17.1 Praxis – Netzwerkadministration und Systemzugriff

In der Netzwerkadministration geht es darum, IT-Systeme, Netzwerke, Benutzer, Dienste und Zugriffe sicher zu verwalten.

Dabei werden technische Werkzeuge, Berechtigungen, Protokolle und Sicherheitsregeln kombiniert.

Typische Aufgaben sind:

```
- Systeme administrieren
- Netzwerkfehler suchen
- Benutzerrechte verwalten
- Remotezugriffe einrichten
- Dienste prüfen
- Logs auswerten
- Konfigurationen dokumentieren
- Sicherheitsregeln kontrollieren
- Backups prüfen
- Updates einspielen
```

Merksatz:

```
Netzwerkadministration ist die praktische Verwaltung von Systemen,
Diensten,
Zugriffen
und Verbindungen.
```

Warum Systemzugriff wichtig ist

Administratoren brauchen Zugriff auf Systeme, um sie zu verwalten.

Gleichzeitig sind Adminzugänge besonders kritisch.

Ein kompromittierter Adminzugang kann ermöglichen:

```
Serverübernahme
Datenzugriff
```

Rechteänderungen
Firewalländerungen
Löschen von Backups
Manipulation von Logs
Installation von Malware
Zugriff auf weitere Systeme

Merksatz:

Adminzugänge sind mächtig
und müssen besonders geschützt werden.

Typische Verwaltungszugriffe

Typische Arten des Systemzugriffs:

SSH
RDP
Weboberfläche
Konsole
VPN
Remote-Support-Tool
Managementnetz
API
Cloud-Portal
Verzeichnisdienst

Merksatz:

Je mächtiger der Zugriff,
desto stärker muss er abgesichert werden.

Lokaler Zugriff

Lokaler Zugriff bedeutet:

Administrator arbeitet direkt am Gerät
oder an einer lokalen Konsole.

Beispiele:

Serverkonsole
Monitor und Tastatur am Gerät
lokale Anmeldung am Notebook
lokale Shell
physische Konsole im Serverraum

Vorteil:

funktioniert oft auch,
wenn Netzwerkdienste gestört sind

Nachteil:

physischer Zugang nötig

Merksatz:

Lokaler Zugriff ist direkter Zugriff am System.

Remotezugriff

Remotezugriff bedeutet:

Ein System wird aus der Ferne administriert.

Beispiele:

SSH auf Linux-Server
RDP auf Windows-Server
Weboberfläche eines Routers
VPN ins Firmennetz

Cloud-Konsole
Remote-Support-Sitzung

Merksatz:

Remotezugriff ermöglicht Verwaltung ohne direkten physischen Zugang.

Remotezugriff als Risiko

Remotezugänge sind attraktive Ziele für Angreifer.

Risiken:

Brute Force
Passwortdiebstahl
Phishing
unsichere Ports
ungepatchte Dienste
fehlende MFA
zu breite Firewall-Regeln
veraltete Remote-Software
öffentlich erreichbare Adminoberflächen

Merksatz:

Remotezugänge niemals unnötig offen ins Internet stellen.

Sichere Grundregeln für Remotezugriff

Wichtige Regeln:

nur notwendige Remotezugänge erlauben
MFA nutzen
starke Authentifizierung verwenden
Zugriff über VPN oder Bastion Host
Adminports nicht breit öffentlich öffnen
Quell-IP einschränken
Logging aktivieren

Benutzer eindeutig zuordnen
keine Sammelkonten nutzen
Rechte minimal vergeben
Zugriffe regelmäßig prüfen

Merksatz:

Remotezugriff braucht Authentifizierung,
Zugriffsbeschränkung
Logging
und Rechtebegrenzung.

SSH

SSH steht für:

Secure Shell

SSH wird vor allem genutzt, um Linux-, Unix- oder Netzwerkgeräte sicher aus der Ferne zu verwalten.

SSH ermöglicht:

verschlüsselte Kommandozeile
sichere Anmeldung
Dateiübertragung je nach Werkzeug
Tunnelung
Verwaltung von Servern
Verwaltung von Netzwerkgeräten

Merksatz:

SSH ist ein verschlüsselter Fernzugriff auf die Kommandozeile.

