17.6 Dateiübertragung, Freigaben und sichere Datenzugriffe in der Praxis

In der Administration müssen Dateien häufig zwischen Systemen, Benutzern, Servern und Diensten übertragen oder gemeinsam bereitgestellt werden.

Typische Beispiele:

```
- Konfigurationsdateien übertragen
- Logdateien herunterladen
- Backups ablegen
- Installationsdateien bereitstellen
- Benutzerfreigaben einrichten
- Projektordner bereitstellen
- Dateien zwischen Servern synchronisieren
- Daten sicher mit externen Personen austauschen
```

Merksatz:

```
Dateiübertragung und Freigaben brauchen immer Technik,
Rechtekonzept
und Sicherheitsregeln.
```

Warum Dateiübertragung sicherheitskritisch ist

Dateien können sensible Informationen enthalten.

Beispiele:

```
Kundendaten
Zugangsdaten
Konfigurationsdateien
Zertifikate
private Schlüssel
Backups
Logdateien
Personalunterlagen
interne Dokumente
```

Quellcode

Risiken:

Datenabfluss
unberechtigter Zugriff
Manipulation
Malware-Verteilung
Verlust von Vertraulichkeit
falsche Berechtigungen
versehentlich öffentliche Freigaben

Merksatz:

Dateien sind oft genauso kritisch wie Datenbanken.

Grundfragen vor jeder Freigabe

Vor einer Freigabe sollte geklärt werden:

Wer braucht Zugriff?

Auf welche Daten?

Mit welchen Rechten?

Von welchem Ort?

Für welchen Zeitraum?

Muss Zugriff protokolliert werden?

Müssen Daten verschlüsselt übertragen werden?

Müssen Daten verschlüsselt gespeichert werden?

Merksatz:

Keine Freigabe ohne Zweck,
Berechtigung
und Begrenzung.

Lesen, Schreiben und Löschen

Die wichtigsten Dateiaktionen sind:

lesen

schreiben

löschen

Lesen:

Datei anzeigen oder herunterladen

Schreiben:

Datei verändern oder neue Datei erstellen

Löschen:

Datei entfernen

Merksatz:

Schreibrechte sind gefährlicher als Leserechte.
Löschrechte sind besonders kritisch.

Minimal notwendige Rechte

Nicht jeder Benutzer braucht Vollzugriff.

Beispiele:

```
Leser:
darf Dateien öffnen,
aber nicht verändern

Bearbeiter:
darf Dateien ändern

Besitzer:
darf Rechte ändern

Administrator:
darf technische Verwaltung durchführen
```

Merksatz:

```
So wenig Rechte wie möglich,
so viele wie nötig.
```

Freigabe und Dateisystem unterscheiden

Bei Dateizugriff gibt es oft mehrere Ebenen.

Beispiel Windows:

```
Freigaberechte

und

NTFS-Rechte
```

Beispiel Linux:

```
Samba-Freigaberechte

und

Linux-Dateirechte
```

Wichtig:

```
Beide Ebenen müssen zusammenpassen.
```

Merksatz:

```
Freigabe erlaubt Zugang.
Dateisystemrechte entscheiden zusätzlich,
was wirklich möglich ist.
```

SMB

SMB steht für:

```
Server Message Block
```

SMB wird häufig für Datei- und Druckerfreigaben in Windows-Netzwerken genutzt.

Typische Nutzung:

```
Netzlaufwerke
gemeinsame Ordner
Druckerfreigaben
Benutzerprofile
Abteilungsfreigaben
Dateiserver
```

Standardport:

```
TCP 445
```

Merksatz:

```
SMB ist das typische Protokoll für Windows-Dateifreigaben.
```

SMB in der Praxis

Beispiele:

```
\\server\freigabe

Netzlaufwerk verbinden

Abteilungsordner bereitstellen

Scanner speichert in Netzwerkordner

Anwendung greift auf zentrale Dateien zu
```

Merksatz:

```
SMB-Freigaben sind praktisch,
aber müssen sauber berechtigt werden.
```

SMB-Sicherheit

Wichtige Maßnahmen:

```
alte SMB-Versionen deaktivieren
keine Gastzugriffe
starke Authentifizierung
Rechte über Gruppen vergeben
Freigaben nicht unnötig breit setzen
Zugriff protokollieren
Adminfreigaben schützen
Netzwerkzugriff begrenzen
Verschlüsselung prüfen
Backups schützen
```

Merksatz:

```
SMB-Freigaben niemals pauschal für alle öffnen.
```

SMB-Versionen

Ältere SMB-Versionen sind unsicherer.

