14.5

VPN-Sicherheit, Zugriffskontrolle und typische Risiken

Ein VPN stellt einen sicheren Tunnel bereit.

Aber:

> Ein VPN allein macht ein Netzwerk nicht automatisch sicher.

Wichtig sind zusätzlich:

- starke Authentifizierung
- klare Berechtigungen
- Firewall-Regeln
- Protokollierung
- Gerätesicherheit
- Rollenmodell
- regelmäßige Prüfung
- Monitoring
- saubere Dokumentation

Merksatz:

> VPN ist ein Zugang ins Netz.
> Deshalb muss dieser Zugang besonders geschützt werden.

Warum VPN-Sicherheit wichtig ist

Ein VPN-Zugang kann sehr mächtig sein.

Wenn ein Angreifer VPN-Zugang erhält, kann er je nach Konfiguration interne Systeme erreichen.

Mögliche Folgen:

- Zugriff auf interne Server
- Zugriff auf Dateifreigaben
- Ausbreitung von Malware

- Angriff auf Managementsysteme
- Datenabfluss
- Manipulation interner Dienste
- Umgehung äußerer Schutzmaßnahmen

Merksatz:

> Ein schlecht abgesicherter VPN-Zugang ist ein großes Risiko.

VPN ist kein Freifahrtschein

Ein häufiger Fehler ist:

> Benutzer ist per VPN verbunden.
> Also darf er alles im internen Netz erreichen.

Das ist unsicher.

Besser:

> Benutzer bekommt nur Zugriff auf die Systeme,
> die er für seine Aufgabe braucht.

Beispiele:

> Mitarbeiter:
> Intranet und Dateiablage
>
> Support:
> Ticketsystem und bestimmte Clients
>
> Administrator:
> Managementsysteme
>
> Dienstleister:
> nur definierter Wartungsserver

Merksatz:

```
VPN verbunden heißt nicht:
Zugriff auf alles erlaubt.
```

Authentifizierung

Authentifizierung bedeutet:

```
Wer bist du?
```

Beim VPN wird geprüft, ob der Benutzer oder das Gerät wirklich berechtigt ist.

Mögliche Faktoren:

```
Benutzername
Passwort
Zertifikat
MFA
Token
Smartcard
Gerätezertifikat
SSO
biometrischer Faktor
```

Merksatz:

```
Authentifizierung prüft die Identität.
```

Autorisierung

Autorisierung bedeutet:

```
Was darfst du?
```

Nach erfolgreicher Anmeldung entscheidet das System, welche Ziele, Dienste und Anwendungen erlaubt sind.

Beispiele:

```
Zugriff auf Servernetz erlaubt?
Zugriff auf Managementnetz erlaubt?
Zugriff auf RDP erlaubt?
Zugriff auf Datenbank verboten?
Zugriff nur auf HTTPS erlaubt?
```

Merksatz:

```
Authentifizierung ist Anmeldung.
Autorisierung ist Berechtigung.
```

MFA bei VPN

MFA steht für:

```
Multi-Faktor-Authentifizierung
```

Dabei werden mehrere Faktoren kombiniert.

Beispiele:

```
Passwort + Authenticator-App

Passwort + Hardwaretoken

Zertifikat + PIN

Smartcard + PIN
```

Warum wichtig?

```
Passwörter können gestohlen werden.
Phishing kann Zugangsdaten abgreifen.
VPN ist aus dem Internet erreichbar.
VPN-Zugang führt oft in interne Netze.
```

Merksatz:

VPN-Zugänge sollten möglichst mit MFA geschützt werden.

MFA ist nicht unfehlbar

MFA erhöht die Sicherheit deutlich, ist aber kein vollständiger Schutz.

Risiken bleiben:

Phishing
MFA-Push-Fatigue
gestohlene Session-Tokens
unsicheres Endgerät
Social Engineering
schlecht konfigurierte Ausnahmen
fehlende Gerätekontrolle

Merksatz:

MFA ist stark,
aber kein Ersatz für weitere Schutzmaßnahmen.

