17.8 Dokumentation, Change Management und sichere Administration in der Praxis

Dokumentation und Change Management sorgen dafür, dass IT-Systeme nachvollziehbar, wartbar und sicher betrieben werden können.

In der Praxis reicht es nicht, dass ein System irgendwie funktioniert.

Wichtig ist auch:

```
- Was wurde eingerichtet?
- Warum wurde es eingerichtet?
- Wer ist verantwortlich?
- Welche Abhängigkeiten gibt es?
- Welche Zugangsdaten oder Rollen werden benötigt?
- Welche Änderungen wurden durchgeführt?
- Wie kann ein Fehler behoben werden?
- Wie kann das System wiederhergestellt werden?
```

Merksatz:

```
Gute Administration ist nicht nur Technik,
sondern auch Nachvollziehbarkeit.
```

Warum Dokumentation wichtig ist

Ohne Dokumentation entstehen viele Probleme.

Beispiele:

```
niemand kennt die IP-Adresse eines Servers
Firewall-Regeln sind unverständlich
Passwörter oder Schlüssel sind unklar verwaltet
Abhängigkeiten sind unbekannt
alte Systeme werden vergessen
Fehler werden mehrfach gesucht
Vertretung ist schwierig
Notfälle dauern länger
```

Änderungen können nicht nachvollzogen werden

Merksatz:

Was nicht dokumentiert ist,
ist im Betrieb schwer kontrollierbar.

Dokumentation als Sicherheitsmaßnahme

Dokumentation ist auch eine Sicherheitsmaßnahme.

Sie hilft bei:

Rechteprüfung
Notfallmaßnahmen
Backup und Restore
Schwachstellenmanagement
Patchmanagement
Incident Response
Auditierung
Zugriffskontrolle
Change Management
Betriebssicherheit

Merksatz:

Gute Dokumentation reduziert Fehler,
Ausfallzeiten
und Sicherheitsrisiken.

Was dokumentiert werden sollte

Typische Inhalte:

Systeme
Server
Netzwerkgeräte
IP-Adressen

```
Hostnamen
Dienste
Ports
Firewall-Regeln
VLANs
Subnetze
DNS-Einträge
DHCP-Bereiche
Benutzerrollen
Gruppen
Backup-Ziele
Restore-Abläufe
Zertifikate
Lizenzen
Wartungsverträge
Verantwortliche
Notfallkontakte
```

Merksatz:

```
Dokumentiert werden sollte alles,
was für Betrieb,
Sicherheit
und Wiederherstellung wichtig ist.
```

Systemdokumentation

Eine Systemdokumentation beschreibt ein einzelnes System oder einen Dienst.

Typische Inhalte:

```
Systemname
Zweck
Standort
IP-Adresse
Betriebssystem
installierte Dienste
offene Ports
Abhängigkeiten
```

verantwortliche Person
Backup-Regel
Monitoring-Regel
Wartungsfenster
Besonderheiten
Wiederherstellungsschritte

Merksatz:

Systemdokumentation erklärt,
wofür ein System da ist
und wie es betrieben wird.

Netzwerkdokumentation

Eine Netzwerkdokumentation beschreibt Aufbau und Kommunikation im Netzwerk.

Typische Inhalte:

Netzplan
Subnetze
VLANs
Router
Switches
Firewalls
WLANs
VPNs
IP-Adressbereiche
DHCP-Bereiche
DNS-Struktur
Trunk-Ports
Access-Ports
Uplinks
WAN-Anbindungen

Merksatz:

Netzwerkdokumentation macht Verbindungen und Abhängigkeiten sichtbar.

IP-Adressdokumentation

IP-Adressen sollten nachvollziehbar verwaltet werden.