Besonders alte Versionen sollten vermieden werden, wenn sie nicht zwingend benötigt werden.

Wichtig:

```
moderne SMB-Versionen nutzen
alte Kompatibilität nur bewusst aktivieren
Altgeräte prüfen
Risiken dokumentieren
```

Merksatz:

```
Alte SMB-Versionen erhöhen das Sicherheitsrisiko.
```

NFS

NFS steht für:

```
Network File System
```

NFS wird häufig in Unix-, Linux- und Serverumgebungen genutzt.

Typische Nutzung:

```
gemeinsame Verzeichnisse
Serverfreigaben
Linux-Dateiserver
Virtualisierungsspeicher
Container- oder Anwendungsdaten
Backup-Ziele
```

Merksatz:

```
NFS ist ein typisches Dateifreigabeprotokoll in Unix- und Linux-Umgebungen.
```

NFS-Sicherheit

Bei NFS wichtig:

erlaubte Clients begrenzen
Exporte sauber konfigurieren
Schreibrechte nur wenn nötig
Root-Zugriff einschränken
Netzwerksegmentierung nutzen
Firewall-Regeln setzen
NFS-Version beachten
Berechtigungen auf Dateisystemebene prüfen

Merksatz:

NFS-Zugriff immer auf notwendige Clients begrenzen.

FTP

FTP steht für:

File Transfer Protocol

FTP dient zur Dateiübertragung.

Problem:

klassisches FTP überträgt Daten und Zugangsdaten unverschlüsselt.

Standardports:

TCP 21 für Steuerverbindung

Datenverbindungen je nach aktivem oder passivem Modus

Merksatz:

Klassisches FTP ist unsicher,
weil es unverschlüsselt ist.

Warum FTP problematisch ist

Bei klassischem FTP können mitgelesen werden:

```
Benutzername
Passwort
Dateinamen
Dateiinhalt
Befehle
```

Risiko:

```
Sniffing
Passwortdiebstahl
Datenabfluss
Manipulation bei unsicherem Netzwerk
```

Merksatz:

```
FTP nicht für vertrauliche Daten oder unsichere Netze verwenden.
```

SFTP

SFTP steht für:

```
SSH File Transfer Protocol
```

SFTP nutzt SSH als sichere Grundlage.

Standardport:

```
TCP 22
```

Vorteile:

```
verschlüsselte Übertragung
SSH-Authentifizierung
Schlüsselanmeldung möglich
häufig auf Servern verfügbar
```

besser geeignet als klassisches FTP

Merksatz:

SFTP ist sichere Dateiübertragung über SSH.

SCP

SCP steht für:

Secure Copy

SCP wird für Dateiübertragung über SSH genutzt.

Typische Nutzung:

Datei auf Server kopieren

Datei vom Server herunterladen

Dateien zwischen Systemen übertragen

Einordnung:

ebenfalls verschlüsselt über SSH

Merksatz:

SCP kopiert Dateien verschlüsselt über SSH.

SFTP und SCP vergleichen

Merkmal	SFTP	SCP
Grundlage	SSH	SSH
Zweck	Dateiübertragung mit Dateiverwaltung	einfaches Kopieren
Bedienung	eher wie Dateisitzung	eher Kopierbefehl

Merkmal	SFTP	SCP
Verschlüsselung	ja	ja
Standardport	TCP 22	TCP 22

Merksatz:

> SFTP und SCP nutzen SSH,
> sind aber nicht dasselbe wie FTP.

