

Referenzprofil

# IT Systems Administrator

Mirko Prehn

Dieses Referenzprofil wurde im Rahmen des bmb+f geförderten Projekts „Arbeitsprozessorientierte Weiterbildung in der IT-Branche“ erarbeitet von:



Fraunhofer ISST

Bildungspartner

## **Danksagung**

---

Diese Profilbeschreibung entstand auf Basis mehrerer Praxisprojekte der Firma Elektro Technologie Zentrum Stuttgart, deren Mitarbeiter Frau Birke und Herrn Denk wir herzlich für ihre fachkundige und umfassende Hilfe danken. Fachlich beratend mitgewirkt haben Herr Mütznier aus dem Fraunhofer-Institut für Software- und Systemtechnik sowie Herr Funk aus dem Elektro Technologie Zentrum Stuttgart. Ohne ihre Hilfe wäre dieses Dokument nicht in dieser hohen Qualität entstanden.

# Inhaltsverzeichnis

---

<b>IT SYSTEMS ADMINISTRATOR .....</b>	<b>1</b>
<b>1 EINFÜHRUNG: REFERENZPROZESSE ALS CURRICULA.....</b>	<b>1</b>
1.1 EREIGNIS-PROZESS-KETTEN: SYMBOLIK .....	2
1.2 REFERENZPROZESS UND TEILPROZESSE.....	3
<b>2 DAS PROFIL: IT SYSTEMS ADMINISTRATOR .....</b>	<b>6</b>
2.1 TÄTIGKEITSBESCHREIBUNG .....	6
2.2 PROFILTYPISCHE ARBEITSPROZESSE .....	6
2.3 PROFILPRÄGENDE KOMPETENZFELDER .....	8
2.4 QUALIFIKATIONSERFORDERNISSE .....	9
2.5 EINORDNUNG INS SYSTEM UND KARRIEREPFADE .....	9
<b>3 REFERENZPROZESSE IT SYSTEMS ADMINISTRATOR .....</b>	<b>11</b>
3.1 CHANGE-MANAGEMENT .....	11
3.1.1 Der Referenzprozess Change-Management .....	12
3.1.2 Prozesskompass Change-Management .....	13
3.1.2.1 Analysieren der Anforderungen.....	14
3.1.2.2 Ausarbeiten eines Angebots .....	17
3.1.2.3 Planen der Abwicklung .....	19
3.1.2.4 Beschaffen der erforderlichen Komponenten.....	21
3.1.2.5 Installieren der Hardwarekomponenten.....	23
3.1.2.6 Installieren und Konfigurieren nach Anforderungen.....	26
3.1.2.7 Überprüfen des installierten und konfigurierten Systems.....	28
3.1.2.8 Durchführen der Übergabe .....	31
3.1.2.9 Erstellen einer Prozessdokumentation.....	33
3.1.2.10 Informieren betroffener Stellen/Personen .....	35
3.2 FAULT-MANAGEMENT .....	37
3.2.1 Referenzprozess Fault-Management .....	38
3.2.2 Prozesskompass Fault-Management.....	39
3.2.2.1 Durchführen der initialen Bereitstellung.....	40
3.2.2.2 Durchführen kontinuierlicher Überwachung.....	43
3.2.2.3 Wahrnehmen der Störung .....	45
3.2.2.4 Ermitteln des Störungsorts.....	47
3.2.2.5 Eingrenzen des Fehlertyps .....	49
3.2.2.6 Planen der Abwicklung .....	52
3.2.2.7 Ausführen der Arbeiten nach Plan .....	54
3.2.2.8 Durchführen von Tests (im Fehlerumfeld) .....	56
3.2.2.9 Erstellen einer Prozessdokumentation.....	59
3.2.2.10 Informieren betroffener Personen/Stellen .....	61
3.3 PERFORMANCE-MANAGEMENT .....	63
3.3.1 Der Referenzprozess Performance-Management .....	64
3.3.2 Prozesskompass Performance-Management .....	65
3.3.2.1 Durchführen der initialen Bereitstellung.....	66
3.3.2.2 Durchführen kontinuierlicher Messungen .....	69
3.3.2.3 Analysieren der Schwellwertüberschreitung .....	71
3.3.2.4 Lokalisieren des Engpasses.....	73
3.3.2.5 Erstellen von Handlungsalternativen.....	75
3.3.2.6 Durchführen Fault-Management .....	77
3.3.2.7 Durchführen Change-Management .....	78
3.3.2.8 Erstellen einer Prozessdokumentation.....	79
3.3.2.9 Informieren betroffener Personen/Stellen .....	80
3.4 SECURITY-MANAGEMENT .....	82
3.4.1 Der Referenzprozess Security-Management .....	83
3.4.2 Prozesskompass Security-Management .....	84
3.4.2.1 Umsetzen der Richtlinien auf Systemebene .....	85
3.4.2.2 Durchführen kontinuierlicher Kontrollen .....	88

3.4.2.3	Umfassendes Informieren.....	90
3.4.2.4	Analysieren des Vorkommnisses .....	92
3.4.2.5	Untersuchen der Auswirkungen.....	94
3.4.2.6	Reaktives Entwickeln von Ad-hoc-Lösungen .....	96
3.4.2.7	Aktives Entwickeln von Umsetzungsmöglichkeiten .....	98
3.4.2.8	Durchführen Change-Management .....	101
3.4.2.9	Ausführen von Sicherheitschecks.....	102
3.4.2.10	Erstellen einer Prozessdokumentation.....	104
3.4.2.11	Informieren betroffener Personen/Stellen .....	106
3.5	DATENSICHERUNG .....	108
3.5.1	Der Referenzprozess Datensicherung .....	109
3.5.2	Prozesskompass Datensicherung .....	110
3.5.2.1	Erarbeiten eines Datensicherungskonzepts.....	111
3.5.2.2	Umsetzen des Datensicherungskonzepts.....	113
3.5.2.3	Durchführen der Datensicherung und Überwachung.....	115
3.5.2.4	Wiederherstellen von Daten.....	117
3.6	BENUTZERVERWALTUNG UND ORGANISATION .....	120
3.6.1	Der Referenzprozess „Benutzerverwaltung und Organisation“ .....	121
3.6.2	Prozesskompass Benutzerverwaltung und Organisation .....	122
3.6.2.1	Erstellen eines Vorschlages für Verfahrens- und Organisationsstrukturen.....	123
3.6.2.2	Erstellen eines Vorschlag für Servicestrukturen .....	125
3.6.2.3	Zulassen von Benutzern .....	127
3.6.2.4	Einweisen der Benutzer .....	129
3.6.2.5	Verwaltung der Lizenzen .....	131
3.6.2.6	Bereitstellen von Systemressourcen.....	133
3.6.2.7	Durchführen von Service .....	135
3.6.2.8	Überprüfen des Services .....	137

# 1 Einführung: Referenzprozesse als Curricula

---

Das Referenzprojekt des IT Systems Administrator verdeutlicht paradigmatisch die diesem Tätigkeitsfeld zu Grunde liegenden Arbeitsprozesse, die mit ihm

en verbundenen Ansprüche sowie die daraus resultierenden Anforderungen an Inhalt und Durchführung einer qualitativ hochwertigen Weiterbildung.

Das Referenzprojekt erfüllt mehrere Funktionen:

## **Aus der Praxis für die Praxis:**

Als Abstraktion tatsächlich stattgefundener Projekte und Prozesse bieten die Referenzprozesse eine realistische und leicht nachvollziehbare Abbildung dessen, was die Tätigkeiten eines IT Systems Administrator sind.

## **Prozessorientierung als innovatives „Curriculum“:**

Als vollständige Darstellung aller wichtigen Arbeitsprozesse sowie der dazugehörigen Qualifikationen, Tätigkeiten und Werkzeuge bieten die Referenzprozesse die Grundlage für die Weiterbildung zum IT Systems Administrator. Alle diese Prozesse müssen - entsprechend den Vorgaben - einmal oder mehrfach durchlaufen werden und ermöglichen dadurch den Weiterzubildenden den arbeitsplatznahen, integrativen Erwerb von relevanten Kompetenzen. Durch den Verbleib im Arbeitsprozess wird nicht nur für die Weiterzubildenden eine hohe Motivation (Arbeit an echten Projekten/Aufgaben) und Nachhaltigkeit erreicht, sondern auch - aus Sicht des Unternehmens - die Kontinuität und Qualität der laufenden Arbeiten gesichert (keine Ausfallzeit durch Seminartage, kein mühsamer Transfer).

## **Qualitätsstandard für die Weiterbildung:**

Als Referenz bieten insbesondere die Teilprozesse und die mit ihnen verbundenen Tätigkeits- und Qualifikationsziele einen Qualitätsmaßstab für die arbeitsprozessorientierte Weiterbildung und die resultierenden Abschlüsse. Vollständige Transparenz und klare Zielvorgaben ermöglichen die qualitativ hochwertige Absicherung auch komplexer Kompetenzen sowie den systematischen Erwerb des notwendigen Erfahrungswissens.

## **Transferprozesse:**

Die Generalisierung des Referenzprojekts aus der Praxis und seine didaktische Anreicherung ermöglichen eine leichte Auswahl angemessener Transferprozesse, deren Bearbeitung die Grundlage der Weiterbildung ist. Transferprozesse sind reale Prozesse, die Referenzprojekte in einer lernförderlichen Umgebung abbilden. Abgeschlossene Transferprozesse auf Basis der hier dargestellten Anforderungen und Qualitätsmaßstäbe sind nicht nur Qualifikationsnachweis des Einzelnen, sondern bilden auch die Basis eines angemesseneren und zielgerichteteren Umgangs mit Geschäfts- und Arbeitsprozessen im Unternehmen.

## 1.1 Ereignis-Prozess-Ketten: Symbolik

---

Die Darstellung der Referenzprozesse in Form von Ereignis-Prozess-Ketten<sup>1</sup> ermöglicht einen schnellen Überblick. Vollständigkeit kann leicht überprüft werden, Anpassungen und Modifikationen in Hinblick auf das eigene Unternehmen sind problemlos möglich und Anknüpfungspunkte an andere Prozesse, aber auch zu weiterführenden Informationen ergeben sich automatisch.

Die bei der Darstellung der Referenz- und Teilprozesse verwendete Modellierungssprache stellt eine Anpassung und Weiterentwicklung der klassischen EPK-Modellierung dar:

Referenz- wie Teilprozesse sind aus der Sicht des jeweiligen Spezialisten, also als Arbeitsprozesse einer Person dargestellt.

Referenz- wie Teilprozesse stellen in der Regel keinen Geschäftsprozess dar.

Die EPK-Symbole werden hier wie folgt verwendet:

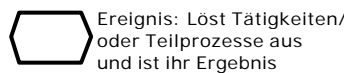
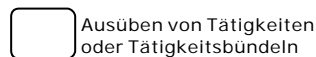
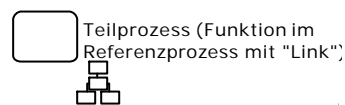


Abbildung 1: Grundlegende Symbole der Referenz- und Teilprozessmodelle

Die wichtigsten Symbole sind:

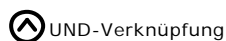
die Tätigkeiten bzw. Tätigkeitsbündel oder Teilprozesse, die mit dem Funktionssymbol dargestellt werden;

die Ereignisse, die Tätigkeiten bzw. Teilprozesse auslösen und Ergebnisse von Teilprozessen sind.

Grundsätzlich gilt:

Auf ein Ereignis folgt immer ein Teilprozess bzw. eine Tätigkeit.

Ergebnisse von Tätigkeiten sind sehr oft Dokumente, diese werden dann zusätzlich durch das Dokument-Symbol dargestellt.

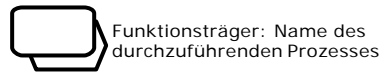


---

<sup>1</sup> vgl. A.-W. Scheer, Wirtschaftsinformatik, Springer 1998

*Abbildung 2: Konnektoren*

Wenn Alternativ-Möglichkeiten bestehen, werden Ereignisse und Teilprozesse/Tätigkeiten über Konnektoren (AND, OR, XOR) verbunden. Dabei steht AND für ein verbindendes „und“, OR für ein „oder“, das alle Möglichkeiten offen lässt und XOR für ein „ausschließendes oder“, welches nur einen der angegebenen Pfade ermöglicht.

*Abbildung 3: Schnittstelle*

Da die Prozesse aus der Sicht des jeweiligen Spezialisten formuliert werden, sind Schnittstellen zu Prozessen anderer Spezialisten oder zu Entscheidungsprozessen auf höherer Ebene notwendig. Dazu wird das Schnittstellensymbol verwendet. Es steht für Prozesse, die der Spezialist nicht selber durchführt, auf deren Durchführung er aber angewiesen ist. Parallel zu jeder Schnittstelle wird die Tätigkeit dargestellt, die der Spezialist selbst in diesem Zusammenhang ausübt, wie „Beraten bei ...“, „Unterstützen bei ...“ oder „Informieren des ...“.

Alle Prozesse werden durch die Verwendung dieser Symbole klar und einfach strukturiert dargestellt und sind offen für die Übertragung in konkrete Transferprozesse.

## 1.2 Referenzprozess und Teilprozesse

---

Die hier vorgestellten Referenzprozesse und ihre Teilprozesse stellen das Curriculum des Spezialistenprofils IT Systems Administrator dar.

Der Referenzprozess erhebt nicht den Anspruch eines Vorgehensmodells, sondern bildet beispielhaft den möglichen Arbeitsprozess und Verlauf eines Projekts auf Spezialistenebene ab.

Er bildet die Grundlage für Weiterbildungen und damit einen Qualitäts-, Niveau- und Komplexitätsmaßstab. Die zugehörigen Teilprozesse sind hier beispielhaft modelliert und stellen eine Möglichkeit der Durchführung dar. Einzelheiten zu den unverzichtbaren Prozessen und Kompetenzfeldern sind hier im Referenzprojekt festgelegt. Die Reihenfolge und die Inhalte der Teilprozesse sind abhängig vom jeweils auszuwählenden Transferprojekt und werden in diesem Zusammenhang festgelegt.

Die Darstellung der Prozesse erfolgt systematisch:

Jeder Prozess wird mit Hilfe von Ereignis-Prozess-Ketten dargestellt. Einem auslösenden Ereignis folgt eine Funktion, die wiederum ein oder mehrere Ereignisse als Ergebnis hat. Ereignisse und Funktionen können mit AND, OR oder XOR, den Konnektoren, verbunden sein.