Zu dokumentieren:

```
IP-Adresse
Hostname
Gerät
Standort
Zweck
MAC-Adresse bei Bedarf
DHCP oder statisch
VLAN
Verantwortlicher
Reservierung
Datum der Änderung
```

Merksatz:

```
IP-Adressen nicht nur merken,
sondern sauber verwalten.
```

IPAM

IPAM steht für:

```
IP Address Management
```

IPAM beschreibt die strukturierte Verwaltung von IP-Adressen, Subnetzen und Zuordnungen.

Vorteile:

```
weniger IP-Konflikte
bessere Übersicht
klare Reservierungen
einfachere Fehlersuche
bessere Planung
saubere Dokumentation
```

Merksatz:

> IPAM ist geordnete IP-Adressverwaltung.

Netzplan

Ein Netzplan stellt die Netzwerkstruktur grafisch dar.

Er kann zeigen:

> Standorte
> Router
> Firewalls
> Switches
> Server
> Clients
> VLANs
> Subnetze
> DMZ
> VPN-Verbindungen
> Internetzugänge
> wichtige Dienste

Merksatz:

> Netzplan zeigt,
> wie Systeme miteinander verbunden sind.

Physischer und logischer Netzplan

Physischer Netzplan:

> zeigt Geräte,
> Kabel,
> Ports,
> Racks
> und Standorte

Logischer Netzplan:

```
zeigt VLANs,
Subnetze,
Routing,
Firewall-Zonen
und Dienste
```

Merksatz:

```
Physisch zeigt Verkabelung.
Logisch zeigt Kommunikationsstruktur.
```

Portdokumentation

Bei Switches und Netzwerkgeräten sollten Ports dokumentiert werden.

Zu dokumentieren:

```
Portnummer
angeschlossenes Gerät
VLAN
Access oder Trunk
Geschwindigkeit
PoE
Beschreibung
Patchpanel-Port
Raum oder Dose
```

Merksatz:

```
Portdokumentation spart Zeit bei Fehlersuche und Umzügen.
```

Firewall-Dokumentation

Firewall-Regeln sollten verständlich dokumentiert sein.

Wichtige Angaben:

Regelname
Zweck
Quelle
Ziel
Port
Protokoll
Richtung
Aktion
Verantwortlicher
Datum
Ablaufdatum bei temporären Regeln
Ticket oder Änderungsnummer

Merksatz:

Jede Firewall-Regel braucht einen Zweck.

Temporäre Firewall-Regeln

Temporäre Regeln sollten ein Ablaufdatum haben.

Problem ohne Ablaufdatum:

Testregel bleibt dauerhaft aktiv.
Angriffsfläche wächst.
Niemand kennt den Zweck.
Regel wird vergessen.

Merksatz:

Temporäre Regeln ohne Ablaufdatum werden oft zu dauerhaften Risiken.

DNS-Dokumentation

DNS-Einträge sollten sauber gepflegt werden.

Zu dokumentieren:

Name
IP-Adresse
Recordtyp
Zweck
Verantwortlicher
TTL
internes oder externes DNS
betroffener Dienst
Änderungsdatum

Merksatz:

DNS ist kritisch,
weil viele Dienste von Namen abhängig sind.

Zertifikatsdokumentation

Zertifikate müssen überwacht und dokumentiert werden.

Wichtige Angaben:

Domainname
Aussteller
Ablaufdatum
verwendeter Dienst
Speicherort
Erneuerungsverfahren
Verantwortlicher
automatische Erneuerung ja oder nein

Merksatz:

Abgelaufene Zertifikate verursachen vermeidbare Ausfälle.

Backup-Dokumentation

Backup-Dokumentation beschreibt, was wie gesichert wird.

Wichtige Angaben:

```
System
Datenumfang
Backup-Art
Backup-Ziel
Frequenz
Aufbewahrung
Verschlüsselung
Verantwortlicher
letzter Restore-Test
Wiederherstellungsanleitung
```

Merksatz:

```
Backup-Dokumentation muss auch den Restore beschreiben.
```

Berechtigungsdokumentation

Berechtigungen sollten nachvollziehbar dokumentiert werden.