FTPS

FTPS bedeutet:

> FTP mit TLS-Verschlüsselung

FTPS ist nicht dasselbe wie SFTP.

FTPS nutzt FTP-Technik mit TLS.

SFTP nutzt SSH.

Merksatz:

> FTPS = FTP über TLS.
> SFTP = Dateiübertragung über SSH.

FTP, FTPS und SFTP vergleichen

Protokoll	Verschlüsselung	Grundlage	Einordnung
FTP	nein	FTP	unsicher in Klartext
FTPS	ja	FTP plus TLS	verschlüsseltes FTP
SFTP	ja	SSH	sichere Dateiübertragung über SSH

Merksatz:

> SFTP und FTPS nicht verwechseln.

HTTPS-Dateidownload

Dateien können auch über HTTPS bereitgestellt werden.

Beispiele:

```
Downloadportal
Cloudspeicher-Link
Softwaredownload
internes Webportal
API-Dateiabruf
```

Vorteile:

```
verschlüsselte Übertragung
browserfähig
gut für Downloads
Zugriff über Webauthentifizierung möglich
```

Risiken:

```
öffentliche Links
falsche Rechte
abgelaufene Links fehlen
keine Zugriffskontrolle
versehentliche Veröffentlichung
```

Merksatz:

```
HTTPS schützt die Übertragung,
aber nicht automatisch die Freigaberechte.
```

WebDAV

WebDAV erweitert HTTP, damit Dateien über Webprotokolle verwaltet werden können.

Typische Nutzung:

Netzlaufwerk über Webzugriff
Dokumentenablage
Dateiablage über HTTPS
Zusammenarbeit über Webserver

Merksatz:

WebDAV ermöglicht Dateiverwaltung über HTTP oder HTTPS.

Cloud-Speicherfreigaben

Cloud-Speicherfreigaben sind verbreitet.

Beispiele:

Linkfreigabe
Freigabe an Benutzer
Freigabe an Gruppe
externe Freigabe
geteilte Ordner
Ablaufdatum für Links

Risiken:

Link öffentlich weitergegeben
falsche Person berechtigt
Schreibrechte statt Leserechte
kein Ablaufdatum
keine MFA
keine Protokollierung

Merksatz:

Cloud-Freigaben regelmäßig prüfen.

Linkfreigabe

Eine Linkfreigabe erlaubt Zugriff über einen Link.

Mögliche Varianten:

```
jeder mit Link kann lesen

jeder mit Link kann bearbeiten

nur bestimmte Personen können zugreifen

Link mit Passwort

Link mit Ablaufdatum
```

Merksatz:

```
Jeder-mit-Link-Freigaben sind besonders kritisch.
```

Ablaufdatum für Freigaben

Freigaben sollten zeitlich begrenzt werden, wenn sie nur vorübergehend benötigt werden.

Beispiele:

```
externer Projektpartner

Bewerbungsunterlagen

temporärer Austausch

Dienstleisterzugang
```

Merksatz:

```
Temporäre Freigaben brauchen ein Ablaufdatum.
```

Externe Freigaben

Externe Freigaben erlauben Zugriff außerhalb der Organisation.

Risiken:

falsche Empfänger
Datenabfluss
unkontrolliertes Weiterleiten
fehlende MFA
unklare Verantwortlichkeit
Datenschutzproblem

Schutz:

nur bei Bedarf
Genehmigung
Ablaufdatum
Passwort oder MFA
Protokollierung
Datenklassifizierung beachten

Merksatz:

Externe Freigaben nur bewusst und kontrolliert einsetzen.

Datenklassifizierung bei Freigaben

Nicht jede Datei darf gleich behandelt werden.

Beispiele:

öffentlich

intern

vertraulich

streng vertraulich

personenbezogen

Je höher der Schutzbedarf, desto strenger müssen Freigabe, Verschlüsselung und Protokollierung sein.

Merksatz:

```
Schutzbedarf bestimmt Freigaberegeln.
```

Verschlüsselung bei Übertragung

Daten sollten bei Übertragung verschlüsselt werden.

