

Contents

1	IT-Operations Handbuch	10
2	1. Einleitung	11
2.1	1.1 Zweck	11
2.2	1.2 Geltungsbereich	11
3	2. Betriebsprozesse	12
3.1	2.1 Monitoring	12
3.2	2.2 Wartungsfenster	12
3.3	2.3 Change Management	12
4	Dokumentenlenkung und Versionierung	13
4.1	Dokumentmetadaten	13
4.2	Versionshistorie	13
4.3	Versionierungsrichtlinien	14
4.4	Review- und Freigabeprozess	14
4.5	Genehmigungsprozesse	15
4.6	Dokumentationsstandards	15
4.7	Dokumentenklassifizierung	16
4.8	Archivierung und Aufbewahrung	16
4.9	Verantwortlichkeiten	17
4.10	Kontakte	17
5	Servicebeschreibung und Kritikalität	18
5.1	Servicebeschreibung	18
5.2	Kritikalität und Schutzbedarf	19
5.3	Servicezeiten und Betriebsfenster	20
5.4	Service Level Agreements (SLA)	21
5.5	Kapazitätsplanung	22
5.6	Verantwortlichkeiten	22
5.7	Kontakte und Eskalation	23
6	Systemübersicht und Architektur	24
6.1	Überblick	24
6.2	Architekturdiagramm	25
6.3	Komponentenliste	25
6.4	Umgebungen	26

6.5	Schnittstellen	27
6.6	Abhängigkeiten zu anderen Systemen	28
6.7	Technologie-Stack	29
6.8	Sicherheitsarchitektur	30
6.9	Verantwortlichkeiten	30
6.10	Kontakte	30
7	Infrastruktur und Plattform	31
7.1	Überblick	31
7.2	Physische Infrastruktur	32
7.3	Netzwerkinfrastruktur	33
7.4	Virtualisierung	35
7.5	Container-Orchestrierung	37
7.6	Cloud-Infrastruktur	37
7.7	Storage-Infrastruktur	39
7.8	Stromversorgung	40
7.9	Kühlung und Klimatisierung	41
7.10	Physische Sicherheit	41
7.11	Kapazitätsplanung	42
7.12	Lifecycle-Management	42
7.13	Compliance und Zertifizierungen	43
7.14	Verantwortlichkeiten	44
7.15	Kontakte	44
8	Rollen und Verantwortlichkeiten	45
8.1	Organisationsstruktur	45
8.2	Führungsebene	45
8.3	IT-Betriebsebene	46
8.4	Weitere IT-Rollen	47
8.5	RACI-Matrix für IT-Betriebsaktivitäten	48
8.6	Kontaktlisten und Erreichbarkeiten	52
8.7	On-Call und Rufbereitschaft	53
8.8	Eskalationspfade	54
8.9	Vertretungsregelungen	55
8.10	Schulung und Qualifikation	55
8.11	Änderungshistorie	56
9	Betriebskonzept und Betriebsprozesse	57
9.1	Übersicht	57
9.2	Betriebsmodell	57
9.3	ITIL-Prozesse	58
9.4	Prozessschnittstellen	59
9.5	Eskalationspfade	60
9.6	Betriebsprozess-Übersicht	61
9.7	Prozess-Metriken und KPIs	62
9.8	Kontinuierliche Verbesserung	63
9.9	Dokumentation und Wissensmanagement	63
9.10	Compliance und Governance	64

9.11 Kontakte	64
10 Betriebsübergabe und Go-Live-Checkliste	65
10.1 Übersicht	65
10.2 Betriebsübergabe-Prozess	65
10.3 Go-Live-Checkliste	66
10.4 Übergabedokumentation	69
10.5 Acceptance-Kriterien	71
10.6 Go/No-Go-Entscheidung	72
10.7 Rollback-Plan	73
10.8 Post-Implementation-Review	73
10.9 Kontakte	74
11 Konfigurationsmanagement und CMDB	75
11.1 Übersicht	75
11.2 Konfigurationsmanagement-Prozess	75
11.3 Configuration Management Database (CMDB)	76
11.4 CI-Kategorien und Attribute	76
11.5 CI-Beziehungen	78
11.6 Change-Prozesse für CIs	79
11.7 CMDB-Datenqualität	81
11.8 CMDB-Zugriff und Berechtigungen	82
11.9 CMDB-Integration	82
11.10CMDB-Reporting	82
11.11CMDB-Wartung	83
11.12Best Practices	84
11.13Kontakte	84
12 Access und Berechtigungsmanagement	85
12.1 Übersicht	85
12.2 Access Management Strategie	85
12.3 Zugriffskontrollmodell	86
12.4 Rollenbasierte Zugriffskontrolle (RBAC)	86
12.5 Berechtigungsmatrix	88
12.6 Access Request Prozess	88
12.7 Privileged Access Management (PAM)	90
12.8 Service Accounts	91
12.9 Access Review Prozess	91
12.10Onboarding und Offboarding	92
12.11Compliance und Auditing	92
12.12Notfall-Zugriff	93
12.13Kontakte	93
13 Monitoring, Alerting und Observability	95
13.1 Übersicht	95
13.2 Monitoring-Strategie	95
13.3 Monitoring-Tools	96
13.4 Infrastructure Monitoring	97

13.5	Application Monitoring	99
13.6	Observability	100
13.7	Alerting	101
13.8	Dashboards	103
13.9	Monitoring-Prozesse	104
13.10	Service Level Indicators (SLIs)	105
13.11	Incident Response	105
13.12	Monitoring-Dokumentation	106
13.13	Monitoring-Tools-Zugriff	106
13.14	Kontakte	107
14	Incident Management Runbook	108
14.1	Zweck und Geltungsbereich	108
14.2	Incident-Definition	108
14.3	Incident-Kategorien	108
14.4	Incident-Prioritäten	109
14.5	Incident-Management-Prozess	110
14.6	Eskalationsprozesse	112
14.7	Standard-Runbooks	113
14.8	Kommunikationsprozesse	115
14.9	Major Incident Management	115
14.10	Metriken und Reporting	116
14.11	Tools und Systeme	116
14.12	Anhang	117
15	Problem Management und Postmortems	119
15.1	Zweck und Geltungsbereich	119
15.2	Problem-Definition	119
15.3	Problem-Management-Prozess	119
15.4	Root Cause Analysis (RCA) Methoden	122
15.5	Postmortem-Prozess	123
15.6	Postmortem-Template	124
15.7	Known Error Database (KEDB)	126
15.8	Proaktives Problem Management	127
15.9	Metriken und Reporting	128
15.10	Rollen und Verantwortlichkeiten	128
15.11	Tools und Systeme	129
15.12	Referenzen	129
16	Change und Release Management	130
16.1	Zweck und Geltungsbereich	130
16.2	Change Management	130
16.3	Release Management	134
16.4	Metriken und Reporting	138
16.5	Rollen und Verantwortlichkeiten	138
16.6	Tools und Systeme	139
16.7	Referenzen	139

17 Backup und Restore	141
17.1 Zweck und Geltungsbereich	141
17.2 Backup-Grundlagen	141
17.3 Backup-Zeitpläne	143
17.4 Backup-Prozesse	144
17.5 Restore-Prozesse	146
17.6 Backup-Technologien	148
17.7 Backup-Sicherheit	149
17.8 Backup-Testing	149
17.9 Metriken und Reporting	150
17.10 Rollen und Verantwortlichkeiten	150
17.11 Compliance und Regulierung	151
17.12 Referenzen	151
18 Disaster Recovery und Business Continuity	153
18.1 Zweck und Geltungsbereich	153
18.2 Grundlagen	153
18.3 Disaster-Szenarien	154
18.4 DR-Strategien	156
18.5 DR-Infrastruktur	157
18.6 Failover-Prozeduren	157
18.7 Failback-Prozeduren	160
18.8 Business Continuity Management	161
18.9 DR-Testing	162
18.10 Metriken und Reporting	162
18.11 Rollen und Verantwortlichkeiten	163
18.12 Referenzen	163
19 Sicherheitsbetrieb und Hardening	164
19.1 Zweck und Geltungsbereich	164
19.2 Sicherheits-Grundlagen	164
19.3 Hardening-Richtlinien	165
19.4 Security-Monitoring	168
19.5 Vulnerability Management	169
19.6 Security Incident Response	171
19.7 Compliance und Regulierung	172
19.8 Security-Awareness und Training	174
19.9 Rollen und Verantwortlichkeiten	174
19.10 Metriken und Reporting	174
19.11 Referenzen	175
20 Patch und Update Management	176
20.1 Zweck und Geltungsbereich	176
20.2 Patch-Management-Grundlagen	176
20.3 Patch-Management-Prozess	177
20.4 Patch-Zeitpläne	181
20.5 Patch-Management-Tools	182
20.6 Rollback-Prozeduren	183

20.7 Compliance und Reporting	185
20.8 Ausnahmen und Sonderfälle	185
20.9 Rollen und Verantwortlichkeiten	186
20.10 Best Practices	187
20.11 Referenzen	187
21 Log Management und Audit	189
21.1 Zweck und Geltungsbereich	189
21.2 Log-Management-Grundlagen	189
21.3 Log-Sammlung und -Aggregation	191
21.4 Log-Retention und -Archivierung	194
21.5 Log-Analyse und -Monitoring	196
21.6 Audit-Trail-Anforderungen	198
21.7 Compliance und Regulierung	199
21.8 Log-Management-Tools	200
21.9 Rollen und Verantwortlichkeiten	200
21.10 Metriken und Reporting	201
21.11 Referenzen	201
22 Kapazitäts- und Performance Management	202
22.1 Übersicht	202
22.2 Kapazitätsplanung	202
22.3 Performance-Monitoring	203
22.4 Trend-Analysen	205
22.5 Skalierungsstrategien	206
22.6 Kapazitätsoptimierung	208
22.7 Reporting	209
22.8 Prozesse und Verantwortlichkeiten	210
22.9 Tools und Systeme	210
22.10 Compliance und Standards	211
22.11 Anhang	211
23 Verfügbarkeit und Service Level	212
23.1 Übersicht	212
23.2 Verfügbarkeitsanforderungen	212
23.3 Service Level Agreements (SLA)	213
23.4 Service Level Objectives (SLO)	215
23.5 Verfügbarkeitsmessung	216
23.6 Service-Level-Reporting	217
23.7 Verfügbarkeitsverbesserungen	219
23.8 SLA-Review und Anpassung	220
23.9 Prozesse und Verantwortlichkeiten	221
23.10 Compliance und Standards	221
23.11 Anhang	222
24 Datenmanagement und Datenschutz	223
24.1 Übersicht	223
24.2 Datenklassifizierung	223

24.3	Datenschutz-Anforderungen (DSGVO)	225
24.4	Datenaufbewahrung und -löschung	227
24.5	Data-Governance	229
24.6	Datensicherheit	231
24.7	Datenschutzvorfälle	232
24.8	Prozesse und Verantwortlichkeiten	233
24.9	Compliance und Standards	233
24.10	Anhang	233
25	Wartung und Operations-Routinen	235
25.1	Übersicht	235
25.2	Wartungsübersicht	235
25.3	Tägliche Routinen	236
25.4	Wöchentliche Routinen	237
25.5	Monatliche Routinen	239
25.6	Quartalsweise Routinen	241
25.7	Jährliche Routinen	242
25.8	Housekeeping-Prozeduren	244
25.9	Automatisierung	245
25.10	Checklisten-Vorlagen	246
25.11	Prozesse und Verantwortlichkeiten	247
25.12	Compliance und Standards	248
25.13	Anhang	248
26	Runbooks und Standardoperationen	249
26.1	Übersicht	249
26.2	Runbook-Struktur	249
26.3	System-Management Runbooks	250
26.4	Datenbank-Management Runbooks	255
26.5	Netzwerk-Management Runbooks	257
26.6	Benutzer-Management Runbooks	259
26.7	Monitoring und Alerting Runbooks	261
26.8	Backup und Recovery Runbooks	263
26.9	Troubleshooting-Guides	264
26.10	Prozesse und Verantwortlichkeiten	266
26.11	Compliance und Standards	266
26.12	Anhang	266
27	Tooling und Zugangswege	268
27.1	Übersicht	268
27.2	Tool-Kategorien	268
27.3	Monitoring und Observability	269
27.4	Infrastructure Management	270
27.5	Security und Compliance	271
27.6	Development und Deployment	272
27.7	Collaboration und Communication	273
27.8	Documentation und Knowledge Management	274
27.9	Backup und Recovery	275

27.10	Zugangswege	275
27.11	Authentifizierungsmethoden	276
27.12	Tool-Zugriffs-Matrix	277
27.13	Notfall-Zugänge	277
27.14	Tool-Lifecycle-Management	278
27.15	Prozesse und Verantwortlichkeiten	278
27.16	Compliance und Standards	279
27.17	Anhang	279
28	Bekannte Probleme und FAQ	280
28.1	Übersicht	280
28.2	Bekannte Probleme	280
28.3	Häufig gestellte Fragen (FAQ)	283
28.4	Troubleshooting-Tipps	289
28.5	Self-Service-Ressourcen	290
28.6	Feedback und Verbesserungen	290
28.7	Prozesse und Verantwortlichkeiten	291
28.8	Compliance und Standards	291
28.9	Anhang	291
29	Kontakte, Eskalation und Anbieter	292
29.1	Übersicht	292
29.2	Interne Kontakte	292
29.3	On-Call und Rufbereitschaft	295
29.4	Eskalationspfade	295
29.5	Externe Anbieter und Lieferanten	297
29.6	Notfall-Kontakte	300
29.7	Kommunikationskanäle	300
29.8	Kontakt-Aktualisierung	302
29.9	Prozesse und Verantwortlichkeiten	302
29.10	Compliance und Standards	303
29.11	Anhang	303
29.12	Schnellreferenz	303
30	Compliance und Audits	305
30.1	Zweck und Geltungsbereich	305
30.2	Compliance-Grundlagen	305
30.3	Relevante Standards und Regulierungen	306
30.4	Compliance-Management-Prozess	308
30.5	Audit-Prozesse	310
30.6	Compliance-Kontrollen und Nachweise	313
30.7	Non-Compliance-Risiken und Maßnahmen	315
30.8	Compliance-Metriken und Reporting	316
30.9	Compliance-Tools und -Systeme	318
30.10	Rollen und Verantwortlichkeiten	318
30.11	Best Practices	319
30.12	Audit-Kalender	320
30.13	Referenzen	320

31 Anhang: Checklisten und Vorlagen	322
31.1 Übersicht	322
31.2 Checklisten	322
31.3 Vorlagen	330
31.4 Formulare	334
31.5 Prozesse und Verantwortlichkeiten	336
31.6 Compliance und Standards	336
31.7 Anhang	336

Chapter 1

IT-Operations Handbuch

Dokument-Metadaten

- **Erstellt am:** 2026-02-05
 - **Autor:** Andreas Huemmer [andreas.huemmer@adminsends.de]
 - **Version:** 0.0.2
 - **Typ:** IT-Operations-Handbuch
-

ewpage

Chapter 2

1. Einleitung

Dieses Handbuch beschreibt die IT-Betriebsprozesse und -standards der Organisation.

2.1 1.1 Zweck

Das IT-Operations-Handbuch definiert Prozesse und Verantwortlichkeiten für den stabilen IT-Betrieb.

2.2 1.2 Geltungsbereich

Dieses Handbuch gilt für alle IT-Systeme und -Services der Organisation.

ewpage

Chapter 3

2. Betriebsprozesse

3.1 2.1 Monitoring

- 24/7 Überwachung aller kritischen Systeme
- Automatische Alarmierung bei Schwellwertüberschreitungen
- Wöchentliche Auswertung der Monitoring-Daten

3.2 2.2 Wartungsfenster

- Geplante Wartungen: Sonntags 02:00-06:00 Uhr
- Notfallwartungen: Nach Genehmigung durch IT-Leitung
- Ankündigung mindestens 48 Stunden im Voraus

3.3 2.3 Change Management

- Alle Änderungen müssen dokumentiert werden
- Kritische Änderungen erfordern Change Advisory Board Genehmigung
- Rollback-Plan ist für alle Änderungen verpflichtend

ewpage

Chapter 4

Dokumentenlenkung und Versionierung

4.1 Dokumentmetadaten

Feld	Wert
Dokumenttitel	IT-Betriebshandbuch – AdminSend GmbH
Dokument-ID	[TODO: Eindeutige Dokument-ID]
System/Service	[TODO: System-/Service-Name]
Eigentümer (Owner)	IT Operations Manager
Verantwortlicher Redakteur	Andreas Huemmer [andreas.huemmer@adminsends.de]
Freigabeinstanz	CIO
Klassifizierung	internal
Ablageort	[TODO: Zentrales Repository/Ablageort]
Organisation	AdminSend GmbH
Standort	München, Deutschland

4.2 Versionshistorie

Version	Datum	Autor	Änderungen	Genehmigung
1.0.0	[TODO: Datum]	Andreas Huemmer [andreas.huemmer@adminsends.de]	Initiale Version	CIO

Hinweis: Nutzen Sie Semantic Versioning (SemVer) für die Versionierung: - **Major.Minor.Patch** (z.B. 1.0.0) - **Major:** Grundlegende Änderungen, Breaking Changes - **Minor:** Neue Features, abwärtskompatibel - **Patch:** Bugfixes, kleine Korrekturen

4.3 Versionierungsrichtlinien

4.3.1 Semantic Versioning (SemVer)

Format: MAJOR.MINOR.PATCH

- **MAJOR:** Inkompatible Änderungen, grundlegende Überarbeitungen
 - Beispiel: Wechsel der Systemarchitektur, neue Betriebsmodelle
- **MINOR:** Neue Funktionalität, abwärtskompatibel
 - Beispiel: Neue Prozesse, zusätzliche Abschnitte
- **PATCH:** Bugfixes, Korrekturen, Klarstellungen
 - Beispiel: Tippfehler, Formatierungen, kleine Ergänzungen

4.3.2 Versionierungsregeln

1. **Initiale Version:** 1.0.0 nach Erstfreigabe
2. **Entwürfe:** 0.x.x vor Erstfreigabe
3. **Änderungen dokumentieren:** Jede Änderung in Versionshistorie eintragen
4. **Datum:** ISO 8601 Format (YYYY-MM-DD)
5. **Autor:** Vollständiger Name und E-Mail

4.4 Review- und Freigabeprozess

4.4.1 1. Änderungsantrag (Change Request)

Verantwortlich: Dokumentverantwortlicher oder Fachbereich

Inhalt: - Beschreibung der Änderung - Begründung und Geschäftswert - Auswirkungenanalyse - Betroffene Abschnitte

Genehmigung: IT Operations Manager

4.4.2 2. Fachreview

Reviewer: - **Operations:** Andreas Huemmer (andreas.huemmer@adminsends.de) - **Architektur:** [TODO: Architektur-Verantwortlicher] - **Security:** Thomas Weber (thomas.weber@adminsends.de) - **Compliance:** [TODO: Compliance-Verantwortlicher]

Prüfkriterien: - Fachliche Korrektheit - Vollständigkeit - Konsistenz mit anderen Dokumenten - Einhaltung von Standards und Best Practices

4.4.3 3. Freigabe

Freigabeinstanz: CIO

Freigabekriterien: - Alle Reviews abgeschlossen - Keine offenen Kommentare - Qualitätskriterien erfüllt - Dokumentationsstandards eingehalten

Freigabeprozess: 1. Review-Kommentare einarbeiten 2. Finale Version erstellen 3. Freigabe durch CIO 4. Version inkrementieren 5. Publikation im Repository

4.4.4 4. Publikation

Verantwortlich: IT Operations Manager

Schritte: 1. Dokument im zentralen Repository ablegen 2. Stakeholder informieren 3. Alte Version archivieren 4. Änderungsnotiz veröffentlichen

4.5 Genehmigungsprozesse

4.5.1 Standard-Änderungen (Patch)

- **Genehmigung:** Dokumentverantwortlicher
- **Review:** Optional
- **Beispiele:** Tippfehler, Formatierung, kleine Ergänzungen

4.5.2 Normale Änderungen (Minor)

- **Genehmigung:** CIO
- **Review:** Fachbereich (Operations/Security)
- **Beispiele:** Neue Abschnitte, Prozessänderungen

4.5.3 Wesentliche Änderungen (Major)

- **Genehmigung:** Anna Schmidt (anna.schmidt@adminsind.de)
- **Review:** Alle Fachbereiche + Management
- **CAB-Sitzung:** Erforderlich
- **Beispiele:** Grundlegende Überarbeitungen, Architekturänderungen

4.6 Dokumentationsstandards

4.6.1 Sprache und Format

- **Sprache:** de
- **Format:** Markdown (.md)
- **Zeichensatz:** UTF-8
- **Zeilenumbruch:** Unix (LF)

4.6.2 Pflichtfelder

Jedes Dokument MUSS folgende Informationen enthalten:

- **Titel:** Eindeutiger Dokumenttitel
- **Version:** Nach SemVer
- **Datum:** Letzte Änderung (ISO 8601)
- **Autor:** Verantwortlicher Redakteur
- **Owner:** Dokumentverantwortlicher
- **Freigabe:** Freigabeinstanz
- **Klassifizierung:** Vertraulichkeitsstufe

4.6.3 Strukturvorgaben

1. **Überschriften:** Hierarchisch (# H1, ## H2, ### H3)
2. **Tabellen:** Markdown-Syntax mit Ausrichtung
3. **Listen:** Nummeriert oder Aufzählungszeichen
4. **Code:** Fenced Code Blocks mit Syntax-Highlighting
5. **Links:** Relative Links bevorzugt

4.6.4 Verlinkungen

- **Interne Links:** Relative Pfade innerhalb des Repositories
- **Externe Links:** Absolute URLs mit Beschreibung
- **Referenzen:** Eindeutige Bezeichner für Querverweise

4.6.5 Metadaten-Platzhalter

Verwenden Sie folgende Platzhalter für organisationsweite Informationen:

- **Organisation:** AdminSend GmbH
- **Rollen:** Max Mustermann, Anna Schmidt, Thomas Weber
- **Dokument:** IT Operations Manager, CIO
- **Autor:** Andreas Huemmer [andreas.huemmer@adminsends.de]

4.7 Dokumentenklassifizierung

Klassifizierung	Beschreibung	Zugriff	Beispiele
Öffentlich	Keine Einschränkungen	Alle	Allgemeine Informationen
Intern	Nur für Mitarbeiter	Mitarbeiter	Betriebshandbücher, Prozesse
Vertraulich	Eingeschränkter Zugriff	Autorisierte Personen	Sicherheitskonzepte, Passwörter
Streng vertraulich	Höchste Vertraulichkeit	Management + Autorisierte	Geschäftsgeheimnisse, Compliance

Aktuelle Klassifizierung: internal

4.8 Archivierung und Aufbewahrung

4.8.1 Aufbewahrungsfristen

- **Aktuelle Version:** Unbegrenzt im Repository
- **Vorversionen:** Mindestens 3 Jahre
- **Entwürfe:** 1 Jahr nach Freigabe
- **Archivierte Dokumente:** Nach Aufbewahrungsrichtlinie

4.8.2 Archivierungsprozess

1. **Versionswechsel:** Alte Version in Archiv verschieben
2. **Metadaten:** Archivierungsdatum und Grund dokumentieren
3. **Zugriff:** Lesezugriff für autorisierte Personen
4. **Löschung:** Nach Ablauf der Aufbewahrungsfrist

4.9 Verantwortlichkeiten

Rolle	Verantwortung	Person
Dokumentverantwortlicher	Gesamtverantwortung, Aktualität	IT Operations Manager
Redakteur	Inhaltliche Pflege, Änderungen	Andreas Huemmer [andreas.huemmer@adminsends.de]
Freigabeinstanz	Genehmigung von Änderungen	CIO
CIO	Strategische Ausrichtung	Anna Schmidt
CISO	Security-Review	Thomas Weber

4.10 Kontakte

Bei Fragen zur Dokumentenlenkung: - **Dokumentverantwortlicher:** IT Operations Manager - **IT Operations Manager:** Andreas Huemmer (andreas.huemmer@adminsends.de) - **CIO:** Anna Schmidt (anna.schmidt@adminsends.de)

Dokumentverantwortlicher: IT Operations Manager

Genehmigt durch: CIO

Version: 1.0.0

Organisation: AdminSend GmbH

ewpage

Chapter 5

Servicebeschreibung und Kritikalität

5.1 Servicebeschreibung

5.1.1 Basis-Informationen

- **Service-Name:** [TODO: Eindeutiger Service-Name]
- **Service-ID:** [TODO: Eindeutige Service-Identifikation]
- **Service-Owner:** IT Operations Manager
- **Technischer Ansprechpartner:** [TODO: Name und Kontakt]
- **Organisation:** AdminSend GmbH

5.1.2 Kurzbeschreibung

[TODO: Beschreiben Sie den Service in 2-3 Sätzen. Was macht der Service? Welche Hauptfunktionen bietet er?]

5.1.3 Geschäftszweck

Geschäftlicher Nutzen: [TODO: Welchen geschäftlichen Wert liefert dieser Service? Welche Geschäftsprozesse unterstützt er?]

Strategische Bedeutung: [TODO: Wie wichtig ist dieser Service für die Unternehmensstrategie?]

5.1.4 Kunden und Nutzergruppen

Nutzergruppe	Anzahl Nutzer	Nutzungsart	Kritikalität
[TODO: Gruppe 1]	[TODO]	[TODO: Primär/Sekundär]	[TODO: Hoch/Mittel/Niedrig]
[TODO: Gruppe 2]	[TODO]	[TODO: Primär/Sekundär]	[TODO: Hoch/Mittel/Niedrig]
[TODO: Gruppe 3]	[TODO]	[TODO: Primär/Sekundär]	[TODO: Hoch/Mittel/Niedrig]

Primäre Nutzergruppen: - [TODO: Beschreibung der Hauptnutzer]

Sekundäre Nutzergruppen: - [TODO: Beschreibung der Nebennutzer]

5.1.5 Abhängigkeiten zu anderen Services

5.1.5.1 Upstream-Abhängigkeiten (Services, von denen dieser Service abhängt)

Service	Abhängigkeitstyp	Kritikalität	Auswirkung bei Ausfall
[TODO: Service 1]	[TODO: Hard/Soft]	[TODO: Hoch/Mittel/Niedrig]	[TODO: Beschreibung]
[TODO: Service 2]	[TODO: Hard/Soft]	[TODO: Hoch/Mittel/Niedrig]	[TODO: Beschreibung]

5.1.5.2 Downstream-Abhängigkeiten (Services, die von diesem Service abhängen)

Service	Abhängigkeitstyp	Kritikalität	Auswirkung bei Ausfall
[TODO: Service 1]	[TODO: Hard/Soft]	[TODO: Hoch/Mittel/Niedrig]	[TODO: Beschreibung]
[TODO: Service 2]	[TODO: Hard/Soft]	[TODO: Hoch/Mittel/Niedrig]	[TODO: Beschreibung]

Hinweis: - **Hard Dependency:** Service funktioniert nicht ohne Abhängigkeit - **Soft Dependency:** Service funktioniert eingeschränkt ohne Abhängigkeit

5.2 Kritikalität und Schutzbedarf

5.2.1 Kritikalitätsbewertung

Die Kritikalität wird nach den Dimensionen Verfügbarkeit, Integrität, Vertraulichkeit und Nachvollziehbarkeit bewertet.

Dimension	Einstufung	Begründung	Maßnahmen
Verfügbarkeit	niedrig mittel hoch	[TODO: Begründung]	[TODO: Schutzmaßnahmen]
Integrität	niedrig mittel hoch	[TODO: Begründung]	[TODO: Schutzmaßnahmen]
Vertraulichkeit	niedrig mittel hoch	[TODO: Begründung]	[TODO: Schutzmaßnahmen]
Nachvollziehbarkeit	niedrig mittel hoch	[TODO: Begründung]	[TODO: Schutzmaßnahmen]

5.2.2 Kritikalitätsstufen

5.2.2.1 Niedrig

- **Verfügbarkeit:** Ausfall tolerierbar für mehrere Tage

- **Integrität:** Datenverlust akzeptabel, einfache Wiederherstellung
- **Vertraulichkeit:** Öffentliche oder unkritische Informationen
- **Nachvollziehbarkeit:** Keine Audit-Anforderungen

5.2.2.2 Mittel

- **Verfügbarkeit:** Ausfall tolerierbar für Stunden bis 1 Tag
- **Integrität:** Datenverlust problematisch, Wiederherstellung erforderlich
- **Vertraulichkeit:** Interne Informationen, eingeschränkter Zugriff
- **Nachvollziehbarkeit:** Basis-Logging erforderlich

5.2.2.3 Hoch

- **Verfügbarkeit:** Ausfall nur für Minuten tolerierbar
- **Integrität:** Datenverlust inakzeptabel, sofortige Wiederherstellung
- **Vertraulichkeit:** Vertrauliche Daten, strenge Zugriffskontrolle
- **Nachvollziehbarkeit:** Vollständiges Audit-Trail erforderlich

5.2.3 Gesamtkritikalität

Kritikalitätseinstufung: [TODO: Niedrig/Mittel/Hoch/Kritisch]

Begründung: [TODO: Zusammenfassende Begründung der Gesamtkritikalität basierend auf den einzelnen Dimensionen]

5.3 Servicezeiten und Betriebsfenster

5.3.1 Servicezeiten

- **Verfügbarkeit:** [TODO: z.B. 24/7, Mo-Fr 08:00-18:00 CET, Business Hours]
- **Support-Zeiten:** [TODO: Wann ist Support verfügbar?]
- **Zeitzone:** [TODO: z.B. CET/CEST, UTC]

5.3.2 Betriebsmodell

- **Betriebsmodell:** [TODO: 24/7, Business Hours, Follow-the-Sun]
- **On-Call-Bereitschaft:** [TODO: Ja/Nein, Zeiten]
- **Eskalationsstufen:** [TODO: Level 1/2/3 Support]

5.3.3 Wartungsfenster

Wartungstyp	Zeitfenster	Frequenz	Dauer	Ankündigung
Geplante Wartung	[TODO: z.B. So 02:00-06:00]	[TODO: Wöchentlich/Monatlich]	[TODO: Stunden]	[TODO: Tage im Voraus]
Notfallwartung	[TODO: Nach Bedarf]	[TODO: Ad-hoc]	[TODO: Variable]	[TODO: Sofort]
Patch-Fenster	[TODO: z.B. 2. Dienstag/Monat]	[TODO: Monatlich]	[TODO: Stunden]	[TODO: Tage im Voraus]

5.3.4 Geplante Downtimes

Kommunikationsprozess: 1. **Ankündigung:** Mindestens [TODO: X Tage] im Voraus
2. **Kanal:** [TODO: E-Mail, Portal, Ticket-System] 3. **Empfänger:** [TODO: Alle Nutzer, Key-Stakeholder] 4. **Inhalt:** Zeitfenster, Grund, Auswirkungen, Ansprechpartner

Verantwortlich: Andreas Huemmer (andreas.huemmer@adminsends.de)

5.4 Service Level Agreements (SLA)

5.4.1 SLA-Übersicht

Kennzahl	Zielwert	Messmethode	Messquelle	Reporting
Verfügbarkeit	[TODO: z.B. 99.9%]	[TODO: Uptime-Monitoring]	[TODO: Monitoring-Tool]	[TODO: Monatlich]
MTTR	[TODO: z.B. 4h]	[TODO: Ticket-Analyse]	[TODO: ITSM-Tool]	[TODO: Monatlich]
MTBF	[TODO: z.B. 720h]	[TODO: Incident-Analyse]	[TODO: ITSM-Tool]	[TODO: Quartalsweise]
Antwortzeit	[TODO: z.B. < 200ms]	[TODO: APM]	[TODO: APM-Tool]	[TODO: Täglich]
Durchsatz	[TODO: z.B. 1000 TPS]	[TODO: Performance-Monitoring]	[TODO: Monitoring-Tool]	[TODO: Täglich]

5.4.2 Service Level Objectives (SLO)

5.4.2.1 Verfügbarkeit

- **Ziel:** [TODO: z.B. 99.9% Uptime pro Monat]
- **Berechnung:** $(\text{Gesamtzeit} - \text{Downtime}) / \text{Gesamtzeit} \times 100\%$
- **Ausnahmen:** Geplante Wartungsfenster
- **Messung:** Kontinuierliches Uptime-Monitoring

5.4.2.2 Performance

- **Antwortzeit (P95):** [TODO: z.B. < 200ms]
- **Antwortzeit (P99):** [TODO: z.B. < 500ms]
- **Durchsatz:** [TODO: z.B. min. 1000 Requests/Sekunde]
- **Fehlerrate:** [TODO: z.B. < 0.1%]

5.4.2.3 Wiederherstellung

- **RTO (Recovery Time Objective):** [TODO: z.B. 4 Stunden]
- **RPO (Recovery Point Objective):** [TODO: z.B. 1 Stunde]
- **MTTR (Mean Time To Repair):** [TODO: z.B. 4 Stunden]
- **MTBF (Mean Time Between Failures):** [TODO: z.B. 720 Stunden]

5.4.3 SLA-Reporting

Reporting-Frequenz: [TODO: Monatlich/Quartalsweise]

Empfänger: - Service Owner: IT Operations Manager - IT Operations Manager: Andreas Huemmer - CIO: Anna Schmidt - [TODO: Weitere Stakeholder]

Inhalt: - Verfügbarkeitsstatistiken - Performance-Metriken - Incident-Übersicht - SLA-Einhaltung
- Verbesserungsmaßnahmen

5.4.4 SLA-Verletzungen

Eskalationsprozess bei SLA-Verletzung:

1. **Automatische Benachrichtigung:** Monitoring-System
2. **Analyse:** IT Operations Team
3. **Eskalation Level 1:** IT Operations Manager
4. **Eskalation Level 2:** CIO
5. **Root-Cause-Analysis:** Innerhalb [TODO: X Tage]
6. **Maßnahmenplan:** Innerhalb [TODO: X Tage]

5.5 Kapazitätsplanung

5.5.1 Aktuelle Kapazität

Ressource	Aktuell	Maximum	Auslastung	Schwellwert
[TODO: CPU]	[TODO]	[TODO]	[TODO]%	[TODO]%
[TODO: RAM]	[TODO]	[TODO]	[TODO]%	[TODO]%
[TODO: Storage]	[TODO]	[TODO]	[TODO]%	[TODO]%
[TODO: Netzwerk]	[TODO]	[TODO]	[TODO]%	[TODO]%

5.5.2 Wachstumsprognose

- **Nutzerwachstum:** [TODO: z.B. +10% pro Jahr]
- **Datenwachstum:** [TODO: z.B. +20% pro Jahr]
- **Transaktionswachstum:** [TODO: z.B. +15% pro Jahr]

5.5.3 Skalierungsstrategien

- **Vertikale Skalierung:** [TODO: Beschreibung]
- **Horizontale Skalierung:** [TODO: Beschreibung]
- **Auto-Scaling:** [TODO: Ja/Nein, Konfiguration]

5.6 Verantwortlichkeiten

Rolle	Verantwortung	Person	Kontakt
Service Owner	Gesamtverantwortung	IT Operations Manager	[TODO: E-Mail]

Rolle	Verantwortung	Person	Kontakt
Technical Lead	Technische Umsetzung	[TODO: Name]	[TODO: E-Mail]
Operations Manager	Täglicher Betrieb	Andreas Huemmer	andreas.huemmer@adminsends.de
Service Desk Lead	First-Level-Support	Julia Becker	julia.becker@adminsends.de

5.7 Kontakte und Eskalation

Bei Fragen zum Service: - **Service Owner:** IT Operations Manager - **IT Operations Manager:** Andreas Huemmer (andreas.huemmer@adminsends.de) - **Service Desk:** Julia Becker (julia.becker@adminsends.de)

Eskalationspfad: 1. **Level 1:** Service Desk - julia.becker@adminsends.de 2. **Level 2:** IT Operations - andreas.huemmer@adminsends.de 3. **Level 3:** CIO - anna.schmidt@adminsends.de

Service Owner: IT Operations Manager

Genehmigt durch: CIO

Version: 1.0.0

Organisation: AdminSend GmbH

ewpage

Chapter 6

Systemübersicht und Architektur

6.1 Überblick

6.1.1 Systemlandschaft

Dieses Kapitel beschreibt die Systemlandschaft und Architektur auf hoher Ebene.

System/Service: [TODO: System-/Service-Name]

Kurzbeschreibung: [TODO: Beschreiben Sie die Systemlandschaft in 2-3 Sätzen. Was ist der Zweck des Systems? Welche Hauptfunktionen bietet es?]

6.1.2 Hauptkomponenten

Komponente	Typ	Zweck	Technologie	Status
[TODO: Komponente 1]	[TODO: App/DB/Queue]	[TODO: Beschreibung]	[TODO: Tech-Stack]	[TODO: Aktiv/Geplant]
[TODO: Komponente 2]	[TODO: App/DB/Queue]	[TODO: Beschreibung]	[TODO: Tech-Stack]	[TODO: Aktiv/Geplant]
[TODO: Komponente 3]	[TODO: App/DB/Queue]	[TODO: Beschreibung]	[TODO: Tech-Stack]	[TODO: Aktiv/Geplant]

6.1.3 Datenflüsse

Hauptdatenflüsse: 1. [TODO: Datenfluss 1 - Quelle → Ziel] 2. [TODO: Datenfluss 2 - Quelle → Ziel] 3. [TODO: Datenfluss 3 - Quelle → Ziel]

Datenvolumen: - [TODO: z.B. 10.000 Transaktionen/Tag] - [TODO: z.B. 100 GB Daten/Monat]

6.1.4 Nutzerzugriffe

Zugriffswege: - **Web-Interface:** [TODO: URL] - **API:** [TODO: API-Endpoint] - **Mobile App:** [TODO: App-Name] - **Desktop-Client:** [TODO: Client-Name]

Authentifizierung: - [TODO: z.B. SSO, LDAP, OAuth2]

Architekturdiagramm

Figure 6.1: Architekturdiagramm

Netzwerkdiagramm

Figure 6.2: Netzwerkdiagramm

6.2 Architekturdiagramm

6.2.1 High-Level-Architektur

Hinweis: Fügen Sie hier ein Architekturdiagramm ein oder verlinken Sie es. Empfohlene Tools: draw.io, PlantUML, Mermaid, Visio

Diagramm-Beschreibung: [TODO: Beschreiben Sie die Hauptelemente des Architekturdiagramms]

6.2.2 Netzwerkarchitektur

Hinweis: Fügen Sie hier ein Netzwerkdiagramm ein.

Netzwerksegmente: - [TODO: z.B. DMZ, Internal, Management]

Firewall-Regeln: - [TODO: Beschreibung der wichtigsten Firewall-Regeln]

6.2.3 Deployment-Architektur

Hinweis: Fügen Sie hier ein Deployment-Diagramm ein.

Deployment-Modell: - [TODO: z.B. On-Premise, Cloud, Hybrid]

6.3 Komponentenliste

6.3.1 Anwendungskomponenten

Komponente	Typ	Zweck	Technologie	Verantwortlich	Kritikalität
[TODO: Frontend]	Web-App	[TODO: Beschreibung]	[TODO: React/Angular/Vue]	[TODO: Team]	L M H
[TODO: Backend]	API-Server	[TODO: Beschreibung]	[TODO: Node.js/Java/Python]	[TODO: Team]	L M H
[TODO: Worker]	Background-Job	[TODO: Beschreibung]	[TODO: Technologie]	[TODO: Team]	L M H

6.3.2 Datenkomponenten

Deployment-Diagramm

Figure 6.3: Deployment-Diagramm

Komponente	Typ	Zweck	Technologie	Größe	Kritikalität		
[TODO: Datenbank]	RDBMS	[TODO: Beschreibung]	[TODO: PostgreSQL/MySQL]	[TODO: GB]	L	M	H
[TODO: Cache]	In-Memory	[TODO: Beschreibung]	[TODO: Redis/Memcached]	[TODO: GB]	L	M	H
[TODO: Queue]	Message-Queue	[TODO: Beschreibung]	[TODO: RabbitMQ/Kafka]	[TODO: Messages/s]	L	M	H

6.3.3 Infrastrukturkomponenten

Komponente	Typ	Zweck	Technologie	Standort	Kritikalität		
[TODO: Load Balancer]	LB	[TODO: Beschreibung]	[TODO: HAProxy/Nginx]	[TODO: Standort]	L	M	H
[TODO: Firewall]	Security	[TODO: Beschreibung]	[TODO: Hersteller]	[TODO: Standort]	L	M	H
[TODO: Monitoring]	Observability	[TODO: Beschreibung]	[TODO: Prometheus/Grafana]	[TODO: Standort]	L	M	H

Legende: - **L:** Low (Niedrig) - **M:** Medium (Mittel) - **H:** High (Hoch)

6.4 Umgebungen

6.4.1 Umgebungsübersicht

Umgebung	Zweck	URL/Endpoint	Besonderheiten	Zugriff
DEV	Entwicklung	[TODO: dev.example.com]	[TODO: Testdaten, Debug-Modus]	[TODO: Entwickler]
TEST	Testing/QA	[TODO: test.example.com]	[TODO: Staging-Daten]	[TODO: QA-Team]
STAGE	Pre-Production	[TODO: stage.example.com]	[TODO: Produktionsähnlich]	[TODO: Ops-Team]
PROD	Produktion	[TODO: www.example.com]	[TODO: Live-System]	[TODO: Autorisiert]

6.4.2 Umgebungskonfiguration

6.4.2.1 Development (DEV)

- **Zweck:** Entwicklung und initiale Tests
- **Daten:** Synthetische Testdaten
- **Monitoring:** Basis-Monitoring
- **Backup:** Nicht erforderlich
- **Verfügbarkeit:** Business Hours

6.4.2.2 Test (TEST)

- **Zweck:** Funktionale und Integrationstests
- **Daten:** Anonymisierte Produktionsdaten
- **Monitoring:** Vollständiges Monitoring
- **Backup:** Wöchentlich
- **Verfügbarkeit:** Business Hours

6.4.2.3 Staging (STAGE)

- **Zweck:** Pre-Production-Tests, Release-Validierung
- **Daten:** Anonymisierte Produktionsdaten (aktuell)
- **Monitoring:** Identisch zu Produktion
- **Backup:** Täglich
- **Verfügbarkeit:** 24/7

6.4.2.4 Production (PROD)

- **Zweck:** Live-Betrieb
- **Daten:** Produktionsdaten
- **Monitoring:** 24/7 Monitoring mit Alerting
- **Backup:** Mehrmals täglich
- **Verfügbarkeit:** 24/7 (gemäß SLA)

6.4.3 Promotion-Prozess

Deployment-Pipeline: 1. **DEV:** Automatisches Deployment bei Code-Commit 2. **TEST:** Automatisches Deployment nach erfolgreichen Unit-Tests 3. **STAGE:** Manuelles Deployment nach QA-Freigabe 4. **PROD:** Manuelles Deployment nach Change-Genehmigung

Genehmigungen: - **DEV** → **TEST:** Automatisch - **TEST** → **STAGE:** QA-Team - **STAGE** → **PROD:** CIO + Change Advisory Board

6.5 Schnittstellen

6.5.1 Inbound-Schnittstellen (Eingehend)

Partner/System	Protokoll	Authentifizierung	Datenformat	Zweck	SLA
[TODO: System 1]	[TODO: HTTPS/REST]	[TODO: OAuth2/API- Key]	[TODO: JSON/XML]	[TODO: Beschreibung]	[TODO: 99.9%]
[TODO: System 2]	[TODO: MQ/AMQP]	[TODO: Certificate]	[TODO: JSON]	[TODO: Beschreibung]	[TODO: 99.5%]
[TODO: System 3]	[TODO: SOAP]	[TODO: WS-Security]	[TODO: XML]	[TODO: Beschreibung]	[TODO: 99.0%]

6.5.2 Outbound-Schnittstellen (Ausgehend)

Partner/System	Protokoll	Authentifizierung	Datenformat	Zweck	SLA
[TODO: System 1]	[TODO: HTTPS/REST]	[TODO: OAuth2]	[TODO: JSON]	[TODO: Beschreibung]	[TODO: 99.9%]
[TODO: System 2]	[TODO: SMTP]	[TODO: TLS]	[TODO: E-Mail]	[TODO: Beschreibung]	[TODO: 99.0%]
[TODO: System 3]	[TODO: FTP/SFTP]	[TODO: SSH-Key]	[TODO: CSV]	[TODO: Beschreibung]	[TODO: 99.5%]

6.5.3 API-Endpunkte

Endpunkt	Methode	Authentifizierung	Rate-Limit	Beschreibung
[TODO: /api/v1/users]	GET/POST	[TODO: Bearer Token]	[TODO: 1000/h]	[TODO: Benutzerverwaltung]
[TODO: /api/v1/data]	GET/PUT	[TODO: API-Key]	[TODO: 5000/h]	[TODO: Datenzugriff]
[TODO: /api/v1/status]	GET	[TODO: None]	[TODO: Unlimited]	[TODO: Health-Check]

6.5.4 Schnittstellendokumentation

API-Dokumentation: [TODO: Link zur API-Dokumentation (z.B. Swagger/OpenAPI)]

Integrationsleitfaden: [TODO: Link zum Integrationsleitfaden]

6.6 Abhängigkeiten zu anderen Systemen

6.6.1 Upstream-Systeme (Abhängigkeiten)

System	Typ	Kritikalität	Auswirkung bei Ausfall	Fallback
[TODO: System 1]	[TODO: Datenquelle]	L M H	[TODO: Beschreibung]	[TODO: Fallback-Strategie]
[TODO: System 2]	[TODO: Auth-Provider]	L M H	[TODO: Beschreibung]	[TODO: Fallback-Strategie]
[TODO: System 3]	[TODO: Payment-Gateway]	L M H	[TODO: Beschreibung]	[TODO: Fallback-Strategie]

6.6.2 Downstream-Systeme (Abhängige Systeme)

System	Typ	Kritikalität	Auswirkung bei Ausfall	Benachrichtigung
[TODO: System 1]	[TODO: Reporting]	L M H	[TODO: Beschreibung]	[TODO: Ja/Nein]
[TODO: System 2]	[TODO: Analytics]	L M H	[TODO: Beschreibung]	[TODO: Ja/Nein]
[TODO: System 3]	[TODO: Archivierung]	L M H	[TODO: Beschreibung]	[TODO: Ja/Nein]

6.7 Technologie-Stack

6.7.1 Frontend

- **Framework:** [TODO: z.B. React 18.x]
- **UI-Library:** [TODO: z.B. Material-UI]
- **State-Management:** [TODO: z.B. Redux]
- **Build-Tool:** [TODO: z.B. Webpack/Vite]

6.7.2 Backend

- **Runtime:** [TODO: z.B. Node.js 20.x]
- **Framework:** [TODO: z.B. Express.js]
- **ORM:** [TODO: z.B. Sequelize/TypeORM]
- **API-Stil:** [TODO: REST/GraphQL/gRPC]

6.7.3 Datenbank

- **RDBMS:** [TODO: z.B. PostgreSQL 15.x]
- **NoSQL:** [TODO: z.B. MongoDB 6.x]
- **Cache:** [TODO: z.B. Redis 7.x]
- **Search:** [TODO: z.B. Elasticsearch 8.x]

6.7.4 Infrastruktur

- **Container:** [TODO: z.B. Docker]
- **Orchestrierung:** [TODO: z.B. Kubernetes]
- **Cloud-Provider:** [TODO: z.B. AWS/Azure/GCP]
- **IaC:** [TODO: z.B. Terraform/Ansible]

6.7.5 Monitoring und Observability

- **Metrics:** [TODO: z.B. Prometheus]
- **Logging:** [TODO: z.B. ELK-Stack]
- **Tracing:** [TODO: z.B. Jaeger]
- **Dashboards:** [TODO: z.B. Grafana]

6.8 Sicherheitsarchitektur

6.8.1 Netzwerksegmentierung

- **DMZ:** [TODO: Beschreibung]
- **Application-Tier:** [TODO: Beschreibung]
- **Data-Tier:** [TODO: Beschreibung]
- **Management-Tier:** [TODO: Beschreibung]

6.8.2 Zugriffskontrolle

- **Authentifizierung:** [TODO: z.B. SSO, MFA]
- **Autorisierung:** [TODO: z.B. RBAC, ABAC]
- **Verschlüsselung:** [TODO: z.B. TLS 1.3, AES-256]

6.8.3 Security-Komponenten

- **WAF:** [TODO: Web Application Firewall]
- **IDS/IPS:** [TODO: Intrusion Detection/Prevention]
- **SIEM:** [TODO: Security Information and Event Management]

6.9 Verantwortlichkeiten

Rolle	Verantwortung	Person	Kontakt
System-Architekt	Architektur-Design	[TODO: Name]	[TODO: E-Mail]
Technical Lead	Technische Umsetzung	[TODO: Name]	[TODO: E-Mail]
Operations Manager	Betrieb und Wartung	Andreas Huemmer	andreas.huemmer@adminsends.de
Security Officer	Sicherheitsarchitektur	Thomas Weber	thomas.weber@adminsends.de

6.10 Kontakte

Bei Fragen zur Systemarchitektur: - **System-Architekt:** [TODO: Name und Kontakt] - **IT Operations Manager:** Andreas Huemmer (andreas.huemmer@adminsends.de) - **CISO:** Thomas Weber (thomas.weber@adminsends.de)

Dokumentverantwortlicher: IT Operations Manager

Genehmigt durch: CIO

Version: 1.0.0

Organisation: AdminSend GmbH

ewpage

Chapter 7

Infrastruktur und Plattform

7.1 Überblick

7.1.1 Infrastrukturlandschaft

Dieses Kapitel beschreibt die physische und virtuelle Infrastruktur, auf der die IT-Services betrieben werden.

Organisation: AdminSend GmbH

Standort: München, Deutschland

Kurzbeschreibung: [TODO: Beschreiben Sie die Infrastrukturlandschaft in 2-3 Sätzen. Welche Hauptkomponenten gibt es? Wo wird die Infrastruktur betrieben?]

7.1.2 Infrastruktur-Übersicht

Kategorie	Anzahl	Typ	Standort	Kritikalität		
Physische Server	[TODO]	[TODO: Rack/Blade]	[TODO]	L	M	H
Virtuelle Maschinen	[TODO]	[TODO: VMware/Hyper-V]	[TODO]	L	M	H
Container	[TODO]	[TODO: Docker/K8s]	[TODO]	L	M	H
Cloud-Instanzen	[TODO]	[TODO: AWS/Azure/GCP]	[TODO]	L	M	H
Netzwerkgeräte	[TODO]	[TODO: Switch/Router]	[TODO]	L	M	H
Storage-Systeme	[TODO]	[TODO: SAN/NAS]	[TODO]	L	M	H

Legende: - **L:** Low (Niedrig) - **M:** Medium (Mittel) - **H:** High (Hoch)

7.2 Physische Infrastruktur

7.2.1 Rechenzentren und Standorte

7.2.1.1 Primärer Standort

- **Standort-Name:** {{ netbox.site.name }}
- **Adresse:** {{ netbox.site.physical_address }}
- **Rechenzentrum:** {{ netbox.site.facility }}
- **Betreiber:** [TODO: RZ-Betreiber]
- **Zertifizierungen:** [TODO: z.B. ISO 27001, Tier III]

Standort-Details: - **Verfügbarkeit:** [TODO: z.B. 99.99%] - **Stromversorgung:** [TODO: z.B. Redundante USV, Notstrom] - **Kühlung:** [TODO: z.B. Redundante Klimatisierung] - **Brandschutz:** [TODO: z.B. Gaslöschanlage] - **Zutrittskontrolle:** [TODO: z.B. Biometrisch, 24/7 Überwachung]

7.2.1.2 Sekundärer Standort (DR)

- **Standort-Name:** [TODO: DR-Standort]
- **Adresse:** [TODO: Adresse]
- **Rechenzentrum:** [TODO: RZ-Name]
- **Betreiber:** [TODO: RZ-Betreiber]
- **Entfernung zum Primärstandort:** [TODO: km]

DR-Konfiguration: - **DR-Strategie:** [TODO: Hot/Warm/Cold Standby] - **Replikation:** [TODO: Synchron/Asynchron] - **RTO:** [TODO: Stunden] - **RPO:** [TODO: Stunden]

7.2.2 Rack-Übersicht

Rack-ID	Standort	Höhe (HE)	Belegung	Stromversorgung	Netzwerk
[TODO: RACK-01]	{{ netbox.site.name }}	[TODO: 42]	[TODO: 80%]	[TODO: 2x 32A]	[TODO: 2x 10G]
[TODO: RACK-02]	{{ netbox.site.name }}	[TODO: 42]	[TODO: 60%]	[TODO: 2x 32A]	[TODO: 2x 10G]
[TODO: RACK-03]	{{ netbox.site.name }}	[TODO: 42]	[TODO: 40%]	[TODO: 2x 16A]	[TODO: 2x 1G]

7.2.3 Server-Hardware

Hostname	Typ	CPU	RAM	Storage	Standort	Rack	Rolle
{{ netbox.device.serial }}	[TODO: Dell R740]	[TODO: 2x Xeon]	[TODO: 256GB]	[TODO: 2TB SSD]	{{ netbox.site.name }}	[TODO: RACK-01]	[TODO: Hypervisor]

Hostname	Typ	CPU	RAM	Storage	Standort	Rack	Rolle
{{ net-box.device.server02.name }}	[TODO: DL380]	[TODO: 2x Xeon]	[TODO: 128GB]	[TODO: 1TB SSD]	{{ net-box.site.name }}	[TODO: RACK-01]	[TODO: Hypervisor]
{{ net-box.device.server03.name }}	[TODO: DL380]	[TODO: 2x Xeon]	[TODO: 64GB]	[TODO: 500GB SSD]	{{ net-box.site.name }}	[TODO: RACK-02]	[TODO: Application]

Hardware-Lifecycle: - **Beschaffung:** [TODO: Prozess] - **Garantie:** [TODO: z.B. 5 Jahre NBD]
- **Refresh-Zyklus:** [TODO: z.B. 5 Jahre] - **End-of-Life:** [TODO: Prozess]

7.3 Netzwerkinfrastruktur

7.3.1 Netzwerkarchitektur

Netzwerk-Topologie: [TODO: z.B. Spine-Leaf, Three-Tier]

Redundanz: [TODO: z.B. Vollständig redundant, N+1]

7.3.2 Core-Netzwerk

Gerät	Typ	Modell	Standort	Rolle	Uplinks
{{ net-box.device.core_switch01.name }}	Core Switch	[TODO: Cisco Nexus]	{{ net-box.site.name }}	[TODO: Core]	[TODO: 4x 100G]
{{ net-box.device.core_switch02.name }}	Core Switch	[TODO: Cisco Nexus]	{{ net-box.site.name }}	[TODO: Core]	[TODO: 4x 100G]

7.3.3 Distribution-Layer

Gerät	Typ	Modell	Standort	Rolle	Uplinks
[TODO: DIST-SW-01]	Distribution Switch	[TODO: Modell]	{{ net-box.site.name }}	[TODO: Distribution]	[TODO: 2x 40G]
[TODO: DIST-SW-02]	Distribution Switch	[TODO: Modell]	{{ net-box.site.name }}	[TODO: Distribution]	[TODO: 2x 40G]

7.3.4 Access-Layer

Gerät	Typ	Modell	Standort	Ports	Uplinks
[TODO: ACC-SW-01]	Access Switch	[TODO: Modell]	{{ net- box.site.name }}	[TODO: 48x 1G]	[TODO: 2x 10G]
[TODO: ACC-SW-02]	Access Switch	[TODO: Modell]	{{ net- box.site.name }}	[TODO: 48x 1G]	[TODO: 2x 10G]

7.3.5 VLAN-Segmentierung

VLAN-ID	Name	Zweck	Subnetz	Gateway
{{ net- box.vlan.management.vid }}	Management	[TODO: Management- Netz]	{{ net- box.vlan.management.vid }}	[TODO: Gateway]
{{ net- box.vlan.production.vid }}	Production	[TODO: Produktions- Netz]	{{ net- box.vlan.production.vid }}	[TODO: Gateway]
[TODO: 30]	DMZ	[TODO: DMZ-Netz]	[TODO: 10.0.30.0/24]	[TODO: 10.0.30.1]
[TODO: 40]	Storage	[TODO: Storage-Netz]	[TODO: 10.0.40.0/24]	[TODO: 10.0.40.1]
[TODO: 50]	Backup	[TODO: Backup-Netz]	[TODO: 10.0.50.0/24]	[TODO: 10.0.50.1]

7.3.6 IP-Adressierung

IP-Adressplan:

Netzwerk	Verwendung	CIDR	Verfügbare IPs	Belegung
[TODO: 10.0.0.0/16]	Gesamt	[TODO: /16]	[TODO: 65534]	[TODO: 40%]
[TODO: 10.0.10.0/24]	Management	[TODO: /24]	[TODO: 254]	[TODO: 60%]
[TODO: 10.0.20.0/24]	Production	[TODO: /24]	[TODO: 254]	[TODO: 80%]
[TODO: 10.0.30.0/24]	DMZ	[TODO: /24]	[TODO: 254]	[TODO: 30%]

IPAM (IP Address Management): - **Tool:** [TODO: z.B. NetBox, phpIPAM] - **Verantwortlich:** Andreas Huemmer

7.3.7 Firewall und Security

Gerät	Typ	Modell	Standort	Rolle	Durchsatz
[TODO: FW-01]	Firewall	[TODO: Palo Alto]	{{ net-box.site.name }}	[TODO: Perimeter]	[TODO: 10 Gbps]
[TODO: FW-02]	Firewall	[TODO: Palo Alto]	{{ net-box.site.name }}	[TODO: Perimeter]	[TODO: 10 Gbps]

Firewall-Regeln: - **Anzahl Regeln:** [TODO: z.B. 500] - **Review-Zyklus:** [TODO: z.B. Quartalsweise] - **Verantwortlich:** Thomas Weber

7.3.8 Load Balancer

Gerät	Typ	Modell	Standort	Algorithmus	Kapazität
[TODO: LB-01]	Load Balancer	[TODO: F5/HAProxy]	{{ net-box.site.name }}	[TODO: Round-Robin]	[TODO: 10k RPS]
[TODO: LB-02]	Load Balancer	[TODO: F5/HAProxy]	{{ net-box.site.name }}	[TODO: Round-Robin]	[TODO: 10k RPS]

7.3.9 WAN-Verbindungen

Provider	Typ	Bandbreite	Standort	SLA	Kosten/Monat
[TODO: Provider 1]	[TODO: MPLS]	[TODO: 1 Gbps]	{{ net-box.site.name }}	[TODO: 99.9%]	[TODO: EUR]
[TODO: Provider 2]	[TODO: Internet]	[TODO: 500 Mbps]	{{ net-box.site.name }}	[TODO: 99.5%]	[TODO: EUR]

7.4 Virtualisierung

7.4.1 Virtualisierungsplattform

Hypervisor: [TODO: z.B. VMware vSphere 8.0, Microsoft Hyper-V, KVM]

Management: [TODO: z.B. vCenter Server, SCVMM]

7.4.2 Cluster-Konfiguration

Cluster-Name	Hypervisor	Hosts	vCPUs	RAM (GB)	Storage (TB)	VMs
{{ net-box.cluster.prod.name }}	[TODO: VMware]	[TODO: 4]	[TODO: 128]	[TODO: 1024]	[TODO: 50]	[TODO: 80]
{{ net-box.cluster.test.name }}	[TODO: VMware]	[TODO: 2]	[TODO: 64]	[TODO: 512]	[TODO: 20]	[TODO: 40]

Cluster-Features: - **HA (High Availability):** [TODO: Ja/Nein, Konfiguration] - **DRS (Distributed Resource Scheduler):** [TODO: Ja/Nein, Modus] - **vMotion/Live Migration:** [TODO: Ja/Nein] - **Fault Tolerance:** [TODO: Ja/Nein]

7.4.3 Virtuelle Maschinen

VM-Name	Cluster	vCPU	RAM (GB)	Storage (GB)	OS	Rolle	Status
{{ net-box.vm.app01.name }}	{{ net-box.cluster.prod.name }}	[TODO: 4]	[TODO: 16]	[TODO: 200]	[TODO: Ubuntu 22.04]	[TODO: App-Server]	[TODO: Running]
{{ net-box.vm.db01.name }}	{{ net-box.cluster.prod.name }}	[TODO: 8]	[TODO: 32]	[TODO: 500]	[TODO: RHEL 9]	[TODO: DB-Server]	[TODO: Running]
{{ net-box.vm.web01.name }}	{{ net-box.cluster.prod.name }}	[TODO: 2]	[TODO: 8]	[TODO: 100]	[TODO: Ubuntu 22.04]	[TODO: Web-Server]	[TODO: Running]

VM-Lifecycle: - **Provisioning:** [TODO: Automatisiert/Manuell, Tool] - **Template-Management:** [TODO: Prozess] - **Snapshot-Policy:** [TODO: Richtlinie] - **Decommissioning:** [TODO: Prozess]

7.4.4 Resource Pools

Pool-Name	Cluster	CPU-Shares	RAM-Reservation	Zweck
[TODO: Production]	{{ net-box.cluster.prod.name }}	[TODO: High]	[TODO: 50%]	[TODO: Produktions-VMs]
[TODO: Development]	{{ net-box.cluster.test.name }}	[TODO: Normal]	[TODO: 25%]	[TODO: Entwicklungs-VMs]
[TODO: Test]	{{ net-box.cluster.test.name }}	[TODO: Low]	[TODO: 10%]	[TODO: Test-VMs]

7.5 Container-Orchestrierung

7.5.1 Kubernetes-Cluster

Kubernetes-Version: [TODO: z.B. 1.28.x]

Distribution: [TODO: z.B. Vanilla K8s, OpenShift, Rancher, EKS, AKS, GKE]

Cluster-Name	Umgebung	Nodes	Pods	Namespaces	Ingress
[TODO: k8s-prod]	Production	[TODO: 6]	[TODO: 200]	[TODO: 20]	[TODO: Nginx]
[TODO: k8s-test]	Test	[TODO: 3]	[TODO: 50]	[TODO: 10]	[TODO: Nginx]

7.5.2 Node-Konfiguration

Node-Name	Rolle	CPU	RAM (GB)	Storage (GB)	Status
[TODO: k8s-master-01]	Control Plane	[TODO: 4]	[TODO: 16]	[TODO: 100]	[TODO: Ready]
[TODO: k8s-worker-01]	Worker	[TODO: 8]	[TODO: 32]	[TODO: 200]	[TODO: Ready]
[TODO: k8s-worker-02]	Worker	[TODO: 8]	[TODO: 32]	[TODO: 200]	[TODO: Ready]

7.5.3 Container-Registry

- **Registry:** [TODO: z.B. Harbor, Docker Hub, ECR, ACR, GCR]
- **URL:** [TODO: registry.example.com]
- **Authentifizierung:** [TODO: z.B. LDAP, OAuth2]
- **Scanning:** [TODO: z.B. Trivy, Clair]

7.5.4 Helm-Charts

- **Chart-Repository:** [TODO: URL]
- **Anzahl Charts:** [TODO: z.B. 50]
- **Versionierung:** [TODO: Prozess]

7.6 Cloud-Infrastruktur

7.6.1 Cloud-Provider

Primärer Cloud-Provider: [TODO: z.B. AWS, Azure, Google Cloud]

Cloud-Strategie: [TODO: z.B. Cloud-First, Hybrid, Multi-Cloud]

7.6.2 Cloud-Accounts

Account-Name	Provider	Account-ID	Umgebung	Zweck	Kosten/Monat
[TODO: prod-account]	[TODO: AWS]	[TODO: 123456789012]	Production	[TODO: Produktions-Workloads]	[TODO: EUR]
[TODO: dev-account]	[TODO: AWS]	[TODO: 987654321098]	Development	[TODO: Entwicklung/Test]	[TODO: EUR]

7.6.3 Cloud-Regionen

Region	Provider	Standort	Zweck	Services
[TODO: eu-central-1]	[TODO: AWS]	Frankfurt	[TODO: Primary]	[TODO: EC2, RDS, S3]
[TODO: eu-west-1]	[TODO: AWS]	Irland	[TODO: DR]	[TODO: EC2, RDS, S3]

7.6.4 Cloud-Ressourcen

7.6.4.1 Compute (IaaS)

Ressource	Typ	Größe	Anzahl	Region	Zweck	Kosten/Monat
[TODO: EC2 Instances]	[TODO: t3.large]	[TODO: 2vCPU/8GB]	[TODO: 10]	[TODO: eu-central-1]	[TODO: App-Server]	[TODO: EUR]
[TODO: Lambda Functions]	[TODO: Serverless]	[TODO: -]	[TODO: 50]	[TODO: eu-central-1]	[TODO: Microservices]	[TODO: EUR]

7.6.4.2 Storage

Ressource	Typ	Größe (TB)	Region	Zweck	Kosten/Monat
[TODO: S3 Buckets]	[TODO: Object Storage]	[TODO: 10]	[TODO: eu-central-1]	[TODO: Backups]	[TODO: EUR]
[TODO: EBS Volumes]	[TODO: Block Storage]	[TODO: 5]	[TODO: eu-central-1]	[TODO: VM-Storage]	[TODO: EUR]

7.6.4.3 Database (PaaS)

Ressource	Typ	Größe	Region	Zweck	Kosten/Monat
[TODO: RDS PostgreSQL]	[TODO: db.r5.large]	[TODO: 500GB]	[TODO: eu-central-1]	[TODO: Produktions-DB]	[TODO: EUR]
[TODO: DynamoDB]	[TODO: NoSQL]	[TODO: On-Demand]	[TODO: eu-central-1]	[TODO: Session-Store]	[TODO: EUR]

7.6.4.4 Networking

Ressource	Typ	Konfiguration	Region	Zweck
[TODO: VPC]	[TODO: Virtual Network]	[TODO: 10.0.0.0/16]	[TODO: eu-central-1]	[TODO: Netzwerk-Isolation]
[TODO: VPN Gateway]	[TODO: Site-to-Site VPN]	[TODO: 1 Gbps]	[TODO: eu-central-1]	[TODO: Hybrid-Connectivity]
[TODO: Direct Connect]	[TODO: Dedicated Line]	[TODO: 10 Gbps]	[TODO: eu-central-1]	[TODO: Low-Latency]

7.6.5 Cloud-Kosten

Gesamtkosten/Monat: [TODO: EUR]

Kostenoptimierung: - **Reserved Instances:** [TODO: Prozentsatz] - **Spot Instances:** [TODO: Prozentsatz] - **Auto-Scaling:** [TODO: Ja/Nein] - **Cost-Monitoring:** [TODO: Tool]

7.7 Storage-Infrastruktur

7.7.1 Storage-Systeme

System	Typ	Kapazität (TB)	Nutzung (%)	Protokoll	Standort	Zweck
[TODO: SAN-01]	SAN	[TODO: 100]	[TODO: 70%]	[TODO: FC/iSCSI]	{{ net-box.site.name}}	[TODO: VM-Storage]
[TODO: NAS-01]	NAS	[TODO: 50]	[TODO: 60%]	[TODO: NFS/CIFS]	{{ net-box.site.name}}	[TODO: File-Shares]
[TODO: OBJ-01]	Object Storage	[TODO: 200]	[TODO: 40%]	[TODO: S3]	[TODO: Cloud]	[TODO: Backups]

7.7.2 Storage-Tiers

Tier	Typ	Performance	Kapazität (TB)	Kosten/TB	Verwendung
Tier 0	[TODO: NVMe SSD]	[TODO: >100k IOPS]	[TODO: 10]	[TODO: Hoch]	[TODO: Datenbanken]
Tier 1	[TODO: SAS SSD]	[TODO: 50k IOPS]	[TODO: 50]	[TODO: Mittel]	[TODO: VMs]
Tier 2	[TODO: SAS HDD]	[TODO: 5k IOPS]	[TODO: 100]	[TODO: Niedrig]	[TODO: Archive]

7.7.3 Storage-Netzwerk

SAN-Fabric: - Protokoll: [TODO: z.B. Fibre Channel 32G, iSCSI 10G] - **Switches:** [TODO: z.B. Brocade, Cisco MDS] - **Redundanz:** [TODO: z.B. Dual-Fabric]

NAS-Netzwerk: - Protokoll: [TODO: z.B. NFS v4, SMB 3.0] - **Netzwerk:** [TODO: z.B. Dedi-ziertes 10G-Netzwerk]

7.7.4 Backup-Storage

System	Typ	Kapazität (TB)	Retention	Standort	Zweck
[TODO: BACKUP-01]	[TODO: Disk]	[TODO: 100]	[TODO: 30 Tage]	{{ net-box.site.name }}	[TODO: Disk-Backup]
[TODO: TAPE-01]	[TODO: Tape Library]	[TODO: 500]	[TODO: 7 Jahre]	{{ net-box.site.name }}	[TODO: Langzeit-Archiv]
[TODO: CLOUD-BACKUP]	[TODO: Cloud]	[TODO: Unlimited]	[TODO: 90 Tage]	[TODO: Cloud]	[TODO: Off-Site-Backup]

7.8 Stromversorgung

7.8.1 Primäre Stromversorgung

- **Anschlussleistung:** [TODO: z.B. 200 kW]
- **Redundanz:** [TODO: z.B. N+1, 2N]
- **Provider:** [TODO: Energieversorger]