Zu dokumentieren:

```
Rolle
Gruppe
Zweck
zugeordnete Rechte
Verantwortlicher
Genehmigungsprozess
Rezertifizierung
Kritikalität
externe Zugriffe
```

Merksatz:

```
Rechte müssen erklärbar und überprüfbar sein.
```

Betriebsdokumentation

Betriebsdokumentation beschreibt, wie ein System im Alltag betrieben wird.

Inhalte:

```
Start und Stopp
Wartung
Updates
Monitoring
Logs
Backup
typische Fehler
Eskalationswege
Ansprechpartner
Notfallmaßnahmen
```

Merksatz:

```
Betriebsdokumentation hilft beim täglichen Betrieb.
```

Runbook

Ein Runbook ist eine Schritt-für-Schritt-Anleitung für wiederkehrende Aufgaben oder Störungen.

Beispiele:

```
Dienst neu starten
Zertifikat erneuern
Backup prüfen
Speicherplatz freigeben
Benutzer entsperren
VPN-Störung prüfen
Datenbank wiederherstellen
Notfallzugang aktivieren
```

Merksatz:

```
Runbook macht Abläufe wiederholbar und nachvollziehbar.
```

Standard Operating Procedure

Standard Operating Procedure wird oft abgekürzt:

```
SOP
```

Eine SOP beschreibt einen standardisierten Ablauf.

Beispiele:

```
Benutzer anlegen
Notebook ausgeben
Server patchen
Firewall-Regel beantragen
Backup-Restore testen
Sicherheitsvorfall melden
```

Merksatz:

```
SOP = standardisierte Vorgehensweise.
```

Wissensdatenbank

Eine Wissensdatenbank sammelt wiederverwendbares Wissen.

Beispiele:

```
Fehlerlösungen
Anleitungen
Standardprozesse
häufige Fragen
Konfigurationshinweise
Netzpläne
Checklisten
Lessons Learned
```

Merksatz:

```
Wissensdatenbank verhindert,
dass Wissen nur in einzelnen Köpfen bleibt.
```

Dokumentation aktuell halten

Dokumentation ist nur hilfreich, wenn sie aktuell bleibt.

Typische Probleme:

```
Server wurde geändert,
Dokumentation nicht

IP-Adresse wurde geändert,
Liste nicht

Firewall-Regel wurde gelöscht,
Dokumentation nicht

Dienst wurde umgezogen,
Runbook nicht angepasst
```

Merksatz:

```
Veraltete Dokumentation kann gefährlicher sein als keine Dokumentation,
weil sie falsche Sicherheit gibt.
```

Dokumentationsqualität

Gute Dokumentation ist:

```
verständlich
aktuell
auffindbar
vollständig genug
nicht unnötig kompliziert
einheitlich strukturiert
versioniert
überprüfbar
```

für Vertretung nutzbar

Merksatz:

Dokumentation muss im Alltag nutzbar sein.

Change Management

Change Management bedeutet:

Änderungen werden kontrolliert geplant,
bewertet,
freigegeben,
umgesetzt,
getestet
und dokumentiert.

Typische Änderungen:

Firewall-Regel ändern
Server aktualisieren
DNS-Eintrag ändern
Zertifikat erneuern
Benutzerrechte ändern
neue Software installieren
Netzwerk umkonfigurieren
Backup-Plan ändern
Cloud-Rolle vergeben
Datenbank migrieren

Merksatz:

Change Management kontrolliert Änderungen im IT-Betrieb.

Warum Change Management wichtig ist

Unkontrollierte Änderungen führen oft zu Fehlern.

Beispiele:

```
Dienst fällt aus
Firewall blockiert Anwendung
falscher DNS-Eintrag
Benutzer verlieren Zugriff
Backup läuft nicht mehr
Sicherheitslücke entsteht
Dokumentation stimmt nicht mehr
niemand weiß,
was geändert wurde
```

Merksatz:

```
Viele Störungen entstehen durch nicht dokumentierte Änderungen.
```

Change

Ein Change ist eine geplante Änderung an einem IT-System, einem Dienst, einer Konfiguration oder einem Prozess.