MFA-Push-Fatigue

MFA-Push-Fatigue bedeutet:

Ein Angreifer löst viele MFA-Anfragen aus,
bis der Benutzer genervt oder aus Versehen bestätigt.

Schutz:

Number Matching
kurze Hinweise zur Anfrage
Schulung
verdächtige Anfragen melden
Rate Limiting
keine blinde Bestätigung

Merksatz:

MFA-Anfragen niemals automatisch bestätigen.

Zertifikatsbasierte VPN-Authentifizierung

VPN kann Zertifikate verwenden.

Dabei kann geprüft werden:

Ist das Gerät zugelassen?
Ist der Benutzer zugelassen?
Ist das Zertifikat gültig?
Wurde das Zertifikat widerrufen?
Vertraut der Client dem VPN-Gateway?

Vorteile:

stärker als Passwort allein
Gerätebindung möglich
Widerruf einzelner Zertifikate möglich
gut für verwaltete Geräte

Merksatz:

Zertifikate können VPN-Zugriffe stärker an Geräte oder Identitäten binden.

Clientzertifikat

Ein Clientzertifikat liegt auf dem Endgerät oder in einem sicheren Speicher.

Es kann beweisen:

Dieses Gerät oder dieser Benutzer ist berechtigt,
sich am VPN anzumelden.

Wichtig:

```
privater Schlüssel schützen
Zertifikat nicht kopieren
verlorene Geräte sperren
Zertifikat bei Austritt widerrufen
Ablaufdatum überwachen
```

Merksatz:

```
Clientzertifikat ist nur sicher,
wenn der private Schlüssel geschützt ist.
```

Serverzertifikat

Das Serverzertifikat des VPN-Gateways hilft dem Client zu prüfen:

```
Verbinde ich mich wirklich mit dem richtigen VPN-Server?
```

Fehler können sein:

```
Zertifikat abgelaufen
Name passt nicht
CA nicht vertrauenswürdig
Zertifikatskette unvollständig
falsches Zertifikat auf Gateway
```

Merksatz:

```
Serverzertifikat schützt vor Verbindung zur falschen Gegenstelle.
```

Zertifikatswiderruf

Wenn ein Zertifikat nicht mehr vertrauenswürdig ist, muss es widerrufen werden.

Gründe:

```
Gerät verloren
privater Schlüssel kompromittiert
```

```
Benutzer ausgeschieden
Dienstleisterzugang beendet
Zertifikat falsch ausgestellt
```

Widerruf kann geprüft werden über:

```
CRL
OCSP
```

Merksatz:

```
Zertifikate müssen widerrufen werden können.
```

Benutzergruppen

VPN-Zugriffe sollten über Gruppen gesteuert werden.

Beispiele:

```
VPN-Mitarbeiter

VPN-Support

VPN-Admins

VPN-Dienstleister

VPN-Partner
```

Vorteil:

```
Regeln bleiben übersichtlich.
Rechte lassen sich zentral verwalten.
Austritte und Rollenwechsel sind einfacher.
Zugriff kann nach Aufgabe getrennt werden.
```

Merksatz:

Gruppen machen VPN-Berechtigungen verwaltbar.

Rollenmodell

Ein Rollenmodell beschreibt, welche Rolle welche Zugriffe bekommt.

Beispiel:

Rolle	erlaubter Zugriff
Mitarbeiter	Intranet, Dateiablage
Support	Ticketsystem, bestimmte Clients
Administrator	Managementnetz, Serververwaltung
Dienstleister	definierter Wartungsserver
Partner	Extranet-Portal
Cloud-Admin	Cloud-Managementzugänge

Merksatz:

Rollenmodell verhindert pauschale Freigaben.

Least Privilege beim VPN

Least Privilege bedeutet:

nur die Rechte,
die wirklich benötigt werden.