7.8.2 USV (Unterbrechungsfreie Stromversorgung)

USV-System	Kapazität (kVA)	Laufzeit (min)	Standort	Status
[TODO: USV-01]	[TODO: 100]	[TODO: 15]	{{ net-box.site.name }}	[TODO: Online]

USV-System	Kapazität (kVA)	Laufzeit (min)	Standort	Status
[TODO: USV-02]	[TODO: 100]	[TODO: 15]	{{ net- box.site.name }}	[TODO: Online]

USV-Wartung: - **Wartungsintervall:** [TODO: z.B. Quartalsweise] - **Batterietest:** [TODO: z.B. Monatlich] - **Verantwortlich:** [TODO: Facility-Management]

7.8.3 Notstromversorgung

- **Notstromaggregat:** [TODO: z.B. 250 kVA Diesel]
- **Kraftstoffvorrat:** [TODO: z.B. 1000 Liter]
- **Laufzeit:** [TODO: z.B. 48 Stunden]
- **Umschaltzeit:** [TODO: z.B. < 10 Sekunden]

7.9 Kühlung und Klimatisierung

7.9.1 Klimatisierung

- **Kühlleistung:** [TODO: z.B. 150 kW]
- **Redundanz:** [TODO: z.B. N+1]
- **Zieltemperatur:** [TODO: z.B. 22°C ±2°C]
- **Luftfeuchtigkeit:** [TODO: z.B. 45% ±5%]

7.9.2 Monitoring

- **Temperatur-Sensoren:** [TODO: Anzahl und Positionen]
- **Luftfeuchtigkeits-Sensoren:** [TODO: Anzahl und Positionen]
- **Alarmer:** [TODO: Schwellwerte und Eskalation]

7.10 Physische Sicherheit

7.10.1 Zutrittskontrolle

- **System:** [TODO: z.B. Biometrisch, Chipkarte]
- **Zutrittsberechtigte:** [TODO: Anzahl Personen]
- **Protokollierung:** [TODO: Aufbewahrungsdauer]
- **Vier-Augen-Prinzip:** [TODO: Ja/Nein, für welche Bereiche]

7.10.2 Videoüberwachung

- **Kameras:** [TODO: Anzahl und Positionen]
- **Aufzeichnung:** [TODO: Aufbewahrungsdauer]
- **Überwachung:** [TODO: 24/7 oder zeitgesteuert]

7.10.3 Brandschutz

- **Brandmeldeanlage:** [TODO: Typ]

- **Löschanlage:** [TODO: z.B. Gaslöschanlage, Sprinkler]
- **Brandabschnitte:** [TODO: Anzahl]
- **Fluchtwege:** [TODO: Anzahl und Kennzeichnung]

7.11 Kapazitätsplanung

7.11.1 Aktuelle Auslastung

Ressource	Kapazität	Genutzt	Verfügbar	Auslastung (%)	Schwellwert (%)
CPU (Cores)	[TODO: 500]	[TODO: 300]	[TODO: 200]	[TODO: 60%]	[TODO: 80%]
RAM (GB)	[TODO: 4000]	[TODO: 2800]	[TODO: 1200]	[TODO: 70%]	[TODO: 85%]
Storage (TB)	[TODO: 200]	[TODO: 140]	[TODO: 60]	[TODO: 70%]	[TODO: 80%]
Netzwerk (Gbps)	[TODO: 100]	[TODO: 40]	[TODO: 60]	[TODO: 40%]	[TODO: 70%]

7.11.2 Wachstumsprognose

Prognosezeitraum: [TODO: z.B. 12 Monate]

Ressource	Aktuell	Prognose (+12M)	Wachstum (%)	Maßnahmen
CPU	[TODO: 300 Cores]	[TODO: 360 Cores]	[TODO: +20%]	[TODO: Beschreibung]
RAM	[TODO: 2800 GB]	[TODO: 3360 GB]	[TODO: +20%]	[TODO: Beschreibung]
Storage	[TODO: 140 TB]	[TODO: 182 TB]	[TODO: +30%]	[TODO: Beschreibung]

7.11.3 Skalierungsstrategien

Vertikale Skalierung: - [TODO: Beschreibung der Strategie] - [TODO: Maximale Grenzen]

Horizontale Skalierung: - [TODO: Beschreibung der Strategie] - [TODO: Auto-Scaling-Konfiguration]

Cloud-Bursting: - [TODO: Ja/Nein, Beschreibung]

7.12 Lifecycle-Management

7.12.1 Hardware-Lifecycle

Phase	Dauer	Aktivitäten	Verantwortlich
Beschaffung	[TODO: 4-8 Wochen]	[TODO: Anforderung, Bestellung, Lieferung]	Andreas Huemmer
Inbetriebnahme	[TODO: 1-2 Wochen]	[TODO: Installation, Konfiguration, Tests]	[TODO: Team]
Betrieb	[TODO: 5 Jahre]	[TODO: Monitoring, Wartung, Support]	[TODO: Team]
Refresh	[TODO: 1-2 Wochen]	[TODO: Migration, Austausch]	[TODO: Team]
Entsorgung	[TODO: 1 Woche]	[TODO: Datenlöschung, Recycling]	[TODO: Team]

7.12.2 Software-Lifecycle

Phase	Dauer	Aktivitäten	Verantwortlich
Evaluation	[TODO: 2-4 Wochen]	[TODO: Anforderungsanalyse, PoC]	[TODO: Team]
Beschaffung	[TODO: 2-4 Wochen]	[TODO: Lizenzierung, Verträge]	[TODO: Team]
Implementierung	[TODO: 4-8 Wochen]	[TODO: Installation, Konfiguration]	[TODO: Team]
Betrieb	[TODO: 3-5 Jahre]	[TODO: Support, Updates]	[TODO: Team]
Ablösung	[TODO: 8-12 Wochen]	[TODO: Migration, Decommissioning]	[TODO: Team]

7.12.3 End-of-Life-Management

Hardware: - **Datenlöschung:** [TODO: Prozess, z.B. DoD 5220.22-M] - **Zertifikat:** [TODO: Ja/Nein] - **Recycling:** [TODO: Zertifizierter Partner]

Software: - **Lizenz-Rückgabe:** [TODO: Prozess] - **Datenexport:** [TODO: Prozess] - **Dokumentation:** [TODO: Archivierung]

7.13 Compliance und Zertifizierungen

7.13.1 Rechenzentrum-Zertifizierungen

- **ISO 27001:** [TODO: Ja/Nein, Gültig bis]
- **ISO 9001:** [TODO: Ja/Nein, Gültig bis]
- **Tier-Zertifizierung:** [TODO: Tier I/II/III/IV]
- **PCI-DSS:** [TODO: Ja/Nein, Level]

7.13.2 Compliance-Anforderungen

- **DSGVO:** [TODO: Maßnahmen]
- **BSI Grundschutz:** [TODO: Ja/Nein, Baustein]
- **KRITIS:** [TODO: Ja/Nein, Sektor]

7.14 Verantwortlichkeiten

Rolle	Verantwortung	Person	Kontakt
Infrastructure Manager	Gesamtverantwortung Infrastruktur	Andreas Huemmer	andreas.huemmer@adminsends.de
Network Administrator	Netzwerkinfrastruktur	[TODO: Name]	[TODO: E-Mail]
Storage Administrator	Storage-Systeme	[TODO: Name]	[TODO: E-Mail]
Virtualization Admin	Virtualisierung	[TODO: Name]	[TODO: E-Mail]
Cloud Architect	Cloud-Infrastruktur	[TODO: Name]	[TODO: E-Mail]
Facility Manager	Physische Infrastruktur	[TODO: Name]	[TODO: E-Mail]

7.15 Kontakte

Bei Fragen zur Infrastruktur: - **IT Operations Manager:** Andreas Huemmer (andreas.huemmer@adminsends.de) - **CIO:** Anna Schmidt (anna.schmidt@adminsends.de)

Notfallkontakte: - **Rechenzentrum:** [TODO: Telefon 24/7] - **Stromversorger:** [TODO: Telefon] - **Facility Management:** [TODO: Telefon]

Dokumentverantwortlicher: IT Operations Manager

Genehmigt durch: CIO

Version: 1.0.0

Organisation: AdminSend GmbH

ewpage

Chapter 8

Rollen und Verantwortlichkeiten

8.1 Organisationsstruktur

8.1.1 Unternehmensinformationen

- **Organisation:** AdminSend GmbH
- **Adresse:** Musterstraße 123, 80331 München
- **Land:** Deutschland
- **Website:** <https://www.adminsend.de>
- **Telefon:** +49 89 12345678
- **E-Mail:** info@adminsend.de

8.1.2 Organisationsübersicht

[TODO: Fügen Sie hier ein Organigramm oder eine Beschreibung der Organisationsstruktur ein]

8.2 Führungsebene

8.2.1 Chief Executive Officer (CEO)

- **Name:** Max Mustermann
- **Titel:** Chief Executive Officer
- **E-Mail:** max.mustermann@adminsend.de
- **Telefon:** +49 89 12345678-100
- **Abteilung:** Management

Verantwortlichkeiten: - Gesamtverantwortung für das Unternehmen - Strategische Ausrichtung und Unternehmensziele - Genehmigung kritischer IT-Investitionen - Eskalationspunkt für geschäftskritische IT-Vorfälle

8.2.2 Chief Information Officer (CIO)

- **Name:** Anna Schmidt
- **Titel:** Chief Information Officer
- **E-Mail:** anna.schmidt@adminsend.de
- **Telefon:** +49 89 12345678-200

- **Abteilung:** IT

Verantwortlichkeiten: - Gesamtverantwortung für IT-Strategie und -Betrieb - IT-Budget und Ressourcenplanung - IT-Governance und Compliance - Genehmigung von Major Changes - Verantwortung für IT-Service-Qualität und SLA-Einhaltung

8.2.3 Chief Information Security Officer (CISO)

- **Name:** Thomas Weber
- **Titel:** Chief Information Security Officer
- **E-Mail:** thomas.weber@adminsends.de
- **Telefon:** +49 89 12345678-300
- **Abteilung:** IT Security

Verantwortlichkeiten: - IT-Sicherheitsstrategie und -Richtlinien - Informationssicherheits-Management (ISMS) - Security Incident Response - Compliance mit Sicherheitsstandards (ISO 27001, BSI Grundschutz) - Risikomanagement und Vulnerability Management - Security Awareness und Training

8.2.4 Chief Financial Officer (CFO)

- **Name:** Maria Müller
- **Titel:** Chief Financial Officer
- **E-Mail:** maria.mueller@adminsends.de
- **Telefon:** +49 89 12345678-400
- **Abteilung:** Finance

Verantwortlichkeiten: - Finanzielle Genehmigung von IT-Projekten - IT-Budget-Überwachung - Kosten-Nutzen-Analysen für IT-Investitionen - Finanzielle Compliance und Audits

8.2.5 Chief Operating Officer (COO)

- **Name:** Peter Fischer
- **Titel:** Chief Operating Officer
- **E-Mail:** peter.fischer@adminsends.de
- **Telefon:** +49 89 12345678-500
- **Abteilung:** Operations

Verantwortlichkeiten: - Operative Geschäftsprozesse - Business Continuity Management - Koordination zwischen IT und Geschäftsbereichen - Service-Level-Anforderungen aus Geschäftssicht

8.3 IT-Betriebsebene

8.3.1 IT Operations Manager

- **Name:** Andreas Huemmer
- **Titel:** IT Operations Manager
- **E-Mail:** andreas.huemmer@adminsends.de
- **Telefon:** +49 89 12345678-250
- **Abteilung:** IT Operations

Verantwortlichkeiten: - Täglicher IT-Betrieb und Service Delivery - Monitoring und Incident Management - Change Management Koordination - Kapazitäts- und Performance-Management - Team-Führung IT Operations - Eskalationsmanagement für operative Vorfälle - Sicherstellung der SLA-Einhaltung

Vertretung: [TODO: Name und Kontakt der Vertretung]

8.3.2 Service Desk Lead

- **Name:** Julia Becker
- **Titel:** Service Desk Lead
- **E-Mail:** julia.becker@adminsind.de
- **Telefon:** +49 89 12345678-111
- **Abteilung:** Service Desk

Verantwortlichkeiten: - First-Level-Support und Incident Management - Ticket-Management und Priorisierung - Nutzer-Kommunikation - Service-Katalog-Pflege - Team-Führung Service Desk - Service-Desk-Metriken und Reporting

Vertretung: [TODO: Name und Kontakt der Vertretung]

8.4 Weitere IT-Rollen

8.4.1 System Administrator

- **Name:** [TODO: Name]
- **E-Mail:** [TODO: E-Mail]
- **Telefon:** [TODO: Telefon]

Verantwortlichkeiten: - Server- und Systemadministration - Patch- und Update-Management - Backup und Restore - System-Monitoring - Dokumentation der Systemkonfigurationen

8.4.2 Network Administrator

- **Name:** [TODO: Name]
- **E-Mail:** [TODO: E-Mail]
- **Telefon:** [TODO: Telefon]

Verantwortlichkeiten: - Netzwerkinfrastruktur-Management - Firewall- und Security-Konfiguration - Netzwerk-Monitoring - VPN- und Remote-Access-Management - Netzwerk-Dokumentation

8.4.3 Database Administrator (DBA)

- **Name:** [TODO: Name]
- **E-Mail:** [TODO: E-Mail]
- **Telefon:** [TODO: Telefon]

Verantwortlichkeiten: - Datenbank-Administration und -Optimierung - Datenbank-Backup und Recovery - Performance-Tuning - Datenbank-Security - Datenbank-Monitoring

8.4.4 Application Manager

- **Name:** [TODO: Name]
- **E-Mail:** [TODO: E-Mail]
- **Telefon:** [TODO: Telefon]

Verantwortlichkeiten: - Applikations-Support und -Wartung - Release-Management für Applikationen - Applikations-Monitoring - Koordination mit Entwicklungsteams - Applikations-Dokumentation

8.4.5 Security Administrator

- **Name:** [TODO: Name]
- **E-Mail:** [TODO: E-Mail]
- **Telefon:** [TODO: Telefon]

Verantwortlichkeiten: - Security-Monitoring und Incident Response - Vulnerability-Scanning und -Management - Security-Patch-Management - Access-Management und Berechtigungen - Security-Audits und Compliance-Checks

8.5 RACI-Matrix für IT-Betriebsaktivitäten

Die RACI-Matrix definiert Verantwortlichkeiten für IT-Betriebsaktivitäten: - **R** = Responsible (Durchführungsverantwortung) - **A** = Accountable (Gesamtverantwortung, Entscheidungsbefugnis) - **C** = Consulted (Konsultiert, muss befragt werden) - **I** = Informed (Informiert, muss informiert werden)

8.5.1 Service Management

Aktivität	CEO	CIO	CISO	CFO	COO	Ops Man- ager	Service Desk	Sys Ad- min	Net Ad- min	DBA	App Man- ager	Sec Ad- min
ServiceA	R	C	C	C	C	C	I	I	I	I	I	I
Strategie												
ServiceI	A	C	I	C	R	C	C	C	C	C	C	C
Design												
ServiceI	A	C	I	C	R	C	R	R	R	R	R	C
Transition												
ServiceI	A	C	I	I	R	R	R	R	R	R	R	R
Operation												
Continual	A	C	I	C	R	C	C	C	C	C	C	C
Im- prove- ment												

8.5.2 Incident Management

Aktivität	CEO	CIO	CISO	CFO	COO	Ops Man- ager	Service Desk	Sys Ad- min	Net Ad- min	DBA	App Man- ager	Sec Ad- min
Incident-Erfassung		I	I	I	I	C	R	C	C	C	C	C
Incident-Klassifizierung		I	C	I	I	C	R	C	C	C	C	C
Incident-Diagnose		I	C	I	I	C	R	R	R	R	R	R
Incident-Lösung		I	C	I	I	A	C	R	R	R	R	R
Incident-Abschluss		I	I	I	I	A	R	C	C	C	C	C
Major Incident	I	A	C	I	C	R	R	R	R	R	R	R

8.5.3 Problem Management

Aktivität	CEO	CIO	CISO	CFO	COO	Ops Man- ager	Service Desk	Sys Ad- min	Net Ad- min	DBA	App Man- ager	Sec Ad- min
Problem-Identifikation		I	C	I	I	A	R	R	R	R	R	R
Problem-Analyse		I	C	I	I	A	C	R	R	R	R	R
Root-Cause-Analysis		I	I	C	I	I	A	C	R	R	R	R
Workaround-Entwicklung		I	C	I	I	A	C	R	R	R	R	R
Known-Error-Dokumentation		I	I	I	I	A	R	C	C	C	C	C
Problem-Lösung		A	C	I	I	R	C	R	R	R	R	R

8.5.4 Change Management

Aktivität	CEO	CIO	CISO	CFO	COO	Ops Man- ager	Service Desk	Sys Ad- min	Net Ad- min	DBA	App Man- ager	Sec Ad- min
Change-Request		I	C	I	I	C	C	R	R	R	R	R
Change-Bewertung		C	C	I	C	A	I	R	R	R	R	R
Change-Genehmigung (Standard)		I	I	I	I	A	I	I	I	I	I	I
Change-Genehmigung (Normal)		A	C	I	C	R	I	I	I	I	I	I
Change-Genehmigung (Emergency)		A	C	I	C	R	I	I	I	I	I	I
Change-Implementierung		I	C	I	I	A	I	R	R	R	R	R
Change-Review		A	C	I	I	R	C	C	C	C	C	C

8.5.5 Security Management

Aktivität	CEO	CIO	CISO	CFO	COO	Ops Man- ager	Service Desk	Sys Ad- min	Net Ad- min	DBA	App Man- ager	Sec Ad- min
Security-Strategie		C	R	C	C	C	I	I	I	I	I	I
Security-Richtlinien		C	R	I	C	C	I	C	C	C	C	C
Security-Monitoring		I	A	I	I	C	I	C	C	C	C	R
Security-Incident		A	R	I	C	C	C	C	C	C	C	R
Vulnerability-Management		I	A	I	I	C	I	C	C	C	C	R
Access-Management		I	A	I	I	C	C	R	R	R	R	R
Security-Audits		A	R	C	C	C	I	C	C	C	C	R

8.5.6 Backup und Recovery

Aktivität	CEO	CIO	CISO	CFO	COO	Ops Man- ager	Service Desk	Sys Ad- min	Net Ad- min	DBA	App Man- ager	Sec Ad- min
Backup-Strategie		A	C	I	C	R	I	C	C	C	C	C
Backup-Durchführung		I	I	I	I	A	I	R	C	R	C	I
Backup-Monitoring		I	I	I	I	A	I	R	C	R	C	I
Backup-Tests		I	C	I	I	A	I	R	C	R	C	C
Restore-Durchführung		I	C	I	I	A	C	R	C	R	C	C
Disaster-Recovery		A	C	I	C	R	C	R	R	R	R	C

8.5.7 Monitoring und Performance

Aktivität	CEO	CIO	CISO	CFO	COO	Ops Man- ager	Service Desk	Sys Ad- min	Net Ad- min	DBA	App Man- ager	Sec Ad- min
Monitoring-Strategie		A	C	I	C	R	I	C	C	C	C	C
Monitoring-Konfiguration		I	C	I	I	A	I	R	R	R	R	R
24/7-Monitoring		I	I	C	I	I	A	R	R	R	R	R
Alert-Management		I	I	C	I	I	A	R	R	R	R	R
Performance-Tuning		I	I	I	I	A	I	R	R	R	R	I
Kapazitätsplanung		I	I	C	C	R	I	C	C	C	C	I

8.5.8 Compliance und Audits

Aktivität	CEO	CIO	CISO	CFO	COO	Ops Man- ager	Service Desk	Sys Ad- min	Net Ad- min	DBA	App Man- ager	Sec Ad- min
Compliance-Strategie		R	C	C	C	C	I	I	I	I	I	I
Compliance-Kontrollen		A	R	C	C	C	I	C	C	C	C	C
Audit-Vorbereitung		I	A	R	C	C	R	C	C	C	C	C

Aktivität	CEO	CIO	CISO	CFO	COO	Ops Man- ager	Service Desk	Sys Ad- min	Net Ad- min	DBA	App Man- ager	Sec Ad- min
Audit-C Durchführung	A	R	C	C	R	C	C	C	C	C	C	C
Audit- I Nachbereitung	A	R	I	C	R	I	C	C	C	C	C	C

8.6 Kontaktlisten und Erreichbarkeiten

8.6.1 Führungsebene - Kontakte

Rolle	Name	E-Mail	Telefon	Mobil	Verfügbarkeit
CEO	Max Mustermann	max.mustermann@adm1n89.de	12345678-100	[TODO]	Mo-Fr 09:00-17:00
CIO	Anna Schmidt	anna.schmidt@adm1n89.de	12345678-200	[TODO]	Mo-Fr 08:00-18:00
CISO	Thomas Weber	thomas.weber@adm1n89.de	12345678-300	[TODO]	Mo-Fr 08:00-18:00
CFO	Maria Müller	maria.mueller@adm1n89.de	12345678-400	[TODO]	Mo-Fr 09:00-17:00
COO	Peter Fischer	peter.fischer@adm1n89.de	12345678-500	[TODO]	Mo-Fr 08:00-18:00

8.6.2 IT-Operations - Kontakte

Rolle	Name	E-Mail	Telefon	Mobil	Verfügbarkeit
IT Ops Manager	Andreas Huemmer	andreas.huemmer@adm1n89.de	12345678-250	[TODO]	Mo-Fr 07:00-19:00
Service Desk Lead	Julia Becker	julia.becker@adm1n89.de	12345678-111	[TODO]	Mo-Fr 08:00-17:00
System Admin	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]
Network Admin	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]
DBA	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]
App Manager	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]
Security Admin	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]

8.6.3 Service Desk - Kontakte

Zentrale Service-Desk-Nummer: [TODO: Telefonnummer]

Service-Desk-E-Mail: [TODO: E-Mail-Adresse]

Service-Portal: [TODO: URL]

Servicezeiten: - **Regulär:** Mo-Fr 08:00-17:00 Uhr - **Erweitert:** [TODO: Falls zutreffend] - **24/7:** [TODO: Falls zutreffend]

8.7 On-Call und Rufbereitschaft

8.7.1 Rufbereitschafts-Modell

Betriebsmodell: [TODO: 24/7, Business Hours, Follow-the-Sun]

Rufbereitschaftszeiten: - **Werktags:** [TODO: z.B. 17:00-08:00 Uhr] - **Wochenende:** [TODO: z.B. Fr 17:00 - Mo 08:00 Uhr] - **Feiertage:** [TODO: 24 Stunden]

8.7.2 Rufbereitschafts-Rotation

Woche	Primär	Sekundär	Eskalation
KW [TODO]	[TODO: Name]	[TODO: Name]	Andreas Huemmer
KW [TODO]	[TODO: Name]	[TODO: Name]	Andreas Huemmer
KW [TODO]	[TODO: Name]	[TODO: Name]	Andreas Huemmer
KW [TODO]	[TODO: Name]	[TODO: Name]	Andreas Huemmer

Rotationsplan: [TODO: Link zum aktuellen Rufbereitschaftsplan]

8.7.3 On-Call-Kontakte

Primäre Rufbereitschaft: - **Telefon:** [TODO: On-Call-Nummer] - **E-Mail:** [TODO: On-Call-E-Mail] - **Erreichbarkeit:** [TODO: Reaktionszeit]

Sekundäre Rufbereitschaft: - **Telefon:** [TODO: Backup-Nummer] - **E-Mail:** [TODO: Backup-E-Mail] - **Erreichbarkeit:** [TODO: Reaktionszeit]

Eskalation: - **IT Operations Manager:** Andreas Huemmer (+49 89 12345678-250) - **CIO:** Anna Schmidt (+49 89 12345678-200)

8.7.4 Rufbereitschafts-Prozess

1. Alarmierung: - Monitoring-System sendet Alert - Automatische Benachrichtigung an On-Call-Person - Kanäle: SMS, Telefon, E-Mail, Push-Notification

2. Reaktion: - **Reaktionszeit:** [TODO: z.B. 15 Minuten] - **Bestätigung:** On-Call-Person bestätigt Empfang - **Erste Analyse:** Innerhalb [TODO: z.B. 30 Minuten]

3. Eskalation: - **Level 1:** Primäre Rufbereitschaft (0-15 Min) - **Level 2:** Sekundäre Rufbereitschaft (15-30 Min) - **Level 3:** IT Operations Manager (30-60 Min) - **Level 4:** CIO (> 60 Min oder kritischer Vorfall)

4. Dokumentation: - Alle Aktivitäten im Ticket-System dokumentieren - Zeitstempel für alle Aktionen - Post-Incident-Review bei Major Incidents

8.7.5 Rufbereitschafts-Richtlinien

Verfügbarkeit: - On-Call-Person muss erreichbar sein - Reaktionszeit: [TODO: z.B. 15 Minuten]
- Zugriff auf Laptop und VPN erforderlich - Nüchternheit während Rufbereitschaft

Kompensation: - Rufbereitschaftspauschale: [TODO: Betrag] - Einsatzvergütung: [TODO: Stundensatz] - Freizeitausgleich: [TODO: Regelung]

Übergabe: - Übergabe-Call am Ende der Rufbereitschaft - Dokumentation offener Vorfälle - Briefing der nächsten On-Call-Person

8.8 Eskalationspfade

8.8.1 Standard-Eskalation

Level 1: Service Desk
↓ (15 Min)
Level 2: Fachspezialist (Sys/Net/DB/App Admin)
↓ (30 Min)
Level 3: IT Operations Manager
↓ (60 Min)
Level 4: CIO
↓ (kritisch)
Level 5: CEO

8.8.2 Security-Incident-Eskalation

Security Alert
↓ (sofort)
Security Administrator
↓ (15 Min)
CISO
↓ (30 Min bei Major Incident)
CIO + CEO
↓ (bei Datenschutzvorfall)
Datenschutzbeauftragter + Behörden

8.8.3 Business-Critical-Incident-Eskalation

Major Incident
↓ (sofort)
IT Operations Manager + On-Call
↓ (15 Min)
CIO + CISO
↓ (30 Min)
COO + CEO
↓ (bei Bedarf)
Externe Dienstleister + Hersteller

8.8.4 Eskalationskriterien

Automatische Eskalation bei: - Keine Reaktion innerhalb der definierten Zeit - Incident kann nicht gelöst werden - Mehrere kritische Systeme betroffen - Datenschutz- oder Security-Vorfall - Geschäftskritische Services ausgefallen

Eskalationszeiten: - **P1 (Kritisch):** 15 Min → 30 Min → 60 Min - **P2 (Hoch):** 30 Min → 60 Min → 2 Std - **P3 (Mittel):** 2 Std → 4 Std → 8 Std - **P4 (Niedrig):** 8 Std → 1 Tag → 2 Tage

8.9 Vertretungsregelungen

8.9.1 Führungsebene - Vertretungen

Rolle	Primär	Vertretung 1	Vertretung 2
CEO	Max Mustermann	[TODO: Name]	[TODO: Name]
CIO	Anna Schmidt	Andreas Huemmer	[TODO: Name]
CISO	Thomas Weber	[TODO: Name]	Anna Schmidt
CFO	Maria Müller	[TODO: Name]	[TODO: Name]
COO	Peter Fischer	[TODO: Name]	[TODO: Name]

8.9.2 IT-Operations - Vertretungen

Rolle	Primär	Vertretung 1	Vertretung 2
IT Ops Manager	Andreas Huemmer	[TODO: Name]	Anna Schmidt
Service Desk Lead	Julia Becker	[TODO: Name]	Andreas Huemmer
System Admin	[TODO: Name]	[TODO: Name]	[TODO: Name]
Network Admin	[TODO: Name]	[TODO: Name]	[TODO: Name]
DBA	[TODO: Name]	[TODO: Name]	[TODO: Name]

8.9.3 Vertretungsprozess

Bei geplanter Abwesenheit: 1. Vertretung mindestens [TODO: z.B. 1 Woche] im Voraus informieren 2. Übergabe-Dokumentation erstellen 3. Offene Themen und Vorfälle übergeben 4. Kontaktinformationen aktualisieren 5. Out-of-Office-Nachricht mit Vertretungskontakt

Bei ungeplanter Abwesenheit: 1. Vorgesetzten informieren 2. Automatische Vertretungsregelung greift 3. Vertretung übernimmt alle laufenden Aufgaben 4. Nachträgliche Übergabe bei Rückkehr

8.10 Schulung und Qualifikation

8.10.1 Erforderliche Qualifikationen

Rolle	Erforderliche Zertifizierungen	Empfohlene Schulungen
IT Ops Manager	ITIL Foundation, ITIL Managing Professional	COBIT, ISO 20000
Service Desk Lead	ITIL Foundation	ITIL Specialist, HDI Support Center Manager
System Admin	[TODO: z.B. MCSA, RHCSA]	[TODO: Hersteller-Zertifizierungen]
Network Admin	[TODO: z.B. CCNA, CCNP]	[TODO: Netzwerk-Sicherheit]
DBA	[TODO: z.B. Oracle DBA, MCDBA]	[TODO: Performance-Tuning]
Security Admin	[TODO: z.B. CISSP, CEH]	[TODO: Security-Frameworks]

8.10.2 Schulungsplan

Jährliche Pflichtschulungen: - IT-Sicherheit und Datenschutz (alle Mitarbeiter) - ITIL-Refresher (IT Operations Team) - Incident-Management-Prozesse (Service Desk) - Change-Management-Prozesse (alle IT-Mitarbeiter)

Individuelle Weiterbildung: - Budget: [TODO: Betrag pro Mitarbeiter/Jahr] - Genehmigung: IT Operations Manager / CIO - Dokumentation: Schulungsnachweise im Personalordner

8.11 Änderungshistorie

Version	Datum	Autor	Änderungen	Genehmigt durch
1.0.0	[TODO]	IT Operations Manager	Initiale Version	CIO

Dokumentverantwortlicher: IT Operations Manager

Genehmigt durch: CIO

Version: 1.0.0

Klassifizierung: internal

Organisation: AdminSend GmbH

ewpage

Chapter 9

Betriebskonzept und Betriebsprozesse

9.1 Übersicht

Dieses Dokument beschreibt das Betriebskonzept und die Betriebsprozesse für den IT-Service. Es definiert Betriebsmodelle, Prozessabläufe nach ITIL-Standards, Schnittstellen zu anderen Prozessen und Eskalationspfade.

Service: {{ meta.service_name }}

Verantwortlich: Andreas Huemmer

Stand: 1.0.0

9.2 Betriebsmodell

9.2.1 Servicezeiten

Betriebsmodell	Beschreibung	Servicezeiten
24/7 Betrieb	Durchgehender Betrieb ohne Unterbrechung	Mo-So, 00:00-24:00 Uhr
Business Hours	Betrieb während Geschäftszeiten	Mo-Fr, 08:00-18:00 Uhr
Extended Hours	Erweiterte Geschäftszeiten	Mo-Fr, 06:00-22:00 Uhr
Follow-the-Sun	Globaler Betrieb über Zeitzonen	24/7 mit regionaler Staffelung

Aktuelles Betriebsmodell: [TODO: Betriebsmodell auswählen]

9.2.2 Wartungsfenster

Typ	Zeitfenster	Frequenz	Dauer
Reguläre Wartung	[TODO: z.B. Sonntag 02:00-06:00]	[TODO: z.B. Monatlich]	[TODO: z.B. 4 Stunden]
Notfallwartung	Nach Bedarf	Ad-hoc	Variable
Patch-Fenster	[TODO: z.B. Dienstag 22:00-24:00]	[TODO: z.B. Wöchentlich]	[TODO: z.B. 2 Stunden]

9.2.3 Support-Modell

Support-Stufen: - **Level 1 (Service Desk):** Julia Becker - julia.becker@adminsends.de - **Level 2 (IT Operations):** Andreas Huemmer - andreas.huemmer@adminsends.de - **Level 3 (Specialist/Vendor):** [TODO: Spezialist-Kontakt]

Rufbereitschaft: - **On-Call Rotation:** [TODO: Rotationsplan beschreiben] - **Erreichbarkeit:** [TODO: Telefon/Pager-Nummer] - **Reaktionszeit:** [TODO: z.B. 15 Minuten]

9.3 ITIL-Prozesse

9.3.1 Service Strategy

Ziel: Strategische Ausrichtung der IT-Services an Geschäftsanforderungen

Aktivitäten: - Service Portfolio Management - Financial Management - Demand Management - Business Relationship Management

Verantwortlich: Anna Schmidt

9.3.2 Service Design

Ziel: Design neuer oder geänderter Services für den Produktivbetrieb

Aktivitäten: - Service Catalogue Management - Service Level Management - Capacity Management - Availability Management - IT Service Continuity Management - Information Security Management - Supplier Management

Verantwortlich: Andreas Huemmer

9.3.3 Service Transition

Ziel: Überführung neuer oder geänderter Services in den Produktivbetrieb

Aktivitäten: - Change Management (siehe Kapitel 0140) - Release and Deployment Management - Service Validation and Testing - Knowledge Management - Configuration Management (siehe Kapitel 0090)

Verantwortlich: Andreas Huemmer

9.3.4 Service Operation

Ziel: Sicherstellung des effektiven und effizienten Betriebs

Aktivitäten: - Incident Management (siehe Kapitel 0120) - Problem Management (siehe Kapitel 0130) - Event Management - Request Fulfillment - Access Management (siehe Kapitel 0100)

Verantwortlich: Julia Becker (Level 1), Andreas Huemmer (Level 2)

9.3.5 Continual Service Improvement (CSI)

Ziel: Kontinuierliche Verbesserung der Service-Qualität

Aktivitäten: - Service Measurement and Reporting - Service Review - Process Improvement - Root Cause Analysis

Verantwortlich: Anna Schmidt

9.4 Prozessschnittstellen

9.4.1 Schnittstellen zu anderen IT-Prozessen

Prozess	Schnittstelle	Informationsfluss	Verantwortlich
Incident Management	Störungsmeldungen → Betrieb	Incidents, Workarounds	Service Desk
Change Management	Change Requests → Betrieb	Changes, RFCs	CAB
Problem Management	Known Errors → Betrieb	Problem Records, Solutions	Problem Manager
Configuration Management	CI-Updates → CMDB	Configuration Items	CMDB Manager
Capacity Management	Kapazitätsdaten → Planung	Performance Metrics	Capacity Manager
Availability Management	Verfügbarkeitsdaten → Reporting	Availability Reports	Availability Manager
Security Management	Security Events → Betrieb	Security Incidents, Patches	Thomas Weber
Backup Management	Backup-Status → Betrieb	Backup Reports, Restore Requests	Backup Administrator

9.4.2 Schnittstellen zu Geschäftsprozessen

Geschäftsprozess	Schnittstelle	Informationsfluss	Ansprechpartner
Beschaffung	Hardware/Software-Anforderungen	Bestellungen, Lieferungen	Procurement
Finanzen	Budget und Kosten	Kostenberichte, Budgetanfragen	Maria Müller

Geschäftsprozess	Schnittstelle	Informationsfluss	Ansprechpartner
Compliance	Audit-Anforderungen	Audit-Berichte, Nachweise	Compliance Officer
HR	Mitarbeiter- Onboarding/Offboarding	Zugriffsverwaltung	HR Department

9.5 Eskalationspfade

9.5.1 Technische Eskalation

Level 1: Service Desk
 Kontakt: Julia Becker
 E-Mail: julia.becker@adminsends.de
 Telefon: +49 89 12345678-111
 Eskalation nach: 30 Minuten (P1), 2 Stunden (P2)

Level 2: IT Operations
 Kontakt: Andreas Huebner
 E-Mail: andreas.huebner@adminsends.de
 Telefon: +49 89 12345678-250
 Eskalation nach: 1 Stunde (P1), 4 Stunden (P2)

Level 3: Specialist/Vendor
 Kontakt: [TODO: Spezialist-Name]
 E-Mail: [TODO: Spezialist-E-Mail]
 Telefon: [TODO: Spezialist-Telefon]
 Eskalation nach: 2 Stunden (P1), 8 Stunden (P2)

9.5.2 Management-Eskalation

Stufe 1: IT Operations Manager
 Kontakt: Andreas Huebner
 E-Mail: andreas.huebner@adminsends.de
 Eskalation bei: Kritische Incidents (P1), SLA-Verletzung

Stufe 2: Chief Information Officer (CIO)
 Kontakt: Anna Schmidt
 E-Mail: anna.schmidt@adminsends.de
 Eskalation bei: Major Incidents, Business Impact

Stufe 3: Chief Executive Officer (CEO)
 Kontakt: Max Mustermann
 E-Mail: max.mustermann@adminsends.de
 Eskalation bei: Unternehmenskritische Ausfälle

9.5.3 Eskalationskriterien

Priorität	Technische Eskalation	Management-Eskalation	Zeitraumen
P1 (Kritisch)	Nach 30 Min (L1→L2), 1h (L2→L3)	Sofort an IT Ops Manager	Sofort
P2 (Hoch)	Nach 2h (L1→L2), 4h (L2→L3)	Nach 4 Stunden an IT Ops Manager	4 Stunden
P3 (Mittel)	Nach 8h (L1→L2), 1 Tag (L2→L3)	Nach 1 Tag an IT Ops Manager	1 Tag
P4 (Niedrig)	Nach 2 Tagen (L1→L2)	Keine automatische Eskalation	2 Tage

9.6 Betriebsprozess-Übersicht

9.6.1 Tägliche Betriebsroutinen

Morgen-Check (08:00 Uhr): - ☐ Monitoring-Dashboards prüfen - ☐ Backup-Status überprüfen - ☐ Offene Incidents reviewen - ☐ System-Health-Check durchführen - ☐ Log-Dateien auf Anomalien prüfen

Tages-Betrieb: - ☐ Incident-Bearbeitung nach Priorität - ☐ Change-Implementierungen durchführen - ☐ Monitoring und Alerting überwachen - ☐ Dokumentation aktualisieren - ☐ Kommunikation mit Stakeholdern

Abend-Check (18:00 Uhr): - ☐ Tages-Incidents abschließen oder übergeben - ☐ Backup-Läufe initiieren - ☐ Wartungsarbeiten vorbereiten - ☐ Handover an Nachtschicht (falls 24/7) - ☐ Tagesbericht erstellen

9.6.2 Wöchentliche Aktivitäten

- ☐ Service-Review-Meeting (Montag)
- ☐ Patch-Management (Dienstag Abend)
- ☐ Kapazitäts-Review (Mittwoch)
- ☐ Problem-Management-Meeting (Donnerstag)
- ☐ Wochenabschluss und Reporting (Freitag)

9.6.3 Monatliche Aktivitäten

- ☐ Service-Level-Reporting
 - ☐ Kapazitätsplanung
 - ☐ Security-Patch-Review
 - ☐ Disaster-Recovery-Test
 - ☐ Compliance-Check
 - ☐ Vendor-Review
-

9.7 Prozess-Metriken und KPIs

9.7.1 Betriebsmetriken

Metrik	Zielwert	Messfrequenz	Verantwortlich
Service Availability	99.5%	Täglich	IT Operations
Mean Time To Repair (MTTR)	4 Stunden	Pro Incident	Service Desk
Mean Time Between Failures (MTBF)	720 Stunden	Monatlich	IT Operations
First Call Resolution Rate	70%	Wöchentlich	Service Desk
Change Success Rate	95%	Monatlich	Change Manager
Backup Success Rate	100%	Täglich	Backup Admin

9.7.2 Prozess-KPIs

KPI	Zielwert	Messfrequenz	Verantwortlich
Incident Resolution Time (P1)	4 Stunden	Pro Incident	Service Desk
Incident Resolution Time (P2)	8 Stunden	Pro Incident	Service Desk

KPI	Zielwert	Messfrequenz	Verantwortlich
Change Lead Time	5 Tage	Pro Change	Change Manager
Problem Resolution Time	30 Tage	Pro Problem	Problem Manager
SLA Compliance	98%	Monatlich	Service Manager

9.8 Kontinuierliche Verbesserung

9.8.1 CSI-Prozess

1. **Identifikation:** Verbesserungspotenziale identifizieren
2. **Analyse:** Root-Cause-Analyse durchführen
3. **Planung:** Verbesserungsmaßnahmen planen
4. **Implementierung:** Maßnahmen umsetzen
5. **Messung:** Erfolg messen und validieren
6. **Review:** Ergebnisse reviewen und dokumentieren

9.8.2 Verbesserungsquellen

- Incident-Analysen und Trends
- Problem-Management-Erkenntnisse
- Service-Review-Meetings
- Kundenfeedback
- Audit-Ergebnisse
- Benchmark-Vergleiche

9.8.3 Verbesserungs-Register

ID	Verbesserung	Priorität	Status	Verantwortlich	Zieldatum
CSI-001	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]
CSI-002	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]

9.9 Dokumentation und Wissensmanagement

9.9.1 Dokumentations-Repository

- **Betriebshandbücher:** Zentrale Ablage für alle Betriebsdokumente
- **Runbooks:** Standardisierte Ablaufbeschreibungen
- **Known Error Database:** Bekannte Fehler und Lösungen
- **Configuration Management Database (CMDB):** CI-Dokumentation
- **Change-Historie:** Dokumentation aller Changes

9.9.2 Wissenstransfer

- **Onboarding:** Einarbeitung neuer Mitarbeiter
 - **Training:** Regelmäßige Schulungen
 - **Documentation:** Kontinuierliche Dokumentation
 - **Knowledge Sharing:** Team-Meetings und Workshops
 - **Lessons Learned:** Post-Incident-Reviews
-

9.10 Compliance und Governance

9.10.1 Relevante Standards

- **ITIL v4:** IT Service Management Framework
- **ISO 20000:** IT Service Management Standard
- **ISO 27001:** Information Security Management
- **COBIT 2019:** IT Governance Framework

9.10.2 Audit-Anforderungen

- Dokumentation aller Betriebsprozesse
 - Nachweisbare Einhaltung von SLAs
 - Change-Management-Protokolle
 - Incident-Management-Berichte
 - Compliance-Nachweise
-

9.11 Kontakte

Betriebsverantwortliche: - **IT Operations Manager:** Andreas Huemmer - andreas.huemmer@adminsendsend.de
- **Service Desk Lead:** Julia Becker - julia.becker@adminsendsend.de - **CIO:** Anna Schmidt - anna.schmidt@adminsendsend.de

Weitere Kontakte: Siehe Kapitel 0270 (Kontakte, Eskalation und Anbieter)

Dokumentverantwortlicher: IT Operations Manager

Genehmigt durch: CIO

Version: 1.0.0

Organisation: AdminSend GmbH

ewpage

Chapter 10

Betriebsübergabe und Go-Live-Checkliste

10.1 Übersicht

Dieses Dokument beschreibt den Prozess der Betriebsübergabe und enthält eine umfassende Go-Live-Checkliste für die Überführung neuer oder geänderter IT-Services in den Produktivbetrieb.

Service: {{ meta.service_name }}

Verantwortlich: Andreas Huemmer

Stand: 1.0.0

10.2 Betriebsübergabe-Prozess

10.2.1 Phasen der Betriebsübergabe

1. Vorbereitung

2. Dokumentation

3. Training

4. Testing

5. Go-Live

6. Hypercare

10.2.2 Rollen und Verantwortlichkeiten

Rolle	Verantwortung	Ansprechpartner
Service Owner	Gesamtverantwortung für Service	[TODO: Name]
IT Operations Manager	Betriebsübernahme koordinieren	Andreas Huemmer
Technical Lead	Technische Implementierung	[TODO: Name]
Service Desk Lead	Support-Bereitschaft	Julia Becker
Change Manager	Change-Genehmigung	[TODO: Name]
CIO	Finale Freigabe	Anna Schmidt

10.3 Go-Live-Checkliste

10.3.1 Phase 1: Vorbereitung (4-6 Wochen vor Go-Live)

10.3.1.1 Projektplanung

- ☐ Go-Live-Datum festgelegt und kommuniziert
- ☐ Projektteam zusammengestellt
- ☐ Rollen und Verantwortlichkeiten definiert
- ☐ Kommunikationsplan erstellt
- ☐ Risikobewertung durchgeführt
- ☐ Rollback-Plan erstellt

10.3.1.2 Infrastruktur

- ☐ Hardware beschafft und installiert
- ☐ Netzwerkanbindung konfiguriert
- ☐ Virtualisierung/Cloud-Ressourcen bereitgestellt
- ☐ Storage-Kapazität allokiert
- ☐ Backup-Infrastruktur eingerichtet
- ☐ Monitoring-Infrastruktur vorbereitet

10.3.1.3 Software und Lizenzen

- ☐ Software-Lizenzen beschafft
- ☐ Software installiert und konfiguriert
- ☐ Patches und Updates eingespielt
- ☐ Lizenz-Compliance geprüft
- ☐ Drittanbieter-Software integriert

10.3.2 Phase 2: Dokumentation (3-4 Wochen vor Go-Live)

10.3.2.1 Betriebsdokumentation

- ☐ Betriebshandbuch erstellt (dieses Dokument)
- ☐ Systemarchitektur dokumentiert (Kapitel 0040)
- ☐ Infrastruktur dokumentiert (Kapitel 0050)
- ☐ Netzwerkdiagramme erstellt
- ☐ Konfigurationsdokumentation vollständig
- ☐ CMDB-Einträge erstellt (Kapitel 0090)

10.3.2.2 Prozessdokumentation

- ☐ Incident-Management-Prozess definiert (Kapitel 0120)
- ☐ Change-Management-Prozess definiert (Kapitel 0140)
- ☐ Backup-Prozess dokumentiert (Kapitel 0150)
- ☐ Monitoring-Prozess dokumentiert (Kapitel 0110)
- ☐ Eskalationspfade definiert (Kapitel 0070)

10.3.2.3 Runbooks und Anleitungen

- ☐ Standard-Runbooks erstellt (Kapitel 0240)
- ☐ Troubleshooting-Guides erstellt
- ☐ Notfall-Runbooks erstellt
- ☐ Wartungs-Checklisten erstellt
- ☐ FAQ-Dokument erstellt (Kapitel 0260)

10.3.3 Phase 3: Training (2-3 Wochen vor Go-Live)

10.3.3.1 Service Desk Training

- ☐ Service-Übersicht präsentiert
- ☐ Incident-Handling trainiert
- ☐ Ticketing-System geschult
- ☐ Eskalationsprozesse erklärt
- ☐ FAQ und Known Issues durchgegangen
- ☐ Hands-on-Training durchgeführt

10.3.3.2 Operations Team Training

- ☐ Technische Architektur erklärt
- ☐ Monitoring-Tools geschult
- ☐ Backup/Restore-Prozeduren trainiert

- ☐ Change-Prozess durchgegangen
- ☐ Notfall-Prozeduren geübt
- ☐ Runbooks durchgearbeitet

10.3.3.3 Management Briefing

- ☐ Service-Übersicht präsentiert
- ☐ SLAs und KPIs erklärt
- ☐ Risiken und Mitigationen besprochen
- ☐ Eskalationsprozesse kommuniziert
- ☐ Reporting-Mechanismen erklärt

10.3.4 Phase 4: Testing (1-2 Wochen vor Go-Live)

10.3.4.1 Funktionale Tests

- ☐ Unit-Tests durchgeführt
- ☐ Integrationstests durchgeführt
- ☐ End-to-End-Tests durchgeführt
- ☐ User Acceptance Tests (UAT) durchgeführt
- ☐ Performance-Tests durchgeführt
- ☐ Security-Tests durchgeführt

10.3.4.2 Betriebstests

- ☐ Backup-Test durchgeführt
- ☐ Restore-Test durchgeführt
- ☐ Failover-Test durchgeführt
- ☐ Monitoring-Alerts getestet
- ☐ Incident-Prozess getestet
- ☐ Eskalationsprozess getestet

10.3.4.3 Disaster Recovery Test

- ☐ DR-Plan getestet
- ☐ Failover zu DR-Site getestet
- ☐ Failback zu Primary Site getestet
- ☐ RTO/RPO validiert
- ☐ DR-Dokumentation aktualisiert

10.3.5 Phase 5: Go-Live (Go-Live-Tag)

10.3.5.1 Pre-Go-Live (24 Stunden vorher)

- ☐ Go/No-Go-Meeting durchgeführt
- ☐ Alle Stakeholder informiert
- ☐ Wartungsfenster kommuniziert
- ☐ Rollback-Plan final geprüft
- ☐ Backup vor Go-Live erstellt
- ☐ Change-Ticket genehmigt

10.3.5.2 Go-Live-Aktivitäten

- ☐ Wartungsfenster gestartet
- ☐ Service-Migration durchgeführt
- ☐ Konfigurationsänderungen angewendet
- ☐ Smoke-Tests durchgeführt
- ☐ Monitoring aktiviert
- ☐ Service-Status kommuniziert

10.3.5.3 Post-Go-Live (unmittelbar nach Go-Live)

- ☐ Service-Verfügbarkeit bestätigt
- ☐ Monitoring-Dashboards geprüft
- ☐ Erste Transaktionen validiert
- ☐ Performance-Metriken geprüft
- ☐ Stakeholder informiert
- ☐ Go-Live-Protokoll erstellt

10.3.6 Phase 6: Hypercare (1-4 Wochen nach Go-Live)

10.3.6.1 Hypercare-Support

- ☐ Erweiterte Support-Zeiten aktiviert
- ☐ Zusätzliche Ressourcen bereitgestellt
- ☐ Tägliche Status-Meetings durchgeführt
- ☐ Incident-Tracking intensiviert
- ☐ Performance-Monitoring verstärkt
- ☐ User-Feedback gesammelt

10.3.6.2 Stabilisierung

- ☐ Kritische Issues behoben
 - ☐ Performance optimiert
 - ☐ Dokumentation aktualisiert
 - ☐ Known Issues dokumentiert
 - ☐ Lessons Learned dokumentiert
 - ☐ Post-Implementation-Review durchgeführt
-

10.4 Übergabedokumentation

10.4.1 Übergabe-Paket

Das Übergabe-Paket muss folgende Dokumente enthalten:

10.4.1.1 Technische Dokumentation

1. **Systemarchitektur** (Kapitel 0040)
 - Architekturdiagramme
 - Komponentenbeschreibungen

- Datenflüsse
- Abhängigkeiten
- 2. **Infrastruktur** (Kapitel 0050)
 - Hardware-Inventar
 - Netzwerkkonfiguration
 - IP-Adressierung
 - Virtualisierung/Cloud-Ressourcen
- 3. **Konfiguration** (Kapitel 0090)
 - Konfigurationsdateien
 - CMDB-Einträge
 - Netzwerk-Konfiguration
 - Security-Konfiguration

10.4.1.2 Betriebsdokumentation

- 4. **Betriebsprozesse** (Kapitel 0070)
 - Betriebsmodell
 - ITIL-Prozesse
 - Eskalationspfade
 - KPIs und Metriken
- 5. **Monitoring** (Kapitel 0110)
 - Monitoring-Strategie
 - Alert-Konfiguration
 - Dashboard-Übersichten
 - Schwellwerte
- 6. **Backup und Recovery** (Kapitel 0150)
 - Backup-Strategie
 - Backup-Zeitpläne
 - Restore-Prozeduren
 - RTO/RPO-Werte

10.4.1.3 Support-Dokumentation

- 7. **Runbooks** (Kapitel 0240)
 - Standard-Operationen
 - Troubleshooting-Guides
 - Notfall-Prozeduren
 - Wartungs-Checklisten
- 8. **Known Issues und FAQ** (Kapitel 0260)
 - Bekannte Probleme
 - Workarounds
 - Häufige Fragen
 - Lösungen
- 9. **Kontakte** (Kapitel 0270)
 - Ansprechpartner
 - Eskalationskontakte
 - Vendor-Kontakte
 - On-Call-Informationen

10.4.2 Übergabe-Meeting

Agenda: 1. Service-Übersicht und Geschäftszweck 2. Technische Architektur und Infrastruktur 3. Betriebsprozesse und Verantwortlichkeiten 4. Monitoring und Alerting 5. Incident- und Problem-Management 6. Backup und Disaster Recovery 7. Known Issues und Risiken 8. Fragen und Antworten

Teilnehmer: - Service Owner - IT Operations Manager: Andreas Huemmer - Technical Lead - Service Desk Lead: Julia Becker - CIO: Anna Schmidt

10.5 Acceptance-Kriterien

10.5.1 Technische Acceptance-Kriterien

Kriterium	Anforderung	Status	Verifiziert durch
Funktionalität	Alle Features funktionieren gemäß Spezifikation		[TODO]
Performance	Response-Zeiten < [TODO] ms		[TODO]
Verfügbarkeit	Service erreichbar 24/7		[TODO]
Skalierbarkeit	Unterstützt [TODO] gleichzeitige Benutzer		[TODO]
Security	Security-Tests bestanden		[TODO]
Backup	Backup-Tests erfolgreich		[TODO]
Monitoring	Alle Metriken werden erfasst		[TODO]
Integration	Alle Schnittstellen funktionieren		[TODO]

10.5.2 Betriebliche Acceptance-Kriterien

Kriterium	Anforderung	Status	Verifiziert durch
Dokumentation	Vollständige Betriebsdokumentation		IT Ops Manager
Training	Team geschult und einsatzbereit		Service Desk Lead
Runbooks	Alle Runbooks erstellt und getestet		IT Ops Manager
CMDB	Alle CIs dokumentiert		CMDB Manager
SLA	SLAs definiert und vereinbart		Service Manager

Kriterium	Anforderung	Status	Verifiziert durch
Support	Support-Prozesse etabliert		Service Desk Lead
Monitoring	Monitoring aktiv und funktional		Monitoring Team
Backup	Backup-Prozess etabliert		Backup Admin

10.5.3 Geschäftliche Acceptance-Kriterien

Kriterium	Anforderung	Status	Verifiziert durch
Business Requirements	Alle Geschäftsanforderungen erfüllt		Service Owner
User Acceptance	UAT erfolgreich abgeschlossen		Business Users
Compliance	Compliance-Anforderungen erfüllt		Compliance Officer
Budget	Innerhalb des Budgets		Maria Müller
Timeline	Zeitplan eingehalten		Project Manager

10.6 Go/No-Go-Entscheidung

10.6.1 Go/No-Go-Meeting

Zeitpunkt: 24 Stunden vor geplantem Go-Live

Teilnehmer: - Service Owner - IT Operations Manager: Andreas Huemmer - Technical Lead - Change Manager - CIO: Anna Schmidt

10.6.2 Entscheidungskriterien

Kriterium	Go	No-Go	Status
Alle Tests bestanden			
Dokumentation vollständig			
Team trainiert			
Keine kritischen Issues			
Rollback-Plan vorhanden			
Stakeholder informiert			
Change genehmigt			
Backup erstellt			

Entscheidung: GO NO-GO

Begründung: [TODO]

Unterschriften: - Service Owner: _____ Datum: _____ - IT Operations Manager: _____ Datum: _____ - CIO: _____
Datum: _____

10.7 Rollback-Plan

10.7.1 Rollback-Trigger

Rollback wird ausgelöst bei: - Kritischen Funktionsausfällen - Schwerwiegenden Performance-Problemen - Datenverlust oder Datenkorruption - Security-Incidents - Nicht erfüllten Acceptance-Kriterien

10.7.2 Rollback-Prozedur

1. **Entscheidung:** IT Operations Manager entscheidet über Rollback
2. **Kommunikation:** Stakeholder informieren
3. **Wartungsfenster:** Falls erforderlich, Wartungsfenster aktivieren
4. **Backup-Restore:** Letztes funktionierendes Backup wiederherstellen
5. **Konfiguration:** Alte Konfiguration wiederherstellen
6. **Validierung:** Funktionalität prüfen
7. **Kommunikation:** Rollback-Abschluss kommunizieren
8. **Post-Mortem:** Ursachenanalyse durchführen

10.7.3 Rollback-Zeitfenster

- **Innerhalb 4 Stunden nach Go-Live:** Schneller Rollback möglich
 - **4-24 Stunden nach Go-Live:** Rollback mit erhöhtem Aufwand
 - **Nach 24 Stunden:** Rollback nur nach sorgfältiger Analyse
-

10.8 Post-Implementation-Review

10.8.1 Review-Meeting

Zeitpunkt: 2-4 Wochen nach Go-Live

Teilnehmer: Alle Projektbeteiligten

Agenda: 1. Go-Live-Verlauf Review 2. Lessons Learned 3. Issues und Resolutionen 4. Performance-Analyse 5. User-Feedback 6. Verbesserungsvorschläge 7. Nächste Schritte

10.8.2 Lessons Learned

Kategorie	Was lief gut?	Was lief schlecht?	Verbesserungen
Planung	[TODO]	[TODO]	[TODO]
Kommunikation	[TODO]	[TODO]	[TODO]
Testing	[TODO]	[TODO]	[TODO]
Training	[TODO]	[TODO]	[TODO]

Kategorie	Was lief gut?	Was lief schlecht?	Verbesserungen
Go-Live	[TODO]	[TODO]	[TODO]
Support	[TODO]	[TODO]	[TODO]

10.8.3 Metriken nach Go-Live

Metrik	Zielwert	Ist-Wert	Status
Verfügbarkeit (erste Woche)	99%	[TODO]%	
Incidents (erste Woche)	10	[TODO]	
MTTR (erste Woche)	4h	[TODO]h	
User Satisfaction	80%	[TODO]%	
Performance	< [TODO] ms	[TODO] ms	

10.9 Kontakte

Go-Live-Team: - **Service Owner:** [TODO: Name] - [TODO: E-Mail] - **IT Operations Manager:** Andreas Huemmer - andreas.huemmer@adminsends.de - **Technical Lead:** [TODO: Name] - [TODO: E-Mail] - **Service Desk Lead:** Julia Becker - julia.becker@adminsends.de - **Change Manager:** [TODO: Name] - [TODO: E-Mail] - **CIO:** Anna Schmidt - anna.schmidt@adminsends.de

Dokumentverantwortlicher: IT Operations Manager

Genehmigt durch: CIO

Version: 1.0.0

Organisation: AdminSend GmbH

ewpage

Chapter 11

Konfigurationsmanagement und CMDB

11.1 Übersicht

Dieses Dokument beschreibt das Konfigurationsmanagement und die Configuration Management Database (CMDB) für den IT-Service. Es definiert CI-Kategorien, Attribute, Beziehungen und Change-Prozesse für Configuration Items.

Service: {{ meta.service_name }}

Verantwortlich: Andreas Huemmer

CMDB-System: NetBox

Stand: 1.0.0

11.2 Konfigurationsmanagement-Prozess

11.2.1 Ziele des Konfigurationsmanagements

- **Transparenz:** Vollständige Übersicht über alle IT-Assets und deren Beziehungen
- **Kontrolle:** Kontrollierte Änderungen an Configuration Items
- **Compliance:** Einhaltung von Lizenz- und Compliance-Anforderungen
- **Planung:** Fundierte Basis für Kapazitäts- und Change-Planung
- **Incident-Support:** Schnellere Incident-Resolution durch CI-Informationen

11.2.2 ITIL Configuration Management Aktivitäten

1. **Management and Planning:** Planung und Steuerung des Konfigurationsmanagements
 2. **Configuration Identification:** Identifikation und Kategorisierung von CIs
 3. **Configuration Control:** Kontrolle von Änderungen an CIs
 4. **Status Accounting:** Erfassung und Reporting des CI-Status
 5. **Verification and Audit:** Überprüfung der CMDB-Datenqualität
-

11.3 Configuration Management Database (CMDB)

11.3.1 CMDB-System: NetBox

NetBox-Instanz: - **URL:** {{ netbox.url }} - **Version:** {{ netbox.version }} - **Verantwortlich:** Andreas Huemmer

NetBox-Funktionen: - IP Address Management (IPAM) - Data Center Infrastructure Management (DCIM) - Device Management - Circuit Management - Virtualization Management - Configuration Context

11.3.2 CMDB-Struktur

CMDB (NetBox)		
Sites	Racks	Devices
IP Addresses	VLANs	Circuits
Clusters	Virtual Machines	Interfaces

11.4 CI-Kategorien und Attribute

11.4.1 Hardware-CIs

11.4.1.1 Server

Kategorie: Hardware > Server

Attribute: - **Name:** {{ netbox.device.name }} - **Hersteller:** {{ netbox.device.manufacturer }} - **Modell:** {{ netbox.device.model }} - **Seriennummer:** {{ netbox.device.serial }} - **Asset-Tag:** {{ netbox.device.asset_tag }} - **Standort:** {{ netbox.device.site }} - **Rack:** {{ netbox.device.rack }} - **Rack-Position:** {{ netbox.device.position }} - **Status:** Active, Planned, Staged, Failed, Decommissioned - **Rolle:** {{ netbox.device.role }} - **Primary IP:** {{ netbox.device.primary_ip }}

11.4.1.2 Netzwerkgeräte

Kategorie: Hardware > Network

Attribute: - **Name:** {{ netbox.device.name }} - **Typ:** Switch, Router, Firewall, Load Balancer - **Hersteller:** {{ netbox.device.manufacturer }} - **Modell:** {{ netbox.device.model }}

Management-IP: {{ netbox.device.primary_ip }} - **Standort:** {{ netbox.device.site }} - **Interfaces:** {{ netbox.device.interfaces }} - **VLANs:** {{ netbox.device.vlans }}

11.4.1.3 Storage

Kategorie: Hardware > Storage

Attribute: - **Name:** {{ netbox.device.name }} - **Typ:** SAN, NAS, DAS - **Kapazität:** [TODO] TB - **Hersteller:** {{ netbox.device.manufacturer }} - **Standort:** {{ netbox.device.site }}

11.4.2 Software-CIs

11.4.2.1 Betriebssysteme

Kategorie: Software > Operating System

Attribute: - **Name:** [TODO: z.B. Ubuntu Server 22.04] - **Version:** [TODO] - **Lizenz:** [TODO] - **Installiert auf:** {{ netbox.device.name }} - **Patch-Level:** [TODO]

11.4.2.2 Anwendungen

Kategorie: Software > Application

Attribute: - **Name:** [TODO: Anwendungsname] - **Version:** [TODO] - **Hersteller:** [TODO] - **Lizenz:** [TODO] - **Lizenzanzahl:** [TODO] - **Installiert auf:** {{ netbox.device.name }} - **Verantwortlich:** [TODO]

11.4.3 Virtualisierung-CIs

11.4.3.1 Hypervisor-Cluster

Kategorie: Virtualization > Cluster

Attribute: - **Name:** {{ netbox.cluster.name }} - **Typ:** {{ netbox.cluster.type }} - **Standort:** {{ netbox.cluster.site }} - **Anzahl Hosts:** {{ netbox.cluster.device_count }}

11.4.3.2 Virtuelle Maschinen

Kategorie: Virtualization > Virtual Machine

Attribute: - **Name:** {{ netbox.vm.name }} - **Cluster:** {{ netbox.vm.cluster }} - **vCPUs:** {{ netbox.vm.vcpus }} - **Memory:** {{ netbox.vm.memory }} GB - **Disk:** {{ netbox.vm.disk }} GB - **Status:** Active, Offline, Staged - **Primary IP:** {{ netbox.vm.primary_ip }} - **Betriebssystem:** [TODO]

11.4.4 Netzwerk-CIs

11.4.4.1 IP-Adressen

Kategorie: Network > IP Address

Attribute: - **IP-Adresse:** {{ netbox.ip.address }} - **VLAN:** {{ netbox.ip.vlan }} - **Status:** Active, Reserved, Deprecated - **DNS-Name:** {{ netbox.ip.dns_name }} - **Zugewiesen zu:** {{ netbox.ip.assigned_to }}

11.4.4.2 VLANs

Kategorie: Network > VLAN

Attribute: - **VLAN-ID:** {{ netbox.vlan.vid }} - **Name:** {{ netbox.vlan.name }} - **Standort:** {{ netbox.vlan.site }} - **Beschreibung:** {{ netbox.vlan.description }}

11.4.4.3 Circuits

Kategorie: Network > Circuit

Attribute: - **Circuit-ID:** {{ netbox.circuit.cid }} - **Provider:** {{ netbox.circuit.provider }} - **Typ:** {{ netbox.circuit.type }} - **Bandbreite:** {{ netbox.circuit.commit_rate }} Mbps - **Status:** Active, Planned, Decommissioned

11.4.5 Standort-CIs

11.4.5.1 Sites

Kategorie: Location > Site

Attribute: - **Name:** {{ netbox.site.name }} - **Adresse:** {{ netbox.site.physical_address }} - **Facility:** {{ netbox.site.facility }} - **Status:** Active, Planned, Retired - **Kontakt:** {{ netbox.site.contact_name }}

11.5 CI-Beziehungen

11.5.1 Beziehungstypen

Beziehung	Beschreibung	Beispiel
Hosted on	CI läuft auf anderem CI	VM hosted on Hypervisor
Connected to	Physische/logische Verbindung	Server connected to Switch
Depends on	Funktionale Abhängigkeit	Application depends on Database
Part of	Komponente eines größeren CI	Disk part of Server
Uses	CI nutzt anderes CI	Application uses IP Address
Managed by	Verwaltungsbeziehung	Device managed by Management System

11.5.2 Beziehungsdiagramm

Application

depends on

Database

hosted on

Virtual Machine

hosted on

Hypervisor

installed on

Physical Server

connected to

Switch

11.5.3 CI-Abhängigkeiten

Beispiel: Web-Application Stack

CI	Abhängig von	Beziehungstyp
Web Application	Application Server	depends on
Application Server	Database Server	depends on
Application Server	Load Balancer	connected to
Database Server	Storage Array	uses
Application Server	Virtual Machine	hosted on
Virtual Machine	Hypervisor Cluster	hosted on
Hypervisor Cluster	Physical Servers	consists of
Physical Servers	Network Switch	connected to

11.6 Change-Prozesse für CIs

11.6.1 CI-Lifecycle

Planned

Staged

Active

Deprecated

Decommissioned

11.6.2 CI-Änderungsprozess

11.6.2.1 1. CI-Erstellung

Trigger: Neue Hardware/Software beschafft

Prozess: 1. CI in CMDB anlegen (Status: Planned) 2. Attribute erfassen 3. Beziehungen definieren 4. Genehmigung durch IT Operations Manager 5. Status auf “Staged” setzen

11.6.2.2 2. CI-Aktivierung

Trigger: CI in Betrieb genommen

Prozess: 1. Change Request erstellen (siehe Kapitel 0140) 2. CI-Konfiguration durchführen 3. Tests durchführen 4. Status auf “Active” setzen 5. Monitoring aktivieren

11.6.2.3 3. CI-Änderung

Trigger: Änderung an bestehendem CI

Prozess: 1. Change Request erstellen 2. Impact-Analyse durchführen 3. Abhängige CIs identifizieren 4. Change durchführen 5. CMDB aktualisieren 6. Validierung durchführen

11.6.2.4 4. CI-Deaktivierung

Trigger: CI außer Betrieb nehmen

Prozess: 1. Change Request erstellen 2. Abhängigkeiten prüfen 3. Backup erstellen 4. CI deaktivieren 5. Status auf “Deprecated” setzen 6. Monitoring deaktivieren

11.6.2.5 5. CI-Löschung

Trigger: CI endgültig entfernen

Prozess: 1. Sicherstellen, dass keine Abhängigkeiten bestehen 2. Daten archivieren 3. Lizenzen zurückgeben 4. Status auf “Decommissioned” setzen 5. Nach Aufbewahrungsfrist aus CMDB löschen

11.6.3 Change-Genehmigung für CIs

CI-Kategorie	Genehmigung erforderlich durch	Change-Typ
Kritische Server	IT Operations Manager + CIO	Normal Change
Netzwerk-Core	IT Operations Manager + CIO	Normal Change
Standard-Server	IT Operations Manager	Standard Change
Workstations	Service Desk Lead	Standard Change
IP-Adressen	Network Administrator	Standard Change
Virtuelle Maschinen	Virtualization Admin	Standard Change

11.7 CMDB-Datenqualität

11.7.1 Datenqualitäts-Metriken

Metrik	Zielwert	Messfrequenz	Verantwortlich
Vollständigkeit	95%	Monatlich	CMDB Manager
Genauigkeit	98%	Monatlich	CMDB Manager
Aktualität	7 Tage	Wöchentlich	CMDB Manager
Konsistenz	95%	Monatlich	CMDB Manager
Eindeutigkeit	100%	Kontinuierlich	CMDB Manager

11.7.2 Datenqualitäts-Prozess

11.7.2.1 Regelmäßige Audits

- **Frequenz:** Quartalsweise
- **Umfang:** Stichprobe von 10% aller CIs
- **Methode:** Vergleich CMDB-Daten mit tatsächlichem Zustand
- **Verantwortlich:** Andreas Huemmer

11.7.2.2 Automatische Validierung

- **Discovery-Tools:** Automatische Erkennung von Geräten und Software
- **Reconciliation:** Abgleich zwischen Discovery und CMDB
- **Alerts:** Benachrichtigung bei Abweichungen
- **Korrektur:** Automatische oder manuelle Korrektur

11.7.2.3 Manuelle Überprüfung

- **Trigger:** Vor jedem Major Change
- **Prozess:** Manuelle Überprüfung betroffener CIs
- **Dokumentation:** Änderungen dokumentieren
- **Genehmigung:** Durch IT Operations Manager

11.8 CMDB-Zugriff und Berechtigungen

11.8.1 Zugriffsrollen

Rolle	Berechtigung	Zugriff auf
CMDB Administrator	Vollzugriff	Alle CIs
IT Operations Manager	Lesen, Schreiben, Löschen	Alle CIs
Network Administrator	Lesen, Schreiben	Netzwerk-CIs
Server Administrator	Lesen, Schreiben	Server-CIs
Service Desk	Lesen	Alle CIs
Auditor	Lesen	Alle CIs (Read-only)

11.8.2 Zugriffskontrolle

CMDB-Administrator: Andreas Huemmer

Zugriff über: {{ netbox.url }}

Authentifizierung: SSO/LDAP

Audit-Logging: Alle Änderungen werden protokolliert

11.9 CMDB-Integration

11.9.1 Integrierte Systeme

System	Integration	Datenfluss	Frequenz
Monitoring	API	CMDB → Monitoring	Real-time
Ticketing	API	CMDB → Ticketing	Real-time
Asset Management	API	Asset Mgmt → CMDB	Täglich
Discovery Tools	API	Discovery → CMDB	Stündlich
Backup System	API	CMDB → Backup	Täglich
Change Management	API	CMDB → Change Mgmt	Real-time

11.9.2 API-Zugriff

NetBox API: - **Endpoint:** {{ netbox.url }}/api/ - **Authentifizierung:** API Token - **Dokumentation:** {{ netbox.url }}/api/docs/ - **Rate Limiting:** [TODO: z.B. 1000 Requests/Stunde]

11.10 CMDB-Reporting

11.10.1 Standard-Reports

11.10.1.1 CI-Inventar-Report

Frequenz: Monatlich

Inhalt: - Anzahl CIs pro Kategorie - CI-Status-Verteilung - Neue CIs im letzten Monat - Deaktivierte CIs im letzten Monat

11.10.1.2 Lizenz-Compliance-Report

Frequenz: Quartalsweise

Inhalt: - Lizenzierte Software - Installierte Instanzen - Lizenz-Compliance-Status - Ablaufende Lizenzen

11.10.1.3 Netzwerk-Inventar-Report

Frequenz: Monatlich

Inhalt: - IP-Adress-Nutzung - VLAN-Übersicht - Netzwerkgeräte-Status - Circuit-Übersicht

11.10.1.4 Change-Impact-Report

Frequenz: Pro Change

Inhalt: - Betroffene CIs - Abhängige CIs - Risikobewertung - Rollback-Plan

11.11 CMDB-Wartung

11.11.1 Wartungsaktivitäten

11.11.1.1 Tägliche Aktivitäten

- ☐ Discovery-Ergebnisse reviewen
- ☐ Neue CIs validieren
- ☐ Änderungen aus Change-Tickets übernehmen
- ☐ Alerts zu Abweichungen prüfen

11.11.1.2 Wöchentliche Aktivitäten

- ☐ Datenqualitäts-Metriken prüfen
- ☐ Verwaiste CIs identifizieren
- ☐ Beziehungen validieren
- ☐ Backup der CMDB durchführen

11.11.1.3 Monatliche Aktivitäten

- ☐ CMDB-Audit durchführen
- ☐ Reports generieren und verteilen
- ☐ Lizenz-Compliance prüfen
- ☐ Veraltete CIs archivieren

11.11.1.4 Quartalsweise Aktivitäten

- ☐ Umfassendes CMDB-Audit
 - ☐ Datenqualitäts-Review
 - ☐ Prozess-Review
 - ☐ Training für CMDB-Nutzer
-

11.12 Best Practices

11.12.1 CMDB-Best-Practices

1. **Eindeutige Identifikation:** Jedes CI muss eindeutig identifizierbar sein
2. **Konsistente Namenskonvention:** Einheitliche Benennung aller CIs
3. **Vollständige Attribute:** Alle relevanten Attribute erfassen
4. **Aktuelle Beziehungen:** Beziehungen zwischen CIs pflegen
5. **Regelmäßige Audits:** Datenqualität kontinuierlich prüfen
6. **Automatisierung:** Discovery und Reconciliation automatisieren
7. **Integration:** CMDB mit anderen Tools integrieren
8. **Dokumentation:** Änderungen dokumentieren
9. **Training:** Nutzer regelmäßig schulen
10. **Governance:** Klare Verantwortlichkeiten definieren

11.12.2 Namenskonventionen

Server: - Format: [Standort]-[Typ]-[Umgebung]-[Nummer] - Beispiel: MUC-SRV-PROD-001

Virtuelle Maschinen: - Format: [Standort]-[Typ]-[Umgebung]-[Applikation]-[Nummer] -
Beispiel: MUC-VM-PROD-WEB-001

Netzwerkgeräte: - Format: [Standort]-[Typ]-[Funktion]-[Nummer] - Beispiel: MUC-SW-CORE-001

11.13 Kontakte

CMDB-Verantwortliche: - **CMDB Administrator:** Andreas Huemmer - andreas.huemmer@adminsends.de
- **Network Administrator:** [TODO: Name] - [TODO: E-Mail] - **Server Administrator:** [TODO:
Name] - [TODO: E-Mail] - **CIO:** Anna Schmidt - anna.schmidt@adminsends.de

NetBox-Support: - **URL:** {{ netbox.url }} - **Dokumentation:** {{ netbox.url }}/docs/ - **Support:** [TODO: Support-Kontakt]

Dokumentverantwortlicher: IT Operations Manager

Genehmigt durch: CIO

Version: 1.0.0

Organisation: AdminSend GmbH

ewpage

Chapter 12

Access und Berechtigungsmanagement

12.1 Übersicht

Dieses Dokument beschreibt das Access- und Berechtigungsmanagement für den IT-Service. Es definiert Zugriffskontrollmodelle, Berechtigungskonzepte und rollenbasierte Zugriffskontrolle (RBAC).