Beispiele:

```
Update installieren
VLAN ändern
Server verschieben
Rechte anpassen
Zertifikat ersetzen
neue Anwendung bereitstellen
```

Merksatz:

```
Change = geplante Änderung im IT-Betrieb.
```

Standard Change

Ein Standard Change ist eine wiederkehrende, bekannte und risikoarme Änderung.

Beispiele:

```
Standardbenutzer anlegen
Drucker zuweisen
Routineupdate nach Prozess
Passwort zurücksetzen
freigegebene Standardsoftware installieren
```

Merkmale:

```
häufig durchgeführt
dokumentierter Ablauf
geringes Risiko
meist vorab genehmigt
```

Merksatz:

```
Standard Change ist bekannte Routineänderung.
```

Normal Change

Ein Normal Change ist eine geplante Änderung, die bewertet und freigegeben werden muss.

Beispiele:

```
neue Firewall-Regel
größeres Update
neue Serverrolle
Änderung an Produktivdatenbank
Netzwerkänderung
Umzug eines Dienstes
```

Merksatz:

```
Normal Change braucht Prüfung und Freigabe.
```

Emergency Change

Ein Emergency Change ist eine dringende Änderung, die schnell durchgeführt werden muss.

Beispiele:

```
kritische Sicherheitslücke schließen
Produktionsausfall beheben
kompromittierten Zugang sperren
Firewall-Regel im Angriff anpassen
defekten Dienst kurzfristig umstellen
```

Wichtig:

```
auch Emergency Changes müssen nachträglich dokumentiert werden.
```

Merksatz:

```
Emergency Change ist dringend,
aber nicht dokumentationsfrei.
```

Change Request

Ein Change Request ist ein Änderungsantrag.

Typische Inhalte:

```
Beschreibung der Änderung
Grund
betroffene Systeme
Risiko
geplanter Zeitpunkt
Verantwortlicher
Testplan
Rollback-Plan
Freigabe
Kommunikationsbedarf
```

Merksatz:

```
Change Request beschreibt,
was geändert werden soll und warum.
```

Risikobewertung bei Changes

Vor Änderungen sollte das Risiko bewertet werden.

Fragen:

```
Welche Systeme sind betroffen?
Welche Benutzer sind betroffen?
Kann es Ausfall geben?
Gibt es Sicherheitsrisiken?
Gibt es Abhängigkeiten?
Gibt es ein Backup?
Gibt es einen Rollback-Plan?
Wurde getestet?
Wann ist ein geeignetes Wartungsfenster?
```

Merksatz:

```
Änderung ohne Risikobewertung ist Blindflug.
```

Wartungsfenster

Ein Wartungsfenster ist ein geplanter Zeitraum für Änderungen.

Ziel:

```
Auswirkungen auf Benutzer reduzieren
Beteiligte informieren
Ressourcen einplanen
Rollback ermöglichen
Monitoring beobachten
```

Merksatz:

```
Wartungsfenster reduziert Betriebsrisiken bei Änderungen.
```

Rollback-Plan

Ein Rollback-Plan beschreibt, wie eine Änderung rückgängig gemacht werden kann.

Beispiele:

```
Backup zurückspielen
Snapshot zurücksetzen
alte Konfigurationsdatei wiederherstellen
alte Softwareversion installieren
DNS-Eintrag zurücksetzen
Firewall-Regel entfernen
```

Merksatz:

```
Vor Änderung wissen,
wie man zurückkommt.
```

Testplan

Ein Testplan beschreibt, wie geprüft wird, ob eine Änderung erfolgreich war.

Beispiele:

```
Dienst startet
Webseite erreichbar
Login funktioniert
Datenbank erreichbar
Backup läuft
Monitoring grün
Benutzer kann arbeiten
Logs zeigen keine Fehler
```

Merksatz:

```
Change ist erst abgeschlossen,
wenn Funktion geprüft wurde.
```

Kommunikation bei Changes

Bei Änderungen müssen betroffene Personen informiert werden.