Beim VPN heißt das:

keine pauschale LAN-Freigabe
keine unnötigen Ports
keine unnötigen Zielnetze
keine Dauerzugänge für Externe
keine gemeinsamen Konten
keine Adminrechte für normale Benutzer

Merksatz:

VPN-Zugriff so eng wie möglich,
so weit wie nötig.

Need to Know beim VPN

Need to Know bedeutet:

Zugriff nur auf Informationen oder Systeme,
die für die Aufgabe notwendig sind.

Beispiel:

Ein Lieferant braucht Zugriff auf Bestelldaten,
aber nicht auf Personalakten.

Ein Wartungsdienstleister braucht Zugriff auf eine Anlage,
aber nicht auf das gesamte Servernetz.

Merksatz:

VPN-Zugriff nach Aufgabe begrenzen,
nicht nach Bequemlichkeit.

Zero Trust und VPN

Zero Trust bedeutet:

kein Zugriff wird automatisch vertraut.

Auch nach VPN-Verbindung wird weiter geprüft:

Wer ist der Benutzer?
Welches Gerät wird genutzt?
Ist MFA erfüllt?
Ist das Gerät aktuell?
Welche Anwendung wird aufgerufen?

Welche Rolle hat der Benutzer?

Ist der Zugriff ungewöhnlich?

Merksatz:

Zero Trust prüft Zugriff fortlaufend und kontextbezogen.

Klassisches VPN und Zero Trust vergleichen

Merkmal	klassisches VPN	Zero-Trust-Zugriff
Zugriff	oft Netzwerkzugriff	meist Anwendungszugriff
Prüfung	häufig beim Tunnelaufbau	kontinuierlicher
Reichweite	kann breit sein	stärker begrenzt
Risiko	laterale Bewegung möglich	weniger pauschaler Netzblick
Vorteil	bewährt, flexibel	feiner steuerbar

Merksatz:

VPN verbindet oft ins Netz.

Zero Trust gibt gezielt Anwendungen frei.

Laterale Bewegung

Laterale Bewegung bedeutet:

Ein Angreifer bewegt sich nach dem ersten Zugriff weiter im internen Netz.

Beispiel:

Angreifer erhält VPN-Zugang.

Danach scannt er interne Server.

Anschließend greift er weitere Systeme an.

Schutz:

Segmentierung
Firewall-Regeln
Least Privilege
Monitoring
EDR
getrennte Adminzugänge
keine pauschale VPN-Freigabe

Merksatz:

VPN darf keine einfache Bewegung durchs ganze Netz ermöglichen.

Netzsegmentierung

Netzsegmentierung bedeutet:

Das Netzwerk wird in getrennte Bereiche aufgeteilt.

Beispiele:

Clientnetz
Servernetz
Managementnetz
DMZ
Gastnetz
IoT-Netz
VPN-Zone
Extranet-Zone

Vorteil:

Ein kompromittierter Bereich kann nicht automatisch alles erreichen.

Merksatz:

Segmentierung begrenzt Schäden.

VPN-Zone

Eine VPN-Zone ist eine eigene Sicherheitszone für VPN-Verkehr.

Beispiele:

```
VPN-Mitarbeiter-Zone

VPN-Admin-Zone

VPN-Dienstleister-Zone

VPN-Partner-Zone
```

Dadurch kann man Firewall-Regeln gezielt definieren.

Merksatz:

```
VPN-Zonen verhindern,
dass VPN-Verkehr wie normales LAN behandelt wird.
```

Admin-VPN besonders schützen

Admin-Zugänge sind besonders kritisch.

Admin-VPN sollte streng geschützt werden:

```
separate Admin-Konten
MFA
Zertifikat
Zugriff nur von verwalteten Geräten
keine private Nutzung
Zugriff nur auf Managementnetze
Protokollierung
Alarmierung bei Fehlversuchen
regelmäßige Prüfung
```

Merksatz:

```
Admin-VPN ist Hochrisiko-Zugang.
```

Dienstleister-VPN besonders begrenzen

Externe Dienstleister sollten keinen breiten VPN-Zugriff erhalten.