SSH-Port

Der Standardport für SSH ist:

```
TCP 22
```

Wichtig:

```
Ein offener SSH-Port im Internet ist ein häufiges Angriffsziel.
```

Schutzmaßnahmen:

```
Zugriff per VPN
Zugriff über Bastion Host
Quell-IP begrenzen
Schlüssel statt Passwort nutzen
MFA je nach Umgebung
Loginversuche begrenzen
Logs überwachen
```

Merksatz:

```
SSH ist sicher verschlüsselt,
aber der Zugang muss trotzdem geschützt werden.
```

SSH mit Passwort

SSH kann mit Benutzername und Passwort genutzt werden.

Risiko:

```
Passwörter können erraten,
gestohlen
oder wiederverwendet werden.
```

Schutz:

```
starke Passwörter
MFA
Rate Limiting
Fail2ban oder vergleichbare Schutzmechanismen
```

```
keine Standardkonten
keine Root-Anmeldung direkt
```

Merksatz:

```
SSH-Passwortlogin ist möglich,
aber stärker angreifbar als Schlüsselanmeldung.
```

SSH mit Schlüssel

Bei SSH-Schlüsseln wird ein Schlüsselpaar verwendet.

Es besteht aus:

```
privatem Schlüssel

und

öffentlichem Schlüssel
```

Der öffentliche Schlüssel liegt auf dem Server.

Der private Schlüssel bleibt beim Benutzer.

Merksatz:

```
SSH-Schlüssel bestehen aus privatem und öffentlichem Schlüssel.
```

Privater SSH-Schlüssel

Der private Schlüssel ist geheim.

Er darf nicht:

```
weitergegeben werden
öffentlich gespeichert werden
in Repositories liegen
in Tickets kopiert werden
in Chatnachrichten stehen
```

unverschlüsselt auf fremden Geräten liegen

Merksatz:

Der private SSH-Schlüssel ist wie ein sehr starkes Passwort zu behandeln.

Öffentlicher SSH-Schlüssel

Der öffentliche Schlüssel darf auf Servern hinterlegt werden.

Er ermöglicht, dass sich der passende private Schlüssel authentifizieren kann.

Wichtig:

öffentlicher Schlüssel ist nicht geheim,
aber seine Zuordnung muss korrekt verwaltet werden.

Merksatz:

Öffentlicher Schlüssel auf Server,
privater Schlüssel beim Benutzer.

SSH-Schlüssel und Passphrase

Ein privater SSH-Schlüssel sollte mit einer Passphrase geschützt werden.

Vorteil:

Wenn der Schlüssel gestohlen wird,
kann er nicht sofort ohne Passphrase genutzt werden.

Merksatz:

SSH-Schlüssel zusätzlich mit Passphrase schützen.

Root-Login über SSH

Direkter Root-Login über SSH ist riskant.

Besser:

```
normaler Benutzer meldet sich an

danach

Rechteerhöhung mit sudo
```

Vorteile:

```
bessere Nachvollziehbarkeit
weniger direkte Angriffsfläche
Benutzeraktionen besser zuordenbar
```

Merksatz:

```
Direkten Root-Login vermeiden.
```

---

sudo

sudo erlaubt, einzelne Befehle mit erhöhten Rechten auszuführen.

Vorteile:

```
normale Anmeldung ohne dauerhafte Adminrechte
gezielte Rechtevergabe
bessere Protokollierung
weniger Risiko als dauerhafte Root-Sitzung
```

Merksatz:

```
sudo ermöglicht kontrollierte Rechteerhöhung.
```

RDP

RDP steht für:

```
Remote Desktop Protocol
```

RDP wird häufig genutzt, um Windows-Systeme grafisch aus der Ferne zu verwalten.

Der Standardport ist:

```
TCP 3389
```

Merksatz:

```
RDP ist grafischer Remotezugriff auf Windows-Systeme.
```

RDP als Risiko

RDP ist ein häufiges Angriffsziel, wenn es direkt aus dem Internet erreichbar ist.