Service: {{ meta.service_name }}

Verantwortlich: Andreas Huemmer

Security Officer: Thomas Weber

Stand: 1.0.0

12.2 Access Management Strategie

12.2.1 Ziele

- **Least Privilege:** Minimale notwendige Berechtigungen
- **Separation of Duties:** Aufgabentrennung zur Risikominimierung
- **Need-to-Know:** Zugriff nur auf erforderliche Informationen
- **Accountability:** Nachvollziehbarkeit aller Zugriffe
- **Compliance:** Einhaltung regulatorischer Anforderungen

12.2.2 Grundprinzipien

1. **Default Deny:** Standardmäßig kein Zugriff, explizite Freigabe erforderlich
 2. **Time-Limited Access:** Zeitlich begrenzte Berechtigungen wo möglich
 3. **Regular Review:** Regelmäßige Überprüfung von Berechtigungen
 4. **Audit Trail:** Vollständige Protokollierung aller Zugriffe
 5. **Multi-Factor Authentication:** MFA für privilegierte Zugriffe
-

12.3 Zugriffskontrollmodell

12.3.1 Authentifizierung

12.3.1.1 Authentifizierungsmethoden

Methode	Verwendung	Sicherheitsstufe
Username/Password	Standard-Zugriff	Basis
Multi-Factor Authentication (MFA)	Privilegierter Zugriff	Hoch
Certificate-Based	System-zu-System	Sehr hoch
SSO (Single Sign-On)	Unternehmensanwendungen	Mittel-Hoch
API Keys	Programmatischer Zugriff	Mittel
Biometric	Hochsicherheitsbereiche	Sehr hoch

12.3.1.2 Authentifizierungs-Infrastruktur

Identity Provider: - **System:** [TODO: z.B. Active Directory, Azure AD, Okta] - **URL:** [TODO: SSO-URL] - **Verantwortlich:** Andreas Huemmer

MFA-System: - **System:** [TODO: z.B. Duo, Microsoft Authenticator] - **Pflicht für:** Administratoren, privilegierte Accounts - **Verantwortlich:** Thomas Weber

12.3.2 Autorisierung

12.3.2.1 Autorisierungsmodelle

Role-Based Access Control (RBAC): - Berechtigungen werden Rollen zugewiesen - Benutzer erhalten Rollen - Vereinfacht Berechtigungsverwaltung

Attribute-Based Access Control (ABAC): - Berechtigungen basieren auf Attributen - Flexibler als RBAC - Komplexere Implementierung

Aktuelles Modell: [TODO: RBAC/ABAC/Hybrid auswählen]

12.4 Rollenbasierte Zugriffskontrolle (RBAC)

12.4.1 Rollen-Hierarchie

Administrator
(Vollzugriff auf alle Systeme und Daten)

Power User
(Erweiterte

Operator
(Betriebszugriff)

Berechtigungen)

Standard User (Basis-Zugriff)	Read-Only (Nur Lesen)
----------------------------------	--------------------------

12.4.2 Rollen-Definition

12.4.2.1 Administrator

Beschreibung: Vollzugriff auf alle Systeme und Funktionen

Berechtigungen: - Vollzugriff auf alle Systeme - Benutzerverwaltung - Konfigurationsänderungen
- System-Administration - Backup/Restore

Zugewiesen an: - Andreas Huemmer - [TODO: Weitere Administratoren]

MFA: Pflicht

12.4.2.2 Power User

Beschreibung: Erweiterte Berechtigungen für spezielle Aufgaben

Berechtigungen: - Lesen und Schreiben in zugewiesenen Bereichen - Erweiterte Funktionen nutzen
- Reports erstellen - Konfiguration in eigenem Bereich

Zugewiesen an: - [TODO: Power User auflisten]

MFA: Empfohlen

12.4.2.3 Operator

Beschreibung: Betriebszugriff für tägliche Aufgaben

Berechtigungen: - Monitoring-Zugriff - Incident-Bearbeitung - Standard-Operationen - Log-Zugriff (Read-only)

Zugewiesen an: - Julia Becker - [TODO: Weitere Operators]

MFA: Optional

12.4.2.4 Standard User

Beschreibung: Basis-Zugriff für normale Benutzer

Berechtigungen: - Zugriff auf eigene Daten - Standard-Funktionen nutzen - Tickets erstellen - Eigenes Profil verwalten

Zugewiesen an: - Alle Mitarbeiter

MFA: Optional

12.4.2.5 Read-Only

Beschreibung: Nur Lesezugriff für Reporting und Auditing

Berechtigungen: - Lesezugriff auf Daten - Reports anzeigen - Dashboards anzeigen - Keine Änderungen möglich

Zugewiesen an: - Auditoren - Management - [TODO: Weitere Read-Only-Benutzer]

MFA: Optional

12.5 Berechtigungsmatrix

12.5.1 System-Berechtigungen

System/Ressource	Administrator	Power User	Operator	Standard User	Read-Only
Server-Administration	Vollzugriff	-	-	-	Lesen
Netzwerk-Konfiguration	Vollzugriff	-	-	-	Lesen
Monitoring-System	Vollzugriff	Lesen/Schreiben	Lesen	-	Lesen
Ticketing-System	Vollzugriff	Lesen/Schreiben	Lesen/Schreiben	Tickets erstellen	Lesen
CMDB	Vollzugriff	Lesen/Schreiben	Lesen	-	Lesen
Backup-System	Vollzugriff	-	Lesen	-	Lesen
Log-Management	Vollzugriff	Lesen	Lesen	-	Lesen
Dokumentation	Vollzugriff	Lesen/Schreiben	Lesen	Lesen	Lesen

12.5.2 Daten-Berechtigungen

Datenklassifizierung	Administrator	Power User	Operator	Standard User	Read-Only
Public	Vollzugriff	Lesen/Schreiben	Lesen	Lesen	Lesen
Internal	Vollzugriff	Lesen/Schreiben	Lesen	Lesen	Lesen
Confidential	Vollzugriff	Nach Bedarf	-	-	Nach Bedarf
Restricted	Nach Bedarf	-	-	-	-

12.6 Access Request Prozess

12.6.1 Zugriffs-Anforderung

1. Antrag
stellen

2. Manager
Genehmigung

3. Security
Review

4. Provisionierung

5. Bestätigung

12.6.2 Antragsprozess

12.6.2.1 1. Antrag stellen

Wer: Benutzer oder Manager

Wie: Ticket im Service Desk System

Informationen: - Benutzername - Angeforderte Rolle/Berechtigung - Geschäftliche Begründung - Zeitraum (falls temporär) - Manager-Genehmigung

12.6.2.2 2. Manager-Genehmigung

Wer: Direkter Vorgesetzter

Prüfung: - Geschäftliche Notwendigkeit - Least Privilege Prinzip - Separation of Duties

Entscheidung: Genehmigen / Ablehnen / Rückfragen

12.6.2.3 3. Security Review

Wer: Thomas Weber oder Security Team

Prüfung: - Compliance-Anforderungen - Risikobewertung - Konfliktprüfung (Separation of Duties)

Entscheidung: Genehmigen / Ablehnen / Anpassen

12.6.2.4 4. Provisionierung

Wer: Andreas Huemmer oder IT Operations

Aktivitäten: - Account erstellen/ändern - Berechtigungen zuweisen - MFA einrichten (falls erforderlich) - Dokumentation in CMDB

SLA: Innerhalb 1 Arbeitstag

12.6.2.5 5. Bestätigung

Wer: IT Operations

Aktivitäten: - Benutzer informieren - Zugangsdaten bereitstellen - Dokumentation abschließen - Ticket schließen

12.7 Privileged Access Management (PAM)

12.7.1 Privilegierte Accounts

12.7.1.1 Definition

Privilegierte Accounts haben erweiterte Berechtigungen und Zugriff auf kritische Systeme.

Beispiele: - Root/Administrator-Accounts - Service-Accounts - Database-Admin-Accounts - Network-Admin-Accounts - Backup-Admin-Accounts

12.7.2 PAM-Anforderungen

Anforderung	Beschreibung	Umsetzung
Separate Accounts	Privilegierte Accounts getrennt von Standard-Accounts	[TODO]
MFA	Multi-Faktor-Authentifizierung Pflicht	[TODO]
Session Recording	Aufzeichnung privilegierter Sessions	[TODO]
Just-in-Time Access	Temporäre Rechtevergabe	[TODO]
Password Vault	Zentrale Passwortverwaltung	[TODO]
Regular Rotation	Regelmäßige Passwort-Rotation	[TODO]
Audit Logging	Vollständige Protokollierung	[TODO]

12.7.3 PAM-System

System: [TODO: z.B. CyberArk, BeyondTrust, Thycotic]

Verantwortlich: Thomas Weber

Zugriff: [TODO: PAM-System-URL]

12.8 Service Accounts

12.8.1 Service Account Management

Definition: Accounts für automatisierte Prozesse und Systemintegrationen

Anforderungen: - Eindeutige Benennung (z.B. `svc_backup`, `svc_monitoring`) - Dokumentation in CMDB - Minimale Berechtigungen - Keine interaktiven Logins - Regelmäßige Passwort-Rotation - Überwachung der Nutzung

12.8.2 Service Account Inventar

Service Account	Verwendung	System	Berechtigungen	Owner
<code>svc_backup</code>	Backup-Prozesse	Backup-System	Lesen, Backup	Backup Admin
<code>svc_monitoring</code>	Monitoring	Monitoring-System	Lesen	Monitoring Team
<code>svc_integration</code>	System-Integration	Integration-Platform	API-Zugriff	Integration Team
[TODO]	[TODO]	[TODO]	[TODO]	[TODO]

12.9 Access Review Prozess

12.9.1 Regelmäßige Reviews

12.9.1.1 Quartalsweise Reviews

Frequenz: Alle 3 Monate

Umfang: Alle Benutzer-Berechtigungen

Verantwortlich: Manager + IT Operations

Prozess: 1. Review-Report generieren 2. Manager prüfen Berechtigungen ihrer Mitarbeiter 3. Nicht mehr benötigte Berechtigungen entfernen 4. Änderungen dokumentieren

12.9.1.2 Jährliche Reviews

Frequenz: Jährlich

Umfang: Vollständiger Access Review

Verantwortlich: Thomas Weber

Prozess: 1. Umfassender Audit aller Accounts 2. Privilegierte Accounts prüfen 3. Service Accounts validieren 4. Compliance-Check 5. Audit-Report erstellen

12.9.2 Automatische Reviews

Trigger: - Mitarbeiter-Wechsel (Abteilung/Rolle) - Projekt-Ende - Inaktive Accounts (> 90 Tage) - Ablauf temporärer Berechtigungen

Aktion: - Automatische Benachrichtigung an Manager - Deaktivierung nach Frist - Dokumentation

12.10 Onboarding und Offboarding

12.10.1 Onboarding-Prozess

12.10.1.1 Neuer Mitarbeiter

Trigger: HR-Benachrichtigung

Zeitraumen: Vor erstem Arbeitstag

Aktivitäten: 1. ☐ Account erstellen 2. ☐ Basis-Berechtigungen zuweisen 3. ☐ E-Mail-Account einrichten 4. ☐ VPN-Zugang bereitstellen 5. ☐ MFA einrichten 6. ☐ Zugangsdaten bereitstellen 7. ☐ Dokumentation in CMDB 8. ☐ Willkommens-E-Mail senden

Verantwortlich: Julia Becker

12.10.2 Offboarding-Prozess

12.10.2.1 Mitarbeiter-Austritt

Trigger: HR-Benachrichtigung

Zeitraumen: Am letzten Arbeitstag

Aktivitäten: 1. ☐ Account deaktivieren 2. ☐ Alle Berechtigungen entfernen 3. ☐ E-Mail-Weiterleitung einrichten (falls erforderlich) 4. ☐ VPN-Zugang sperren 5. ☐ Hardware zurücknehmen 6. ☐ Daten archivieren 7. ☐ Dokumentation aktualisieren 8. ☐ Manager informieren

Verantwortlich: Julia Becker

12.10.2.2 Rollenwechsel

Trigger: HR-Benachrichtigung oder Manager-Anfrage

Zeitraumen: Zum Wechseldatum

Aktivitäten: 1. ☐ Alte Berechtigungen entfernen 2. ☐ Neue Berechtigungen zuweisen 3. ☐ Access Review durchführen 4. ☐ Dokumentation aktualisieren 5. ☐ Benutzer informieren

12.11 Compliance und Auditing

12.11.1 Compliance-Anforderungen

Standard	Anforderung	Umsetzung
DSGVO	Zugriffskontrolle auf personenbezogene Daten	RBAC, Audit Logging
ISO 27001	Access Control Policy	Dieses Dokument
SOX	Separation of Duties	Rollen-Trennung
PCI DSS	Restricted Access to Cardholder Data	Berechtigungsmatrix

12.11.2 Audit-Logging

Protokollierte Events: - Login-Versuche (erfolgreich und fehlgeschlagen) - Berechtigungsänderungen - Privilegierte Aktionen - Zugriff auf sensible Daten - Account-Erstellung/-Löschung - Passwort-Änderungen

Log-Retention: [TODO: z.B. 1 Jahr]

Log-System: [TODO: z.B. Splunk, ELK]

Verantwortlich: Thomas Weber

12.11.3 Audit-Reports

Monatliche Reports: - Neue Accounts - Gelöschte Accounts - Berechtigungsänderungen - Fehlgeschlagene Login-Versuche - Privilegierte Zugriffe

Quartalsweise Reports: - Access Review Ergebnisse - Compliance-Status - Risiko-Assessment - Verbesserungsvorschläge

12.12 Notfall-Zugriff

12.12.1 Break-Glass-Accounts

Definition: Notfall-Accounts für kritische Situationen

Verwendung: - Nur bei kritischen Ausfällen - Wenn normale Zugriffswege nicht verfügbar - Nach Genehmigung durch Anna Schmidt

Anforderungen: - Physisch gesicherte Passwörter - Vollständige Protokollierung - Sofortige Benachrichtigung an Management - Post-Incident-Review

Accounts: - `emergency_admin` - Vollzugriff auf alle Systeme - `emergency_network` - Netzwerk-Notfallzugriff

Passwort-Verwaltung: - Versiegelte Umschläge im Safe - Zugriff nur durch Anna Schmidt oder Thomas Weber

12.13 Kontakte

Access Management Team: - **IT Operations Manager:** Andreas Huemmer - andreas.huemmer@adminsends.de - **CISO:** Thomas Weber - thomas.weber@adminsends.de - **Service Desk Lead:** Julia Becker - julia.becker@adminsends.de - **CIO:** Anna Schmidt - anna.schmidt@adminsends.de

Notfall-Kontakte: - **Break-Glass-Freigabe:** Anna Schmidt - +49 89 12345678-200 - **Security-Incident:** Thomas Weber - +49 89 12345678-300

Dokumentverantwortlicher: IT Operations Manager

Genehmigt durch: CIO

Version: 1.0.0

Organisation: AdminSend GmbH

ewpage

Chapter 13

Monitoring, Alerting und Observability

13.1 Übersicht

Dieses Dokument beschreibt die Monitoring-, Alerting- und Observability-Strategie für den IT-Service. Es definiert Monitoring-Tools, Alerting-Regeln, Schwellwerte und Observability-Konzepte.

Service: {{ meta.service_name }}

Verantwortlich: Andreas Huemmer

Stand: 1.0.0

13.2 Monitoring-Strategie

13.2.1 Monitoring-Ziele

- **Proaktive Erkennung:** Probleme erkennen bevor sie Auswirkungen haben
- **Performance-Optimierung:** Engpässe identifizieren und beheben
- **Verfügbarkeit:** Service-Verfügbarkeit sicherstellen
- **Kapazitätsplanung:** Trends erkennen für Kapazitätsplanung
- **Compliance:** Nachweis der Service-Level-Einhaltung

13.2.2 Monitoring-Ebenen

Layer 7: Business Metrics

(Transaktionen, User Experience, Business KPIs)

Layer 6: Application Monitoring

(Application Performance, Errors, Response Times)

Layer 5: Service Monitoring
(Service Health, API Endpoints, Dependencies)

Layer 4: Infrastructure Monitoring
(Servers, Network, Storage, Virtualization)

Layer 3: System Monitoring
(CPU, Memory, Disk, Network Interfaces)

Layer 2: Network Monitoring
(Connectivity, Bandwidth, Latency, Packet Loss)

Layer 1: Physical Monitoring
(Power, Cooling, Environmental)

13.3 Monitoring-Tools

13.3.1 Tool-Stack

Tool	Verwendung	Verantwortlich	URL
[TODO: z.B. Prometheus]	Metriken-Sammlung	Monitoring Team	[TODO]
[TODO: z.B. Grafana]	Visualisierung	Monitoring Team	[TODO]
[TODO: z.B. Nagios/Zabbix]	Infrastructure Monitoring	IT Operations	[TODO]
[TODO: z.B. ELK Stack]	Log-Aggregation	IT Operations	[TODO]
[TODO: z.B. Jaeger]	Distributed Tracing	Development Team	[TODO]
[TODO: z.B. Pingdom]	Synthetic Monitoring	IT Operations	[TODO]
[TODO: z.B. New Relic/Datadog]	APM	Development Team	[TODO]

13.3.2 Tool-Integration

Datenfluss:

Agents
(Exporters)

Collectors
(Prometheus)

Storage
(TSDB)

Visualization Alerting
(Grafana) (Alertmanager)

13.4 Infrastructure Monitoring

13.4.1 Server-Monitoring

13.4.1.1 Metriken

Metrik	Beschreibung	Schwellwert		Frequenz
		Warning	Critical	
CPU Usage	CPU-Auslastung	> 80%	> 95%	1 Min
Memory Usage	RAM-Auslastung	> 85%	> 95%	1 Min
Disk Usage	Festplatten-Auslastung	> 80%	> 90%	5 Min
Disk I/O	Disk-Operationen	> 80%	> 95%	1 Min
Network Traffic	Netzwerk-Durchsatz	> 80%	> 95%	1 Min

Metrik	Beschreibung	Schwellwert	Schwellwert Critical	Frequenz
		Warning		
Load Average	System-Last	> 4.0	> 8.0	1 Min
Swap Usage	Swap-Nutzung	> 50%	> 80%	5 Min

13.4.1.2 Überwachte Server

Server	Standort	Rolle	Monitoring-Agent	Status
{{ net-box.device.name }}	{{ netbox.device.site }}	{{ net-box.device.role }}	[TODO: Agent]	Aktiv
[TODO]	[TODO]	[TODO]	[TODO]	Aktiv

13.4.2 Netzwerk-Monitoring

13.4.2.1 Metriken

Metrik	Beschreibung	Schwellwert	Schwellwert Critical	Frequenz
		Warning		
Interface Status	Port Up/Down	Down	Down > 5 Min	30 Sek
Bandwidth Usage	Bandbreiten-Auslastung	> 80%	> 95%	1 Min
Packet Loss	Paketverlust	> 1%	> 5%	1 Min
Latency	Netzwerk-Latenz	> 50ms	> 100ms	1 Min
Error Rate	Fehlerrate	> 0.1%	> 1%	1 Min
CRC Errors	CRC-Fehler	> 0	> 100	5 Min

13.4.2.2 Überwachte Netzwerkgeräte

Gerät	Typ	Standort	Management-IP	Status
{{ net-box.device.name }}	{{ net-box.device.device_type }}	{{ netbox.device.site }}	{{ net-box.device.primary_ip }}	Aktiv
[TODO]	[TODO]	[TODO]	[TODO]	Aktiv

13.4.3 Storage-Monitoring

13.4.3.1 Metriken

Metrik	Beschreibung	Schwellwert Warning	Schwellwert Critical	Frequenz
Capacity	Speicherkapazität	> 80%	> 90%	5 Min
IOPS	I/O-Operationen	> 80% Max	> 95% Max	1 Min
Throughput	Durchsatz	> 80% Max	> 95% Max	1 Min
Latency	Zugriffszeit	> 20ms	> 50ms	1 Min
Disk Health	Festplatten-Gesundheit	SMART Warning	SMART Error	1 Stunde

13.4.4 Virtualisierung-Monitoring

13.4.4.1 Hypervisor-Metriken

Metrik	Beschreibung	Schwellwert Warning	Schwellwert Critical	Frequenz
Host CPU	CPU-Auslastung	> 80%	> 95%	1 Min
Host Memory	Host RAM-Auslastung	> 85%	> 95%	1 Min
VM Count	Anzahl VMs	> 80% Max	> 95% Max	5 Min
Datastore Usage	Datastore-Auslastung	> 80%	> 90%	5 Min
VM Performance	VM-Performance	Degraded	Critical	1 Min

13.5 Application Monitoring

13.5.1 Application Performance Monitoring (APM)

13.5.1.1 Metriken

Metrik	Beschreibung	Schwellwert Warning	Schwellwert Critical	Frequenz
Response Time	Antwortzeit	> 500ms	> 2000ms	Real-time
Error Rate	Fehlerrate	> 1%	> 5%	Real-time
Throughput	Requests/Sekunde	< 80% Normal	< 50% Normal	Real-time
Apdex Score	User Satisfaction	< 0.85	< 0.70	Real-time
Database Query Time	DB-Abfragezeit	> 100ms	> 500ms	Real-time

Metrik	Beschreibung	Schwellwert		Frequenz
		Warning	Schwellwert Critical	
External API Latency	API-Latenz	> 200ms	> 1000ms	Real-time

13.5.2 Synthetic Monitoring

Überwachte Endpunkte:

Endpunkt	Typ	Frequenz	Erwartete Response	Timeout
[TODO: URL]	HTTP/HTTPS	1 Min	200 OK	5 Sek
[TODO: URL]	API	1 Min	200 OK	3 Sek
[TODO: URL]	Health Check	30 Sek	200 OK	2 Sek

Prüfungen: - HTTP-Status-Code - Response-Zeit - Content-Validierung - SSL-Zertifikat-Gültigkeit - DNS-Auflösung

13.6 Observability

13.6.1 Die drei Säulen der Observability

13.6.1.1 1. Metrics (Metriken)

Definition: Numerische Werte über Zeit

Verwendung: Trends, Alerts, Dashboards

Tools: Prometheus, Grafana

Beispiele: - CPU-Auslastung - Request-Rate - Error-Rate - Response-Time

13.6.1.2 2. Logs (Protokolle)

Definition: Ereignis-basierte Aufzeichnungen

Verwendung: Debugging, Audit, Troubleshooting

Tools: ELK Stack, Splunk

Beispiele: - Application-Logs - System-Logs - Access-Logs - Error-Logs

13.6.1.3 3. Traces (Ablaufverfolgung)

Definition: Request-Flow durch verteilte Systeme

Verwendung: Performance-Analyse, Bottleneck-Identifikation

Tools: Jaeger, Zipkin

Beispiele: - Distributed Tracing - Service-Dependencies - Latency-Breakdown - Error-Propagation

13.6.2 Observability-Strategie

User Request

Metrics Collection → Prometheus

Log Aggregation → ELK Stack

Distributed Tracing → Jaeger

Correlation &
Visualization → Grafana

13.7 Alerting

13.7.1 Alerting-Strategie

Prinzipien: - **Actionable:** Jeder Alert erfordert eine Aktion - **Relevant:** Nur kritische Ereignisse alarmieren - **Timely:** Alerts in Echtzeit - **Clear:** Eindeutige Alert-Beschreibungen - **Escalation:** Definierte Eskalationspfade

13.7.2 Alert-Severity-Levels

Level	Beschreibung	Reaktionszeit	Eskalation	Beispiel
Critical	Service-Ausfall	Sofort	Sofort	Service Down
High	Schwerwiegendes Problem	15 Min	Nach 30 Min	CPU > 95%
Medium	Problem erfordert Aufmerksamkeit	1 Stunde	Nach 4 Stunden	Disk > 85%
Low	Informativ, keine sofortige Aktion	1 Tag	Keine	Backup Warning
Info	Informativ	Keine	Keine	Backup Success

13.7.3 Alerting-Regeln

13.7.3.1 Infrastructure Alerts

Alert	Bedingung	Severity	Aktion	Verantwortlich
Server Down	Ping failed > 5 Min	Critical	Sofort prüfen	Julia Becker
High CPU	CPU > 95% für 5 Min	High	Performance prüfen	IT Operations
High Memory	Memory > 95% für 5 Min	High	Memory-Leak prüfen	IT Operations
Disk Full	Disk > 90%	High	Speicher freigeben	IT Operations
Disk Warning	Disk > 80%	Medium	Kapazität planen	IT Operations

13.7.3.2 Application Alerts

Alert	Bedingung	Severity	Aktion	Verantwortlich
Service Down	Health Check failed	Critical	Service restart	Julia Becker
High Error Rate	Errors > 5% für 5 Min	High	Logs prüfen	Development Team
Slow Response	Response Time > 2s	High	Performance prüfen	Development Team
API Failure	External API down	High	Vendor kontaktieren	IT Operations

13.7.3.3 Network Alerts

Alert	Bedingung	Severity	Aktion	Verantwortlich
Link Down	Interface down > 5 Min	Critical	Verbindung prüfen	Network Team
High Bandwidth	Bandwidth > 95%	High	Traffic analysieren	Network Team
High Latency	Latency > 100ms	Medium	Routing prüfen	Network Team
Packet Loss	Loss > 5%	High	Verbindung prüfen	Network Team

13.7.4 Alert-Routing

Alert Trigger

Alert Manager

E-Mail

Slack

SMS

PagerDuty

13.7.5 Alert-Empfänger

Severity	Primär	Sekundär	Eskalation
Critical	On-Call Engineer	IT Ops Manager	CIO
High	IT Operations Team	IT Ops Manager	-
Medium	IT Operations Team	-	-
Low	E-Mail an Team	-	-

On-Call-Rotation: - **Woche 1:** [TODO: Name] - **Woche 2:** [TODO: Name] - **Woche 3:** [TODO: Name] - **Woche 4:** [TODO: Name]

13.8 Dashboards

13.8.1 Dashboard-Übersicht

13.8.1.1 Executive Dashboard

Zielgruppe: Management

Inhalt: - Service-Verfügbarkeit (aktuell und historisch) - SLA-Compliance - Incident-Übersicht - Performance-Trends - Kosten-Übersicht

URL: [TODO: Dashboard-URL]

13.8.1.2 Operations Dashboard

Zielgruppe: IT Operations

Inhalt: - Aktuelle Alerts - System-Health-Status - Performance-Metriken - Capacity-Trends - Incident-Status

URL: [TODO: Dashboard-URL]

13.8.1.3 Application Dashboard

Zielgruppe: Development Team

Inhalt: - Application-Performance - Error-Rates - Response-Times - Database-Performance - API-Latencies

URL: [TODO: Dashboard-URL]

13.8.1.4 Infrastructure Dashboard

Zielgruppe: Infrastructure Team

Inhalt: - Server-Status - Network-Status - Storage-Status - Virtualization-Status - Environmental-Status

URL: [TODO: Dashboard-URL]

13.8.2 Dashboard-Best-Practices

1. **Single Pane of Glass:** Alle wichtigen Informationen auf einen Blick
 2. **Color Coding:** Rot (Critical), Orange (Warning), Grün (OK)
 3. **Drill-Down:** Von Übersicht zu Details navigieren
 4. **Real-Time:** Aktuelle Daten anzeigen
 5. **Historical:** Trends über Zeit zeigen
 6. **Annotations:** Wichtige Events markieren
-

13.9 Monitoring-Prozesse

13.9.1 Tägliche Monitoring-Routinen

Morgen-Check (08:00 Uhr): - [] Dashboards prüfen - [] Offene Alerts reviewen - [] Overnight-Incidents prüfen - [] Backup-Status validieren - [] Performance-Trends analysieren

Tags-Monitoring: - [] Kontinuierliche Alert-Überwachung - [] Incident-Response bei Alerts - [] Performance-Optimierung - [] Kapazitäts-Monitoring

Abend-Check (18:00 Uhr): - [] Tages-Alerts reviewen - [] Offene Issues dokumentieren - [] Handover an Nachtschicht (falls 24/7) - [] Wartungsarbeiten planen

13.9.2 Wöchentliche Aktivitäten

- ☐ Monitoring-Daten analysieren
- ☐ Alert-Tuning durchführen
- ☐ False-Positives reduzieren
- ☐ Dashboard-Updates
- ☐ Kapazitäts-Trends reviewen

13.9.3 Monatliche Aktivitäten

- ☐ Monitoring-Coverage prüfen
 - ☐ SLA-Reports erstellen
 - ☐ Performance-Trends analysieren
 - ☐ Monitoring-Tools aktualisieren
 - ☐ Alert-Regeln optimieren
-

13.10 Service Level Indicators (SLIs)

13.10.1 Definierte SLIs

SLI	Beschreibung	Messung	Zielwert
Availability	Service-Verfügbarkeit	Uptime / Total Time	99.5%
Latency	Response-Zeit	P95 Response Time	500ms
Error Rate	Fehlerrate	Errors / Total Requests	0.1%
Throughput	Durchsatz	Requests / Second	[TODO]
Saturation	Ressourcen-Auslastung	CPU/Memory/Disk Usage	80%

13.10.2 SLI-Monitoring

Datenquellen: - Synthetic Monitoring - Real User Monitoring (RUM) - Application Logs - Infrastructure Metrics

Reporting: - Echtzeit-Dashboards - Tägliche Reports - Monatliche SLA-Reports

13.11 Incident Response

13.11.1 Monitoring-basierte Incident Response

Alert Trigger

Alert Received

Initial Triage

Incident Created

Investigation

Resolution

Post-Mortem

Details: Siehe Kapitel 0120 (Incident Management)

13.12 Monitoring-Dokumentation

13.12.1 Runbooks

Für jeden kritischen Alert existiert ein Runbook: - Alert-Beschreibung - Mögliche Ursachen - Diagnose-Schritte - Lösungsschritte - Eskalationspfad

Runbook-Verzeichnis: Siehe Kapitel 0240 (Runbooks)

13.12.2 Known Issues

Bekannte Monitoring-Probleme und Workarounds: - False-Positive-Alerts - Monitoring-Gaps - Tool-Limitierungen

Known Issues: Siehe Kapitel 0260 (Bekannte Probleme und FAQ)

13.13 Monitoring-Tools-Zugriff

13.13.1 Tool-Zugänge

Tool	URL	Authentifizierung	Zugriff
[TODO: Monitoring-Tool]	[TODO: URL]	SSO	IT Operations
[TODO: Dashboard-Tool]	[TODO: URL]	SSO	Alle
[TODO: Log-Tool]	[TODO: URL]	SSO	IT Operations
[TODO: APM-Tool]	[TODO: URL]	SSO	Development

13.13.2 Berechtigungen

- **Administrator:** Andreas Huemmer
 - **Operator:** IT Operations Team
 - **Read-Only:** Management, Auditors
-

13.14 Kontakte

Monitoring-Team: - **IT Operations Manager:** Andreas Huemmer - andreas.huemmer@adminsends.de
- **Service Desk Lead:** Julia Becker - julia.becker@adminsends.de - **On-Call Engineer:** [TODO:
Rotation] - [TODO: On-Call-Nummer]

Eskalation: - **Level 2:** Andreas Huemmer - +49 89 12345678-250 - **Level 3:** Anna Schmidt - +49
89 12345678-200

Dokumentverantwortlicher: IT Operations Manager

Genehmigt durch: CIO

Version: 1.0.0

Organisation: AdminSend GmbH

ewpage

Chapter 14

Incident Management Runbook

14.1 Zweck und Geltungsbereich

Dieses Dokument beschreibt den Incident-Management-Prozess für AdminSend GmbH gemäß ITIL v4 Best Practices. Es definiert Kategorien, Prioritäten, Eskalationsprozesse und Standard-Runbooks für die Behandlung von Service-Störungen.

Geltungsbereich: Alle IT-Services und -Systeme von AdminSend GmbH

Verantwortlich: Andreas Huemmer (andreas.huemmer@adminsends.de)

14.2 Incident-Definition

Ein **Incident** ist eine ungeplante Unterbrechung oder Qualitätsminderung eines IT-Service. Das Ziel des Incident Managements ist die schnellstmögliche Wiederherstellung des normalen Service-Betriebs.

14.2.1 Abgrenzung zu anderen Prozessen

Prozess	Fokus	Ziel
Incident Management	Symptombehandlung	Schnelle Wiederherstellung
Problem Management	Ursachenanalyse	Dauerhafte Lösung
Change Management	Geplante Änderungen	Kontrollierte Implementierung
Service Request	Standardanfragen	Erfüllung von Anforderungen

14.3 Incident-Kategorien

14.3.1 Kategorisierung nach Bereich

Kategorie	Beschreibung	Beispiele
Hardware	Physische Geräte und Komponenten	Server-Ausfall, Festplatten-Defekt, Netzwerk-Hardware
Software	Anwendungen und Betriebssysteme	Applikations-Crash, Lizenz-Probleme, Software-Bugs
Netzwerk	Netzwerkverbindungen und -dienste	Verbindungsabbrüche, DNS-Probleme, Firewall-Blockaden
Security	Sicherheitsvorfälle	Malware, Unauthorized Access, Data Breach
Performance	Leistungsprobleme	Langsame Antwortzeiten, Hohe CPU-Last, Memory Leaks
Daten	Datenverlust oder -korruption	Datenbank-Korruption, Backup-Fehler, Datenverlust
Benutzer	Zugriffs- und Berechtigungsprobleme	Login-Probleme, Passwort-Reset, Fehlende Berechtigungen

14.3.2 Kategorisierung nach Service

- E-Mail-Service
- File-Server
- Datenbank-Service
- Web-Applikationen
- Netzwerk-Infrastruktur
- Backup-Systeme
- Monitoring-Systeme
- [Weitere Services gemäß Service-Katalog]

14.4 Incident-Prioritäten

Die Priorität eines Incidents ergibt sich aus **Impact** (Auswirkung) und **Urgency** (Dringlichkeit).

14.4.1 Impact-Bewertung

Impact	Beschreibung	Betroffene Nutzer
Hoch	Kritischer Service komplett ausgefallen	> 50% der Nutzer oder geschäftskritischer Service
Mittel	Service eingeschränkt verfügbar	10-50% der Nutzer oder wichtiger Service
Niedrig	Einzelne Nutzer betroffen	< 10% der Nutzer oder unkritischer Service

14.4.2 Urgency-Bewertung

Urgency	Beschreibung	Zeitfenster
Hoch	Sofortige Bearbeitung erforderlich	Geschäftsprozess blockiert
Mittel	Zeitnahe Bearbeitung erforderlich	Geschäftsprozess beeinträchtigt
Niedrig	Kann geplant bearbeitet werden	Keine unmittelbare Auswirkung

14.4.3 Prioritäts-Matrix

	Urgency: Hoch	Urgency: Mittel	Urgency: Niedrig
Impact: Hoch	P1 - Kritisch	P2 - Hoch	P3 - Mittel
Impact: Mittel	P2 - Hoch	P3 - Mittel	P4 - Niedrig
Impact: Niedrig	P3 - Mittel	P4 - Niedrig	P5 - Geplant

14.4.4 Service Level Targets

Priorität	Reaktionszeit	Lösungszeit	Eskalation nach
P1 - Kritisch	15 Minuten	4 Stunden	1 Stunde
P2 - Hoch	30 Minuten	8 Stunden	2 Stunden
P3 - Mittel	2 Stunden	24 Stunden	8 Stunden
P4 - Niedrig	4 Stunden	48 Stunden	24 Stunden
P5 - Geplant	1 Arbeitstag	5 Arbeitstage	-

14.5 Incident-Management-Prozess

14.5.1 Prozessübersicht (ITIL v4)

Incident
Detection

Incident
Logging

Categorization
& Prioritization

Initial
Diagnosis

Known	Yes
Error?	Apply
	Workaround
No	

Investigation
& Diagnosis

Resolution
& Recovery

Incident
Closure

14.5.2 1. Incident Detection

Erkennungsquellen: - Monitoring-Alerts ({{ netbox.monitoring_system }}) - Service Desk Tickets - Benutzer-Meldungen - Automatische Event-Korrelation

Verantwortlich: Monitoring-System, Service Desk

14.5.3 2. Incident Logging

Erforderliche Informationen: - Incident-ID (automatisch generiert) - Zeitstempel der Meldung - Betroffener Service/System - Symptombeschreibung - Betroffene Nutzer/Standorte - Melder (Name, Kontakt)

Tool: {{ meta.ticketing_system }}

Verantwortlich: Service Desk

14.5.4 3. Categorization & Prioritization

Aktivitäten: - Kategorie zuweisen (Hardware, Software, Netzwerk, etc.) - Impact bewerten - Urgency bewerten - Priorität berechnen (P1-P5) - Betroffenen Service identifizieren

Verantwortlich: Service Desk / Incident Manager

14.5.5 4. Initial Diagnosis

Aktivitäten: - Symptome analysieren - Logs prüfen - Monitoring-Daten auswerten - Known Error Database durchsuchen - Erste Lösungsversuche (Level 1)

Verantwortlich: Service Desk (Level 1)

14.5.6 5. Investigation & Diagnosis

Aktivitäten: - Detaillierte technische Analyse - Root-Cause-Identifikation (wenn möglich) - Workaround-Entwicklung - Eskalation an Spezialisten (Level 2/3)

Verantwortlich: IT Operations Team (Level 2/3)

14.5.7 6. Resolution & Recovery

Aktivitäten: - Lösung implementieren - Service wiederherstellen - Funktionalität testen - Nutzer informieren

Verantwortlich: IT Operations Team

14.5.8 7. Incident Closure

Aktivitäten: - Nutzer-Bestätigung einholen - Dokumentation vervollständigen - Incident schließen - Ggf. Problem-Ticket erstellen

Verantwortlich: Service Desk

14.6 Eskalationsprozesse

14.6.1 Hierarchische Eskalation

Level	Rolle	Kontakt	Eskalation bei
Level 1	Service Desk	julia.becker@adminsends.de	Standard-Incidents
Level 2	IT Operations Team	andreas.huemmer@adminsends.de	Komplexe technische Probleme
Level 3	Spezialisten / Vendor	[Vendor-Kontakte]	Spezialwissen erforderlich
Management	CIO	anna.schmidt@adminsends.de	Incidents > 2h

14.6.2 Funktionale Eskalation

Bereich	Ansprechpartner	Kontakt	Zuständigkeit
Netzwerk	Network Team	E-Mail	Netzwerk-Infrastruktur
Server	Server Team	E-Mail	Server und Virtualisierung
Datenbank	DBA Team	E-Mail	Datenbank-Systeme
Security	Security Team	thomas.weber@adminsends.de	Sicherheitsvorfälle

Bereich	Ansprechpartner	Kontakt	Zuständigkeit
Applikationen	Application Team	E-Mail	Business-Applikationen

14.6.3 Eskalations-Trigger

Automatische Eskalation bei: - P1-Incident nicht gelöst nach 1 Stunde - P2-Incident nicht gelöst nach 2 Stunden - P3-Incident nicht gelöst nach 8 Stunden - Mehrfache Wiederöffnung desselben Incidents - Security-Incidents (sofort an CISO)

Management-Eskalation bei: - P1-Incidents (Information an CIO) - Incidents mit hoher Medienaufmerksamkeit - Incidents mit rechtlichen Implikationen - Mehrere gleichzeitige P1/P2-Incidents

14.7 Standard-Runbooks

14.7.1 Runbook 1: Server nicht erreichbar

Symptome: Server antwortet nicht auf Ping, Services nicht verfügbar

Priorität: P1 oder P2 (abhängig von Service-Kritikalität)

Diagnose-Schritte: 1. Ping-Test durchführen: `ping {{ netbox.server.ip }}` 2. Monitoring-Dashboard prüfen 3. Physischen Zustand prüfen (falls vor Ort) 4. Netzwerk-Konnektivität prüfen 5. Hypervisor-Status prüfen (bei VMs)

Lösungsschritte: 1. Netzwerk-Verbindung wiederherstellen (falls Netzwerk-Problem) 2. Server-Neustart durchführen (falls hängend) 3. Hypervisor-Migration durchführen (bei VM-Problem) 4. Hardware-Austausch initiieren (bei Hardware-Defekt) 5. Backup-System aktivieren (falls primäres System defekt)

Eskalation: Nach 30 Minuten an Level 2, nach 1 Stunde an Management

14.7.2 Runbook 2: Applikation langsam / nicht erreichbar

Symptome: Lange Antwortzeiten, Timeouts, HTTP 500/503 Fehler

Priorität: P2 oder P3

Diagnose-Schritte: 1. Applikations-Logs prüfen 2. Performance-Metriken analysieren (CPU, RAM, Disk I/O) 3. Datenbank-Performance prüfen 4. Netzwerk-Latenz messen 5. Load-Balancer-Status prüfen

Lösungsschritte: 1. Applikations-Neustart durchführen 2. Cache leeren 3. Datenbank-Queries optimieren 4. Ressourcen skalieren (CPU/RAM erhöhen) 5. Traffic auf andere Instanzen umleiten

Eskalation: Nach 2 Stunden an Application Team

14.7.3 Runbook 3: Datenbank-Verbindungsfehler

Symptome: Connection timeout, "Too many connections", Applikation kann nicht auf DB zugreifen

Priorität: P1 oder P2

Diagnose-Schritte: 1. Datenbank-Status prüfen: `systemctl status postgresql` 2. Connection-Pool prüfen 3. Datenbank-Logs analysieren 4. Disk-Space prüfen 5. Netzwerk-Konnektivität zur DB prüfen

Lösungsschritte: 1. Datenbank-Service neu starten 2. Connection-Pool-Limits erhöhen 3. Lange laufende Queries beenden 4. Disk-Space freigeben 5. Failover zu Standby-Datenbank

Eskalation: Sofort an DBA Team bei P1

14.7.4 Runbook 4: Backup fehlgeschlagen

Symptome: Backup-Job meldet Fehler, Backup-Monitoring-Alert

Priorität: P2 oder P3

Diagnose-Schritte: 1. Backup-Logs prüfen 2. Disk-Space auf Backup-Target prüfen 3. Netzwerk-Verbindung zu Backup-Storage prüfen 4. Backup-Software-Status prüfen 5. Quell-System-Status prüfen

Lösungsschritte: 1. Backup-Job manuell neu starten 2. Disk-Space auf Backup-Target freigeben 3. Netzwerk-Verbindung wiederherstellen 4. Backup-Software neu starten 5. Alternative Backup-Methode verwenden

Eskalation: Nach 4 Stunden an Backup-Team

14.7.5 Runbook 5: Security-Incident (Malware/Intrusion)

Symptome: Malware-Alert, ungewöhnliche Netzwerk-Aktivität, Unauthorized Access

Priorität: P1 (immer)

Diagnose-Schritte: 1. Alert-Details analysieren 2. Betroffene Systeme identifizieren 3. Ausmaß der Kompromittierung bewerten 4. Logs sichern (Forensik) 5. CISO informieren

Lösungsschritte: 1. Betroffene Systeme isolieren (Netzwerk-Trennung) 2. Malware-Scan durchführen 3. Kompromittierte Accounts sperren 4. Passwörter zurücksetzen 5. Forensische Analyse durchführen 6. Systeme neu aufsetzen (falls erforderlich)

Eskalation: Sofort an CISO (thomas.weber@adminsind.de)

14.7.6 Runbook 6: Netzwerk-Ausfall

Symptome: Keine Netzwerk-Konnektivität, Geräte nicht erreichbar

Priorität: P1 oder P2

Diagnose-Schritte: 1. Betroffene Netzwerk-Segmente identifizieren 2. Switch/Router-Status prüfen 3. Physische Verkabelung prüfen 4. VLAN-Konfiguration prüfen 5. Routing-Tabellen prüfen

Lösungsschritte: 1. Netzwerk-Geräte neu starten 2. Defekte Kabel austauschen 3. VLAN-Konfiguration korrigieren 4. Routing-Probleme beheben 5. Failover zu Backup-Verbindung

Eskalation: Nach 30 Minuten an Network Team

14.8 Kommunikationsprozesse

14.8.1 Interne Kommunikation

Bei Incident-Eröffnung: - Service Desk informiert betroffene Nutzer - IT Operations Team wird bei P1/P2 sofort informiert - Management wird bei P1 informiert

Während der Bearbeitung: - Regelmäßige Status-Updates (P1: alle 30 Min, P2: alle 2h) - Eskalations-Benachrichtigungen - Team-Kommunikation über {{ meta.collaboration_tool }}

Bei Incident-Lösung: - Nutzer-Benachrichtigung über Lösung - Management-Information bei P1/P2 - Dokumentation im Ticket-System

14.8.2 Externe Kommunikation

Stakeholder-Information: - Geschäftsführung bei kritischen Incidents - Kunden bei Service-Ausfällen - Externe Partner bei Abhängigkeiten

Kommunikationskanäle: - E-Mail: info@adminsends.de - Status-Page: {{ meta.status_page_url }} - Telefon: +49 89 12345678

Kommunikations-Template:

Betreff: [P1/P2] Service-Störung: [Service-Name]

Sehr geehrte Damen und Herren,

wir informieren Sie über eine aktuelle Service-Störung:

Service: [Service-Name]

Priorität: [P1/P2/P3]

Beginn: [Zeitstempel]

Auswirkung: [Beschreibung]

Status: [In Bearbeitung / Gelöst]

Wir arbeiten mit Hochdruck an der Lösung und halten Sie auf dem Laufenden.

Nächstes Update: [Zeitpunkt]

Mit freundlichen Grüßen

AdminSend GmbH

IT Operations Team

14.9 Major Incident Management

14.9.1 Definition Major Incident

Ein **Major Incident** ist ein Incident mit: - Priorität P1 - Auswirkung auf kritische Geschäftsprozesse - Hohe Anzahl betroffener Nutzer (> 50%) - Potenzielle finanzielle oder rechtliche Konsequenzen

14.9.2 Major Incident Team

Rolle	Person	Verantwortung
Incident Manager	Andreas Huemmer	Koordination und Kommunikation
Technical Lead	[Name]	Technische Lösungsfindung
Communication Lead	[Name]	Stakeholder-Kommunikation
Management Rep	Anna Schmidt	Entscheidungen und Eskalation

14.9.3 Major Incident Prozess

1. **Incident Declaration:** Incident Manager erklärt Major Incident
2. **Team Assembly:** Major Incident Team wird zusammengerufen
3. **War Room:** Dedizierter Kommunikationskanal (z.B. Conference Call)
4. **Status Updates:** Alle 30 Minuten an Stakeholder
5. **Resolution:** Koordinierte Lösungsumsetzung
6. **Post-Incident Review:** Pflicht-Postmortem innerhalb 48h

14.10 Metriken und Reporting

14.10.1 Key Performance Indicators (KPIs)

Metrik	Zielwert	Messung
Mean Time to Respond (MTTR)	< 15 Min (P1)	Durchschnittliche Reaktionszeit
Mean Time to Resolve (MTTR)	< 4h (P1)	Durchschnittliche Lösungszeit
First Call Resolution Rate	> 70%	Lösung beim ersten Kontakt
Incident Reopen Rate	< 5%	Wiederöffnungsrate
SLA Compliance	> 95%	Einhaltung der SLA-Zeiten

14.10.2 Reporting

Tägliches Reporting: - Anzahl offener Incidents (nach Priorität) - P1/P2 Incidents in Bearbeitung - SLA-Verstöße

Wöchentliches Reporting: - Incident-Trend-Analyse - Top-5 Incident-Kategorien - Eskalations-Statistik

Monatliches Reporting: - KPI-Dashboard - Service-Verfügbarkeit - Verbesserungsmaßnahmen

14.11 Tools und Systeme

14.11.1 Incident-Management-Tool

- **System:** {{ meta.ticketing_system }}

- **URL:** {{ meta.ticketing_system_url }}
- **Zugriff:** Alle IT-Mitarbeiter

14.11.2 Monitoring-System

- **System:** {{ netbox.monitoring_system }}
- **URL:** {{ meta.monitoring_url }}
- **Zugriff:** IT Operations Team

14.11.3 Kommunikations-Tools

- **Chat:** {{ meta.collaboration_tool }}
- **Conference:** {{ meta.conference_system }}
- **Status-Page:** {{ meta.status_page_url }}

14.12 Anhang

14.12.1 Incident-Kategorien (vollständig)

- Hardware > Server
- Hardware > Storage
- Hardware > Network
- Software > Operating System
- Software > Application
- Software > Database
- Network > Connectivity
- Network > Performance
- Security > Malware
- Security > Unauthorized Access
- Security > Data Breach
- Performance > Slow Response
- Performance > High Load
- Data > Corruption
- Data > Loss
- User > Access
- User > Authentication

14.12.2 Kontakte und Rufbereitschaft

Team	Primär	Sekundär	Rufbereitschaft
Service Desk	julia.becker@adminsends.de	[Backup]	24/7
IT Operations	andreas.huemmer@adminsends.de	[Backup]	24/7
Network Team	E-Mail	[Backup]	On-Call
Security Team	thomas.weber@adminsends.de	[Backup]	24/7

14.12.3 Referenzen

- ITIL v4 Foundation

- ISO/IEC 20000-1:2018 - Service Management
- Interne Service-Level-Agreements
- Eskalations-Matrix

Dokumentverantwortlicher: IT Operations Manager

Genehmigt durch: CIO

Version: 1.0.0

Klassifizierung: internal

Letzte Aktualisierung: {{ meta.date }}

ewpage

Chapter 15

Problem Management und Postmortems

15.1 Zweck und Geltungsbereich

Dieses Dokument beschreibt den Problem-Management-Prozess für AdminSend GmbH gemäß ITIL v4 Best Practices. Es definiert die systematische Analyse wiederkehrender Incidents, Root-Cause-Analysis-Methoden, Postmortem-Prozesse und die Verwaltung der Known Error Database.

Geltungsbereich: Alle IT-Services und -Systeme von AdminSend GmbH

Verantwortlich: Andreas Huemmer (andreas.huemmer@adminsends.de)

15.2 Problem-Definition

Ein **Problem** ist die unbekannte Ursache eines oder mehrerer Incidents. Das Ziel des Problem Managements ist die Identifikation und Beseitigung der Grundursache, um zukünftige Incidents zu verhindern.

15.2.1 Abgrenzung Incident vs. Problem

Aspekt	Incident	Problem
Fokus	Symptome	Ursachen
Ziel	Schnelle Wiederherstellung	Dauerhafte Lösung
Zeitraumen	Sofort	Geplant
Ansatz	Workaround	Root-Cause-Elimination
Prozess	Reaktiv	Proaktiv

15.3 Problem-Management-Prozess

15.3.1 Prozessübersicht (ITIL v4)

Problem
Detection

Problem
Logging

Problem
Categorization

Problem
Prioritization

Investigation
& Diagnosis
(RCA)

Workaround
Identification

Known Error
Recording

Problem
Resolution

Problem
Closure

15.3.2 1. Problem Detection

Erkennungsquellen: - Wiederkehrende Incidents (> 3x in 30 Tagen) - Trend-Analyse von Incident-Daten - Proaktive Monitoring-Analysen - Major Incident Reviews - Vendor-Bulletins und Security-Advisories

Trigger für Problem-Erstellung: - Mehrere ähnliche Incidents - Incidents mit hohem Business-Impact - Incidents ohne bekannte Lösung - Strukturelle Schwachstellen

Verantwortlich: Problem Manager, IT Operations Team

15.3.3 2. Problem Logging

Erforderliche Informationen: - Problem-ID (automatisch generiert) - Verknüpfte Incident-IDs - Symptombeschreibung - Betroffene Services/Systeme - Betroffene Configuration Items (CIs) - Erste Hypothesen zur Ursache

Tool: {{ meta.ticketing_system }}

Verantwortlich: Problem Manager

15.3.4 3. Problem Categorization

Kategorien: - Hardware-Probleme - Software-Probleme - Netzwerk-Probleme - Prozess-Probleme - Dokumentations-Probleme - Kapazitäts-Probleme - Sicherheits-Probleme

Verantwortlich: Problem Manager

15.3.5 4. Problem Prioritization

Prioritäts-Faktoren: - Anzahl betroffener Incidents - Business-Impact - Häufigkeit des Auftretens - Verfügbarkeit von Workarounds - Ressourcen-Verfügbarkeit

Prioritäts-Stufen:

Priorität	Beschreibung	Bearbeitungszeit
P1 - Kritisch	Häufige P1-Incidents, kein Workaround	Sofort
P2 - Hoch	Häufige P2-Incidents, temporärer Workaround	1 Woche
P3 - Mittel	Moderate Häufigkeit, Workaround vorhanden	1 Monat
P4 - Niedrig	Seltene Incidents, geringer Impact	Geplant

15.3.6 5. Investigation & Diagnosis (Root Cause Analysis)

RCA-Methoden: - 5-Why-Analyse - Fishbone-Diagramm (Ishikawa) - Fault Tree Analysis - Timeline-Analyse - Log-Korrelation

Aktivitäten: - Daten sammeln (Logs, Monitoring, Konfigurationen) - Hypothesen entwickeln - Tests durchführen - Root-Cause identifizieren - Dokumentation erstellen

Verantwortlich: Problem Manager, Technical Specialists

15.3.7 6. Workaround Identification

Workaround-Kriterien: - Reduziert Impact oder Häufigkeit - Praktikabel für Incident-Teams - Dokumentiert und getestet - Temporäre Lösung bis zur permanenten Behebung

Dokumentation: - Workaround-Beschreibung - Anwendungsschritte - Einschränkungen - Gültigkeitsdauer

15.3.8 7. Known Error Recording

Known Error Database (KEDB): - Problem-Beschreibung - Root-Cause - Workaround - Permanente Lösung (wenn verfügbar) - Verknüpfte Incidents - Verknüpfte CIs

Zugriff: Alle IT-Mitarbeiter (Read), Problem Manager (Write)

15.3.9 8. Problem Resolution

Lösungsansätze: - Software-Patch oder -Update - Konfigurationsänderung - Hardware-Austausch - Prozess-Verbesserung - Dokumentations-Update - Training

Change-Management: - Permanente Lösungen erfordern Change-Request - Change-Planung und -Genehmigung - Implementierung über Change-Prozess

15.3.10 9. Problem Closure

Closure-Kriterien: - Root-Cause identifiziert und dokumentiert - Permanente Lösung implementiert - Keine neuen Incidents aufgetreten (Monitoring-Periode) - Dokumentation vollständig - Lessons Learned dokumentiert

Verantwortlich: Problem Manager

15.4 Root Cause Analysis (RCA) Methoden

15.4.1 5-Why-Analyse

Methode: Fünffach "Warum?" fragen, um zur Grundursache zu gelangen

Beispiel: 1. **Warum** ist die Datenbank ausgefallen? → Disk voll 2. **Warum** war die Disk voll? → Log-Dateien nicht rotiert 3. **Warum** wurden Logs nicht rotiert? → Logrotate-Job fehlgeschlagen 4. **Warum** ist der Job fehlgeschlagen? → Falsche Cron-Konfiguration 5. **Warum** war die Konfiguration falsch? → Keine Validierung nach Change

Root-Cause: Fehlende Change-Validierung

15.4.2 Fishbone-Diagramm (Ishikawa)

Kategorien: - **Menschen:** Fehler, Wissen, Training - **Methoden:** Prozesse, Verfahren, Standards - **Maschinen:** Hardware, Software, Tools - **Material:** Daten, Konfigurationen, Dokumentation - **Umgebung:** Infrastruktur, Netzwerk, Standort - **Management:** Entscheidungen, Ressourcen, Prioritäten

Anwendung: 1. Problem als “Fischkopf” definieren 2. Hauptkategorien als “Gräten” zeichnen 3. Ursachen pro Kategorie identifizieren 4. Tiefere Ursachen als Unter-Gräten hinzufügen 5. Root-Cause identifizieren

15.4.3 Timeline-Analyse

Methode: Chronologische Rekonstruktion der Ereignisse

Schritte: 1. Zeitstrahl erstellen 2. Alle relevanten Events eintragen 3. Kausalitäten identifizieren 4. Kritischen Pfad herausarbeiten 5. Root-Cause am Anfang der Kausalkette finden

Datenquellen: - Incident-Tickets - Change-Records - Monitoring-Logs - System-Logs - Deployment-Historie

15.5 Postmortem-Prozess

15.5.1 Postmortem-Definition

Ein **Postmortem** ist eine strukturierte Analyse eines Major Incidents oder kritischen Problems mit dem Ziel, Lessons Learned zu identifizieren und Verbesserungen umzusetzen.

15.5.2 Postmortem-Trigger

Pflicht-Postmortems bei: - Major Incidents (P1) - Service-Ausfälle > 4 Stunden - Datenverlust oder Security-Breach - Incidents mit Medienaufmerksamkeit - Wiederholte Incidents trotz vorheriger Lösung

Optional-Postmortems bei: - P2-Incidents mit interessanten Lessons Learned - Erfolgreiche Incident-Bewältigung (Best Practices) - Near-Miss-Situationen

15.5.3 Postmortem-Timeline

Phase	Zeitpunkt	Aktivität
Initiierung	Innerhalb 24h	Postmortem ankündigen, Teilnehmer einladen
Datensammlung	24-48h	Logs, Timelines, Fakten sammeln
Meeting	Innerhalb 1 Woche	Postmortem-Meeting durchführen
Dokumentation	Innerhalb 2 Wochen	Postmortem-Report finalisieren
Follow-up	Laufend	Action Items umsetzen und tracken

15.5.4 Postmortem-Meeting

Teilnehmer: - Incident Manager - Betroffene Teams - Service Owner - Management (bei Major Incidents) - Optional: Externe Stakeholder

Agenda: 1. **Incident-Übersicht** (5 Min) - Was ist passiert? - Wann ist es passiert? - Wer war betroffen?

2. **Timeline-Review** (15 Min)
 - Chronologische Ereignisse
 - Entscheidungspunkte
 - Kommunikation
3. **Root-Cause-Analysis** (20 Min)
 - 5-Why oder Fishbone
 - Beitragende Faktoren
 - Grundursache
4. **What Went Well** (10 Min)
 - Erfolgreiche Maßnahmen
 - Gute Zusammenarbeit
 - Effektive Tools
5. **What Went Wrong** (10 Min)
 - Probleme und Verzögerungen
 - Kommunikationsprobleme
 - Tool- oder Prozess-Mängel
6. **Action Items** (15 Min)
 - Verbesserungsmaßnahmen
 - Verantwortliche
 - Deadlines

Dauer: 60-90 Minuten

Moderator: Problem Manager oder neutraler Facilitator

15.5.5 Postmortem-Prinzipien

Blameless Culture: - Fokus auf Systeme und Prozesse, nicht auf Personen - Keine Schuldzuweisungen - Psychologische Sicherheit - Lernen aus Fehlern

Faktenbasiert: - Objektive Daten (Logs, Metriken) - Keine Spekulationen - Verifizierbare Aussagen

Konstruktiv: - Lösungsorientiert - Konkrete Action Items - Umsetzbare Verbesserungen

15.6 Postmortem-Template

15.6.1 1. Executive Summary

Incident-Übersicht: - **Incident-ID:** [ID] - **Datum/Zeit:** [Start] - [Ende] - **Dauer:** [Stunden] - **Priorität:** P1 / P2 - **Betroffener Service:** [Service-Name] - **Impact:** [Anzahl Nutzer, Business-Impact]

Zusammenfassung: [2-3 Sätze: Was ist passiert und was war die Ursache?]