Sicherer ist:

```
eigenes Konto pro Person
keine Sammelkonten
MFA
zeitliche Begrenzung
Zugriff nur auf Zielsystem
Protokollierung
Freigabeprozess
Deaktivierung nach Wartung
regelmäßige Prüfung
```

Merksatz:

```
Dienstleisterzugang muss eng,
nachvollziehbar
und zeitlich begrenzt sein.
```

Sammelkonten vermeiden

Sammelkonten sind gemeinsame Benutzerkonten, die mehrere Personen nutzen.

Problem:

```
keine eindeutige Zuordnung
schwierige Nachvollziehbarkeit
Passwort wird weitergegeben
Sperrung einzelner Personen schwer
Sicherheitsvorfälle schwer aufklärbar
```

Merksatz:

Jeder VPN-Benutzer braucht ein eigenes Konto.

Zeitlich begrenzter Zugriff

Manche VPN-Zugänge sollten nur für ein Zeitfenster aktiv sein.

Beispiele:

Wartung am Samstag
Projektzugang für zwei Wochen
externer Support während Störung
temporäre Migration

Nach Ende:

Zugriff deaktivieren
Regel entfernen
Konto sperren
Logs prüfen
Dokumentation aktualisieren

Merksatz:

Temporärer Zugriff darf nicht dauerhaft bleiben.

Offboarding

Offboarding bedeutet:

Zugriffe bei Austritt oder Rollenwechsel entfernen.

Beim VPN wichtig:

Konto deaktivieren
Gruppenmitgliedschaft entfernen
Zertifikate widerrufen
Tokens sperren

Gerätezugriff entziehen
Dienstleisterzugänge prüfen
Dokumentation aktualisieren

Merksatz:

Wer nicht mehr berechtigt ist,
darf keinen VPN-Zugang behalten.

Gerätesicherheit beim VPN

Ein VPN-Client ist ein Einstiegspunkt ins interne Netz.

Deshalb sollte das Gerät sicher sein.

Wichtige Anforderungen:

aktuelles Betriebssystem
aktuelle Sicherheitsupdates
Schutzsoftware
Festplattenverschlüsselung
Bildschirmsperre
kein lokaler Admin für Alltagsnutzer
sichere Konfiguration
MDM oder Gerätemanagement
keine Malware

Merksatz:

Unsicheres Gerät plus VPN ist gefährlich.

Managed Device

Ein Managed Device ist ein verwaltetes Gerät.

Das Unternehmen kann Vorgaben prüfen und durchsetzen.

Beispiele:

```
Updates
Verschlüsselung
Gerätesperre
Zertifikate
VPN-Profil
Sicherheitsrichtlinien
Softwarestand
Remote Wipe bei Verlust
```

Merksatz:

```
Verwaltete Geräte sind für VPN-Zugänge besser kontrollierbar.
```

BYOD und VPN

BYOD steht für:

```
Bring Your Own Device
```

Dabei nutzt ein Benutzer ein privates Gerät beruflich.

Bei VPN ist das riskant, wenn das private Gerät nicht kontrolliert wird.

Fragen:

```
Ist das Gerät aktuell?
Ist es verschlüsselt?
Ist es kompromittiert?
Gibt es MDM?
Sind Firmen- und Privatdaten getrennt?
Kann Zugriff bei Verlust entzogen werden?
```

Merksatz:

```
BYOD-VPN braucht klare Regeln und technische Kontrolle.
```

Geräteprüfung vor VPN-Zugang

Manche Umgebungen prüfen Geräte vor dem Zugriff.

Prüfkriterien:

aktueller Patchstand
aktivierte Festplattenverschlüsselung
aktive Schutzsoftware
Gerätezertifikat vorhanden
nicht gerootet oder jailbroken
MDM-konform
sichere Bildschirmperre

Merksatz:

Nicht jedes Gerät sollte automatisch VPN-Zugang bekommen.