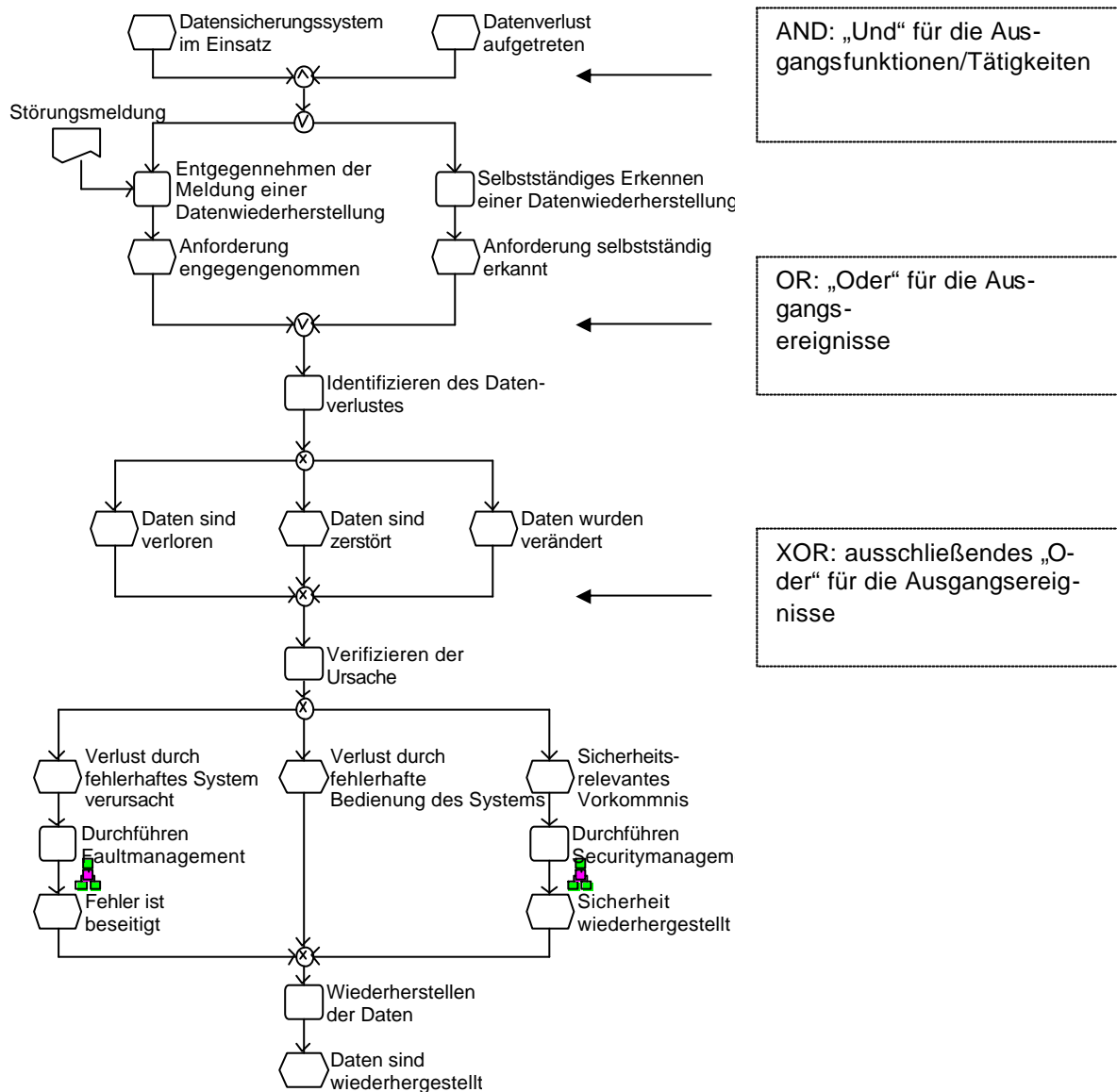


Abbildung 4: Beispielprozess (Teilprozess "Datensicherung") mit unterschiedlicher Verwendung von Konnektoren

Die Verbindung von Referenzprozess und Teilprozessen erfolgt über die Funktionen des Referenzprozesses:

Jede Funktion im Referenzprozess steht für einen Teilprozess.

Ereignisse, die dem jeweiligen Teilprozess direkt vor oder nachgeordnet sind, sind Anfangs- und Endereignisse der jeweiligen Teilprozesse. Damit stellen die Teilprozesse die Funktionen des Referenzprozesses ausführlich dar und ein Hin- und Herbewegen zwischen Referenz- und Teilprozessen ist jederzeit problemlos möglich.



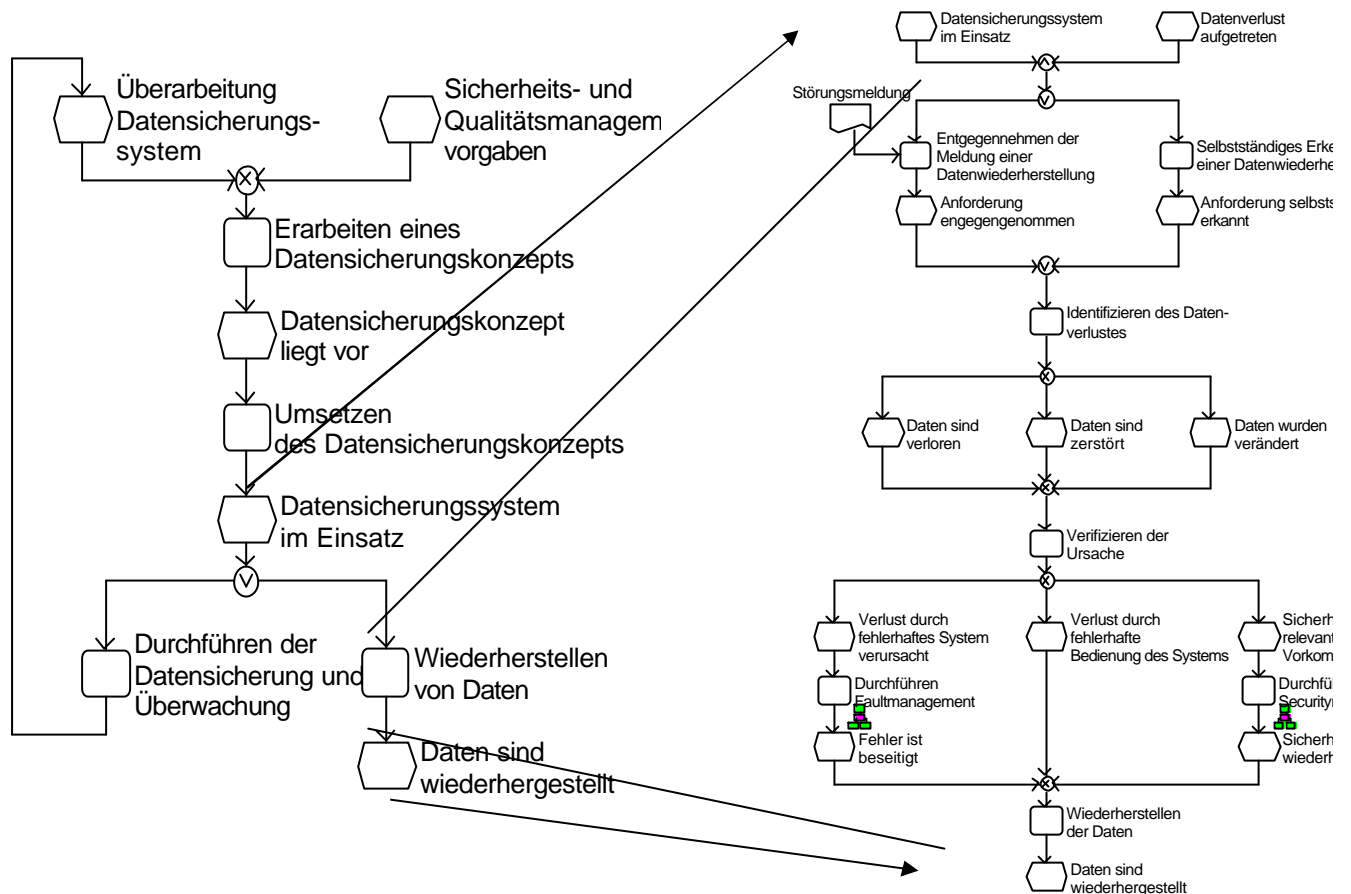


Abbildung 5: Referenzprozess „Datensicherung“ des IT Administrators

Abbildung 6: Teilprozess des IT Administrators "Datenwiederherstellung"

"

Die Teilprozesse stellen so die wesentlichen Teile eines Projekts dar und lassen sich entsprechend auf Transferprojekte übertragen. Den Teilprozessen sind die jeweils wesentlichen Tätigkeiten und Kompetenzfelder zugeordnet.

## 2 Das Profil: IT Systems Administrator

---

IT Systems Administrator<sup>2</sup> betreiben komplexe IT-Systeme. Sie analysieren und bewerten den Bedarf an Soft- und Hardware, planen entsprechende Beschaffungen, installieren und konfigurieren Software, Systeme und Komponenten. Sie organisieren den Betrieb von Hard- und Software, einschließlich automatischer Updates und Backups sowie den Benutzersupport. Sie administrieren Server und Anwendungen, verwalten Nutzerkonten, Zugriffsrechte und Verzeichnisdienste. Sie analysieren Probleme, isolieren und beheben fehlerhafte Zustände und erarbeiten Richtlinien für den Systembetrieb. Sie erarbeiten neue technische Konzepte für den Systembetrieb und entwickeln die Systeme unter Beachtung der Auswirkungen der Veränderungen bedarfsgerecht und wirtschaftlich weiter. IT Systems Administrator planen und überprüfen Sicherheitsmaßnahmen gegen Angriffe von außen und von innen.

### 2.1 Tätigkeitsbeschreibung

---

Das Profil des IT Systems Administrator lässt sich in sechs Referenzprozesse (Change-, Fault-, Performance-, Security-Management, Datensicherung sowie Benutzerberatung und Organisation) unterteilen. Dabei kann es sich um die Betreuung eines einzelnen Systems ohne die Verbindung zu anderen Systemen handeln, so dass keine Schnittstellen berücksichtigt werden müssen. In der Regel wird es aber Verbindungen zu einem oder mehreren Systemen geben, die sich entweder innerhalb des eigenen Zugriffsbereichs befinden und daher selbst verwaltet werden können oder aber externe Verbindungen darstellen, so dass der eigene Zugriffsbereich an diese Infrastrukturschnittstellen angepasst werden muss.

Jeder dieser Teilprozesse ist so beschrieben, dass er die Kernaufgaben eines IT-Systemadministrators beschreibt und verläuft im Wesentlichen linear: Analyse, Planung, Durchführung und Test. Es ist dabei anzumerken, dass sich die Teilprozesse Fault-, Performance- und Security-Management gegebenenfalls des Prozesses Change-Management bedienen, sofern eine Änderung am IT-System notwendig ist.

Die jeweiligen Ausprägungen der einzelnen Teilprozesse können in Form, Tiefe und Umfang stark schwanken, welches aber nicht den grundsätzlichen Verlauf beeinflusst.

### 2.2 Profiltypische Arbeitsprozesse

---

Die im Folgenden beschriebenen Teilprozesse dokumentieren den gesamten profiltypischen Arbeitsprozess der IT-Spezialisten. Die Beherrschung dieses Arbeitsprozesses in Verbindung mit den Kompetenzen in den jeweiligen Kompetenzfeldern und der Berufserfahrung bilden die Grundlage für die berufliche Handlungskompetenz.

- 1 Change-Management
  - 1.1 Analysieren der Anforderung, Prüfen des Änderungsbedarfs aus technischer Sicht, Durchführen von Evaluierungen und Variantenvergleichen. Durchführen von Wirtschaftlichkeitsbetrachtungen.
  - 1.2 Erstellen und Weiterentwickeln von Betriebskonzepten, Planen der Änderungen.
  - 1.3 Ausarbeiten von Angeboten, Führen und Begleiten von Vertragsverhandlungen.

---

<sup>2</sup> Das Kapitel 2 gibt – mit Ausnahme des Abschnittes 2.1 „Tätigkeitsbeschreibung“ – den offiziellen Text der „Verordnung über die Spezialistenprofile im Rahmen des Verfahrens zur Ordnung der IT-Weiterbildung“ vom 25.05.2002 (Bundesanzeiger 105, ausgegeben am 12.06.2002) wieder.

- 1.4 Beschaffen von Hard- und Software.
- 1.5 Vorbereiten und Inbetriebnahme von informationstechnischer Hardware. Installieren der Betriebssysteme und der Software. Installieren von Übertragungsmedien und Schnittstellen. Installieren von Serverdiensten.
- 1.6 Konfigurieren der Hard- und Software sowie der Betriebssysteme. Abstimmen von Schnittstellen. Konfigurieren von Serverdiensten.
- 1.7 Prüfen der durchgeführten Änderungen. Integrieren des Systems in die bestehende Infrastruktur.
- 1.8 Durchführen der Übergabe an (interne) Kunden. Durchführen von Einweisungen und Schulungen von Nutzern in neue und geänderte Systeme.
- 1.9 Erstellen von Prozessdokumentationen.
- 2 Fault-, Performance- und Security-Management
  - 2.1 Durchführen der initialen Bereitstellung. Umsetzen des Sicherheitskonzepts.
  - 2.2 Durchführen kontinuierlicher Überwachungen, Messungen und Kontrollen.
  - 2.3 Wahrnehmen von Störungen, Analysieren von Schwellwertüberschreitungen, Vorkommnissen und ihres Bedrohungspotentials.
  - 2.4 Lokalisieren von Störungen oder Engpässen.
  - 2.5 Eingrenzen der Fehlerart. Gegebenenfalls Prüfen der Aktivitäten eines Angreifers und Feststellen von Schädigungen.
  - 2.6 Reaktives Entwickeln von Ad-hoc-Lösungen falls notwendig.
  - 2.7 Planen der Problembeseitigung, Spezifizieren der Parameter für Ressourcenplanungen sowie Vergleichen und Auswählen von Handlungsalternativen.
  - 2.8 Durchführen von Fehlerbeseitigungen, Tuning bzw. Ausführen von Change-Managementprozessen. Testen der erfolgten Änderung.
  - 2.9 Informieren betroffener Personen und Stellen. Durchführen von Einweisungen und Schulungen in geänderte oder neue Systeme.
  - 2.10 Erstellen von Prozessdokumentationen.
- 3 Datensicherung und Backup
  - 3.1 Erarbeiten von Datensicherungs- und Backup-Konzepten sowie Ausfallszenarien gemäß Sicherheits- und Qualitätsmanagementvorgaben.
  - 3.2 Umsetzen des Konzepts: Planung, Beschaffung erforderlicher Hard- und Software, Installation und Konfiguration.
  - 3.3 Regelmäßiges Durchführen von Datensicherungen und Backups bzw. Überwachen der Durchführung.
  - 3.4 Sichern der Datenintegrität und -vertraulichkeit.
- 4 Organisation und Beratung
  - 4.1 Verwalten von Nutzern und Rechten, Betreiben von Verzeichnisdiensten.
  - 4.2 Technisches Beraten von nichtfachlichen Projektleitern bei Projektplanung und Projektmanagement im Netzwerkbereich.
  - 4.3 Durchführen Support für (interne) Kunden zur Gewährleistung der Kundenzufriedenheit.