Zu klären:

```
Wer ist betroffen?
Wann findet Änderung statt?
Welche Einschränkungen gibt es?
Wie lange dauert es?
Was ist nach der Änderung zu prüfen?
Wer ist Ansprechpartner?
Was passiert bei Problemen?
```

Merksatz:

```
Gute Kommunikation verhindert unnötige Störungen und Rückfragen.
```

Change-Freigabe

Kritische Änderungen sollten freigegeben werden.

Mögliche Freigaben durch:

```
Systemverantwortliche
IT-Leitung
Fachbereich
Sicherheitsverantwortliche
Datenschutz
Change Advisory Board je nach Organisation
```

Merksatz:

```
Kritische Änderungen nicht ungeprüft durchführen.
```

Change Advisory Board

Change Advisory Board wird oft abgekürzt:

```
CAB
```

Ein CAB bewertet und genehmigt wichtige Änderungen.

Es prüft zum Beispiel:

```
Risiko
Auswirkung
Zeitpunkt
Abhängigkeiten
Rollback
Kommunikation
Priorität
```

Merksatz:

```
CAB koordiniert wichtige Changes.
```

Configuration Management

Configuration Management bedeutet:

```
Konfigurationen von Systemen werden strukturiert verwaltet.
```

Dazu gehören:

```
Soll-Zustand
Ist-Zustand
Änderungen
Versionen
Abhängigkeiten
Dokumentation
Standardisierung
```

Merksatz:

```
Configuration Management hält technische Zustände kontrollierbar.
```

Configuration Item

Configuration Item wird oft abgekürzt:

```
CI
```

Ein CI ist ein verwaltetes Element der IT-Umgebung.

Beispiele:

```
Server
Anwendung
Datenbank
Switch
Firewall
Laptop
Dienst
Lizenz
Zertifikat
virtuelle Maschine
```

Merksatz:

```
CI = verwaltetes IT-Element.
```

CMDB

CMDB steht für:

```
Configuration Management Database
```

Eine CMDB enthält Informationen über Configuration Items und deren Beziehungen.

Beispiele:

```
Server gehört zu Anwendung
Anwendung nutzt Datenbank
Datenbank läuft auf VM
VM liegt auf Host
Dienst nutzt Zertifikat
Firewall-Regel erlaubt Zugriff
```

Merksatz:

```
CMDB zeigt Systeme und Abhängigkeiten strukturiert.
```

Asset Management

Asset Management verwaltet IT-Vermögenswerte.

Beispiele:

```
Geräte
Server
Laptops
Monitore
Smartphones
Lizenzen
Verträge
Zubehör
```

Ziel:

```
wissen,
was vorhanden ist,
wem es gehört,
wo es ist
und welchen Status es hat
```

Merksatz:

```
Asset Management verwaltet IT-Bestand.
```

Inventarisierung

Inventarisierung ist die Erfassung von IT-Objekten.

Zu erfassen:

Gerätename
Seriennummer
Standort
Benutzer
IP-Adresse
Betriebssystem
Softwarestand
Garantie
Kaufdatum
Zustand
Verantwortlicher

Merksatz:

Ohne Inventar ist Verwaltung und Sicherheit unvollständig.

Lizenzmanagement

Lizenzmanagement stellt sicher, dass Software korrekt lizenziert ist.

Zu prüfen:

Anzahl installierter Lizenzen
Anzahl gekaufter Lizenzen
Lizenzbedingungen
Laufzeiten
Abonnements
Wartungsverträge
Nutzerzuordnung
Auditfähigkeit

Merksatz:

Lizenzmanagement verhindert Unterlizenzierung,
unnötige Kosten
und Auditprobleme.

Versionierung von Konfigurationen

Konfigurationen sollten versioniert werden.