Posture Check

Posture Check bedeutet:

Der Sicherheitszustand eines Geräts wird geprüft.

Beispiele:

Ist Antivirus aktiv?
Ist das Betriebssystem aktuell?
Ist die Festplatte verschlüsselt?
Ist das Gerät verwaltet?
Ist ein Zertifikat vorhanden?

Merksatz:

Posture Check prüft,
ob ein Gerät sicher genug für Zugriff ist.

VPN und Malware

Wenn ein Gerät mit Malware infiziert ist, kann VPN gefährlich werden.

Risiken:

```
Malware erreicht interne Systeme.
Zugangsdaten werden abgegriffen.
interne Server werden gescannt.
Daten werden exfiltriert.
Ransomware breitet sich aus.
```

Schutz:

```
Endgeräteschutz
EDR
Segmentierung
Least Privilege
Monitoring
keine pauschalen Freigaben
```

Merksatz:

```
VPN kann Malware einen Weg ins interne Netz geben,
wenn Zugriffe zu breit sind.
```

VPN und Phishing

Angreifer versuchen oft, VPN-Zugangsdaten zu stehlen.

Typische Methoden:

```
gefälschte Loginseiten
gefälschte Support-Mails
MFA-Abfragen auslösen
Passwort-Wiederverwendung ausnutzen
Schadsoftware auf Endgerät
```

Schutz:

```
MFA
Schulung
```

Passwortmanager
Zertifikate
verdächtige Logins erkennen
klare Meldewege

Merksatz:

VPN-Zugangsdaten sind ein attraktives Angriffsziel.

VPN und Brute Force

Brute Force bedeutet:

Angreifer probieren viele Zugangsdaten aus.

Schutzmaßnahmen:

MFA
Account Lockout
Rate Limiting
starke Passwörter
keine Standardkonten
Geoblocking bei Bedarf
Monitoring
Alarmierung

Merksatz:

VPN-Loginversuche müssen überwacht und begrenzt werden.

VPN und Passwort-Wiederverwendung

Wenn Benutzer dasselbe Passwort bei mehreren Diensten verwenden, kann ein fremder Datenabfluss zum VPN-Risiko werden.

Beispiel:

```
Passwort aus privatem Dienst wird geleakt.
Angreifer probiert es am VPN-Portal.
Login funktioniert.
```

Schutz:

```
Passwortmanager
eindeutige Passwörter
MFA
Leak-Erkennung
Schulung
```

Merksatz:

```
Wiederverwendete Passwörter gefährden VPN-Zugänge.
```

VPN und Logging

VPN-Zugriffe sollten protokolliert werden.

Wichtige Informationen:

```
Benutzer
Gerät
Quell-IP
Zeitpunkt
VPN-IP
Verbindungsdauer
MFA-Ergebnis
zugewiesene Gruppe
Fehlergrund
getrennte Verbindung
Zielzugriffe je nach System
```

Merksatz:

```
VPN-Logs ermöglichen Nachvollziehbarkeit.
```

VPN und Alarmierung

Bestimmte VPN-Ereignisse sollten Alarm auslösen.

Beispiele:

```
viele fehlgeschlagene Logins
Login aus ungewöhnlichem Land
Admin-VPN außerhalb Arbeitszeit
neues Gerät
abgelaufenes Zertifikat
Dienstleisterzugang außerhalb Zeitfenster
ungewöhnlich lange Verbindung
ungewöhnlich hoher Datenverkehr
```

Merksatz:

```
Kritische VPN-Ereignisse sollten nicht unbemerkt bleiben.
```

VPN und Monitoring

VPN-Infrastruktur sollte überwacht werden.

Wichtige Werte:

```
Tunnelstatus
aktive Benutzer
CPU des Gateways
RAM
Bandbreite
Paketverlust
Latenz
Fehlversuche
Zertifikatsablauf
Lizenzgrenzen
Verbindungsabbrüche
```

Merksatz:

VPN ist kritische Infrastruktur und gehört ins Monitoring.