## 2.3 Profilprägende Kompetenzfelder

---

Die Beherrschung der profiltypischen Arbeitsprozesse setzt Kompetenzen unterschiedlicher Reichweite in den nachstehend aufgeführten beruflichen Kompetenzfeldern<sup>3</sup> voraus. Den Kompetenzfeldern sind Wissen und Fähigkeiten sowie typische Methoden und Werkzeuge unterschiedlicher Breite und Tiefe zugeordnet.

Grundlegend zu beherrschende, gemeinsame Kompetenzfelder<sup>4</sup>:

- Unternehmensziele und Kundeninteressen,
- Problemanalyse, -lösung,
- Kommunikation, Präsentation,
- Konflikterkennung, -lösung,
- Fremdsprachliche Kommunikation (englisch),
- Projektorganisation, -kooperation,
- Zeitmanagement, Aufgabenplanung und -priorisierung,
- Wirtschaftliches Handeln,
- Selbstlernen, Lernorganisation,
- Innovationspotenziale,
- Datenschutz, -sicherheit,
- Dokumentation, -standards,
- Qualitätssicherung.

Fundiert zu beherrschende, gruppenspezifische Kompetenzfelder:

- Datenbanken, Netzwerke, Betriebssysteme
- Datensicherungskonzepte,
- Sicherheitskonzepte und -überwachung,
- Statistik und Datenvisualisierung,
- Wirtschaftlichkeitsanalysen,
- Marktüberblick,
- Unternehmensorganisation,
- Nutzerorientierte Problemanalyse, -lösung.

Routiniert zu beherrschende, profilspezifische Kompetenzfelder:

- Betriebssystemkonzepte,
- Systemmanagement-, Systemanalysewerkzeuge,
- Systemkomponenten,
- Übertragungsprotokolle,
- Client-Server-Systeme, heterogene Systeme,
- Systemintegration und -anpassung,
- Serverdienste, Anwendungen.

---

<sup>3</sup> Die Kompetenzfelder werden in der nachfolgenden Auflistung jeweils durch ein zusammenfassendes Stichwort benannt. Da die Weiterbildung zum Spezialisten auf die erfolgreiche Bewältigung zunehmend offener beruflicher Handlungssituationen sowie ganzheitlichen Kompetenzerwerb abzielt, bildet der Kompetenzerwerb einen integralen Bestandteil der Arbeits- und Weiterbildungsprozesse und lässt sich nur im Zusammenhang mit diesen operationalisieren (vgl. dazu die Abschnitte „Kompetenzfelder“ in den folgenden Kapiteln und die dortigen beispielhaften Zuordnungen).

<sup>4</sup> Jeder Spezialist muss in den in diesem Abschnitt genannten „weichen“ Kompetenzfeldern wie „Kommunikation, Präsentation“, „Konflikterkennung, -lösung“ usw. ein Niveau erreichen, dass über dem einer Fachkraft liegt. D.h. er muss auch in diesen Feldern zu eigenständigem Handeln in der Lage sein und zum Erreichen des Ziels in dem jeweiligen Feld gegebenenfalls über den Rahmen bekannter Verfahren und Lösungen hinaus gehen können.

## 2.4 Qualifikationserfordernisse

---

Im Regelfall wird ein hinreichendes Qualifikationsniveau auf der Basis einschlägiger Berufsausbildung oder Berufserfahrung vorausgesetzt.

## 2.5 Einordnung ins System und Karrierepfade

---

Das neue IT-Weiterbildungssystem gibt auf Basis der vier neuen IT-Ausbildungsberufe drei Ebenen für die Weiterqualifizierung vor: Spezialisten, wie auch der IT Systems Administrator einer ist, operative und strategische Professionals. Auf der Ebene der Spezialisten existieren eine Reihe verwandter Profile und selbstverständlich kann sich auch der IT Systems Administrator zu einem Professional weiterqualifizieren.

### Verwandte Profile

Der IT Systems Administrator weist eine Reihe verwandter Profile auf, die sich in drei Gruppen einteilen lassen:

- Administratoren mit erweiterten Aufgabenbereich, dazu gehören der IT Trainer im Bereich der Schulung von Benutzern an verschiedenen Systemen und nicht zuletzt der Business Systems Advisor;
- Profile, deren Aufgabengebiete sich mit denen des IT Systems Administrator überschneiden können, wie der Network Administrator, der IT Configuration Coordinator, der IT Security Coordinator. Beispielsweise arbeitet der IT Security Coordinator Sicherheitsrichtlinien aus, die der IT Systems Administrator im gesamten IT-System einführen und deren Einhaltung kontrollieren muss.

### Aufstiegsqualifizierung

Das Tätigkeitsfeld des IT Systems Administrator ist eine ideale Grundlage für Aufstiegsqualifizierungen insbesondere zum IT Systems Manager und zum IT Business Manager. Zum Beispiel können IT Business Manager Rechenzentren leiten.



### 3 Referenzprozesse IT Systems Administrator

---

Die Referenzprozesse des IT Systems Administrator beschreiben die Administration eines IT-Systems, vom Aufbau eines Systems über die Fehlerbeseitigung und Performanceoptimierung bis zur Etablierung von Sicherheitskonzepten.

Die Referenzprozesse des IT Systems Administrator sind:

- Change-Management
- Fault-Management
- Performance-Management
- Security-Management
- Datensicherung
- Benutzerverwaltung und Organisation

Im folgenden werden die Referenzprozesse der Reihe nach vorgestellt und in Teilprozessen detailliert ausgeführt.

#### 3.1 Change-Management

---

Sobald Veränderungen an einem bestehenden IT-System vorgenommen werden müssen bzw. ein völlig neues IT-System aufgebaut werden soll, bedienen sich IT Systems Administrator dieses Teilprozesses.

Ein wesentlicher Bestandteil dieses Prozesses ist das von den ISO Standards her bekannte Konfigurationsmanagement, der gesamte Teilprozess ist jedoch deutlich umfangreicher.

Angestoßen durch einen Änderungsbedarf analysieren IT Systems Administrator die Anforderungen. Sie führen einen Variantenvergleich durch, um somit sowohl auf technischer als auch wirtschaftlicher Seite eine möglichst optimale Lösung zu entwickeln und planen deren Umsetzung.

Sofern notwendig, beschaffen IT Systems Administrator die benötigten Komponenten (Soft- und Hardware). Sie führen die dazu notwendigen Verhandlungen mit den Lieferanten durch.

Je nach Anforderung werden entweder neue Hardware in das IT-System integriert, neue Software installiert und konfiguriert oder bestehende Komponenten angepasst.

Nach erfolgter Installation unterziehen IT Systems Administrator ihr IT-System einen ersten Test um zu überprüfen, ob die Komponenten wie gewünscht funktionieren. Ein weiterer Test wird nach der Konfiguration durchgeführt. Hierbei wird überprüft, ob die konfigurierte Hard- und Software keine unerwünschten Seiteneffekte verursacht. Ein abschließender Test überprüft, ob die Anforderungen korrekt umgesetzt wurden. Gegebenenfalls werden Nacharbeiten durchgeführt, um das Change-Management erfolgreich abzuschließen.

Der gesamte Prozess und die durchgeführten Änderungen (Konfigurationsdatei) werden dokumentiert und durch einen Soll-Ist-Vergleich komplettiert. In umfangreichen Projekten muss gegebenenfalls der Prozess Change-Management einmal in der Evaluationsphase und einmal in der Umsetzungs- und Produktionsphase durchlaufen werden.

### 3.1.1 Der Referenzprozess Change-Management

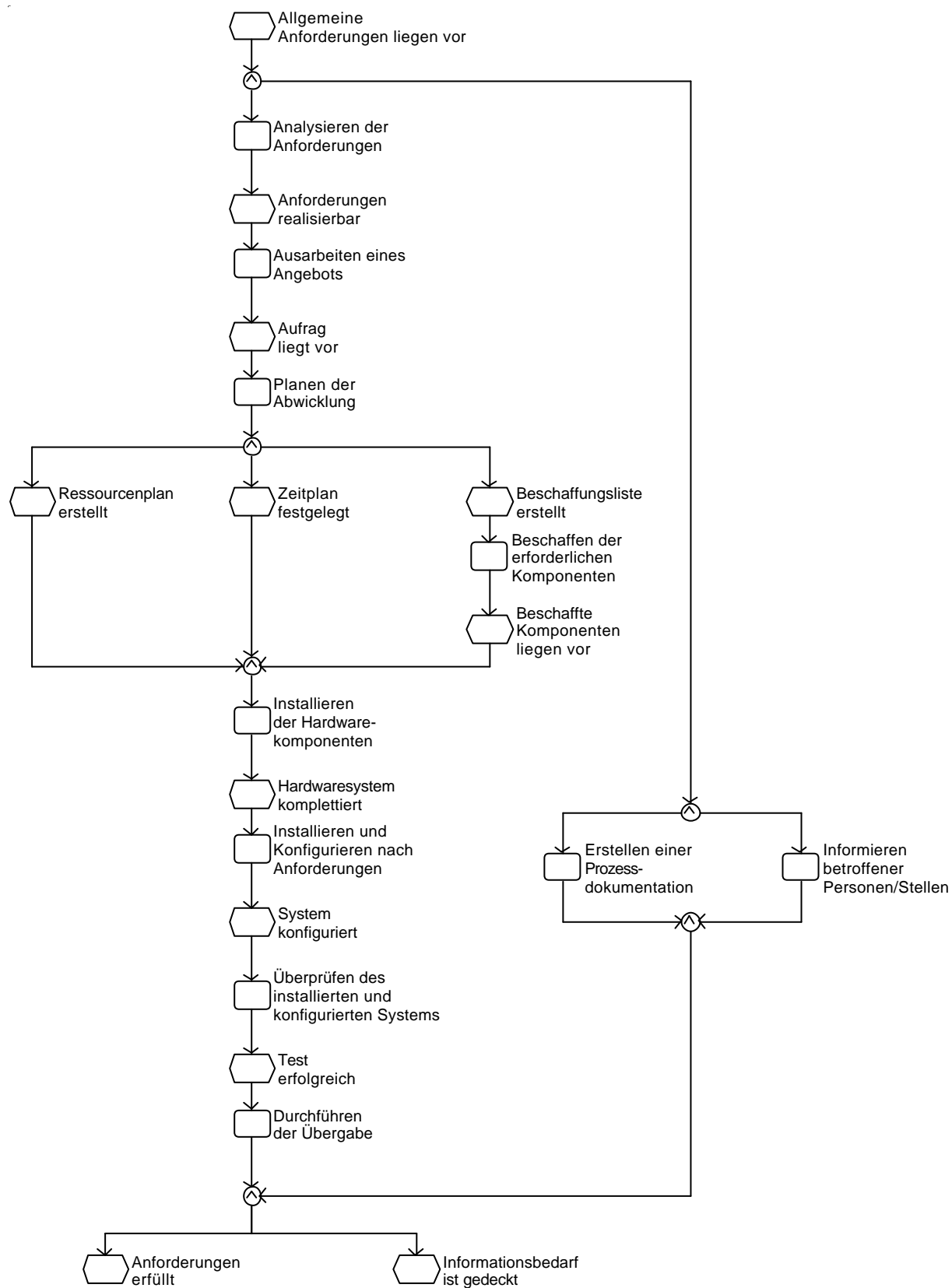


Abbildung 7: Referenzprozess Change-Management



### **3.1.2 Prozesskompass Change-Management**

Zusammenfassend sind folgende Teilprozesse im Referenzprozess Change-Management enthalten:

1. Analysieren der Anforderungen
2. Ausarbeiten eines Angebots
3. Planen der Abwicklung
4. Beschaffen der erforderlichen Komponenten
5. Installieren der Hardwarekomponenten
6. Installieren und Konfigurieren nach Anforderungen
7. Überprüfen des installierten und konfigurierten Systems
8. Durchführen der Übergabe
9. Erstellen der Prozessdokumentation
10. Informieren betroffener Personen/Stellen

### 3.1.2.1 Analysieren der Anforderungen

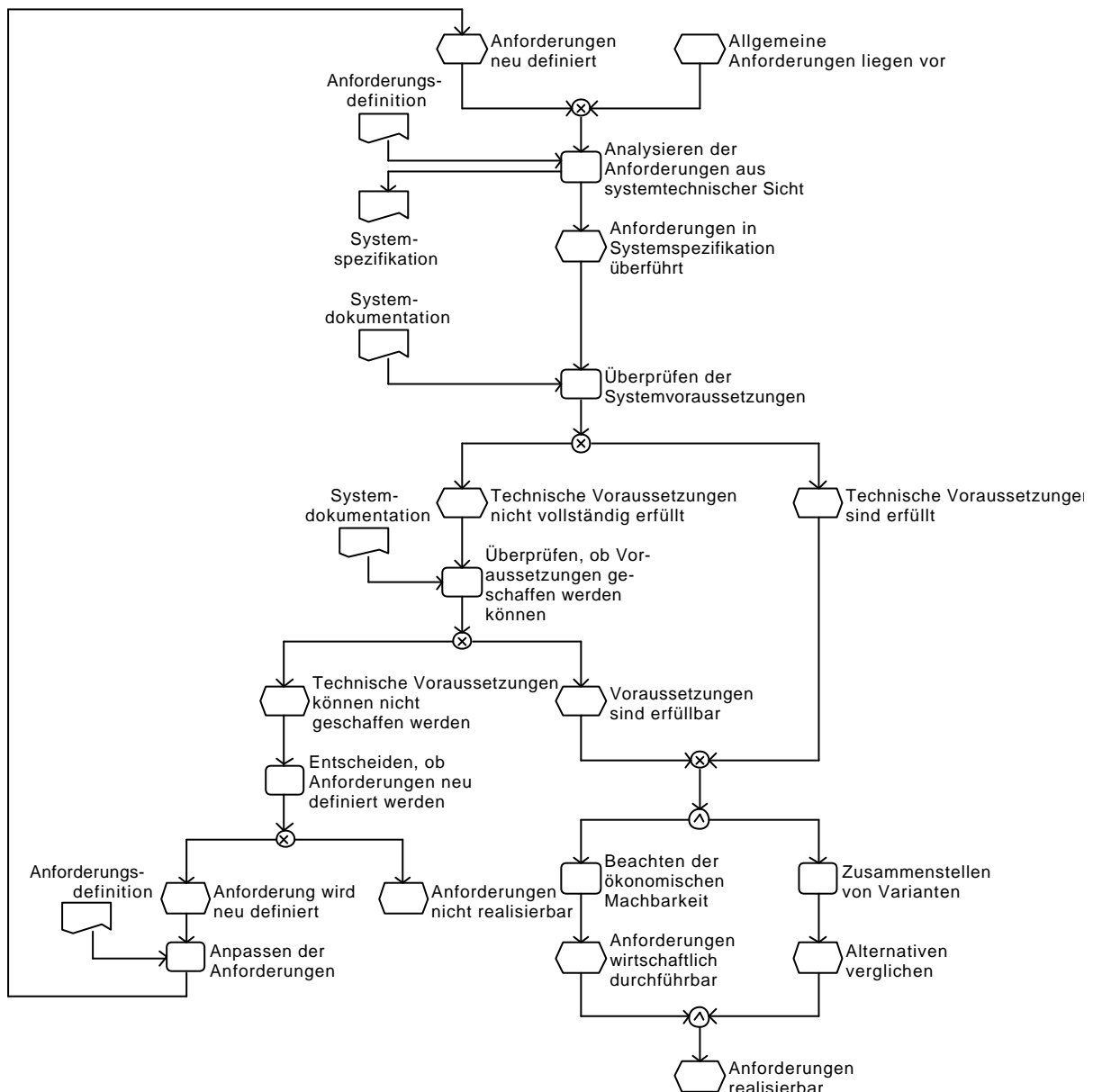


Abbildung 8: Analysieren der Anforderungen

Jeder Change-Managementprozess beginnt mit einer Analyse der Anforderungen. Hierzu prüfen IT Systems Administrator, welche Anforderungen aus technischer Sicht hinsichtlich des Änderungsbedarfs bestehen. Danach ist zu prüfen, welche technischen Voraussetzungen vorhanden sein müssen um den Änderungsbedarf zu befriedigen bzw. ob die Systemvoraussetzungen geschaffen werden können. Das Ergebnis dieses Teilprozesses ist eine systemtechnische Bewertung der Anforderungen, die ökonomische Machbarkeitsprüfung sowie der erste Variantenvergleich der zu erstellenden Lösung die als Grundlage für den nächsten Schritt, der Ausarbeitung eines Angebots dienen.