15.6.2 2. Timeline

Zeit	Event	Aktion	Verantwortlich
10:00	Alert: Database CPU 100%	Monitoring-Alert ausgelöst	Monitoring-System
10:05	Service Desk erhält Anrufe	Incident-Ticket erstellt	Service Desk
10:15	Eskalation an DBA-Team	Datenbank-Analyse gestartet	IT Operations
10:30	Root-Cause identifiziert	Slow Query gefunden	DBA-Team
10:45	Query optimiert	Deployment durchgeführt	DBA-Team
11:00	Service wiederhergestellt	Monitoring bestätigt	IT Operations

15.6.3 3. Root Cause Analysis

5-Why-Analyse: 1. Warum war die Datenbank überlastet? → Slow Query 2. Warum gab es eine Slow Query? → Fehlender Index 3. Warum fehlte der Index? → Nicht im Deployment enthalten 4. Warum war er nicht im Deployment? → Nicht in Code-Review erkannt 5. Warum wurde es nicht erkannt? → Keine Performance-Tests

Root-Cause: Fehlende Performance-Tests im CI/CD-Pipeline

Beitragende Faktoren: - Unzureichende Code-Review-Checkliste - Keine automatisierten Query-Analysen - Fehlende Staging-Umgebung mit Produktions-Datenvolumen

15.6.4 4. Impact Assessment

Technischer Impact: - Datenbank-CPU: 100% für 60 Minuten - Antwortzeiten: > 30 Sekunden (normal: < 1s) - Service-Verfügbarkeit: 0% für 60 Minuten

Business-Impact: - Betroffene Nutzer: 500 (100%) - Geschäftsprozesse blockiert: Order Processing - Geschätzter Umsatzverlust: [Betrag] - Reputationsschaden: Mittel

SLA-Impact: - SLA-Ziel: 99.9% Verfügbarkeit - Tatsächliche Verfügbarkeit: 99.86% - SLA-Verstoß: Ja

15.6.5 5. What Went Well

- Schnelle Eskalation an DBA-Team (10 Minuten)
- Effektive Kommunikation zwischen Teams
- Root-Cause schnell identifiziert (25 Minuten)
- Lösung erfolgreich implementiert
- Keine Datenverluste

15.6.6 6. What Went Wrong

- Slow Query nicht vor Deployment erkannt
- Keine automatischen Performance-Tests
- Staging-Umgebung nicht repräsentativ

- Monitoring-Alert zu spät (CPU-Threshold zu hoch)
- Rollback-Prozedur nicht dokumentiert

15.6.7 7. Action Items

ID	Maßnahme	Verantwortlich	Deadline	Status
AI-001	Performance-Tests in CI/CD integrieren	DevOps-Team	2 Wochen	Open
AI-002	Code-Review-Checkliste erweitern	Dev-Team	1 Woche	Open
AI-003	Staging-Datenbank mit Prod-Volumen	DBA-Team	1 Monat	Open
AI-004	Monitoring-Thresholds anpassen	Ops-Team	1 Woche	Open
AI-005	Rollback-Runbook erstellen	DBA-Team	2 Wochen	Open

15.6.8 8. Lessons Learned

Technisch: - Performance-Tests sind essentiell vor Deployments - Staging-Umgebung muss Produktions-Datenvolumen simulieren - Automatisierte Query-Analyse kann Probleme früh erkennen

Prozess: - Code-Review-Checklisten müssen Performance-Aspekte abdecken - Rollback-Prozeduren müssen dokumentiert und getestet sein - Monitoring-Thresholds müssen regelmäßig überprüft werden

Organisatorisch: - Team-Kommunikation funktionierte gut - Eskalationsprozesse waren effektiv - Dokumentation muss verbessert werden

15.6.9 9. Follow-up

Review-Termin: [Datum, 4 Wochen nach Incident]

Review-Agenda: - Status aller Action Items - Wirksamkeit der Maßnahmen - Weitere Verbesserungen

Verantwortlich: Problem Manager

15.7 Known Error Database (KEDB)

15.7.1 KEDB-Struktur

Erforderliche Felder: - **Known-Error-ID:** Eindeutige Kennung - **Titel:** Kurzbeschreibung - **Symptome:** Wie äußert sich das Problem? - **Root-Cause:** Identifizierte Grundursache -

Workaround: Temporäre Lösung - **Permanente Lösung:** Dauerhafte Behebung (wenn verfügbar) - **Betroffene CIs:** Configuration Items - **Verknüpfte Incidents:** Incident-IDs - **Verknüpfte Problems:** Problem-IDs - **Status:** Open, Workaround Available, Resolved, Closed - **Priorität:** P1-P4 - **Erstellt:** Datum, Autor - **Aktualisiert:** Datum, Autor

15.7.2 KEDB-Beispiel

Known-Error-ID: KE-2024-001

Titel: PostgreSQL Connection Pool Exhaustion

Symptome: - Applikation meldet "Connection timeout" - Datenbank-Logs zeigen "too many connections" - Monitoring zeigt 100% Connection-Pool-Auslastung

Root-Cause: - Connection-Pool-Limit zu niedrig konfiguriert (`max_connections=100`) - Applikation gibt Connections nicht korrekt frei (Connection Leak) - Fehlende Connection-Timeout-Konfiguration

Workaround: 1. PostgreSQL-Service neu starten: `systemctl restart postgresql` 2. Applikation neu starten: `systemctl restart app-service` 3. Monitoring: Connection-Pool-Auslastung beobachten

Permanente Lösung: 1. `max_connections` in `postgresql.conf` erhöhen: `max_connections = 200` 2. Connection-Leak in Applikation beheben (Code-Fix) 3. Connection-Timeout konfigurieren: `idle_in_transaction_session_timeout = 60000` 4. Connection-Pool-Monitoring verbessern

Betroffene CIs: - `{{ netbox.database.server }}` - `{{ netbox.application.server }}`

Verknüpfte Incidents: INC-2024-123, INC-2024-145, INC-2024-167

Status: Resolved

Priorität: P2

15.7.3 KEDB-Nutzung

Incident-Bearbeitung: 1. Incident-Symptome mit KEDB abgleichen 2. Bei Treffer: Workaround anwenden 3. Incident mit Known-Error verknüpfen 4. Problem-Ticket referenzieren

Problem-Analyse: 1. Neue Known Errors in KEDB eintragen 2. Workarounds dokumentieren 3. Permanente Lösungen tracken 4. Status aktualisieren

Wissensmanagement: - KEDB als Wissensdatenbank nutzen - Regelmäßige Reviews (monatlich) - Veraltete Einträge archivieren - Best Practices dokumentieren

15.8 Proaktives Problem Management

15.8.1 Trend-Analyse

Datenquellen: - Incident-Statistiken - Monitoring-Metriken - Performance-Daten - Kapazitäts-Auslastung

Analyse-Methoden: - Zeitreihen-Analyse - Korrelations-Analyse - Anomalie-Erkennung - Predictive Analytics

Ziel: Probleme identifizieren, bevor sie zu Incidents werden

15.8.2 Proaktive Maßnahmen

Regelmäßige Reviews: - Wöchentliche Incident-Trend-Reviews - Monatliche Problem-Reviews - Quartalsweise Service-Reviews

Präventive Maßnahmen: - Kapazitäts-Upgrades - Software-Updates und Patches - Konfigurationsoptimierungen - Prozess-Verbesserungen - Training und Dokumentation

15.8.3 Continuous Improvement

Verbesserungs-Zyklus: 1. **Measure:** Metriken erfassen 2. **Analyze:** Trends identifizieren 3. **Improve:** Maßnahmen umsetzen 4. **Control:** Wirksamkeit prüfen

Verbesserungs-Bereiche: - Prozesse - Tools - Dokumentation - Skills und Training - Infrastruktur

15.9 Metriken und Reporting

15.9.1 Key Performance Indicators (KPIs)

Metrik	Zielwert	Messung
Problem Resolution Rate	> 80%	Gelöste Problems / Gesamt-Problems
Mean Time to Resolve Problem	< 30 Tage	Durchschnittliche Lösungszeit
Known Error Utilization	> 60%	Incidents mit KEDB-Workaround
Recurring Incident Rate	< 10%	Incidents mit bekannter Ursache
Postmortem Completion Rate	100%	Postmortems für Major Incidents

15.9.2 Reporting

Monatliches Problem-Report: - Anzahl offener Problems (nach Priorität) - Neu erstellte Problems - Gelöste Problems - Top-5 Problem-Kategorien - KEDB-Statistiken - Action Items Status

Quartalsweise Trend-Analyse: - Problem-Trends über Zeit - Wiederkehrende Problem-Muster - Verbesserungs-Maßnahmen-Wirksamkeit - ROI von Problem-Management

15.10 Rollen und Verantwortlichkeiten

15.10.1 Problem Manager

Verantwortlichkeiten: - Problem-Prozess-Ownership - Problem-Priorisierung - RCA-Koordination - KEDB-Verwaltung - Postmortem-Moderation - Reporting

Person: Andreas Huemmer

15.10.2 Technical Specialists

Verantwortlichkeiten: - Technische Analyse - RCA-Durchführung - Lösungsentwicklung - Workaround-Identifikation

Teams: Server-Team, Network-Team, DBA-Team, Application-Team

15.10.3 Service Owner

Verantwortlichkeiten: - Business-Impact-Bewertung - Priorisierungs-Entscheidungen - Ressourcen-Bereitstellung - Stakeholder-Kommunikation

15.11 Tools und Systeme

15.11.1 Problem-Management-Tool

- **System:** {{ meta.ticketing_system }}
- **URL:** {{ meta.ticketing_system_url }}
- **Zugriff:** IT Operations Team

15.11.2 Known Error Database

- **System:** {{ meta.ticketing_system }} (KEDB-Modul)
- **URL:** {{ meta.kedb_url }}
- **Zugriff:** Alle IT-Mitarbeiter (Read)

15.11.3 RCA-Tools

- **Collaboration:** {{ meta.collaboration_tool }}
- **Diagramming:** {{ meta.diagramming_tool }}
- **Log-Analysis:** {{ meta.log_analysis_tool }}

15.12 Referenzen

- ITIL v4 Foundation - Problem Management
- ISO/IEC 20000-1:2018 - Problem Management
- Site Reliability Engineering (SRE) - Postmortem Culture
- Interne Incident-Management-Prozesse
- Change-Management-Prozesse

Dokumentverantwortlicher: IT Operations Manager

Genehmigt durch: CIO

Version: 1.0.0

Klassifizierung: internal

Letzte Aktualisierung: {{ meta.date }}

ewpage

Chapter 16

Change und Release Management

16.1 Zweck und Geltungsbereich

Dieses Dokument beschreibt die Change- und Release-Management-Prozesse für AdminSend GmbH gemäß ITIL v4 Best Practices. Es definiert Change-Kategorien, Genehmigungsprozesse, Release-Strategien und Rollback-Prozeduren zur kontrollierten Durchführung von Änderungen an IT-Services und -Systemen.

Geltungsbereich: Alle IT-Services, Systeme und Infrastruktur-Komponenten von AdminSend GmbH

Verantwortlich: Andreas Huemmer (andreas.huemmer@adminsends.de)

16.2 Change Management

16.2.1 Change-Definition

Ein **Change** ist das Hinzufügen, Ändern oder Entfernen von etwas, das direkte oder indirekte Auswirkungen auf Services haben könnte. Das Ziel des Change Managements ist die Minimierung von Risiken bei gleichzeitiger Maximierung des Business-Value.

16.2.2 Change-Prinzipien

Kernprinzipien: - **Kontrolliert:** Alle Changes durchlaufen definierte Prozesse - **Dokumentiert:** Vollständige Dokumentation aller Changes - **Genehmigt:** Autorisierung vor Implementierung - **Getestet:** Validierung vor Produktiv-Deployment - **Rückgängig machbar:** Rollback-Plan für jeden Change

16.2.3 Change-Kategorien

16.2.3.1 Standard Change

Definition: Vorab genehmigte, risikoarme, häufig durchgeführte Changes mit dokumentierter Prozedur.

Eigenschaften: - Niedriges Risiko - Bekannte Prozedur - Vorab-Genehmigung durch CAB - Keine individuelle Genehmigung erforderlich - Dokumentierte Runbooks

Beispiele: - Passwort-Reset - Benutzer-Anlage/Löschung - Standard-Software-Installation - Backup-Restore (nicht-kritisch) - Zertifikats-Erneuerung - Routine-Patches (getestet)

Genehmigung: Automatisch (vorab genehmigt)

Bearbeitungszeit: Sofort bis 24 Stunden

16.2.3.2 Normal Change

Definition: Changes, die individuelle Bewertung, Genehmigung und Planung erfordern.

Eigenschaften: - Mittleres bis hohes Risiko - Individuelle Bewertung erforderlich - CAB-Genehmigung erforderlich - Detaillierte Planung - Test-Phase erforderlich

Beispiele: - Neue Software-Deployments - Infrastruktur-Änderungen - Netzwerk-Rekonfigurationen - Datenbank-Schema-Änderungen - Major-Version-Upgrades - Neue Service-Einführungen

Genehmigung: Change Advisory Board (CAB)

Bearbeitungszeit: 1-4 Wochen (abhängig von Komplexität)

16.2.3.3 Emergency Change

Definition: Dringende Changes zur Behebung von kritischen Incidents oder Sicherheitsproblemen.

Eigenschaften: - Hohe Dringlichkeit - Verkürzte Genehmigungsprozesse - Minimale Dokumentation vor Implementierung - Nachträgliche vollständige Dokumentation - Emergency CAB (ECAB) Genehmigung

Beispiele: - Security-Patches (Zero-Day) - Kritische Bugfixes - Disaster-Recovery-Maßnahmen - Service-Wiederherstellung - Sicherheitsvorfälle

Genehmigung: Emergency CAB (ECAB) oder CIO

Bearbeitungszeit: Sofort bis 4 Stunden

16.2.4 Change-Prozess

16.2.4.1 Prozessübersicht

Change Request
Creation

Change
Assessment

Change
Authorization
(CAB)

Change
Planning

Change
Implementation

Change
Review

Change
Closure

16.2.4.2 1. Change Request Creation

Erforderliche Informationen: - **Change-ID:** Automatisch generiert - **Titel:** Kurzbeschreibung
- **Beschreibung:** Detaillierte Beschreibung der Änderung - **Begründung:** Business-Reason,
Problem-Referenz - **Kategorie:** Standard / Normal / Emergency - **Betroffene Services:** Service-
Liste - **Betroffene CIs:** Configuration Items - **Risiko-Bewertung:** Niedrig / Mittel / Hoch -
Implementierungs-Plan: Schritt-für-Schritt-Anleitung - **Rollback-Plan:** Rückgängig-Machung
- **Test-Plan:** Validierungs-Schritte - **Zeitfenster:** Geplantes Wartungsfenster - **Requester:**
Antragsteller - **Implementer:** Durchführender

Tool: {{ meta.ticketing_system }}

Verantwortlich: Change Requester

16.2.4.3 2. Change Assessment

Bewertungs-Kriterien: - **Impact:** Auswirkung auf Services und Nutzer - **Risiko:** Wahrschein-
lichkeit und Schwere von Problemen - **Komplexität:** Technische Komplexität - **Abhängigkeiten:**
Betroffene Systeme und Services - **Ressourcen:** Erforderliche Skills und Zeit

Risiko-Matrix:

	Impact: Niedrig	Impact: Mittel	Impact: Hoch
Wahrscheinlichkeit: Niedrig	Niedriges Risiko	Mittleres Risiko	Mittleres Risiko
Wahrscheinlichkeit: Mittel	Mittleres Risiko	Mittleres Risiko	Hohes Risiko

	Impact: Niedrig	Impact: Mittel	Impact: Hoch
Wahrscheinlichkeit: Hoch	Mittleres Risiko	Hohes Risiko	Sehr hohes Risiko

Verantwortlich: Change Manager

16.2.4.4 3. Change Authorization (CAB)

Change Advisory Board (CAB):

Mitglieder: - **Chair:** Andreas Huemmer (Change Manager) - **CIO:** Anna Schmidt - **CISO:** Thomas Weber - **Service Owner:** [Service-abhängig] - **Technical Leads:** [Change-abhängig] - **Business Representatives:** [Bei Business-Impact]

CAB-Meeting: - **Frequenz:** Wöchentlich (Dienstag 10:00) - **Dauer:** 60 Minuten - **Agenda:** Review aller Normal Changes - **Entscheidung:** Genehmigen / Ablehnen / Zurückstellen

Emergency CAB (ECAB): - **Mitglieder:** CIO, Change Manager, Technical Lead - **Einberufung:** Ad-hoc bei Emergency Changes - **Entscheidung:** Innerhalb 1 Stunde

Genehmigungskriterien: - Vollständige Dokumentation - Akzeptables Risiko - Ressourcen verfügbar - Test-Plan vorhanden - Rollback-Plan vorhanden - Wartungsfenster verfügbar

16.2.4.5 4. Change Planning

Planungs-Aktivitäten: - Detaillierte Implementierungs-Schritte - Ressourcen-Allokation - Zeitplan erstellen - Kommunikations-Plan - Test-Szenarien definieren - Rollback-Trigger definieren

Change-Kalender: - Alle geplanten Changes visualisieren - Konflikte identifizieren - Wartungsfenster koordinieren - Stakeholder informieren

Verantwortlich: Change Implementer, Change Manager

16.2.4.6 5. Change Implementation

Pre-Implementation: - Backup erstellen - Rollback-Prozedur bereitstellen - Team-Briefing durchführen - Stakeholder informieren

Implementation: - Implementierungs-Plan Schritt-für-Schritt ausführen - Fortschritt dokumentieren - Bei Problemen: Rollback-Trigger prüfen

Post-Implementation: - Funktionalität testen - Monitoring prüfen - Stakeholder informieren - Dokumentation aktualisieren

Verantwortlich: Change Implementer

16.2.4.7 6. Change Review

Review-Aktivitäten: - Erfolg der Implementierung bewerten - Abweichungen vom Plan dokumentieren - Lessons Learned identifizieren - Metriken erfassen (Dauer, Downtime, etc.)

Review-Kriterien: - Change erfolgreich implementiert? - Rollback erforderlich gewesen? - Unerwartete Probleme aufgetreten? - Zeitplan eingehalten? - Dokumentation vollständig?

Verantwortlich: Change Manager

16.2.4.8 7. Change Closure

Closure-Aktivitäten: - Dokumentation finalisieren - CMDB aktualisieren - Change-Ticket schließen - Metriken in Reporting aufnehmen

Verantwortlich: Change Manager

16.2.5 Wartungsfenster

Standard-Wartungsfenster:

Typ	Zeitfenster	Frequenz	Genehmigung
Routine	Dienstag 22:00-02:00	Wöchentlich	Standard Changes
Geplant	Samstag 20:00-06:00	Monatlich	Normal Changes
Emergency	Jederzeit	Ad-hoc	Emergency Changes

Wartungsfenster-Regeln: - Minimale Service-Unterbrechung - Nutzer-Benachrichtigung 48h vorher - Rollback-Zeit einplanen (50% der Implementierungszeit) - Keine Changes während Business-Critical-Zeiten

16.2.6 Rollback-Prozeduren

Rollback-Trigger: - Kritische Fehler während Implementation - Service-Verfügbarkeit < SLA - Unerwartete Auswirkungen auf andere Services - Test-Validierung fehlgeschlagen - Change Manager Entscheidung

Rollback-Plan-Anforderungen: - Schritt-für-Schritt-Anleitung - Geschätzte Rollback-Dauer - Erforderliche Ressourcen - Daten-Wiederherstellung (falls erforderlich) - Validierungs-Schritte

Rollback-Prozess: 1. Rollback-Entscheidung treffen 2. Stakeholder informieren 3. Rollback-Plan ausführen 4. System-Status validieren 5. Incident-Ticket erstellen (falls erforderlich) 6. Post-Rollback-Review durchführen

16.3 Release Management

16.3.1 Release-Definition

Ein **Release** ist eine Sammlung von Hardware, Software, Dokumentation, Prozessen oder anderen Komponenten, die erforderlich sind, um eine oder mehrere genehmigte Changes zu implementieren.

16.3.2 Release-Typen

16.3.2.1 Major Release

Definition: Signifikante neue Funktionalität oder Architektur-Änderungen

Eigenschaften: - Große Änderungen - Umfangreiche Tests erforderlich - Lange Planungsphase - Hohes Risiko - Umfangreiche Dokumentation

Beispiele: - Neue Software-Version (z.B. v2.0.0) - Plattform-Migration - Architektur-Redesign

Frequenz: Quartalsweise oder halbjährlich

Genehmigung: CAB + Management

16.3.2.2 Minor Release

Definition: Neue Features oder Verbesserungen ohne Architektur-Änderungen

Eigenschaften: - Moderate Änderungen - Standard-Tests - Mittleres Risiko - Abwärtskompatibel

Beispiele: - Feature-Releases (z.B. v1.1.0) - Performance-Verbesserungen - Neue Integrationen

Frequenz: Monatlich

Genehmigung: CAB

16.3.2.3 Patch Release

Definition: Bugfixes und Security-Patches

Eigenschaften: - Kleine Änderungen - Fokus auf Stabilität - Niedriges Risiko - Schnelle Implementierung

Beispiele: - Bugfix-Releases (z.B. v1.0.1) - Security-Patches - Hotfixes

Frequenz: Bei Bedarf (wöchentlich)

Genehmigung: Change Manager

16.3.3 Release-Prozess

16.3.3.1 Prozessübersicht

Release
Planning

Release
Build

Release
Testing

Release
Deployment

Release
Review

16.3.3.2 1. Release Planning

Planungs-Aktivitäten: - Release-Scope definieren - Changes für Release auswählen - Release-Zeitplan erstellen - Ressourcen planen - Risiko-Assessment durchführen - Kommunikations-Plan erstellen

Release-Scope: - Inkludierte Changes - Neue Features - Bugfixes - Abhängigkeiten - Ausschlüsse

Verantwortlich: Release Manager

16.3.3.3 2. Release Build

Build-Aktivitäten: - Code-Integration - Automatisierte Builds (CI/CD) - Artefakt-Erstellung - Versionierung - Build-Dokumentation

Build-Pipeline: 1. Code-Commit 2. Automatische Tests (Unit, Integration) 3. Code-Quality-Checks (Linting, Security-Scan) 4. Build-Artefakt erstellen 5. Artefakt in Repository speichern

Verantwortlich: DevOps-Team

16.3.3.4 3. Release Testing

Test-Phasen:

Phase	Umgebung	Fokus	Dauer
Unit Tests	Dev	Code-Funktionalität	Automatisch
Integration Tests	Dev	Komponenten-Integration	Automatisch
System Tests	Test	Gesamtsystem	1-2 Tage
UAT	Staging	Business-Anforderungen	3-5 Tage
Performance Tests	Staging	Last und Performance	1-2 Tage
Security Tests	Staging	Sicherheit	1-2 Tage

Test-Kriterien: - Alle Tests bestanden - Keine kritischen Bugs - Performance-Ziele erreicht - Security-Scan ohne High-Findings - UAT-Abnahme durch Business

Verantwortlich: QA-Team, Business-Users

16.3.3.5 4. Release Deployment

Deployment-Strategien:

16.3.3.5.1 Blue-Green Deployment Beschreibung: Zwei identische Produktions-Umgebungen (Blue und Green). Neue Version wird in inaktiver Umgebung deployed, dann Traffic umgeschaltet.

Vorteile: - Zero-Downtime - Schneller Rollback - Vollständige Tests in Prod-Umgebung

Nachteile: - Doppelte Infrastruktur-Kosten - Datenbank-Migrationen komplex

Anwendung: Kritische Services mit hohen Verfügbarkeits-Anforderungen

16.3.3.5.2 Canary Deployment Beschreibung: Neue Version wird schrittweise für einen kleinen Prozentsatz der Nutzer ausgerollt, dann graduell erhöht.

Vorteile: - Risiko-Minimierung - Frühe Fehler-Erkennung - Graduelles Rollout

Nachteile: - Komplexe Traffic-Steuerung - Längere Deployment-Dauer

Anwendung: Services mit großer Nutzerbasis

16.3.3.5.3 Rolling Deployment Beschreibung: Neue Version wird schrittweise auf Server-Instanzen deployed, während alte Version weiterläuft.

Vorteile: - Keine zusätzliche Infrastruktur - Graduelles Rollout - Automatisierbar

Nachteile: - Temporäre Versions-Inkonsistenz - Komplexe Rollbacks

Anwendung: Standard-Deployments mit Load-Balancing

16.3.3.5.4 Big Bang Deployment Beschreibung: Alle Komponenten werden gleichzeitig aktualisiert.

Vorteile: - Einfach - Schnell - Keine Versions-Inkonsistenz

Nachteile: - Downtime erforderlich - Hohes Risiko - Komplexe Rollbacks

Anwendung: Nur für unkritische Services oder mit Wartungsfenster

Deployment-Checkliste: - ☐ Backup erstellt - ☐ Rollback-Plan bereit - ☐ Monitoring aktiviert - ☐ Stakeholder informiert - ☐ Team verfügbar - ☐ Deployment-Runbook geprüft - ☐ Change-Ticket genehmigt

Verantwortlich: DevOps-Team, Release Manager

16.3.3.6 5. Release Review

Review-Aktivitäten: - Deployment-Erfolg bewerten - Metriken analysieren - Lessons Learned dokumentieren - Verbesserungen identifizieren

Review-Metriken: - Deployment-Dauer - Downtime (falls vorhanden) - Anzahl Rollbacks - Post-Deployment-Incidents - User-Feedback

Verantwortlich: Release Manager

16.3.4 CI/CD Pipeline

Continuous Integration (CI): - Automatische Builds bei Code-Commit - Automatische Tests (Unit, Integration) - Code-Quality-Checks - Security-Scans - Artefakt-Erstellung

Continuous Deployment (CD): - Automatisches Deployment in Dev/Test - Manuelles Deployment in Staging/Prod - Automatische Rollbacks bei Fehlern - Deployment-Monitoring

Pipeline-Tools: - **CI/CD-System:** {{ meta.cicd_system }} - **Version Control:** {{ meta.version_control }} - **Artefakt-Repository:** {{ meta.artifact_repository }} - **Container-Registry:** {{ meta.container_registry }}

16.4 Metriken und Reporting

16.4.1 Change-Management-Metriken

Metrik	Zielwert	Messung
Change Success Rate	> 95%	Erfolgreiche Changes / Gesamt-Changes
Emergency Change Rate	< 5%	Emergency Changes / Gesamt-Changes
Change-Related Incidents	< 10%	Incidents durch Changes / Gesamt-Incidents
CAB Approval Rate	> 90%	Genehmigte Changes / Eingereichte Changes
Rollback Rate	< 5%	Rollbacks / Implementierte Changes

16.4.2 Release-Management-Metriken

Metrik	Zielwert	Messung
Release Frequency	Monatlich	Anzahl Releases pro Monat
Lead Time	< 2 Wochen	Zeit von Commit bis Produktion
Deployment Frequency	Wöchentlich	Anzahl Deployments pro Woche
Mean Time to Recovery	< 1 Stunde	Durchschnittliche Wiederherstellungszeit
Change Failure Rate	< 15%	Fehlgeschlagene Deployments / Gesamt

16.4.3 Reporting

Wöchentliches Change-Report: - Anzahl Changes (nach Kategorie) - Geplante Changes (nächste Woche) - Change-Kalender - Offene Change-Requests

Monatliches Release-Report: - Release-Übersicht - Deployment-Statistiken - Metriken-Dashboard - Verbesserungs-Maßnahmen

16.5 Rollen und Verantwortlichkeiten

16.5.1 Change Manager

Verantwortlichkeiten: - Change-Prozess-Ownership - CAB-Moderation - Change-Assessment - Change-Kalender-Verwaltung - Reporting

Person: Andreas Huemmer

16.5.2 Release Manager

Verantwortlichkeiten: - Release-Planung - Release-Koordination - Deployment-Oversight - Release-Dokumentation

Person: [Name]

16.5.3 Change Advisory Board (CAB)

Verantwortlichkeiten: - Change-Bewertung - Change-Genehmigung - Risiko-Assessment - Priorisierung

Mitglieder: Siehe Abschnitt “Change Authorization”

16.6 Tools und Systeme

16.6.1 Change-Management-Tool

- **System:** {{ meta.ticketing_system }}
- **URL:** {{ meta.ticketing_system_url }}
- **Zugriff:** Alle IT-Mitarbeiter

16.6.2 CI/CD-Pipeline

- **System:** {{ meta.cicd_system }}
- **URL:** {{ meta.cicd_url }}
- **Zugriff:** DevOps-Team

16.6.3 Version Control

- **System:** {{ meta.version_control }}
- **URL:** {{ meta.version_control_url }}
- **Zugriff:** Development-Team

16.7 Referenzen

- ITIL v4 Foundation - Change Enablement
- ITIL v4 Foundation - Release Management
- ISO/IEC 20000-1:2018 - Change Management
- DevOps Handbook - Deployment Strategies
- Site Reliability Engineering (SRE) - Release Engineering

Dokumentverantwortlicher: IT Operations Manager

Genehmigt durch: CIO

Version: 1.0.0

Klassifizierung: internal

Letzte Aktualisierung: {{ meta.date }}

ewpage

Chapter 17

Backup und Restore

17.1 Zweck und Geltungsbereich

Dieses Dokument beschreibt die Backup- und Restore-Strategien für AdminSend GmbH. Es definiert Backup-Methoden, Zeitpläne, Aufbewahrungsfristen, RPO/RTO-Ziele und Restore-Prozeduren zur Sicherstellung der Datenintegrität und -verfügbarkeit.

Geltungsbereich: Alle IT-Systeme, Datenbanken, Applikationen und Daten von AdminSend GmbH

Verantwortlich: Andreas Huemmer (andreas.huemmer@adminsends.de)

17.2 Backup-Grundlagen

17.2.1 Backup-Ziele

Primäre Ziele: - **Datenschutz:** Schutz vor Datenverlust - **Disaster Recovery:** Wiederherstellung nach Katastrophen - **Compliance:** Erfüllung regulatorischer Anforderungen - **Business Continuity:** Minimierung von Ausfallzeiten - **Ransomware-Schutz:** Wiederherstellung nach Cyber-Angriffen

17.2.2 Recovery-Ziele

17.2.2.1 Recovery Point Objective (RPO)

Definition: Maximaler tolerierbarer Datenverlust (Zeitspanne zwischen letztem Backup und Ausfall)

RPO-Kategorien:

Kategorie	RPO	Backup-Frequenz	Anwendung
Kritisch	< 1 Stunde	Continuous / Hourly	Transaktionssysteme, Datenbanken
Wichtig	< 4 Stunden	4x täglich	Business-Applikationen
Standard	< 24 Stunden	Täglich	File-Server, E-Mail

Kategorie	RPO	Backup-Frequenz	Anwendung
Unkritisch	< 7 Tage	Wöchentlich	Archiv-Daten, Test-Systeme

17.2.2.2 Recovery Time Objective (RTO)

Definition: Maximale tolerierbare Ausfallzeit (Zeit bis zur Wiederherstellung)

RTO-Kategorien:

Kategorie	RTO	Restore-Methode	Anwendung
Kritisch	< 1 Stunde	Hot-Standby, Snapshots	Produktions- Datenbanken
Wichtig	< 4 Stunden	Schnelle Restore-Systeme	Business- Applikationen
Standard	< 24 Stunden	Standard-Restore	File-Server
Unkritisch	< 7 Tage	Archiv-Restore	Test-Systeme

17.2.3 Backup-Strategien

17.2.3.1 Full Backup

Beschreibung: Vollständige Sicherung aller Daten

Vorteile: - Einfache Wiederherstellung - Nur ein Backup-Set erforderlich - Schnelle Restore-Zeit

Nachteile: - Lange Backup-Dauer - Hoher Speicherbedarf - Hohe Netzwerk-Last

Anwendung: Wöchentliche Basis-Backups

17.2.3.2 Incremental Backup

Beschreibung: Sicherung nur der seit letztem Backup (Full oder Incremental) geänderten Daten

Vorteile: - Schnelle Backup-Dauer - Geringer Speicherbedarf - Geringe Netzwerk-Last

Nachteile: - Komplexe Wiederherstellung - Alle Incremental-Backups erforderlich - Längere Restore-Zeit

Anwendung: Tägliche Backups zwischen Full-Backups

17.2.3.3 Differential Backup

Beschreibung: Sicherung aller seit letztem Full-Backup geänderten Daten

Vorteile: - Schnellere Wiederherstellung als Incremental - Nur Full + letztes Differential erforderlich - Moderate Backup-Dauer

Nachteile: - Wachsende Backup-Größe - Höherer Speicherbedarf als Incremental

Anwendung: Alternative zu Incremental bei kritischen Systemen

17.2.3.4 Continuous Data Protection (CDP)

Beschreibung: Kontinuierliche Sicherung aller Änderungen in Echtzeit

Vorteile: - Minimaler Datenverlust (RPO < 1 Min) - Point-in-Time-Recovery - Keine Backup-Fenster erforderlich

Nachteile: - Hohe Kosten - Komplexe Infrastruktur - Hohe Performance-Anforderungen

Anwendung: Kritische Datenbanken und Transaktionssysteme

17.2.4 Backup-Architektur

17.2.4.1 3-2-1-Backup-Regel

Regel: 3 Kopien, 2 verschiedene Medien, 1 Offsite-Kopie

Umsetzung: - **3 Kopien:** Produktiv-Daten + 2 Backups - **2 Medien:** Disk + Tape oder Cloud - **1 Offsite:** Geografisch getrennte Kopie

Beispiel: 1. Produktiv-Daten auf `{{ netbox.storage.primary }}` 2. Backup auf `{{ netbox.storage.backup_disk }}` 3. Offsite-Backup in `{{ meta.backup_cloud_provider }}`

17.2.4.2 Backup-Tiers

Tier	Speicher-Typ	Restore-Zeit	Kosten	Anwendung
Tier 1	SSD / NVMe	Minuten	Hoch	Snapshots, CDP
Tier 2	HDD / NAS	Stunden	Mittel	Tägliche Backups
Tier 3	Tape / Object Storage	Tage	Niedrig	Langzeit-Archivierung
Tier 4	Cloud Cold Storage	Wochen	Sehr niedrig	Compliance-Archiv

17.3 Backup-Zeitpläne

17.3.1 Produktions-Systeme

17.3.1.1 Datenbanken (Kritisch)

System: `{{ netbox.database.server }}`

Backup-Strategie: - **Full Backup:** Sonntag 02:00 - **Differential Backup:** Täglich 02:00 (Mo-Sa) - **Transaction Log Backup:** Stündlich - **Snapshots:** Alle 4 Stunden

RPO: < 1 Stunde

RTO: < 1 Stunde

Aufbewahrung: - Tägliche Backups: 30 Tage - Wöchentliche Backups: 12 Wochen - Monatliche Backups: 12 Monate - Jährliche Backups: 7 Jahre

17.3.1.2 Applikations-Server (Wichtig)

System: {{ netbox.application.server }}

Backup-Strategie: - **Full Backup:** Sonntag 03:00 - **Incremental Backup:** Täglich 03:00 (Mo-Sa) - **Snapshots:** Täglich vor Deployments

RPO: < 24 Stunden

RTO: < 4 Stunden

Aufbewahrung: - Tägliche Backups: 14 Tage - Wöchentliche Backups: 8 Wochen - Monatliche Backups: 6 Monate

17.3.1.3 File-Server (Standard)

System: {{ netbox.fileserver.server }}

Backup-Strategie: - **Full Backup:** Sonntag 01:00 - **Incremental Backup:** Täglich 01:00 (Mo-Sa)

RPO: < 24 Stunden

RTO: < 24 Stunden

Aufbewahrung: - Tägliche Backups: 7 Tage - Wöchentliche Backups: 4 Wochen - Monatliche Backups: 3 Monate

17.3.2 Backup-Kalender

Tag	01:00	02:00	03:00	Stündlich
Sonntag	File-Server (Full)	Datenbank (Full)	App-Server (Full)	DB-Logs
Montag	File-Server (Inc)	Datenbank (Diff)	App-Server (Inc)	DB-Logs
Dienstag	File-Server (Inc)	Datenbank (Diff)	App-Server (Inc)	DB-Logs
Mittwoch	File-Server (Inc)	Datenbank (Diff)	App-Server (Inc)	DB-Logs
Donnerstag	File-Server (Inc)	Datenbank (Diff)	App-Server (Inc)	DB-Logs
Freitag	File-Server (Inc)	Datenbank (Diff)	App-Server (Inc)	DB-Logs
Samstag	File-Server (Inc)	Datenbank (Diff)	App-Server (Inc)	DB-Logs

17.4 Backup-Prozesse

17.4.1 Backup-Prozess-Übersicht

Backup
Scheduling

Pre-Backup
Checks

Backup
Execution

Backup
Verification

Backup
Reporting

Offsite
Replication

17.4.2 1. Backup Scheduling

Automatisierung: - Backup-Jobs in `{{ meta.backup_system }}` konfiguriert - Zeitgesteuerte Ausführung - Abhängigkeiten zwischen Jobs - Retry-Mechanismen bei Fehlern

Verantwortlich: Backup-Administrator

17.4.3 2. Pre-Backup Checks

Prüfungen: - Ausreichend Speicherplatz verfügbar - Backup-Target erreichbar - Quell-System verfügbar - Keine laufenden Wartungsarbeiten - Vorheriges Backup erfolgreich

Bei Fehlern: Alert an Operations-Team

17.4.4 3. Backup Execution

Aktivitäten: - Applikations-konsistente Snapshots erstellen - Daten komprimieren - Daten verschlüsseln (AES-256) - Daten auf Backup-Target übertragen - Metadaten speichern

Monitoring: Echtzeit-Überwachung in `{{ meta.monitoring_system }}`

17.4.5 4. Backup Verification

Verifikations-Methoden: - **Checksum-Validierung:** MD5/SHA-256 Prüfsummen - **Katalog-Prüfung:** Backup-Katalog-Konsistenz - **Restore-Test:** Stichproben-Restores (monatlich) - **Integritäts-Scan:** Backup-Daten-Integrität

Bei Fehlern: Backup wiederholen, Alert eskalieren

17.4.6 5. Backup Reporting

Reports: - Backup-Status (Erfolg/Fehler) - Backup-Größe und -Dauer - Speicherplatz-Auslastung
- Fehlgeschlagene Backups - Trend-Analysen

Empfänger: andreas.huemmer@adminsends.de

17.4.7 6. Offsite Replication

Replikations-Methoden: - **Cloud-Sync:** Automatische Replikation zu {{ meta.backup_cloud_provider }}
- **Tape-Rotation:** Wöchentliche Tape-Auslagerung - **Remote-Site:** Replikation zu {{ net-box.site.dr_location }}

Verschlüsselung: TLS in Transit, AES-256 at Rest

17.5 Restore-Prozesse

17.5.1 Restore-Prozess-Übersicht

Restore
Request

Restore
Planning

Restore
Preparation

Restore
Execution

Restore
Verification

Restore
Documentation

17.5.2 1. Restore Request

Restore-Gründe: - Datenverlust (versehentliches Löschen) - Daten-Korruption - Ransomware-Angriff - Hardware-Ausfall - Disaster-Recovery - Test/Entwicklung

Erforderliche Informationen: - Was soll wiederhergestellt werden? - Welcher Zeitpunkt? (Point-in-Time) - Wohin soll wiederhergestellt werden? - Dringlichkeit (RTO) - Genehmigung

Tool: {{ meta.ticketing_system }}

17.5.3 2. Restore Planning

Planungs-Aktivitäten: - Backup-Set identifizieren - Restore-Methode auswählen - Restore-Ziel vorbereiten - Downtime planen (falls erforderlich) - Stakeholder informieren

Restore-Methoden: - **File-Level-Restore:** Einzelne Dateien/Ordner - **Volume-Level-Restore:** Komplette Volumes - **System-Level-Restore:** Bare-Metal-Recovery - **Database-Restore:** Datenbank-Wiederherstellung - **VM-Restore:** Virtuelle Maschinen

17.5.4 3. Restore Preparation

Vorbereitungen: - Backup-Integrität prüfen - Restore-Ziel bereitstellen - Ausreichend Speicherplatz sicherstellen - Netzwerk-Konnektivität prüfen - Backup-Medien mounten (falls Tape)

17.5.5 4. Restore Execution

Restore-Schritte:

17.5.5.1 File-Level-Restore

1. Backup-Katalog durchsuchen
2. Dateien/Ordner auswählen
3. Restore-Ziel angeben
4. Restore starten
5. Fortschritt überwachen

Geschätzte Dauer: 10 GB/Stunde (von Disk)

17.5.5.2 Database-Restore

1. Datenbank-Service stoppen
2. Full-Backup wiederherstellen
3. Differential-Backup anwenden (falls vorhanden)
4. Transaction-Logs anwenden (Point-in-Time)
5. Datenbank-Konsistenz prüfen
6. Datenbank-Service starten

Geschätzte Dauer: 100 GB/Stunde

17.5.5.3 VM-Restore

1. VM ausschalten (falls läuft)
2. VM-Backup auswählen

3. Restore-Ziel (Datastore) auswählen
4. VM wiederherstellen
5. VM-Konfiguration prüfen
6. VM starten

Geschätzte Dauer: 50 GB/Stunde

17.5.5.4 Bare-Metal-Restore

1. Boot-Medium erstellen
2. System von Boot-Medium starten
3. Backup-Quelle verbinden
4. System-Backup auswählen
5. Restore auf Hardware durchführen
6. System neu starten

Geschätzte Dauer: 20 GB/Stunde

17.5.6 5. Restore Verification

Verifikations-Schritte: - Daten-Vollständigkeit prüfen - Daten-Integrität validieren - Applikations-Funktionalität testen - Performance-Check durchführen - Nutzer-Akzeptanz einholen

Verifikations-Checkliste: - [] Alle angeforderten Daten wiederhergestellt - [] Daten-Integrität bestätigt - [] Applikation funktionsfähig - [] Performance akzeptabel - [] Nutzer informiert

17.5.7 6. Restore Documentation

Dokumentation: - Restore-Ticket aktualisieren - Restore-Dauer dokumentieren - Probleme und Lösungen festhalten - Lessons Learned identifizieren - Metriken erfassen

17.6 Backup-Technologien

17.6.1 Backup-Software

Primäres Backup-System: - **System:** {{ meta.backup_system }} - **Version:** {{ meta.backup_system_version }} - **Lizenz:** {{ meta.backup_system_license }}

Funktionen: - Applikations-konsistente Backups - Deduplizierung - Kompression - Verschlüsselung - Cloud-Integration - Automatische Verifikation

17.6.2 Snapshot-Technologie

Storage-Snapshots: - **System:** {{ netbox.storage.system }} - **Snapshot-Frequenz:** Alle 4 Stunden - **Aufbewahrung:** 48 Stunden - **Verwendung:** Schnelle Rollbacks, Pre-Change-Snapshots

VM-Snapshots: - **System:** {{ netbox.hypervisor.system }} - **Snapshot-Typ:** Crash-consistent - **Verwendung:** Pre-Deployment-Snapshots - **Warnung:** Keine Langzeit-Backup-Lösung

17.6.3 Cloud-Backup

Cloud-Provider: - **Provider:** {{ meta.backup_cloud_provider }} - **Region:** {{ meta.backup_cloud_region }} - **Storage-Tier:** Standard / Glacier

Vorteile: - Offsite-Backup automatisch - Skalierbar - Geo-Redundanz - Pay-per-Use

Nachteile: - Abhängigkeit von Internet-Verbindung - Restore-Dauer bei großen Datenmengen - Laufende Kosten

17.7 Backup-Sicherheit

17.7.1 Verschlüsselung

In Transit: - TLS 1.3 für Netzwerk-Übertragung - VPN für Remote-Backups

At Rest: - AES-256 Verschlüsselung - Separate Schlüssel-Verwaltung - Key-Rotation alle 90 Tage

Key-Management: - Schlüssel in {{ meta.key_management_system }} - Zugriff nur für autorisierte Administratoren - Backup der Schlüssel (Escrow)

17.7.2 Immutable Backups

Konzept: Backups können nicht geändert oder gelöscht werden (Schutz vor Ransomware)

Implementierung: - Object-Lock in Cloud-Storage - WORM-Tapes (Write Once Read Many) - Air-Gapped-Backups

Aufbewahrung: Mindestens 30 Tage immutable

17.7.3 Zugriffskontrolle

Berechtigungen: - Backup-Administratoren: Vollzugriff - System-Administratoren: Restore-Berechtigung - Service Desk: Keine Backup-Berechtigung

Audit-Logging: - Alle Backup/Restore-Aktivitäten geloggt - Logs in SIEM-System {{ meta.siem_system }} - Monatliche Audit-Reviews

17.8 Backup-Testing

17.8.1 Test-Strategie

Test-Typen: - **Verifikations-Tests:** Automatisch nach jedem Backup - **Restore-Tests:** Monatliche Stichproben - **DR-Tests:** Quartalsweise Full-Restore-Tests - **Compliance-Tests:** Jährliche Audits

17.8.2 Restore-Test-Prozess

Monatlicher Restore-Test: 1. Zufälliges System auswählen 2. Restore in isolierte Test-Umgebung 3. Funktionalität validieren 4. Restore-Dauer messen 5. Ergebnisse dokumentieren

Test-Kriterien: - Restore erfolgreich - RTO eingehalten - Daten vollständig - Applikation funktionsfähig

Bei Fehlern: - Incident-Ticket erstellen - Backup-Strategie überprüfen - Korrekturmaßnahmen umsetzen - Re-Test durchführen

17.8.3 DR-Test

Quartalsweiser DR-Test: 1. Disaster-Szenario simulieren 2. Komplettes System in DR-Site wiederherstellen 3. Failover durchführen 4. Business-Prozesse testen 5. Failback durchführen

Dokumentation: - Test-Plan - Test-Ergebnisse - Identifizierte Probleme - Verbesserungs-Maßnahmen

17.9 Metriken und Reporting

17.9.1 Backup-Metriken

Metrik	Zielwert	Messung
Backup Success Rate	> 98%	Erfolgreiche Backups / Gesamt-Backups
Backup Window Compliance	> 95%	Backups in Zeitfenster / Gesamt-Backups
Restore Success Rate	> 99%	Erfolgreiche Restores / Gesamt-Restores
RTO Compliance	> 95%	Restores innerhalb RTO / Gesamt-Restores
RPO Compliance	> 99%	Datenverlust < RPO / Gesamt-Incidents

17.9.2 Reporting

Tägliches Backup-Report: - Backup-Status (Erfolg/Fehler) - Fehlgeschlagene Backups - Speicherplatz-Auslastung - Alerts und Warnungen

Monatliches Backup-Report: - Backup-Statistiken - Restore-Aktivitäten - Metriken-Dashboard - Trend-Analysen - Kapazitäts-Planung

Quartalsweises Management-Report: - Backup-Strategie-Review - DR-Test-Ergebnisse - Compliance-Status - Verbesserungs-Maßnahmen - Budget-Planung

17.10 Rollen und Verantwortlichkeiten

17.10.1 Backup-Administrator

Verantwortlichkeiten: - Backup-System-Verwaltung - Backup-Job-Konfiguration - Monitoring und Alerting - Restore-Durchführung - Reporting

Person: [Name]

17.10.2 Storage-Administrator

Verantwortlichkeiten: - Backup-Storage-Verwaltung - Kapazitäts-Planung - Performance-Optimierung - Snapshot-Management

Person: [Name]

17.10.3 IT Operations Manager

Verantwortlichkeiten: - Backup-Strategie-Ownership - Budget-Verantwortung - Compliance-Sicherstellung - Eskalations-Management

Person: Andreas Huemmer

17.11 Compliance und Regulierung

17.11.1 Regulatorische Anforderungen

DSGVO: - Daten-Verschlüsselung - Zugriffskontrolle - Audit-Logging - Daten-Löschung nach Aufbewahrungsfrist

ISO 27001: - Backup-Policy dokumentiert - Regelmäßige Backup-Tests - Incident-Response-Plan - Kontinuierliche Verbesserung

Branchenspezifisch: - [Weitere regulatorische Anforderungen]

17.11.2 Aufbewahrungsfristen

Daten-Typ	Aufbewahrungsfrist	Begründung
Finanzdaten	10 Jahre	Steuerrecht
Personaldaten	7 Jahre	Arbeitsrecht
Vertragsdaten	6 Jahre	Vertragsrecht
E-Mails	6 Jahre	Compliance
System-Logs	1 Jahr	Security
Backup-Logs	3 Jahre	Audit

17.12 Referenzen

- ITIL v4 - Service Continuity Management
- ISO/IEC 27001:2013 - Backup Controls
- DSGVO - Artikel 32 (Datensicherheit)
- 3-2-1-Backup-Regel
- Backup-System-Dokumentation: `{{ meta.backup_system_docs }}`

Dokumentverantwortlicher: IT Operations Manager

Genehmigt durch: CIO

Version: 1.0.0

Klassifizierung: internal

Letzte Aktualisierung: {{ meta.date }}

ewpage

Chapter 18

Disaster Recovery und Business Continuity

18.1 Zweck und Geltungsbereich

Dieses Dokument beschreibt die Disaster-Recovery- und Business-Continuity-Strategien für AdminSend GmbH. Es definiert Disaster-Szenarien, Impact-Analysen, DR-Strategien, Failover-/Failback-Prozeduren und Business-Continuity-Pläne zur Sicherstellung der Geschäftskontinuität bei Katastrophen.

Geltungsbereich: Alle kritischen IT-Services und Geschäftsprozesse von AdminSend GmbH

Verantwortlich: Anna Schmidt (anna.schmidt@adminsends.de)

18.2 Grundlagen

18.2.1 Definitionen

Disaster (Katastrophe): Ein Ereignis, das zu einem signifikanten Ausfall von IT-Services oder Geschäftsprozessen führt und normale Wiederherstellungsmaßnahmen übersteigt.

Disaster Recovery (DR): Prozesse und Technologien zur Wiederherstellung von IT-Systemen und -Services nach einer Katastrophe.

Business Continuity (BC): Fähigkeit einer Organisation, kritische Geschäftsprozesse während und nach einer Störung aufrechtzuerhalten.

18.2.2 Abgrenzung DR vs. BC

Aspekt	Disaster Recovery	Business Continuity
Fokus	IT-Systeme und -Infrastruktur	Geschäftsprozesse
Scope	Technische Wiederherstellung	Gesamte Organisation
Ziel	System-Verfügbarkeit	Geschäftskontinuität
Verantwortung	IT-Abteilung	Management + alle Abteilungen
Zeitraumen	Stunden bis Tage	Sofort bis Wochen

18.2.3 Recovery-Ziele

18.2.3.1 Recovery Time Objective (RTO)

Definition: Maximale tolerierbare Ausfallzeit eines Services

RTO-Kategorien für DR:

Service-Tier	RTO	DR-Strategie	Beispiele
Tier 0 - Kritisch	< 1 Stunde	Hot Standby	Transaktionssysteme, E-Commerce
Tier 1 - Wichtig	< 4 Stunden	Warm Standby	ERP, CRM, E-Mail
Tier 2 - Standard	< 24 Stunden	Cold Standby	File-Server, Intranet
Tier 3 - Unkritisch	< 7 Tage	Backup-Restore	Test-Systeme, Archive

18.2.3.2 Recovery Point Objective (RPO)

Definition: Maximaler tolerierbarer Datenverlust

RPO-Kategorien für DR:

Service-Tier	RPO	Replikations-Methode
Tier 0 - Kritisch	< 15 Minuten	Synchrone Replikation
Tier 1 - Wichtig	< 1 Stunde	Asynchrone Replikation
Tier 2 - Standard	< 24 Stunden	Tägliche Backups
Tier 3 - Unkritisch	< 7 Tage	Wöchentliche Backups

18.3 Disaster-Szenarien

18.3.1 Szenario-Kategorien

18.3.1.1 Naturkatastrophen

Szenarien: - Feuer im Rechenzentrum - Überschwemmung - Erdbeben - Sturm/Unwetter - Stromausfall (regional)

Wahrscheinlichkeit: Niedrig

Impact: Sehr hoch

Betroffene Standorte: {{ netbox.site.primary }}, {{ netbox.site.secondary }}

Mitigations: - Geografisch getrennte DR-Site - Redundante Stromversorgung (USV, Generator) - Gebäude-Sicherheitsmaßnahmen - Versicherungen

18.3.1.2 Technische Ausfälle

Szenarien: - Kompletter Rechenzentrum-Ausfall - Netzwerk-Ausfall (WAN) - Storage-System-Ausfall - Hypervisor-Cluster-Ausfall - Cloud-Provider-Ausfall

Wahrscheinlichkeit: Mittel

Impact: Hoch

Mitigations: - Redundante Systeme - Multi-Cloud-Strategie - Automatische Failover-Mechanismen
- Regelmäßige Wartung

18.3.1.3 Cyber-Angriffe

Szenarien: - Ransomware-Angriff - DDoS-Attacke - Data Breach - Insider-Threat - Supply-Chain-Angriff

Wahrscheinlichkeit: Hoch

Impact: Sehr hoch

Mitigations: - Security-Monitoring (SIEM) - Immutable Backups - Network-Segmentierung - Incident-Response-Plan - Security-Awareness-Training

18.3.1.4 Menschliche Fehler

Szenarien: - Versehentliches Löschen kritischer Daten - Fehlkonfiguration mit Service-Ausfall - Ungetestete Changes in Produktion - Fehlerhaftes Deployment

Wahrscheinlichkeit: Mittel

Impact: Mittel bis Hoch

Mitigations: - Change-Management-Prozesse - 4-Augen-Prinzip - Automatisierte Deployments - Rollback-Mechanismen - Regelmäßige Backups

18.3.2 Business Impact Analysis (BIA)

18.3.2.1 Kritische Geschäftsprozesse

Geschäftsprozess	Abhängige IT-Services	RTO	RPO	Finanzieller Impact/Stunde
Order Processing	ERP, Datenbank, E-Commerce	1h	15 Min	50.000 €
Customer Support	CRM, Ticketing, Telefonie	2h	1h	10.000 €
E-Mail-Kommunikation	E-Mail-Server, Exchange	4h	1h	5.000 €
Finanzbuchhaltung	ERP, Datenbank	8h	4h	2.000 €
Personalverwaltung	HR-System	24h	24h	500 €

18.3.2.2 Impact-Bewertung

Finanzielle Auswirkungen: - Direkte Kosten (Umsatzverlust) - Indirekte Kosten (Produktivitätsverlust) - Wiederherstellungskosten - Strafbzahlungen (SLA-Verstöße)

Nicht-finanzielle Auswirkungen: - Reputationsschaden - Kundenverlust - Rechtliche Konsequenzen - Mitarbeiter-Moral

Impact-Matrix:

	< 1h	1-4h	4-24h	> 24h
Kritisch	Katastrophal	Sehr hoch	Hoch	Mittel
Wichtig	Sehr hoch	Hoch	Mittel	Niedrig
Standard	Hoch	Mittel	Niedrig	Minimal
Unkritisch	Mittel	Niedrig	Minimal	Minimal

18.4 DR-Strategien

18.4.1 Hot Standby (Aktiv-Aktiv)

Beschreibung: - Parallele Produktions-Umgebungen an zwei Standorten - Synchrone Daten-Replikation - Load-Balancing zwischen Standorten - Automatisches Failover

Vorteile: - RTO: < 1 Stunde (oft Minuten) - RPO: < 15 Minuten - Keine Downtime bei Failover
- Kontinuierliche Verfügbarkeit

Nachteile: - Sehr hohe Kosten (doppelte Infrastruktur) - Komplexe Konfiguration - Hohe Netzwerk-Anforderungen

Anwendung: Tier 0 Services ({{ netbox.service.critical }})

Kosten: ~200% der Produktions-Infrastruktur

18.4.2 Warm Standby (Aktiv-Passiv)

Beschreibung: - DR-Site mit reduzierten Ressourcen - Asynchrone Daten-Replikation - Systeme laufen, aber nicht produktiv - Manuelles oder automatisches Failover

Vorteile: - RTO: < 4 Stunden - RPO: < 1 Stunde - Moderate Kosten - Schnelle Aktivierung

Nachteile: - Kurze Downtime bei Failover - Reduzierte Performance initial - Regelmäßige Tests erforderlich

Anwendung: Tier 1 Services ({{ netbox.service.important }})

Kosten: ~50-70% der Produktions-Infrastruktur

18.4.3 Cold Standby (Backup-basiert)

Beschreibung: - DR-Site mit minimaler Infrastruktur - Backup-basierte Wiederherstellung - Systeme werden bei Bedarf aufgebaut - Manuelle Aktivierung

Vorteile: - RTO: < 24 Stunden - RPO: < 24 Stunden - Niedrige Kosten - Einfache Verwaltung

Nachteile: - Längere Downtime - Manuelle Prozesse - Höheres Risiko

Anwendung: Tier 2 Services ({{ netbox.service.standard }})

Kosten: ~20-30% der Produktions-Infrastruktur

18.4.4 Backup & Restore

Beschreibung: - Keine dedizierte DR-Site - Wiederherstellung aus Backups - Neue Hardware bei Bedarf beschaffen - Vollständig manueller Prozess

Vorteile: - Minimale Kosten - Einfache Verwaltung

Nachteile: - RTO: > 7 Tage - RPO: > 7 Tage - Sehr hohes Risiko - Lange Wiederherstellungszeit

Anwendung: Tier 3 Services (unkritisch)

Kosten: Nur Backup-Kosten

18.5 DR-Infrastruktur

18.5.1 Primärer Standort

Standort: {{ netbox.site.primary }}

Adresse: {{ netbox.site.primary_address }}

Rechenzentrum: {{ netbox.site.primary_datacenter }}

Infrastruktur: - Produktions-Server: {{ netbox.device.count_primary }} - Storage-Kapazität: {{ netbox.storage.capacity_primary }} - Netzwerk-Bandbreite: {{ netbox.network.bandwidth_primary }} - Stromversorgung: Redundant (N+1)

18.5.2 DR-Standort

Standort: {{ netbox.site.dr }}

Adresse: {{ netbox.site.dr_address }}

Rechenzentrum: {{ netbox.site.dr_datacenter }}

Entfernung: {{ netbox.site.distance }} km

Infrastruktur: - DR-Server: {{ netbox.device.count_dr }} - Storage-Kapazität: {{ netbox.storage.capacity_dr }} - Netzwerk-Bandbreite: {{ netbox.network.bandwidth_dr }} - Stromversorgung: Redundant (N+1)

18.5.3 Replikations-Verbindung

Verbindungstyp: {{ netbox.network.replication_type }}

Bandbreite: {{ netbox.network.replication_bandwidth }}

Latenz: {{ netbox.network.replication_latency }} ms

Redundanz: Dual-Path

Replikations-Technologien: - Storage-Replikation: {{ meta.storage_replication_tech }} - Datenbank-Replikation: {{ meta.database_replication_tech }} - VM-Replikation: {{ meta.vm_replication_tech }}

18.6 Failover-Prozeduren

18.6.1 Failover-Trigger

Automatische Failover-Trigger: - Primärer Standort nicht erreichbar (> 5 Min) - Kritische System-Ausfälle (> 3 Systeme) - Storage-System-Ausfall - Netzwerk-Ausfall (WAN)

Manuelle Failover-Trigger: - Naturkatastrophe am primären Standort - Geplante Wartung (Standort-Wechsel) - DR-Test - Management-Entscheidung

18.6.2 Failover-Prozess

18.6.2.1 Prozess-Übersicht

Disaster
Declaration

DR-Team
Activation

Impact
Assessment

Failover
Execution

Service
Validation

Communication
& Monitoring

18.6.2.2 1. Disaster Declaration

Verantwortlich: CIO oder IT Operations Manager

Kriterien: - Primärer Standort nicht verfügbar - RTO-Gefährdung für kritische Services - Keine schnelle Wiederherstellung möglich

Aktivitäten: - Disaster offiziell erklären - DR-Team aktivieren - Management informieren - Kommunikations-Plan aktivieren

18.6.2.3 2. DR-Team Activation

DR-Team-Mitglieder: - **DR-Coordinator:** Anna Schmidt - **Technical Lead:** Andreas Huemmer - **Network Lead:** [Name] - **Storage Lead:** [Name] - **Application Lead:** [Name] - **Communication Lead:** [Name]

Aktivitäten: - Team-Mitglieder kontaktieren - War-Room einrichten (physisch oder virtuell) -

Kommunikations-Kanäle aktivieren - Checklisten bereitstellen

18.6.2.4 3. Impact Assessment

Bewertungs-Aktivitäten: - Ausmaß des Disasters bewerten - Betroffene Systeme identifizieren - Verfügbarkeit der DR-Site prüfen - Replikations-Status prüfen - Geschätztes RTO/RPO ermitteln

Entscheidung: - Vollständiger Failover zu DR-Site - Partieller Failover (nur kritische Services) - Alternative Maßnahmen

18.6.2.5 4. Failover Execution

Failover-Schritte (Hot Standby):

1. **DNS-Umstellung vorbereiten**
 - DNS-TTL auf 60 Sekunden reduzieren (falls nicht bereits)
 - DNS-Einträge für DR-Site vorbereiten
2. **Load-Balancer umkonfigurieren**
 - Traffic von Primary zu DR umleiten
 - Health-Checks auf DR-Systeme umstellen
3. **Datenbank-Failover**
 - Replikation stoppen
 - DR-Datenbank zu Primary promoten
 - Applikations-Verbindungen umstellen
4. **Applikations-Aktivierung**
 - Applikations-Services auf DR-Site starten
 - Konfigurationen validieren
 - Verbindungen zu Datenbank prüfen
5. **DNS-Umstellung durchführen**
 - DNS-Einträge auf DR-Site umstellen
 - DNS-Propagation überwachen
6. **Netzwerk-Routing anpassen**
 - VPN-Verbindungen zu DR-Site umleiten
 - Firewall-Regeln anpassen
 - Monitoring auf DR-Site umstellen

Geschätzte Dauer: 30-60 Minuten (Hot Standby)

Failover-Schritte (Warm Standby):

1. **DR-Systeme hochfahren**
 - Server starten
 - Storage-Systeme aktivieren
 - Netzwerk-Komponenten prüfen
2. **Daten-Synchronisation finalisieren**
 - Letzte Replikation durchführen
 - Daten-Konsistenz prüfen
 - Backups einspielen (falls erforderlich)
3. **Datenbank-Wiederherstellung**
 - Datenbank-Services starten
 - Konsistenz-Checks durchführen

- Performance-Tuning
4. **Applikations-Deployment**
 - Applikationen deployen
 - Konfigurationen anpassen
 - Integrationen testen
 5. **Netzwerk und DNS**
 - Siehe Hot-Standby-Schritte 5-6

Geschätzte Dauer: 2-4 Stunden (Warm Standby)

18.6.2.6 5. Service Validation

Validierungs-Schritte: - [] Alle kritischen Services erreichbar - [] Datenbank-Verbindungen funktionieren - [] Applikations-Funktionalität getestet - [] Performance akzeptabel - [] Monitoring aktiv - [] Backup-Jobs laufen

Test-Szenarien: - Login-Test - Transaktions-Test - Integrations-Test - Performance-Test

18.6.2.7 6. Communication & Monitoring

Kommunikation: - Stakeholder über Failover informieren - Status-Updates (alle 30 Min) - Nutzer-Kommunikation - Management-Briefing

Monitoring: - Kontinuierliche Überwachung der DR-Site - Performance-Metriken - Error-Logs - Nutzer-Feedback

18.7 Failback-Prozeduren

18.7.1 Failback-Planung

Failback-Trigger: - Primärer Standort wiederhergestellt - Alle Systeme getestet und validiert - Geplantes Wartungsfenster verfügbar - Management-Genehmigung

Failback-Strategie: - **Geplanter Failback:** Während Wartungsfenster - **Schrittweiser Failback:** Service für Service - **Vollständiger Failback:** Alle Services gleichzeitig

18.7.2 Failback-Prozess

18.7.2.1 1. Primären Standort vorbereiten

Aktivitäten: - Infrastruktur-Schäden beheben - Systeme neu aufbauen (falls erforderlich) - Netzwerk-Konnektivität wiederherstellen - Replikation von DR zu Primary einrichten

Validierung: - Alle Systeme funktionsfähig - Replikation läuft - Performance akzeptabel

18.7.2.2 2. Daten-Synchronisation

Aktivitäten: - Reverse-Replikation (DR → Primary) - Daten-Konsistenz sicherstellen - Delta-Synchronisation durchführen

Dauer: Abhängig von Datenvolumen (Stunden bis Tage)

18.7.2.3 3. Failback-Execution

Schritte: 1. Wartungsfenster ankündigen 2. Replikation finalisieren 3. Applikationen auf Primary starten 4. DNS und Load-Balancer umstellen 5. DR-Site in Standby-Modus versetzen

Geschätzte Dauer: 2-4 Stunden

18.7.2.4 4. Post-Failback-Validation

Validierung: - Alle Services auf Primary laufen - Replikation Primary → DR wiederhergestellt - Monitoring aktiv - Backup-Jobs laufen

18.8 Business Continuity Management

18.8.1 BC-Strategie

Ziele: - Kritische Geschäftsprozesse aufrechterhalten - Mitarbeiter-Sicherheit gewährleisten - Kommunikation sicherstellen - Reputation schützen

18.8.2 BC-Pläne

18.8.2.1 Notfall-Kommunikation

Kommunikations-Kanäle: - **Primär:** E-Mail (info@adminsends.de) - **Sekundär:** Telefon (+49 89 12345678) - **Notfall:** Mobile Apps, SMS

Kontakt-Listen: - Management-Team - Alle Mitarbeiter - Kunden - Partner und Lieferanten - Behörden

18.8.2.2 Alternative Arbeitsplätze

Home-Office: - VPN-Zugang für alle Mitarbeiter - Laptops und mobile Geräte - Cloud-basierte Collaboration-Tools

Backup-Büro: - Standort: [Adresse] - Kapazität: [Anzahl Arbeitsplätze] - Ausstattung: IT, Telefonie, Internet

18.8.2.3 Kritische Lieferanten

Lieferant	Service	Kontakt	Backup-Lieferant
{{ meta.isp_provider }}	Internet	{{ meta.isp_contact }}	{{ meta.isp_backup }}
{{ meta.cloud_provider }}	Cloud-Services	{{ meta.cloud_contact }}	{{ meta.cloud_backup }}
{{ meta.hardware_vendor }}	Hardware	{{ meta.hardware_contact }}	-

18.9 DR-Testing

18.9.1 Test-Strategie

Test-Typen: - **Tabletop-Exercise:** Theoretische Durchsprache (quartalsweise) - **Partial-Failover-Test:** Einzelne Services (halbjährlich) - **Full-Failover-Test:** Kompletter Failover (jährlich)

18.9.2 Test-Prozess

18.9.2.1 Tabletop-Exercise

Dauer: 2-3 Stunden

Teilnehmer: - DR-Team - Management - Service-Owner

Ablauf: 1. Disaster-Szenario präsentieren 2. Rollen und Verantwortlichkeiten durchgehen 3. Prozess-Schritte durchsprechen 4. Probleme identifizieren 5. Verbesserungen dokumentieren

18.9.2.2 Full-Failover-Test

Dauer: 1 Tag

Vorbereitung: - Test-Plan erstellen - Stakeholder informieren - Wartungsfenster planen - Rollback-Plan bereitstellen

Durchführung: 1. Failover zu DR-Site 2. Services validieren 3. Business-Prozesse testen 4. Performance messen 5. Failback zu Primary

Nachbereitung: - Test-Report erstellen - Lessons Learned dokumentieren - Verbesserungen umsetzen - Nächsten Test planen

18.10 Metriken und Reporting

18.10.1 DR-Metriken

Metrik	Zielwert	Messung
RTO Achievement	> 95%	Tatsächliches RTO / Ziel-RTO
RPO Achievement	> 99%	Tatsächliches RPO / Ziel-RPO
DR-Test Success Rate	100%	Erfolgreiche Tests / Gesamt-Tests
Failover Time	< Ziel-RTO	Durchschnittliche Failover-Dauer
Data Loss	< Ziel-RPO	Durchschnittlicher Datenverlust

18.10.2 Reporting

Quartalsweises DR-Report: - DR-Test-Ergebnisse - RTO/RPO-Compliance - Infrastruktur-Status - Verbesserungs-Maßnahmen

Jährliches BC-Report: - BC-Strategie-Review - BIA-Update - DR-Kosten-Analyse - Management-Präsentation

18.11 Rollen und Verantwortlichkeiten

18.11.1 DR-Coordinator

Verantwortlichkeiten: - DR-Strategie-Ownership - DR-Plan-Verwaltung - DR-Tests koordinieren
- Disaster-Declaration

Person: Anna Schmidt

18.11.2 BC-Manager

Verantwortlichkeiten: - BC-Strategie-Entwicklung - BIA durchführen - BC-Pläne erstellen - BC-Training

Person: Peter Fischer

18.11.3 DR-Team

Mitglieder: Siehe Abschnitt “DR-Team Activation”

18.12 Referenzen

- ITIL v4 - Service Continuity Management
- ISO 22301:2019 - Business Continuity Management
- ISO/IEC 27031:2011 - ICT Readiness for Business Continuity
- NIST SP 800-34 - Contingency Planning Guide
- Business Impact Analysis (BIA) Dokument

Dokumentverantwortlicher: IT Operations Manager

Genehmigt durch: CIO

Version: 1.0.0

Klassifizierung: internal

Letzte Aktualisierung: {{ meta.date }}

ewpage

Chapter 19

Sicherheitsbetrieb und Hardening

19.1 Zweck und Geltungsbereich

Dieses Dokument beschreibt die Sicherheitsbetriebsprozesse und Hardening-Richtlinien für AdminSend GmbH. Es definiert Security-Monitoring, Incident-Response-Prozesse, Vulnerability-Management und Compliance-Anforderungen zur Sicherstellung der Informationssicherheit.