Risiken:

```
Brute Force
Credential Stuffing
Exploits gegen ungepatchte Dienste
Ransomware-Einstieg
gestohlene Zugangsdaten
fehlende MFA
```

Merksatz:

```
RDP sollte nicht direkt und breit aus dem Internet erreichbar sein.
```

RDP sicher nutzen

Schutzmaßnahmen:

```
RDP nur über VPN
RDP Gateway verwenden
MFA nutzen
Quell-IP einschränken
```

starke Passwörter
Account Lockout
Network Level Authentication
Updates einspielen
Logs überwachen
Adminrechte begrenzen

Merksatz:

RDP über VPN oder Gateway absichern.

Weboberflächen

Viele Systeme werden über Weboberflächen verwaltet.

Beispiele:

Router
Firewalls
Switches
NAS
Drucker
Hypervisor
Cloud-Portale
Monitoring-Systeme
Backup-Systeme

Risiken:

Standardpasswörter
fehlende Updates
unsichere TLS-Konfiguration
öffentliche Erreichbarkeit
schwache Rechteverwaltung
fehlende MFA

Merksatz:

Admin-Weboberflächen gehören nicht ungeschützt ins Internet.

Weboberflächen sicher betreiben

Maßnahmen:

nur intern oder über VPN erreichbar machen
starke Passwörter
MFA wenn möglich
HTTPS nutzen
Zertifikate prüfen
Standardkonten deaktivieren
Updates einspielen
Zugriff protokollieren
Rollen und Rechte begrenzen

Merksatz:

Webadministration braucht Zugriffsschutz,
Verschlüsselung
und Updates.

VPN für Administration

VPN ermöglicht, dass Administratoren sicher in ein internes Netz gelangen.

Vorteile:

Adminports müssen nicht direkt öffentlich sein
Zugriff kann zentral gesteuert werden
MFA kann vorgeschaltet werden
interne Dienste bleiben privat
Logs können zentral ausgewertet werden

Merksatz:

```
VPN schützt Adminzugänge,
ersetzt aber keine Rechteverwaltung.
```

Bastion Host

Ein Bastion Host ist ein besonders geschützter Sprungserver.

Ablauf:

```
Administrator
verbindet sich zum Bastion Host

und von dort

zum Zielsystem
```

Vorteile:

```
weniger direkte Adminzugänge
zentrale Protokollierung
Zugriff kontrollierbarer
Zielsysteme bleiben privat
```

Merksatz:

```
Bastion Host bündelt und schützt Adminzugriffe.
```

Jump Server

Jump Server ist ein ähnlicher Begriff wie Bastion Host.

Er dient als Zwischensystem, um interne Systeme zu administrieren.

Wichtig:

```
stark härten
MFA nutzen
Zugriff protokollieren
```

```
Benutzer eindeutig zuordnen
keine unnötigen Tools installieren
regelmäßig patchen
```

Merksatz:

```
Jump Server ist ein kontrollierter Sprungpunkt für Administration.
```

Managementnetz

Ein Managementnetz ist ein eigenes Netz für administrative Zugriffe.

Darin liegen zum Beispiel:

```
Verwaltungsinterfaces
Hypervisor-Management
Switch-Management
Firewall-Management
Server-Management
Backup-Management
Storage-Management
```

Ziel:

```
Managementzugriffe vom normalen Benutzernetz trennen.
```

Merksatz:

```
Managementzugänge gehören in ein getrenntes Managementnetz.
```

Warum Managementnetz wichtig ist

Wenn Managementschnittstellen im normalen Clientnetz erreichbar sind, können kompromittierte Clients leichter Adminsysteme angreifen.

Ein getrenntes Managementnetz reduziert:

Angriffsfläche
laterale Bewegung
unkontrollierte Zugriffe
Risiko durch Malware
versehentliche Änderungen

Merksatz:

Managementnetz schützt besonders kritische Verwaltungszugänge.

Out-of-Band-Management

Out-of-Band-Management bedeutet:

Verwaltung erfolgt über einen getrennten Verwaltungsweg,
unabhängig vom normalen Produktionsnetz.