#### 3.1.2.1.1 Tätigkeiten: Analysieren der Anforderungen

Der IT Systems Administrator muss folgende Tätigkeiten durchführen um die Anforderungen, die an den Change-Managementprozess gestellt sind, zu analysieren:

- Überführen der Anforderungen in Systemspezifikationen
- Überprüfen der Systemvoraussetzungen
- Überprüfen der ökonomischen Machbarkeit und
- Durchführen eines Variantenvergleichs

Falls technische Voraussetzungen nicht erfüllt sind:

- Überprüfen, ob Voraussetzungen geschaffen werden können

Falls technische Voraussetzungen nicht geschaffen werden können:

- Entscheiden, ob Anforderungen neu definiert werden

Falls Anforderungen neu definiert werden:

- Anpassen der Anforderungen

### **3.1.2.1.2 Kompetenzfelder: Analysieren der Anforderungen**

Fähigkeiten/Fertigkeiten

- Spezielle Anforderungen verstehen können
- Anforderungen in systemtechnische Spezifikationen überführen können
- Systemtechnische Voraussetzungen prüfen können
- Nachträgliche Schaffung von Voraussetzungen prüfen können
- Bewusstsein über Sicherheitsaspekte haben
- Vorhandene Systeme analysieren können
- Durchführen von Wirtschaftlichkeitsbetrachtungen
- Zukünftigen Bedarf prognostizieren können
- Alternativen vergleichen können
- Anforderungsdefinitionen anpassen können
- Dokumentieren können

Wissen

- Kenntnisse in der Verwendung von Betriebssystemen und deren Systemarchitektur
- Kenntnisse beim Verstehen von Hardwarevoraussetzungen
- Kenntnisse im Umgang mit Systemtopologien und Referenzmodellen
- Kenntnisse bei der Planung von Prozessen und über organisatorische Auswirkungen
- Systemspezifische Auswirkungen von speziellen Anforderungen der Entscheider und der Organisation kennen
- Standards der Dokumentation für die Vorbereitung auf Kundengespräche kennen
- Auswirkungen von Hard- und Softwareschnittstellen in Bezug auf die geplanten Änderungen kennen
- Auswirkungen auf die derzeitige Netzwerkstruktur in Bezug auf die geplanten Änderungen kennen
- Betriebswirtschaftliche Grundkenntnisse in der Kosten- und Nutzenanalyse
- Techniken der Datensicherung kennen

Werkzeuge

- Kaufmännische Software
- Diagnose- und Prognosesoftware
- Kalkulationssoftware

### **3.1.2.1.3 Beispiel: Analysieren der Anforderungen**

In einer Firma soll eine gemeinsame Groupwareplattform aufgebaut und betrieben werden. Im Haus sind derzeit ca. 200 Mitarbeiter beschäftigt, wobei jeder Mitarbeiter einen eigenen PC besitzt. Da ein Teil dieser Mitarbeiter auch außerhalb der Firma tätig ist, besitzen diese anstatt des PCs ein Notebook. Die Firma gliedert sich in Abteilungen und unterschiedlichen Arbeitsgruppen, die projektbezogen zusammengesetzt werden. Von den Benutzern wurde schon häufiger der Wunsch geäußert, dass es für Besprechungsplanungen innerhalb der Projekte einen gemeinsamen Gruppenkalender geben soll. Des Weiteren wurde schon häufig der Hinweis von der Systemadministration an die Geschäftsleitung angetragen, auf der Ebene der Mails eine einheitliche Plattform zu betreiben, da dann der administrative Aufwand geringer eingeschätzt wird. Für den innerbetrieblichen Ideenaustausch soll auf Wunsch der Geschäftsleitung ein Diskussionsbord im Intranet geben, welches man auch in das Internet der Firma stellen soll. Da viele organisatorische Arbeitsschritte, wie die Urlaubsanmeldung oder das Bestellen von Büromitteln kostengünstiger gestaltet werden soll, muss über eine Workflow-Anwendung nachgedacht werden. Mit dem neuen System sollen

zunächst die Grundlagen bereitgestellt werden. Die Geschäftsleitung weist an, dass dies mithilfe einer Lotus Domino/Notes-Umgebung umgesetzt werden soll.

Der IT Systems Administrator überprüft zunächst, welche Hardwarevoraussetzungen für die Installation eines Servers als auch der Klienten vorhanden sein soll. Da alle PCs und Notebooks Microsoft Windows 2000 mit einem Pentium 4 Prozessor, mindestens 512 MB Arbeitsspeicher und eine Netzwerkkarte besitzen sowie die Notebooks über ein eingebautes Modem verfügen, sind die klientseitigen Systemvoraussetzungen gegeben. Da die Anforderungen an Systemhardware von der Art der Verwendung abhängt, muss dies hier zunächst festgestellt werden. Alle Benutzer sollen Domino als Mailplattform benutzen. Des Weiteren sollen die Grundlagen geschaffen werden, dass Domino als Informationsspeicher (Diskussionsforum, Projekt- und Teammanagement) dienen soll. Da es neben der Zentrale eine Außenstelle gibt, müssen diese beiden separaten Netzwerke in ein System integriert werden. Dies soll über einen zentralen Server, einem Applikationsserver für den Informationsspeicher und jeweils einem Mailserver geschehen. Für die Ausfallsicherung wird ein RAID-5 Plattensystem in jedem Server vorgeschlagen. Jeder Server soll mit mindestens zwei Prozessoren und jeweils 1 GB Arbeitsspeicher ausgestattet werden. Der zentrale Server erhält aufgrund der höher zu erwartenden Netz- und Datenlast zwei Netzwerkkarten und mindestens 2 GB Arbeitsspeicher sowie ein RAID-5 System mit mindestens der Kapazität aller anderen drei Server. Die Außendienstmitarbeiter sollen über RAS den Zugriff auf die Domino-Domäne (Mail- und Applikationsdatenbanken) erhalten. Verbunden werden die Server (die sich in der Zentrale befinden) über LAN und der externe Mailserver über eine DSL-Leitung. Für das kontrollierte Herunterfahren der Server bei Ausfall der Energieversorgung soll eine unterbrechungsfreie Stromversorgung Sorge tragen. Die technischen Voraussetzungen für die Server müssen und können noch geschaffen werden.

Für die Mailserver wird nach den Erfahrungen aus vergangenen Projekten der Funktions- und Lizenzumfang eines Domino-Mail-Servers genügen, der Applikationsserver wird durch einen Domino-Anwendungsserver bereitgestellt. Da noch nicht gewiss ist, wie sich die gesamte Firma weiterentwickelt, wird der zentrale Server ebenfalls durch einen Domino-Anwendungsserver bereitgestellt.

### 3.1.2.2 Ausarbeiten eines Angebots

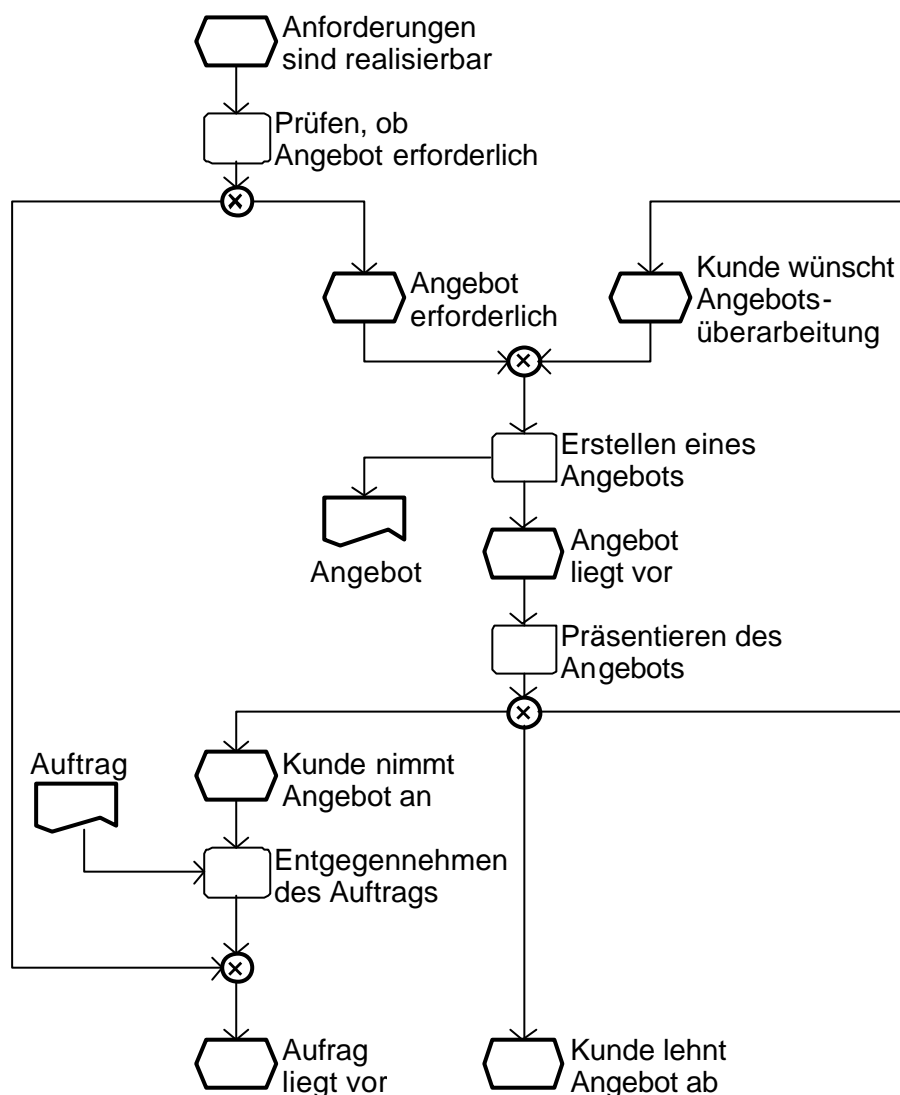


Abbildung 9: Ausarbeiten eines Angebots

Nachdem die Durchführbarkeit geprüft worden ist, kann (dem Kunden) ein konkretes Angebot unterbreitet werden, dass in einen Auftrag seitens des Kunden führen sollte. Eventuell muss das präsentierte Angebot überarbeitet werden. Hat der Kunde das Angebot akzeptiert, liegt der entgeltliche Auftrag vor.

#### 3.1.2.2.1 Tätigkeiten: Ausarbeiten eines Angebots

Der IT Systems Administrator muss folgende Tätigkeiten durchführen, um ein Angebot auszuarbeiten:

- Prüfen, ob Angebot erforderlich ist
- Erstellen eines Angebots
- Präsentieren des Angebots
- Entgegennehmen des Auftrags

#### 3.1.2.2.2 Kompetenzfelder: Ausarbeiten eines Angebots

Fähigkeiten/Fertigkeiten

- Angebot erstellen können
- Preise vergleichen können
- Präsentieren können
- Verhandlungsgeschick haben

- Rhetorische Kenntnisse besitzen
- Wissen
- Kenntnisse und Erfahrungen bei der Vorbereitung und Durchführung von Präsentationen
  - Betriebswirtschaftliche Grundkenntnisse in der Vertragsgestaltung
  - Rechtliche Rahmenbedingungen von Angeboten und deren Auswirkungen kennen
  - Kenntnisse bei der Planung von Prozessen und über organisatorische Auswirkungen
  - Standards der Dokumentation für die Nachbereitung von Kundengesprächen kennen
- Werkzeuge
- Kaufmännische Software
  - Präsentationstechniken

### **3.1.2.2.3 Beispiel: Ausarbeiten eines Angebots**

Das gesamte Groupware-System, d. h. zwei Applikations- und zwei Mailserver mit ihren spezifischen Hardwareanforderungen sowie 200 Lotus Noteskunden werden in einer Übersicht zusammengetragen, ein Systemplan entworfen und eine erste Abschätzung des Aufwands und der für die Installation benötigte Zeit durchgeführt. Es werden zunächst die wichtigsten Kostenfaktoren aufgelistet und dann der voraussichtliche finanzielle Aufwand kalkuliert. Dies wird in einem Angebotsentwurf der Geschäftsleitung präsentiert. Die Geschäftsleitung kritisiert die zu hohen Kosten und regt einen Variantenvergleich mit und ohne einer unterbrechungsfreien Stromversorgung für alle Server an. Im Ergebnis wird die unterbrechungsfreie Stromversorgung für die beiden Mailserver und den einen Applikationsserver nicht benötigt. Die eventuell zu erwartenden Datenverluste werden von der Geschäftsleitung als niedrig eingeschätzt. Des Weiteren kommt während der Präsentation heraus, dass aufgrund guter Aussichten im folgenden Jahr 50 weitere Mitarbeiter eingestellt werden. Diese Anforderungen werden nun in einer neuen Aufstellung mitberücksichtigt. Das modifizierte Dokument (Angebot) wird der Geschäftsleitung erneut vorgelegt und präsentiert, jetzt stimmt die Geschäftsleitung der Installation des gesamten Systems zu und es liegt im Ergebnis ein konkreter Auftrag inklusive des Budgetrahmens für die Systemadministration vor.