Geltungsbereich: Alle IT-Systeme, Netzwerke, Applikationen und Daten von AdminSend GmbH

Verantwortlich: Thomas Weber (thomas.weber@adminsends.de)

19.2 Sicherheits-Grundlagen

19.2.1 Security-Ziele (CIA-Triade)

Confidentiality (Vertraulichkeit): - Schutz vor unbefugtem Zugriff - Verschlüsselung sensibler Daten - Zugriffskontrolle und Authentifizierung - Data Loss Prevention (DLP)

Integrity (Integrität): - Schutz vor unbefugter Änderung - Digitale Signaturen - Checksums und Hashing - Change-Management-Prozesse

Availability (Verfügbarkeit): - Schutz vor Denial-of-Service - Redundanz und Hochverfügbarkeit - Backup und Disaster Recovery - Kapazitäts-Management

19.2.2 Defense-in-Depth-Strategie

Sicherheits-Schichten:

Perimeter Security	Firewall, IDS/IPS, DDoS-Protection
Network Security	Segmentierung, VLANs, NAC
Host Security	Hardening, Antivirus, EDR
Application Security	WAF, Input-Validation, SAST/DAST

Data Security

Encryption, DLP, Backup

Identity & Access Management

MFA, RBAC, PAM

19.2.3 Security-Frameworks

ISO 27001:2013: - Informationssicherheits-Managementsystem (ISMS) - 114 Controls in 14 Kategorien - Risiko-basierter Ansatz - Kontinuierliche Verbesserung

BSI Grundschutz: - IT-Grundschutz-Kompodium - Bausteine für IT-Systeme - Standard-Sicherheitsmaßnahmen - Basis-Absicherung und Kern-Absicherung

NIST Cybersecurity Framework: - Identify, Protect, Detect, Respond, Recover - Risiko-Management-Ansatz - Branchenübergreifend anwendbar

CIS Controls: - 18 kritische Sicherheitskontrollen - Priorisierte Umsetzung - Messbare Implementierung

19.3 Hardening-Richtlinien

19.3.1 Betriebssystem-Hardening

19.3.1.1 Linux-Server-Hardening

Basis-Härtung: - Minimale Installation (nur benötigte Pakete) - Regelmäßige Updates und Patches - Deaktivierung ungenutzter Services - Firewall-Konfiguration (iptables/nftables) - SELinux oder AppArmor aktivieren

Benutzer und Authentifizierung: - Root-Login per SSH deaktivieren - SSH-Key-basierte Authentifizierung - Sudo statt direktem Root-Zugriff - Passwort-Policies (Komplexität, Ablauf) - Account-Lockout nach Fehlversuchen

Netzwerk-Härtung: - Unnötige Netzwerk-Services deaktivieren - TCP-Wrapper konfigurieren - IP-Tables Regeln restriktiv - IPv6 deaktivieren (falls nicht benötigt)

Logging und Monitoring: - Syslog-Server-Konfiguration - Audit-Daemon (auditd) aktivieren - Log-Rotation konfigurieren - Zentrale Log-Sammlung

Referenz: CIS Benchmark für Linux

19.3.1.2 Windows-Server-Hardening

Basis-Härtung: - Windows-Updates automatisch - Unnötige Features deaktivieren - Windows Firewall aktivieren - Windows Defender aktivieren - BitLocker für Disk-Verschlüsselung

Benutzer und Authentifizierung: - Lokale Administrator-Konten umbenennen - Passwort-Policies via GPO - Account-Lockout-Policies - Privileged Access Management (PAM) - LAPS für lokale Admin-Passwörter

Netzwerk-Härtung: - SMBv1 deaktivieren - LLMNR und NetBIOS deaktivieren - Windows Firewall-Regeln restriktiv - IPSec für Server-Kommunikation

Logging und Monitoring: - Advanced Audit Policy konfigurieren - PowerShell-Logging aktivieren
 - Event-Log-Forwarding - Sysmon installieren

Referenz: CIS Benchmark für Windows Server, Microsoft Security Baseline

19.3.2 Netzwerk-Hardening

19.3.2.1 Firewall-Konfiguration

Prinzipien: - Default Deny (alles verbieten, nur Benötigtes erlauben) - Least Privilege (minimale Berechtigungen) - Segmentierung (Netzwerk-Zonen)

Firewall-Regeln:

Quelle	Ziel	Port	Protokoll	Aktion	Begründung
Internet	DMZ	443	TCP	Allow	HTTPS-Traffic
DMZ	Internal	3306	TCP	Allow	Datenbank-Zugriff
Internal	Internet	80,443	TCP	Allow	Web-Zugriff
Any	Any	Any	Any	Deny	Default-Regel

Firewall-System: {{ netbox.firewall.system }}

Management: {{ netbox.firewall.management_url }}

19.3.2.2 Netzwerk-Segmentierung

Netzwerk-Zonen:

Zone	VLAN	Subnet	Zweck	Security-Level
DMZ	{{ netbox.vlan.dmz }}	{{ net-box.subnet.dmz }}	Öffentliche Services	Hoch
Production	{{ net-box.vlan.production }}	{{ net-box.subnet.production }}	Produktions-Systeme	Sehr hoch
Management	{{ net-box.vlan.management }}	{{ net-box.subnet.management }}	Admin-Zugriff	Kritisch
User	{{ netbox.vlan.user }}	{{ net-box.subnet.user }}	Benutzer-Netzwerk	Mittel
Guest	{{ netbox.vlan.guest }}	{{ net-box.subnet.guest }}	Gast-WLAN	Niedrig

Segmentierungs-Regeln: - Keine direkte Kommunikation zwischen Zonen - Traffic über Firewall/Router - Micro-Segmentierung für kritische Systeme - Zero-Trust-Prinzip

19.3.2.3 VPN-Härtung

VPN-Typ: {{ meta.vpn_type }}

Verschlüsselung: AES-256

Authentifizierung: Certificate-based + MFA

Härtungs-Maßnahmen: - Starke Verschlüsselungs-Algorithmen - Perfect Forward Secrecy (PFS)
- Certificate-based Authentication - Multi-Factor-Authentication (MFA) - Split-Tunneling deaktivieren - Inaktivitäts-Timeout (15 Min)

19.3.3 Applikations-Hardening

19.3.3.1 Web-Applikationen

OWASP Top 10 Mitigations:

Risiko	Mitigation
Injection	Prepared Statements, Input-Validation
Broken Authentication	MFA, Session-Management, Passwort-Policies
Sensitive Data Exposure	Encryption at Rest/Transit, HTTPS
XML External Entities	Disable XML External Entity Processing
Broken Access Control	RBAC, Least Privilege
Security Misconfiguration	Hardening, Security-Headers
XSS	Input-Validation, Output-Encoding, CSP
Insecure Deserialization	Input-Validation, Integrity-Checks
Using Components with Known Vulnerabilities	Dependency-Scanning, Updates
Insufficient Logging	Security-Logging, Monitoring

Security-Headers:

Strict-Transport-Security: max-age=31536000; includeSubDomains

X-Frame-Options: DENY

X-Content-Type-Options: nosniff

Content-Security-Policy: default-src 'self'

X-XSS-Protection: 1; mode=block

Referrer-Policy: no-referrer

19.3.3.2 Datenbank-Hardening

MySQL/MariaDB: - Root-Passwort ändern - Anonyme Benutzer entfernen - Test-Datenbank löschen - Remote-Root-Login deaktivieren - Least-Privilege für Applikations-Benutzer - SSL/TLS für Verbindungen - Audit-Plugin aktivieren

PostgreSQL: - pg_hba.conf restriktiv konfigurieren - SSL-Verbindungen erzwingen - Passwort-Verschlüsselung (SCRAM-SHA-256) - Audit-Logging aktivieren - Least-Privilege-Berechtigungen

Referenz: CIS Benchmark für Datenbanken

19.3.4 Cloud-Hardening

19.3.4.1 AWS-Hardening

IAM-Best-Practices: - Root-Account nicht verwenden - MFA für alle Benutzer - Least-Privilege-Policies - Rollen statt Benutzer für Services - Access-Keys rotieren

Netzwerk-Sicherheit: - Security-Groups restriktiv - NACLs für zusätzliche Kontrolle - VPC-Flow-Logs aktivieren - Private Subnets für Backend - VPN/Direct-Connect für Hybrid

Monitoring: - CloudTrail aktivieren - GuardDuty aktivieren - Config-Rules für Compliance - CloudWatch-Alarme

Referenz: CIS AWS Foundations Benchmark

19.3.4.2 Azure-Hardening

Identity-Management: - Azure AD mit MFA - Conditional Access Policies - Privileged Identity Management (PIM) - Identity Protection

Netzwerk-Sicherheit: - Network Security Groups (NSG) - Azure Firewall - DDoS Protection Standard - Private Endpoints

Monitoring: - Azure Security Center - Azure Sentinel - Activity Logs - Diagnostic Settings

Referenz: CIS Microsoft Azure Foundations Benchmark

19.4 Security-Monitoring

19.4.1 Security Information and Event Management (SIEM)

SIEM-System: {{ meta.siem_system }}

Version: {{ meta.siem_version }}

Management: {{ meta.siem_url }}

Log-Quellen: - Firewalls und IDS/IPS - Server (Windows, Linux) - Netzwerk-Geräte (Switches, Router) - Applikationen - Cloud-Services (AWS, Azure) - Endpoint-Security (EDR) - Identity-Management (AD, Azure AD)

Use-Cases:

Use-Case	Beschreibung	Priorität
Failed Login Attempts	Mehrfache fehlgeschlagene Logins	Hoch
Privilege Escalation	Unerwartete Admin-Rechte	Kritisch
Malware Detection	Antivirus/EDR-Alerts	Kritisch
Data Exfiltration	Ungewöhnliche Daten-Transfers	Hoch
Lateral Movement	Ungewöhnliche Netzwerk-Verbindungen	Hoch
Account Anomalies	Ungewöhnliche Account-Aktivitäten	Mittel

Use-Case	Beschreibung	Priorität
Configuration Changes	Änderungen an kritischen Systemen	Mittel

19.4.2 Intrusion Detection/Prevention (IDS/IPS)

IDS/IPS-System: {{ netbox.ids.system }}

Deployment: Inline (IPS-Modus)

Standort: {{ netbox.ids.location }}

Erkennungs-Methoden: - **Signature-based:** Bekannte Angriffsmuster - **Anomaly-based:** Abweichungen vom Normalverhalten - **Heuristic-based:** Verdächtiges Verhalten

Regel-Sets: - Emerging Threats - Snort Community Rules - Custom Rules für spezifische Umgebung

Tuning: - False-Positive-Reduktion - Regel-Priorisierung - Whitelist für legitimen Traffic

19.4.3 Endpoint Detection and Response (EDR)

EDR-System: {{ meta.edr_system }}

Abdeckung: Alle Workstations und Server

Funktionen: - Real-time Threat Detection - Behavioral Analysis - Automated Response - Forensic Capabilities - Threat Hunting

Response-Aktionen: - Alert generieren - Prozess beenden - Netzwerk-Verbindung blockieren - Host isolieren - Forensic-Daten sammeln

19.4.4 Security-Metriken

Metrik	Zielwert	Messung
Mean Time to Detect (MTTD)	< 1 Stunde	Durchschnittliche Erkennungszeit
Mean Time to Respond (MTTR)	< 4 Stunden	Durchschnittliche Response-Zeit
False Positive Rate	< 5%	False Positives / Gesamt-Alerts
Security Incidents	Trend abnehmend	Anzahl Incidents pro Monat
Patch Compliance	> 95%	Gepatchte Systeme / Gesamt-Systeme

19.5 Vulnerability Management

19.5.1 Vulnerability-Scanning

Scanning-Tools: - **Netzwerk-Scanner:** {{ meta.vulnerability_scanner }} - **Web-App-Scanner:** {{ meta.web_scanner }} - **Container-Scanner:** {{ meta.container_scanner }}

Scan-Frequenz: - **Kritische Systeme:** Wöchentlich - **Produktions-Systeme:** Monatlich - **Entwicklungs-Systeme:** Quartalsweise - **Ad-hoc:** Nach neuen Vulnerabilities (Zero-Days)

Scan-Typen: - **Authenticated Scans:** Mit Credentials (detaillierter) - **Unauthenticated Scans:** Ohne Credentials (Angreifer-Perspektive) - **Internal Scans:** Aus internem Netzwerk - **External Scans:** Aus Internet

19.5.2 Vulnerability-Bewertung

CVSS-Score (Common Vulnerability Scoring System):

CVSS-Score	Severity	SLA für Remediation
9.0 - 10.0	Critical	7 Tage
7.0 - 8.9	High	30 Tage
4.0 - 6.9	Medium	90 Tage
0.1 - 3.9	Low	180 Tage

Priorisierungs-Faktoren: - CVSS-Score - Exploit-Verfügbarkeit - Asset-Kritikalität - Exposure (Internet-facing) - Daten-Sensitivität

19.5.3 Remediation-Prozess

Vulnerability
Identified

Risk
Assessment

Remediation
Planning

Patch/Fix
Implementation

Verification
& Closure

Remediation-Optionen: - **Patching:** Software-Updates installieren - **Configuration Change:** Sichere Konfiguration - **Workaround:** Temporäre Mitigation - **Compensating Control:** Alternative Sicherheitsmaßnahme - **Accept Risk:** Risiko akzeptieren (mit Management-Genehmigung)

19.5.4 Penetration Testing

Test-Frequenz: Jährlich + nach größeren Changes

Test-Typen: - **Black-Box:** Keine Vorkenntnisse - **Gray-Box:** Teilweise Informationen - **White-Box:** Vollständige Informationen

Test-Scope: - Externe Infrastruktur (Internet-facing) - Interne Netzwerk-Segmente - Web-Applikationen - Mobile Apps - Social Engineering

Penetration-Test-Provider: {{ meta.pentest_provider }}

19.6 Security Incident Response

19.6.1 Incident-Kategorien

Kategorie	Beispiele	Severity
Malware	Virus, Ransomware, Trojaner	Hoch - Kritisch
Unauthorized Access	Kompromittierte Accounts, Brute-Force	Hoch
Data Breach	Daten-Exfiltration, Daten-Leak	Kritisch
DDoS	Denial-of-Service-Angriffe	Hoch
Phishing	Phishing-E-Mails, Social Engineering	Mittel - Hoch
Insider Threat	Böswillige Insider-Aktivitäten	Hoch - Kritisch
Policy Violation	Verstoß gegen Security-Policies	Niedrig - Mittel

19.6.2 Incident-Response-Prozess

19.6.2.1 1. Preparation

Vorbereitungs-Aktivitäten: - Incident-Response-Team definieren - Incident-Response-Plan erstellen - Tools und Ressourcen bereitstellen - Training und Übungen durchführen - Kontakt-Listen pflegen

IR-Team: - **IR-Manager:** Thomas Weber - **Technical Lead:** Andreas Huemmer - **Forensic Analyst:** [Name] - **Communication Lead:** [Name] - **Legal Counsel:** [Name]

19.6.2.2 2. Detection & Analysis

Erkennungs-Quellen: - SIEM-Alerts - IDS/IPS-Alerts - EDR-Alerts - Benutzer-Meldungen - Threat Intelligence

Analyse-Aktivitäten: - Alert-Validierung (True/False Positive) - Scope-Ermittlung (betroffene Systeme) - Impact-Assessment - Incident-Klassifizierung - Incident-Priorisierung

Incident-Ticket: {{ meta.ticketing_system }}

19.6.2.3 3. Containment

Short-term Containment: - Betroffene Systeme isolieren - Netzwerk-Verbindungen blockieren - Kompromittierte Accounts deaktivieren - Malware-Ausbreitung stoppen

Long-term Containment: - Temporäre Fixes implementieren - Systeme in isolierte Umgebung verschieben - Monitoring verstärken

19.6.2.4 4. Eradication

Eradication-Aktivitäten: - Malware entfernen - Backdoors schließen - Kompromittierte Accounts löschen - Vulnerabilities patchen - Systeme neu aufsetzen (falls erforderlich)

19.6.2.5 5. Recovery

Recovery-Aktivitäten: - Systeme aus sauberen Backups wiederherstellen - Passwörter zurücksetzen - Systeme härten - Monitoring aktivieren - Schrittweise in Produktion nehmen

Validierung: - Keine Malware-Spuren - Keine Backdoors - Normale Funktionalität - Performance akzeptabel

19.6.2.6 6. Post-Incident Activity

Lessons-Learned-Meeting: - Was ist passiert? - Wie wurde es erkannt? - Was lief gut? - Was lief schlecht? - Verbesserungs-Maßnahmen

Dokumentation: - Incident-Report erstellen - Timeline dokumentieren - IOCs (Indicators of Compromise) sammeln - Kosten erfassen

Follow-up: - Verbesserungs-Maßnahmen umsetzen - Policies aktualisieren - Training durchführen - Threat-Intelligence teilen

19.6.3 Incident-Response-Playbooks

Ransomware-Playbook: 1. Betroffene Systeme sofort isolieren 2. Keine Lösegeldzahlung (Policy) 3. Forensic-Analyse durchführen 4. Strafverfolgung informieren 5. Aus Backups wiederherstellen 6. Vulnerabilities patchen

Data-Breach-Playbook: 1. Scope ermitteln (welche Daten, wie viele Betroffene) 2. Exfiltration stoppen 3. Forensic-Analyse 4. Legal-Team einbinden 5. Meldepflichten prüfen (DSGVO: 72h) 6. Betroffene informieren 7. Aufsichtsbehörde melden

Phishing-Playbook: 1. Phishing-E-Mail identifizieren 2. E-Mail-Filter aktualisieren 3. Betroffene Benutzer identifizieren 4. Passwörter zurücksetzen (falls Credentials eingegeben) 5. Awareness-Training durchführen

19.7 Compliance und Regulierung

19.7.1 ISO 27001:2013

Implementierungs-Status:

Annex A Control	Titel	Status	Verantwortlich
A.9	Access Control	Implementiert	Thomas Weber
A.10	Cryptography	Implementiert	IT-Security
A.12	Operations Security	Implementiert	IT-Operations
A.13	Communications Security	Implementiert	Network-Team
A.14	System Acquisition	Teilweise	IT-Management
A.16	Incident Management	Implementiert	IR-Team
A.17	Business Continuity	Implementiert	BC-Manager
A.18	Compliance	Implementiert	Compliance-Officer

Audit-Frequenz: Jährlich (extern), Quartalsweise (intern)

Nächstes Audit: {{ meta.next_iso_audit }}

19.7.2 BSI Grundschutz

Basis-Absicherung: - Alle Bausteine der Basis-Absicherung implementiert - Standard-Sicherheitsmaßnahmen umgesetzt - Dokumentation vollständig

Kern-Absicherung: - Kritische Bausteine identifiziert - Erhöhte Sicherheitsmaßnahmen implementiert - Regelmäßige Reviews

Zertifizierung: [Geplant/In Arbeit/Zertifiziert]

19.7.3 DSGVO (GDPR)

Technische und organisatorische Maßnahmen (TOMs):

Maßnahme	Implementierung
Verschlüsselung	AES-256 at Rest, TLS 1.3 in Transit
Pseudonymisierung	Wo möglich implementiert
Zugriffskontrolle	RBAC, MFA, PAM
Logging	Zentrale Log-Sammlung, SIEM
Backup	3-2-1-Regel, verschlüsselt
Incident Response	IR-Plan, 72h-Meldepflicht

Datenschutz-Folgenabschätzung (DSFA): - Für Hochrisiko-Verarbeitungen durchgeführt - Dokumentiert und genehmigt

Datenschutzbeauftragter: {{ meta.data_protection_officer }}

19.7.4 Weitere Standards

PCI-DSS: [Falls zutreffend]

HIPAA: [Falls zutreffend]

SOX: [Falls zutreffend]

19.8 Security-Awareness und Training

19.8.1 Awareness-Programm

Zielgruppe: Alle Mitarbeiter

Trainings-Themen: - Passwort-Sicherheit - Phishing-Erkennung - Social Engineering - Sichere Nutzung von IT-Systemen - Daten-Klassifizierung - Incident-Meldung - DSGVO-Grundlagen

Trainings-Frequenz: - Onboarding: Sofort - Auffrischung: Jährlich - Phishing-Simulationen: Quartalsweise

Phishing-Simulationen: - Quartalsweise Kampagnen - Verschiedene Phishing-Typen - Sofortiges Feedback - Zusätzliches Training bei Klick

19.8.2 Security-Champions

Konzept: Security-Ansprechpartner in jeder Abteilung

Aufgaben: - Security-Awareness fördern - Security-Fragen beantworten - Security-Incidents melden - Best Practices verbreiten

Training: Erweiterte Security-Schulungen

19.9 Rollen und Verantwortlichkeiten

19.9.1 Chief Information Security Officer (CISO)

Verantwortlichkeiten: - Security-Strategie-Ownership - Risiko-Management - Compliance-Sicherstellung - Incident-Response-Koordination - Security-Budget

Person: Thomas Weber

19.9.2 Security-Operations-Team

Verantwortlichkeiten: - SIEM-Monitoring - Incident-Response - Vulnerability-Management - Security-Tool-Verwaltung

Team-Größe: [Anzahl]

19.9.3 IT-Operations-Team

Verantwortlichkeiten: - System-Hardening - Patch-Management - Security-Konfiguration - Backup-Sicherheit

Lead: Andreas Huemmer

19.10 Metriken und Reporting

19.10.1 Security-Metriken

Metrik	Zielwert	Frequenz
Security Incidents	Trend abnehmend	Monatlich
MTTD	< 1 Stunde	Monatlich
MTTR	< 4 Stunden	Monatlich
Patch Compliance	> 95%	Wöchentlich
Vulnerability Remediation	> 90% in SLA	Monatlich
Phishing-Click-Rate	< 5%	Quartalsweise
Security-Training-Completion	100%	Jährlich

19.10.2 Reporting

Wöchentliches Security-Dashboard: - Neue Security-Incidents - Offene Vulnerabilities - Patch-Status - SIEM-Alert-Statistiken

Monatliches Security-Report: - Security-Metriken - Incident-Zusammenfassung - Vulnerability-Trends - Compliance-Status

Quartalsweises Management-Report: - Security-Posture-Assessment - Risiko-Bewertung - Compliance-Status - Budget und Ressourcen - Strategische Empfehlungen

19.11 Referenzen

- ISO/IEC 27001:2013 - Information Security Management
- BSI IT-Grundschutz-Kompendium
- NIST Cybersecurity Framework
- CIS Controls v8
- OWASP Top 10
- SANS Top 25 Software Errors
- MITRE ATT&CK Framework
- DSGVO (GDPR)

Dokumentverantwortlicher: IT Operations Manager

Genehmigt durch: CIO

Version: 1.0.0

Klassifizierung: internal

Letzte Aktualisierung: {{ meta.date }}

ewpage

Chapter 20

Patch und Update Management

20.1 Zweck und Geltungsbereich

Dieses Dokument beschreibt die Patch- und Update-Management-Prozesse für AdminSend GmbH. Es definiert Patch-Kategorien, Zeitpläne, Test- und Rollout-Prozesse sowie Vulnerability-Scanning und Priorisierung zur Sicherstellung der System-Sicherheit und -Stabilität.

Geltungsbereich: Alle IT-Systeme, Betriebssysteme, Applikationen und Firmware von AdminSend GmbH

Verantwortlich: Andreas Huemmer (andreas.huemmer@adminsends.de)

20.2 Patch-Management-Grundlagen

20.2.1 Ziele

Primäre Ziele: - **Sicherheit:** Schließen von Sicherheitslücken - **Stabilität:** Behebung von Bugs und Fehlern - **Compliance:** Erfüllung regulatorischer Anforderungen - **Performance:** Optimierung und neue Features - **Kompatibilität:** Unterstützung neuer Technologien

20.2.2 Patch-Kategorien

20.2.2.1 Security Patches (Sicherheits-Updates)

Beschreibung: Patches, die Sicherheitslücken schließen

Priorität: Kritisch bis Hoch

Beispiele: - CVE-behaftete Vulnerabilities - Zero-Day-Exploits - Kritische Sicherheitslücken

SLA: - **Critical (CVSS 9.0-10.0):** 7 Tage - **High (CVSS 7.0-8.9):** 30 Tage - **Medium (CVSS 4.0-6.9):** 90 Tage - **Low (CVSS 0.1-3.9):** 180 Tage

20.2.2.2 Feature Updates (Funktions-Updates)

Beschreibung: Updates mit neuen Funktionen und Verbesserungen

Priorität: Mittel

Beispiele: - Neue Features - Performance-Verbesserungen - UI/UX-Verbesserungen

SLA: Nach Bedarf, geplant in Wartungsfenstern

20.2.2.3 Bugfix Patches (Fehlerbehebungen)

Beschreibung: Patches zur Behebung von Bugs ohne Sicherheitsrelevanz

Priorität: Niedrig bis Mittel

Beispiele: - Funktionale Fehler - Performance-Probleme - Kompatibilitäts-Probleme

SLA: 90 Tage oder nach Bedarf

20.2.2.4 Firmware Updates

Beschreibung: Updates für Hardware-Firmware

Priorität: Mittel bis Hoch

Beispiele: - BIOS/UEFI-Updates - Storage-Controller-Firmware - Netzwerk-Equipment-Firmware

SLA: Nach Herstellerempfehlung, geplant

20.2.3 Patch-Quellen

System-Typ	Patch-Quelle	Update-Mechanismus
Windows	Windows Update, WSUS	Automatisch/Manuell
Linux (RHEL/CentOS)	Red Hat Network, YUM	yum update
Linux (Ubuntu/Debian)	Ubuntu Repositories, APT	apt update && apt upgrade
VMware	VMware Update Manager	VUM
Applikationen	Vendor-Websites, Package-Manager	Manuell/Automatisch
Firmware	Vendor-Support-Sites	Manuell
Cloud-Services	Provider-Managed	Automatisch

20.3 Patch-Management-Prozess

20.3.1 Prozess-Übersicht

Vulnerability
Identification

Patch
Assessment

Patch
Acquisition

Patch
Testing

Patch
Deployment

Verification
& Reporting

20.3.2 1. Vulnerability Identification

Identifikations-Quellen: - **Vulnerability-Scanner:** {{ meta.vulnerability_scanner }} - **Vendor-Advisories:** Microsoft, Red Hat, VMware, etc. - **Security-Mailinglists:** CERT, US-CERT, vendor-specific - **Threat-Intelligence:** {{ meta.threat_intelligence_source }} - **SIEM-Alerts:** {{ meta.siem_system }}

Aktivitäten: - Vulnerability-Scans durchführen (wöchentlich) - Vendor-Advisories überwachen (täglich) - CVE-Datenbank prüfen - Betroffene Systeme identifizieren - Patch-Verfügbarkeit prüfen

Verantwortlich: Security-Operations-Team

20.3.3 2. Patch Assessment

Bewertungs-Kriterien:

Kriterium	Bewertung
CVSS-Score	0.0 - 10.0
Exploit-Verfügbarkeit	Ja/Nein
Asset-Kritikalität	Kritisch/Wichtig/Standard
Exposure	Internet-facing/Internal
Vendor-Empfehlung	Sofort/Geplant/Optional

Risiko-Matrix:

	Internet-facing	Internal
Critical (CVSS 9-10)	Sofort (7 Tage)	Hoch (14 Tage)
High (CVSS 7-8.9)	Hoch (14 Tage)	Mittel (30 Tage)
Medium (CVSS 4-6.9)	Mittel (30 Tage)	Niedrig (90 Tage)

	Internet-facing	Internal
Low (CVSS 0-3.9)	Niedrig (90 Tage)	Sehr niedrig (180 Tage)

Impact-Assessment: - Welche Systeme sind betroffen? - Welche Business-Prozesse sind abhängig?
- Ist ein Reboot erforderlich? - Gibt es bekannte Kompatibilitäts-Probleme? - Welches Wartungs-
fenster ist verfügbar?

Entscheidung: - **Patch:** Patch installieren - **Defer:** Patch verschieben (mit Begründung) - **Re-**
ject: Patch nicht installieren (mit Begründung) - **Workaround:** Alternative Mitigation

Verantwortlich: Patch-Management-Team

20.3.4 3. Patch Acquisition

Beschaffungs-Aktivitäten: - Patch von Vendor-Quelle herunterladen - Patch-Integrität veri-
fizieren (Checksums, Signaturen) - Patch in Patch-Repository speichern - Patch-Metadaten doku-
mentieren

Patch-Repository: {{ meta.patch_repository }}

Dokumentation: - Patch-ID - Vendor - Release-Date - CVE-IDs - Betroffene Systeme -
Installations-Anweisungen

Verantwortlich: Patch-Management-Team

20.3.5 4. Patch Testing

Test-Umgebungen:

Umgebung	Zweck	Systeme
Dev	Entwickler-Tests	{{ netbox.environment.dev }}
Test	Funktionale Tests	{{ netbox.environment.test }}
Staging	Pre-Production-Tests	{{ netbox.environment.staging }}
Production	Produktiv-Systeme	{{ netbox.environment.production }}

Test-Prozess:

20.3.5.1 Phase 1: Dev-Testing (Optional)

Dauer: 1-2 Tage

Aktivitäten: - Patch in Dev-Umgebung installieren - Basis-Funktionalität testen - Offensichtliche
Probleme identifizieren

20.3.5.2 Phase 2: Test-Testing

Dauer: 3-5 Tage

Aktivitäten: - Patch in Test-Umgebung installieren - Funktionale Tests durchführen - Performance-Tests durchführen - Kompatibilitäts-Tests durchführen - Rollback-Prozedur testen

Test-Checkliste: - ☐ Patch erfolgreich installiert - ☐ System startet nach Reboot - ☐ Applikationen starten - ☐ Basis-Funktionalität funktioniert - ☐ Performance akzeptabel - ☐ Keine Error-Logs - ☐ Rollback erfolgreich getestet

20.3.5.3 Phase 3: Staging-Testing

Dauer: 2-3 Tage

Aktivitäten: - Patch in Staging-Umgebung installieren - Business-Prozess-Tests durchführen - User-Acceptance-Tests (UAT) - Last-Tests (falls kritisch)

Go/No-Go-Entscheidung: - Alle Tests bestanden → Go - Kritische Probleme → No-Go, Patch zurückstellen - Nicht-kritische Probleme → Go mit Workaround

Verantwortlich: QA-Team, Applikations-Owner

Ausnahmen (Emergency-Patches): - Kritische Security-Patches können Test-Phase verkürzen - Mindestens Basis-Tests in Test-Umgebung - Erhöhtes Risiko akzeptiert und dokumentiert

20.3.6 5. Patch Deployment

Deployment-Strategien:

20.3.6.1 Phased Rollout (Standard)

Beschreibung: Schrittweise Ausrollung in Phasen

Phasen: 1. **Pilot-Gruppe:** 5-10% der Systeme (1-2 Tage) 2. **Phase 1:** 25% der Systeme (2-3 Tage) 3. **Phase 2:** 50% der Systeme (2-3 Tage) 4. **Phase 3:** Alle verbleibenden Systeme

Vorteile: - Risiko-Minimierung - Frühe Problem-Erkennung - Kontrollierte Ausrollung

Anwendung: Standard-Patches, Feature-Updates

20.3.6.2 Big Bang (Alle auf einmal)

Beschreibung: Alle Systeme gleichzeitig patchen

Vorteile: - Schnelle Ausrollung - Einfache Koordination

Nachteile: - Hohes Risiko - Große Impact bei Problemen

Anwendung: Nur für unkritische Systeme oder in Notfällen

20.3.6.3 Rolling Update

Beschreibung: Systeme nacheinander patchen (z.B. in Clustern)

Vorteile: - Keine Downtime - Kontinuierliche Verfügbarkeit

Anwendung: Hochverfügbare Systeme, Load-Balanced-Cluster

Deployment-Methoden:

Methode	Tool	Anwendung
Automatisch	WSUS, SCCM, Ansible	Standard-Patches
Semi-Automatisch	Patch-Management-Tool	Geplante Patches
Manuell	Remote-Session	Kritische Systeme, Firmware

Deployment-Zeitfenster:

System-Tier	Wartungsfenster	Frequenz
Tier 0 (Kritisch)	Sonntag 02:00-06:00	Monatlich
Tier 1 (Wichtig)	Samstag 22:00-02:00	Monatlich
Tier 2 (Standard)	Mittwoch 20:00-22:00	Monatlich
Tier 3 (Unkritisch)	Jederzeit	Nach Bedarf

Deployment-Checkliste: - ☐ Change-Ticket erstellt und genehmigt - ☐ Stakeholder informiert - ☐ Backup erstellt - ☐ Rollback-Plan bereit - ☐ Monitoring aktiviert - ☐ On-Call-Team verfügbar

Verantwortlich: IT-Operations-Team

20.3.7 6. Verification & Reporting

Verifikations-Aktivitäten: - Patch-Installation bestätigen - System-Funktionalität prüfen - Performance-Metriken überwachen - Error-Logs prüfen - Vulnerability-Scan wiederholen

Verifikations-Checkliste: - ☐ Patch auf allen Ziel-Systemen installiert - ☐ Systeme laufen stabil - ☐ Keine kritischen Errors - ☐ Performance normal - ☐ Vulnerability geschlossen (Scan)

Reporting: - Patch-Status-Report - Erfolgs-/Fehler-Rate - Offene Patches - Compliance-Status

Verantwortlich: Patch-Management-Team

20.4 Patch-Zeitpläne

20.4.1 Monatlicher Patch-Zyklus

Microsoft Patch Tuesday: - **Patch-Release:** 2. Dienstag im Monat - **Assessment:** Dienstag-Mittwoch - **Testing:** Mittwoch-Freitag (Woche 1) - **Staging:** Montag-Mittwoch (Woche 2) - **Production-Deployment:** Samstag/Sonntag (Woche 2-3)

Linux-Patches: - **Assessment:** Wöchentlich (Montag) - **Testing:** Dienstag-Donnerstag - **Deployment:** Samstag (monatlich)

Applikations-Patches: - **Assessment:** Bei Vendor-Release - **Testing:** 1 Woche - **Deployment:** Nächstes Wartungsfenster

20.4.2 Emergency-Patches

Trigger: - Critical-Vulnerability (CVSS > 9.0) - Aktive Exploits in the Wild - Zero-Day-Vulnerabilities - Vendor-Empfehlung "Sofort"

Prozess: - **Assessment:** Sofort (< 4 Stunden) - **Testing:** Minimal (< 8 Stunden) - **Deployment:** Sofort (< 24 Stunden)

Genehmigung: CIO oder CISO

Kommunikation: Alle Stakeholder sofort informieren

20.4.3 Patch-Kalender

Woche	Montag	Dienstag	Mittwoch	Donnerstag	Freitag	Samstag	Sonntag
Woche 1	Assessment	Testing	Testing	Testing	Testing	-	-
Woche 2	Staging	Staging	Staging	Go/No-Go	-	Tier 1 Deploy	Tier 0 Deploy
Woche 3	Verification	Reporting	Tier 2 Deploy	-	-	-	-
Woche 4	-	-	-	-	-	-	-

20.5 Patch-Management-Tools

20.5.1 Windows-Patch-Management

Tool: Windows Server Update Services (WSUS)

Server: {{ netbox.wsus.server }}

Management: {{ netbox.wsus.management_url }}

Konfiguration: - Automatische Synchronisation mit Microsoft Update - Patch-Approval-Workflow - Computer-Gruppen nach Tier - Reporting und Compliance-Dashboard

Patch-Gruppen: - **Pilot:** Test-Systeme - **Tier-0:** Kritische Produktions-Systeme - **Tier-1:** Wichtige Produktions-Systeme - **Tier-2:** Standard-Systeme - **Tier-3:** Unkritische Systeme

20.5.2 Linux-Patch-Management

Tool: Ansible / Satellite

Server: {{ netbox.ansible.server }}

Playbooks: - patch-assessment.yml - Verfügbare Updates prüfen - patch-security.yml - Nur Security-Updates - patch-all.yml - Alle Updates - patch-rollback.yml - Rollback

Beispiel-Playbook:

```
---
- name: Patch Linux Servers
  hosts: linux_servers
  become: yes
  tasks:
    - name: Update package cache
```

```

apt:
  update_cache: yes
  when: ansible_os_family == "Debian"

- name: Install security updates
  apt:
    upgrade: safe
    autoremove: yes
    when: ansible_os_family == "Debian"

- name: Check if reboot required
  stat:
    path: /var/run/reboot-required
  register: reboot_required

- name: Reboot if required
  reboot:
    msg: "Reboot for security updates"
    when: reboot_required.stat.exists

```

20.5.3 VMware-Patch-Management

Tool: VMware Update Manager (VUM)

Integration: vCenter {{ netbox.vcenter.server }}

Baseline-Gruppen: - **Critical-Patches:** Kritische Security-Patches - **Non-Critical-Patches:** Alle anderen Patches - **Upgrades:** ESXi-Upgrades

Remediation-Prozess: - Baseline-Compliance prüfen - Hosts in Maintenance-Mode - Patches installieren - Hosts rebooten - Compliance verifizieren

20.5.4 Vulnerability-Scanner

Tool: {{ meta.vulnerability_scanner }}

Scan-Frequenz: Wöchentlich

Scan-Profile: - **Full-Scan:** Alle Vulnerabilities - **Patch-Scan:** Nur fehlende Patches - **Compliance-Scan:** Compliance-Checks

Integration: SIEM, Ticketing-System

20.6 Rollback-Prozeduren

20.6.1 Rollback-Trigger

Rollback erforderlich bei: - Kritische Funktionalität nicht verfügbar - Performance-Degradation > 20% - Daten-Korruption - Sicherheits-Probleme durch Patch - Business-Prozess-Ausfall

Rollback-Entscheidung: IT Operations Manager oder höher

20.6.2 Rollback-Methoden

20.6.2.1 Windows-Rollback

Methode 1: Windows-Uninstall

Patch-Liste anzeigen

Get-HotFix

Patch deinstallieren

wusa /uninstall /kb:KBXXXXXX /quiet /norestart

Methode 2: System-Restore - Restore-Point vor Patch-Installation - System-Wiederherstellung durchführen

Methode 3: Backup-Restore - VM-Snapshot wiederherstellen - Bare-Metal-Restore

20.6.2.2 Linux-Rollback

Methode 1: Package-Downgrade

Ubuntu/Debian

apt-cache policy <package>

apt-get install <package>=<old-version>

RHEL/CentOS

yum downgrade <package>

Methode 2: Snapshot-Rollback - LVM-Snapshot wiederherstellen - VM-Snapshot wiederherstellen

20.6.2.3 VMware-Rollback

Methode: VUM-Rollback - Baseline-Remediation rückgängig machen - Vorherige Patch-Version installieren

20.6.3 Rollback-Prozess

1. Rollback-Entscheidung treffen

- Impact bewerten
- Stakeholder informieren

2. Rollback durchführen

- Rollback-Methode auswählen
- Rollback ausführen
- System neu starten (falls erforderlich)

3. Verifikation

- Funktionalität prüfen
- Performance prüfen
- Logs prüfen

4. Dokumentation

- Rollback-Grund dokumentieren
- Lessons Learned

- Alternative Lösungen evaluieren

20.7 Compliance und Reporting

20.7.1 Patch-Compliance-Metriken

Metrik	Zielwert	Messung
Patch Compliance Rate	> 95%	Gepatchte Systeme / Gesamt-Systeme
Critical Patch SLA	> 95%	Patches in SLA / Gesamt-Patches
Mean Time to Patch (MTTP)	< 30 Tage	Durchschnittliche Patch-Dauer
Patch Success Rate	> 98%	Erfolgreiche Patches / Gesamt-Patches
Rollback Rate	< 2%	Rollbacks / Gesamt-Patches

20.7.2 Patch-Compliance-Dashboard

Metriken: - Patch-Status nach System-Tier - Offene Critical-Patches - SLA-Compliance - Patch-Trends (monatlich) - Top-10-Vulnerabilities

Tool: {{ meta.patch_dashboard }}

Zugriff: IT-Management, Security-Team

20.7.3 Reporting

Wöchentliches Patch-Status-Report: - Neue Patches verfügbar - Patches in Testing - Geplante Deployments - Offene Critical-Patches

Monatliches Patch-Compliance-Report: - Patch-Compliance-Rate - SLA-Compliance - Patch-Statistiken - Trend-Analysen - Verbesserungs-Maßnahmen

Quartalsweises Management-Report: - Patch-Management-Strategie-Review - Risiko-Assessment - Compliance-Status - Budget und Ressourcen

Empfänger: - Wöchentlich: IT-Operations-Team - Monatlich: IT-Management, Security-Team - Quartalsweise: CIO, CISO, Management

20.8 Ausnahmen und Sonderfälle

20.8.1 Patch-Ausnahmen

Gründe für Ausnahmen: - Vendor-Support endet (End-of-Life) - Applikations-Inkompatibilität - Business-kritische Systeme (Change-Freeze) - Spezielle Vendor-Anforderungen

Ausnahme-Prozess: 1. Ausnahme-Antrag stellen 2. Risiko-Assessment durchführen 3. Kompensations-Maßnahmen definieren 4. Management-Genehmigung einholen 5. Ausnahme dokumentieren 6. Regelmäßig reviewen (quartalsweise)

Ausnahme-Register: {{ meta.exception_register }}

20.8.2 End-of-Life-Systeme

Strategie: - Migration planen - Netzwerk-Segmentierung - Zusätzliche Monitoring - Kompensations-Kontrollen - Risiko-Akzeptanz dokumentieren

EOL-Register: {{ meta.eol_register }}

20.8.3 Legacy-Applikationen

Herausforderungen: - Keine Patches verfügbar - Inkompatibilität mit neuen OS-Versionen - Vendor-Support eingestellt

Mitigations: - Virtualisierung/Containerisierung - Netzwerk-Isolation - WAF/IPS vor Applikation - Regelmäßige Vulnerability-Scans - Migrations-Roadmap

20.9 Rollen und Verantwortlichkeiten

20.9.1 Patch-Management-Team

Verantwortlichkeiten: - Patch-Prozess-Ownership - Vulnerability-Assessment - Patch-Testing-Koordination - Deployment-Planung - Reporting

Team-Lead: Andreas Huemmer

20.9.2 System-Administratoren

Verantwortlichkeiten: - Patch-Deployment durchführen - System-Monitoring - Rollback-Durchführung - Dokumentation

20.9.3 Security-Team

Verantwortlichkeiten: - Vulnerability-Scanning - Risiko-Assessment - Security-Patch-Priorisierung - Compliance-Überwachung

Lead: Thomas Weber

20.9.4 Applikations-Owner

Verantwortlichkeiten: - Applikations-Kompatibilität prüfen - User-Acceptance-Tests - Go/No-Go-Entscheidung - Business-Impact-Assessment

20.9.5 Change-Manager

Verantwortlichkeiten: - Change-Tickets genehmigen - Change-Kalender verwalten - Stakeholder-Kommunikation - Post-Implementation-Review

20.10 Best Practices

20.10.1 Patch-Management-Best-Practices

1. **Regelmäßige Vulnerability-Scans**
 - Wöchentliche Scans
 - Automatisierte Scans
 - Priorisierung nach Risiko
2. **Test vor Deployment**
 - Immer in Test-Umgebung testen
 - Rollback-Plan bereit haben
 - Dokumentation aktuell halten
3. **Phased Rollout**
 - Pilot-Gruppe zuerst
 - Schrittweise Ausrollung
 - Monitoring während Rollout
4. **Backup vor Patching**
 - Immer Backup erstellen
 - Backup-Integrität prüfen
 - Restore-Prozedur testen
5. **Kommunikation**
 - Stakeholder frühzeitig informieren
 - Status-Updates während Deployment
 - Post-Deployment-Kommunikation
6. **Dokumentation**
 - Patch-Prozess dokumentieren
 - Lessons Learned festhalten
 - Knowledge-Base pflegen
7. **Automatisierung**
 - Patch-Deployment automatisieren
 - Reporting automatisieren
 - Compliance-Checks automatisieren
8. **Kontinuierliche Verbesserung**
 - Prozess regelmäßig reviewen
 - Metriken analysieren
 - Optimierungen umsetzen

20.11 Referenzen

- NIST SP 800-40 Rev. 4 - Guide to Enterprise Patch Management Planning
 - ISO/IEC 27002:2013 - Control 12.6.1 (Management of Technical Vulnerabilities)
 - CIS Controls v8 - Control 7 (Continuous Vulnerability Management)
 - ITIL v4 - Change Enablement Practice
 - Vendor-Patch-Dokumentation (Microsoft, Red Hat, VMware)
 - CVE Database: <https://cve.mitre.org>
 - NVD Database: <https://nvd.nist.gov>
-

Dokumentverantwortlicher: IT Operations Manager

Genehmigt durch: CIO

Version: 1.0.0

Klassifizierung: internal

Letzte Aktualisierung: {{ meta.date }}

ewpage

Chapter 21

Log Management und Audit

21.1 Zweck und Geltungsbereich

Dieses Dokument beschreibt die Log-Management- und Audit-Prozesse für AdminSend GmbH. Es definiert Log-Sammlung, -Aggregation, -Retention, Audit-Trail-Anforderungen und SIEM-Integration zur Sicherstellung von Nachvollziehbarkeit, Compliance und Security-Monitoring.

Geltungsbereich: Alle IT-Systeme, Netzwerke, Applikationen und Security-Komponenten von AdminSend GmbH

Verantwortlich: Thomas Weber (thomas.weber@adminsends.de)

21.2 Log-Management-Grundlagen

21.2.1 Ziele

Primäre Ziele: - **Security-Monitoring:** Erkennung von Sicherheitsvorfällen - **Compliance:** Erfüllung regulatorischer Anforderungen - **Troubleshooting:** Fehleranalyse und Problemlösung - **Forensik:** Nachvollziehbarkeit von Ereignissen - **Audit:** Nachweis von Kontrollen und Prozessen - **Performance-Analyse:** System- und Applikations-Performance

21.2.2 Log-Typen

21.2.2.1 System-Logs

Beschreibung: Betriebssystem-Ereignisse

Beispiele: - Windows Event Logs (Security, System, Application) - Linux Syslog (/var/log/messages, /var/log/auth.log) - Boot-Logs, Kernel-Logs

Wichtige Events: - System-Start/-Stop - Service-Start/-Stop - Fehler und Warnungen - Hardware-Events

21.2.2.2 Security-Logs

Beschreibung: Sicherheitsrelevante Ereignisse

Beispiele: - Authentifizierungs-Events (Login, Logout, Failed Login) - Autorisierungs-Events (Zugriffsverweigerung) - Privilegien-Änderungen - Security-Policy-Änderungen - Firewall-Logs - IDS/IPS-Alerts

Wichtige Events: - Failed Login Attempts - Privilege Escalation - Account-Änderungen - Security-Policy-Änderungen

21.2.2.3 Application-Logs

Beschreibung: Applikations-spezifische Ereignisse

Beispiele: - Web-Server-Logs (Apache, Nginx, IIS) - Datenbank-Logs (MySQL, PostgreSQL, SQL Server) - Applikations-Logs (Custom-Apps) - Middleware-Logs (Tomcat, JBoss)

Wichtige Events: - Applikations-Fehler - Transaktions-Logs - Performance-Metriken - User-Aktivitäten

21.2.2.4 Network-Logs

Beschreibung: Netzwerk-Ereignisse

Beispiele: - Firewall-Logs - Router/Switch-Logs - VPN-Logs - DNS-Logs - DHCP-Logs - Proxy-Logs

Wichtige Events: - Verbindungs-Versuche (erlaubt/blockiert) - Netzwerk-Änderungen - Bandwidth-Nutzung - Anomalien

21.2.2.5 Audit-Logs

Beschreibung: Compliance- und Audit-relevante Ereignisse

Beispiele: - Daten-Zugriffe - Konfigurations-Änderungen - Administrative Aktivitäten - Privilegierte Zugriffe

Wichtige Events: - Wer hat was wann gemacht? - Änderungen an kritischen Systemen - Zugriff auf sensible Daten

21.2.3 Log-Levels

Level	Beschreibung	Verwendung	Beispiel
EMERGENCY	System unbrauchbar	Kritische Systemfehler	Kernel Panic
ALERT	Sofortige Aktion erforderlich	Kritische Fehler	Datenbank nicht erreichbar
CRITICAL	Kritische Bedingungen	Schwere Fehler	Disk voll
ERROR	Fehler-Bedingungen	Fehler	Applikations-Fehler
WARNING	Warnungs-Bedingungen	Warnungen	Disk 80% voll
NOTICE	Normale aber signifikante Bedingung	Wichtige Events	Service gestartet
INFO	Informations-Meldungen	Normale Events	User-Login
DEBUG	Debug-Meldungen	Entwicklung	Funktions-Aufrufe

Level	Beschreibung	Verwendung	Beispiel
-------	--------------	------------	----------

21.3 Log-Sammlung und -Aggregation

21.3.1 Log-Architektur

Log-Quellen

Servers, Network, Applications, Security-Devices

Syslog, Agents, APIs

Log-Collectors/Forwarders

Rsyslog, Fluentd, Logstash, Splunk Forwarders

Parsing, Filtering, Enrichment

Log-Aggregation-Plattform

SIEM, ELK Stack, Splunk, Graylog

Hot Storage
(Fast Access)

Cold Storage / Archive
(Long-term Retention)

21.3.2 Log-Sammlung-Methoden

21.3.2.1 Syslog

Protokoll: RFC 5424 (Syslog Protocol)

Transport: UDP 514 (Standard), TCP 514 (Reliable), TLS 6514 (Secure)

Vorteile: - Standard-Protokoll - Weit verbreitet - Einfache Konfiguration

Nachteile: - UDP nicht zuverlässig - Begrenzte Struktur - Keine Authentifizierung (ohne TLS)

Verwendung: Linux/Unix-Systeme, Netzwerk-Geräte

21.3.2.2 Agent-basiert

Agents: - Splunk Universal Forwarder - Elastic Beats (Filebeat, Metricbeat) - Fluentd - NXLog

Vorteile: - Zuverlässige Übertragung - Lokale Pufferung - Parsing und Filtering - Verschlüsselte Übertragung

Nachteile: - Agent-Installation erforderlich - Agent-Management - Ressourcen-Verbrauch

Verwendung: Server, Workstations

21.3.2.3 API-basiert

Methoden: - REST APIs - Cloud-Provider-APIs (AWS CloudWatch, Azure Monitor) - Webhook-Integration

Vorteile: - Strukturierte Daten - Echtzeit-Integration - Keine Agent-Installation

Nachteile: - API-Limits - Netzwerk-Abhängigkeit - Komplexere Konfiguration

Verwendung: Cloud-Services, SaaS-Applikationen

21.3.2.4 Windows Event Forwarding (WEF)

Methode: Windows-native Event-Forwarding

Vorteile: - Keine zusätzlichen Agents - Zentrale Konfiguration via GPO - Zuverlässig

Nachteile: - Nur Windows - Begrenzte Parsing-Optionen

Verwendung: Windows-Umgebungen

21.3.3 Log-Aggregation-Plattform

SIEM-System: {{ meta.siem_system }}

Version: {{ meta.siem_version }}

Management-URL: {{ meta.siem_url }}

Komponenten: - **Log-Collectors:** {{ meta.log_collectors }} - **Indexer:** {{ meta.log_indexers }} - **Search-Heads:** {{ meta.log_search_heads }} - **Storage:** {{ meta.log_storage }}

Kapazität: - **Ingestion-Rate:** {{ meta.log_ingestion_rate }} GB/Tag - **Storage-Kapazität:** {{ meta.log_storage_capacity }} TB - **Retention (Hot):** {{ meta.log_retention_hot }} Tage - **Retention (Cold):** {{ meta.log_retention_cold }} Tage

21.3.4 Log-Quellen-Konfiguration

21.3.4.1 Linux-Server

Rsyslog-Konfiguration:

```
# /etc/rsyslog.d/50-remote.conf
```

```
# Alle Logs an zentralen Syslog-Server senden
```

```
*. * @syslog.{{ meta.organization.domain }}:514
```

```
# Nur Security-Logs senden
```

```
authpriv.* @syslog.{{ meta.organization.domain }}:514
```

```
# TLS-verschlüsselt
$DefaultNetstreamDriver gtls
$ActionSendStreamDriverMode 1
$ActionSendStreamDriverAuthMode x509/name
*. * @@syslog.{{ meta.organization.domain }}:6514
```

21.3.4.2 Windows-Server

Event-Forwarding-Konfiguration:

```
# Event-Forwarding aktivieren
wecutil qc
```

```
# Subscription erstellen
wecutil cs subscription.xml
```

```
# Subscription-XML
<Subscription>
  <SubscriptionId>Security-Events</SubscriptionId>
  <DestinationUrl>http://wec-server.{{ meta.organization.domain }}:5985/wsman</DestinationUrl>
  <Query>
    <QueryList>
      <Query Id="0">
        <Select Path="Security">*[System[(EventID=4624 or EventID=4625)]]</Select>
      </Query>
    </QueryList>
  </Query>
</Subscription>
```

21.3.4.3 Firewall

Syslog-Konfiguration: - Syslog-Server: {{ netbox.syslog.server }} - Facility: Local6 - Severity: Informational und höher - Format: RFC 5424

Geloggte Events: - Alle erlaubten/blockierten Verbindungen - Policy-Änderungen - VPN-Verbindungen - Admin-Zugriffe

21.3.4.4 Web-Server (Apache)

Log-Konfiguration:

```
# /etc/apache2/sites-available/default-ssl.conf
```

```
# Access-Log
CustomLog /var/log/apache2/access.log combined
```

```
# Error-Log
ErrorLog /var/log/apache2/error.log
LogLevel warn
```

```
# Forwarding an Syslog
CustomLog "|/usr/bin/logger -t apache -p local6.info" combined
```

21.3.4.5 Datenbank (MySQL)

Log-Konfiguration:

```
# /etc/mysql/my.cnf

[mysqld]
# General Query Log (nur für Debugging)
general_log = 0
general_log_file = /var/log/mysql/query.log

# Error Log
log_error = /var/log/mysql/error.log

# Slow Query Log
slow_query_log = 1
slow_query_log_file = /var/log/mysql/slow.log
long_query_time = 2

# Audit Plugin (für Compliance)
plugin-load = audit_log.so
audit_log_file = /var/log/mysql/audit.log
audit_log_format = JSON
```

21.4 Log-Retention und -Archivierung

21.4.1 Retention-Policies

21.4.1.1 Retention nach Log-Typ

Log-Typ	Hot Storage	Cold Storage	Gesamt	Begründung
Security-Logs	90 Tage	7 Jahre	7 Jahre	Compliance, Forensik
Audit-Logs	90 Tage	7 Jahre	7 Jahre	Compliance, Regulierung
System-Logs	30 Tage	1 Jahr	1 Jahr	Troubleshooting
Application-Logs	30 Tage	1 Jahr	1 Jahr	Troubleshooting
Network-Logs	30 Tage	1 Jahr	1 Jahr	Security, Troubleshooting
Web-Access-Logs	30 Tage	6 Monate	6 Monate	Analytics, Security
Debug-Logs	7 Tage	-	7 Tage	Entwicklung

21.4.1.2 Retention nach Compliance

DSGVO: - Personenbezogene Daten: Nur so lange wie erforderlich - Zugriffs-Logs: 6 Monate (empfohlen) - Security-Logs: 1-2 Jahre

ISO 27001: - Security-Logs: Mindestens 1 Jahr - Audit-Logs: Mindestens 1 Jahr

Branchenspezifisch: - Finanzsektor: 7-10 Jahre - Gesundheitswesen: 10 Jahre - Telekommunikation: 6 Monate (Vorratsdatenspeicherung)

21.4.2 Storage-Tiers

21.4.2.1 Hot Storage (Schneller Zugriff)

Technologie: SSD, NVMe

Retention: 30-90 Tage

Zugriff: Echtzeit-Suche, Dashboards

Kosten: Hoch

Verwendung: - Aktive Monitoring - Security-Analysen - Troubleshooting

21.4.2.2 Warm Storage (Mittlerer Zugriff)

Technologie: HDD, Object Storage

Retention: 3-12 Monate

Zugriff: Suche (langsamer)

Kosten: Mittel

Verwendung: - Historische Analysen - Compliance-Audits - Forensik

21.4.2.3 Cold Storage (Archiv)

Technologie: Tape, Cloud Glacier, Object Storage

Retention: 1-7 Jahre

Zugriff: Restore erforderlich (Stunden bis Tage)

Kosten: Niedrig

Verwendung: - Langzeit-Archivierung - Compliance-Anforderungen - Rechtliche Aufbewahrung

21.4.3 Archivierungs-Prozess

Automatische Archivierung: 1. Logs älter als Hot-Retention werden komprimiert 2. Komprimierte Logs werden zu Warm/Cold Storage verschoben 3. Metadaten bleiben für Suche verfügbar 4. Originale werden aus Hot Storage gelöscht

Archiv-Format: - Kompression: gzip, bzip2 - Verschlüsselung: AES-256 - Integrität: SHA-256 Checksums - Metadaten: JSON-Index

Archiv-Speicherort: `{{ meta.log_archive_location }}`

21.4.4 Log-Löschung

Automatische Löschung: - Logs älter als Retention-Policy werden automatisch gelöscht - Löschung wird geloggt (Audit-Trail) - Checksums vor Löschung verifizieren

Manuelle Löschung: - Nur mit Management-Genehmigung - Begründung dokumentieren - Löschungs-Protokoll erstellen

DSGVO-Löschung: - Recht auf Vergessenwerden - Personenbezogene Daten löschen - Dokumentation der Löschung

21.5 Log-Analyse und -Monitoring

21.5.1 SIEM-Integration

SIEM-System: {{ meta.siem_system }}

Funktionen: - **Real-time Monitoring:** Echtzeit-Überwachung - **Correlation:** Event-Korrelation - **Alerting:** Automatische Alerts - **Dashboards:** Visualisierung - **Reporting:** Compliance-Reports - **Threat Intelligence:** Integration von Threat-Feeds

21.5.2 Use-Cases und Correlation-Rules

21.5.2.1 Failed Login Attempts

Use-Case: Erkennung von Brute-Force-Angriffen

Regel:

```
IF failed_login_count > 5
  AND time_window = 5 minutes
  AND same_source_ip
THEN alert "Possible Brute-Force Attack"
```

Severity: High

Response: Account temporär sperren, IP blockieren

21.5.2.2 Privilege Escalation

Use-Case: Erkennung von unautorisierten Privilegien-Änderungen

Regel:

```
IF event_type = "privilege_change"
  AND new_privilege = "admin"
  AND user NOT IN admin_group
THEN alert "Unauthorized Privilege Escalation"
```

Severity: Critical

Response: Sofortige Untersuchung, Account deaktivieren

21.5.2.3 Data Exfiltration

Use-Case: Erkennung von ungewöhnlichen Daten-Transfers

Regel:

```
IF data_transfer_size > 1GB
  AND destination = external
```

```
AND time = outside_business_hours
THEN alert "Possible Data Exfiltration"
```

Severity: Critical

Response: Verbindung blockieren, Forensik starten

21.5.2.4 Malware Detection

Use-Case: Erkennung von Malware-Aktivitäten

Regel:

```
IF antivirus_alert = "malware_detected"
  OR process_name IN malware_indicators
  OR network_connection TO known_c2_server
THEN alert "Malware Detected"
```

Severity: Critical

Response: Host isolieren, Incident-Response

21.5.2.5 Configuration Changes

Use-Case: Überwachung von kritischen Konfigurations-Änderungen

Regel:

```
IF event_type = "config_change"
  AND system IN critical_systems
  AND user NOT IN authorized_admins
THEN alert "Unauthorized Configuration Change"
```

Severity: High

Response: Change verifizieren, ggf. rollback

21.5.3 Dashboards

21.5.3.1 Security-Dashboard

Metriken: - Failed Login Attempts (letzte 24h) - Security-Alerts (nach Severity) - Top-10-Angreifer-IPs - Malware-Detections - Firewall-Blocks

Zielgruppe: Security-Operations-Team

21.5.3.2 Operations-Dashboard

Metriken: - System-Errors (nach System) - Application-Errors (nach App) - Performance-Metriken - Disk-Space-Warnungen - Service-Verfügbarkeit

Zielgruppe: IT-Operations-Team

21.5.3.3 Compliance-Dashboard

Metriken: - Audit-Log-Coverage - Retention-Compliance - Access-Reviews - Policy-Violations - Privileged-Access-Monitoring

Zielgruppe: Compliance-Officer, Auditoren

21.5.4 Alerting

Alert-Kanäle: - **E-Mail:** `{{ meta.alert_email }}` - **SMS:** Für kritische Alerts - **Ticketing:** `{{ meta.ticketing_system }}` - **SIEM-Console:** Real-time Alerts - **Slack/Teams:** Team-Benachrichtigungen

Alert-Priorisierung:

Severity	Response-Zeit	Eskalation	Beispiel
Critical	Sofort	Sofort an On-Call	Malware, Data Breach
High	< 1 Stunde	Nach 1h	Failed Logins, Privilege Escalation
Medium	< 4 Stunden	Nach 4h	Config Changes, Policy Violations
Low	< 24 Stunden	Nach 24h	Informational Events

Alert-Tuning: - False-Positive-Reduktion - Threshold-Anpassung - Whitelist für legitime Aktivitäten - Regelmäßige Review (monatlich)

21.6 Audit-Trail-Anforderungen

21.6.1 Audit-Logging-Prinzipien

Was wird geloggt: - **Wer:** User-ID, IP-Adresse, Session-ID - **Was:** Aktion, Ressource, Änderungen - **Wann:** Timestamp (UTC) - **Wo:** System, Applikation, Komponente - **Ergebnis:** Erfolg/Fehler, Fehlercode

Audit-Log-Format:

```
{
  "timestamp": "2024-01-31T10:30:45Z",
  "user": "jdoe",
  "source_ip": "192.168.1.100",
  "action": "file_access",
  "resource": "/data/sensitive/customer_data.csv",
  "result": "success",
  "system": "fileserver01",
  "session_id": "abc123xyz"
}
```

21.6.2 Kritische Audit-Events

21.6.2.1 Authentifizierung und Autorisierung

Events: - Login (erfolgreich/fehlgeschlagen) - Logout - Passwort-Änderung - Account-Erstellung/-Löschung - Privilegien-Änderung - Rollen-Zuweisung

21.6.2.2 Daten-Zugriff

Events: - Zugriff auf sensible Daten - Daten-Export - Daten-Änderung - Daten-Löschung - Datenbank-Queries (bei sensiblen Daten)

21.6.2.3 System-Änderungen

Events: - Konfigurations-Änderungen - Software-Installation/-Deinstallation - Service-Start/-Stop - Firewall-Regel-Änderungen - Netzwerk-Änderungen

21.6.2.4 Administrative Aktivitäten

Events: - Privilegierte Zugriffe - Backup/Restore-Operationen - Security-Policy-Änderungen - Audit-Log-Zugriffe - System-Wartung

21.6.3 Audit-Log-Integrität

Schutzmaßnahmen: - **Write-Once:** Logs können nicht geändert werden - **Digitale Signaturen:** Logs werden signiert - **Checksums:** Integritäts-Prüfung - **Separate Storage:** Logs auf separatem System - **Access-Control:** Nur autorisierte Zugriffe

Verifikation: - Regelmäßige Integritäts-Checks - Checksum-Validierung - Signatur-Verifikation - Anomalie-Erkennung (fehlende Logs)

21.7 Compliance und Regulierung

21.7.1 DSGVO (GDPR)

Anforderungen: - Logging von Zugriff auf personenbezogene Daten - Recht auf Auskunft (welche Daten wurden verarbeitet) - Recht auf Löschung (Logs mit personenbezogenen Daten) - Meldepflicht bei Data Breach (72h)

Umsetzung: - Zugriffs-Logs für alle personenbezogenen Daten - Pseudonymisierung wo möglich - Retention-Policies beachten - Lösch-Prozesse implementiert

21.7.2 ISO 27001

Anforderungen: - A.12.4.1: Event-Logging - A.12.4.2: Schutz von Log-Informationen - A.12.4.3: Administrator- und Operator-Logs - A.12.4.4: Zeitsynchronisation

Umsetzung: - Umfassendes Event-Logging - Log-Integrität sichergestellt - Privilegierte Zugriffe geloggt - NTP-Synchronisation

21.7.3 PCI-DSS (falls zutreffend)

Anforderungen: - Requirement 10: Track and monitor all access to network resources and cardholder data - Audit-Trails für alle Zugriffe - Tägliche Log-Reviews - Retention: Mindestens 1 Jahr (3 Monate online)

21.7.4 SOX (falls zutreffend)

Anforderungen: - Audit-Trails für finanzrelevante Systeme - Änderungs-Nachvollziehbarkeit - Access-Controls geloggt - Retention: 7 Jahre

21.8 Log-Management-Tools

21.8.1 SIEM-Plattform

System: {{ meta.siem_system }}

Komponenten: - Indexer - Search-Heads - Forwarders - Deployment-Server

21.8.2 Log-Collectors

Rsyslog: - Zentrale Syslog-Server - Filtering und Parsing - Forwarding an SIEM

Fluentd/Fluent Bit: - Lightweight Log-Collector - Plugin-basiert - Kubernetes-Integration

Elastic Beats: - Filebeat: Log-Files - Metricbeat: System-Metriken - Packetbeat: Network-Traffic
- Auditbeat: Audit-Daten

21.8.3 Log-Analysis-Tools

Kibana: - Visualisierung - Dashboards - Ad-hoc-Queries

Grafana: - Metriken-Visualisierung - Alerting - Multi-Source-Integration

21.9 Rollen und Verantwortlichkeiten

21.9.1 Log-Management-Team

Verantwortlichkeiten: - Log-Infrastruktur-Verwaltung - Log-Sammlung-Konfiguration - Retention-Policy-Umsetzung - Tool-Administration

Team-Lead: Andreas Huemmer

21.9.2 Security-Operations-Team

Verantwortlichkeiten: - SIEM-Monitoring - Alert-Response - Use-Case-Entwicklung - Threat-Hunting

Team-Lead: Thomas Weber

21.9.3 Compliance-Officer

Verantwortlichkeiten: - Compliance-Anforderungen definieren - Audit-Unterstützung - Retention-Policy-Review - Regulierungs-Überwachung

Person: {{ meta.compliance_officer }}

21.10 Metriken und Reporting

21.10.1 Log-Management-Metriken

Metrik	Zielwert	Messung
Log-Collection-Rate	> 99%	Gesammelte Logs / Erwartete Logs
Log-Ingestion-Latency	< 5 Min	Zeit von Event bis SIEM
Storage-Utilization	< 80%	Verwendeter Storage / Gesamt-Storage
Alert-Response-Time	< 15 Min	Zeit von Alert bis Response
False-Positive-Rate	< 10%	False Positives / Gesamt-Alerts

21.10.2 Reporting

Tägliches Log-Status-Report: - Log-Collection-Status - Fehlende Log-Quellen - Storage-Auslastung - Kritische Alerts

Wöchentliches Security-Report: - Security-Events-Zusammenfassung - Top-Alerts - Trend-Analysen - Anomalien

Monatliches Compliance-Report: - Audit-Log-Coverage - Retention-Compliance - Access-Reviews - Policy-Violations

Quartalsweises Management-Report: - Log-Management-Strategie-Review - Kapazitäts-Planung - Compliance-Status - Verbesserungs-Maßnahmen

21.11 Referenzen

- ISO/IEC 27001:2013 - A.12.4 (Logging and Monitoring)
- NIST SP 800-92 - Guide to Computer Security Log Management
- PCI-DSS v4.0 - Requirement 10
- DSGVO - Artikel 30 (Verzeichnis von Verarbeitungstätigkeiten)
- CIS Controls v8 - Control 8 (Audit Log Management)
- ITIL v4 - Monitoring and Event Management

Dokumentverantwortlicher: IT Operations Manager

Genehmigt durch: CIO

Version: 1.0.0

Klassifizierung: internal

Letzte Aktualisierung: {{ meta.date }}

ewpage

Chapter 22

Kapazitäts- und Performance Management

22.1 Übersicht

Dieses Dokument beschreibt die Prozesse und Methoden für das Kapazitäts- und Performance Management des IT-Service. Ziel ist es, sicherzustellen, dass ausreichende IT-Ressourcen zur Verfügung stehen, um die aktuellen und zukünftigen Geschäftsanforderungen zu erfüllen.