Vorteile:

- Änderungen nachvollziehen
- alte Zustände wiederherstellen
- Fehler vergleichen
- Zusammenarbeit ermöglichen
- Rollback erleichtern

Beispiele:

- Firewall-Konfiguration
- Switch-Konfiguration
- Skripte
- Webserver-Konfiguration
- Infrastrukturdefinitionen

Merksatz:

> Versionierung macht Änderungen nachvollziehbar.

Konfigurationsbackup

Viele Geräte brauchen eigene Konfigurationsbackups.

Beispiele:

- Switches
- Router
- Firewalls
- WLAN-Controller
- NAS
- Hypervisor
- Backup-Systeme

Merksatz:

```
Nicht nur Daten,
auch Konfigurationen sichern.
```

Passwort- und Secret-Dokumentation

Passwörter, Tokens und Schlüssel gehören nicht in normale Dokumentation.

Sie gehören in sichere Systeme wie:

```
Passwortmanager
Secret Manager
PAM-System
verschlüsselter Tresor
```

Dokumentation sollte nur beschreiben:

```
wo Secret verwaltet wird
wer Zugriff beantragen darf
wofür es genutzt wird
```

Merksatz:

```
Dokumentation beschreibt Secrets,
speichert sie aber nicht im Klartext.
```

Sichere Ablage von Dokumentation

Dokumentation kann selbst sensible Informationen enthalten.

Beispiele:

```
Netzpläne
IP-Adressen
Firewall-Regeln
Adminwege
Backup-Orte
Systemdetails
Notfallprozesse
```

Schutzmaßnahmen:

Zugriff begrenzen
Rollen nutzen
Versionierung
Backup
Verschlüsselung je nach Schutzbedarf
Änderungsverlauf
regelmäßige Prüfung

Merksatz:

IT-Dokumentation ist selbst schützenswert.

Lessons Learned

Lessons Learned bedeutet:

Aus Fehlern,
Störungen
und Projekten werden Verbesserungen abgeleitet.

Fragen:

Was ist passiert?
Warum ist es passiert?
Was hat gut funktioniert?
Was hat nicht funktioniert?
Welche Dokumentation fehlte?
Welche Prozesse müssen angepasst werden?
Welche technische Maßnahme fehlt?
Wie verhindern wir Wiederholung?

Merksatz:

Lessons Learned macht Erfahrungen nutzbar.

Post-Incident-Review

Ein Post-Incident-Review ist die Auswertung nach einem Vorfall.

Ziel:

```
Ursache verstehen
Reaktion bewerten
Dokumentation verbessern
Sicherheitslücken schließen
Prozesse anpassen
Wiederholung verhindern
```

Merksatz:

```
Nach einem Vorfall sollte nicht nur repariert,
sondern gelernt werden.
```

Typische Praxisfehler

Häufige Fehler:

```
keine Dokumentation
veraltete Dokumentation
IP-Adressen nur im Kopf
Firewall-Regeln ohne Zweck
temporäre Regeln ohne Ablaufdatum
keine Netzpläne
keine Restore-Anleitung
keine Verantwortlichen
Änderungen ohne Ticket
kein Rollback-Plan
keine Kommunikation
Secrets in Klartextdokumenten
Konfigurationen nicht gesichert
Lizenzen nicht geprüft
```

Merksatz:

Fehlende Dokumentation wird spätestens im Notfall teuer.

Checkliste: gute IT-Dokumentation

Systeme erfassen.
Dienste erfassen.
IP-Adressen dokumentieren.
Netzpläne pflegen.
Firewall-Regeln beschreiben.
DNS-Einträge dokumentieren.
Zertifikate überwachen.
Backup und Restore beschreiben.
Rechte und Rollen dokumentieren.
Verantwortliche benennen.
Runbooks erstellen.
Notfallkontakte pflegen.
Änderungen versionieren.
Dokumentation regelmäßig prüfen.
Zugriff auf Dokumentation absichern.

Merksatz:

Dokumentation muss aktuell,
auffindbar
und verständlich sein.