### 3.1.2.3 Planen der Abwicklung

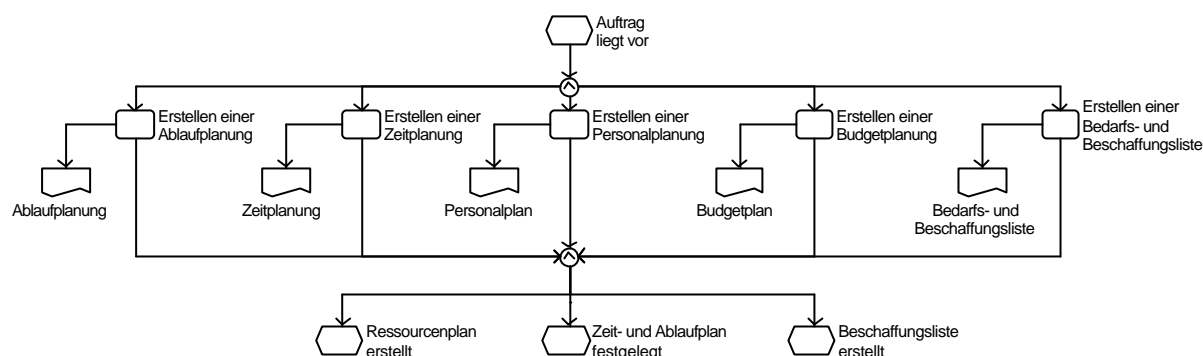


Abbildung 10: Planen der Abwicklung

Nachdem der Kunde das Angebot angenommen hat, muss eine Abwicklungsplanung erfolgen. Aus dem Angebot können Parameter spezifiziert werden, die in diese Planung einfließen müssen. Das Ergebnis ist ein Ressourcen-, ein Zeit- und Ablaufplan sowie eine Beschaffungsliste über die zu beschaffende Hard- und Software (Komponenten).

#### 3.1.2.3.1 Tätigkeiten: Planen der Abwicklung

Folgende Tätigkeiten muss ein IT Systems Administrator bei der Planung der Abwicklung durchführen:

- Erstellen einer Zeitplanung
- Erstellen einer Ablaufplanung
- Erstellen einer Bedarfs- und Beschaffungsliste
- Erstellen einer Personalplanung
- Erstellen einer Budgetplanung

#### 3.1.2.3.2 Kompetenzfelder: Planen der Abwicklung

Fähigkeiten/Fertigkeiten

- Zeitplanung erstellen können
- Beschaffungsliste erstellen können
- Zukünftigen Bedarf ermitteln können
- Sich selbst und eventuell Mitarbeiter beurteilen und einschätzen können
- Personalplanung erstellen können
- Budgetplanung erstellen können
- Ablaufplanung erstellen können
- Planungen zusammenführen können
- Spezielle Anforderungen verstehen können
- Kaufmännisches Rechnen durchführen können
- Zukünftige Aufwände kalkulieren und prognostizieren können
- Dokumentieren können
- Rechtliche Rahmenbedingungen einhalten

Wissen

- Kenntnisse bei der Planung von Prozessen und Projekten sowie über organisatorische Auswirkungen
- Standards der Dokumentation für die Planungsabläufe von Projekten kennen
- Betriebswirtschaftliche Grundkenntnisse in der Kosten- und Nutzenanalyse

Werkzeuge

- Projektmanagementsoftware
- Kaufmännische Software
- Tabellenkalkulation

#### 3.1.2.3.3 Beispiel: Planen der Abwicklung

In einem ersten Schritt wird überlegt, wie die Installation und Integration in das derzeitige Netz erfolgen soll. Dabei werden neben der Konkretisierung des Projektziels, d. h. einer lauf-

fähigen und fehlerfreien Integration des geplanten Groupware-Systems mit einer Teilanbindung der Notebooks über ein RAS-Dienst, konkrete Projektteilaufgaben identifiziert. So müssen die Lizenzen für die Klienten und Server beschafft und die notwendige Hardware für die fünf Server identifiziert werden. Diese werden in einer Beschaffungsliste notiert. Als nächstes wird der Ablauf festgelegt, d. h. zunächst müssen die Server mit einem Betriebssystem (Microsoft Windows 2000) versehen werden. Danach müssen diese konfiguriert werden, d. h. unter anderem, dass der RAS-Dienst installiert und konfiguriert werden muss. Für den Webzugriff wird ein Webserver installiert und konfiguriert. Als nächstes müssen die Domino-server aufgespielt werden und die Organisationsstruktur, Benutzer sowie die Postfächer erstellt werden. Dann wird der RAS-Dienst bei den beiden Servern konfiguriert. Danach wird die automatische Replikation zwischen den Servern eingerichtet und die unterbrechungsfreie Stromversorgung integriert. Zum Schluss werden die Server getestet. Die Vorgehensweise wird in einem groben Ablaufplan festgehalten, der als Inhaltsverzeichnis für die Projektdokumentation dienen wird.

Die Installation der Server soll jeweils eine Woche in Anspruch nehmen und die Konfiguration jeweils noch einmal drei Tage. Da die Aufgaben skalierbar sind werden die Server insgesamt von drei Mitarbeitern erledigt, was die Gesamtzeit um zwei Wochen kürzt. Als Kostengrundlage werden Personentage für Mitarbeiter der Firma verwendet. Die Hard- und Softwarekosten werden separat berechnet.



### 3.1.2.4 Beschaffen der erforderlichen Komponenten

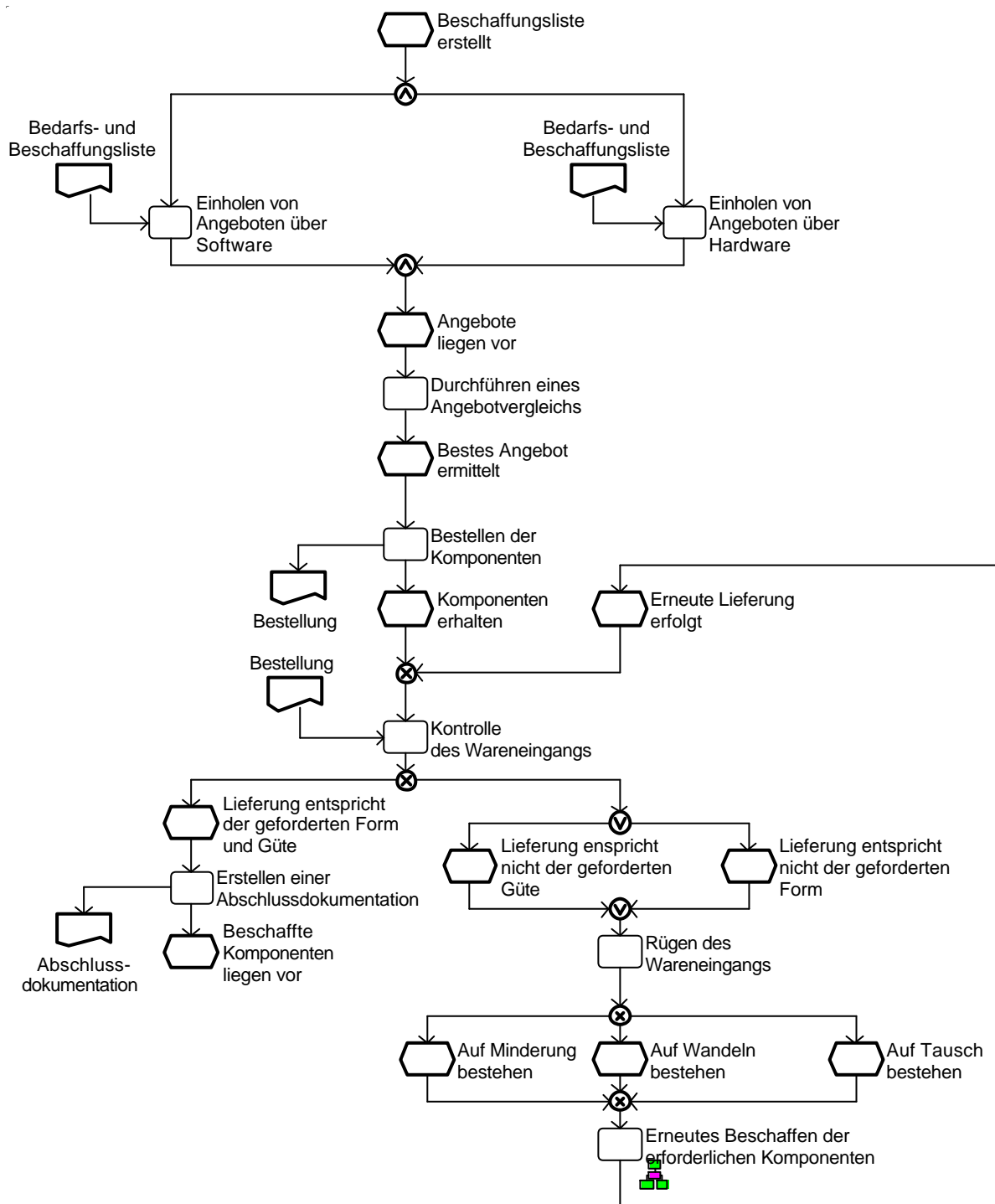


Abbildung 11: Beschaffung der erforderlichen Komponenten

Anhand der vorher erstellten Spezifikation erfolgt nun ein Beschaffungsvorgang. Hier müssen Angebote über die zu beschaffende Hard- und Software eingeholt und miteinander verglichen werden. Ist ein attraktives Angebot identifiziert, wird eine Bestellung ausgelöst. Ist die Lieferung erfolgt, wird sie mit der Bestellung verglichen und auf eventuelle Lieferschäden kontrolliert. Entspricht der Liefereingang jedoch nicht der geforderten Form und Güte, muss gerügt werden und ein erneuter Bestellvorgang eingeleitet werden. Eventuell müssen neue Angebote eingeholt und miteinander verglichen werden. Verläuft die Kontrolle jedoch ohne Probleme, wird die gesamte Lieferung an die Komponentenmontage übergeben.

#### **3.1.2.4.1 Tätigkeiten: Beschaffen der erforderlichen Komponenten**

Die folgenden Tätigkeiten müssen vom IT Systems Administrator bei der Beschaffung der für die Erfüllung des Auftrages erforderlichen Komponenten durchgeführt werden:

- Einholen von Angeboten über Software
- Einholen von Angeboten über Hardware
- Durchführen eines Angebotsvergleichs
- Bestellen der Komponenten
- Kontrolle des Wareneingangs
- Erstellen einer Abschlussdokumentation

Entspricht die Lieferung nicht der erforderlichen Form oder Güte:

- Rügen des Wareneingangs
- Erneutes Beschaffen der erforderlichen Komponenten

#### **3.1.2.4.2 Kompetenzfelder: Beschaffen der erforderlichen Komponenten**

Fähigkeiten/Fertigkeiten

- Angebote einholen können
- Angebote analysieren, bewerten und beurteilen können
- Komponenten bestellen können
- Wareneingang kontrollieren können
- Dokumentieren können
- Reklamationen erstellen können
- Technische Beschreibungen verstehen können
- Gespräche mit Lieferanten führen können, dabei in der Lage sein, die eigene (fachliche) Meinung auch in Konfliktsituationen zu vertreten

Wissen

- Betriebswirtschaftliche Grundkenntnisse des Kosten/Nutzenvergleichs von Angeboten kennen
- Richtlinien der Organisation für die Angebotsbewertung kennen
- Rechtliche Auswirkungen von Angeboten kennen
- Rechtliche Auswirkungen von Reklamationen kennen
- Überblick über relevante Hard- und Softwareprodukte und deren Preise kennen
- Funktionsfähigkeit und Güte von Hard- und Software kennen
- Standards der Dokumentation für Arbeitstätigkeiten am IT-System kennen

Werkzeuge

- Kaufmännische Software
- wenn vorhanden: Warenwirtschaftssysteme
- Textverarbeitung
- Kalkulationssoftware

#### **3.1.2.4.3 Beispiel: Beschaffen der erforderlichen Komponenten**

Es werden zwei Angebotstypen für die Server eingeholt. Zum einen eine Komplettlösung mit vorkonfigurierter Hard- und Software und zum anderen Angebot über Einzelkomponenten. Nachdem von mehreren potentiellen Lieferanten Angebote vorliegen, stellt sich heraus, dass die Komplettlösung mit vorkonfigurierter Hard- und Software die günstigere Lösung ist und somit der Budgetrahmen geringer in Anspruch genommen wird, als ursprünglich angenommen. Der IT Systems Administrator weist die Bestellung der vier Server an.

Nachdem die Hard- und Software eingegangen ist, überprüft der Administrator, ob alles richtig geliefert wurde. Die fünf Rechner haben keine äußerlich feststellbaren Mängel. Die einzelnen Systemkonfigurationen werden in die Projekttakte eingetragen.