Dokumentverantwortlicher: IT Operations Manager

Genehmigt durch: CIO

Version: 1.0.0

Organisation: AdminSend GmbH

22.2 Kapazitätsplanung

22.2.1 Planungszyklus

Phase	Zeitraum	Verantwortlich	Aktivitäten
Kurzfristig	1-3 Monate	Andreas Huemmer	Monitoring, Anpassungen
Mittelfristig	3-12 Monate	Anna Schmidt	Kapazitätsprognosen, Budgetplanung
Langfristig	1-3 Jahre	Max Mustermann	Strategische Planung, Investitionen

22.2.2 Kapazitätsdimensionen

22.2.2.1 Compute-Ressourcen

- **CPU-Kapazität:** `{{ netbox.cluster.total_cpu_cores }}` Cores
- **RAM-Kapazität:** `{{ netbox.cluster.total_memory_gb }}` GB

- **Auslastungsziel:** 70% (Durchschnitt), 85% (Peak)
- **Skalierungsschwelle:** 80% über 7 Tage

22.2.2.2 Storage-Ressourcen

- **Gesamtkapazität:** `{{ netbox.storage.total_capacity_tb }}` TB
- **Verfügbare Kapazität:** `{{ netbox.storage.available_capacity_tb }}` TB
- **Auslastungsziel:** 75% (Durchschnitt), 85% (Maximum)
- **Skalierungsschwelle:** 80% Auslastung

22.2.2.3 Netzwerk-Ressourcen

- **Bandbreite WAN:** `{{ netbox.circuit.bandwidth_mbps }}` Mbps
- **Bandbreite LAN:** `{{ netbox.network.lan_bandwidth_gbps }}` Gbps
- **Auslastungsziel:** 60% (Durchschnitt), 80% (Peak)
- **Skalierungsschwelle:** 75% über 5 Tage

22.2.3 Kapazitätsmodellierung

22.2.3.1 Wachstumsprognosen

Ressource	Aktuell	+6 Monate	+12 Monate	+24 Monate
CPU (Cores)	[TODO]	[TODO]	[TODO]	[TODO]
RAM (GB)	[TODO]	[TODO]	[TODO]	[TODO]
Storage (TB)	[TODO]	[TODO]	[TODO]	[TODO]
Netzwerk (Gbps)	[TODO]	[TODO]	[TODO]	[TODO]
Benutzer	[TODO]	[TODO]	[TODO]	[TODO]

22.2.3.2 Einflussfaktoren

- Geschäftswachstum und neue Projekte
- Saisonale Schwankungen
- Technologische Änderungen
- Regulatorische Anforderungen
- Merger & Acquisitions

22.3 Performance-Monitoring

22.3.1 Performance-Metriken

22.3.1.1 System-Performance

Metrik	Zielwert	Warnschwelle	Kritisch	Messintervall
CPU-Auslastung	< 70%	> 80%	> 90%	1 Minute
RAM-Auslastung	< 75%	> 85%	> 95%	1 Minute
Disk I/O Latenz	< 10ms	> 20ms	> 50ms	1 Minute

Metrik	Zielwert	Warnschwelle	Kritisch	Messintervall
Disk I/O Throughput	> 100 MB/s	< 50 MB/s	< 20 MB/s	1 Minute
Netzwerk-Latenz	< 5ms	> 10ms	> 20ms	30 Sekunden
Netzwerk-Paketverlust	< 0.1%	> 0.5%	> 1%	1 Minute

22.3.1.2 Anwendungs-Performance

Metrik	Zielwert	Warnschwelle	Kritisch	Messintervall
Response Time	< 200ms	> 500ms	> 1000ms	1 Minute
Throughput (TPS)	> 1000	< 500	< 100	1 Minute
Error Rate	< 0.1%	> 1%	> 5%	1 Minute
Concurrent Users	[TODO]	[TODO]	[TODO]	5 Minuten
Queue Length	< 10	> 50	> 100	1 Minute

22.3.1.3 Datenbank-Performance

Metrik	Zielwert	Warnschwelle	Kritisch	Messintervall
Query Response Time	< 100ms	> 500ms	> 2000ms	1 Minute
Connection Pool Usage	< 70%	> 85%	> 95%	1 Minute
Lock Wait Time	< 10ms	> 100ms	> 500ms	1 Minute
Deadlocks	0	> 1/h	> 5/h	5 Minuten
Cache Hit Ratio	> 95%	< 90%	< 80%	5 Minuten

22.3.2 Monitoring-Tools

Tool	Zweck	Zugriff	Verantwortlich
[TODO: Monitoring-Tool]	System-Monitoring	[TODO: URL]	Andreas Huemmer
[TODO: APM-Tool]	Application Performance	[TODO: URL]	Andreas Huemmer
[TODO: DB-Monitoring]	Datenbank-Performance	[TODO: URL]	Andreas Huemmer
[TODO: Network-Tool]	Netzwerk-Monitoring	[TODO: URL]	Andreas Huemmer

22.3.3 Performance-Dashboards

22.3.3.1 Übersichts-Dashboard

- Gesamtsystem-Health-Status
- Kritische Performance-Metriken
- Aktuelle Incidents und Alerts
- Kapazitätsauslastung

22.3.3.2 Detail-Dashboards

- **Compute:** CPU, RAM, Prozesse
 - **Storage:** Disk-Auslastung, I/O-Performance
 - **Netzwerk:** Bandbreite, Latenz, Paketverlust
 - **Anwendung:** Response Times, Throughput, Errors
 - **Datenbank:** Query-Performance, Connections, Locks
-

22.4 Trend-Analysen

22.4.1 Analyse-Prozess

22.4.1.1 Wöchentliche Analyse

- **Durchführung:** Jeden Montag
- **Verantwortlich:** IT Operations Team
- **Fokus:** Kurzfristige Trends und Anomalien
- **Output:** Wochenbericht mit Handlungsempfehlungen

22.4.1.2 Monatliche Analyse

- **Durchführung:** Erster Arbeitstag des Monats
- **Verantwortlich:** Andreas Huemmer
- **Fokus:** Mittelfristige Trends und Kapazitätsprognosen
- **Output:** Monatsbericht mit Kapazitätsempfehlungen

22.4.1.3 Quartalsweise Analyse

- **Durchführung:** Quartalsende
- **Verantwortlich:** Anna Schmidt
- **Fokus:** Strategische Trends und Investitionsplanung
- **Output:** Quartalsbericht mit Budget-Empfehlungen

22.4.2 Trend-Metriken

22.4.2.1 Wachstumstrends

Metrik	Aktuell	Trend (30d)	Trend (90d)	Prognose (12m)
CPU-Auslastung	[TODO]%	[TODO]	[TODO]	[TODO]
RAM-Auslastung	[TODO]%	[TODO]	[TODO]	[TODO]
Storage-Auslastung	[TODO]%	[TODO]	[TODO]	[TODO]
Netzwerk-Traffic	[TODO] GB/d	[TODO]	[TODO]	[TODO]
Benutzeranzahl	[TODO]	[TODO]	[TODO]	[TODO]
Transaktionen/Tag	[TODO]	[TODO]	[TODO]	[TODO]

22.4.2.2 Performance-Trends

Metrik	Aktuell	Trend (30d)	Ziel	Status
Avg. Response Time	[TODO]ms	[TODO]	< 200ms	/ /
95th Percentile RT	[TODO]ms	[TODO]	< 500ms	/ /
Error Rate	[TODO]%	[TODO]	< 0.1%	/ /
Availability	[TODO]%	[TODO]	> 99.5%	/ /

22.4.3 Anomalie-Erkennung

22.4.3.1 Erkennungsmethoden

- **Statistische Analyse:** Standardabweichungen, Ausreißer
- **Machine Learning:** Anomalie-Detection-Algorithmen
- **Baseline-Vergleich:** Abweichungen von historischen Baselines
- **Schwellwert-Überwachung:** Überschreitung definierter Limits

22.4.3.2 Anomalie-Behandlung

1. **Erkennung:** Automatische Alerts bei Anomalien
 2. **Analyse:** Ursachenforschung durch Operations-Team
 3. **Bewertung:** Impact-Assessment und Priorisierung
 4. **Maßnahmen:** Korrekturmaßnahmen oder Eskalation
 5. **Dokumentation:** Lessons Learned und Prozessverbesserung
-

22.5 Skalierungsstrategien

22.5.1 Vertikale Skalierung (Scale-Up)

22.5.1.1 Anwendungsfälle

- Datenbank-Server mit hohen I/O-Anforderungen
- Monolithische Anwendungen
- Legacy-Systeme ohne Cluster-Unterstützung

22.5.1.2 Vorteile

- Einfache Implementierung
- Keine Anwendungsänderungen erforderlich
- Geringere Komplexität

22.5.1.3 Nachteile

- Hardware-Limits
- Single Point of Failure
- Höhere Kosten pro Einheit

22.5.1.4 Implementierung

1. Performance-Analyse und Bottleneck-Identifikation

2. Hardware-Upgrade-Planung
3. Wartungsfenster-Koordination
4. Upgrade-Durchführung
5. Performance-Validierung

22.5.2 Horizontale Skalierung (Scale-Out)

22.5.2.1 Anwendungsfälle

- Zustandslose Web-Anwendungen
- Microservices-Architekturen
- Container-basierte Workloads

22.5.2.2 Vorteile

- Nahezu unbegrenzte Skalierbarkeit
- Höhere Verfügbarkeit durch Redundanz
- Kosteneffizienz durch Commodity-Hardware

22.5.2.3 Nachteile

- Höhere Komplexität
- Anwendungsänderungen erforderlich
- Load-Balancing und State-Management

22.5.2.4 Implementierung

1. Anwendungs-Architektur-Review
2. Load-Balancer-Konfiguration
3. Auto-Scaling-Regeln definieren
4. Deployment-Automatisierung
5. Monitoring und Optimierung

22.5.3 Auto-Scaling

22.5.3.1 Trigger-Bedingungen

Metrik	Scale-Up	Scale-Down	Cool-Down
CPU-Auslastung	> 75% (5 Min)	< 30% (15 Min)	5 Minuten
RAM-Auslastung	> 80% (5 Min)	< 40% (15 Min)	5 Minuten
Request Queue	> 50 (3 Min)	< 10 (10 Min)	3 Minuten
Response Time	> 500ms (5 Min)	< 200ms (15 Min)	5 Minuten

22.5.3.2 Skalierungsgrenzen

- **Minimum Instances:** [TODO]
- **Maximum Instances:** [TODO]
- **Scale-Up Increment:** [TODO] Instanzen
- **Scale-Down Increment:** [TODO] Instanz

22.5.4 Cloud-Skalierung

22.5.4.1 Cloud-Provider

- **Provider:** `{{ meta.organization.cloud_provider }}`
- **Region:** `{{ meta.organization.cloud_region }}`
- **Verfügbarkeitszonen:** `[TODO]`

22.5.4.2 Skalierungsoptionen

- **Compute:** EC2 Auto Scaling Groups / Azure VM Scale Sets
- **Container:** ECS/EKS / AKS / GKE
- **Serverless:** Lambda / Azure Functions
- **Datenbank:** RDS Read Replicas / Cosmos DB Auto-Scale

22.6 Kapazitätsoptimierung

22.6.1 Optimierungsmaßnahmen

22.6.1.1 Ressourcen-Konsolidierung

- Virtualisierung und Containerisierung
- Server-Konsolidierung
- Storage-Tiering und Deduplizierung
- Netzwerk-Optimierung

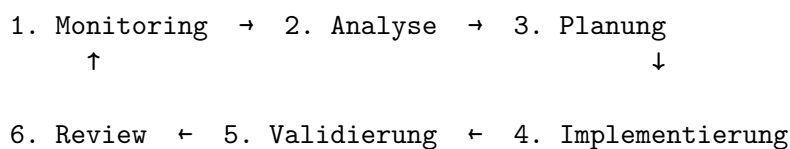
22.6.1.2 Performance-Tuning

- Anwendungs-Optimierung
- Datenbank-Tuning (Indizes, Queries)
- Caching-Strategien
- Content Delivery Networks (CDN)

22.6.1.3 Kostenoptimierung

- Reserved Instances / Savings Plans
- Spot Instances für nicht-kritische Workloads
- Rightsizing von Ressourcen
- Lifecycle-Policies für Storage

22.6.2 Optimierungs-Zyklus



22.7 Reporting

22.7.1 Performance-Reports

22.7.1.1 Wöchentlicher Performance-Report

- **Empfänger:** IT Operations Team
- **Inhalt:**
 - Performance-Metriken der Woche
 - Incidents und Ausfälle
 - Trend-Analyse
 - Handlungsempfehlungen

22.7.1.2 Monatlicher Kapazitäts-Report

- **Empfänger:** Anna Schmidt, Andreas Huemmer
- **Inhalt:**
 - Kapazitätsauslastung
 - Wachstumstrends
 - Skalierungsempfehlungen
 - Budget-Implikationen

22.7.1.3 Quartalsweiser Management-Report

- **Empfänger:** Max Mustermann, Anna Schmidt, Maria Müller
- **Inhalt:**
 - Strategische Kapazitätsplanung
 - Investitionsempfehlungen
 - ROI-Analysen
 - Risikobewertung

22.7.2 Report-Vorlagen

22.7.2.1 Performance-KPIs

KPI	Ziel	Aktuell	Trend	Status	
System Availability	> 99.5%	[TODO]%	[TODO]	/	/
Avg. Response Time	< 200ms	[TODO]ms	[TODO]	/	/
CPU-Auslastung	< 70%	[TODO]%	[TODO]	/	/
Storage-Auslastung	< 75%	[TODO]%	[TODO]	/	/

22.8 Prozesse und Verantwortlichkeiten

22.8.1 RACI-Matrix

Aktivität	CIO	Ops Manager	Ops Team	Finance
Kapazitätsplanung	A	R	C	I
Performance-Monitoring	I	A	R	-
Trend-Analyse	C	A	R	-
Skalierungsentscheidungen	A	R	C	C
Budget-Planung	A	C	I	R
Optimierungsmaßnahmen	C	A	R	-
Reporting	I	R	C	I

Legende: R = Responsible, A = Accountable, C = Consulted, I = Informed

22.8.2 Eskalationspfad

1. **Level 1:** Operations Team - Tägliches Monitoring und Optimierung
 2. **Level 2:** Andreas Huemmer - Kapazitätsentscheidungen
 3. **Level 3:** Anna Schmidt - Strategische Planung und Budget
 4. **Level 4:** Max Mustermann - Investitionsentscheidungen
-

22.9 Tools und Systeme

22.9.1 Monitoring-Tools

- **System-Monitoring:** [TODO: Tool-Name und URL]
- **Application Performance Monitoring:** [TODO: Tool-Name und URL]
- **Database Monitoring:** [TODO: Tool-Name und URL]
- **Network Monitoring:** [TODO: Tool-Name und URL]

22.9.2 Analyse-Tools

- **Capacity Planning:** [TODO: Tool-Name]
- **Trend Analysis:** [TODO: Tool-Name]
- **Reporting:** [TODO: Tool-Name]

22.9.3 Automatisierung

- **Auto-Scaling:** [TODO: Tool/Plattform]
 - **Alerting:** [TODO: Tool-Name]
 - **Orchestration:** [TODO: Tool-Name]
-

22.10 Compliance und Standards

22.10.1 Relevante Standards

- **ITIL v4:** Capacity and Performance Management Practice
- **ISO 20000:** Clause 8.7 - Capacity Management
- **COBIT 2019:** APO03 - Managed Architecture, BAI04 - Managed Availability and Capacity

22.10.2 Audit-Anforderungen

- Dokumentation der Kapazitätsplanung
 - Performance-Metriken und Trends
 - Skalierungsentscheidungen und Begründungen
 - Budget-Nachweise
-

22.11 Anhang

22.11.1 Glossar

Begriff	Definition
Capacity Planning	Prozess zur Sicherstellung ausreichender IT-Ressourcen
Performance Management	Überwachung und Optimierung der System-Performance
Vertical Scaling	Erhöhung der Ressourcen eines einzelnen Systems
Horizontal Scaling	Hinzufügen weiterer Systeme zur Lastverteilung
Auto-Scaling	Automatische Anpassung der Ressourcen basierend auf Last
Rightsizing	Optimierung der Ressourcengröße für Workloads

22.11.2 Referenzen

- ITIL v4 Foundation Handbook
 - ISO/IEC 20000-1:2018
 - COBIT 2019 Framework
 - Cloud Provider Best Practices
-

Letzte Aktualisierung: {{ meta.date }}

Nächste Review: [TODO: Datum]

Kontakt: andreas.huemmer@adminsends.de

ewpage

Chapter 23

Verfügbarkeit und Service Level

23.1 Übersicht

Dieses Dokument definiert die Verfügbarkeitsanforderungen, Service Level Agreements (SLAs) und Service Level Objectives (SLOs) für den IT-Service. Es beschreibt die Messmethoden, Reporting-Prozesse und Maßnahmen zur kontinuierlichen Verbesserung der Serviceverfügbarkeit.

Dokumentverantwortlicher: IT Operations Manager

Genehmigt durch: CIO

Version: 1.0.0

Organisation: AdminSend GmbH

23.2 Verfügbarkeitsanforderungen

23.2.1 Service-Klassifizierung

Service-Klasse	Verfügbarkeit	Max. Ausfallzeit/Jahr	Max. Ausfallzeit/Monat	Geschäftskritikalität
Kritisch	99.95%	4.38 Stunden	21.6 Minuten	Hoch
Wichtig	99.5%	43.8 Stunden	3.6 Stunden	Mittel
Standard	99.0%	87.6 Stunden	7.2 Stunden	Niedrig
Unkritisch	95.0%	438 Stunden	36 Stunden	Sehr niedrig

23.2.2 Service-Zeiten

23.2.2.1 Produktions-Services

- **Verfügbarkeit:** 24/7/365
- **Support-Zeiten:** 24/7 mit On-Call-Bereitschaft
- **Wartungsfenster:** Sonntag 02:00-06:00 Uhr (nach Ankündigung)
- **Notfall-Wartung:** Nach Genehmigung durch Anna Schmidt

23.2.2.2 Business-Services

- **Verfügbarkeit:** Mo-Fr 06:00-22:00 Uhr
- **Support-Zeiten:** Mo-Fr 08:00-18:00 Uhr
- **Wartungsfenster:** Samstag 20:00-24:00 Uhr
- **Notfall-Wartung:** Nach Genehmigung durch Andreas Huemmer

23.2.2.3 Entwicklungs-/Test-Services

- **Verfügbarkeit:** Mo-Fr 08:00-18:00 Uhr
- **Support-Zeiten:** Best Effort
- **Wartungsfenster:** Jederzeit nach Ankündigung
- **Notfall-Wartung:** Nicht erforderlich

23.2.3 Geplante Wartungsfenster

Wartungstyp	Frequenz	Dauer	Ankündigungsfrist	Genehmigung
Routine-Wartung	Monatlich	2-4 Stunden	7 Tage	Ops Manager
Patch-Deployment	Monatlich	1-2 Stunden	5 Tage	Ops Manager
Major-Upgrade	Quartalsweise	4-8 Stunden	14 Tage	CIO
Notfall-Wartung	Ad-hoc	Variable	4 Stunden	CIO

23.3 Service Level Agreements (SLA)

23.3.1 SLA-Definitionen

23.3.1.1 Verfügbarkeits-SLA

Service: [TODO: Service-Name]

Gültig ab: [TODO: Datum]

Laufzeit: 12 Monate mit automatischer Verlängerung

Metrik	Zielwert	Messmethode	Messintervall
Verfügbarkeit	99.5%	Uptime-Monitoring	Monatlich
Geplante Ausfallzeit	< 4h/Monat	Change-Kalender	Monatlich
Ungeplante Ausfallzeit	< 2h/Monat	Incident-Tracking	Monatlich
MTBF (Mean Time Between Failures)	> 720h	Incident-Analyse	Quartalsweise
MTTR (Mean Time To Repair)	< 2h	Incident-Tickets	Monatlich

23.3.1.2 Performance-SLA

Metrik	Zielwert	Warnschwelle	Messmethode	Messintervall
Response Time (Avg)	< 200ms	> 300ms	APM-Tool	Kontinuierlich
Response Time (95th)	< 500ms	> 750ms	APM-Tool	Kontinuierlich
Response Time (99th)	< 1000ms	> 1500ms	APM-Tool	Kontinuierlich
Throughput	> 1000 TPS	< 800 TPS	APM-Tool	Kontinuierlich
Error Rate	< 0.1%	> 0.5%	APM-Tool	Kontinuierlich

23.3.1.3 Support-SLA

Priorität	Reaktionszeit	Lösungszeit	Verfügbarkeit	Eskalation
P1 - Kritisch	15 Minuten	4 Stunden	24/7	Sofort an CIO
P2 - Hoch	1 Stunde	8 Stunden	24/7	Nach 4h an Ops Manager
P3 - Mittel	4 Stunden	24 Stunden	Mo-Fr 08-18	Nach 24h an Ops Manager
P4 - Niedrig	8 Stunden	72 Stunden	Mo-Fr 08-18	Nach 72h an Ops Manager

23.3.2 SLA-Vertragspartner

23.3.2.1 Interne SLAs

- **Service Provider:** IT Operations (Andreas Huemmer)
- **Service Consumer:** Fachabteilungen
- **Verantwortlich:** Anna Schmidt
- **Review-Zyklus:** Quartalsweise

23.3.2.2 Externe SLAs

- **Service Provider:** AdminSend GmbH
- **Service Consumer:** [TODO: Kunde/Partner]
- **Vertragslaufzeit:** [TODO: Laufzeit]
- **Vertragsstrafen:** [TODO: Penalties bei SLA-Verletzung]

23.3.3 SLA-Ausnahmen

23.3.3.1 Ausschlusskriterien (Force Majeure)

- Naturkatastrophen
- Terroranschläge
- Kriege und Unruhen
- Pandemien
- Stromausfälle außerhalb der Kontrolle

23.3.3.2 Geplante Ausnahmen

- Angekündigte Wartungsfenster
- Genehmigte Notfall-Wartungen
- Vom Kunden verursachte Ausfälle
- Drittanbieter-Ausfälle außerhalb der Kontrolle

23.4 Service Level Objectives (SLO)

23.4.1 Interne SLOs

23.4.1.1 Infrastruktur-SLOs

Komponente	SLO	Messmethode	Verantwortlich
Compute-Cluster	99.9%	Hypervisor-Monitoring	Andreas Huemmer
Storage-System	99.95%	Storage-Monitoring	Andreas Huemmer
Netzwerk-Core	99.99%	Network-Monitoring	Andreas Huemmer
Firewall	99.95%	Security-Monitoring	Thomas Weber
Load Balancer	99.9%	LB-Monitoring	Andreas Huemmer

23.4.1.2 Anwendungs-SLOs

Anwendung	Verfügbarkeit	Response Time	Error Rate	Verantwortlich
[TODO: App 1]	99.5%	< 200ms	< 0.1%	[TODO]
[TODO: App 2]	99.0%	< 500ms	< 0.5%	[TODO]
[TODO: App 3]	99.9%	< 100ms	< 0.05%	[TODO]

23.4.1.3 Datenbank-SLOs

Datenbank	Verfügbarkeit	Query Time	Connection Time	Verantwortlich
[TODO: DB 1]	99.95%	< 50ms	< 10ms	[TODO]
[TODO: DB 2]	99.5%	< 100ms	< 20ms	[TODO]

23.4.2 Error Budget

23.4.2.1 Error Budget Konzept

- **Definition:** Tolerierbare Ausfallzeit innerhalb des SLO-Zeitraums
- **Berechnung:** $(100\% - \text{SLO}) \times \text{Zeitraum}$
- **Verwendung:** Balance zwischen Innovation und Stabilität

23.4.2.2 Error Budget Beispiel (99.5% SLO)

Zeitraum	Verfügbarkeit	Error Budget	Ausfallzeit
Monat	99.5%	0.5%	3.6 Stunden
Quartal	99.5%	0.5%	10.8 Stunden
Jahr	99.5%	0.5%	43.8 Stunden

23.4.2.3 Error Budget Policy

Wenn Error Budget > 50% verbleibend: - Normale Entwicklungsgeschwindigkeit - Neue Features und Experimente erlaubt - Routine-Wartungen wie geplant

Wenn Error Budget 25-50% verbleibend: - Erhöhte Vorsicht bei Changes - Fokus auf Stabilität - Zusätzliche Testing-Anforderungen

Wenn Error Budget < 25% verbleibend: - Feature-Freeze - Nur kritische Bugfixes - Fokus auf Reliability-Verbesserungen - Postmortem für alle Incidents

Wenn Error Budget aufgebraucht: - Vollständiger Change-Freeze - Nur Notfall-Fixes - Root-Cause-Analyse aller Ausfälle - Verbesserungsplan vor Wiederaufnahme

23.5 Verfügbarkeitsmessung

23.5.1 Messmethoden

23.5.1.1 Synthetische Monitoring

- **Methode:** Automatisierte Tests von definierten Endpunkten
- **Frequenz:** Alle 1-5 Minuten
- **Standorte:** Mehrere geografische Locations
- **Metriken:** Verfügbarkeit, Response Time, Funktionalität

23.5.1.2 Real User Monitoring (RUM)

- **Methode:** Messung echter Benutzer-Interaktionen
- **Erfassung:** Client-seitige Metriken
- **Metriken:** Page Load Time, User Experience, Fehlerrate
- **Datenschutz:** DSGVO-konform, anonymisiert

23.5.1.3 Server-seitiges Monitoring

- **Methode:** Überwachung von Server-Metriken
- **Erfassung:** Logs, Metriken, Traces
- **Metriken:** Uptime, Resource Usage, Error Logs
- **Aggregation:** Zentrales Monitoring-System

23.5.2 Verfügbarkeitsberechnung

23.5.2.1 Formel

Verfügbarkeit (%) = (Gesamtzeit - Ausfallzeit) / Gesamtzeit × 100

23.5.2.2 Beispielberechnung (Monat mit 720 Stunden)

Gesamtzeit: 720 Stunden

Geplante Wartung: 2 Stunden (ausgeschlossen)

Ungeplante Ausfälle: 1.5 Stunden

Verfügbare Zeit: 720 - 2 = 718 Stunden

Tatsächliche Verfügbarkeit: (718 - 1.5) / 718 × 100 = 99.79%

23.5.2.3 Ausschlüsse

- Geplante und angekündigte Wartungsfenster
- Vom Kunden verursachte Ausfälle
- Force Majeure Ereignisse
- Drittanbieter-Ausfälle (nach Vereinbarung)

23.5.3 Monitoring-Tools

Tool	Zweck	Messintervall	Zugriff
[TODO: Uptime-Tool]	Verfügbarkeitsmonitoring	1 Minute	[TODO: URL]
[TODO: APM-Tool]	Performance-Monitoring	Kontinuierlich	[TODO: URL]
[TODO: RUM-Tool]	Real User Monitoring	Kontinuierlich	[TODO: URL]
[TODO: Log-Tool]	Log-Aggregation	Echtzeit	[TODO: URL]

23.6 Service-Level-Reporting

23.6.1 Report-Typen

23.6.1.1 Täglicher Verfügbarkeits-Report

- **Empfänger:** IT Operations Team
- **Inhalt:**
 - Verfügbarkeit der letzten 24 Stunden
 - Incidents und Ausfälle
 - Performance-Metriken
 - Aktuelle Alerts
- **Versand:** Automatisch um 08:00 Uhr

23.6.1.2 Wöchentlicher SLA-Report

- **Empfänger:** Andreas Huemmer
- **Inhalt:**

- Wochenverfügbarkeit
- SLA-Compliance-Status
- Trend-Analyse
- Handlungsempfehlungen
- **Versand:** Jeden Montag

23.6.1.3 Monatlicher SLA-Report

- **Empfänger:** Anna Schmidt, Stakeholder
- **Inhalt:**
 - Monatsverfügbarkeit
 - SLA-Erfüllung vs. Ziele
 - Incident-Zusammenfassung
 - Error Budget Status
 - Verbesserungsmaßnahmen
- **Versand:** Erster Arbeitstag des Folgemonats

23.6.1.4 Quartalsweiser Management-Report

- **Empfänger:** Max Mustermann, Anna Schmidt, Maria Müller
- **Inhalt:**
 - Quartalsverfügbarkeit
 - SLA-Trends
 - Kosten-Nutzen-Analyse
 - Strategische Empfehlungen
- **Versand:** Quartalsende + 5 Arbeitstage

23.6.2 Report-Metriken

23.6.2.1 Verfügbarkeits-Dashboard

Metrik	Ziel	Aktuell (Monat)	Trend	Status
Gesamtverfügbarkeit	99.5%	[TODO]%	[TODO]	/ /
Ungeplante Ausfälle	< 2h	[TODO]h	[TODO]	/ /
MTBF	> 720h	[TODO]h	[TODO]	/ /
MTTR	< 2h	[TODO]h	[TODO]	/ /
Error Budget verbleibend	> 0%	[TODO]%	[TODO]	/ /

23.6.2.2 Incident-Statistiken

Priorität	Anzahl	Avg. MTTR	SLA-Erfüllung	Trend
P1 - Kritisch	[TODO]	[TODO]h	[TODO]%	[TODO]
P2 - Hoch	[TODO]	[TODO]h	[TODO]%	[TODO]
P3 - Mittel	[TODO]	[TODO]h	[TODO]%	[TODO]
P4 - Niedrig	[TODO]	[TODO]h	[TODO]%	[TODO]

23.7 Verfügbarkeitsverbesserungen

23.7.1 Verbesserungsmaßnahmen

23.7.1.1 Redundanz und Hochverfügbarkeit

- **Aktiv-Aktiv-Cluster:** Lastverteilung über mehrere Knoten
- **Aktiv-Passiv-Cluster:** Failover-Konfiguration
- **Geografische Redundanz:** Multi-Region-Deployment
- **Datenbank-Replikation:** Synchrone/Asynchrone Replikation
- **Load Balancing:** Verteilung der Last auf mehrere Instanzen

23.7.1.2 Automatisierung

- **Auto-Healing:** Automatische Wiederherstellung bei Fehlern
- **Auto-Scaling:** Automatische Kapazitätsanpassung
- **Automated Failover:** Automatischer Failover bei Ausfall
- **Health Checks:** Kontinuierliche Gesundheitsprüfungen
- **Self-Service:** Automatisierte Bereitstellung

23.7.1.3 Monitoring und Alerting

- **Proaktives Monitoring:** Früherkennung von Problemen
- **Predictive Analytics:** Vorhersage von Ausfällen
- **Intelligent Alerting:** Reduzierung von False Positives
- **Anomalie-Erkennung:** ML-basierte Anomalie-Erkennung
- **Distributed Tracing:** End-to-End-Nachverfolgung

23.7.1.4 Prozessverbesserungen

- **Incident Management:** Optimierung der Incident-Prozesse
- **Change Management:** Reduzierung von Change-bedingten Ausfällen
- **Capacity Management:** Proaktive Kapazitätsplanung
- **Disaster Recovery:** Verbesserung der DR-Prozesse
- **Continuous Improvement:** Regelmäßige Retrospektiven

23.7.2 Verbesserungs-Roadmap

Quartal	Maßnahme	Erwarteter Impact	Verantwortlich	Status
Q1 2026	[TODO]	+0.1% Verfügbarkeit	[TODO]	Geplant
Q2 2026	[TODO]	-30min MTTR	[TODO]	Geplant
Q3 2026	[TODO]	+0.2% Verfügbarkeit	[TODO]	Geplant
Q4 2026	[TODO]	-50% Incidents	[TODO]	Geplant

23.7.3 Lessons Learned

23.7.3.1 Postmortem-Prozess

1. **Incident-Dokumentation:** Detaillierte Beschreibung des Vorfalls
2. **Timeline-Erstellung:** Chronologischer Ablauf

3. **Root-Cause-Analysis:** 5-Why-Methode
4. **Impact-Assessment:** Betroffene Systeme und Benutzer
5. **Corrective Actions:** Sofortmaßnahmen und langfristige Verbesserungen
6. **Follow-Up:** Überprüfung der Umsetzung

23.7.3.2 Postmortem-Template

- **Incident-ID:** [TODO]
 - **Datum/Zeit:** [TODO]
 - **Dauer:** [TODO]
 - **Betroffene Services:** [TODO]
 - **Root Cause:** [TODO]
 - **Maßnahmen:** [TODO]
 - **Verantwortlich:** [TODO]
 - **Status:** [TODO]
-

23.8 SLA-Review und Anpassung

23.8.1 Review-Prozess

23.8.1.1 Quartalsweiser SLA-Review

- **Teilnehmer:** Anna Schmidt, Andreas Huemmer, Stakeholder
- **Agenda:**
 - SLA-Erfüllung der letzten 3 Monate
 - Trend-Analyse
 - Verbesserungspotenziale
 - Anpassungsbedarf
- **Output:** Review-Protokoll mit Handlungsempfehlungen

23.8.1.2 Jährlicher SLA-Review

- **Teilnehmer:** Max Mustermann, Anna Schmidt, Maria Müller, Stakeholder
- **Agenda:**
 - Jahresverfügbarkeit
 - SLA-Angemessenheit
 - Kosten-Nutzen-Analyse
 - Strategische Ausrichtung
- **Output:** SLA-Anpassungen für das Folgejahr

23.8.2 Anpassungskriterien

23.8.2.1 SLA-Verschärfung (höhere Anforderungen)

- Geschäftskritikalität gestiegen
- Wettbewerbsdruck
- Regulatorische Anforderungen
- Kundenfeedback

23.8.2.2 SLA-Lockerung (niedrigere Anforderungen)

- Kosten-Nutzen-Verhältnis
 - Technische Machbarkeit
 - Geschäftspriorität gesunken
 - Realistische Zielsetzung
-

23.9 Prozesse und Verantwortlichkeiten

23.9.1 RACI-Matrix

Aktivität	CIO	Ops Manager	Ops Team	Stakeholder
SLA-Definition	A	R	C	C
Verfügbarkeitsmessung	I	A	R	-
SLA-Reporting	C	A	R	I
SLA-Review	A	R	C	C
Verbesserungsmaßnahmen	A	R	C	I
Incident-Response	I	A	R	I
Postmortems	C	A	R	I

Legende: R = Responsible, A = Accountable, C = Consulted, I = Informed

23.9.2 Eskalationspfad

1. **Level 1:** Operations Team - Incident-Response und Monitoring
 2. **Level 2:** Andreas Huemmer - SLA-Verletzungen
 3. **Level 3:** Anna Schmidt - Kritische SLA-Verletzungen
 4. **Level 4:** Max Mustermann - Vertragliche Konsequenzen
-

23.10 Compliance und Standards

23.10.1 Relevante Standards

- **ITIL v4:** Availability Management Practice
- **ISO 20000:** Clause 8.9 - Availability Management
- **COBIT 2019:** DSS01 - Managed Operations

23.10.2 Audit-Anforderungen

- SLA-Dokumentation und Verträge
 - Verfügbarkeits-Reports und Metriken
 - Incident-Dokumentation
 - Verbesserungsmaßnahmen-Nachweise
-

23.11 Anhang

23.11.1 Glossar

Begriff	Definition
SLA	Service Level Agreement - Vereinbarung über Serviceleistungen
SLO	Service Level Objective - Internes Serviceziel
SLI	Service Level Indicator - Messbare Metrik
MTBF	Mean Time Between Failures - Durchschnittliche Zeit zwischen Ausfällen
MTTR	Mean Time To Repair - Durchschnittliche Reparaturzeit
Error Budget	Tolerierbare Ausfallzeit innerhalb des SLO-Zeitraums
Uptime	Verfügbare Zeit eines Systems
Downtime	Ausfallzeit eines Systems

23.11.2 Referenzen

- ITIL v4 Foundation Handbook
- ISO/IEC 20000-1:2018
- COBIT 2019 Framework
- Site Reliability Engineering (Google)

Letzte Aktualisierung: {{ meta.date }}

Nächste Review: [TODO: Datum]

Kontakt: andreas.huemmer@adminsends.de

ewpage

Chapter 24

Datenmanagement und Datenschutz

24.1 Übersicht

Dieses Dokument beschreibt die Prozesse und Richtlinien für das Datenmanagement und den Datenschutz im IT-Service. Es definiert Datenklassifizierung, Datenschutzanforderungen gemäß DSGVO, Datenaufbewahrung und -löschung sowie Data-Governance-Strukturen.

Dokumentverantwortlicher: IT Operations Manager

Genehmigt durch: CIO

Version: 1.0.0

Organisation: AdminSend GmbH

24.2 Datenklassifizierung

24.2.1 Klassifizierungsstufen

Stufe	Beschreibung	Beispiele	Schutzmaßnahmen
Öffentlich	Für die Öffentlichkeit bestimmt	Marketing-Material, Pressemitteilungen	Keine besonderen Maßnahmen
Intern	Nur für interne Nutzung	Interne Richtlinien, Organigramme	Zugriffskontrolle
Vertraulich	Sensible Geschäftsinformationen	Verträge, Finanzberichte, Strategien	Verschlüsselung, strenge Zugriffskontrolle
Streng vertraulich	Höchst sensible Daten	Personaldaten, Gesundheitsdaten, Gehälter	Verschlüsselung, MFA, Audit-Logging

24.2.2 Klassifizierungskriterien

24.2.2.1 Geschäftswert

- **Hoch:** Kritisch für Geschäftsbetrieb

- **Mittel:** Wichtig für Geschäftsprozesse
- **Niedrig:** Unterstützende Informationen

24.2.2.2 Vertraulichkeit

- **Hoch:** Schwerwiegende Schäden bei Offenlegung
- **Mittel:** Moderate Schäden bei Offenlegung
- **Niedrig:** Geringe oder keine Schäden

24.2.2.3 Integrität

- **Hoch:** Kritisch für Entscheidungen
- **Mittel:** Wichtig für Prozesse
- **Niedrig:** Informativ

24.2.2.4 Verfügbarkeit

- **Hoch:** Sofortige Verfügbarkeit erforderlich
- **Mittel:** Verfügbarkeit innerhalb von Stunden
- **Niedrig:** Verfügbarkeit innerhalb von Tagen

24.2.3 Klassifizierungsprozess

1. **Datenidentifikation:** Erfassung aller Datenbestände
2. **Bewertung:** Anwendung der Klassifizierungskriterien
3. **Kennzeichnung:** Markierung der Daten mit Klassifizierungsstufe
4. **Dokumentation:** Erfassung in Data-Inventory
5. **Review:** Jährliche Überprüfung der Klassifizierung

24.2.4 Daten-Inventory

Datenbestand	Klassifizierung	Speicherort	Verantwortlich	Aufbewahrung
[TODO]	[TODO]	{{ net- box.storage.location }}	[TODO]	[TODO]
[TODO]	[TODO]	{{ net- box.storage.location }}	[TODO]	[TODO]
[TODO]	[TODO]	{{ net- box.storage.location }}	[TODO]	[TODO]

24.3 Datenschutz-Anforderungen (DSGVO)

24.3.1 Rechtliche Grundlagen

24.3.1.1 EU-Datenschutz-Grundverordnung (DSGVO)

- **Gültig seit:** 25. Mai 2018
- **Anwendungsbereich:** Verarbeitung personenbezogener Daten in der EU
- **Bußgelder:** Bis zu 20 Mio. EUR oder 4% des weltweiten Jahresumsatzes

24.3.1.2 Bundesdatenschutzgesetz (BDSG)

- **Gültig seit:** 25. Mai 2018
- **Ergänzung:** Nationale Regelungen zur DSGVO
- **Anwendung:** Deutschland-spezifische Anforderungen

24.3.2 Personenbezogene Daten

24.3.2.1 Definition

Alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen.

24.3.2.2 Kategorien

Kategorie	Beispiele	Besondere Schutzmaßnahmen
Basisdaten	Name, Adresse, E-Mail, Telefon	Zugriffskontrolle, Verschlüsselung
Identifikationsdaten	Personalausweisnummer, Sozialversicherungsnummer	Strenge Zugriffskontrolle, Verschlüsselung
Besondere Kategorien	Gesundheit, Religion, politische Meinung	Höchste Schutzmaßnahmen, explizite Einwilligung
Finanzdaten	Bankverbindung, Kreditkartennummer	PCI-DSS-Compliance, Tokenisierung
Standortdaten	GPS-Koordinaten, IP-Adressen	Anonymisierung, Pseudonymisierung

24.3.3 DSGVO-Grundsätze

24.3.3.1 Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz

- Rechtsgrundlage für jede Verarbeitung
- Transparente Information der Betroffenen
- Dokumentation der Verarbeitungszwecke

24.3.3.2 Zweckbindung

- Daten nur für festgelegte Zwecke erheben
- Keine Weiterverarbeitung für andere Zwecke
- Dokumentation der Verarbeitungszwecke

24.3.3.3 Datenminimierung

- Nur notwendige Daten erheben
- Keine übermäßige Datensammlung
- Regelmäßige Überprüfung der Notwendigkeit

24.3.3.4 Richtigkeit

- Sicherstellung der Datenaktualität
- Korrektur unrichtiger Daten
- Löschung veralteter Daten

24.3.3.5 Speicherbegrenzung

- Daten nur so lange speichern wie nötig
- Definierte Aufbewahrungsfristen
- Automatische Löschung nach Fristablauf

24.3.3.6 Integrität und Vertraulichkeit

- Schutz vor unbefugtem Zugriff
- Verschlüsselung sensibler Daten
- Zugriffskontrolle und Audit-Logging

24.3.3.7 Rechenschaftspflicht

- Nachweis der DSGVO-Compliance
- Dokumentation aller Verarbeitungstätigkeiten
- Regelmäßige Audits

24.3.4 Betroffenenrechte

Recht	Beschreibung	Reaktionszeit	Verantwortlich
Auskunftsrecht	Information über gespeicherte Daten	1 Monat	Thomas Weber
Berichtigungsrecht	Korrektur unrichtiger Daten	Unverzüglich	Thomas Weber
Löschungsrecht	Löschung personenbezogener Daten	Unverzüglich	Thomas Weber
Einschränkung	Einschränkung der Verarbeitung	Unverzüglich	Thomas Weber
Datenübertragbarkeit	Übertragung an anderen Verantwortlichen	1 Monat	Thomas Weber
Widerspruchsrecht	Widerspruch gegen Verarbeitung	Unverzüglich	Thomas Weber

24.3.5 Datenschutz-Folgenabschätzung (DSFA)

24.3.5.1 Durchführungspflicht

- Hohes Risiko für Rechte und Freiheiten
- Neue Technologien
- Umfangreiche Verarbeitung besonderer Kategorien
- Systematische Überwachung

24.3.5.2 DSFA-Prozess

1. **Beschreibung:** Verarbeitungsvorgänge und Zwecke
2. **Notwendigkeit:** Bewertung der Erforderlichkeit
3. **Risikobewertung:** Identifikation und Bewertung von Risiken
4. **Schutzmaßnahmen:** Definition von Maßnahmen zur Risikominimierung
5. **Dokumentation:** Erstellung des DSFA-Berichts
6. **Konsultation:** Ggf. Konsultation der Aufsichtsbehörde

24.3.6 Datenschutzbeauftragter (DSB)

- **Name:** [TODO: Name des DSB]
 - **Kontakt:** [TODO: E-Mail und Telefon]
 - **Aufgaben:**
 - Überwachung der DSGVO-Compliance
 - Beratung bei Datenschutzfragen
 - Schulung der Mitarbeiter
 - Zusammenarbeit mit Aufsichtsbehörden
 - Anlaufstelle für Betroffene
-

24.4 Datenaufbewahrung und -löschung

24.4.1 Aufbewahrungsfristen

24.4.1.1 Gesetzliche Aufbewahrungsfristen

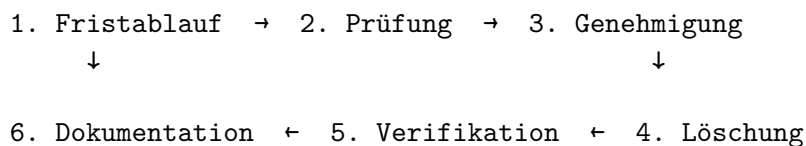
Datenart	Aufbewahrungsfrist	Rechtsgrundlage	Verantwortlich
Geschäftsbriefe	6 Jahre	HGB § 257	Maria Müller
Buchungsbelege	10 Jahre	HGB § 257, AO § 147	Maria Müller
Jahresabschlüsse	10 Jahre	HGB § 257	Maria Müller
Lohnunterlagen	6 Jahre	AO § 147	Maria Müller
Steuerunterlagen	10 Jahre	AO § 147	Maria Müller
Personalakten	3-10 Jahre	Verschiedene	Peter Fischer

24.4.1.2 Betriebliche Aufbewahrungsfristen

Datenart	Aufbewahrungsfrist	Grund	Verantwortlich
Verträge	Vertragslaufzeit + 3 Jahre	Gewährleistung	[TODO]
Projektdokumentation	5 Jahre	Nachvollziehbarkeit	[TODO]
Audit-Logs	1 Jahr	Sicherheit	Thomas Weber
Backup-Daten	30-90 Tage	Wiederherstellung	Andreas Huemmer
E-Mails	1-3 Jahre	Geschäftskommunikation	[TODO]

24.4.2 Löschkonzept

24.4.2.1 Löschprozess



24.4.2.2 Löschmethoden

Datenträger	Methode	Standard	Verantwortlich
Festplatten	Secure Erase / Degaussing	NIST SP 800-88	Andreas Huemmer
SSDs	Crypto Erase / Zerstörung	NIST SP 800-88	Andreas Huemmer
Backup-Medien	Überschreiben / Zerstörung	NIST SP 800-88	Andreas Huemmer
Cloud-Daten	API-basierte Löschung	Provider-Standard	Andreas Huemmer
Datenbanken	SQL DELETE / TRUNCATE	Datenbankstandard	Andreas Huemmer
Papier	Aktenvernichtung (P-4)	DIN 66399	Peter Fischer

24.4.2.3 Löschnachweis

- Dokumentation aller Löschvorgänge
- Protokollierung von Datum, Datenart, Methode
- Aufbewahrung der Löschnachweise für 3 Jahre
- Verantwortlich: Thomas Weber

24.4.3 Archivierung

24.4.3.1 Archivierungsprozess

1. **Identifikation:** Daten, die archiviert werden müssen

2. **Vorbereitung:** Datenbereinigung und -validierung
3. **Archivierung:** Transfer in Archivsystem
4. **Indexierung:** Metadaten für Wiederauffindbarkeit
5. **Verifikation:** Prüfung der Archivintegrität
6. **Dokumentation:** Erfassung im Archivregister

24.4.3.2 Archivierungssysteme

System	Datenart	Aufbewahrung	Zugriff	Verantwortlich
[TODO: Archivsystem]	[TODO]	[TODO] Jahre	[TODO]	[TODO]

24.5 Data-Governance

24.5.1 Governance-Struktur

24.5.1.1 Data Governance Board

- **Vorsitz:** Anna Schmidt
- **Mitglieder:** Thomas Weber, Maria Müller, Fachbereichsleiter
- **Frequenz:** Quartalsweise
- **Aufgaben:**
 - Strategische Daten-Governance
 - Genehmigung von Data Policies
 - Überwachung der Compliance
 - Eskalation von Datenschutzvorfällen

24.5.1.2 Data Stewards

- **Rolle:** Fachliche Datenverantwortliche
- **Aufgaben:**
 - Datenqualität sicherstellen
 - Datenklassifizierung durchführen
 - Zugriffsgenehmigungen erteilen
 - Datenschutz-Compliance überwachen

24.5.1.3 Data Custodians

- **Rolle:** Technische Datenverantwortliche
- **Aufgaben:**
 - Technische Umsetzung der Data Policies
 - Datensicherheit gewährleisten
 - Backup und Recovery
 - Zugriffskontrolle implementieren

24.5.2 Data Policies

24.5.2.1 Datennutzungsrichtlinie

- Erlaubte und verbotene Datennutzungen
- Genehmigungsprozesse für Datennutzung
- Sanktionen bei Verstößen

24.5.2.2 Datenzugriffsrichtlinie

- Zugriffskontrollmodell (RBAC, ABAC)
- Genehmigungsprozesse für Zugriffe
- Regelmäßige Zugriffsprüfungen

24.5.2.3 Datensicherheitsrichtlinie

- Verschlüsselungsanforderungen
- Sicherheitsmaßnahmen nach Klassifizierung
- Incident-Response-Prozesse

24.5.2.4 Datenqualitätsrichtlinie

- Datenqualitätskriterien
- Datenvalidierung und -bereinigung
- Datenqualitäts-Metriken

24.5.3 Datenqualitätsmanagement

24.5.3.1 Datenqualitätsdimensionen

Dimension	Beschreibung	Zielwert	Messmethode
Vollständigkeit	Alle erforderlichen Daten vorhanden	> 95%	Automatische Prüfung
Richtigkeit	Daten korrekt und fehlerfrei	> 98%	Stichproben
Konsistenz	Daten widerspruchsfrei	> 99%	Automatische Prüfung
Aktualität	Daten auf dem neuesten Stand	> 95%	Zeitstempel-Prüfung
Eindeutigkeit	Keine Duplikate	> 99%	Duplikatsprüfung

24.5.3.2 Datenqualitätsprozess

1. **Messung:** Erfassung der Datenqualitäts-Metriken
2. **Analyse:** Identifikation von Qualitätsproblemen
3. **Bereinigung:** Korrektur fehlerhafter Daten
4. **Prävention:** Maßnahmen zur Vermeidung zukünftiger Probleme
5. **Monitoring:** Kontinuierliche Überwachung

24.6 Datensicherheit

24.6.1 Verschlüsselung

24.6.1.1 Verschlüsselung im Ruhezustand (Data at Rest)

Datenart	Verschlüsselung	Algorithmus	Schlüssellänge	Verantwortlich
Streng vertraulich	Pflicht	AES	256 Bit	Thomas Weber
Vertraulich	Pflicht	AES	256 Bit	Thomas Weber
Intern	Empfohlen	AES	128/256 Bit	Andreas Huemmer
Öffentlich	Nicht erforderlich	-	-	-

24.6.1.2 Verschlüsselung in Übertragung (Data in Transit)

Verbindungstyp	Protokoll	Mindestversion	Verantwortlich
Web-Traffic	HTTPS/TLS	TLS 1.2	Andreas Huemmer
E-Mail	TLS/S/MIME	TLS 1.2	Andreas Huemmer
Dateiübertragung	SFTP/FTPS	TLS 1.2	Andreas Huemmer
VPN	IPsec/OpenVPN	-	Andreas Huemmer
Datenbank	TLS	TLS 1.2	Andreas Huemmer

24.6.2 Zugriffskontrolle

24.6.2.1 Zugriffskontrollmodell

- **Modell:** Role-Based Access Control (RBAC)
- **Prinzip:** Least Privilege, Need-to-Know
- **Authentifizierung:** Multi-Faktor-Authentifizierung (MFA) für sensible Daten
- **Autorisierung:** Rollenbasierte Berechtigungen

24.6.2.2 Zugriffsrechte-Review

- **Frequenz:** Quartalsweise
- **Verantwortlich:** Data Stewards
- **Prozess:**
 1. Export aller Zugriffsrechte
 2. Review durch Fachbereich
 3. Entfernung nicht mehr benötigter Rechte
 4. Dokumentation der Änderungen

24.6.3 Audit-Logging

24.6.3.1 Logging-Anforderungen

Ereignistyp	Logging	Aufbewahrung	Verantwortlich
Datenzugriff (vertraulich)	Pflicht	1 Jahr	Thomas Weber
Datenänderung	Pflicht	1 Jahr	Thomas Weber
Datenlöschung	Pflicht	3 Jahre	Thomas Weber
Zugriffsverweigerung	Pflicht	1 Jahr	Thomas Weber
Admin-Aktivitäten	Pflicht	1 Jahr	Thomas Weber

24.6.3.2 Log-Inhalte

- Zeitstempel
 - Benutzer-ID
 - Aktion (Lesen, Schreiben, Löschen)
 - Betroffene Daten/Objekte
 - Quell-IP-Adresse
 - Ergebnis (Erfolg/Fehler)
-

24.7 Datenschutzvorfälle

24.7.1 Meldepflicht

24.7.1.1 DSGVO-Meldepflicht

- **Frist:** 72 Stunden nach Bekanntwerden
- **Empfänger:** Zuständige Aufsichtsbehörde
- **Inhalt:**
 - Art der Verletzung
 - Betroffene Datenkategorien und Personen
 - Wahrscheinliche Folgen
 - Ergriffene Maßnahmen

24.7.1.2 Benachrichtigung Betroffener

- **Voraussetzung:** Hohes Risiko für Rechte und Freiheiten
- **Frist:** Unverzüglich
- **Inhalt:**
 - Art der Verletzung
 - Kontaktstelle
 - Wahrscheinliche Folgen
 - Ergriffene Maßnahmen

24.7.2 Incident-Response-Prozess

1. **Erkennung:** Identifikation des Datenschutzvorfalls
2. **Bewertung:** Einschätzung des Risikos
3. **Eindämmung:** Sofortmaßnahmen zur Schadensbegrenzung
4. **Meldung:** Meldung an Aufsichtsbehörde (falls erforderlich)
5. **Benachrichtigung:** Information der Betroffenen (falls erforderlich)

6. **Untersuchung:** Root-Cause-Analyse
 7. **Behebung:** Korrekturmaßnahmen
 8. **Dokumentation:** Erfassung im Incident-Register
 9. **Lessons Learned:** Prozessverbesserungen
-

24.8 Prozesse und Verantwortlichkeiten

24.8.1 RACI-Matrix

Aktivität	CIO	CISO	Ops Manager	DSB	Data Stewards
Datenklassifizierung	I	C	I	C	R/A
DSGVO-Compliance	A	R	C	C	I
Datenschutz-Folgenabschätzung	C	R	C	A	C
Datenaufbewahrung	C	C	R	C	A
Datenlöschung	I	C	R	C	A
Data-Governance	A	C	C	C	R
Datensicherheit	C	A	R	C	I
Datenschutzvorfälle	A	R	C	C	I

Legende: R = Responsible, A = Accountable, C = Consulted, I = Informed

24.9 Compliance und Standards

24.9.1 Relevante Standards

- **DSGVO:** EU-Datenschutz-Grundverordnung
- **BDSG:** Bundesdatenschutzgesetz
- **ISO 27001:** Informationssicherheitsmanagement
- **ISO 27701:** Privacy Information Management
- **NIST SP 800-88:** Guidelines for Media Sanitization

24.9.2 Audit-Anforderungen

- Verzeichnis von Verarbeitungstätigkeiten
 - Datenschutz-Folgenabschätzungen
 - Auftragsverarbeitungsverträge
 - Löschnachweise
 - Audit-Logs
-

24.10 Anhang

24.10.1 Glossar

Begriff	Definition
DSGVO	Datenschutz-Grundverordnung der EU
Personenbezogene Daten	Daten, die sich auf eine identifizierbare Person beziehen
Data Steward	Fachlicher Datenverantwortlicher
Data Custodian	Technischer Datenverantwortlicher
DSFA	Datenschutz-Folgenabschätzung
Pseudonymisierung	Verarbeitung ohne Zuordnung zu einer Person ohne Zusatzinformationen
Anonymisierung	Irreversible Entfernung des Personenbezugs

24.10.2 Referenzen

- EU-Datenschutz-Grundverordnung (DSGVO)
- Bundesdatenschutzgesetz (BDSG)
- ISO/IEC 27001:2013
- ISO/IEC 27701:2019
- NIST SP 800-88 Rev. 1

Letzte Aktualisierung: {{ meta.date }}

Nächste Review: [TODO: Datum]

Kontakt: thomas.weber@adminsind.de

ewpage

Chapter 25

Wartung und Operations-Routinen

25.1 Übersicht

Dieses Dokument beschreibt die regelmäßigen Wartungsaufgaben, Operations-Checklisten und Housekeeping-Prozeduren für den IT-Service. Ziel ist es, die Systemstabilität, Performance und Sicherheit durch proaktive Wartung zu gewährleisten.

Dokumentverantwortlicher: IT Operations Manager

Genehmigt durch: CIO

Version: 1.0.0

Organisation: AdminSend GmbH

25.2 Wartungsübersicht

25.2.1 Wartungskategorien

Kategorie	Beschreibung	Frequenz	Verantwortlich
Präventiv	Vorbeugende Maßnahmen zur Fehlervermeidung	Regelmäßig	Andreas Huemmer
Korrektiv	Behebung bekannter Probleme	Bei Bedarf	Andreas Huemmer
Adaptiv	Anpassung an neue Anforderungen	Bei Bedarf	Andreas Huemmer
Perfektiv	Verbesserung und Optimierung	Geplant	Andreas Huemmer

25.2.2 Wartungsfenster

25.2.2.1 Reguläre Wartungsfenster

Typ	Zeitfenster	Dauer	Ankündigung	Genehmigung
Wöchentlich	Sonntag 02:00-04:00	2 Stunden	3 Tage	Ops Manager
Monatlich	Erster Sonntag 02:00-06:00	4 Stunden	7 Tage	Ops Manager
Quartalsweise	Erster Sonntag im Quartal 00:00-08:00	8 Stunden	14 Tage	CIO

25.2.2.2 Notfall-Wartung

- **Zeitfenster:** Jederzeit nach Genehmigung
- **Ankündigung:** Minimum 4 Stunden (wenn möglich)
- **Genehmigung:** Anna Schmidt
- **Kommunikation:** Alle Stakeholder informieren

25.3 Tägliche Routinen

25.3.1 Morgen-Checks (08:00 Uhr)

25.3.1.1 System-Health-Check

- ☐ Monitoring-Dashboard prüfen
- ☐ Kritische Alerts überprüfen
- ☐ System-Verfügbarkeit validieren
- ☐ Performance-Metriken prüfen
- ☐ Backup-Status überprüfen

25.3.1.2 Incident-Review

- ☐ Overnight-Incidents prüfen
- ☐ Offene Tickets reviewen
- ☐ Prioritäten für den Tag setzen
- ☐ Eskalationen identifizieren

25.3.1.3 Kapazitäts-Check

- ☐ CPU-Auslastung prüfen
- ☐ RAM-Auslastung prüfen
- ☐ Storage-Auslastung prüfen
- ☐ Netzwerk-Auslastung prüfen

Verantwortlich: Operations Team

Dauer: 15-30 Minuten

Dokumentation: Daily Operations Log

25.3.2 Mittags-Checks (12:00 Uhr)

25.3.2.1 Performance-Monitoring

- ☐ Response-Times prüfen
- ☐ Error-Rates überprüfen
- ☐ Throughput validieren
- ☐ Queue-Längen prüfen

25.3.2.2 Security-Check

- ☐ Security-Alerts prüfen
- ☐ Failed-Login-Attempts reviewen
- ☐ Firewall-Logs prüfen
- ☐ Anomalien identifizieren

Verantwortlich: Operations Team

Dauer: 10-15 Minuten

Dokumentation: Daily Operations Log

25.3.3 Abend-Checks (18:00 Uhr)

25.3.3.1 Tagesabschluss

- ☐ Alle Incidents des Tages reviewen
- ☐ Offene Tickets aktualisieren
- ☐ Backup-Jobs für die Nacht vorbereiten
- ☐ Wartungsarbeiten für die Nacht planen

25.3.3.2 Übergabe an Nachtschicht/On-Call

- ☐ Kritische Themen kommunizieren
- ☐ Laufende Arbeiten dokumentieren
- ☐ On-Call-Kontakte aktualisieren
- ☐ Eskalationspfade bestätigen

Verantwortlich: Operations Team

Dauer: 15-20 Minuten

Dokumentation: Shift Handover Log

25.4 Wöchentliche Routinen

25.4.1 Montag: Wochenplanung

25.4.1.1 Wochenstart-Meeting (09:00 Uhr)

- ☐ Wochenend-Incidents reviewen
- ☐ Wochenziele definieren
- ☐ Wartungsarbeiten planen
- ☐ Ressourcen zuweisen

- ☐ Risiken identifizieren

Teilnehmer: Andreas Huemmer, Operations Team

Dauer: 30 Minuten

Dokumentation: Weekly Planning Notes

25.4.1.2 System-Updates prüfen

- ☐ Verfügbare Updates identifizieren
- ☐ Kritikalität bewerten
- ☐ Test-Planung durchführen
- ☐ Deployment-Zeitplan erstellen

Verantwortlich: Operations Team

Dauer: 1 Stunde

25.4.2 Dienstag: Backup-Validierung

25.4.2.1 Backup-Verifikation

- ☐ Backup-Logs der letzten Woche prüfen
- ☐ Backup-Erfolgsrate validieren
- ☐ Backup-Größen überprüfen
- ☐ Fehlgeschlagene Backups analysieren
- ☐ Restore-Test durchführen (stichprobenartig)

Verantwortlich: Operations Team

Dauer: 1-2 Stunden

Dokumentation: Backup Verification Report

25.4.3 Mittwoch: Performance-Analyse

25.4.3.1 Wöchentliche Performance-Review

- ☐ Performance-Trends analysieren
- ☐ Bottlenecks identifizieren
- ☐ Kapazitätsprognosen aktualisieren
- ☐ Optimierungspotenziale identifizieren

Verantwortlich: Operations Team

Dauer: 1 Stunde

Dokumentation: Weekly Performance Report

25.4.4 Donnerstag: Security-Review

25.4.4.1 Wöchentlicher Security-Check

- ☐ Security-Logs analysieren
- ☐ Vulnerability-Scans reviewen
- ☐ Patch-Status prüfen
- ☐ Security-Incidents reviewen
- ☐ Compliance-Status prüfen

Verantwortlich: Operations Team, Thomas Weber

Dauer: 1-2 Stunden

Dokumentation: Weekly Security Report

25.4.5 Freitag: Wochenabschluss

25.4.5.1 Wochenabschluss-Meeting (15:00 Uhr)

- ☐ Wochenziele reviewen
- ☐ Incidents der Woche zusammenfassen
- ☐ Lessons Learned diskutieren
- ☐ Nächste Woche vorbereiten
- ☐ Wochenend-On-Call briefen

Teilnehmer: Andreas Huemmer, Operations Team

Dauer: 30 Minuten

Dokumentation: Weekly Summary Report

25.4.5.2 Housekeeping

- ☐ Temporäre Dateien bereinigen
- ☐ Log-Rotation durchführen
- ☐ Alte Tickets archivieren
- ☐ Dokumentation aktualisieren

Verantwortlich: Operations Team

Dauer: 1 Stunde

25.4.6 Sonntag: Wartungsfenster

25.4.6.1 Wöchentliche Wartung (02:00-04:00 Uhr)

- ☐ System-Updates installieren
- ☐ Datenbank-Wartung durchführen
- ☐ Log-Archivierung
- ☐ Disk-Cleanup
- ☐ Performance-Optimierung

Verantwortlich: On-Call Engineer

Dauer: 2 Stunden

Dokumentation: Maintenance Log

25.5 Monatliche Routinen

25.5.1 Erste Woche: Monatsplanung

25.5.1.1 Monatsstart-Meeting

- ☐ Vormonat reviewen
- ☐ Monatsziele definieren

- ☐ Größere Wartungsarbeiten planen
- ☐ Budget-Status prüfen
- ☐ Kapazitätsplanung aktualisieren

Teilnehmer: Anna Schmidt, Andreas Huemmer, Team Leads

Dauer: 1 Stunde

Dokumentation: Monthly Planning Document

25.5.2 Erste Woche: Patch-Management

25.5.2.1 Monatliches Patch-Deployment

- ☐ Patch-Verfügbarkeit prüfen
- ☐ Kritikalität bewerten
- ☐ Test-Umgebung patchen
- ☐ Validierung durchführen
- ☐ Produktions-Deployment planen
- ☐ Rollback-Plan erstellen

Verantwortlich: Operations Team

Dauer: 4-8 Stunden (über mehrere Tage)

Dokumentation: Patch Management Report

25.5.3 Zweite Woche: Capacity-Review

25.5.3.1 Monatliche Kapazitätsanalyse

- ☐ Ressourcen-Auslastung analysieren
- ☐ Wachstumstrends identifizieren
- ☐ Kapazitätsprognosen erstellen
- ☐ Skalierungsbedarf bewerten
- ☐ Budget-Implicationen prüfen

Verantwortlich: Andreas Huemmer

Dauer: 2-3 Stunden

Dokumentation: Monthly Capacity Report

25.5.4 Dritte Woche: Security-Audit

25.5.4.1 Monatliches Security-Audit

- ☐ Zugriffsrechte reviewen
- ☐ Inaktive Accounts deaktivieren
- ☐ Passwort-Policies prüfen
- ☐ Firewall-Regeln reviewen
- ☐ Vulnerability-Scan durchführen
- ☐ Compliance-Status prüfen

Verantwortlich: Thomas Weber, Operations Team

Dauer: 3-4 Stunden

Dokumentation: Monthly Security Audit Report

25.5.5 Vierte Woche: Disaster-Recovery-Test

25.5.5.1 Monatlicher DR-Test

- ☐ DR-Szenario auswählen
- ☐ Test-Plan erstellen
- ☐ DR-Prozeduren durchführen
- ☐ Ergebnisse dokumentieren
- ☐ Verbesserungen identifizieren
- ☐ DR-Plan aktualisieren

Verantwortlich: Andreas Huemmer

Dauer: 2-4 Stunden

Dokumentation: DR Test Report

25.5.6 Monatsende: Reporting

25.5.6.1 Monatliche Reports erstellen

- ☐ Verfügbarkeits-Report
- ☐ Performance-Report
- ☐ Incident-Report
- ☐ Capacity-Report
- ☐ Security-Report
- ☐ SLA-Compliance-Report

Verantwortlich: Andreas Huemmer

Dauer: 2-3 Stunden

Empfänger: Anna Schmidt, Stakeholder

25.6 Quartalsweise Routinen

25.6.1 Erste Woche: Quartalsplanung

25.6.1.1 Quartalsstart-Meeting

- ☐ Vorquartal reviewen
- ☐ Quartalsziele definieren
- ☐ Größere Projekte planen
- ☐ Budget-Review durchführen
- ☐ Ressourcenplanung aktualisieren

Teilnehmer: Max Mustermann, Anna Schmidt, Andreas Huemmer

Dauer: 2 Stunden

Dokumentation: Quarterly Planning Document

25.6.2 Zweite Woche: Infrastruktur-Review

25.6.2.1 Quartalsweise Infrastruktur-Analyse

- ☐ Hardware-Zustand prüfen

- ☐ End-of-Life-Systeme identifizieren
- ☐ Upgrade-Bedarf bewerten
- ☐ Konsolidierungspotenziale identifizieren
- ☐ Investitionsplanung durchführen

Verantwortlich: Andreas Huemmer

Dauer: 1 Tag

Dokumentation: Quarterly Infrastructure Report

25.6.3 Dritte Woche: Prozess-Review

25.6.3.1 Quartalsweise Prozess-Optimierung

- ☐ Betriebsprozesse reviewen
- ☐ Ineffizienzen identifizieren
- ☐ Automatisierungspotenziale bewerten
- ☐ Verbesserungsmaßnahmen definieren
- ☐ Implementierungsplan erstellen

Verantwortlich: Andreas Huemmer, Team Leads

Dauer: 1 Tag

Dokumentation: Process Improvement Plan

25.6.4 Vierte Woche: Disaster-Recovery-Volltest

25.6.4.1 Quartalsweiser vollständiger DR-Test

- ☐ Vollständiges DR-Szenario durchführen
- ☐ Alle kritischen Systeme testen
- ☐ RTO/RPO validieren
- ☐ Team-Koordination testen
- ☐ Kommunikationsprozesse validieren
- ☐ Lessons Learned dokumentieren

Verantwortlich: Anna Schmidt, Andreas Huemmer

Dauer: 1 Tag

Dokumentation: Quarterly DR Test Report

25.7 Jährliche Routinen

25.7.1 Q1: Jahresplanung

25.7.1.1 Jahresstart-Meeting

- ☐ Vorjahr reviewen
- ☐ Jahresziele definieren
- ☐ Strategische Initiativen planen
- ☐ Jahresbudget finalisieren
- ☐ Ressourcenplanung für das Jahr

Teilnehmer: Max Mustermann, Anna Schmidt, Maria Müller, Andreas Huemmer

Dauer: 1 Tag

Dokumentation: Annual Planning Document

25.7.2 Q2: Infrastruktur-Audit

25.7.2.1 Jährliches Infrastruktur-Audit

- ☐ Vollständiges Hardware-Inventory
- ☐ Software-Lizenz-Audit
- ☐ Compliance-Audit durchführen
- ☐ Security-Assessment
- ☐ Architektur-Review
- ☐ Modernisierungsbedarf identifizieren

Verantwortlich: Anna Schmidt, Andreas Huemmer

Dauer: 1 Woche

Dokumentation: Annual Infrastructure Audit Report

25.7.3 Q3: Disaster-Recovery-Volltest

25.7.3.1 Jährlicher umfassender DR-Test

- ☐ Vollständiger Failover-Test
- ☐ Alle Systeme und Prozesse testen
- ☐ Business-Continuity-Plan validieren
- ☐ Externe Stakeholder einbeziehen
- ☐ Kommunikationsprozesse testen
- ☐ Umfassende Dokumentation

Verantwortlich: Anna Schmidt, Andreas Huemmer

Dauer: 2-3 Tage

Dokumentation: Annual DR Test Report

25.7.4 Q4: Jahresabschluss

25.7.4.1 Jahresabschluss-Review

- ☐ Jahresziele reviewen
- ☐ KPIs analysieren
- ☐ Budget-Abweichungen prüfen
- ☐ Lessons Learned dokumentieren
- ☐ Nächstes Jahr vorbereiten
- ☐ Management-Präsentation erstellen

Teilnehmer: Max Mustermann, Anna Schmidt, Maria Müller, Andreas Huemmer

Dauer: 1 Tag

Dokumentation: Annual Review Report

25.8 Housekeeping-Prozeduren

25.8.1 Datenbank-Wartung

25.8.1.1 Wöchentliche Datenbank-Wartung

- ☐ Index-Fragmentierung prüfen
- ☐ Statistiken aktualisieren
- ☐ Transaktionslogs bereinigen
- ☐ Datenbank-Integrität prüfen
- ☐ Performance-Metriken analysieren

Verantwortlich: Database Administrator

Frequenz: Wöchentlich (Sonntag 02:00 Uhr)

Dauer: 1-2 Stunden

25.8.1.2 Monatliche Datenbank-Wartung

- ☐ Index-Rebuild durchführen
- ☐ Datenbank-Shrink (falls erforderlich)
- ☐ Alte Daten archivieren
- ☐ Backup-Strategie validieren
- ☐ Disaster-Recovery-Test

Verantwortlich: Database Administrator

Frequenz: Monatlich (Erster Sonntag 02:00 Uhr)

Dauer: 2-4 Stunden

25.8.2 Log-Management

25.8.2.1 Tägliche Log-Rotation

- ☐ Application-Logs rotieren
- ☐ System-Logs rotieren
- ☐ Alte Logs komprimieren
- ☐ Logs zu zentralem System senden

Verantwortlich: Automatisiert

Frequenz: Täglich (00:00 Uhr)

Dauer: Automatisch

25.8.2.2 Wöchentliche Log-Archivierung

- ☐ Logs der letzten Woche archivieren
- ☐ Archiv-Integrität prüfen
- ☐ Alte Archive löschen (nach Retention-Policy)
- ☐ Archiv-Speicherplatz prüfen

Verantwortlich: Operations Team

Frequenz: Wöchentlich (Sonntag)

Dauer: 30 Minuten

25.8.3 Storage-Housekeeping

25.8.3.1 Wöchentliches Storage-Cleanup

- ☐ Temporäre Dateien löschen
- ☐ Alte Downloads bereinigen
- ☐ Cache-Verzeichnisse leeren
- ☐ Verwaiste Dateien identifizieren
- ☐ Storage-Auslastung prüfen

Verantwortlich: Operations Team

Frequenz: Wöchentlich (Freitag)

Dauer: 1 Stunde

25.8.3.2 Monatliches Storage-Audit

- ☐ Storage-Auslastung analysieren
- ☐ Große Dateien identifizieren
- ☐ Duplikate finden und entfernen
- ☐ Archivierungskandidaten identifizieren
- ☐ Storage-Optimierung durchführen

Verantwortlich: Operations Team

Frequenz: Monatlich

Dauer: 2-3 Stunden

25.8.4 System-Cleanup

25.8.4.1 Wöchentliches System-Cleanup

- ☐ Temporäre Dateien löschen
- ☐ Package-Cache bereinigen
- ☐ Alte Kernel-Versionen entfernen
- ☐ Verwaiste Packages entfernen
- ☐ System-Logs bereinigen

Verantwortlich: Operations Team

Frequenz: Wöchentlich (Sonntag)

Dauer: 30 Minuten

25.9 Automatisierung

25.9.1 Automatisierte Routinen

Routine	Frequenz	Tool/Script	Verantwortlich
Backup-Jobs	Täglich	[TODO: Backup-Tool]	Andreas Huemmer
Log-Rotation	Täglich	logrotate	Automatisiert
Health-Checks	Stündlich	[TODO: Monitoring-Tool]	Automatisiert
Disk-Cleanup	Wöchentlich	[TODO: Script]	Automatisiert

Routine	Frequenz	Tool/Script	Verantwortlich
Security-Scans	Täglich	[TODO: Security-Tool]	Automatisiert
Performance-Reports	Wöchentlich	[TODO: Script]	Automatisiert

25.9.2 Automatisierungs-Roadmap

Quartal	Routine	Erwarteter Nutzen	Status
Q1 2026	[TODO]	[TODO] Stunden/Monat	Geplant
Q2 2026	[TODO]	[TODO] Stunden/Monat	Geplant
Q3 2026	[TODO]	[TODO] Stunden/Monat	Geplant
Q4 2026	[TODO]	[TODO] Stunden/Monat	Geplant

25.10 Checklisten-Vorlagen

25.10.1 Daily Operations Checklist

Daily Operations Checklist - [DATUM]

Morgen-Check (08:00)

- [] Monitoring-Dashboard geprüft
- [] Kritische Alerts überprüft
- [] System-Verfügbarkeit validiert
- [] Backup-Status überprüft
- [] Overnight-Incidents geprüft

Mittags-Check (12:00)

- [] Performance-Metriken geprüft
- [] Security-Alerts überprüft
- [] Kapazitäts-Status validiert

Abend-Check (18:00)

- [] Tages-Incidents reviewt
- [] Offene Tickets aktualisiert
- [] Nachtschicht-Übergabe durchgeführt

Durchgeführt von: [NAME]

Besonderheiten: [NOTIZEN]

25.10.2 Weekly Maintenance Checklist

Weekly Maintenance Checklist - KW [NUMMER]

Montag: Planung

- [] Wochenend-Incidents reviewt

- [] Wochenziele definiert
- [] Wartungsarbeiten geplant

Dienstag: Backup

- [] Backup-Logs geprüft
- [] Restore-Test durchgeführt

Mittwoch: Performance

- [] Performance-Trends analysiert
- [] Bottlenecks identifiziert

Donnerstag: Security

- [] Security-Logs analysiert
- [] Vulnerability-Scans reviewt

Freitag: Abschluss

- [] Wochenziele reviewt
- [] Housekeeping durchgeführt
- [] Wochenend-On-Call gebrieft

Sonntag: Wartung

- [] System-Updates installiert
- [] Datenbank-Wartung durchgeführt
- [] Disk-Cleanup durchgeführt

Durchgeführt von: [NAME]

Besonderheiten: [NOTIZEN]

25.11 Prozesse und Verantwortlichkeiten

25.11.1 RACI-Matrix

Aktivität	CIO	Ops Manager	Ops Team	On-Call
Tägliche Routinen	I	A	R	C
Wöchentliche Routinen	I	A	R	C
Monatliche Routinen	C	A	R	I
Quartalsweise Routinen	A	R	C	I
Jährliche Routinen	A	R	C	I
Automatisierung	C	A	R	I
Housekeeping	I	A	R	C

Legende: R = Responsible, A = Accountable, C = Consulted, I = Informed

25.12 Compliance und Standards

25.12.1 Relevante Standards

- **ITIL v4:** Service Operation Practice
- **ISO 20000:** Clause 8.1 - Operational Planning and Control
- **COBIT 2019:** DSS01 - Managed Operations

25.12.2 Audit-Anforderungen

- Wartungsprotokolle
 - Checklisten-Dokumentation
 - Automatisierungs-Scripts
 - Compliance-Nachweise
-

25.13 Anhang

25.13.1 Glossar

Begriff	Definition
Housekeeping	Regelmäßige Aufräum- und Wartungsarbeiten
Operations Routine	Wiederkehrende betriebliche Aufgabe
Preventive Maintenance	Vorbeugende Wartung zur Fehlervermeidung
Corrective Maintenance	Behebung bekannter Probleme

25.13.2 Referenzen

- ITIL v4 Foundation Handbook
 - ISO/IEC 20000-1:2018
 - COBIT 2019 Framework
-

Letzte Aktualisierung: {{ meta.date }}

Nächste Review: [TODO: Datum]

Kontakt: andreas.huemmer@adminsends.de

ewpage

Chapter 26

Runbooks und Standardoperationen

26.1 Übersicht

Dieses Dokument enthält Standard-Runbooks, Schritt-für-Schritt-Anleitungen und Troubleshooting-Guides für häufige Betriebsaufgaben. Ziel ist es, konsistente und effiziente Durchführung von Standardoperationen zu gewährleisten.