Beispiele:

iLO
iDRAC
IPMI
serielle Konsole
separates Managementinterface

Vorteil:

Zugriff auch bei Störung des normalen Systems möglich

Risiko:

sehr mächtiger Zugriff,
deshalb besonders schützen

Merksatz:

Out-of-Band-Management ist mächtig und muss streng abgesichert werden.

Benutzerkonten

Benutzerkonten sind Grundlage für Zugriff.

Wichtige Regeln:

persönliches Konto pro Benutzer
keine Sammelkonten
starke Passwörter
MFA bei kritischen Zugängen
Rollen und Gruppen nutzen
Rechte regelmäßig prüfen
Konten bei Austritt deaktivieren
Admin- und Benutzerkonto trennen

Merksatz:

Zugriffe müssen eindeutig Personen zugeordnet werden können.

Sammelkonten

Sammelkonten sind Konten, die mehrere Personen gemeinsam nutzen.

Problem:

keine eindeutige Nachvollziehbarkeit
Passwortweitergabe
schwieriges Offboarding
schlechte Protokollierung
höheres Missbrauchsrisiko

Merksatz:

Sammelkonten vermeiden,
besonders bei Administrationszugängen.

Admin- und Benutzerkonto trennen

Administratoren sollten nicht ständig mit Adminrechten arbeiten.

Besser:

```
normales Benutzerkonto für Alltag

separates Adminkonto für Administration
```

Vorteile:

```
weniger Schaden durch Phishing
weniger Malware-Risiko
bessere Kontrolle
klarere Protokollierung
```

Merksatz:

```
Adminrechte nur verwenden,
wenn sie wirklich benötigt werden.
```

Least Privilege in der Administration

Least Privilege bedeutet:

```
nur notwendige Rechte vergeben.
```

Beispiele:

```
Helpdesk darf Passwörter zurücksetzen,
aber keine Server löschen.

Datenbankadmin darf Datenbank verwalten,
aber keine Firewall ändern.

Netzwerkadmin darf Switches verwalten,
aber keine Personalakten lesen.
```

Merksatz:

```
Adminrechte nach Aufgabe trennen.
```

Rollenbasierte Rechtevergabe

Rollenbasierte Rechtevergabe bedeutet:

```
Rechte werden über Rollen oder Gruppen vergeben.
```

Beispiele:

```
Helpdesk
Serveradministration
Netzwerkadministration
Datenbankadministration
Backup-Operator
Sicherheitsadministrator
Leser
```

Vorteile:

```
übersichtlicher
leichter zu prüfen
einfacher beim Onboarding und Offboarding
```

Merksatz:

```
Rollen vereinfachen Berechtigungsverwaltung.
```

Privileged Access Management

Privileged Access Management wird oft abgekürzt:

```
PAM
```

PAM kontrolliert besonders mächtige Zugriffe.

Funktionen können sein:

```
zeitlich begrenzte Adminrechte
Genehmigungspflicht
MFA
Sitzungsaufzeichnung
Passworttresor
Protokollierung
Notfallzugriff
```

Merksatz:

```
PAM schützt besonders kritische Adminrechte.
```

Just-in-Time-Administration

Just-in-Time-Administration bedeutet:

```
Adminrechte werden nur für einen begrenzten Zeitraum aktiviert.
```

Beispiel:

```
Admin erhält für 1 Stunde Rechte zur Wartung.
```

Danach werden Rechte automatisch entzogen.

Merksatz:

```
Just-in-Time reduziert dauerhafte Adminrechte.
```

Protokollierung von Adminzugriffen

Adminaktionen sollten protokolliert werden.

Wichtige Informationen:

```
Benutzer
Zeitpunkt
Quellsystem
Zielsystem
ausgeführte Aktion
Erfolg oder Fehler
geänderte Konfiguration
verwendetes Konto
```

Merksatz:

```
Adminzugriffe müssen nachvollziehbar sein.
```

Audit-Logs

Audit-Logs dokumentieren sicherheitsrelevante Aktionen.