### 3.1.2.5 Installieren der Hardwarekomponenten

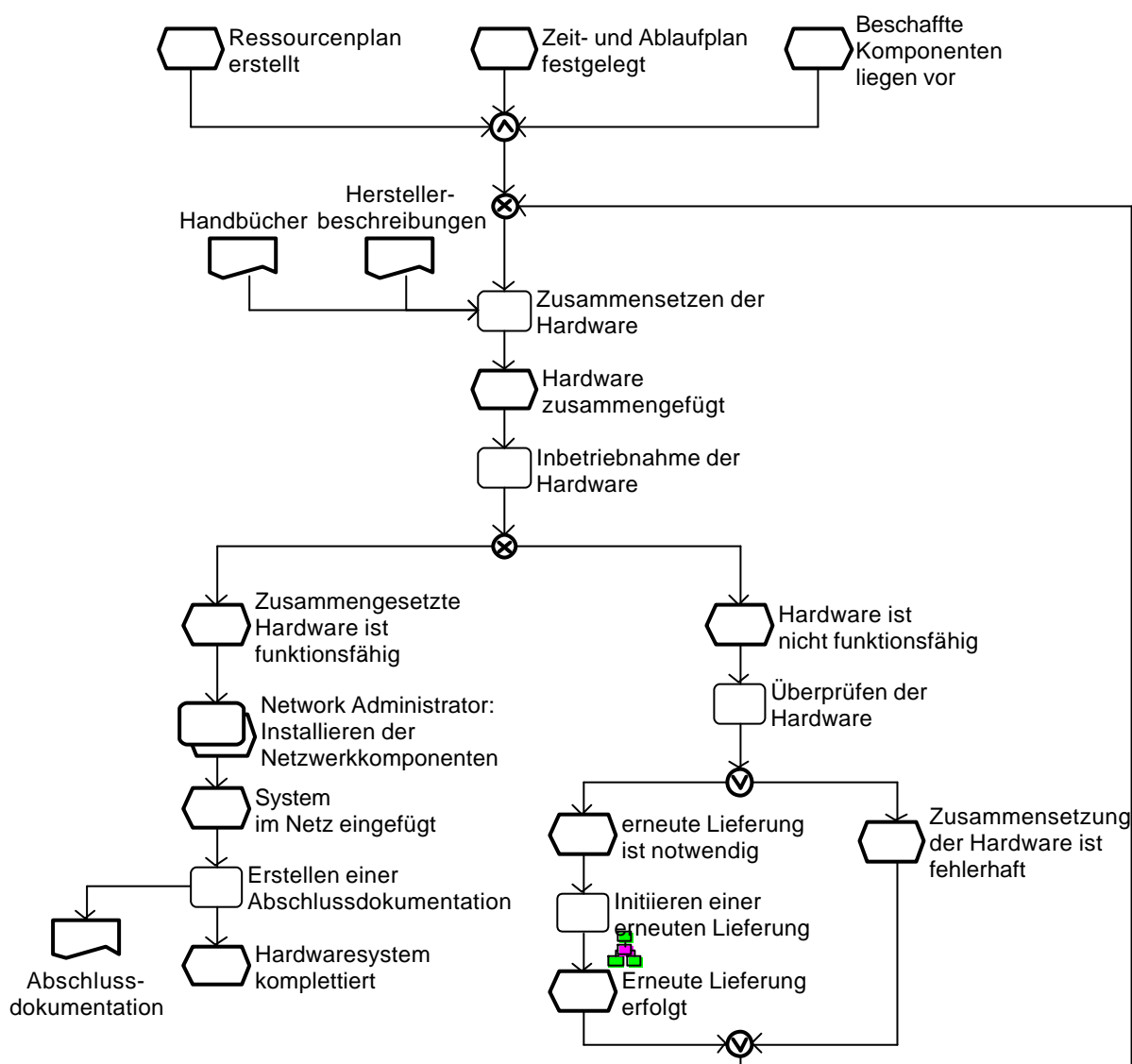


Abbildung 12: Installieren der Hardwarekomponenten

Nachdem alle benötigten Hardwarekomponenten vorliegen, können diese zusammengesetzt werden. Zur Installation werden Beschreibungen und Handbücher der Hersteller herangezogen. Nachdem die Hardwarekomponenten zu einem Gesamtsystem komplettiert worden sind, werden sie überprüft. Beim Zusammensetzen der benötigten Netzwerkkomponenten wird der Network Administrator herangezogen. Funktioniert die zusammengesetzte Hardware nicht wie gewünscht, muss zum einen überprüft werden, ob sie richtig zusammengesetzt wurde oder ob dennoch Fehler bei der Hardware vorliegen. Dann sollte eine erneute Lieferung initiiert werden. Zum Schluss wird eine Abschlussdokumentation erstellt, die neben den ausgeführten Tätigkeiten auch eventuell aufgetretene Probleme enthält. Eventuell kann später daraus ein Verfahrenshandbuch oder eine Best Practices erstellt werden.

#### 3.1.2.5.1 Tätigkeiten: Installieren der Hardwarekomponenten

Für das Installieren der Hardwarekomponenten muss der IT Systems Administrator folgende Tätigkeiten durchführen:

- Zusammensetzen der Hardware
- Inbetriebnahme der Hardware
- Network Administrator: Installieren der Netzwerkkomponenten

Falls die Hardware nicht funktionsfähig ist:

- Überprüfen der Hardware

Falls eine erneute Lieferung notwendig ist:

- Initiieren einer erneuten Lieferung

Auf jeden Fall:

- Erstellen einer Abschlussdokumentation

### **3.1.2.5.2 Kompetenzfelder: Installieren der Hardwarekomponenten**

Fähigkeiten/Fertigkeiten

- Leitungen in Betrieb nehmen können
- Hardware richtig zusammensetzen können
- Hardwarefehler entdecken können
- Dokumentieren können
- Zusammen mit dem Network Administrator Netzwerkkomponenten installieren können
- Seine Kompetenzgrenzen bei der Beschaffung neuer Hardwarekomponenten kennen (Budgetverantwortung)

Wissen

- Betriebsarten von Systemen und benutzen Hardwarekomponenten
- Grundlegende Kenntnisse in der Organisation, Dimensionierung, Topologien und Komponenten von Netzwerken
- Grundlegende Kenntnisse in der Architektur von Kommunikationssystemen haben
- Kenntnisse in der strukturierten Verkabelung
- Kenntnisse und Erfahrungen im Zusammensetzen von Hardware in Bezug auf zu Grunde liegenden Hardwarearchitekturen
- Besonderheiten von Datenübertragungssystemen und –techniken sowie der verwendeten Hardwareschnittstellen
- Kenntnisse von Hardwarestandards und Standards der Konfiguration von Hardwaresystemen
- Kenntnisse im Umgang mit Konfigurationsmanagementsoftware
- Standards der Dokumentation in Bezug auf die Installation von Hardwarekomponenten
- Gefahren des elektrischen und des elektrostatischen Stroms und Arbeitsschutzgesetze und Bestimmungen beim Umgang mit elektrischem Strom kennen
- Kenntnisse im Umgang mit Prüfgeräten

Werkzeuge

- VDE-Prüfgerät
- Textverarbeitung
- Antistatikhandgelenkmanschetten
- Konfigurationsmanagementsoftware (CMS)

### **3.1.2.5.3 Beispiel: Installieren der Hardwarekomponenten**

Die fünf Server werden an einem Testplatz aufgebaut. Um die Integration von Lotus Notes bei der Installation mit zu berücksichtigen, werden zwei typische PC-Klienten und ein Notebook ebenfalls neben dem Server aufgebaut. Nun werden diese in Betrieb genommen. Da auch hier keine Fehler erkennbar sind, werden die für den Netzbetrieb notwendigen Einstellungen getroffen. Die anderen vier Servernetzwerkkarten und die PCs werden mit der Unterstützung eines NetzwerkAdministrators an aktive Netzwerkkomponenten angeschlossen. Das Notebook wird an eine ISDN-Telefonleitung angeschlossen. Die Netzwerkkarte des Mailservers, der später in der Außenstelle in Betrieb genommen werden soll, wird an eine eigens für solche Tests vorgesehene DSL-Leitung angeschlossen. Die USV werden nun an den zentralen Server angeschlossen und überprüft, ob sie fehlerfrei läuft. Die durchgeführten Hardwarekonfigurationen werden am Schluss in die Projekttakte übertragen.

Dabei stellt sich heraus, dass ein Server keine Netzverbindung aufbauen kann, obwohl die Konfigurationen stimmen. Da alle Netzwerkkarten der Server baugleich sind, wird davon ausgegangen, dass in diesem Server eine Karte defekt ist. Ein Ausbau und erneuter Einbau in einen anderen Rechner bestätigt den Verdacht. Der IT Systems Administrator weist eine erneute Bestellung an. Nachdem die Netzwerkkarte geliefert wurde, wird sie zunächst sepa-

rat getestet. Tritt dabei kein Fehler auf, wird diese in den Server eingebaut und die technischen Daten (MAC-Adresse) in die Projekttakte eingetragen. Da sich nun der Server fehlerfrei ans Netz anmeldet, ist die Installation aller Hardwarekomponenten somit abgeschlossen und es können nun die nötigen Betriebssystem- und Softwarekomponenten installiert werden.

### 3.1.2.6 Installieren und Konfigurieren nach Anforderungen

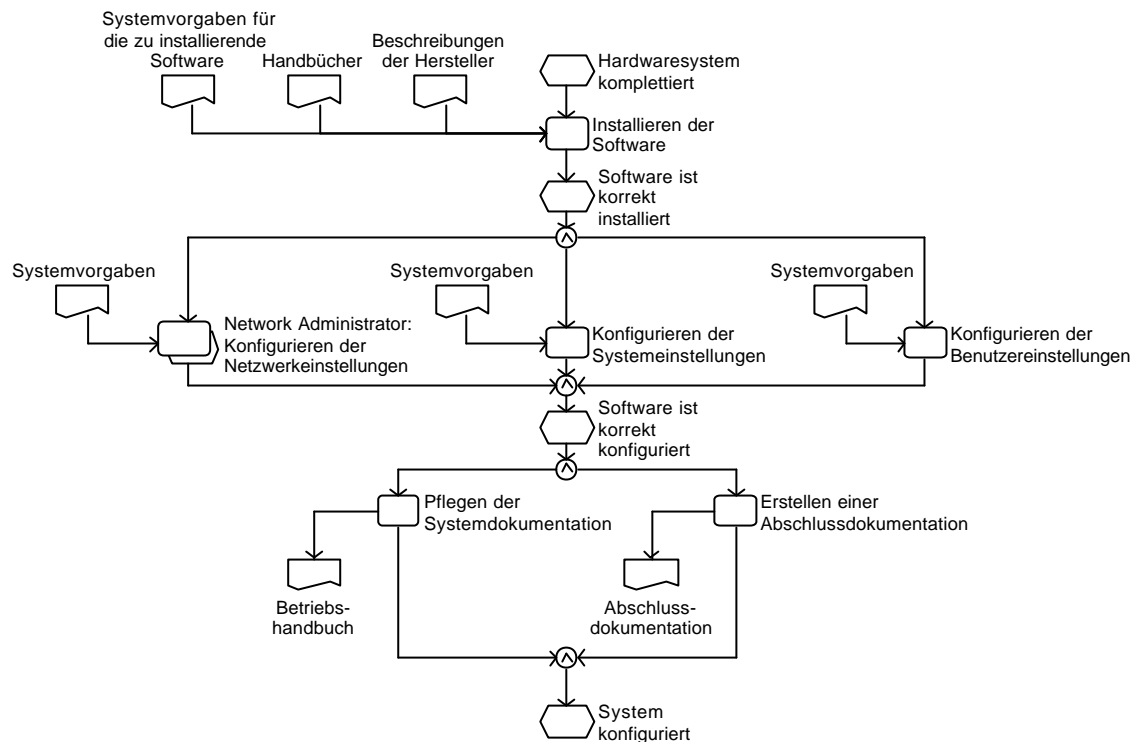


Abbildung 13: Installieren und Konfigurieren nach Anforderungen

Ist die Hardware zusammengesetzt und einem ersten Funktionstest unterzogen worden, kann mit der Installation der Software begonnen werden. Diese wird unter Zuhilfenahme von Beschreibungen der Hersteller, Handbücher und den Systemvorgaben für das zu installierende System durchgeführt. Nach einem erfolgreichen Test der einzelnen Komponenten, konfiguriert man die installierte Software nach Anforderungen. Nach erfolgreicher Konfiguration der System- und Benutzereinstellungen sowie der Netzwerkeinstellungen mit Zuhilfenahme des Network Administrator werden die Änderungen in der Systemdokumentation eingepflegt und eine Abschlussdokumentation erstellt.

#### 3.1.2.6.1 Tätigkeiten: Installieren und Konfigurieren nach Anforderungen

Für die Installation und Konfiguration des Systems muss der IT Systems Administrator folgende Tätigkeiten durchführen:

- Installieren der Software
- Zusammen mit dem Network Administrator: Konfigurieren der Netzwerkeinstellungen
- Konfigurieren der Systemeinstellungen
- Konfigurieren der Benutzereinstellungen
- Pflegen der Systemdokumentation
- Erstellen einer Abschlussdokumentation

#### 3.1.2.6.2 Kompetenzfelder: Installieren und Konfigurieren nach Anforderungen

Fähigkeiten/Fertigkeiten

- Dokumentieren können
- Zusammen mit dem Network Administrator Netzwerkeinstellungen konfigurieren können
- Systemeinstellungen konfigurieren können
- Benutzereinstellungen konfigurieren können
- Sicherheitsvorgaben und –richtlinien beachten und umsetzen können
- Systemdokumentationen verstehen können
- Anforderungen der Systeme und Software beachten und umsetzen können

- Nach alternativen Informationen für die Konfiguration von Softwaresystemen selbstständig suchen können
- Spezielle Anforderungen erfüllen können
- Zweckmäßigkeit von Betriebs- und Verfahrenshandbüchern kennen
- Recherchieren können

#### Wissen

- Über Kenntnisse der verwendeten Systemarchitekturen verfügen
- Kenntnisse und Erfahrungswerte von Besonderheiten bei der Installation und Konfiguration von Betriebssystemen und Software sowie bei der Änderung von Einstellungen besitzen
- Kenntnisse bei der Verwendung von Referenzmodellen der Installation und Konfiguration von Systemsoftware besitzen
- Kenntnisse im Umgang mit Kommunikations- und Netzwerkprotokollen vorweisen können
- Skriptsprachenkenntnisse für die Automatisierung von Installations- und Konfigurationstätigkeiten sowie der Benutzereinstellungen haben
- Kenntnisse beim Umgang und der Verwendung von Softwareschnittstellen und Diensten für die Integration in bestehende IT-Systemlandschaften besitzen
- Kenntnisse im Umgang mit technischen Begriffen (auch englischen Ausdrücken) vorweisen
- Chancen und Risiken von Speichermedien (wie Disketten, Festplatten und Compact Disc) kennen und diese mit den Geschäftsrisiken abgleichen können
- Standards der Dokumentation in Bezug auf die Konfiguration von Systemen kennen

#### Werkzeuge

- Softwaredistributionssysteme
- Systemrichtlinieneditoren
- Automatische Konfigurationswerkzeuge
- Skripteditoren
- Datenbanken
- Konfigurationsmanagementsoftware (CMS)
- Textverarbeitung

### 3.1.2.6.3 *Beispiel: Installieren und Konfigurieren nach Anforderung*

Zunächst müssen die Betriebssysteme (Windows 2000 Professional) für die Server installiert werden. Als nächstes werden zum einen die neuesten Servicepacks installiert und zum anderen die notwendigen Konfigurationen zusammen mit dem Network Administrator durchgeführt und die Server in Netzbetrieb genommen. Die für den Betrieb der USV notwendigen Einstellungen werden beim zentralen Server konfiguriert. Für die Einwahl der externen Rechner wird der Remote Access Service Dienst auf dem zentralen Server konfiguriert. Da bei der Installation und Konfiguration nicht die neuesten Daten aus der I386 benutzt wurden, muss erneut das Servicepack installiert werden. Zunächst werden zwei Benutzerkonten, einen für die Wartung des noch zu installierenden Dominoservers und einen für die Einwahl auf dem Server, angelegt.