Geeignete Protokolle:

```
SFTP
SCP
FTPS
HTTPS
VPN
SMB-Verschlüsselung je nach Umgebung
```

Unsicher oder kritisch:

```
FTP
Telnet
HTTP bei vertraulichen Daten
unverschlüsselte Protokolle
```

Merksatz:

```
Vertrauliche Daten nicht unverschlüsselt übertragen.
```

Verschlüsselung bei Speicherung

Daten können auch im Ruhezustand verschlüsselt werden.

Beispiele:

```
Festplattenverschlüsselung
Serververschlüsselung
Datenbankverschlüsselung
Backup-Verschlüsselung
```

Cloud-Speicherverschlüsselung
verschlüsselte Archive

Merksatz:

Verschlüsselung bei Speicherung schützt bei Diebstahl oder unberechtigtem Zugriff auf Speicher.

Passwortgeschützte Archive

Archive können mit Passwort geschützt werden.

Beispiele:

ZIP mit Passwort

7z mit Passwort

Wichtig:

Passwort getrennt vom Archiv übermitteln
starke Verschlüsselung nutzen
Passwort nicht in derselben E-Mail senden
sichere Alternative prüfen

Merksatz:

Passwort und Datei nicht über denselben unsicheren Kanal senden.

Prüfsummen

Prüfsummen helfen, Dateien auf Integrität zu prüfen.

Beispiele:

SHA-256
SHA-512

Zweck:

```
feststellen,
ob Datei verändert wurde
Download prüfen
Übertragungsfehler erkennen
Manipulation erkennen
```

Merksatz:

```
Prüfsumme prüft Integrität,
aber nicht automatisch Vertrauenswürdigkeit.
```

Digitale Signatur bei Dateien

Eine digitale Signatur kann prüfen, ob eine Datei vom erwarteten Herausgeber stammt und nicht verändert wurde.

Beispiele:

```
signierte Softwarepakete
signierte Skripte
signierte Installationsdateien
```

Merksatz:

```
Signatur prüft Herkunft und Integrität.
```

Malware-Risiko bei Dateiübertragung

Dateien können Malware enthalten.

Risiken:

```
Makros in Dokumenten
Skripte
ausführbare Dateien
manipulierte PDFs
Archive mit Schadsoftware
ISO-Dateien
```

```
LNK-Dateien
Webshells bei Uploads
```

Schutz:

```
Malware-Scan
Dateitypen begrenzen
Makros blockieren
Uploads prüfen
Benutzer schulen
nur vertrauenswürdige Quellen
```

Merksatz:

```
Dateiübertragung kann auch Malware übertragen.
```

Upload-Verzeichnisse

Upload-Verzeichnisse sind besonders kritisch.

Schutzmaßnahmen:

```
keine Ausführung erlauben
Dateitypen begrenzen
Dateigröße begrenzen
zufällige Dateinamen
Malware-Scan
Speicherung außerhalb des Webroots
Rechte begrenzen
Protokollierung
```

Merksatz:

```
Hochgeladene Dateien dürfen nicht ungeprüft ausführbar sein.
```

Synchronisation

Synchronisation hält Dateien an mehreren Orten gleich.

Beispiele:

Cloud-Sync
Ordnersynchronisation
Server-zu-Server-Sync
Notebook und Cloudspeicher
mobile Geräte

Risiko:

Löschungen werden synchronisiert
Ransomware verschlüsselt synchronisierte Dateien
falsche Version überschreibt richtige Datei
Datenabfluss durch falsche Freigabe

Merksatz:

Synchronisation ist kein Backup.

Backup und Dateiübertragung unterscheiden

Dateiübertragung:

bewegt oder kopiert Dateien

Synchronisation:

hält Orte gleich

Backup:

erstellt wiederherstellbare Sicherungen mit Aufbewahrung

Merksatz:

Kopie,
Sync

und Backup sind nicht dasselbe.

Versionierung

Versionierung speichert ältere Dateiversionen.