Beispiele:

```
Benutzer angelegt
Rolle geändert
Firewall-Regel geändert
Dienst gestoppt
Backup gelöscht
Schlüssel erstellt
Adminrechte vergeben
Systemkonfiguration verändert
```

Merksatz:

```
Audit-Logs zeigen,
wer was wann geändert hat.
```

Logschutz

Logs müssen geschützt werden, weil Angreifer sie manipulieren oder löschen könnten.

Maßnahmen:

zentrale Logsammlung
eingeschränkte Schreibrechte
getrennte Speicherung
unveränderliche Logs je nach Bedarf
Zeitstempel
Zugriffskontrolle
regelmäßige Prüfung

Merksatz:

Logs sind nur wertvoll,
wenn sie vollständig und vertrauenswürdig sind.

Zeitserver und Logs

Für Logauswertung müssen Systeme die gleiche Zeitbasis haben.

Dafür wird NTP genutzt.

Wenn Zeiten stark abweichen, wird die Analyse schwieriger.

Beispiel:

Firewall-Log,
Server-Log
und Authentifizierungslog
passen zeitlich nicht zusammen.

Merksatz:

Saubere Zeit synchronisation ist wichtig für Loganalyse.

Dokumentation in der Administration

Dokumentiert werden sollten:

Systeme
IP-Adressen

Hostnamen
Zuständigkeiten
Zugangskonzepte
Rollen
Firewall-Regeln
Dienste
Abhängigkeiten
Backup-Regeln
Wartungsfenster
Änderungen
Notfallzugriffe

Merksatz:

Gute Dokumentation macht Administration nachvollziehbar und wartbar.

Change Management

Change Management bedeutet:

Änderungen werden geplant,
geprüft,
freigegeben,
umgesetzt
und dokumentiert.

Beispiele:

Firewall-Regel ändern
Benutzerrechte erweitern
Serverdienst aktualisieren
VPN-Gruppe anlegen
Zertifikat erneuern
Backup-Plan ändern
Switch-Konfiguration anpassen

Merksatz:

Änderungen brauchen Kontrolle und Dokumentation.

Vier-Augen-Prinzip

Vier-Augen-Prinzip bedeutet:

kritische Aktionen werden von mindestens zwei Personen geprüft oder freigegeben.

Beispiele:

Adminrechte vergeben
Backup löschen
Firewall ins Internet öffnen
Produktivsystem ändern
Daten exportieren
Notfallzugang aktivieren

Merksatz:

Vier-Augen-Prinzip reduziert Fehler und Missbrauch.

Offboarding

Offboarding bedeutet:

Zugriffe werden entfernt,
wenn eine Person das Unternehmen verlässt
oder eine Rolle wechselt.

Zu prüfen:

Benutzerkonto
Gruppenmitgliedschaften
VPN-Zugang
SSH-Schlüssel
Cloud-Zugänge

lokale Adminrechte
API-Schlüssel
geteilte Freigaben
Geräte
E-Mail-Weiterleitungen

Merksatz:

Nicht entfernte Zugänge sind ein Sicherheitsrisiko.

Onboarding

Onboarding bedeutet:

neue Benutzer erhalten benötigte Zugänge.

Wichtig:

nach Rolle vergeben
nur notwendige Rechte
dokumentieren
MFA einrichten
Schulung durchführen
Verantwortlichkeiten klären

Merksatz:

Onboarding sollte geordnet über Rollen und Prozesse laufen.

Break-Glass-Konto

Ein Break-Glass-Konto ist ein Notfallkonto.

Es wird genutzt, wenn normale Adminwege nicht funktionieren.

Beispiele:

Identitätsdienst gestört
MFA-System ausgefallen
zentrale Anmeldung nicht möglich
Administratoren ausgesperrt

Wichtig:

stark schützen
selten nutzen
Nutzung protokollieren
regelmäßig prüfen
Zugriff begrenzen
Notfallprozess dokumentieren

Merksatz:

Break-Glass-Konto ist Notfallzugang,
kein Alltagskonto.