Als nächstes wird die Einwahl des Notebooks in den zentralen Server überprüft. Läuft dies ohne Fehler ab, wird nun der Domino Server nach den Anforderungen installiert und die notwendigen Einstellungen in den Serverdokumenten vorgenommen. Dann wird die Replikation zwischen den Servern, die sich in der Zentrale befinden, eingerichtet und überprüft. Der später extern stehende Server wird über die DSL-Leitung angeschlossen, das Verbindungsdokument konfiguriert und wird anschließend auf fehlerfreie Replikation mit den anderen Servern überprüft. Es werden für einen Test Mailfächer, Benutzergruppen und Benutzer nach Anforderung eingerichtet und ihnen die entsprechenden Rechte zugewiesen. Des Weiteren werden die für den Betrieb der Dominoserver notwendigen Datenbanken eingerichtet und deren Funktion getestet. Zusammen mit dem Network Administrator werden die für die Einwahl der Notebooks notwendigen Einstellungen im zentralen Server vorgenommen. Auf dem Notebook und den Klienten-PCs wird Lotus Notes installiert und die für die Anbindung notwendigen Einstellungen durchgeführt. Alle durchgeführten Installationen und Konfigurationen werden in die Projektakte eingetragen und abschließend die für den späteren Betrieb notwendige Systemdokumentation gepflegt.

### 3.1.2.7 Überprüfen des installierten und konfigurierten Systems

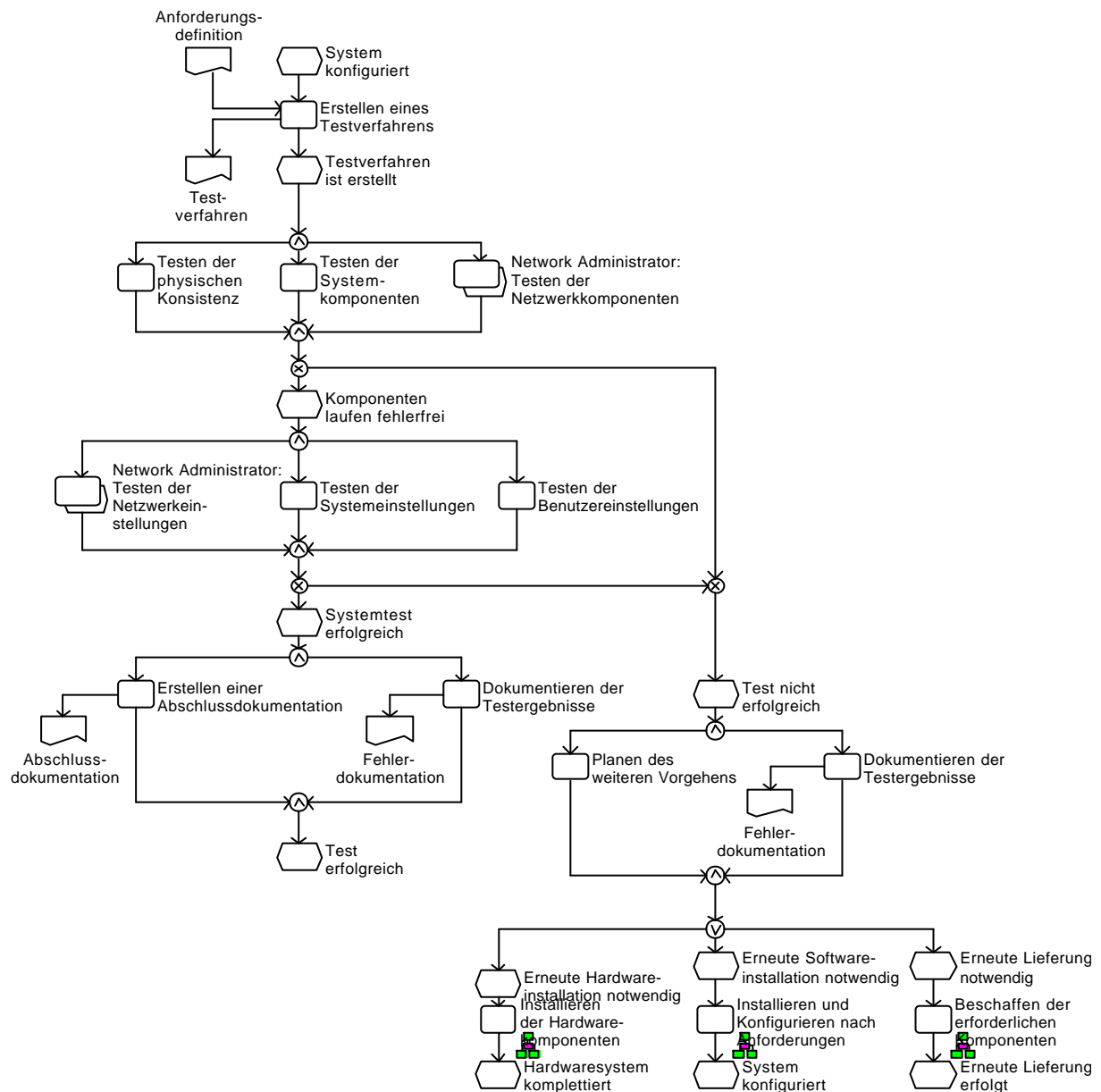


Abbildung 14: Überprüfen des installierten und konfigurierten Systems

Ist das Gesamtsystem installiert und konfiguriert, wird es zu Testzwecken erstmalig in Betrieb genommen. Dazu werden nach dem erstellten Testverfahren die physische Konsistenz, die Systemkomponenten und, zusammen mit dem Network Administrator die Netzwerkkomponenten auf einwandfreie Funktion überprüft. Ist dieser Schritt mit positivem Ergebnis abgeschlossen worden, werden zusammen mit dem Network Administrator die Netzwerkeinstellungen, die System- und die Benutzereinstellungen überprüft. Sollte es hier zu Fehlermeldungen oder Fehlverhalten kommen, wird das weitere Vorgehen geplant und die entstandenen Fehler zu einer Fehlerdokumentation zusammengetragen. Gegebenenfalls ist eine erneute Hardwareinstallation, eine erneute Installation und Konfiguration der Softwarekomponenten nach den Systemvorgaben oder eine erneute Lieferung fehlerhaft oder nichtfunktionierender Komponenten durchzuführen. Führt das zum gewünschten Testergebnis bzw. war dieses in Ordnung, werden alle getesteten Komponenten zu einer Fehlerdokumentation zusammengetragen und eine Abschlussdokumentation erstellt. Das System ist für die Übergabe bereit.



### **3.1.2.7.1 Tätigkeiten: Überprüfen des installierten und konfigurierten Systems**

Der IT Systems Administrator muss für das Überprüfen des installierten und konfigurierten Systems folgende Tätigkeiten ausführen:

- Erstellen eines Testverfahrens
- Testen der physischen Konsistenz
- Testen der Systemkomponenten
- Zusammen mit dem Network Administrator: Testen der Netzwerkkomponenten

War der Test erfolgreich:

- Zusammen mit dem Network Administrator: Testen der Netzwerkeinstellungen
- Testen der Systemeinstellungen
- Testen der Benutzereinstellungen

Wenn die Tests nicht zum gewünschten Ergebnis führen:

- Planen des Weiteren Vorgehens
- Dokumentieren der Testergebnisse

Eventuell müssen folgende Teilprozesse erneut durchgeführt werden:

- Installieren der Hardwarekomponenten
- Installieren und Konfigurieren nach Anforderungen
- Beschaffen der erforderlichen Komponenten

Sind die Testergebnisse zufriedenstellend:

- Erstellen einer Abschlussdokumentation
- Dokumentieren der Testergebnisse

### **3.1.2.7.2 Kompetenzfelder: Überprüfen des installierten und konfigurierten Systems**

Fähigkeiten/Fertigkeiten

- Datenleitungen testen können
- Netzwerkkomponenten und Netzwerkeinstellungen zusammen mit dem Network Administrator überprüfen können
- Zielgerichtete Gespräche führen können
- Systemeinstellungen testen können
- Benutzereinstellungen testen können
- Systematisches Vorgehen bei Tests besitzen
- Testverfahren erstellen und weiterentwickeln können
- Testverfahren kennen
- Systemanforderungen verstehen und umsetzen können
- Systemeigene Werkzeuge kennen und nutzen können
- Ergebnis- und Fehlerprotokolle interpretieren können
- Dienste kennen und deren Laufzeit beobachten und überprüfen können
- Anforderungsdefinitionen verifizieren können
- Vorhandene Informationsquellen aus Herstellerdokumentationen, Systembeschreibungen etc. effektiv nutzen können
- Informationsquellen erschließen können
- Aufwände abschätzen und weitere Vorgehen planen können
- Aus Erfahrungen planen können
- Testergebnisse fehlerfrei dokumentieren können
- Dokumentieren können

Wissen

- Grundlegende Kenntnisse in der Organisation und Komponenten von Netzwerken
- Kenntnisse über die verwendeten Systemarchitekturen, Betriebssysteme und Softwaresysteme
- Betriebsarten von Hardware kennen
- Verwendete Schnittstellenfunktionen zu anderen Systemen und innerhalb des eigenen Systems kennen
- Kenntnisse der Funktion von Kommunikations- und Netzwerkprotokollen sowie der verwendeten Dienste und Komponente besitzen

- Testverfahren und Vorgehensmodelle für Testverfahren kennen und Verwendung von Protokollen für Tests und Konfigurationen kennen
- Funktionsweise von Datenübertragungssystemen und –techniken sowie von Systemsoftware kennen
- Standards von Testverfahren kennen
- Standards der Dokumentation in Bezug auf das Nachvollziehen von Fehlerzuständen und getesteten Systembereichen kennen

#### Werkzeuge

- Ereignismonitore
- Performancemonitore (im Systemtestumfeld)
- Testsoftware
- Diagnosesoftware
- Textverarbeitung

### **3.1.2.7.3 Beispiel: Überprüfen des installierten und konfigurierten Systems**

Für die Hardware existieren spezielle Testverfahren, um die Stabilität zu überprüfen. Diese werden zunächst recherchiert und in ein Testverfahren überführt. So werden gekaufte Monitore einem Dauertest unterzogen und ein spezieller Bildschirmschoner verwendet, der unterschiedliche Betriebsmodi des Monitors durchtesten kann. Für Arbeitsspeicher können spezielle Speichertester eingesetzt werden, um eventuell vorhandene fehlerhafte Speicherblöcke zu identifizieren. In dieser Phase müssen eventuell aufgetretene Störungen bei Softwarekomponenten identifiziert werden, die durch die Installation anderer Software verursacht wurden. Aus diesem Grund wird das Gesamtsystem getestet.

So wird der Zugriff der Server zum einen über die Klienten-PCs getestet, zum anderen wird die erfolgreiche Einwahl des externen Notebooks überprüft. Als nächstes wird die Replikation zwischen Klient und Server überprüft und eine Testmail gesendet. Danach wird über die Mailverfolgung geprüft, wie die Emails versendet werden. Hier muss auf die Besonderheit geachtet werden, dass der eine Mailserver zunächst selbstständig eine DSL-Verbindung aufbauen muss und dann die für ihn bestimmten Mails empfängt bzw. seine in der mail.box angesammelten Mails versendet. Beim zentralen Server wird ein Stromausfall simuliert, um zu überprüfen, ob die USV fehlerfrei funktioniert.

Zum Schluss werden die Zugriffsrechte der unterschiedlichen Benutzergruppen getestet. Die Server stehen nun, da es beim Gesamttest zu keinem Fehler kommt, zur Übergabe bereit. Alle getesteten Komponenten und Einstellungen sowie die Durchführungsreihenfolge dieser Tests werden in einem Testbericht zusammengestellt und in die Projektakte eingefügt.

### 3.1.2.8 Durchführen der Übergabe

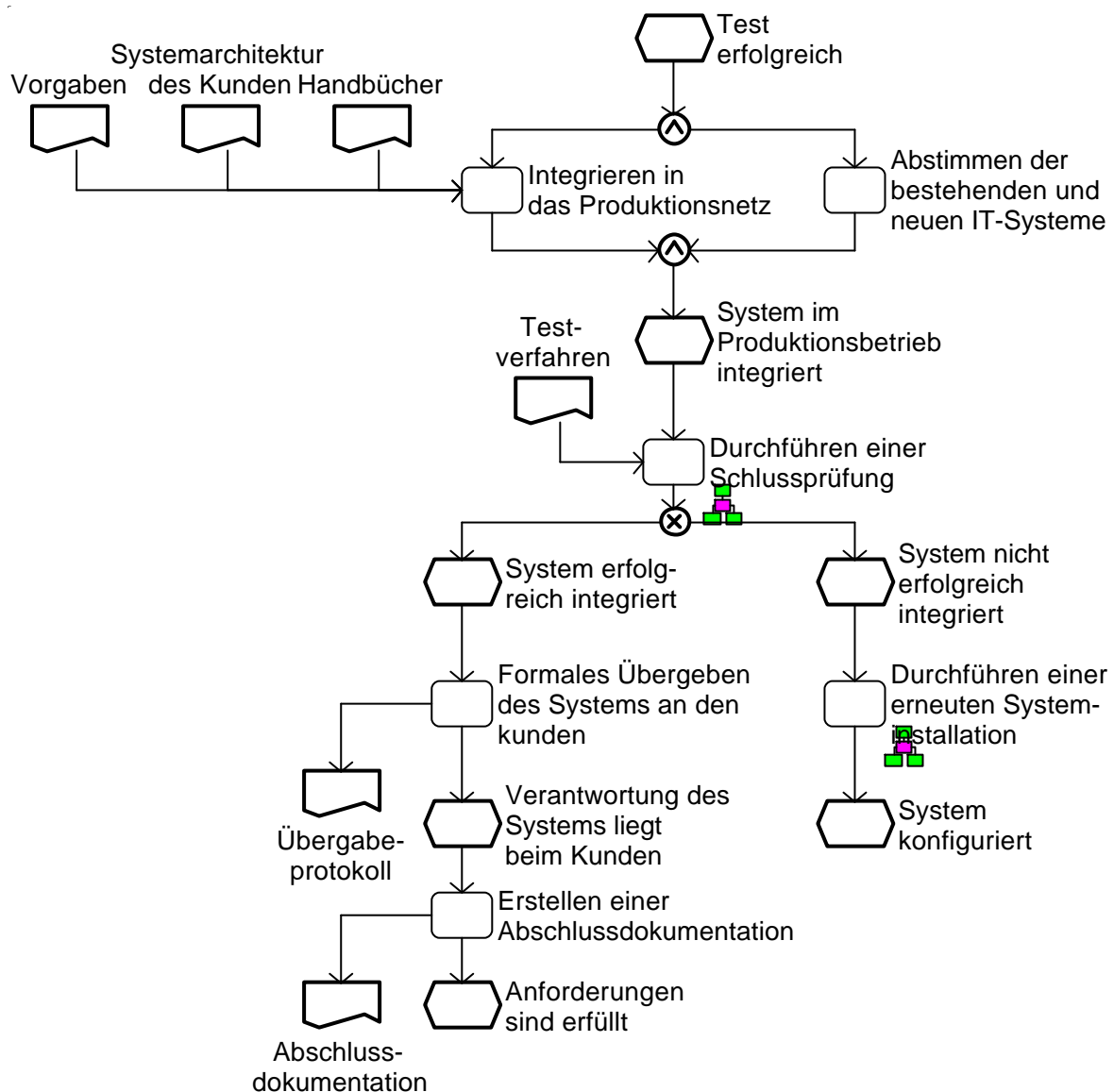


Abbildung 15: Durchführen der Übergabe

Sind die Tests vollständig abgeschlossen und alle Systemkomponenten in Ordnung, erfolgt die Integration in das Produktionsnetz des Kunden (sofern diese nicht bereits erfolgt ist). Dabei muss auf Sicherheitsvorgaben des Kunden geachtet werden und ein Ausfall der bestehenden Systeme vermieden werden. Auch hier erfolgt noch einmal eine Überprüfung aller Funktionen des Systems. Sollten sich hier Fehler zeigen, wird der Prozess der erneuten Systeminstallation durchlaufen. Ist der Abschlusstest erfolgreich, wird das System dem Kunden übergeben. Als Ergebnis wird die Anforderung erfüllt.