Vorteile:

```
versehentliche Änderungen rückgängig machen
ältere Stände wiederherstellen
Ransomware-Schäden begrenzen
Bearbeitungsverlauf nachvollziehen
```

Grenze:

```
Versionierung ersetzt kein vollständiges Backup.
```

Merksatz:

```
Versionierung hilft,
aber ersetzt kein Backup-Konzept.
```

DLP

DLP steht für:

```
Data Loss Prevention
```

DLP soll verhindern, dass sensible Daten unkontrolliert abfließen.

Beispiele:

```
blockiert Upload vertraulicher Dateien
warnt bei Versand personenbezogener Daten
verhindert Kopieren auf USB
kontrolliert Cloud-Freigaben
erkennt Kreditkartendaten oder Personaldaten
```

Merksatz:

> DLP schützt vor unerwünschtem Datenabfluss.

Freigabeprotokollierung

Freigaben sollten protokolliert werden.

Wichtige Fragen:

> Wer hat Datei geöffnet?
> Wer hat Datei geändert?
> Wer hat Datei gelöscht?
> Wer hat Freigabe erstellt?
> Wer hat extern geteilt?
> Wann wurde Zugriff genutzt?
> Von welchem Gerät oder welcher IP?

Merksatz:

> Kritische Datenzugriffe müssen nachvollziehbar sein.

Besitzer von Freigaben

Jede Freigabe sollte einen Verantwortlichen haben.

Aufgaben:

> Zweck prüfen
> Berechtigungen prüfen
> alte Freigaben entfernen
> externe Zugriffe kontrollieren
> Datenklassifizierung beachten
> Löschung oder Archivierung entscheiden

Merksatz:

> Freigaben ohne Verantwortlichen werden schnell unübersichtlich.

Freigaben regelmäßig prüfen

Zu prüfen:

Gibt es unnötige Freigaben?
Gibt es Jeder- oder Everyone-Rechte?
Gibt es externe Benutzer?
Gibt es Schreibrechte,
obwohl Leserechte reichen?
Gibt es alte Projektordner?
Gibt es Freigaben ohne Besitzer?
Gibt es sensible Daten in falschen Ordnern?

Merksatz:

Freigaben altern und müssen regelmäßig bereinigt werden.

Typische Fehler bei Freigaben

Häufige Fehler:

Jeder hat Vollzugriff
externe Links ohne Ablaufdatum
Schreibrechte statt Leserechte
alte Benutzer noch berechtigt
Gastzugriff aktiv
sensible Daten in öffentlichen Ordnern
Freigabe ohne Besitzer
keine Protokollierung
keine Klassifizierung
Synchronisation wird als Backup verstanden

Merksatz:

Die häufigste Freigabenpanne ist zu breiter Zugriff.

Fehlersuche bei Dateiübertragung

Bei Problemen prüfen:

```
Ist Ziel erreichbar?
Stimmt DNS?
Stimmt Port?
Blockiert Firewall?
Ist Protokoll korrekt?
Stimmen Benutzername und Passwort?
Hat Benutzer Rechte?
Ist Speicherplatz frei?
Ist Datei gesperrt?
Ist Pfad korrekt?
Ist Zertifikat gültig?
Gibt es Logs?
Ist Dateiname erlaubt?
Ist Datei zu groß?
```

Merksatz:

```
Dateiübertragungsfehler können Netzwerk-,
Rechte-,
Speicher-
oder Protokollprobleme sein.
```

Fehlerbild: Zugriff verweigert

Mögliche Ursachen:

```
Benutzer nicht berechtigt
Gruppe fehlt
falsche Anmeldung
Freigaberecht fehlt
Dateisystemrecht fehlt
Deny-Regel aktiv
Datei gesperrt
Konto deaktiviert
externe Freigabe abgelaufen
MFA oder Conditional Access blockiert
```

Merksatz:

Zugriff verweigert ist meistens ein Rechte- oder Identitätsproblem.