Checkliste: Change Management

Änderung beschreiben.
Grund nennen.
Betroffene Systeme bestimmen.
Risiko bewerten.
Abhängigkeiten prüfen.
Backup oder Snapshot prüfen.
Wartungsfenster festlegen.
Testplan erstellen.
Rollback-Plan erstellen.

Freigabe einholen.

Betroffene informieren.

Änderung durchführen.

Funktion testen.

Monitoring prüfen.

Dokumentation aktualisieren.

Ergebnis abschließen.

Merksatz:

Change Management begleitet die Änderung von Planung bis Abschluss.

Typische IHK-Fragen

In AP1 und AP2 kann zum Beispiel gefragt werden:

- Warum ist IT-Dokumentation wichtig?
- Was gehört in eine Systemdokumentation?
- Was gehört in eine Netzwerkdokumentation?
- Was ist ein Netzplan?
- Was ist der Unterschied zwischen physischem und logischem Netzplan?
- Was ist IPAM?
- Warum sollten Firewall-Regeln dokumentiert werden?
- Warum brauchen temporäre Regeln ein Ablaufdatum?
- Warum müssen Zertifikate dokumentiert werden?
- Was ist ein Runbook?
- Was ist eine SOP?
- Was ist Change Management?
- Was ist ein Change Request?
- Was ist ein Standard Change?
- Was ist ein Normal Change?
- Was ist ein Emergency Change?
- Was ist ein Rollback-Plan?
- Was ist ein Wartungsfenster?
- Was ist ein CAB?
- Was ist eine CMDB?
- Was ist Asset Management?
- Warum sollten Konfigurationen versioniert werden?

Typische Prüfungsfallen

Dokumentation ist keine Nebensache.

Veraltete Dokumentation kann falsche Entscheidungen verursachen.

Netzplan und IP-Liste sind nicht dasselbe.

Physischer Netzplan zeigt Verkabelung.

Logischer Netzplan zeigt Netzwerkstruktur.

Firewall-Regeln brauchen Zweck und Verantwortlichen.

Temporäre Regeln brauchen Ablaufdatum.

Zertifikate müssen vor Ablauf überwacht werden.

Runbook ist konkrete Anleitung.

SOP ist standardisierter Ablauf.

Change Management verhindert unkontrollierte Änderungen.

Emergency Change muss nachträglich dokumentiert werden.

Rollback-Plan vor Änderung erstellen.

Testplan nach Änderung durchführen.

Wartungsfenster reduziert Auswirkungen.

CMDB zeigt IT-Elemente und Beziehungen.

Asset Management verwaltet Bestand.

Secrets gehören nicht in Klartextdokumentation.

Konfigurationen sollten gesichert und versioniert werden.

Wichtige Begriffe kurz erklärt

Begriff	Kurze Erklärung
Dokumentation	nachvollziehbare Beschreibung von IT-Systemen
Systemdokumentation	Beschreibung eines Systems oder Dienstes
Netzwerkdokumentation	Beschreibung der Netzwerkstruktur
IPAM	IP Address Management
Netzplan	grafische Darstellung eines Netzwerks
physischer Netzplan	Darstellung von Geräten, Kabeln und Ports
logischer Netzplan	Darstellung von VLANs, Subnetzen und Routing
Portdokumentation	Zuordnung von Switchports und Anschlüssen
Firewall-Dokumentation	Beschreibung von Firewall-Regeln
DNS-Dokumentation	Verwaltung von DNS-Einträgen
Zertifikatsdokumentation	Übersicht über Zertifikate und Ablaufdaten
Backup-Dokumentation	Beschreibung von Sicherung und Wiederherstellung
Betriebsdokumentation	Anleitung für laufenden Betrieb
Runbook	Schritt-für-Schritt-Anleitung
SOP	Standard Operating Procedure
Wissensdatenbank	Sammlung wiederverwendbaren Wissens
Change Management	kontrollierter Änderungsprozess
Change	geplante Änderung
Standard Change	bekannte risikoarme Routineänderung
Normal Change	geplante Änderung mit Prüfung
Emergency Change	dringende Änderung
Change Request	Änderungsantrag
Wartungsfenster	geplanter Zeitraum für Änderungen
Rollback-Plan	Plan zur Rücknahme einer Änderung
Testplan	Prüfung nach einer Änderung
CAB	Change Advisory Board
Configuration Management	strukturierte Verwaltung von Konfigurationen
CI	Configuration Item
CMDB	Configuration Management Database
Asset Management	Verwaltung von IT-Bestand