Dokumentverantwortlicher: IT Operations Manager

Genehmigt durch: CIO

Version: 1.0.0

Organisation: AdminSend GmbH

26.2 Runbook-Struktur

26.2.1 Runbook-Template

Jedes Runbook folgt dieser standardisierten Struktur:

```
# [RUNBOOK-TITEL]

**Runbook-ID:** RB- [NUMMER]
**Version:** [VERSION]
**Letzte Aktualisierung:** [DATUM]
**Verantwortlich:** [NAME]

## Zweck
[Beschreibung des Zwecks und Anwendungsfalls]

## Voraussetzungen
- [Erforderliche Berechtigungen]
- [Erforderliche Tools]
- [Erforderliches Wissen]

## Geschätzte Dauer
```

```
[ZEIT] Minuten/Stunden

## Risikobewertung
- **Risiko:** Niedrig / Mittel / Hoch
- **Impact:** Niedrig / Mittel / Hoch
- **Rollback möglich:** Ja / Nein

## Schritte
1. [Schritt 1]
2. [Schritt 2]
3. [Schritt 3]

## Validierung
- [Validierungsschritt 1]
- [Validierungsschritt 2]

## Rollback
[Rollback-Prozedur falls erforderlich]

## Troubleshooting
[Häufige Probleme und Lösungen]

## Referenzen
- [Dokumentation]
- [Tickets]
```

26.3 System-Management Runbooks

26.3.1 RB-001: Server-Neustart

Runbook-ID: RB-001

Version: 1.0

Verantwortlich: Andreas Huemmer

26.3.1.1 Zweck

Kontrollierter Neustart eines Servers zur Behebung von Problemen oder nach Updates.

26.3.1.2 Voraussetzungen

- Root/Administrator-Zugriff auf Server
- Genehmigung für Neustart (bei Produktionssystemen)
- Wartungsfenster (falls erforderlich)

26.3.1.3 Geschätzte Dauer

15-30 Minuten

26.3.1.4 Risikobewertung

- **Risiko:** Mittel
- **Impact:** Hoch (bei Produktionssystemen)
- **Rollback möglich:** Nein

26.3.1.5 Schritte

1. Vorbereitung

```
# Aktuelle Systemlast prüfen
uptime
top

# Laufende Prozesse prüfen
ps aux | grep [kritische_prozesse]

# Benutzer informieren (falls erforderlich)
wall "System wird in 5 Minuten neu gestartet"
```

2. Services stoppen

```
# Anwendungs-Services stoppen
systemctl stop [service_name]

# Status prüfen
systemctl status [service_name]
```

3. Neustart durchführen

```
# Neustart initiieren
shutdown -r now
# oder
reboot
```

4. Nach Neustart: Validierung

```
# System-Uptime prüfen
uptime

# Services prüfen
systemctl status [service_name]

# Logs prüfen
journalctl -xe
tail -f /var/log/syslog
```

26.3.1.6 Validierung

- ☐ Server ist erreichbar (ping, SSH)
- ☐ Alle kritischen Services laufen
- ☐ Keine Fehler in System-Logs

- ☐ Monitoring zeigt grünen Status
- ☐ Anwendung ist funktionsfähig

26.3.1.7 Troubleshooting

- **Problem:** Server startet nicht
 - **Lösung:** Console-Zugriff nutzen, Boot-Logs prüfen
 - **Problem:** Services starten nicht
 - **Lösung:** Manuell starten, Logs prüfen, Dependencies prüfen
-

26.3.2 RB-002: Service-Neustart

Runbook-ID: RB-002

Version: 1.0

Verantwortlich: Andreas Huemmer

26.3.2.1 Zweck

Neustart eines einzelnen Services ohne System-Neustart.

26.3.2.2 Voraussetzungen

- Sudo/Administrator-Rechte
- Service-Name bekannt

26.3.2.3 Geschätzte Dauer

5-10 Minuten

26.3.2.4 Schritte

1. Service-Status prüfen

```
# Linux
systemctl status [service_name]
```

```
# Windows
Get-Service [service_name]
```

2. Service stoppen

```
# Linux
systemctl stop [service_name]
```

```
# Windows
Stop-Service [service_name]
```

3. Warten und validieren

```
# Prozess-Ende bestätigen
ps aux | grep [service_name]
```

```
# Ports freigegeben prüfen  
netstat -tulpn | grep [port]
```

4. Service starten

```
# Linux  
systemctl start [service_name]  
  
# Windows  
Start-Service [service_name]
```

5. Validierung

```
# Status prüfen  
systemctl status [service_name]  
  
# Logs prüfen  
journalctl -u [service_name] -f
```

26.3.2.5 Validierung

- ☐ Service läuft (Status: active/running)
 - ☐ Keine Fehler in Logs
 - ☐ Port ist gebunden
 - ☐ Anwendung antwortet
-

26.3.3 RB-003: Disk-Space-Cleanup

Runbook-ID: RB-003

Version: 1.0

Verantwortlich: Andreas Huemmer

26.3.3.1 Zweck

Freigabe von Speicherplatz bei kritischer Disk-Auslastung.

26.3.3.2 Voraussetzungen

- Root/Administrator-Zugriff
- Backup vor größeren Löschungen

26.3.3.3 Geschätzte Dauer

30-60 Minuten

26.3.3.4 Schritte

1. Disk-Auslastung analysieren

```
# Gesamtübersicht
df -h

# Größte Verzeichnisse finden
du -h / | sort -rh | head -20

# Größte Dateien finden
find / -type f -size +100M -exec ls -lh {} \; 2>/dev/null
```

2. Log-Dateien bereinigen

```
# Alte Logs löschen
find /var/log -type f -name "*.log" -mtime +30 -delete

# Komprimierte Logs löschen
find /var/log -type f -name "*.gz" -mtime +90 -delete

# Journal-Logs bereinigen
journalctl --vacuum-time=30d
```

3. Temporäre Dateien löschen

```
# /tmp bereinigen
find /tmp -type f -mtime +7 -delete

# /var/tmp bereinigen
find /var/tmp -type f -mtime +30 -delete
```

4. Package-Cache bereinigen

```
# Debian/Ubuntu
apt-get clean
apt-get autoclean
apt-get autoremove

# RedHat/CentOS
yum clean all

# Docker
docker system prune -a
```

5. Alte Backups archivieren/löschen

```
# Alte Backups identifizieren
find /backup -type f -mtime +90

# Nach Genehmigung löschen
find /backup -type f -mtime +90 -delete
```

26.3.3.5 Validierung

- ☐ Disk-Auslastung unter 80%

- ☐ Kritische Services laufen weiter
 - ☐ Keine wichtigen Daten gelöscht
 - ☐ Monitoring-Alerts gelöst
-

26.4 Datenbank-Management Runbooks

26.4.1 RB-010: Datenbank-Backup

Runbook-ID: RB-010

Version: 1.0

Verantwortlich: Database Administrator

26.4.1.1 Zweck

Manuelles Datenbank-Backup vor kritischen Änderungen.

26.4.1.2 Voraussetzungen

- Datenbank-Admin-Rechte
- Ausreichend Speicherplatz
- Backup-Verzeichnis vorhanden

26.4.1.3 Geschätzte Dauer

15-60 Minuten (abhängig von DB-Größe)

26.4.1.4 Schritte

PostgreSQL:

Full Backup

```
pg_dump -U postgres -F c -b -v -f /backup/db_$(date +%Y%m%d_%H%M%S).backup [database_name]
```

Schema-only Backup

```
pg_dump -U postgres -s -f /backup/schema_$(date +%Y%m%d_%H%M%S).sql [database_name]
```

MySQL/MariaDB:

Full Backup

```
mysqldump -u root -p --single-transaction --routines --triggers [database_name] > /backup/db_$(date +%Y%m%d_%H%M%S).sql
```

All Databases

```
mysqldump -u root -p --all-databases > /backup/all_dbs_$(date +%Y%m%d_%H%M%S).sql
```

MongoDB:

Full Backup

```
mongodump --out /backup/mongodb_$(date +%Y%m%d_%H%M%S)
```

Specific Database

```
mongodump --db [database_name] --out /backup/mongodb_$(date +%Y%m%d_%H%M%S)
```

26.4.1.5 Validierung

- ☐ Backup-Datei erstellt
 - ☐ Backup-Größe plausibel
 - ☐ Backup-Integrität geprüft
 - ☐ Backup-Speicherort dokumentiert
-

26.4.2 RB-011: Datenbank-Restore

Runbook-ID: RB-011

Version: 1.0

Verantwortlich: Database Administrator

26.4.2.1 Zweck

Wiederherstellung einer Datenbank aus Backup.

26.4.2.2 Voraussetzungen

- Datenbank-Admin-Rechte
- Gültiges Backup vorhanden
- Wartungsfenster (für Produktionssysteme)

26.4.2.3 Geschätzte Dauer

30-120 Minuten (abhängig von DB-Größe)

26.4.2.4 Risikobewertung

- **Risiko:** Hoch
- **Impact:** Hoch
- **Rollback möglich:** Ja (mit aktuellem Backup)

26.4.2.5 Schritte

1. Vorbereitung

Aktuelles Backup erstellen (Sicherheit!)
[siehe RB-010]

Benutzer informieren
Services stoppen

2. Restore durchführen

PostgreSQL:

Datenbank löschen und neu erstellen
dropdb [database_name]
createdb [database_name]

```
# Restore
pg_restore -U postgres -d [database_name] -v /backup/db_backup.backup

MySQL/MariaDB:

# Restore
mysql -u root -p [database_name] < /backup/db_backup.sql

MongoDB:

# Restore
mongorestore --db [database_name] /backup/mongodb_backup/[database_name]
```

3. Validierung

```
# Tabellen/Collections prüfen
# Datensätze zählen
# Integrität prüfen
```

26.4.2.6 Validierung

- ☐ Datenbank ist erreichbar
 - ☐ Alle Tabellen/Collections vorhanden
 - ☐ Datensatz-Anzahl plausibel
 - ☐ Anwendung funktioniert
 - ☐ Keine Fehler in Logs
-

26.5 Netzwerk-Management Runbooks

26.5.1 RB-020: Firewall-Regel hinzufügen

Runbook-ID: RB-020

Version: 1.0

Verantwortlich: Thomas Weber

26.5.1.1 Zweck

Hinzufügen einer neuen Firewall-Regel.

26.5.1.2 Voraussetzungen

- Firewall-Admin-Rechte
- Change-Ticket genehmigt
- Regel-Details dokumentiert

26.5.1.3 Geschätzte Dauer

15-30 Minuten

26.5.1.4 Schritte

1. Regel-Details dokumentieren

- Quell-IP/Netzwerk
- Ziel-IP/Netzwerk
- Port/Protokoll
- Aktion (Allow/Deny)
- Begründung

2. Regel hinzufügen

iptables (Linux):

Regel hinzufügen

```
iptables -A INPUT -s [source_ip] -p tcp --dport [port] -j ACCEPT
```

Regel speichern

```
iptables-save > /etc/iptables/rules.v4
```

firewalld (Linux):

Port öffnen

```
firewall-cmd --permanent --add-port=[port]/tcp
```

Reload

```
firewall-cmd --reload
```

Windows Firewall:

Regel hinzufügen

```
New-NetFirewallRule -DisplayName "[Rule Name]" -Direction Inbound -Protocol TCP -LocalPort
```

3. Validierung

Regel prüfen

```
iptables -L -n -v
```

Konnektivität testen

```
telnet [target_ip] [port]
```

```
nc -zv [target_ip] [port]
```

26.5.1.5 Validierung

- ☐ Regel ist aktiv
 - ☐ Konnektivität funktioniert
 - ☐ Keine unerwünschten Nebeneffekte
 - ☐ Regel dokumentiert
-

26.6 Benutzer-Management Runbooks

26.6.1 RB-030: Benutzer-Account erstellen

Runbook-ID: RB-030

Version: 1.0

Verantwortlich: Andreas Huemmer

26.6.1.1 Zweck

Erstellung eines neuen Benutzer-Accounts.

26.6.1.2 Voraussetzungen

- Admin-Rechte
- Genehmigtes Ticket
- Benutzer-Details vorhanden

26.6.1.3 Geschätzte Dauer

10-15 Minuten

26.6.1.4 Schritte

1. Benutzer-Details sammeln

- Vollständiger Name
- E-Mail-Adresse
- Abteilung
- Erforderliche Gruppen/Rollen
- Manager/Genehmiger

2. Account erstellen

Linux:

Benutzer erstellen

```
useradd -m -s /bin/bash -c "[Full Name]" [username]
```

Passwort setzen

```
passwd [username]
```

Zu Gruppen hinzufügen

```
usermod -aG [group1],[group2] [username]
```

Active Directory:

Benutzer erstellen

```
New-ADUser -Name "[Full Name]" -GivenName "[First]" -Surname "[Last]" -  
-SamAccountName [username] -UserPrincipalName [username]@domain.com -  
-Path "OU=Users,DC=domain,DC=com" -AccountPassword (ConvertTo-SecureString "[password]"  
-Enabled $true
```

Zu Gruppen hinzufügen

```
Add-ADGroupMember -Identity "[Group Name]" -Members [username]
```

3. Berechtigungen zuweisen

- Dateisystem-Berechtigungen
- Anwendungs-Zugriffe
- E-Mail-Account
- VPN-Zugang

4. Benutzer informieren

- Willkommens-E-Mail senden
- Zugangsdaten übermitteln (sicher!)
- Dokumentation bereitstellen

26.6.1.5 Validierung

- ☐ Account ist aktiv
 - ☐ Login funktioniert
 - ☐ Berechtigungen korrekt
 - ☐ Benutzer informiert
 - ☐ Dokumentiert in CMDB
-

26.6.2 RB-031: Benutzer-Account deaktivieren

Runbook-ID: RB-031

Version: 1.0

Verantwortlich: Andreas Huemmer

26.6.2.1 Zweck

Deaktivierung eines Benutzer-Accounts (z.B. bei Austritt).

26.6.2.2 Voraussetzungen

- Admin-Rechte
- Genehmigtes Ticket
- Offboarding-Checkliste

26.6.2.3 Geschätzte Dauer

20-30 Minuten

26.6.2.4 Schritte

1. Account deaktivieren

Linux:

```
# Account sperren
```

```
usermod -L [username]
```

```
passwd -l [username]
```

```
# Shell deaktivieren
```

```
usermod -s /sbin/nologin [username]
```

Active Directory:

```
# Account deaktivieren
```

```
Disable-ADAccount -Identity [username]
```

```
# Beschreibung aktualisieren
```

```
Set-ADUser -Identity [username] -Description "Deactivated on $(Get-Date -Format 'yyyy-MM-d
```

2. Zugriffe entfernen

- VPN-Zugang deaktivieren
- E-Mail-Weiterleitung einrichten
- Gruppen-Mitgliedschaften entfernen
- Anwendungs-Zugriffe widerrufen
- Hardware zurückfordern

3. Daten sichern

- Home-Verzeichnis archivieren
- E-Mails archivieren
- Wichtige Dateien sichern

4. Dokumentation

- Offboarding-Checkliste abarbeiten
- CMDB aktualisieren
- Manager informieren

26.6.2.5 Validierung

- ☐ Account ist deaktiviert
- ☐ Login nicht mehr möglich
- ☐ Alle Zugriffe entfernt
- ☐ Daten gesichert
- ☐ Dokumentiert

26.7 Monitoring und Alerting Runbooks

26.7.1 RB-040: Alert-Untersuchung

Runbook-ID: RB-040

Version: 1.0

Verantwortlich: Andreas Huemmer

26.7.1.1 Zweck

Systematische Untersuchung eines Monitoring-Alerts.

26.7.1.2 Voraussetzungen

- Zugriff auf Monitoring-System
- Zugriff auf betroffene Systeme

26.7.1.3 Geschätzte Dauer

15-60 Minuten

26.7.1.4 Schritte

1. Alert-Details erfassen

- Alert-Name und Severity
- Betroffenes System/Service
- Zeitpunkt des Auftretens
- Alert-Beschreibung

2. Erste Analyse

```
# System-Status prüfen
uptime
top
df -h
free -m

# Service-Status prüfen
systemctl status [service]

# Logs prüfen
journalctl -xe
tail -f /var/log/[relevant_log]
```

3. Ursache identifizieren

- Korrelation mit anderen Events
- Änderungen in letzter Zeit
- Bekannte Probleme prüfen
- Metriken analysieren

4. Maßnahmen ergreifen

- Sofortmaßnahmen (falls erforderlich)
- Incident-Ticket erstellen
- Eskalation (falls erforderlich)
- Dokumentation

5. Validierung

- Alert ist gelöst

- System funktioniert normal
- Keine weiteren Alerts

26.7.1.5 Troubleshooting-Matrix

Alert-Typ	Erste Prüfung	Häufige Ursachen	Sofortmaßnahme
High CPU	top, ps aux	Runaway-Prozess	Prozess beenden
High Memory	free -m, ps aux	Memory-Leak	Service-Neustart
Disk Full	df -h, du -h	Log-Dateien, Backups	Cleanup durchführen
Service Down	systemctl status	Crash, Config-Fehler	Service-Neustart
High Latency	ping, traceroute	Netzwerk, Last	Load-Balancing prüfen

26.8 Backup und Recovery Runbooks

26.8.1 RB-050: Backup-Verifikation

Runbook-ID: RB-050

Version: 1.0

Verantwortlich: Andreas Huemmer

26.8.1.1 Zweck

Regelmäßige Überprüfung der Backup-Integrität.

26.8.1.2 Voraussetzungen

- Zugriff auf Backup-System
- Test-Umgebung verfügbar

26.8.1.3 Geschätzte Dauer

30-60 Minuten

26.8.1.4 Schritte

1. Backup-Status prüfen

```
# Letzte Backups anzeigen
[backup_tool] list --last 7

# Backup-Logs prüfen
tail -100 /var/log/backup.log
```

2. Backup-Integrität prüfen

```
# Checksummen validieren
[backup_tool] verify [backup_id]
```

```
# Backup-Größe prüfen  
ls -lh /backup/
```

3. Restore-Test durchführen

- Zufälliges Backup auswählen
- In Test-Umgebung wiederherstellen
- Funktionalität validieren
- Ergebnis dokumentieren

4. Dokumentation

- Test-Ergebnis festhalten
- Probleme dokumentieren
- Verbesserungen identifizieren

26.8.1.5 Validierung

- ☐ Alle Backups erfolgreich
 - ☐ Integrität bestätigt
 - ☐ Restore-Test erfolgreich
 - ☐ Dokumentiert
-

26.9 Troubleshooting-Guides

26.9.1 Allgemeine Troubleshooting-Methodik

1. Problem identifizieren

- Symptome sammeln
- Fehlermeldungen notieren
- Zeitpunkt des Auftretens

2. Informationen sammeln

- Logs analysieren
- Monitoring-Daten prüfen
- Änderungen identifizieren

3. Hypothese bilden

- Mögliche Ursachen auflisten
- Wahrscheinlichkeit bewerten
- Priorisieren

4. Testen

- Hypothese testen
- Ergebnisse dokumentieren
- Nächste Hypothese

5. Lösung implementieren

- Korrekturmaßnahme durchführen
- Validieren
- Dokumentieren

6. Prävention

- Root-Cause-Analysis

- Verbesserungen identifizieren
- Implementieren

26.9.2 Häufige Probleme und Lösungen

26.9.2.1 Problem: Service startet nicht

Symptome: - Service-Status: failed - Fehlermeldung in Logs

Diagnose:

Status prüfen

```
systemctl status [service]
```

Logs prüfen

```
journalctl -u [service] -n 50
```

Config-Test

```
[service] -t # (z.B. nginx -t, apache2ctl configtest)
```

Lösungen: 1. Config-Fehler korrigieren 2. Dependencies prüfen 3. Berechtigungen prüfen 4. Ports prüfen (bereits belegt?)

26.9.2.2 Problem: Hohe CPU-Last

Symptome: - CPU-Auslastung > 80% - System langsam

Diagnose:

Top-Prozesse identifizieren

```
top
```

```
htop
```

Prozess-Details

```
ps aux | sort -nrk 3,3 | head -n 5
```

Lösungen: 1. Runaway-Prozess beenden 2. Ressourcen-Limits setzen 3. Skalierung prüfen 4. Code-Optimierung

26.9.2.3 Problem: Disk voll

Symptome: - Disk-Auslastung > 90% - "No space left on device" Fehler

Diagnose:

Auslastung prüfen

```
df -h
```

Große Dateien finden

```
du -h / | sort -rh | head -20
find / -type f -size +100M
```

Lösungen: 1. Logs bereinigen 2. Temporäre Dateien löschen 3. Alte Backups archivieren 4. Storage erweitern

26.10 Prozesse und Verantwortlichkeiten

26.10.1 RACI-Matrix

Aktivität	CIO	Ops Manager	Ops Team	On-Call
Runbook-Erstellung	C	A	R	C
Runbook-Ausführung	I	C	R	R
Runbook-Aktualisierung	I	A	R	C
Troubleshooting	I	C	R	R

Legende: R = Responsible, A = Accountable, C = Consulted, I = Informed

26.11 Compliance und Standards

26.11.1 Relevante Standards

- **ITIL v4:** Service Operation Practice
 - **ISO 20000:** Clause 8.1 - Operational Planning and Control
 - **COBIT 2019:** DSS01 - Managed Operations
-

26.12 Anhang

26.12.1 Glossar

Begriff	Definition
Runbook	Dokumentierte Schritt-für-Schritt-Anleitung für Standardoperationen
Troubleshooting	Systematische Fehlersuche und -behebung
Standard Operating Procedure (SOP)	Standardisierte Betriebsanweisung

26.12.2 Referenzen

- ITIL v4 Foundation Handbook
 - ISO/IEC 20000-1:2018
 - COBIT 2019 Framework
-

Letzte Aktualisierung: {{ meta.date }}
Nächste Review: [TODO: Datum]
Kontakt: andreas.huemmer@adminsind.de
ewpage

Chapter 27

Tooling und Zugangswege

27.1 Übersicht

Dieses Dokument beschreibt die verwendeten Tools und Systeme, Zugriffswege und URLs sowie Authentifizierungsmethoden für den IT-Service. Ziel ist es, einen zentralen Überblick über alle relevanten Werkzeuge und deren Zugang zu bieten.

Dokumentverantwortlicher: IT Operations Manager

Genehmigt durch: CIO

Version: 1.0.0

Organisation: AdminSend GmbH

27.2 Tool-Kategorien

27.2.1 Übersicht der Tool-Kategorien

Kategorie	Anzahl Tools	Hauptverantwortlich	Kritikalität
Monitoring & Observability	[TODO]	Andreas Huemmer	Hoch
Infrastructure Management	[TODO]	Andreas Huemmer	Hoch
Security & Compliance	[TODO]	Thomas Weber	Hoch
Development & Deployment	[TODO]	Andreas Huemmer	Mittel
Collaboration & Communication	[TODO]	Peter Fischer	Mittel
Documentation & Knowledge	[TODO]	Andreas Huemmer	Mittel
Backup & Recovery	[TODO]	Andreas Huemmer	Hoch

27.3 Monitoring und Observability

27.3.1 System-Monitoring

27.3.1.1 [TODO: Monitoring-Tool Name]

- **Zweck:** System- und Infrastruktur-Monitoring
- **URL:** [TODO: <https://monitoring.example.com>]
- **Zugriff:** VPN + SSO
- **Authentifizierung:** AdminSend GmbH SSO
- **Verantwortlich:** Andreas Huemmer
- **Support:** [TODO: Support-Kontakt]
- **Dokumentation:** [TODO: Dokumentations-URL]

Hauptfunktionen: - Server-Monitoring (CPU, RAM, Disk, Network) - Service-Monitoring (Up-time, Response Time) - Alerting und Notifications - Dashboards und Visualisierung

Zugriffsberechtigung: - **Admin:** IT Operations Manager, Senior Engineers - **Read/Write:** Operations Team - **Read-Only:** Management, Stakeholder

27.3.2 Application Performance Monitoring (APM)

27.3.2.1 [TODO: APM-Tool Name]

- **Zweck:** Anwendungs-Performance-Überwachung
- **URL:** [TODO: <https://apm.example.com>]
- **Zugriff:** VPN + SSO
- **Authentifizierung:** AdminSend GmbH SSO
- **Verantwortlich:** Andreas Huemmer
- **Support:** [TODO: Support-Kontakt]

Hauptfunktionen: - Transaction-Tracing - Error-Tracking - Performance-Metriken - User-Experience-Monitoring

27.3.3 Log-Management

27.3.3.1 [TODO: Log-Management-Tool Name]

- **Zweck:** Zentrale Log-Aggregation und -Analyse
- **URL:** [TODO: <https://logs.example.com>]
- **Zugriff:** VPN + SSO
- **Authentifizierung:** AdminSend GmbH SSO
- **Verantwortlich:** Andreas Huemmer
- **Support:** [TODO: Support-Kontakt]

Hauptfunktionen: - Log-Aggregation von allen Systemen - Log-Suche und -Filterung - Log-Analyse und Visualisierung - Alerting auf Log-Patterns

27.4 Infrastructure Management

27.4.1 Configuration Management Database (CMDB)

27.4.1.1 NetBox

- **Zweck:** CMDB und IPAM
- **URL:** {{ netbox.url }}
- **Zugriff:** VPN + Username/Password
- **Authentifizierung:** Lokale Accounts oder LDAP
- **Verantwortlich:** Andreas Huemmer
- **API:** {{ netbox.api_url }}
- **Dokumentation:** <https://docs.netbox.dev/>

Hauptfunktionen: - Geräte-Inventar - IP-Adress-Management (IPAM) - Rack-Management - Kabel-Dokumentation - Virtualisierungs-Tracking

Zugriffsberechtigung: - **Admin:** IT Operations Manager - **Read/Write:** Operations Team, Network Team - **Read-Only:** Management, Auditors

27.4.2 Virtualisierung

27.4.2.1 [TODO: Hypervisor-Management]

- **Zweck:** Virtualisierungs-Management
- **URL:** [TODO: <https://vcenter.example.com>]
- **Zugriff:** VPN + Username/Password
- **Authentifizierung:** Lokale Accounts oder AD
- **Verantwortlich:** Andreas Huemmer
- **Support:** [TODO: Support-Kontakt]

Hauptfunktionen: - VM-Verwaltung - Resource-Allocation - Snapshot-Management - Migration und HA

27.4.3 Container-Orchestrierung

27.4.3.1 [TODO: Container-Plattform]

- **Zweck:** Container-Orchestrierung
- **URL:** [TODO: <https://k8s.example.com>]
- **Zugriff:** VPN + kubectl + Token
- **Authentifizierung:** Service-Accounts, RBAC
- **Verantwortlich:** Andreas Huemmer
- **Support:** [TODO: Support-Kontakt]

Hauptfunktionen: - Container-Deployment - Service-Discovery - Load-Balancing - Auto-Scaling

27.4.4 Cloud-Management

27.4.4.1 [TODO: Cloud-Provider Console]

- **Zweck:** Cloud-Ressourcen-Management
- **URL:** [TODO: <https://console.cloud-provider.com>]
- **Zugriff:** Internet + MFA
- **Authentifizierung:** Cloud-Provider-Accounts + MFA
- **Verantwortlich:** Anna Schmidt
- **Support:** Cloud-Provider-Support

Hauptfunktionen: - Compute-Ressourcen - Storage-Management - Networking - IAM und Security

27.5 Security und Compliance

27.5.1 Security Information and Event Management (SIEM)

27.5.1.1 [TODO: SIEM-Tool Name]

- **Zweck:** Security-Event-Monitoring und -Analyse
- **URL:** [TODO: <https://siem.example.com>]
- **Zugriff:** VPN + SSO
- **Authentifizierung:** AdminSend GmbH SSO
- **Verantwortlich:** Thomas Weber
- **Support:** [TODO: Support-Kontakt]

Hauptfunktionen: - Security-Event-Aggregation - Threat-Detection - Incident-Response - Compliance-Reporting

27.5.2 Vulnerability Management

27.5.2.1 [TODO: Vulnerability-Scanner]

- **Zweck:** Schwachstellen-Scanning
- **URL:** [TODO: <https://vuln.example.com>]
- **Zugriff:** VPN + Username/Password
- **Authentifizierung:** Lokale Accounts
- **Verantwortlich:** Thomas Weber
- **Support:** [TODO: Support-Kontakt]

Hauptfunktionen: - Vulnerability-Scanning - Patch-Management - Compliance-Checks - Reporting

27.5.3 Identity and Access Management (IAM)

27.5.3.1 Active Directory / LDAP

- **Zweck:** Zentrale Benutzerverwaltung
- **URL:** [TODO: ldap://ad.example.com]
- **Zugriff:** Intern + VPN
- **Authentifizierung:** Admin-Accounts
- **Verantwortlich:** Andreas Huemmer
- **Support:** [TODO: Support-Kontakt]

Hauptfunktionen: - Benutzerverwaltung - Gruppenverwaltung - Authentifizierung - Autorisierung

27.5.4 Multi-Factor Authentication (MFA)

27.5.4.1 [TODO: MFA-Solution]

- **Zweck:** Zwei-Faktor-Authentifizierung
- **URL:** [TODO: https://mfa.example.com]
- **Zugriff:** Internet
- **Authentifizierung:** Username + MFA-Token
- **Verantwortlich:** Thomas Weber
- **Support:** [TODO: Support-Kontakt]

Hauptfunktionen: - MFA-Enrollment - Token-Management - Push-Notifications - Backup-Codes

27.6 Development und Deployment

27.6.1 Version Control

27.6.1.1 [TODO: Git-Platform]

- **Zweck:** Source-Code-Management
- **URL:** [TODO: https://git.example.com]
- **Zugriff:** VPN + SSO
- **Authentifizierung:** AdminSend GmbH SSO + SSH-Keys
- **Verantwortlich:** Andreas Huemmer
- **Support:** [TODO: Support-Kontakt]

Hauptfunktionen: - Git-Repositories - Code-Review - CI/CD-Integration - Issue-Tracking

27.6.2 CI/CD Pipeline

27.6.2.1 [TODO: CI/CD-Tool]

- **Zweck:** Continuous Integration/Deployment
- **URL:** [TODO: https://ci.example.com]
- **Zugriff:** VPN + SSO

- **Authentifizierung:** AdminSend GmbH SSO
- **Verantwortlich:** Andreas Huemmer
- **Support:** [TODO: Support-Kontakt]

Hauptfunktionen: - Build-Automation - Test-Automation - Deployment-Automation - Pipeline-Management

27.6.3 Artifact Repository

27.6.3.1 [TODO: Artifact-Repository]

- **Zweck:** Binary-Artifact-Storage
- **URL:** [TODO: <https://artifacts.example.com>]
- **Zugriff:** VPN + Token
- **Authentifizierung:** API-Tokens
- **Verantwortlich:** Andreas Huemmer
- **Support:** [TODO: Support-Kontakt]

Hauptfunktionen: - Package-Management - Container-Registry - Dependency-Management - Version-Management

27.7 Collaboration und Communication

27.7.1 Ticketing-System

27.7.1.1 [TODO: Ticketing-Tool]

- **Zweck:** Incident- und Request-Management
- **URL:** [TODO: <https://tickets.example.com>]
- **Zugriff:** Internet + SSO
- **Authentifizierung:** AdminSend GmbH SSO
- **Verantwortlich:** Andreas Huemmer
- **Support:** [TODO: Support-Kontakt]

Hauptfunktionen: - Incident-Management - Request-Management - Change-Management - SLA-Tracking

27.7.2 Team-Kommunikation

27.7.2.1 [TODO: Chat-Platform]

- **Zweck:** Team-Kommunikation und Collaboration
- **URL:** [TODO: <https://chat.example.com>]
- **Zugriff:** Internet + SSO
- **Authentifizierung:** AdminSend GmbH SSO
- **Verantwortlich:** Peter Fischer
- **Support:** [TODO: Support-Kontakt]

Hauptfunktionen: - Team-Chat - Channels und Direct Messages - File-Sharing - Integration mit anderen Tools

27.7.3 Video-Conferencing

27.7.3.1 [TODO: Video-Tool]

- **Zweck:** Video-Konferenzen
- **URL:** [TODO: <https://meet.example.com>]
- **Zugriff:** Internet
- **Authentifizierung:** AdminSend GmbH SSO
- **Verantwortlich:** Peter Fischer
- **Support:** [TODO: Support-Kontakt]

Hauptfunktionen: - Video-Calls - Screen-Sharing - Recording - Chat

27.8 Documentation und Knowledge Management

27.8.1 Wiki / Knowledge Base

27.8.1.1 [TODO: Wiki-Plattform]

- **Zweck:** Dokumentation und Wissensdatenbank
- **URL:** [TODO: <https://wiki.example.com>]
- **Zugriff:** VPN + SSO
- **Authentifizierung:** AdminSend GmbH SSO
- **Verantwortlich:** Andreas Huemmer
- **Support:** [TODO: Support-Kontakt]

Hauptfunktionen: - Dokumentations-Management - Wissensartikel - Suche und Navigation - Versionierung

27.8.2 Diagramm-Tool

27.8.2.1 [TODO: Diagramming-Tool]

- **Zweck:** Architektur- und Netzwerk-Diagramme
- **URL:** [TODO: <https://diagrams.example.com>]
- **Zugriff:** Internet + SSO
- **Authentifizierung:** AdminSend GmbH SSO
- **Verantwortlich:** Andreas Huemmer
- **Support:** [TODO: Support-Kontakt]

Hauptfunktionen: - Diagramm-Erstellung - Collaboration - Export in verschiedene Formate - Versionierung

27.9 Backup und Recovery

27.9.1 Backup-System

27.9.1.1 [TODO: Backup-Solution]

- **Zweck:** Backup und Recovery
- **URL:** [TODO: <https://backup.example.com>]
- **Zugriff:** VPN + Username/Password
- **Authentifizierung:** Lokale Accounts
- **Verantwortlich:** Andreas Huemmer
- **Support:** [TODO: Support-Kontakt]

Hauptfunktionen: - Backup-Scheduling - Backup-Monitoring - Restore-Funktionen - Retention-Management

27.10 Zugangswege

27.10.1 VPN-Zugang

27.10.1.1 Corporate VPN

- **Zweck:** Sicherer Remote-Zugriff
- **URL:** [TODO: <https://vpn.example.com>]
- **Client:** [TODO: VPN-Client-Name]
- **Authentifizierung:** AdminSend GmbH AD + MFA
- **Verantwortlich:** Thomas Weber
- **Support:** julia.becker@adminsends.de

Verbindungsanleitung: 1. VPN-Client installieren 2. Profil importieren/konfigurieren 3. Mit AD-Credentials + MFA verbinden 4. Verbindung validieren

Troubleshooting: - **Problem:** Verbindung schlägt fehl - **Lösung:** Credentials prüfen, MFA-Token prüfen, Netzwerk prüfen - **Problem:** Langsame Verbindung - **Lösung:** Anderen VPN-Gateway wählen, Split-Tunneling prüfen

27.10.2 SSH-Zugang

27.10.2.1 SSH-Bastion-Host

- **Zweck:** Sicherer SSH-Zugang zu Servern
- **Hostname:** [TODO: bastion.example.com]
- **Port:** 22
- **Authentifizierung:** SSH-Keys + MFA
- **Verantwortlich:** Andreas Huemmer

Verbindungsanleitung:

```
# SSH-Key generieren (falls nicht vorhanden)
ssh-keygen -t ed25519 -C "your_email@example.com"
```

```
# Public Key zum Bastion-Host hinzufügen
# (durch Admin)

# Verbindung zum Bastion-Host
ssh -i ~/.ssh/id_ed25519 username@bastion.example.com

# Von Bastion zu Ziel-Server
ssh username@target-server
```

27.10.3 Remote Desktop

27.10.3.1 RDP-Gateway

- **Zweck:** Remote-Desktop-Zugriff auf Windows-Server
- **URL:** [TODO: https://rdp.example.com]
- **Authentifizierung:** AdminSend GmbH AD + MFA
- **Verantwortlich:** Andreas Huemmer

Verbindungsanleitung: 1. RDP-Client öffnen 2. Gateway-Adresse eingeben 3. Mit AD-Credentials + MFA authentifizieren 4. Ziel-Server auswählen

27.11 Authentifizierungsmethoden

27.11.1 Single Sign-On (SSO)

27.11.1.1 AdminSend GmbH SSO

- **Provider:** [TODO: SSO-Provider]
- **Protokoll:** SAML 2.0 / OAuth 2.0 / OpenID Connect
- **MFA:** Erforderlich für alle externen Zugriffe
- **Session-Timeout:** 8 Stunden
- **Verantwortlich:** Thomas Weber

Unterstützte Anwendungen: - [TODO: Liste der SSO-integrierten Anwendungen]

27.11.2 API-Authentifizierung

27.11.2.1 API-Tokens

- **Verwendung:** Programmatischer Zugriff auf APIs
- **Generierung:** Über jeweiliges Tool-Interface
- **Rotation:** Alle 90 Tage
- **Speicherung:** Secrets-Management-System
- **Verantwortlich:** Andreas Huemmer

Best Practices: - Tokens niemals in Code committen - Minimale Berechtigungen (Least Privilege)
- Regelmäßige Rotation - Monitoring der Token-Nutzung

27.11.3 SSH-Keys

27.11.3.1 SSH-Key-Management

- **Key-Typ:** ED25519 (bevorzugt) oder RSA 4096
- **Passphrase:** Erforderlich
- **Rotation:** Jährlich
- **Speicherung:** Lokal, verschlüsselt
- **Verantwortlich:** Andreas Huemmer

Key-Generierung:

```
# ED25519 (empfohlen)
ssh-keygen -t ed25519 -C "your_email@example.com"

# RSA 4096 (alternativ)
ssh-keygen -t rsa -b 4096 -C "your_email@example.com"
```

27.12 Tool-Zugriffs-Matrix

27.12.1 Zugriffsberechtigung nach Rolle

Tool	Ops Manager	Ops Team	Security Team	Management	Auditor
Monitoring	Admin	Read/Write	Read	Read	Read
CMDB (NetBox)	Admin	Read/Write	Read	Read	Read
SIEM	Read	Read	Admin	Read	Read
Backup-System	Admin	Read/Write	Read	-	Read
Cloud-Console	Admin	Read/Write	Read	Read	-
Ticketing	Admin	Read/Write	Read/Write	Read	Read
Wiki	Admin	Read/Write	Read/Write	Read	Read
VPN	Ja	Ja	Ja	Ja	Ja
SSH-Bastion	Ja	Ja	Ja	-	-

27.13 Notfall-Zugänge

27.13.1 Break-Glass-Accounts

27.13.1.1 Emergency-Admin-Account

- **Zweck:** Notfall-Zugriff bei SSO-Ausfall
- **Speicherung:** Versiegelter Umschlag im Safe

- **Zugriff:** Nur durch Anna Schmidt oder Thomas Weber
- **Protokollierung:** Jede Nutzung wird geloggt und reviewt
- **Passwort-Rotation:** Quartalsweise

Nutzungsprozess: 1. Notfall identifizieren und dokumentieren 2. Genehmigung durch CIO/CISO einholen 3. Umschlag öffnen und dokumentieren 4. Zugriff durchführen 5. Alle Aktionen protokollieren 6. Passwort ändern und neuen Umschlag versiegeln 7. Incident-Report erstellen

27.14 Tool-Lifecycle-Management

27.14.1 Tool-Bewertung

27.14.1.1 Neue Tools evaluieren

1. **Anforderungsanalyse:** Bedarf identifizieren
2. **Marktanalyse:** Verfügbare Lösungen recherchieren
3. **Proof of Concept:** Top 3 Lösungen testen
4. **Bewertung:** Funktionalität, Kosten, Integration
5. **Entscheidung:** Tool auswählen
6. **Implementierung:** Rollout planen und durchführen

27.14.1.2 Tool-Review

- **Frequenz:** Jährlich
- **Kriterien:**
 - Nutzung und Akzeptanz
 - Kosten-Nutzen-Verhältnis
 - Technische Aktualität
 - Support-Qualität
 - Integration mit anderen Tools

27.15 Prozesse und Verantwortlichkeiten

27.15.1 RACI-Matrix

Aktivität	CIO	CISO	Ops Manager	Ops Team
Tool-Auswahl	A	C	R	C
Tool-Implementierung	C	C	A	R
Zugriffsverwaltung	C	A	R	I
Tool-Wartung	I	C	A	R
Tool-Review	A	C	R	C
Notfall-Zugang	A	A	C	I

Legende: R = Responsible, A = Accountable, C = Consulted, I = Informed

27.16 Compliance und Standards

27.16.1 Relevante Standards

- **ISO 27001:** A.9 - Access Control
- **ISO 27001:** A.12 - Operations Security
- **COBIT 2019:** DSS05 - Managed Security Services

27.16.2 Audit-Anforderungen

- Tool-Inventar
 - Zugriffsprotokolle
 - Authentifizierungs-Logs
 - Notfall-Zugriffs-Dokumentation
-

27.17 Anhang

27.17.1 Glossar

Begriff	Definition
SSO	Single Sign-On - Einmalige Anmeldung für mehrere Systeme
MFA	Multi-Factor Authentication - Mehr-Faktor-Authentifizierung
VPN	Virtual Private Network - Virtuelles privates Netzwerk
API	Application Programming Interface - Programmierschnittstelle
CMDB	Configuration Management Database - Konfigurationsdatenbank
SIEM	Security Information and Event Management

27.17.2 Referenzen

- ISO/IEC 27001:2013
 - COBIT 2019 Framework
 - NIST Cybersecurity Framework
-

Letzte Aktualisierung: {{ meta.date }}

Nächste Review: [TODO: Datum]

Kontakt: andreas.huemmer@adminsends.de

ewpage

Chapter 28

Bekannte Probleme und FAQ

28.1 Übersicht

Dieses Dokument enthält bekannte Probleme und Workarounds, häufig gestellte Fragen (FAQ) sowie Troubleshooting-Tipps für den IT-Service. Ziel ist es, schnelle Lösungen für wiederkehrende Probleme bereitzustellen und die Effizienz des Supports zu erhöhen.

Dokumentverantwortlicher: IT Operations Manager

Genehmigt durch: CIO

Version: 1.0.0

Organisation: AdminSend GmbH

28.2 Bekannte Probleme

28.2.1 Problem-Tracking

Alle bekannten Probleme werden im Ticketing-System mit dem Label “Known Issue” erfasst und hier dokumentiert.

Verantwortlich: Andreas Huemmer

Review-Zyklus: Monatlich

28.2.2 KI-001: [TODO: Problem-Titel]

Status: Offen / In Bearbeitung / Gelöst

Priorität: P1 (Kritisch) / P2 (Hoch) / P3 (Mittel) / P4 (Niedrig)

Erstellt: [TODO: Datum]

Letzte Aktualisierung: [TODO: Datum]

Ticket-ID: [TODO: Ticket-Nummer]

28.2.2.1 Beschreibung

[TODO: Detaillierte Beschreibung des Problems]

28.2.2.2 Betroffene Systeme

- [TODO: System 1]
- [TODO: System 2]

28.2.2.3 Symptome

- [TODO: Symptom 1]
- [TODO: Symptom 2]

28.2.2.4 Root Cause

[TODO: Ursache des Problems, falls bekannt]

28.2.2.5 Workaround

[TODO: Schritt-für-Schritt-Workaround]

1. Schritt 1
2. Schritt 2
3. Schritt 3

28.2.2.6 Permanente Lösung

- **Status:** Geplant / In Entwicklung / Getestet / Deployed
- **ETA:** [TODO: Voraussichtliches Datum]
- **Verantwortlich:** [TODO: Name]

28.2.2.7 Betroffene Benutzer

[TODO: Anzahl oder Beschreibung der betroffenen Benutzer]

28.2.2.8 Kommunikation

- [TODO: Datum] - Benutzer informiert
- [TODO: Datum] - Update kommuniziert
- [TODO: Datum] - Lösung kommuniziert

28.2.3 KI-002: Intermittierende Netzwerk-Timeouts

Status: In Bearbeitung

Priorität: P2 (Hoch)

Erstellt: 2025-01-15

Letzte Aktualisierung: 2025-01-28

Ticket-ID: INC-12345

28.2.3.1 Beschreibung

Benutzer erleben sporadische Netzwerk-Timeouts beim Zugriff auf interne Anwendungen. Die Timeouts treten unregelmäßig auf und dauern 30-60 Sekunden.

28.2.3.2 Betroffene Systeme

- Intranet-Portal
- File-Server
- E-Mail-System

28.2.3.3 Symptome

- Verbindungsabbrüche ohne Fehlermeldung
- Langsame Ladezeiten
- Timeout-Fehler nach 30-60 Sekunden

28.2.3.4 Root Cause

Überlastung des Core-Switches während Backup-Zeiten (22:00-02:00 Uhr).

28.2.3.5 Workaround

1. Kritische Arbeiten außerhalb der Backup-Zeiten durchführen
2. Bei Timeout: Seite neu laden (F5)
3. Alternative Route über VPN nutzen (falls verfügbar)

28.2.3.6 Permanente Lösung

- **Status:** Geplant
- **ETA:** Q2 2026
- **Maßnahme:** Upgrade des Core-Switches auf höhere Bandbreite
- **Verantwortlich:** Andreas Huemmer

28.2.3.7 Betroffene Benutzer

Alle internen Benutzer während Backup-Zeiten

28.2.4 KI-003: Langsame Datenbank-Queries

Status: Gelöst

Priorität: P2 (Hoch)

Erstellt: 2025-01-10

Gelöst: 2025-01-25

Ticket-ID: INC-12340

28.2.4.1 Beschreibung

Bestimmte Datenbank-Queries liefen sehr langsam (> 10 Sekunden), was zu Timeouts in der Anwendung führte.

28.2.4.2 Betroffene Systeme

- Produktions-Datenbank
- Web-Anwendung

28.2.4.3 Symptome

- Langsame Seitenladezeiten
- Timeout-Fehler
- Hohe CPU-Last auf DB-Server

28.2.4.4 Root Cause

Fehlende Indizes auf häufig abgefragten Tabellen.

28.2.4.5 Lösung

```
-- Fehlende Indizes hinzugefügt
CREATE INDEX idx_users_email ON users(email);
CREATE INDEX idx_orders_date ON orders(order_date);
CREATE INDEX idx_products_category ON products(category_id);

-- Statistiken aktualisiert
ANALYZE TABLE users;
ANALYZE TABLE orders;
ANALYZE TABLE products;
```

28.2.4.6 Ergebnis

- Query-Zeit reduziert von 10+ Sekunden auf < 100ms
 - CPU-Last auf DB-Server normalisiert
 - Keine Timeouts mehr
-

28.3 Häufig gestellte Fragen (FAQ)

28.3.1 Allgemeine Fragen

28.3.1.1 F: Wie erreiche ich den IT-Support?

A: Der IT-Support ist über folgende Kanäle erreichbar: - **E-Mail:** julia.becker@adminsends.de
- **Telefon:** +49 89 12345678-111 - **Ticketing-System:** [TODO: URL] - **Chat:** [TODO: Chat-Kanal]

Support-Zeiten: - Mo-Fr: 08:00-18:00 Uhr - 24/7 für kritische Incidents (P1)

28.3.1.2 F: Wie erstelle ich ein Support-Ticket?

A: Support-Tickets können über folgende Wege erstellt werden:

1. Web-Portal:

- [TODO: Ticketing-URL] aufrufen
- Mit SSO anmelden
- "Neues Ticket" klicken

- Formular ausfüllen und absenden
- 2. **E-Mail:**
 - E-Mail an julia.becker@adminsind.de
 - Betreff: Kurze Problembeschreibung
 - Inhalt: Detaillierte Beschreibung, Screenshots
- 3. **Telefon:**
 - +49 89 12345678-111 anrufen
 - Problem schildern
 - Ticket-Nummer notieren

28.3.1.3 F: Wie priorisiert der Support Tickets?

A: Tickets werden nach folgenden Prioritäten bearbeitet:

Priorität	Beschreibung	Reaktionszeit	Lösungszeit
P1 - Kritisch	Kompletter Systemausfall	15 Minuten	4 Stunden
P2 - Hoch	Teilausfall, viele Benutzer betroffen	1 Stunde	8 Stunden
P3 - Mittel	Einzelne Benutzer betroffen	4 Stunden	24 Stunden
P4 - Niedrig	Fragen, Feature-Requests	8 Stunden	72 Stunden

28.3.2 Zugriff und Authentifizierung

28.3.2.1 F: Ich habe mein Passwort vergessen. Was soll ich tun?

A: Passwort-Reset über Self-Service-Portal:

1. [TODO: Self-Service-URL] aufrufen
2. "Passwort vergessen" klicken
3. Benutzername oder E-Mail eingeben
4. Sicherheitsfragen beantworten oder Code per E-Mail/SMS erhalten
5. Neues Passwort setzen

Alternativ: IT-Support kontaktieren

28.3.2.2 F: Wie richte ich MFA (Multi-Faktor-Authentifizierung) ein?

A: MFA-Einrichtung:

1. [TODO: MFA-Portal-URL] aufrufen
2. Mit aktuellem Passwort anmelden
3. MFA-Methode wählen:

- **Authenticator-App** (empfohlen): QR-Code scannen
 - **SMS:** Telefonnummer verifizieren
 - **Hardware-Token:** Token registrieren
4. Backup-Codes generieren und sicher speichern
 5. MFA testen

Wichtig: Backup-Codes an sicherem Ort aufbewahren!

28.3.2.3 F: Ich kann mich nicht per VPN verbinden. Was kann ich tun?

A: VPN-Troubleshooting:

1. **Credentials prüfen:**
 - Benutzername korrekt?
 - Passwort korrekt?
 - MFA-Token aktuell?
2. **VPN-Client prüfen:**
 - Neueste Version installiert?
 - Profil korrekt konfiguriert?
3. **Netzwerk prüfen:**
 - Internet-Verbindung funktioniert?
 - Firewall blockiert VPN nicht?
4. **Alternativen:**
 - Anderen VPN-Gateway versuchen
 - VPN-Client neu installieren

Wenn nichts hilft: IT-Support kontaktieren mit: - VPN-Client-Version - Fehlermeldung (Screenshot) - Zeitpunkt des Problems

28.3.3 Anwendungen

28.3.3.1 F: Die Anwendung lädt sehr langsam. Was kann ich tun?

A: Performance-Troubleshooting:

1. **Browser-Cache leeren:**
 - Chrome: Strg+Shift+Entf
 - Firefox: Strg+Shift+Entf
 - Edge: Strg+Shift+Entf
2. **Browser-Erweiterungen deaktivieren:**
 - Temporär alle Erweiterungen deaktivieren
 - Testen ob Performance besser
3. **Anderen Browser testen:**
 - Chrome, Firefox, oder Edge versuchen
4. **Netzwerk prüfen:**
 - Speedtest durchführen
 - VPN-Verbindung prüfen
5. **System-Ressourcen prüfen:**

- Task-Manager öffnen
- CPU/RAM-Auslastung prüfen
- Andere Programme schließen

Wenn Problem weiterhin besteht: Ticket erstellen mit: - Browser und Version - Betroffene Anwendung - Zeitpunkt des Problems - Screenshot

28.3.3.2 F: Ich erhalte einen “500 Internal Server Error”. Was bedeutet das?

A: Ein 500-Fehler bedeutet, dass ein Problem auf dem Server aufgetreten ist.

Sofortmaßnahmen: 1. Seite neu laden (F5) 2. 5 Minuten warten und erneut versuchen 3. Browser-Cache leeren 4. Anderen Browser versuchen

Wenn Fehler weiterhin auftritt: - Ticket erstellen (P2 - Hoch) - Screenshot des Fehlers anhängen - Genaue URL angeben - Zeitpunkt notieren

Für IT-Team: - Server-Logs prüfen - Anwendungs-Logs prüfen - Monitoring-Alerts prüfen

28.3.4 E-Mail

28.3.4.1 F: Ich kann keine E-Mails senden. Was soll ich tun?

A: E-Mail-Versand-Troubleshooting:

1. **Postausgang prüfen:**
 - Sind E-Mails im Postausgang hängen geblieben?
 - Fehlermeldung vorhanden?
2. **Postfach-Größe prüfen:**
 - Ist das Postfach voll?
 - Alte E-Mails archivieren/löschen
3. **Anhänge prüfen:**
 - Sind Anhänge zu groß? (Max: [TODO: Größe])
 - Anhänge komprimieren oder über File-Sharing senden
4. **Empfänger-Adresse prüfen:**
 - Ist die E-Mail-Adresse korrekt?
 - Tippfehler?
5. **Spam-Filter:**
 - Wurde E-Mail als Spam markiert?

Wenn Problem weiterhin besteht: IT-Support kontaktieren

28.3.4.2 F: Ich erhalte viele Spam-E-Mails. Was kann ich tun?

A: Spam-Reduzierung:

1. **Spam-Filter trainieren:**
 - Spam-E-Mails als “Spam” markieren

- Nicht als “Spam” markierte E-Mails als “Kein Spam” markieren
- 2. **Absender blockieren:**
 - Absender zur Blocklist hinzufügen
- 3. **E-Mail-Regeln erstellen:**
 - Automatische Filterung basierend auf Absender/Betreff
- 4. **Vorsicht bei E-Mail-Weitergabe:**
 - E-Mail-Adresse nicht öffentlich posten
 - Separate E-Mail für Newsletter verwenden

Bei verdächtigen E-Mails: - **NICHT** auf Links klicken - **NICHT** Anhänge öffnen - An thomas.weber@adminsind.de weiterleiten - E-Mail löschen

28.3.5 Dateien und Storage

28.3.5.1 F: Ich habe versehentlich eine Datei gelöscht. Kann sie wiederhergestellt werden?

A: Datei-Wiederherstellung:

1. **Papierkorb prüfen:**
 - Windows: Papierkorb auf Desktop
 - macOS: Papierkorb im Dock
 - Linux: Trash-Ordner
2. **Netzwerk-Laufwerk:**
 - Vorgängerversionen prüfen (Rechtsklick → Eigenschaften → Vorgängerversionen)
 - Shadow Copies verfügbar?
3. **Backup-Wiederherstellung:**
 - Ticket erstellen (P3 - Mittel)
 - Dateiname, Pfad und ungefähres Löschedatum angeben
 - IT-Team stellt aus Backup wieder her

Wichtig: Je schneller gemeldet, desto höher die Erfolgsaussicht!

Backup-Retention: - Tägliche Backups: 30 Tage - Wöchentliche Backups: 90 Tage - Monatliche Backups: 1 Jahr

28.3.5.2 F: Mein Netzwerk-Laufwerk ist voll. Was soll ich tun?

A: Storage-Management:

1. **Speicherplatz analysieren:**
 - Große Dateien identifizieren
 - Alte/unnötige Dateien löschen
2. **Dateien archivieren:**
 - Alte Projekte archivieren
 - Auf Archiv-Storage verschieben
3. **Duplikate entfernen:**
 - Doppelte Dateien identifizieren und löschen

4. **Komprimierung:**

- Große Dateien komprimieren (ZIP, 7z)

5. **Quota-Erhöhung beantragen:**

- Ticket erstellen mit Begründung
- Genehmigung durch Manager erforderlich

Quota-Limits: - Standard-Benutzer: [TODO: Größe] - Power-User: [TODO: Größe] - Projekt-Shares: [TODO: Größe]

28.3.6 Hardware

28.3.6.1 F: Mein Computer ist sehr langsam. Was kann ich tun?

A: Performance-Optimierung:

1. **Neustart:**

- Computer neu starten
- Oft löst dies bereits das Problem

2. **Programme schließen:**

- Unnötige Programme beenden
- Task-Manager prüfen (Strg+Shift+Esc)

3. **Disk-Cleanup:**

- Temporäre Dateien löschen
- Disk-Cleanup-Tool ausführen

4. **Updates prüfen:**

- Windows-Updates installieren
- Anwendungs-Updates installieren

5. **Malware-Scan:**

- Antivirus-Scan durchführen

Wenn Problem weiterhin besteht: - Ticket erstellen - Hardware-Upgrade prüfen - Neuinstallation erwägen

28.3.6.2 F: Wie beantrage ich neue Hardware?

A: Hardware-Anforderung:

1. **Ticket erstellen:**

- Kategorie: "Hardware-Anfrage"
- Gewünschte Hardware spezifizieren
- Begründung angeben

2. **Genehmigung:**

- Manager-Genehmigung erforderlich
- Budget-Prüfung durch Maria Müller

3. **Beschaffung:**

- IT-Team bestellt Hardware
- Lieferzeit: [TODO: Zeitraum]

4. **Installation:**

- Termin mit IT-Team vereinbaren
- Alte Hardware wird zurückgenommen

Standard-Hardware: - Laptop: [TODO: Modell] - Desktop: [TODO: Modell] - Monitor: [TODO: Modell] - Peripherie: Maus, Tastatur, Headset

28.4 Troubleshooting-Tipps

28.4.1 Allgemeine Troubleshooting-Schritte

1. **Neustart:**
 - Oft die einfachste Lösung
 - Computer, Anwendung, oder Service neu starten
 2. **Fehler dokumentieren:**
 - Screenshot erstellen
 - Fehlermeldung notieren
 - Zeitpunkt festhalten
 3. **Reproduzieren:**
 - Problem erneut auslösen
 - Schritte dokumentieren
 4. **Isolieren:**
 - Anderer Computer?
 - Anderer Browser?
 - Anderes Netzwerk?
 5. **Recherchieren:**
 - Bekannte Probleme prüfen (dieses Dokument)
 - Wiki durchsuchen
 - Kollegen fragen
 6. **Eskalieren:**
 - Ticket erstellen
 - IT-Support kontaktieren
-

28.4.2 Browser-Probleme

Symptome: - Seite lädt nicht - Fehlerhafte Darstellung - Funktionen funktionieren nicht

Lösungen: 1. Cache leeren (Strg+Shift+Entf) 2. Cookies löschen 3. Browser-Erweiterungen deaktivieren 4. Inkognito-Modus testen 5. Anderen Browser testen 6. Browser neu installieren

28.4.3 Netzwerk-Probleme

Symptome: - Keine Verbindung - Langsame Verbindung - Intermittierende Verbindung

Lösungen: 1. Netzwerk-Kabel prüfen 2. WLAN-Verbindung prüfen 3. Router neu starten 4. IP-Konfiguration erneuern (ipconfig /renew) 5. DNS-Cache leeren (ipconfig /flushdns) 6. VPN-Verbindung prüfen

28.4.4 Anwendungs-Probleme

Symptome: - Anwendung startet nicht - Anwendung stürzt ab - Funktionen fehlen

Lösungen: 1. Anwendung neu starten 2. Computer neu starten 3. Anwendung neu installieren 4. Updates installieren 5. Kompatibilitätsmodus testen (Windows) 6. Logs prüfen

28.5 Self-Service-Ressourcen

28.5.1 Dokumentation

- **Wiki:** [TODO: Wiki-URL]
- **Video-Tutorials:** [TODO: Video-URL]
- **Handbücher:** [TODO: Handbuch-URL]

28.5.2 Tools

- **Self-Service-Portal:** [TODO: Portal-URL]
- **Passwort-Reset:** [TODO: Reset-URL]
- **Software-Download:** [TODO: Download-URL]

28.5.3 Schulungen

- **Online-Kurse:** [TODO: Kurs-URL]
 - **Webinare:** [TODO: Webinar-Kalender]
 - **Präsenz-Schulungen:** Anfrage über IT-Support
-

28.6 Feedback und Verbesserungen

28.6.1 Feedback geben

Haben Sie Vorschläge zur Verbesserung dieses Dokuments oder der IT-Services?

Kontakt: - **E-Mail:** andreas.huemmer@adminsends.de - **Feedback-Formular:** [TODO: Formular-URL]

28.6.2 Dokument-Updates

Dieses Dokument wird regelmäßig aktualisiert basierend auf: - Neuen bekannten Problemen - Häufig gestellten Fragen - Benutzer-Feedback - Prozessverbesserungen

Review-Zyklus: Monatlich

Verantwortlich: Andreas Huemmer

28.7 Prozesse und Verantwortlichkeiten

28.7.1 RACI-Matrix

Aktivität	Ops Manager	Ops Team	Service Desk	Benutzer
Bekannte Probleme dokumentieren	A	R	C	I
FAQ aktualisieren	A	R	C	I
Workarounds entwickeln	A	R	C	-
Benutzer-Support	C	C	R	-
Feedback sammeln	A	C	R	R

Legende: R = Responsible, A = Accountable, C = Consulted, I = Informed

28.8 Compliance und Standards

28.8.1 Relevante Standards

- **ITIL v4:** Service Desk Practice, Knowledge Management
 - **ISO 20000:** Clause 8.2 - Service Desk
 - **COBIT 2019:** DSS02 - Managed Service Requests and Incidents
-

28.9 Anhang

28.9.1 Glossar

Begriff	Definition
Known Issue	Bekanntes Problem mit dokumentiertem Workaround
FAQ	Frequently Asked Questions - Häufig gestellte Fragen
Workaround	Temporäre Lösung für ein Problem
Root Cause	Grundursache eines Problems
Self-Service	Benutzer löst Problem selbst ohne Support

28.9.2 Referenzen

- ITIL v4 Foundation Handbook
 - ISO/IEC 20000-1:2018
 - COBIT 2019 Framework
-

Letzte Aktualisierung: {{ meta.date }}

Nächste Review: [TODO: Datum]

Kontakt: andreas.huemmer@adminsends.de

ewpage

Chapter 29

Kontakte, Eskalation und Anbieter

29.1 Übersicht

Dieses Dokument enthält Kontaktlisten, Eskalationspfade, Anbieter und Lieferanten sowie Support-Kontakte für den IT-Service. Ziel ist es, schnellen Zugriff auf relevante Kontaktinformationen in allen Situationen zu gewährleisten.