VPN und Protokollierung von Adminaktionen

Bei Admin-VPN reicht oft nicht nur der Login.

Zusätzlich wichtig:

Welche Systeme wurden verwaltet?
Welche Änderungen wurden durchgeführt?
Welche Befehle wurden ausgeführt?
Welche Tickets gehören dazu?
Wer hat die Änderung freigegeben?

Je nach Umgebung werden dafür Bastion Hosts, Jump Server oder Session Recording genutzt.

Merksatz:

Adminzugriffe müssen besonders nachvollziehbar sein.

Bastion Host

Ein Bastion Host ist ein besonders gehärteter Zwischenserver für administrative Zugriffe.

Ablauf:

Admin verbindet sich per VPN.
Admin verbindet sich auf Bastion Host.
Von dort geht es zu Zielsystemen.

Vorteile:

zentraler Kontrollpunkt
bessere Protokollierung
weniger direkte Zugriffe
klare Zugriffspfade

Merksatz:

Bastion Host bündelt und kontrolliert Adminzugriffe.

Jump Server

Jump Server ist ein ähnlicher Begriff wie Bastion Host.

Er dient als Sprungpunkt in geschützte Netze.

Beispiele:

Zugriff auf Servernetz
Zugriff auf Managementnetz
Zugriff auf OT-Netz
Zugriff auf Cloud-Adminsysteme

Merksatz:

Jump Server verhindert direkte Adminzugriffe von beliebigen Clients.

VPN und Managementnetz

Managementnetze enthalten besonders kritische Systeme.

Beispiele:

Switch-Verwaltung
Firewall-Verwaltung
Hypervisor
Backup-System
Monitoring
Storage-System
Domain Controller
Admin-Portale

VPN-Zugriff auf Managementnetze sollte nur für berechtigte Admins erlaubt sein.

Merksatz:

Managementnetz niemals breit per VPN freigeben.

VPN und DMZ

Ein VPN-Gateway kann in einer DMZ stehen.

Grund:

Es ist von außen erreichbar.

Nach erfolgreicher Anmeldung wird der Verkehr kontrolliert weitergeleitet.

Wichtig:

DMZ vom LAN trennen
nur notwendige Regeln
Gateway härten
Logs prüfen
Updates durchführen
Monitoring aktivieren

Merksatz:

VPN-Gateway von außen erreichbar,
LAN-Zugriff danach streng regeln.

VPN und Patchmanagement

VPN-Systeme müssen aktuell gehalten werden.

Wichtig:

VPN-Gateway patchen
VPN-Client aktualisieren
Betriebssystem aktualisieren
Bibliotheken aktualisieren
alte Protokolle deaktivieren
bekannte Schwachstellen beachten

Merksatz:

> VPN-Systeme sind internetnah und müssen aktuell bleiben.

VPN und Hardening

Hardening bedeutet:

> System sicher konfigurieren und unnötige Angriffsfläche reduzieren.

Beim VPN:

> nur notwendige Protokolle aktivieren
> starke Kryptografie
> alte Verfahren deaktivieren
> Adminzugänge begrenzen
> Logs aktivieren
> MFA erzwingen
> Standardkonten entfernen
> sichere TLS-Konfiguration
> regelmäßige Prüfung

Merksatz:

> Hardening verringert die Angriffsfläche.

VPN und Backup der Konfiguration

VPN-Konfigurationen sollten gesichert werden.

Warum?

> Wiederherstellung nach Ausfall
> Fehlkonfiguration rückgängig machen
> Migration
> Vergleich nach Änderungen
> Disaster Recovery

Wichtig:

```
Backups sicher speichern,
weil sie sensible Informationen enthalten können.
```

Merksatz:

```
VPN-Konfigurationsbackup sicher aufbewahren.
```

VPN und Änderungsmanagement

VPN-Änderungen sollten kontrolliert durchgeführt werden.