Fehlerbild: Verbindung nicht möglich

Mögliche Ursachen:

Server offline
DNS falsch
Port blockiert
Dienst läuft nicht
Firewall blockiert
VPN fehlt
falsches Protokoll
Routingproblem
falsche Adresse
Zugriff nur intern erlaubt

Merksatz:

Keine Verbindung zuerst mit Netzwerk,
Port
und Dienst prüfen.

Fehlerbild: Dateiübertragung langsam

Mögliche Ursachen:

geringe Bandbreite
hohe Latenz
Paketverlust
viele kleine Dateien
Virenscan
langsamer Datenträger
WLAN-Probleme
VPN-Overhead
Serverlast

Cloud-Limitierung

Merksatz:

Langsame Dateiübertragung kann an Netzwerk,
Speicher
oder Anwendung liegen.

Checkliste: sichere Dateiübertragung und Freigaben

Zweck der Freigabe klären.
Datenklassifizierung prüfen.
Benutzer oder Gruppen festlegen.
Nur notwendige Rechte vergeben.
Schreibrechte begrenzen.
Externe Freigaben begründen.
Ablaufdatum setzen.
Verschlüsselte Übertragung nutzen.
Unsichere Protokolle vermeiden.
Zugriff protokollieren.
Freigaben regelmäßig prüfen.
Alte Zugriffe entfernen.
Malware-Scan für Uploads nutzen.
Backups getrennt planen.
Synchronisation nicht als Backup ansehen.
Verantwortlichen für Freigabe benennen.

Merksatz:

Sichere Freigaben sind begrenzt,
verschlüsselt,
dokumentiert
und regelmäßig geprüft.

Typische IHK-Fragen

In AP1 und AP2 kann zum Beispiel gefragt werden:

- Was ist SMB?
- Wofür wird SMB genutzt?
- Welchen Standardport nutzt SMB?
- Was ist NFS?
- Wofür wird NFS genutzt?
- Warum ist klassisches FTP unsicher?
- Was ist SFTP?
- Was ist SCP?
- Was ist FTPS?
- Was ist der Unterschied zwischen SFTP und FTPS?
- Warum sollte man vertrauliche Daten verschlüsselt übertragen?
- Was ist eine Linkfreigabe?
- Warum sind Jeder-mit-Link-Freigaben kritisch?
- Warum ist ein Ablaufdatum bei Freigaben sinnvoll?
- Was ist DLP?
- Warum ist Synchronisation kein Backup?
- Was ist Versionierung?
- Was prüft eine Prüfsumme?
- Was prüft eine digitale Signatur?
- Warum sind Upload-Verzeichnisse gefährlich?

Typische Prüfungsfallen

FTP ist unverschlüsselt.

SFTP ist nicht FTP mit TLS.

FTPS ist nicht SFTP.

SFTP nutzt SSH.

SCP nutzt SSH.

SMB nutzt typischerweise TCP 445.

Freigaberechte und Dateisystemrechte zusammen prüfen.

Schreibrechte nicht vergeben,

wenn Leserechte reichen.

Jeder-mit-Link ist besonders kritisch.

Externe Freigaben brauchen Kontrolle.

Ablaufdatum reduziert Risiko.

HTTPS schützt Übertragung,
aber nicht automatisch Berechtigung.

Prüfsumme prüft Integrität,
nicht automatisch Vertrauenswürdigkeit.

Digitale Signatur prüft Herkunft und Integrität.

Uploads können Malware enthalten.

Synchronisation ist kein Backup.

Versionierung ersetzt kein vollständiges Backup.

DLP schützt vor Datenabfluss.

Zugriff verweigert ist nicht automatisch ein Netzwerkproblem.