Begriff	Kurze Erklärung
Inventarisierung	Erfassung von IT-Objekten
Lizenzmanagement	Verwaltung von Softwarelizenzen
Konfigurationsbackup	Sicherung technischer Konfigurationen
Lessons Learned	Erkenntnisse aus Fehlern oder Projekten
Post-Incident-Review	Auswertung nach einem Vorfall

IHK-sichere Kurzformulierung

Dokumentation und Change Management sind wichtige Bestandteile sicherer und zuverlässiger IT-Administration. Dokumentation beschreibt Systeme, Netzwerke, IP-Adressen, Dienste, Firewall-Regeln, Berechtigungen, Backups, Zertifikate, Verantwortlichkeiten und Notfallmaßnahmen. Change Management sorgt dafür, dass Änderungen geplant, bewertet, freigegeben, durchgeführt, getestet und dokumentiert werden. Wichtige Elemente sind Change Request, Risikobewertung, Wartungsfenster, Testplan, Rollback-Plan, Kommunikation und Aktualisierung der Dokumentation. Eine CMDB kann Configuration Items und deren Beziehungen verwalten, während Asset Management den IT-Bestand erfasst. Gute Dokumentation muss aktuell, verständlich, geschützt und für Betrieb sowie Notfälle nutzbar sein.

Merksätze

Gute Administration ist nachvollziehbar.

Dokumentation reduziert Fehler.

Dokumentation ist Sicherheitsmaßnahme.

Systeme,
Dienste,
Netze
und Rechte dokumentieren.

IP-Adressen sauber verwalten.

IPAM hilft bei IP-Adressverwaltung.

Netzplan zeigt Verbindungen.

Physischer Netzplan zeigt Verkabelung.

Logischer Netzplan zeigt Kommunikation.

Firewall-Regeln brauchen Zweck.

Temporäre Regeln brauchen Ablaufdatum.

DNS-Dokumentation verhindert Namenschaos.

Zertifikate vor Ablauf überwachen.

Backup-Dokumentation muss Restore enthalten.

Rechte müssen nachvollziehbar sein.

Runbook ist Schritt-für-Schritt-Anleitung.

SOP ist standardisierter Ablauf.

Wissensdatenbank hält Wissen verfügbar.

Dokumentation aktuell halten.

Veraltete Dokumentation kann gefährlich sein.

Change Management kontrolliert Änderungen.

Change Request beschreibt Änderung.

Standard Change ist Routine.

Normal Change braucht Prüfung.

Emergency Change ist dringend,
aber nicht dokumentationsfrei.

Risiko vor Änderung bewerten.

Wartungsfenster planen.

Rollback vor Änderung planen.

Testplan nach Änderung durchführen.

Betroffene informieren.

CAB bewertet wichtige Changes.

Configuration Management verwaltet technische Zustände.

CI ist verwaltetes IT-Element.

CMDB zeigt Beziehungen.

Asset Management verwaltet Bestand.

Inventarisierung ist Grundlage für Betrieb und Sicherheit.

Lizenzmanagement verhindert Kosten- und Auditprobleme.

Konfigurationen versionieren.

Konfigurationen sichern.

Secrets nicht in Klartext dokumentieren.

Dokumentation selbst schützen.

Lessons Learned verbessern Prozesse.

Nach Vorfällen auswerten und verbessern.