Beispiele für Änderungen:

```
neue Firewall-Regel
neue VPN-Gruppe
neuer Dienstleisterzugang
Zertifikat erneuern
Protokoll wechseln
Gateway aktualisieren
neue Route hinzufügen
```

Wichtig:

```
Zweck dokumentieren
Test durchführen
Rollback planen
Verantwortlichen nennen
Ticket oder Änderungsnachweis erfassen
```

Merksatz:

```
VPN-Änderungen brauchen Dokumentation und Rückweg.
```

Typische VPN-Sicherheitsfehler

Häufige Fehler:

- VPN ohne MFA
- gemeinsame Konten
- zu breite Firewall-Regeln
- VPN → LAN any allow
- Adminzugriff ohne Trennung
- Dienstleisterzugang dauerhaft aktiv
- alte VPN-Protokolle
- schwache PSKs
- fehlende Logs
- keine Alarmierung
- unsichere Endgeräte
- keine Zertifikatsprüfung
- veraltete VPN-Gateways
- fehlendes Offboarding

Merksatz:

Die meisten VPN-Risiken entstehen durch zu breite oder schlecht kontrollierte Zugriffe.

Sichere VPN-Grundregeln

1. MFA aktivieren.
2. Eigene Konten pro Benutzer nutzen.
3. Keine Sammelkonten verwenden.
4. Rollenmodell erstellen.
5. VPN-Zonen nutzen.
6. Firewall-Regeln eng setzen.
7. Dienstleisterzugriffe zeitlich begrenzen.
8. Adminzugänge trennen.
9. Geräte prüfen.
10. Logs und Monitoring aktivieren.
11. Alte Protokolle deaktivieren.
12. Zertifikate verwalten.
13. Offboarding durchführen.
14. Änderungen dokumentieren.

Merksatz:

VPN-Sicherheit entsteht durch Technik,
Prozesse
und klare Rechte.

Typische IHK-Fragen

In AP1 und AP2 kann zum Beispiel gefragt werden:

- Warum ist VPN allein kein vollständiges Sicherheitskonzept?
- Warum sollte VPN mit MFA abgesichert werden?
- Was ist der Unterschied zwischen Authentifizierung und Autorisierung?
- Warum sind Sammelkonten problematisch?
- Warum sollte VPN-Zugriff nach Rollen begrenzt werden?
- Was bedeutet Least Privilege beim VPN?
- Warum sind Dienstleisterzugänge besonders kritisch?
- Was ist ein Bastion Host?
- Was ist ein Jump Server?
- Warum ist Gerätesicherheit beim VPN wichtig?
- Was ist ein Posture Check?
- Warum sind VPN-Logs wichtig?
- Welche Ereignisse sollten bei VPN alarmiert werden?
- Warum muss ein VPN-Gateway gepatcht werden?
- Welche typischen VPN-Sicherheitsfehler gibt es?

Typische Prüfungsfallen

VPN ist nicht automatisch sicher,
nur weil es verschlüsselt.

VPN schützt den Tunnel,
aber nicht automatisch alle Zielsysteme.

VPN ersetzt keine Firewall-Regeln.

VPN ersetzt keine Benutzerrechte.

VPN ohne MFA ist riskant.

Authentifizierung ist nicht Autorisierung.

VPN verbunden heißt nicht:
alles erlaubt.

Sammelkonten sind schlecht nachvollziehbar.

Dienstleisterzugänge zeitlich begrenzen.

Adminzugänge getrennt behandeln.

Managementnetz besonders schützen.

BYOD braucht klare Regeln.

Unsichere Endgeräte sind Risiko.

Zertifikate brauchen Verwaltung und Widerruf.

VPN-Logs sind sicherheitsrelevant.

Monitoring erkennt ungewöhnliche Zugriffe.

Patchmanagement für VPN-Gateways ist kritisch.

Alte VPN-Protokolle vermeiden.

Least Privilege gilt auch im VPN.