Sichere Administrationsregeln

Wichtige Regeln:

keine Adminarbeit mit Alltagskonto
keine Sammelkonten
MFA für Adminzugänge
Remotezugriff nur kontrolliert
Adminports nicht offen ins Internet
Zugriffe protokollieren
Rechte regelmäßig prüfen
Änderungen dokumentieren
Notfallzugänge absichern
Offboarding ernst nehmen

Merksatz:

Administration braucht technische und organisatorische Kontrolle.

Typische Praxisfehler

Häufige Fehler:

```
RDP offen im Internet
SSH mit Passwort und schwachem Passwort
Standardpasswort auf Weboberfläche
gleiche Adminzugänge für mehrere Personen
keine MFA
alte Benutzerkonten aktiv
Adminrechte dauerhaft vergeben
keine Logs
keine Dokumentation
Managementinterfaces im Clientnetz
Backups ohne Zugriffsschutz
Notfallkonto ungeprüft
```

Merksatz:

```
Viele Sicherheitsprobleme entstehen durch bequeme,
aber unsichere Administration.
```

Typische IHK-Fragen

In AP1 und AP2 kann zum Beispiel gefragt werden:

```
- Was ist Remotezugriff?
- Was ist SSH?
- Wofür wird SSH genutzt?
- Was ist der Standardport von SSH?
- Warum ist SSH mit Schlüsseln sicherer als nur Passwort?
- Was ist RDP?
- Was ist der Standardport von RDP?
- Warum sollte RDP nicht offen im Internet stehen?
- Was ist ein Bastion Host?
- Was ist ein Jump Server?
- Was ist ein Managementnetz?
- Was bedeutet Out-of-Band-Management?
```

- Warum sollten Admin- und Benutzerkonto getrennt werden?
- Warum sind Sammelkonten problematisch?
- Was bedeutet Least Privilege?
- Was ist PAM?
- Was bedeutet Just-in-Time-Administration?
- Warum sind Audit-Logs wichtig?
- Warum ist NTP für Logs wichtig?
- Was ist ein Break-Glass-Konto?
- Was ist Offboarding?

Typische Prüfungsfallen

Remotezugriff ist praktisch,
aber sicherheitskritisch.

SSH ist verschlüsselt,
aber trotzdem angreifbar,
wenn Zugang schlecht geschützt ist.

SSH-Standardport ist TCP 22.

RDP-Standardport ist TCP 3389.

RDP nicht breit öffentlich freigeben.

Admin-Weboberflächen nicht öffentlich bereitstellen.

VPN schützt Transport,
ersetzt aber keine Rechteverwaltung.

Bastion Host ist ein Sprungserver.

Managementnetz vom Clientnetz trennen.

Out-of-Band-Management besonders schützen.

Sammelkonten vermeiden.

Admin- und Alltagskonto trennen.

Least Privilege gilt auch für Administratoren.

PAM schützt privilegierte Zugriffe.

Just-in-Time reduziert dauerhafte Adminrechte.

Audit-Logs müssen vor dem Vorfall aktiv sein.

Logs brauchen korrekte Zeitbasis.

NTP hilft bei zeitlich korrekter Loganalyse.

Offboarding muss alle Zugänge entfernen.

Break-Glass-Konto ist Notfallzugang,
kein normales Admin-Konto.

Wichtige Begriffe kurz erklärt

Begriff	Kurze Erklärung
Netzwerkadministration	Verwaltung von Netzwerken und Systemen
Systemzugriff	Zugriff auf IT-Systeme zur Nutzung oder Verwaltung
lokaler Zugriff	direkter Zugriff am Gerät
Remotezugriff	Zugriff aus der Ferne
SSH	verschlüsselter Kommandozeilenzugriff
privater Schlüssel	geheimer Teil eines SSH-Schlüsselpaares
öffentlicher Schlüssel	Teil des Schlüsselpaares auf dem Server
sudo	kontrollierte Rechteerhöhung
RDP	grafischer Remotezugriff auf Windows-Systeme
Weboberfläche	Verwaltung über Browser
VPN	verschlüsselter Zugang zu internem Netz
Bastion Host	besonders geschützter Sprungserver
Jump Server	Zwischensystem für Administration
Managementnetz	getrenntes Netz für Verwaltung
Out-of-Band-Management	Verwaltung über getrennten Verwaltungsweg

