCP 22.

SFTP ist Dateiübertragung über SSH.

FTPS = FTP mit TLS.

FTPS ist nicht SFTP.

Implizites FTPS nutzt häufig TCP 990.

SMB = Server Message Block.

SMB nutzt typischerweise TCP 445.

SMB = Datei- und Druckerfreigaben.

SMB-Freigabe = Netzwerkordner.

UNC-Pfad = `\\server\freigabe`.

Netzlaufwerk = eingebundene Freigabe.

Freigaberechte und Dateisystemrechte zusammen prüfen.

Die strengere Berechtigung begrenzt den Zugriff.

Rechte möglichst über Gruppen vergeben.

Least Privilege beachten.

SMBv1 vermeiden.

SMB nicht ungeschützt ins Internet öffnen.

Datei-Probleme mit DNS,
Port,
Dienst,
Anmeldung
und Berechtigungen prüfen.