Zero Trust kann breiten VPN-Zugriff reduzieren.

Wichtige Begriffe kurz erklärt

Begriff	Kurze Erklärung
Authentifizierung	Identität prüfen
Autorisierung	Rechte prüfen
MFA	Multi-Faktor-Authentifizierung

Begriff	Kurze Erklärung
Clientzertifikat	Zertifikat für Benutzer oder Gerät
Serverzertifikat	Zertifikat des VPN-Gateways
Zertifikatswiderruf	Zertifikat für ungültig erklären
CRL	Zertifikatsperrliste
OCSP	Online-Prüfung von Zertifikatsstatus
Benutzergruppe	Gruppe zur Rechtevergabe
Rollenmodell	Zuordnung von Rollen zu Zugriffsrechten
Least Privilege	nur notwendige Rechte
Need to Know	Zugriff nur bei Bedarf
Zero Trust	kein automatisches Vertrauen
laterale Bewegung	Ausbreitung im internen Netz
Segmentierung	Trennung von Netzbereichen
VPN-Zone	eigene Sicherheitszone für VPN
BYOD	private Geräte im Unternehmenseinsatz
Managed Device	verwaltetes Gerät
Posture Check	Prüfung des Gerätezustands
Bastion Host	gehärteter Zwischenserver
Jump Server	Sprungserver für Adminzugriffe
Hardening	sichere Systemkonfiguration
Offboarding	Entfernen nicht mehr nötiger Zugriffe
Sammelkonto	gemeinsam genutztes Benutzerkonto

IHK-sichere Kurzformulierung

Ein VPN stellt einen geschützten Tunnel bereit, ist aber allein kein vollständiges Sicherheitskonzept. VPN-Zugriffe müssen durch starke Authentifizierung, möglichst MFA, Zertifikate, Benutzergruppen, Rollenmodelle, Firewall-Regeln, Least Privilege, Gerätesicherheit, Logging und Monitoring abgesichert werden. Authentifizierung prüft die Identität eines Benutzers oder Geräts, während Autorisierung festlegt, welche Ressourcen genutzt werden dürfen. Externe Dienstleister und Administratoren benötigen besonders streng begrenzte und nachvollziehbare Zugänge. Sammelkonten, pauschale LAN-Freigaben, fehlende MFA, veraltete VPN-Protokolle und unsichere Endgeräte sind typische Sicherheitsrisiken.

Merksätze

VPN ist ein Zugang ins Netz.

VPN allein ist kein vollständiges Sicherheitskonzept.

VPN schützt den Tunnel,
nicht automatisch alle Ziele.

Authentifizierung = Wer bist du?

Autorisierung = Was darfst du?

MFA schützt VPN-Zugänge deutlich besser.

MFA ist wichtig,
aber nicht unfehlbar.

Zertifikate binden Zugriff an Identität oder Gerät.

Privater Schlüssel muss geschützt werden.

Zertifikate müssen widerrufen werden können.

Gruppen steuern VPN-Zugriff.

Rollenmodell verhindert Pauschalfreigaben.

Least Privilege gilt auch im VPN.

Need to Know begrenzt Informationszugriff.

Zero Trust vertraut nicht automatisch.

Laterale Bewegung verhindern.

Segmentierung begrenzt Schäden.

VPN-Zonen trennen Zugriffe.

Admin-VPN besonders schützen.

Dienstleister-VPN zeitlich begrenzen.

Sammelkonten vermeiden.

Offboarding konsequent durchführen.

Unsichere Endgeräte sind Risiko.

BYOD braucht klare Regeln.

Posture Check prüft Gerätesicherheit.

Malware auf VPN-Client gefährdet interne Systeme.

VPN-Logins überwachen.

Auffällige VPN-Ereignisse alarmieren.

Bastion Host bündelt Adminzugriffe.

Managementnetz niemals breit freigeben.

VPN-Gateway patchen.

Hardening reduziert Angriffsfläche.

VPN-Änderungen dokumentieren.