Begriff	Kurze Erklärung
Benutzerkonto	persönliche Identität im System
Sammelkonto	gemeinsam genutztes Konto
Adminkonto	Konto mit erhöhten Rechten
Least Privilege	minimale notwendige Rechte
Rollenmodell	Rechtevergabe über Rollen
PAM	Privileged Access Management
Just-in-Time	zeitlich begrenzte Rechte
Audit-Log	Protokoll sicherheitsrelevanter Aktionen
Logschutz	Schutz vor Manipulation oder Verlust von Logs
NTP	Zeitsynchronisation
Dokumentation	nachvollziehbare Beschreibung von Systemen und Änderungen
Change Management	kontrollierter Änderungsprozess
Vier-Augen-Prinzip	Prüfung durch mindestens zwei Personen
Offboarding	Entfernen nicht mehr benötigter Zugänge
Onboarding	geordnete Vergabe neuer Zugänge
Break-Glass-Konto	Notfallkonto

IHK-sichere Kurzformulierung

Netzwerkadministration umfasst die praktische Verwaltung von Systemen, Diensten, Netzwerken und Zugängen. Remotezugriffe wie SSH, RDP, Weboberflächen, VPN, Bastion Hosts oder Managementnetze ermöglichen Administration aus der Ferne, sind aber sicherheitskritisch. SSH dient dem verschlüsselten Kommandozeilenzugriff, RDP dem grafischen Fernzugriff auf Windows-Systeme. Adminzugänge sollten nicht direkt und breit aus dem Internet erreichbar sein, sondern durch VPN, Bastion Host, MFA, Quell-IP-Beschränkung, Logging und Least Privilege abgesichert werden. Persönliche Benutzerkonten, getrennte Admin- und Alltagskonten, Audit-Logs, Change Management, Offboarding und geschützte Notfallkonten sind wichtige Grundlagen sicherer Administration.

Merksätze

```
Netzwerkadministration verwaltet Systeme,
Dienste,
Zugriffe
und Verbindungen.
```

Adminzugänge sind besonders kritisch.

Remotezugriff braucht starke Absicherung.

SSH = verschlüsselter Kommandozeilenzugriff.

SSH nutzt standardmäßig TCP 22.

Privater SSH-Schlüssel bleibt geheim.

Öffentlicher SSH-Schlüssel liegt auf dem Server.

SSH-Schlüssel mit Passphrase schützen.

Direkten Root-Login vermeiden.

sudo kontrolliert Rechteerhöhung.

RDP = grafischer Windows-Remotezugriff.

RDP nutzt standardmäßig TCP 3389.

RDP nicht breit ins Internet öffnen.

Admin-Weboberflächen intern oder über VPN bereitstellen.

VPN schützt Zugang,
ersetzt aber keine Rechteverwaltung.

Bastion Host ist ein geschützter Sprungserver.

Jump Server ist ein Zwischensystem für Administration.

Managementnetz vom normalen Clientnetz trennen.

Out-of-Band-Management besonders schützen.

Persönliche Konten statt Sammelkonten.

Admin- und Alltagskonto trennen.

Least Privilege gilt auch für Admins.

Rollen vereinfachen Rechtevergabe.

PAM schützt privilegierte Zugriffe.

Just-in-Time reduziert dauerhafte Adminrechte.

Adminaktionen protokollieren.

Audit-Logs zeigen sicherheitsrelevante Änderungen.

Logs vor Manipulation schützen.

NTP ist wichtig für Loganalyse.

Dokumentation ist Teil sicherer Administration.

Änderungen kontrolliert durchführen.

Vier-Augen-Prinzip bei kritischen Aktionen nutzen.

Offboarding entfernt alte Zugänge.

Break-Glass-Konto ist nur für Notfälle.

Sichere Administration braucht Technik,
Prozesse
und Nachvollziehbarkeit.