Dokumentverantwortlicher: IT Operations Manager

Genehmigt durch: CIO

Version: 1.0.0

Organisation: AdminSend GmbH

29.2 Interne Kontakte

29.2.1 Management

29.2.1.1 Chief Executive Officer (CEO)

- **Name:** Max Mustermann
- **Titel:** Chief Executive Officer
- **E-Mail:** max.mustermann@adminsends.de
- **Telefon:** +49 89 12345678-100
- **Abteilung:** Management
- **Verfügbarkeit:** Mo-Fr 09:00-18:00
- **Eskalation:** Nur für kritische Business-Impact-Situationen

29.2.1.2 Chief Information Officer (CIO)

- **Name:** Anna Schmidt
- **Titel:** Chief Information Officer
- **E-Mail:** anna.schmidt@adminsends.de
- **Telefon:** +49 89 12345678-200
- **Abteilung:** IT
- **Verfügbarkeit:** Mo-Fr 08:00-18:00

- **Eskalation:** IT-strategische Entscheidungen, kritische Incidents

29.2.1.3 Chief Information Security Officer (CISO)

- **Name:** Thomas Weber
- **Titel:** Chief Information Security Officer
- **E-Mail:** thomas.weber@adminsends.de
- **Telefon:** +49 89 12345678-300
- **Abteilung:** IT Security
- **Verfügbarkeit:** Mo-Fr 08:00-18:00, 24/7 für Security-Incidents
- **Eskalation:** Security-Incidents, Compliance-Fragen

29.2.1.4 Chief Financial Officer (CFO)

- **Name:** Maria Müller
- **Titel:** Chief Financial Officer
- **E-Mail:** maria.mueller@adminsends.de
- **Telefon:** +49 89 12345678-400
- **Abteilung:** Finance
- **Verfügbarkeit:** Mo-Fr 09:00-17:00
- **Eskalation:** Budget-Fragen, finanzielle Genehmigungen

29.2.1.5 Chief Operating Officer (COO)

- **Name:** Peter Fischer
 - **Titel:** Chief Operating Officer
 - **E-Mail:** peter.fischer@adminsends.de
 - **Telefon:** +49 89 12345678-500
 - **Abteilung:** Operations
 - **Verfügbarkeit:** Mo-Fr 08:00-18:00
 - **Eskalation:** Betriebliche Auswirkungen, Prozessfragen
-

29.2.2 IT-Operations

29.2.2.1 IT Operations Manager

- **Name:** Andreas Huemmer
- **Titel:** IT Operations Manager
- **E-Mail:** andreas.huemmer@adminsends.de
- **Telefon:** +49 89 12345678-250
- **Abteilung:** IT Operations
- **Verfügbarkeit:** Mo-Fr 08:00-18:00, On-Call für P1-Incidents
- **Verantwortung:** Gesamtverantwortung IT-Betrieb

29.2.2.2 Service Desk Lead

- **Name:** Julia Becker
- **Titel:** Service Desk Lead
- **E-Mail:** julia.becker@adminsends.de

- **Telefon:** +49 89 12345678-111
- **Abteilung:** Service Desk
- **Verfügbarkeit:** Mo-Fr 08:00-18:00
- **Verantwortung:** First-Level-Support, Ticket-Management

29.2.2.3 Operations Team

- **E-Mail:** [TODO: ops-team@example.com]
 - **Telefon:** [TODO: +49 89 12345678-250]
 - **Verfügbarkeit:** Mo-Fr 08:00-18:00
 - **Verantwortung:** Täglicher Betrieb, Monitoring, Incident-Response
-

29.2.3 Spezialisierte Teams

29.2.3.1 Network Team

- **Team Lead:** [TODO: Name]
- **E-Mail:** [TODO: network-team@example.com]
- **Telefon:** [TODO: Telefonnummer]
- **Verfügbarkeit:** Mo-Fr 08:00-18:00
- **Verantwortung:** Netzwerk-Infrastruktur, Firewall, VPN

29.2.3.2 Security Team

- **Team Lead:** Thomas Weber
- **E-Mail:** [TODO: security-team@example.com]
- **Telefon:** [TODO: Telefonnummer]
- **Verfügbarkeit:** Mo-Fr 08:00-18:00, 24/7 für Security-Incidents
- **Verantwortung:** IT-Sicherheit, Compliance, Incident-Response

29.2.3.3 Database Team

- **Team Lead:** [TODO: Name]
- **E-Mail:** [TODO: dba-team@example.com]
- **Telefon:** [TODO: Telefonnummer]
- **Verfügbarkeit:** Mo-Fr 08:00-18:00
- **Verantwortung:** Datenbank-Administration, Performance-Tuning

29.2.3.4 Application Team

- **Team Lead:** [TODO: Name]
 - **E-Mail:** [TODO: app-team@example.com]
 - **Telefon:** [TODO: Telefonnummer]
 - **Verfügbarkeit:** Mo-Fr 08:00-18:00
 - **Verantwortung:** Anwendungs-Support, Deployment
-

29.3 On-Call und Rufbereitschaft

29.3.1 On-Call-Rotation

29.3.1.1 Primärer On-Call

- **Aktuell:** [TODO: Name]
- **E-Mail:** [TODO: E-Mail]
- **Telefon:** [TODO: Mobilnummer]
- **Verfügbarkeit:** 24/7
- **Rotation:** Wöchentlich (Montag 08:00 Uhr)

29.3.1.2 Sekundärer On-Call (Backup)

- **Aktuell:** [TODO: Name]
- **E-Mail:** [TODO: E-Mail]
- **Telefon:** [TODO: Mobilnummer]
- **Verfügbarkeit:** 24/7
- **Rotation:** Wöchentlich (Montag 08:00 Uhr)

29.3.2 On-Call-Kalender

- **URL:** [TODO: Kalender-URL]
- **Zugriff:** Alle IT-Mitarbeiter
- **Aktualisierung:** Automatisch durch Rotation-Tool

29.3.3 On-Call-Richtlinien

- **Reaktionszeit P1:** 15 Minuten
 - **Reaktionszeit P2:** 1 Stunde
 - **Erreichbarkeit:** Telefon und E-Mail
 - **Eskalation:** Nach 30 Minuten ohne Antwort
-

29.4 Eskalationspfade

29.4.1 Incident-Eskalation

29.4.1.1 Level 1: Service Desk

- **Kontakt:** julia.becker@adminsends.de
- **Telefon:** +49 89 12345678-111
- **Verfügbarkeit:** Mo-Fr 08:00-18:00
- **Verantwortung:** First-Level-Support, Ticket-Erstellung

Eskalation zu Level 2: - P1: Sofort - P2: Nach 1 Stunde ohne Lösung - P3: Nach 4 Stunden ohne Lösung - P4: Nach 8 Stunden ohne Lösung

29.4.1.2 Level 2: Operations Team

- **Kontakt:** [TODO: ops-team@example.com]
- **Telefon:** [TODO: Telefonnummer]
- **Verfügbarkeit:** Mo-Fr 08:00-18:00, On-Call 24/7
- **Verantwortung:** Second-Level-Support, technische Analyse

Eskalation zu Level 3: - P1: Nach 2 Stunden ohne Lösung - P2: Nach 4 Stunden ohne Lösung - P3: Nach 8 Stunden ohne Lösung

29.4.1.3 Level 3: IT Operations Manager

- **Kontakt:** andreas.huemmer@adminsends.de
- **Telefon:** +49 89 12345678-250
- **Verfügbarkeit:** Mo-Fr 08:00-18:00, On-Call für P1
- **Verantwortung:** Koordination, Ressourcen-Allokation

Eskalation zu Level 4: - P1: Nach 4 Stunden ohne Lösung - P2: Nach 8 Stunden ohne Lösung - Wenn externe Unterstützung erforderlich

29.4.1.4 Level 4: CIO

- **Kontakt:** anna.schmidt@adminsends.de
- **Telefon:** +49 89 12345678-200
- **Verfügbarkeit:** Mo-Fr 08:00-18:00, erreichbar für kritische Incidents
- **Verantwortung:** Strategische Entscheidungen, Management-Kommunikation

Eskalation zu Level 5: - Kritischer Business-Impact - Medienrelevanz - Regulatorische Auswirkungen

29.4.1.5 Level 5: CEO

- **Kontakt:** max.mustermann@adminsends.de
 - **Telefon:** +49 89 12345678-100
 - **Verfügbarkeit:** Nach Vereinbarung
 - **Verantwortung:** Unternehmensweite Entscheidungen
-

29.4.2 Security-Incident-Eskalation

29.4.2.1 Level 1: Security Team

- **Kontakt:** [TODO: security-team@example.com]
- **Telefon:** [TODO: Telefonnummer]
- **Verfügbarkeit:** 24/7
- **Verantwortung:** Incident-Response, Forensik

Eskalation zu Level 2: - Kritischer Security-Incident - Datenverlust oder -diebstahl - Compliance-Verletzung

29.4.2.2 Level 2: CISO

- **Kontakt:** thomas.weber@adminsind.de
- **Telefon:** +49 89 12345678-300
- **Verfügbarkeit:** 24/7 für Security-Incidents
- **Verantwortung:** Security-Strategie, Compliance

Eskalation zu Level 3: - Schwerwiegender Datenverlust - Öffentliche Bekanntmachung erforderlich - Regulatorische Meldepflicht

29.4.2.3 Level 3: CIO / CEO

- **Kontakt:** anna.schmidt@adminsind.de / max.mustermann@adminsind.de
 - **Verfügbarkeit:** Nach Vereinbarung
 - **Verantwortung:** Unternehmensweite Kommunikation, rechtliche Schritte
-

29.5 Externe Anbieter und Lieferanten

29.5.1 Hardware-Anbieter

29.5.1.1 [TODO: Hardware-Vendor Name]

- **Ansprechpartner:** [TODO: Name]
 - **E-Mail:** [TODO: E-Mail]
 - **Telefon:** [TODO: Telefonnummer]
 - **Support-Hotline:** [TODO: Support-Nummer]
 - **Vertragsnummer:** [TODO: Vertragsnummer]
 - **Vertragsende:** [TODO: Datum]
 - **Support-Level:** [TODO: 24/7, Business Hours]
 - **Reaktionszeit:** [TODO: 4h, 8h, Next Business Day]
 - **Leistungen:**
 - Hardware-Lieferung
 - Garantie und Reparatur
 - Ersatzteil-Service
-

29.5.2 Software-Anbieter

29.5.2.1 [TODO: Software-Vendor Name]

- **Ansprechpartner:** [TODO: Name]
- **E-Mail:** [TODO: E-Mail]

- **Telefon:** [TODO: Telefonnummer]
 - **Support-Portal:** [TODO: URL]
 - **Vertragsnummer:** [TODO: Vertragsnummer]
 - **Lizenzanzahl:** [TODO: Anzahl]
 - **Vertragsende:** [TODO: Datum]
 - **Support-Level:** [TODO: Standard, Premium, Enterprise]
 - **Leistungen:**
 - Software-Updates
 - Bug-Fixes
 - Technischer Support
 - Schulungen
-

29.5.3 Cloud-Provider

29.5.3.1 [TODO: Cloud-Provider Name]

- **Account-Manager:** [TODO: Name]
- **E-Mail:** [TODO: E-Mail]
- **Telefon:** [TODO: Telefonnummer]
- **Support-Hotline:** [TODO: Support-Nummer]
- **Account-ID:** [TODO: Account-ID]
- **Support-Plan:** [TODO: Basic, Business, Enterprise]
- **Leistungen:**
 - Cloud-Infrastruktur
 - 24/7 Support
 - SLA: [TODO: Verfügbarkeit]
 - Technischer Support

Support-Kanäle: - **Telefon:** [TODO: Nummer] - **Chat:** [TODO: URL] - **Ticket:** [TODO: Portal-URL] - **Emergency:** [TODO: Emergency-Nummer]

29.5.4 Netzwerk-Provider

29.5.4.1 Internet-Provider

- **Anbieter:** [TODO: Provider-Name]
- **Ansprechpartner:** [TODO: Name]
- **E-Mail:** [TODO: E-Mail]
- **Telefon:** [TODO: Telefonnummer]
- **Störungshotline:** [TODO: Störungs-Nummer]
- **Vertragsnummer:** [TODO: Vertragsnummer]
- **Bandbreite:** [TODO: Bandbreite]
- **SLA:** [TODO: Verfügbarkeit]
- **Leistungen:**
 - Internet-Konnektivität
 - 24/7 Support
 - Störungsbehebung

29.5.5 Managed-Service-Provider

29.5.5.1 [TODO: MSP Name]

- **Ansprechpartner:** [TODO: Name]
 - **E-Mail:** [TODO: E-Mail]
 - **Telefon:** [TODO: Telefonnummer]
 - **Support-Hotline:** [TODO: Support-Nummer]
 - **Vertragsnummer:** [TODO: Vertragsnummer]
 - **Vertragsende:** [TODO: Datum]
 - **Support-Level:** [TODO: 24/7, Business Hours]
 - **Leistungen:**
 - [TODO: Managed Services]
 - [TODO: Monitoring]
 - [TODO: Support]
-

29.5.6 Backup-Service-Provider

29.5.6.1 [TODO: Backup-Provider Name]

- **Ansprechpartner:** [TODO: Name]
 - **E-Mail:** [TODO: E-Mail]
 - **Telefon:** [TODO: Telefonnummer]
 - **Support-Hotline:** [TODO: Support-Nummer]
 - **Vertragsnummer:** [TODO: Vertragsnummer]
 - **Storage-Kapazität:** [TODO: Kapazität]
 - **Retention:** [TODO: Aufbewahrungsdauer]
 - **Leistungen:**
 - Backup-Storage
 - Disaster-Recovery
 - 24/7 Support
-

29.5.7 Security-Service-Provider

29.5.7.1 [TODO: Security-Provider Name]

- **Ansprechpartner:** [TODO: Name]
- **E-Mail:** [TODO: E-Mail]
- **Telefon:** [TODO: Telefonnummer]
- **SOC-Hotline:** [TODO: SOC-Nummer]
- **Vertragsnummer:** [TODO: Vertragsnummer]
- **Leistungen:**
 - Security-Monitoring
 - Incident-Response
 - Threat-Intelligence

29.6 Notfall-Kontakte

29.6.1 Kritische Situationen

29.6.1.1 Feuer / Medizinischer Notfall

- **Notruf:** 112
- **Gebäudesicherheit:** [TODO: Telefonnummer]
- **Erste-Hilfe:** [TODO: Ersthelfer-Kontakt]

29.6.1.2 Polizei

- **Notruf:** 110
- **Lokale Polizei:** [TODO: Telefonnummer]

29.6.1.3 Gebäudemanagement

- **Facility Management:** [TODO: Telefonnummer]
- **Verfügbarkeit:** 24/7
- **Verantwortung:** Gebäudesicherheit, Zugang

29.6.1.4 Rechtsabteilung

- **Ansprechpartner:** [TODO: Name]
- **E-Mail:** [TODO: E-Mail]
- **Telefon:** [TODO: Telefonnummer]
- **Verfügbarkeit:** Mo-Fr 09:00-17:00, Notfall-Hotline
- **Verantwortung:** Rechtliche Beratung, Verträge

29.6.1.5 PR / Kommunikation

- **Ansprechpartner:** [TODO: Name]
- **E-Mail:** [TODO: E-Mail]
- **Telefon:** [TODO: Telefonnummer]
- **Verfügbarkeit:** Mo-Fr 09:00-18:00, Notfall-Hotline
- **Verantwortung:** Externe Kommunikation, Medien

29.7 Kommunikationskanäle

29.7.1 Interne Kommunikation

29.7.1.1 E-Mail

- **Primär:** Offizielle Kommunikation
- **Verteiler:**

- IT-Team: [TODO: it-team@example.com]
- Management: [TODO: management@example.com]
- All-Hands: [TODO: all@example.com]

29.7.1.2 Chat / Collaboration

- **Platform:** [TODO: Chat-Platform]
- **Channels:**
 - #it-operations: Täglicher Betrieb
 - #incidents: Incident-Kommunikation
 - #changes: Change-Kommunikation
 - #general: Allgemeine Kommunikation

29.7.1.3 Telefon-Konferenz

- **System:** [TODO: Conferencing-System]
- **Bridge-Nummer:** [TODO: Telefonnummer]
- **PIN:** [TODO: PIN]

29.7.1.4 Video-Konferenz

- **System:** [TODO: Video-System]
- **URL:** [TODO: Meeting-URL]

29.7.2 Externe Kommunikation

29.7.2.1 Kunden-Kommunikation

- **E-Mail:** [TODO: support@example.com]
- **Telefon:** [TODO: Support-Nummer]
- **Portal:** [TODO: Portal-URL]

29.7.2.2 Status-Page

- **URL:** [TODO: status.example.com]
- **Zweck:** Öffentliche Status-Updates
- **Aktualisierung:** Bei Incidents und Wartungen

29.7.2.3 Social Media

- **Twitter:** [TODO: @company]
 - **LinkedIn:** [TODO: Company-Page]
 - **Zweck:** Öffentliche Ankündigungen
-

29.8 Kontakt-Aktualisierung

29.8.1 Aktualisierungsprozess

1. **Änderungen melden:**
 - E-Mail an andreas.huemmer@adminsends.de
 - Neue Kontaktdaten angeben
 - Gültigkeitsdatum angeben
2. **Validierung:**
 - IT Operations Manager prüft Änderung
 - Genehmigung einholen (falls erforderlich)
3. **Aktualisierung:**
 - Dokument aktualisieren
 - CMDB aktualisieren
 - Betroffene Teams informieren
4. **Verifikation:**
 - Neue Kontaktdaten testen
 - Bestätigung einholen

29.8.2 Review-Zyklus

- **Frequenz:** Quartalsweise
 - **Verantwortlich:** Andreas Huemmer
 - **Prozess:**
 - Alle Kontakte durchgehen
 - Aktualität prüfen
 - Änderungen dokumentieren
 - Teams informieren
-

29.9 Prozesse und Verantwortlichkeiten

29.9.1 RACI-Matrix

Aktivität	CIO	Ops Manager	Ops Team	Service Desk
Kontakt-Verwaltung	C	A	R	C
Eskalation Level 1-2	I	C	R	R
Eskalation Level 3-4	A	R	C	I
Anbieter-Management	A	R	C	I
Notfall-Kommunikation	A	R	C	I

Legende: R = Responsible, A = Accountable, C = Consulted, I = Informed

29.10 Compliance und Standards

29.10.1 Relevante Standards

- **ITIL v4:** Service Desk Practice, Incident Management
- **ISO 20000:** Clause 8.2 - Service Desk
- **COBIT 2019:** DSS02 - Managed Service Requests and Incidents

29.10.2 Audit-Anforderungen

- Aktuelle Kontaktlisten
 - Eskalationspfad-Dokumentation
 - Anbieter-Verträge
 - Kommunikations-Protokolle
-

29.11 Anhang

29.11.1 Glossar

Begriff	Definition
On-Call	Rufbereitschaft außerhalb regulärer Arbeitszeiten
Eskalation	Weiterleitung an höhere Support-Ebene
SLA	Service Level Agreement - Vereinbarung über Serviceleistungen
MSP	Managed Service Provider - Externer Dienstleister

29.11.2 Referenzen

- ITIL v4 Foundation Handbook
 - ISO/IEC 20000-1:2018
 - COBIT 2019 Framework
-

29.12 Schnellreferenz

29.12.1 Wichtigste Kontakte

Situation	Kontakt	Telefon
IT-Support	Julia Becker	+49 89 12345678-111
Kritischer Incident	IT Operations Manager	+49 89 12345678-250
Security-Incident	Thomas Weber	+49 89 12345678-300
Management-Eskalation	Anna Schmidt	+49 89 12345678-200
Notfall (Feuer/Medizin)	Notruf	112
Polizei	Notruf	110

Letzte Aktualisierung: {{ meta.date }}
Nächste Review: [TODO: Datum]
Kontakt: andreas.huemmer@adminsind.de
ewpage

Chapter 30

Compliance und Audits

30.1 Zweck und Geltungsbereich

Dieses Dokument beschreibt die Compliance- und Audit-Prozesse für AdminSend GmbH. Es definiert relevante Standards, Audit-Prozesse, Compliance-Kontrollen, Nachweise und Non-Compliance-Risiken zur Sicherstellung der Einhaltung regulatorischer und vertraglicher Anforderungen.

Geltungsbereich: Alle IT-Systeme, Prozesse und Aktivitäten von AdminSend GmbH

Verantwortlich: {{ meta.compliance_officer }} ({{ meta.compliance_officer_email }})

30.2 Compliance-Grundlagen

30.2.1 Compliance-Definition

Compliance: Einhaltung von Gesetzen, Vorschriften, Standards, Richtlinien und vertraglichen Verpflichtungen

Ziele: - **Rechtssicherheit:** Vermeidung rechtlicher Konsequenzen - **Risikominimierung:** Reduzierung von Compliance-Risiken - **Reputation:** Schutz des Unternehmensrufs - **Vertrauen:** Vertrauen von Kunden und Partnern - **Wettbewerbsvorteil:** Zertifizierungen als Differenzierungsmerkmal

30.2.2 Compliance-Bereiche

Regulatorische Compliance: - Gesetzliche Anforderungen (DSGVO, IT-Sicherheitsgesetz) - Branchenspezifische Regulierungen - Datenschutz-Anforderungen

Standard-Compliance: - ISO-Standards (ISO 27001, ISO 20000) - Branchenstandards (PCI-DSS, HIPAA) - Best-Practice-Frameworks (ITIL, COBIT)

Vertragliche Compliance: - Service-Level-Agreements (SLAs) - Kunden-Verträge - Lieferanten-Verträge

Interne Compliance: - Unternehmens-Policies - IT-Richtlinien - Sicherheits-Standards

30.3 Relevante Standards und Regulierungen

30.3.1 ISO/IEC 27001:2013 - Informationssicherheits-Management

Beschreibung: Internationaler Standard für Informationssicherheits-Managementsysteme (ISMS)

Geltungsbereich: Alle IT-Systeme und Informationsverarbeitung

Status: {{ meta.iso27001_status }}

Zertifizierung: {{ meta.iso27001_certification }}

Zertifizierungs-Stelle: {{ meta.iso27001_certifier }}

Gültig bis: {{ meta.iso27001_valid_until }}

Kern-Anforderungen: - ISMS etablieren, implementieren, betreiben, überwachen, reviewen, warten und verbessern - Risiko-Assessment und -Treatment - 114 Controls in 14 Kategorien (Annex A) - Management-Review und kontinuierliche Verbesserung

Audit-Frequenz: - **Zertifizierungs-Audit:** Alle 3 Jahre - **Überwachungs-Audit:** Jährlich - **Internes Audit:** Quartalsweise

Verantwortlich: Thomas Weber

30.3.2 ISO/IEC 20000-1:2018 - IT-Service-Management

Beschreibung: Internationaler Standard für IT-Service-Management-Systeme (SMS)

Geltungsbereich: IT-Service-Management-Prozesse

Status: {{ meta.iso20000_status }}

Kern-Anforderungen: - Service-Management-System (SMS) - Service-Planung und -Bereitstellung - Relationship-Prozesse - Resolution-Prozesse - Control-Prozesse

Alignment: ITIL v4 Framework

Verantwortlich: Andreas Huemmer

30.3.3 DSGVO (GDPR) - Datenschutz-Grundverordnung

Beschreibung: EU-Verordnung zum Schutz personenbezogener Daten

Geltungsbereich: Alle Verarbeitungen personenbezogener Daten

Inkrafttreten: 25. Mai 2018

Kern-Anforderungen: - Rechtmäßigkeit der Verarbeitung (Art. 6) - Informationspflichten (Art. 13, 14) - Betroffenenrechte (Art. 15-22) - Technische und organisatorische Maßnahmen (Art. 32) - Meldepflicht bei Data Breach (Art. 33, 34) - Datenschutz-Folgenabschätzung (Art. 35)

Bußgelder: Bis zu 20 Mio. € oder 4% des weltweiten Jahresumsatzes

Datenschutzbeauftragter: {{ meta.data_protection_officer }}

Verzeichnis von Verarbeitungstätigkeiten: {{ meta.processing_activities_register }}

30.3.4 BSI IT-Grundschutz

Beschreibung: Methodik des Bundesamts für Sicherheit in der Informationstechnik

Geltungsbereich: IT-Sicherheit

Status: {{ meta.bsi_grundschutz_status }}

Absicherungs-Level: - **Basis-Absicherung:** Standard-Sicherheitsmaßnahmen - **Kern-Absicherung:** Erhöhte Sicherheitsanforderungen - **Standard-Absicherung:** Vollständige Umsetzung

Bausteine: IT-Grundschutz-Kompendium

Verantwortlich: Thomas Weber

30.3.5 PCI-DSS (Payment Card Industry Data Security Standard)

Beschreibung: Sicherheitsstandard für Kreditkarten-Datenverarbeitung

Geltungsbereich: Systeme, die Kreditkarten-Daten verarbeiten, speichern oder übertragen

Status: {{ meta.pci_dss_status }}

12 Anforderungen: 1. Firewall-Konfiguration 2. Keine Standard-Passwörter 3. Schutz gespeicherter Karteninhaber-Daten 4. Verschlüsselung bei Übertragung 5. Antivirus-Software 6. Sichere Systeme und Applikationen 7. Zugriffsbeschränkung (Need-to-Know) 8. Eindeutige IDs für Zugriffe 9. Physischer Zugriff beschränken 10. Tracking und Monitoring 11. Regelmäßige Security-Tests 12. Informationssicherheits-Policy

Compliance-Level: {{ meta.pci_dss_level }}

QSA (Qualified Security Assessor): {{ meta.pci_dss_qsa }}

30.3.6 SOX (Sarbanes-Oxley Act)

Beschreibung: US-Gesetz für finanzielle Berichterstattung

Geltungsbereich: Finanzrelevante IT-Systeme (falls börsennotiert)

Status: {{ meta.sox_status }}

IT-relevante Anforderungen: - Section 302: Management-Verantwortung für interne Kontrollen - Section 404: Assessment der internen Kontrollen - Section 409: Zeitnahe Offenlegung - IT-General-Controls (ITGC) - Application-Controls

Verantwortlich: Maria Müller

30.3.7 COBIT 2019

Beschreibung: Framework für IT-Governance und -Management

Geltungsbereich: IT-Governance

Status: {{ meta.cobit_status }}

Governance-Objectives: - EDM01: Ensured Governance Framework Setting and Maintenance
- EDM02: Ensured Benefits Delivery - EDM03: Ensured Risk Optimization - EDM04: Ensured Resource Optimization - EDM05: Ensured Stakeholder Engagement

Management-Objectives: 40 Objectives in 5 Domänen (APO, BAI, DSS, MEA, EDM)

30.3.8 Branchenspezifische Regulierungen

Telekommunikation: - Telekommunikationsgesetz (TKG) - Vorratsdatenspeicherung

Gesundheitswesen: - HIPAA (Health Insurance Portability and Accountability Act) - Patientendaten-Schutz-Gesetz

Finanzsektor: - MaRisk (Mindestanforderungen an das Risikomanagement) - BAIT (Bankaufsichtliche Anforderungen an die IT)

Energie: - IT-Sicherheitskatalog nach § 11 Abs. 1a EnWG

30.4 Compliance-Management-Prozess

30.4.1 Prozess-Übersicht

Compliance
Identification

Gap
Analysis

Remediation
Planning

Implementation
& Monitoring

Audit &
Assessment

Continuous
Improvement

30.4.2 1. Compliance Identification

Aktivitäten: - Relevante Gesetze und Regulierungen identifizieren - Anwendbare Standards ermitteln - Vertragliche Verpflichtungen erfassen - Interne Policies definieren

Quellen: - Rechtsabteilung - Branchenverbände - Kunden-Anforderungen - Management-Vorgaben

Dokumentation: Compliance-Register

Verantwortlich: Compliance-Officer

30.4.3 2. Gap Analysis

Aktivitäten: - Ist-Zustand erfassen - Soll-Zustand definieren - Gaps identifizieren - Risiken bewerten - Priorisierung

Methoden: - Self-Assessment - Compliance-Scans - Dokumenten-Review - Interviews

Output: Gap-Analysis-Report

Verantwortlich: Compliance-Team, Fachbereiche

30.4.4 3. Remediation Planning

Aktivitäten: - Maßnahmen definieren - Verantwortlichkeiten zuweisen - Zeitpläne erstellen - Budget planen - Risiken managen

Priorisierung: - **Critical:** Sofort (< 30 Tage) - **High:** Kurzfristig (< 90 Tage) - **Medium:** Mittelfristig (< 180 Tage) - **Low:** Langfristig (< 365 Tage)

Output: Remediation-Plan

Verantwortlich: Compliance-Officer, Fachbereichs-Leiter

30.4.5 4. Implementation & Monitoring

Aktivitäten: - Maßnahmen umsetzen - Fortschritt überwachen - Probleme eskalieren - Dokumentation pflegen

Monitoring: - Wöchentliche Status-Updates - Monatliche Reviews - Quartalsweise Management-Reports

Tools: - Compliance-Management-System - Ticketing-System - Projekt-Management-Tools

Verantwortlich: Fachbereiche, Compliance-Team

30.4.6 5. Audit & Assessment

Aktivitäten: - Interne Audits durchführen - Externe Audits koordinieren - Findings dokumentieren - Corrective Actions planen

Audit-Typen: - Interne Audits - Externe Audits (Zertifizierung) - Kunden-Audits - Regulierungs-Audits

Verantwortlich: Internal Audit, Externe Auditoren

30.4.7 6. Continuous Improvement

Aktivitäten: - Lessons Learned dokumentieren - Prozesse optimieren - Best Practices implementieren - Training durchführen

Methoden: - PDCA-Zyklus (Plan-Do-Check-Act) - Root-Cause-Analysis - Benchmarking

Verantwortlich: Compliance-Officer, Management

30.5 Audit-Prozesse

30.5.1 Audit-Typen

30.5.1.1 Interne Audits

Zweck: Selbstbewertung der Compliance

Frequenz: - **ISO 27001:** Quartalsweise - **ISO 20000:** Quartalsweise - **DSGVO:** Halbjährlich - **Interne Policies:** Jährlich

Durchführung: - Internal Audit Team - Unabhängig von geprüftem Bereich - Risiko-basierter Ansatz

Prozess: 1. Audit-Planung 2. Audit-Vorbereitung 3. Audit-Durchführung (Interviews, Dokumenten-Review, Tests) 4. Findings dokumentieren 5. Audit-Report erstellen 6. Corrective Actions planen 7. Follow-up

Verantwortlich: Internal Audit Team

30.5.1.2 Externe Audits (Zertifizierung)

Zweck: Zertifizierung nach Standards

Frequenz: - **Zertifizierungs-Audit:** Alle 3 Jahre - **Überwachungs-Audit:** Jährlich - **Re-Zertifizierung:** Alle 3 Jahre

Durchführung: - Akkreditierte Zertifizierungs-Stelle - Unabhängige Auditoren - Dokumenten-Review und On-Site-Audit

Audit-Phasen: - **Stage 1:** Dokumenten-Review - **Stage 2:** On-Site-Audit - **Surveillance:** Jährliche Überwachung

Zertifizierungs-Stellen: - ISO 27001: {{ meta.iso27001_certifier }} - ISO 20000: {{ meta.iso20000_certifier }}

30.5.1.3 Kunden-Audits

Zweck: Nachweis der Compliance gegenüber Kunden

Frequenz: Nach Kunden-Anforderung

Durchführung: - Kunden-Auditoren - Vor-Ort oder Remote - Fokus auf vertragliche Anforderungen

Vorbereitung: - Audit-Scope klären - Dokumentation bereitstellen - Ansprechpartner benennen - Räumlichkeiten vorbereiten

Verantwortlich: Account-Manager, Compliance-Officer

30.5.1.4 Regulierungs-Audits

Zweck: Überprüfung durch Aufsichtsbehörden

Frequenz: Ad-hoc oder regelmäßig (je nach Regulierung)

Durchführung: - Aufsichtsbehörden (z.B. Datenschutzbehörde, BaFin) - Angekündigt oder unangekündigt - Umfassende Prüfung

Beispiele: - Datenschutzbehörde (DSGVO-Compliance) - BaFin (Finanzsektor) - Bundesnetzagentur (Telekommunikation)

Vorbereitung: - Dokumentation aktuell halten - Prozesse etabliert - Ansprechpartner definiert

30.5.2 Audit-Vorbereitung

Checkliste: - ☐ Audit-Scope definiert - ☐ Audit-Plan erstellt - ☐ Dokumentation aktualisiert - ☐ Ansprechpartner benannt - ☐ Räumlichkeiten vorbereitet - ☐ IT-Systeme zugänglich - ☐ Stakeholder informiert - ☐ Pre-Audit-Meeting durchgeführt

Dokumentation: - Policies und Procedures - Risiko-Assessments - Asset-Inventar - Netzwerk-Diagramme - Zugriffs-Kontrollen - Incident-Reports - Change-Logs - Audit-Logs - Training-Records - Vendor-Verträge

Verantwortlich: Compliance-Officer, Fachbereiche

30.5.3 Audit-Durchführung

Audit-Methoden:

30.5.3.1 Dokumenten-Review

Aktivitäten: - Policies und Procedures prüfen - Dokumentations-Vollständigkeit - Aktualität der Dokumente - Konsistenz

30.5.3.2 Interviews

Aktivitäten: - Mitarbeiter-Interviews - Management-Interviews - Prozess-Verständnis prüfen - Awareness-Level bewerten

Interviewpartner: - Management - IT-Operations - Security-Team - Entwickler - End-User

30.5.3.3 System-Tests

Aktivitäten: - Konfigurations-Reviews - Zugriffs-Kontrollen testen - Log-Reviews - Vulnerability-Scans - Penetration-Tests (falls Scope)

30.5.3.4 Observations

Aktivitäten: - Prozess-Beobachtungen - Arbeitsplatz-Inspektionen - Physische Sicherheit prüfen - Verhaltens-Compliance

30.5.4 Audit-Findings

Finding-Kategorien:

Kategorie	Beschreibung	Beispiel
Critical	Schwerwiegende Non-Compliance	Fehlende Verschlüsselung sensibler Daten
Major	Signifikante Non-Compliance	Unvollständige Dokumentation
Minor	Kleinere Abweichungen	Veraltete Dokumente
Observation	Verbesserungs-Potenzial	Prozess-Optimierung möglich

Finding-Dokumentation: - Finding-ID - Kategorie (Critical/Major/Minor/Observation) - Beschreibung - Betroffene Systeme/Prozesse - Anforderung (Standard-Referenz) - Evidenz - Risiko-Bewertung - Empfohlene Corrective Action

Beispiel-Finding:

Finding-ID: AUD-2024-001

Kategorie: Major

Beschreibung: Passwort-Policy nicht durchgesetzt

Anforderung: ISO 27001 A.9.4.3

Evidenz: 15 von 50 Accounts ohne Passwort-Ablauf

Risiko: Hoch (Unauthorized Access)

Empfehlung: Passwort-Policy via GPO durchsetzen

Frist: 30 Tage

30.5.5 Corrective Actions

Corrective-Action-Prozess:

- 1. Finding-Review**
 - Finding verstehen
 - Root-Cause identifizieren
 - Impact bewerten
- 2. Action-Planning**
 - Maßnahmen definieren
 - Verantwortliche benennen
 - Zeitplan erstellen
 - Ressourcen planen
- 3. Implementation**
 - Maßnahmen umsetzen
 - Fortschritt überwachen
 - Dokumentation pflegen
- 4. Verification**
 - Wirksamkeit prüfen
 - Evidenz sammeln
 - Auditor informieren
- 5. Closure**
 - Finding schließen

- Lessons Learned
- Prozess-Verbesserung

Corrective-Action-Plan:

Finding-ID	Maßnahme	Verantwortlich	Frist	Status
AUD-2024-001	GPO für Passwort-Policy	IT-Admin	30 Tage	In Progress
AUD-2024-002	Dokumentation aktualisieren	Compliance	14 Tage	Completed

Tracking: Compliance-Management-System

30.5.6 Audit-Reporting

Audit-Report-Inhalte: - Executive Summary - Audit-Scope und -Methodik - Findings (nach Kategorie) - Positive Observations - Corrective-Action-Plan - Recommendations - Conclusion

Report-Empfänger: - Management - Audit-Committee - Betroffene Fachbereiche - Externe Auditoren (bei Follow-up)

Vertraulichkeit: Confidential

30.6 Compliance-Kontrollen und Nachweise

30.6.1 Technische Kontrollen

30.6.1.1 Zugriffskontrolle

Kontrollen: - Multi-Factor-Authentication (MFA) - Role-Based Access Control (RBAC) - Least-Privilege-Prinzip - Privileged Access Management (PAM) - Access-Reviews (quartalsweise)

Nachweise: - Access-Control-Matrix - User-Access-Reports - Access-Review-Protokolle - MFA-Aktivierungs-Rate

30.6.1.2 Verschlüsselung

Kontrollen: - Encryption at Rest (AES-256) - Encryption in Transit (TLS 1.3) - Key-Management - Certificate-Management

Nachweise: - Verschlüsselungs-Inventar - Key-Management-Procedures - Certificate-Inventar - Encryption-Scan-Reports

30.6.1.3 Logging und Monitoring

Kontrollen: - Zentrale Log-Sammlung - SIEM-Monitoring - Audit-Trails - Log-Retention (nach Policy)

Nachweise: - Log-Collection-Status - SIEM-Use-Cases - Audit-Log-Samples - Retention-Compliance-Reports

30.6.1.4 Vulnerability Management

Kontrollen: - Regelmäßige Vulnerability-Scans - Patch-Management - Penetration-Tests - Security-Assessments

Nachweise: - Scan-Reports - Patch-Compliance-Reports - Pentest-Reports - Remediation-Tracking

30.6.2 Organisatorische Kontrollen

30.6.2.1 Policies und Procedures

Kontrollen: - Dokumentierte Policies - Regelmäßige Reviews - Management-Approval - Kommunikation an Mitarbeiter

Nachweise: - Policy-Dokumente - Review-Protokolle - Approval-Signaturen - Kommunikations-Nachweise

30.6.2.2 Training und Awareness

Kontrollen: - Security-Awareness-Training - Role-spezifisches Training - Phishing-Simulationen - Training-Tracking

Nachweise: - Training-Records - Teilnahme-Listen - Phishing-Simulation-Results - Awareness-Kampagnen-Dokumentation

30.6.2.3 Incident Management

Kontrollen: - Incident-Response-Plan - Incident-Tracking - Post-Incident-Reviews - Lessons-Learned-Prozess

Nachweise: - Incident-Reports - Response-Timelines - Post-Incident-Review-Protokolle - Improvement-Actions

30.6.2.4 Change Management

Kontrollen: - Change-Approval-Prozess - Change-Advisory-Board (CAB) - Change-Dokumentation - Rollback-Procedures

Nachweise: - Change-Tickets - CAB-Meeting-Protokolle - Change-Success-Rate - Rollback-Dokumentation

30.6.3 Physische Kontrollen

30.6.3.1 Zutrittskontrolle

Kontrollen: - Badge-System - Besucher-Management - Video-Überwachung - Alarm-Systeme

Nachweise: - Zutritts-Logs - Besucher-Logs - Video-Aufzeichnungen (falls erlaubt) - Alarm-Protokolle

30.6.3.2 Umgebungs-Kontrollen

Kontrollen: - Klimatisierung - USV (Unterbrechungsfreie Stromversorgung) - Brandschutz - Wasser-Schutz

Nachweise: - Wartungs-Protokolle - USV-Test-Protokolle - Brandschutz-Übungen - Umgebungs-Monitoring-Logs

30.7 Non-Compliance-Risiken und Maßnahmen

30.7.1 Risiko-Kategorien

30.7.1.1 Rechtliche Risiken

Risiken: - Bußgelder und Strafen - Gerichtsverfahren - Haftungsansprüche - Geschäftsführer-Haftung

Beispiele: - DSGVO-Verstoß: Bis zu 20 Mio. € oder 4% Jahresumsatz - PCI-DSS-Verstoß: Bis zu 500.000 \$ pro Monat - SOX-Verstoß: Strafrechtliche Konsequenzen

Mitigations: - Compliance-Programm etablieren - Regelmäßige Audits - Legal-Counsel einbinden - Versicherungen (Cyber-Insurance)

30.7.1.2 Finanzielle Risiken

Risiken: - Bußgelder - Vertragsstrafen - Umsatzverluste - Erhöhte Versicherungs-Prämien

Beispiele: - SLA-Verstöße: Vertragsstrafen - Zertifizierungs-Verlust: Kunden-Verlust - Data Breach: Schadenersatz

Mitigations: - Risiko-Assessment - Finanzielle Rücklagen - Versicherungen - Vertrags-Management

30.7.1.3 Reputations-Risiken

Risiken: - Vertrauensverlust - Negative Presse - Kunden-Abwanderung - Schwierigkeiten bei Neukundengewinnung

Beispiele: - Data Breach öffentlich bekannt - Compliance-Verstöße in Medien - Zertifizierungs-Entzug

Mitigations: - Proaktive Kommunikation - Crisis-Management-Plan - PR-Strategie - Transparenz

30.7.1.4 Operative Risiken

Risiken: - Service-Unterbrechungen - Ineffiziente Prozesse - Mitarbeiter-Frustration - Vendor-Probleme

Beispiele: - Audit-Findings führen zu Service-Änderungen - Compliance-Anforderungen verzögern Projekte - Zusätzlicher Aufwand für Dokumentation

Mitigations: - Compliance by Design - Prozess-Automatisierung - Training und Awareness - Vendor-Management

30.7.2 Risiko-Management

Risiko-Bewertung:

Wahrscheinlichkeit	Impact	Risiko-Level	Maßnahmen
Hoch	Hoch	Kritisch	Sofortige Maßnahmen
Hoch	Mittel	Hoch	Kurzfristige Maßnahmen
Mittel	Hoch	Hoch	Kurzfristige Maßnahmen
Mittel	Mittel	Mittel	Mittelfristige Maßnahmen
Niedrig	Hoch	Mittel	Monitoring
Niedrig	Mittel	Niedrig	Akzeptieren oder Monitoring
Niedrig	Niedrig	Sehr niedrig	Akzeptieren

Risiko-Treatment-Optionen: - **Avoid:** Risiko vermeiden (Aktivität einstellen) - **Mitigate:** Risiko reduzieren (Kontrollen implementieren) - **Transfer:** Risiko übertragen (Versicherung, Outsourcing) - **Accept:** Risiko akzeptieren (mit Management-Genehmigung)

Risiko-Register: `{{ meta.risk_register }}`

30.7.3 Incident-Response bei Non-Compliance

Prozess:

1. **Detection**
 - Non-Compliance identifiziert
 - Severity bewerten
 - Stakeholder informieren
2. **Assessment**
 - Scope ermitteln
 - Impact analysieren
 - Meldepflichten prüfen
3. **Containment**
 - Sofort-Maßnahmen
 - Weitere Verstöße verhindern
 - Dokumentation starten
4. **Remediation**
 - Corrective Actions
 - Root-Cause-Analysis
 - Preventive Actions
5. **Reporting**
 - Interne Meldung
 - Externe Meldung (falls erforderlich)
 - Management-Briefing
6. **Lessons Learned**
 - Post-Incident-Review
 - Prozess-Verbesserungen
 - Training-Updates

30.8 Compliance-Metriken und Reporting

30.8.1 Key Performance Indicators (KPIs)

KPI	Zielwert	Messung	Frequenz
Audit-Findings-Rate	< 5 Major Findings	Findings pro Audit	Nach Audit
Corrective-Action-Closure-Rate	> 95% in Frist	Geschlossene CAs / Gesamt-CAs	Monatlich
Training-Completion-Rate	100%	Absolvierte Trainings / Pflicht-Trainings	Quartalsweise
Policy-Review-Compliance	100%	Reviewte Policies / Gesamt-Policies	Jährlich
Incident-Reporting-Time	< 24h	Zeit von Incident bis Meldung	Pro Incident
Vulnerability-Remediation-SLA	> 95%	Remediated in SLA / Gesamt	Monatlich

30.8.2 Compliance-Dashboard

Metriken: - Compliance-Status nach Standard - Offene Audit-Findings - Corrective-Actions-Status - Training-Completion-Rate - Policy-Review-Status - Incident-Trends

Tool: {{ meta.compliance_dashboard }}

Zugriff: Management, Compliance-Team, Auditoren

30.8.3 Reporting

30.8.3.1 Monatliches Compliance-Status-Report

Inhalte: - Compliance-Status-Übersicht - Neue Findings - Corrective-Actions-Fortschritt - Upcoming Audits - Risiken und Issues

Empfänger: Compliance-Officer, Management

30.8.3.2 Quartalsweises Compliance-Management-Report

Inhalte: - Compliance-KPIs - Audit-Zusammenfassung - Risiko-Assessment - Training-Status - Budget und Ressourcen - Strategische Empfehlungen

Empfänger: Management, Audit-Committee, Board

30.8.3.3 Jährliches Compliance-Review

Inhalte: - Jahres-Rückblick - Zertifizierungs-Status - Compliance-Programm-Effektivität - Lessons Learned - Strategische Planung für nächstes Jahr - Budget-Planung

Empfänger: Management, Board, Stakeholder

30.9 Compliance-Tools und -Systeme

30.9.1 Governance, Risk, and Compliance (GRC) Platform

System: {{ meta.grc_system }}

Version: {{ meta.grc_version }}

Management-URL: {{ meta.grc_url }}

Funktionen: - Compliance-Management - Risiko-Management - Audit-Management - Policy-Management - Incident-Management - Reporting und Dashboards

30.9.2 Dokumenten-Management

System: {{ meta.document_management_system }}

Funktionen: - Zentrale Dokumenten-Ablage - Versions-Kontrolle - Approval-Workflows - Zugriffs-Kontrolle - Audit-Trail

Dokumenten-Typen: - Policies und Procedures - Audit-Reports - Compliance-Nachweise - Training-Materialien - Verträge

30.9.3 Compliance-Scanning-Tools

Vulnerability-Scanner: {{ meta.vulnerability_scanner }}

Configuration-Scanner: {{ meta.config_scanner }}

Compliance-Scanner: {{ meta.compliance_scanner }}

Funktionen: - Automatische Compliance-Checks - Konfigurations-Audits - Benchmark-Vergleiche (CIS, STIG) - Continuous-Compliance-Monitoring

30.9.4 Training-Management

System: {{ meta.training_system }}

Funktionen: - Training-Katalog - Enrollment und Tracking - Zertifikate - Reporting - Phishing-Simulationen

30.10 Rollen und Verantwortlichkeiten

30.10.1 Compliance-Officer

Verantwortlichkeiten: - Compliance-Programm-Ownership - Compliance-Strategie - Audit-Koordination - Risiko-Management - Reporting an Management

Person: {{ meta.compliance_officer }}

30.10.2 Data Protection Officer (DPO)

Verantwortlichkeiten: - DSGVO-Compliance - Datenschutz-Beratung - Überwachung der Datenverarbeitung - Zusammenarbeit mit Aufsichtsbehörden - Schulungen

Person: {{ meta.data_protection_officer }}

30.10.3 Internal Audit Team

Verantwortlichkeiten: - Interne Audits durchführen - Audit-Planung - Findings dokumentieren - Follow-up auf Corrective Actions

Team-Lead: {{ meta.internal_audit_lead }}

30.10.4 CISO (Chief Information Security Officer)

Verantwortlichkeiten: - Security-Compliance - ISO 27001-Ownership - Security-Audits - Risiko-Management

Person: Thomas Weber

30.10.5 IT Operations Manager

Verantwortlichkeiten: - Operative Compliance-Umsetzung - ISO 20000-Ownership - Prozess-Compliance - Tool-Implementation

Person: Andreas Huemmer

30.10.6 Fachbereichs-Leiter

Verantwortlichkeiten: - Compliance in ihrem Bereich - Mitarbeiter-Training - Corrective-Actions-Umsetzung - Dokumentation

30.11 Best Practices

30.11.1 Compliance-Best-Practices

1. **Compliance by Design**
 - Compliance von Anfang an berücksichtigen
 - Nicht nachträglich “aufsetzen”
 - In Entwicklungs-Prozesse integrieren
2. **Automatisierung**
 - Compliance-Checks automatisieren
 - Continuous-Compliance-Monitoring
 - Automatische Reporting
3. **Dokumentation**
 - Alles dokumentieren
 - Dokumentation aktuell halten
 - Zentrale Ablage
4. **Training und Awareness**
 - Regelmäßige Trainings
 - Role-spezifische Schulungen
 - Awareness-Kampagnen
5. **Proaktives Management**
 - Nicht auf Audits warten
 - Regelmäßige Self-Assessments
 - Continuous Improvement
6. **Stakeholder-Engagement**

- Management-Support sichern
 - Fachbereiche einbinden
 - Kommunikation fördern
7. **Risiko-basierter Ansatz**
- Fokus auf kritische Bereiche
 - Ressourcen effizient einsetzen
 - Priorisierung
8. **Vendor-Management**
- Vendor-Compliance prüfen
 - Verträge mit Compliance-Klauseln
 - Regelmäßige Vendor-Audits

30.12 Audit-Kalender

30.12.1 Jährlicher Audit-Kalender

Monat	Audit-Typ	Standard	Durchführung
Januar	Internes Audit	ISO 27001	Internal Audit Team
Februar	Compliance-Review	DSGVO	DPO
März	Internes Audit	ISO 20000	Internal Audit Team
April	Externes Audit	ISO 27001	Zertifizierungs-Stelle
Mai	Vulnerability-Assessment	PCI-DSS	QSA
Juni	Internes Audit	ISO 27001	Internal Audit Team
Juli	Compliance-Review	Interne Policies	Compliance-Officer
August	Internes Audit	ISO 20000	Internal Audit Team
September	Externes Audit	ISO 20000	Zertifizierungs-Stelle
Oktober	Internes Audit	ISO 27001	Internal Audit Team
November	Penetration-Test	Security	Externe Pentester
Dezember	Jahres-Review	Alle Standards	Compliance-Officer

Hinweis: Kunden-Audits und Regulierungs-Audits werden ad-hoc eingeplant

30.13 Referenzen

- ISO/IEC 27001:2013 - Information Security Management
- ISO/IEC 20000-1:2018 - IT Service Management
- DSGVO (EU 2016/679) - Datenschutz-Grundverordnung
- BSI IT-Grundschutz-Kompendium
- PCI-DSS v4.0 - Payment Card Industry Data Security Standard
- SOX (Sarbanes-Oxley Act)
- COBIT 2019 - Control Objectives for Information and Related Technologies
- NIST SP 800-53 - Security and Privacy Controls
- CIS Controls v8 - Center for Internet Security Controls

Dokumentverantwortlicher: IT Operations Manager

Genehmigt durch: CIO

Version: 1.0.0

Klassifizierung: internal

Letzte Aktualisierung: {{ meta.date }}

ewpage

Chapter 31

Anhang: Checklisten und Vorlagen

31.1 Übersicht

Dieses Dokument enthält eine Sammlung von Checklisten, Vorlagen für Standarddokumente und Formularen für den IT-Betrieb. Ziel ist es, konsistente und effiziente Durchführung von Standardprozessen zu gewährleisten.

Dokumentverantwortlicher: IT Operations Manager

Genehmigt durch: CIO

Version: 1.0.0

Organisation: AdminSend GmbH

31.2 Checklisten

31.2.1 Incident-Management-Checklisten

31.2.1.1 Incident-Response-Checkliste

Incident-Response-Checkliste

****Incident-ID:**** [INC-XXXXX]
****Datum/Zeit:**** [YYYY-MM-DD HH:MM]
****Melder:**** [Name]
****Priorität:**** P1 / P2 / P3 / P4

Phase 1: Erkennung und Erfassung

- [] Incident erkannt und dokumentiert
- [] Priorität bewertet (P1-P4)
- [] Ticket erstellt
- [] Betroffene Systeme identifiziert
- [] Betroffene Benutzer identifiziert
- [] Erste Symptome dokumentiert

Phase 2: Klassifizierung und Priorisierung

- [] Incident-Kategorie zugewiesen
- [] Business-Impact bewertet
- [] Dringlichkeit bewertet
- [] Priorität bestätigt
- [] Verantwortlichen zugewiesen

Phase 3: Diagnose und Untersuchung

- [] Logs analysiert
- [] Monitoring-Daten geprüft
- [] Ähnliche Incidents gesucht
- [] Known Issues geprüft
- [] Root-Cause identifiziert (falls möglich)

Phase 4: Lösung und Wiederherstellung

- [] Lösungsansatz definiert
- [] Genehmigung eingeholt (falls erforderlich)
- [] Lösung implementiert
- [] Funktionalität validiert
- [] Benutzer informiert

Phase 5: Abschluss

- [] Incident gelöst
- [] Dokumentation vervollständigt
- [] Benutzer-Bestätigung eingeholt
- [] Ticket geschlossen
- [] Lessons Learned dokumentiert (bei P1/P2)

Kommunikation

- [] Stakeholder informiert
- [] Status-Updates kommuniziert
- [] Lösung kommuniziert

Bearbeitet von: [Name]

Abgeschlossen am: [YYYY-MM-DD HH:MM]

Dauer: [HH:MM]

31.2.1.2 Major-Incident-Checkliste

Major-Incident-Checkliste (P1)

Incident-ID: [INC-XXXXX]

Datum/Zeit: [YYYY-MM-DD HH:MM]

Incident-Manager: [Name]

Sofortmaßnahmen (0-15 Minuten)

- [] Major-Incident erklärt
- [] Incident-Manager benannt

- [] War-Room eingerichtet (physisch/virtuell)
- [] Kommunikations-Kanal etabliert
- [] Management informiert (CIO)
- [] Erste Status-Meldung versendet

Incident-Management (15-60 Minuten)

- [] Technisches Team zusammengestellt
- [] Rollen und Verantwortlichkeiten geklärt
- [] Diagnose gestartet
- [] Workaround gesucht
- [] Status-Updates alle 30 Minuten
- [] Eskalation vorbereitet (falls erforderlich)

Lösungsfindung (1-4 Stunden)

- [] Root-Cause identifiziert
- [] Lösungsansatz definiert
- [] Risikobewertung durchgeführt
- [] Genehmigung eingeholt
- [] Implementierung gestartet
- [] Rollback-Plan bereit

Wiederherstellung

- [] Lösung implementiert
- [] Funktionalität validiert
- [] Monitoring intensiviert
- [] Benutzer informiert
- [] Services wiederhergestellt

Nachbereitung

- [] Incident geschlossen
- [] Postmortem geplant (innerhalb 48h)
- [] Dokumentation vervollständigt
- [] Management-Report erstellt
- [] Verbesserungsmaßnahmen definiert

Kommunikation

- [] Initiale Benachrichtigung (< 15 Min)
- [] Status-Updates (alle 30 Min)
- [] Lösungs-Benachrichtigung
- [] Abschluss-Benachrichtigung
- [] Postmortem-Einladung

Incident-Manager: [Name]

Technischer Lead: [Name]

Kommunikations-Lead: [Name]

31.2.2 Change-Management-Checklisten

31.2.2.1 Standard-Change-Checkliste

Standard-Change-Checkliste

****Change-ID:**** [CHG-XXXXX]

****Datum:**** [YYYY-MM-DD]

****Change-Manager:**** [Name]

Planung

- [] Change-Request erstellt
- [] Beschreibung vollständig
- [] Begründung dokumentiert
- [] Risikobewertung durchgeführt
- [] Betroffene Systeme identifiziert
- [] Abhängigkeiten identifiziert
- [] Zeitfenster definiert
- [] Ressourcen allokiert

Genehmigung

- [] Change-Kategorie bestimmt (Standard/Normal/Emergency)
- [] Genehmiger identifiziert
- [] Genehmigung eingeholt
- [] CAB-Review (falls erforderlich)

Vorbereitung

- [] Implementierungsplan erstellt
- [] Rollback-Plan erstellt
- [] Test-Plan erstellt
- [] Kommunikationsplan erstellt
- [] Backup durchgeführt
- [] Test-Umgebung validiert

Implementierung

- [] Wartungsfenster gestartet
- [] Benutzer informiert
- [] Change implementiert
- [] Schritt-für-Schritt dokumentiert
- [] Probleme dokumentiert

Validierung

- [] Funktionalität getestet
- [] Performance validiert
- [] Monitoring geprüft
- [] Keine Fehler in Logs
- [] Benutzer-Akzeptanz-Test (falls erforderlich)

Abschluss

- [] Change erfolgreich
- [] Dokumentation aktualisiert
- [] CMDB aktualisiert
- [] Benutzer informiert
- [] Change geschlossen
- [] Lessons Learned (bei Problemen)

Rollback (falls erforderlich)

- [] Rollback-Entscheidung getroffen
- [] Rollback-Plan ausgeführt
- [] System wiederhergestellt
- [] Validierung durchgeführt
- [] Incident erstellt für Analyse

Change-Manager: [Name]

Implementiert von: [Name]

Status: Erfolgreich / Rollback / Abgebrochen

31.2.3 Backup und Recovery Checklisten

31.2.3.1 Backup-Verifikations-Checkliste

Backup-Verifikations-Checkliste

Datum: [YYYY-MM-DD]

Durchgeführt von: [Name]

Backup-Status

- [] Alle geplanten Backups durchgeführt
- [] Backup-Logs geprüft
- [] Keine Fehler in Logs
- [] Backup-Größen plausibel
- [] Backup-Zeiten akzeptabel

Backup-Integrität

- [] Checksummen validiert
- [] Backup-Dateien lesbar
- [] Keine Korruption festgestellt
- [] Verschlüsselung funktioniert

Restore-Test

- [] Zufälliges Backup ausgewählt
- [] Test-Umgebung vorbereitet
- [] Restore durchgeführt
- [] Daten validiert
- [] Funktionalität getestet
- [] Restore-Zeit gemessen

```

## Dokumentation
- [ ] Test-Ergebnis dokumentiert
- [ ] Probleme dokumentiert
- [ ] Verbesserungen identifiziert
- [ ] Report erstellt

## Systeme geprüft
- [ ] Datenbanken
- [ ] File-Server
- [ ] Anwendungs-Server
- [ ] Konfigurationen
- [ ] Virtualisierungs-Hosts

**Ergebnis:** Erfolgreich / Mit Problemen / Fehlgeschlagen
**Nächster Test:** [YYYY-MM-DD]

```

31.2.3.2 Disaster-Recovery-Test-Checkliste

```

# Disaster-Recovery-Test-Checkliste

**Test-Datum:** [YYYY-MM-DD]
**Test-Leiter:** [Name]
**Szenario:** [Beschreibung]

## Vorbereitung
- [ ] Test-Szenario definiert
- [ ] Test-Plan erstellt
- [ ] Teilnehmer informiert
- [ ] Test-Umgebung vorbereitet
- [ ] Backup-Daten bereitgestellt
- [ ] Kommunikationskanäle getestet

## Disaster-Simulation
- [ ] Disaster-Szenario ausgelöst
- [ ] Incident-Response aktiviert
- [ ] Kommunikation gestartet
- [ ] DR-Team mobilisiert
- [ ] DR-Standort aktiviert (falls zutreffend)

## Recovery-Durchführung
- [ ] DR-Plan befolgt
- [ ] Systeme wiederhergestellt
- [ ] Daten wiederhergestellt
- [ ] Netzwerk wiederhergestellt
- [ ] Anwendungen wiederhergestellt
- [ ] Zeiten gemessen (RTO/RPO)

```

```

## Validierung
- [ ] Alle kritischen Systeme online
- [ ] Datenintegrität geprüft
- [ ] Funktionalität getestet
- [ ] Performance akzeptabel
- [ ] Benutzer-Zugriff funktioniert

## Rückkehr zum Normalbetrieb
- [ ] Failback-Plan ausgeführt
- [ ] Primäre Systeme wiederhergestellt
- [ ] Daten synchronisiert
- [ ] Normalbetrieb wiederhergestellt
- [ ] DR-Standort deaktiviert

## Nachbereitung
- [ ] Test-Ergebnisse dokumentiert
- [ ] RTO/RPO-Zeiten dokumentiert
- [ ] Probleme identifiziert
- [ ] Verbesserungen definiert
- [ ] DR-Plan aktualisiert
- [ ] Lessons-Learned-Session durchgeführt

## Metriken
- **RTO-Ziel:** [Zeit]
- **RTO-Erreicht:** [Zeit]
- **RPO-Ziel:** [Zeit]
- **RPO-Erreicht:** [Zeit]
- **Erfolgsrate:** [%]

**Test-Ergebnis:** Erfolgreich / Teilweise erfolgreich / Fehlgeschlagen
**Nächster Test:** [YYYY-MM-DD]

```

31.2.4 Security-Checklisten

31.2.4.1 Security-Incident-Response-Checkliste

Security-Incident-Response-Checkliste

```

**Incident-ID:** [SEC-XXXXX]
**Datum/Zeit:** [YYYY-MM-DD HH:MM]
**Incident-Commander:** [Name]

```

Phase 1: Identifikation (0-30 Minuten)

```

- [ ] Security-Event erkannt
- [ ] Incident bestätigt
- [ ] Severity bewertet

```

- [] CISO informiert
- [] Security-Team mobilisiert
- [] Incident-Ticket erstellt

Phase 2: Eindämmung (30 Min - 2 Stunden)

- [] Betroffene Systeme identifiziert
- [] Systeme isoliert (falls erforderlich)
- [] Accounts gesperrt (falls erforderlich)
- [] Netzwerk-Segmentierung aktiviert
- [] Forensik-Daten gesichert
- [] Weitere Ausbreitung verhindert

Phase 3: Eradikation (2-8 Stunden)

- [] Malware entfernt
- [] Backdoors geschlossen
- [] Schwachstellen gepatcht
- [] Kompromittierte Accounts zurückgesetzt
- [] Systeme gehärtet

Phase 4: Wiederherstellung (8-24 Stunden)

- [] Systeme aus sauberem Backup wiederhergestellt
- [] Passwörter zurückgesetzt
- [] Monitoring intensiviert
- [] Systeme schrittweise online gebracht
- [] Funktionalität validiert

Phase 5: Lessons Learned (24-48 Stunden)

- [] Postmortem durchgeführt
- [] Timeline erstellt
- [] Root-Cause identifiziert
- [] Verbesserungen definiert
- [] Incident-Report erstellt

Kommunikation

- [] Management informiert
- [] Betroffene Benutzer informiert
- [] Behörden informiert (falls erforderlich)
- [] Kunden informiert (falls erforderlich)
- [] Medien-Statement (falls erforderlich)

Compliance

- [] DSGVO-Meldepflicht geprüft (72h)
- [] Aufsichtsbehörde informiert (falls erforderlich)
- [] Betroffene benachrichtigt (falls erforderlich)
- [] Dokumentation für Audit

Incident-Commander: [Name]

Forensik-Lead: [Name]

```
**Kommunikations-Lead:** [Name]
**Status:** Offen / Eingedämmt / Gelöst
```

31.3 Vorlagen

31.3.1 Incident-Report-Vorlage

Incident-Report

```
**Incident-ID:** [INC-XXXXX]
**Datum:** [YYYY-MM-DD]
**Erstellt von:** [Name]
```

Executive Summary

[Kurze Zusammenfassung des Incidents für Management]

Incident-Details

```
- **Priorität:** P1 / P2 / P3 / P4
- **Kategorie:** [Kategorie]
- **Betroffene Systeme:** [Liste]
- **Betroffene Benutzer:** [Anzahl/Beschreibung]
- **Beginn:** [YYYY-MM-DD HH:MM]
- **Ende:** [YYYY-MM-DD HH:MM]
- **Dauer:** [HH:MM]
```

Timeline

```
| Zeit | Ereignis | Aktion |
|---|---|---|
| HH:MM | [Ereignis] | [Aktion] |
| HH:MM | [Ereignis] | [Aktion] |
```

Root Cause

[Detaillierte Beschreibung der Ursache]

Impact

```
- **Business-Impact:** [Beschreibung]
- **Finanzielle Auswirkungen:** [Schätzung]
- **Reputations-Schaden:** [Bewertung]
- **Betroffene Services:** [Liste]
```

Lösung

[Beschreibung der implementierten Lösung]

Verbesserungsmaßnahmen

```
1. [Maßnahme 1] - Verantwortlich: [Name] - Frist: [Datum]
2. [Maßnahme 2] - Verantwortlich: [Name] - Frist: [Datum]
```

3. [Maßnahme 3] - Verantwortlich: [Name] - Frist: [Datum]

Lessons Learned

- [Lesson 1]
- [Lesson 2]
- [Lesson 3]

Anhänge

- [Logs]
- [Screenshots]
- [Monitoring-Daten]

Erstellt von: [Name]

Genehmigt von: Andreas Huemmer

Datum: [YYYY-MM-DD]

31.3.2 Change-Request-Vorlage

Change-Request

Change-ID: [CHG-XXXXX]

Datum: [YYYY-MM-DD]

Antragsteller: [Name]

Change-Details

- **Titel:** [Kurzer Titel]
- **Kategorie:** Standard / Normal / Emergency
- **Priorität:** Niedrig / Mittel / Hoch / Kritisch
- **Geplantes Datum:** [YYYY-MM-DD]
- **Geplante Zeit:** [HH:MM - HH:MM]
- **Dauer:** [Geschätzte Dauer]

Beschreibung

[Detaillierte Beschreibung des Changes]

Begründung

[Warum ist dieser Change notwendig?]

Betroffene Systeme

- [System 1]
- [System 2]
- [System 3]

Betroffene Benutzer

[Anzahl und Beschreibung der betroffenen Benutzer]

Risikobewertung

```

- **Risiko:** Niedrig / Mittel / Hoch
- **Impact:** Niedrig / Mittel / Hoch
- **Wahrscheinlichkeit:** Niedrig / Mittel / Hoch

## Risiken und Mitigationen
| Risiko | Wahrscheinlichkeit | Impact | Mitigation |
|---|---|---|---|
| [Risiko 1] | [L/M/H] | [L/M/H] | [Maßnahme] |
| [Risiko 2] | [L/M/H] | [L/M/H] | [Maßnahme] |

## Implementierungsplan
1. [Schritt 1]
2. [Schritt 2]
3. [Schritt 3]

## Rollback-Plan
1. [Schritt 1]
2. [Schritt 2]
3. [Schritt 3]

## Test-Plan
1. [Test 1]
2. [Test 2]
3. [Test 3]

## Kommunikationsplan
- **Vor Change:** [Wer, Wann, Wie]
- **Während Change:** [Wer, Wann, Wie]
- **Nach Change:** [Wer, Wann, Wie]

## Genehmigungen
- [ ] Technische Genehmigung: [Name] - [Datum]
- [ ] Business-Genehmigung: [Name] - [Datum]
- [ ] CAB-Genehmigung: [Name] - [Datum]

**Antragsteller:** [Name]
**Change-Manager:** Andreas Hueimmer
**Status:** Beantragt / Genehmigt / Abgelehnt / Implementiert

```

31.3.3 Postmortem-Vorlage

```

# Postmortem

**Incident-ID:** [INC-XXXXX]
**Datum:** [YYYY-MM-DD]
**Facilitator:** [Name]
**Teilnehmer:** [Namen]

```

```

## Incident-Zusammenfassung
[Kurze Zusammenfassung des Incidents]

## Timeline
| Zeit | Ereignis | Wer | Aktion |
|---|---|---|---|
| HH:MM | [Ereignis] | [Name] | [Aktion] |
| HH:MM | [Ereignis] | [Name] | [Aktion] |

## Was lief gut?
- [Punkt 1]
- [Punkt 2]
- [Punkt 3]

## Was lief nicht gut?
- [Punkt 1]
- [Punkt 2]
- [Punkt 3]

## Root Cause
[5-Why-Analyse oder andere Root-Cause-Methode]

1. **Warum trat das Problem auf?** [Antwort]
2. **Warum?** [Antwort]
3. **Warum?** [Antwort]
4. **Warum?** [Antwort]
5. **Warum?** [Antwort]

**Root Cause:** [Finale Ursache]

## Action Items
| # | Aktion | Verantwortlich | Frist | Status |
|---|---|---|---|---|
| 1 | [Aktion] | [Name] | [Datum] | Offen |
| 2 | [Aktion] | [Name] | [Datum] | Offen |
| 3 | [Aktion] | [Name] | [Datum] | Offen |

## Lessons Learned
- [Lesson 1]
- [Lesson 2]
- [Lesson 3]

## Verbesserungen
### Kurzfristig (< 1 Monat)
- [Verbesserung 1]
- [Verbesserung 2]

```

```

### Mittelfristig (1-3 Monate)
- [Verbesserung 1]
- [Verbesserung 2]

### Langfristig (> 3 Monate)
- [Verbesserung 1]
- [Verbesserung 2]

**Facilitator:** [Name]
**Datum:** [YYYY-MM-DD]
**Follow-Up:** [Datum für Review der Action Items]

```

31.4 Formulare

31.4.1 Zugriffs-Anforderungs-Formular

```

# Zugriffs-Anforderung

**Antragsteller:** [Name]
**Datum:** [YYYY-MM-DD]
**Abteilung:** [Abteilung]

## Benutzer-Informationen
- **Name:** [Vollständiger Name]
- **E-Mail:** [E-Mail-Adresse]
- **Telefon:** [Telefonnummer]
- **Abteilung:** [Abteilung]
- **Position:** [Position]
- **Manager:** [Manager-Name]

## Zugriffs-Details
- **System/Anwendung:** [Name]
- **Zugriffs-Level:** Read / Write / Admin
- **Begründung:** [Geschäftliche Begründung]
- **Dauer:** Permanent / Temporär bis [Datum]

## Erforderliche Berechtigungen
- [ ] [Berechtigung 1]
- [ ] [Berechtigung 2]
- [ ] [Berechtigung 3]

## Genehmigungen
- [ ] Manager-Genehmigung: [Name] - [Datum]
- [ ] Data-Owner-Genehmigung: [Name] - [Datum]
- [ ] Security-Genehmigung: [Name] - [Datum]

```

```

## IT-Bearbeitung
- **Bearbeitet von:** [Name]
- **Datum:** [YYYY-MM-DD]
- **Zugriff gewährt:** Ja / Nein
- **Kommentare:** [Kommentare]

**Status:** Beantragt / Genehmigt / Abgelehnt / Implementiert

```

31.4.2 Hardware-Anforderungs-Formular

Hardware-Anforderung

```

**Antragsteller:** [Name]
**Datum:** [YYYY-MM-DD]
**Abteilung:** [Abteilung]

## Benutzer-Informationen
- **Name:** [Vollständiger Name]
- **E-Mail:** [E-Mail-Adresse]
- **Abteilung:** [Abteilung]
- **Standort:** [Standort]
- **Manager:** [Manager-Name]

## Hardware-Details
- **Typ:** Laptop / Desktop / Monitor / Peripherie / Sonstiges
- **Spezifikation:** [Gewünschte Spezifikation]
- **Begründung:** [Geschäftliche Begründung]
- **Dringlichkeit:** Normal / Hoch / Kritisch

## Alte Hardware (falls Ersatz)
- **Typ:** [Typ]
- **Modell:** [Modell]
- **Seriennummer:** [Seriennummer]
- **Zustand:** [Zustand]
- **Rückgabe:** Ja / Nein

## Kosten
- **Geschätzte Kosten:** [Betrag]
- **Budget-Code:** [Budget-Code]
- **Kostenstelle:** [Kostenstelle]

## Genehmigungen
- [ ] Manager-Genehmigung: [Name] - [Datum]
- [ ] Budget-Genehmigung: [Name] - [Datum]
- [ ] IT-Genehmigung: [Name] - [Datum]

## IT-Bearbeitung

```

- ****Bearbeitet von:**** [Name]
- ****Bestelldatum:**** [YYYY-MM-DD]
- ****Lieferdatum:**** [YYYY-MM-DD]
- ****Installationsdatum:**** [YYYY-MM-DD]
- ****Asset-Tag:**** [Asset-Tag]

****Status:**** Beantragt / Genehmigt / Bestellt / Geliefert / Installiert

31.5 Prozesse und Verantwortlichkeiten

31.5.1 RACI-Matrix

Aktivität	Ops Manager	Ops Team	Service Desk	Benutzer
Checklisten-Erstellung	A	R	C	-
Vorlagen-Erstellung	A	R	C	-
Checklisten-Nutzung	C	R	R	-
Vorlagen-Nutzung	C	R	R	R
Aktualisierung	A	R	C	-

Legende: R = Responsible, A = Accountable, C = Consulted, I = Informed

31.6 Compliance und Standards

31.6.1 Relevante Standards

- **ITIL v4:** Service Operation Practice
 - **ISO 20000:** Clause 8.1 - Operational Planning and Control
 - **COBIT 2019:** DSS01 - Managed Operations
-

31.7 Anhang

31.7.1 Glossar

Begriff	Definition
Checkliste	Strukturierte Liste von Aufgaben oder Prüfpunkten
Vorlage	Standardisiertes Dokument-Format
Formular	Strukturiertes Eingabe-Dokument
Postmortem	Nachträgliche Analyse eines Incidents

31.7.2 Referenzen

- ITIL v4 Foundation Handbook

- ISO/IEC 20000-1:2018
- COBIT 2019 Framework

Letzte Aktualisierung: {{ meta.date }}

Nächste Review: [TODO: Datum]

Kontakt: andreas.huemmer@adminsind.de

ewpage