Wichtige Begriffe kurz erklärt

Begriff	Kurze Erklärung
Dateiübertragung	Kopieren oder Bewegen von Dateien
Freigabe	bereitgestellter Zugriff auf Dateien oder Ordner
Leserecht	Datei anzeigen oder herunterladen
Schreibrecht	Datei ändern oder erstellen
Löschrecht	Datei entfernen
SMB	Windows-Dateifreigabeprotokoll
TCP 445	Standardport für SMB
NFS	Network File System

Begriff	Kurze Erklärung
FTP	unverschlüsseltes Dateiübertragungsprotokoll
SFTP	Dateiübertragung über SSH
SCP	sicheres Kopieren über SSH
FTPS	FTP mit TLS
HTTPS-Download	Dateiabruf über verschlüsseltes Webprotokoll
WebDAV	Dateiverwaltung über HTTP oder HTTPS
Linkfreigabe	Zugriff über Link
externe Freigabe	Freigabe außerhalb der Organisation
Ablaufdatum	zeitliche Begrenzung einer Freigabe
Datenklassifizierung	Einteilung nach Schutzbedarf
Verschlüsselung bei Übertragung	Schutz während Transport
Verschlüsselung bei Speicherung	Schutz ruhender Daten
Prüfsumme	Integritätsprüfung einer Datei
digitale Signatur	Herkunfts- und Integritätsprüfung
Upload-Verzeichnis	Speicherort für hochgeladene Dateien
Synchronisation	Abgleich von Dateien zwischen Orten
Backup	wiederherstellbare Sicherung
Versionierung	Speicherung älterer Dateiversionen
DLP	Data Loss Prevention
Freigabeprotokollierung	Nachvollziehen von Zugriffen

IHK-sichere Kurzformulierung

Dateiübertragung und Freigaben dienen dazu, Dateien zwischen Benutzern, Systemen und Diensten bereitzustellen oder zu übertragen. Dabei müssen Vertraulichkeit, Integrität und Verfügbarkeit beachtet werden. SMB wird häufig für Windows-Dateifreigaben genutzt und verwendet typischerweise TCP-Port 445. NFS wird häufig in Unix- und Linux-Umgebungen eingesetzt. Klassisches FTP ist unsicher, weil es unverschlüsselt überträgt. SFTP und SCP nutzen SSH, FTPS nutzt FTP mit TLS. Freigaben sollten nach Least Privilege eingerichtet, regelmäßig geprüft, protokolliert und bei externem Zugriff zeitlich begrenzt werden. Synchronisation ist kein Backup, da Änderungen oder Löschungen mit übertragen werden können.

Merksätze

Dateien können sehr sensible Informationen enthalten.

Keine Freigabe ohne Zweck.

Rechte so eng wie möglich vergeben.

Schreibrechte nur bei Bedarf.

Löschrechte besonders vorsichtig vergeben.

Freigabe und Dateisystemrechte zusammen prüfen.

SMB ist typisch für Windows-Freigaben.

SMB nutzt typischerweise TCP 445.

Alte SMB-Versionen vermeiden.

NFS ist typisch für Unix- und Linux-Freigaben.

NFS-Zugriff auf notwendige Clients begrenzen.

FTP ist unverschlüsselt.

FTP nicht für vertrauliche Daten nutzen.

SFTP nutzt SSH.

SCP kopiert über SSH.

FTPS ist FTP mit TLS.

SFTP und FTPS nicht verwechseln.

HTTPS schützt Übertragung,
aber nicht automatisch Rechte.

Jeder-mit-Link ist kritisch.

Externe Freigaben kontrollieren.

Temporäre Freigaben mit Ablaufdatum versehen.

Schutzbedarf bestimmt Freigaberegeln.

Vertrauliche Daten verschlüsselt übertragen.

Passwort und Datei getrennt übermitteln.

Prüfsumme prüft Integrität.

Signatur prüft Herkunft und Integrität.

Dateiübertragung kann Malware übertragen.

Upload-Verzeichnisse besonders absichern.

Synchronisation ist kein Backup.

Versionierung hilft,
ersetzt aber kein Backup.

DLP schützt vor Datenabfluss.

Freigaben brauchen Verantwortliche.

Freigaben regelmäßig prüfen.

Zugriff verweigert ist oft ein Rechteproblem.

Keine Verbindung ist oft Netzwerk,
Port
oder Dienst.

Sichere Freigaben sind begrenzt,
dokumentiert
und regelmäßig geprüft.