#### 3.1.2.8.1 Tätigkeiten: Durchführen der Übergabe

Für das Übergeben des Systems muss der IT Systems Administrator folgende Tätigkeiten durchführen:

- Integrieren in das Produktionsnetz
- Abstimmen der bestehenden und neuen IT-Systeme
- Durchführen einer Abschlussprüfung
- Formales Übergeben des Systems an den Kunden
- Erstellen einer Abschlussdokumentation

Falls das System nicht erfolgreich in den Produktionsbetrieb integriert wurde:

- Durchführen einer erneuten Systeminstallation

#### **3.1.2.8.2 Kompetenzfelder: Durchführen der Übergabe**

##### Fähigkeiten/Fertigkeiten

- System in das Produktionsnetz integrieren können
- Auf betroffene etablierte IT-Systeme im Produktionsnetz achten
- Schlussprüfung durchführen können
- System an Kunden (formal) übergeben können
- Dokumentieren können
- Kundenorientiert handeln können
- Verhandlungsgeschick beweisen können
- Teamfähig sein und zielgerichtete Gespräche führen können
- Kommunikativ sein

##### Wissen

- Rechtliche Rahmenbedingungen bei der Lieferung von bestellten Gütern kennen
- Allgemeine Geschäftsbedingungen (AGB) der Organisation und des Kunden kennen
- Verwendete Systemarchitekturen und Systeme, die beim Kunden eingesetzt sind, kennen
- Topologien des Kundennetzwerkes kennen und die daraus resultierenden Konfigurationsänderungen des zu übergebenden IT-Systems kennen
- Eingesetzte Kommunikations- und Netzwerkprotokolle des Kundensystems kennen und die Auswirkungen auf das zu übergebende System kennen
- Standards der Dokumentation in Bezug auf die Übergabe von IT-Systemen kennen

##### Werkzeuge

- Systemmanagementsoftware
- Netzwerkmanagementsoftware
- Konfigurationsmanagementsoftware
- Datenbanken
- Textverarbeitung

#### **3.1.2.8.3 Beispiel: Durchführen der Übergabe**

Die Server werden in der Zentrale und der Außenstelle aufgebaut, die USV an den zentralen Server angeschlossen und alle Rechner an das Hausnetz angeschlossen. Nun werden in einem abschließenden Test noch einmal alle Komponenten (Hard- und Software) getestet. Werden auch hier keine Fehler aufgedeckt, ist das System nun formal in Betrieb. In einem nächsten Schritt müssen die 200 Mitarbeiter-PCs mit Lotus Notes ausgestattet werden.

### 3.1.2.9 Erstellen einer Prozessdokumentation

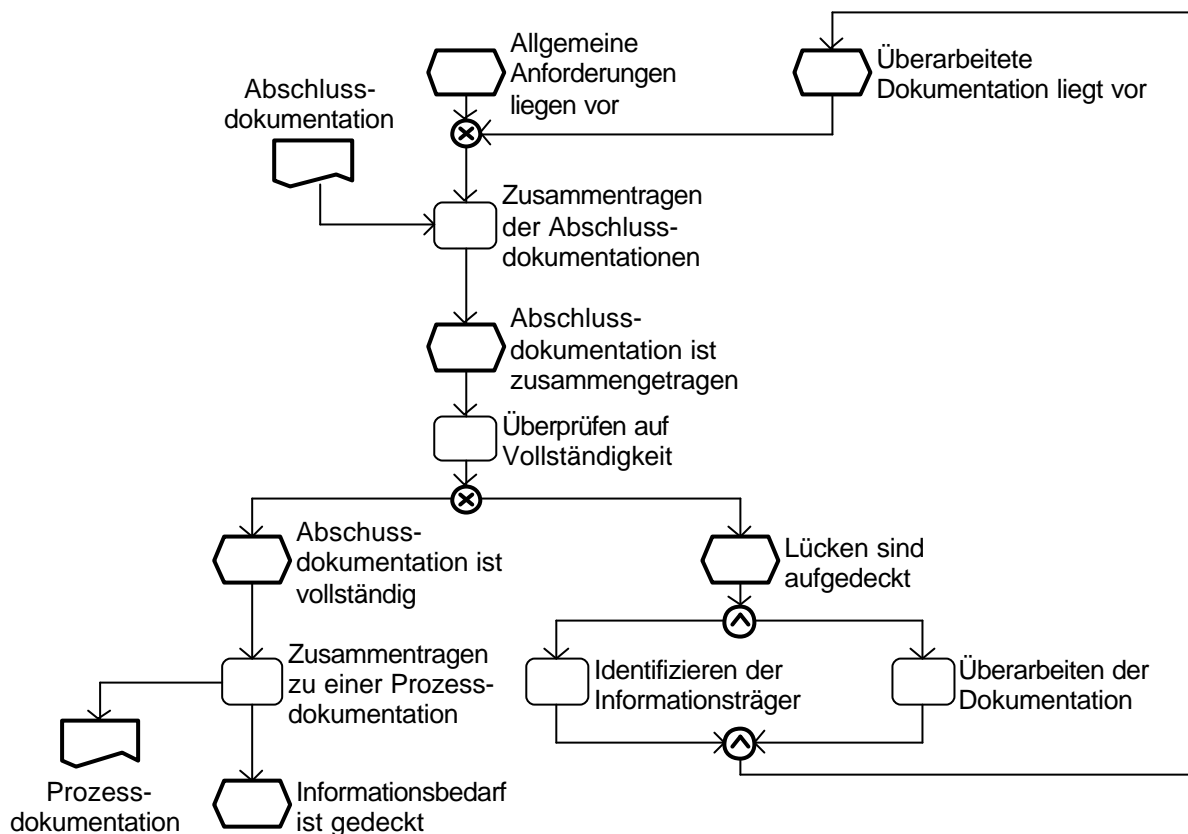


Abbildung 16: Erstellen einer Prozessdokumentation

Der Teilprozess „Erstellen einer Prozessdokumentation“ setzt sich aus einer kontinuierlichen Prozessdokumentation und Dokumentationen zu einzelnen Teilprozessen zusammen. Es ist sowohl das Vorgehen als auch die technischen Einstellwerte zu dokumentieren. Hier fallen die Tätigkeiten „Erstellen einer Abschlussdokumentation“, „Pflegen der Systemdokumentationen“ und „Dokumentieren der Testergebnisse“ hinein. Diese einzelnen Dokumente werden zusammengetragen, danach auf Vollständigkeit überprüft und zu einer abschließenden Prozessdokumentation zusammengefügt. Ziel dieses Prozesses ist es den kontinuierlichen Informationsbedarf zu decken. D. h. zum einen, dass einmal erarbeitete Prozessschritte mit der Dokumentation für Dritte nachvollziehbar werden und nicht erneut erarbeitet werden müssen, was die Effizienz im betrieblichen Alltag steigert. Zum anderen soll die Prozessdokumentation als Grundlage für eventuell zu erstellende Verfahrenshandbücher oder Best Practices dienen.

#### 3.1.2.9.1 Tätigkeiten: Erstellen einer Prozessdokumentation

Um eine Prozessdokumentation im Change-Management durchführen zu können, muss der IT Systems Administrator, meist parallel zu den Tätigkeiten der anderen Teilprozesse, folgende Tätigkeiten durchführen:

- Zusammentragen der Abschlussdokumentation
- Überprüfen auf Vollständigkeit

Falls die einzelnen Abschlussdokumentationen Lücken aufweisen:

- Identifizieren der Informationsträger
- Überarbeiten der Dokumentation

Auf jeden Fall:

- Zusammentragen zu einer Prozessdokumentation

### **3.1.2.9.2 Kompetenzfelder: Erstellen einer Prozessdokumentation**

#### Fähigkeiten/Fertigkeiten

- (Parallel zur Ausarbeitung) den gesamten Prozess dokumentieren können
- Übertragen der Tätigkeiten in Betriebshandbücher und Verfahrensanweisungen
- Betriebsvereinbarungen beachten können
- Sicherheitsrelevantes einschätzen und vor widerrechtlichen Zugriffen schützen können
- Informationslücken entdecken können

#### Wissen

- Standards der Dokumentation in Bezug auf das Nachvollziehen von Prozessschritten kennen
- Rechtliche Auswirkungen in Bezug auf Dokumentationslücken kennen

#### Werkzeuge

- Textverarbeitung

### **3.1.2.9.3 Beispiel: Erstellen einer Prozessdokumentation**

Die Dokumentation setzt sich aus den stetig zu erfolgenden Teildokumentationen während der Durchführung der einzelnen Prozessschritte zusammen. Diese werden im Verlauf des Projektes in einer Projektakte zusammengetragen. Da das Dokument für die Übergabe des Systems vollständig sein muss, werden noch einmal alle Eintragungen in das Systemhandbuch, Tätigkeiten und Konfigurationseinstellungen und sämtliche Gesprächsprotokolle überprüft, um anschließend einen Soll-Ist-Vergleich durchzuführen. Dieser ermöglicht zum einen eine Kontrolle, ob alle Anforderungen erfüllt wurden, und zum anderen kann er zum internen Controlling verwendet werden.

Für eine nicht in diesem Prozess involvierte Person müssen die durchgeführten Tätigkeiten nachvollziehbar und verständlich dokumentiert sein. So werden, wie schon in den einzelnen Teilprozessen beschrieben, unter anderem Netzwerkeinstellungen und Softwarekonfigurationen dokumentiert, noch auszuführende Tätigkeiten erfasst (wie die Installation der Lotus-Notes-Klienten) und auf aufgetretene Probleme bei der Installation der Hard- und Softwarekomponenten hingewiesen. Die so zusammengetragene Prozessdokumentation soll den Anspruch haben, dass man daraus eine „Best Practice“ für ähnlicher Projekte ableiten kann.

### **3.1.2.10 Informieren betroffener Stellen/Personen**

#### **3.1.2.10.1 Tätigkeiten: Informieren betroffener Stellen/Personen**

In diesem Abschnitt werden die Kommunikationsmaßnahmen als kontinuierliche, den gesamten Prozess begleitende Teilprozesse beschrieben.

Solche Ad-hoc-Kommunikationsmaßnahmen werden durchgeführt, wenn bestimmte Personen oder Stellen über den aktuellen Stand der Bearbeitung informiert werden müssen. Dazu zählen aber auch die Einweisung der Nutzer nach dem erfolgreich durchgeführten Änderungsprozess sowie ausführlichere Nutzerschulungen zu neu installierten Systemen.

Diese Tätigkeiten werden kumuliert im Referenzprozess „Benutzerberatung und Organisation“ (siehe Abschnitt 3.6ff.) durchgeführt. In diesen fallen auch die konkrete Schulung und Einweisung in das System.

#### **3.1.2.10.2 Kompetenzfelder: Informieren betroffener Stellen/Personen**

Fähigkeiten/Fertigkeiten

- Systemeinweisungen organisieren und durchführen können (siehe Abschnitt 3.6.2.4 Einweisen der Benutzer)
- Erklären können
- Dokumentieren können

Wissen

- Je nach Informationsbedarf Kenntnisse über relevante Themen, die den Nutzer betreffen können, besitzen

Werkzeuge

- Informationsverteiler

#### **3.1.2.10.3 Beispiel: Informieren betroffener Stellen/Personen**

Das Informieren von Personen und Stellen ist als prozessbegleitende Maßnahme zu verstehen. So muss der IT Systems Administrator die Geschäftsleitung über den Projektstand informieren, sie bei aufgetretenen Schwierigkeiten in Kenntnis setzen und eventuell durchgeführte Änderungen anzeigen. Da es sich bei diesem Projekt um ein internes handelt und kein Kundenkontakt gepflegt werden muss, sollte der IT Systems Administrator jedoch die Geschäftsleitung wie einen solchen behandeln.

Des Weiteren muss der IT Systems Administrator den Einkauf informieren, wenn die Lieferung der Hard- oder Software nicht die geforderte Form oder Güte besitzt. D. h. für ihn, dass er immer im engen Kontakt mit anderen Abteilungen oder Bereichen im Betrieb stehen muss.

Da es in diesem Projekt vorrangig um die Bereitstellung einer Serverstruktur geht, müssen Mitarbeiter noch nicht in der Hinsicht informiert oder eventuell auf die neue Software geschult werden. Nichtsdestotrotz ist in einer nächsten Phase die Installation und Konfiguration der Lotus-Notes-Klienten vorgesehen. Diesbezüglich müssen die Mitarbeiter in Kenntnis gesetzt werden, um so im Vorfeld auftretende Schwierigkeiten zu identifizieren und Blockaden oder Differenzen in Bezug auf die Software rechtzeitig entgegenzutreten zu können. Der IT Systems Administrator kann daraus bereits wichtige Informationen über die zu erstellenden Lehrmaterialien erhalten.





## 3.2 Fault-Management

---

Das Fehler- oder Störungsmanagement dient der Erfassung und Beseitigung von Unregelmäßigkeiten und Fehlerzuständen im System. Nach einer Erarbeitung eines Konzeptes, welches einen Überblick über das Gesamtsystem ermöglicht, werden Softwareprodukte eingesetzt, eigene Tools entwickelt und eingesetzt, die kontinuierlich den Systemstatus erfassen können.

Im Falle einer Störung, die entweder durch die Systemüberwachung oder durch externe Benachrichtigung bekannt wird, führt der Administrator eine systematische Fehlersuche durch. So werden Ort und Art des Fehlers identifiziert.

Liegt eine exakte Fehlerbeschreibung vor, entwickelt der Administrator einen Störungsbehebungsplan und setzt diesen um. Sollte dabei das IT-System im Gesamten betroffen sein, nimmt der IT Systems Administrator unter der Zuhilfenahme des Referenzprozesses „Change-Management“ Änderungen am Gesamtsystem vor. Dabei soll speziell eine Erstellung und die Pflege einer Best Practice-Datenbank für das Störungsmanagement vorangetrieben werden. Ein Test des Systems weist den Erfolg der Fehlerbeseitigung nach.

### 3.2.1 Referenzprozess Fault-Management

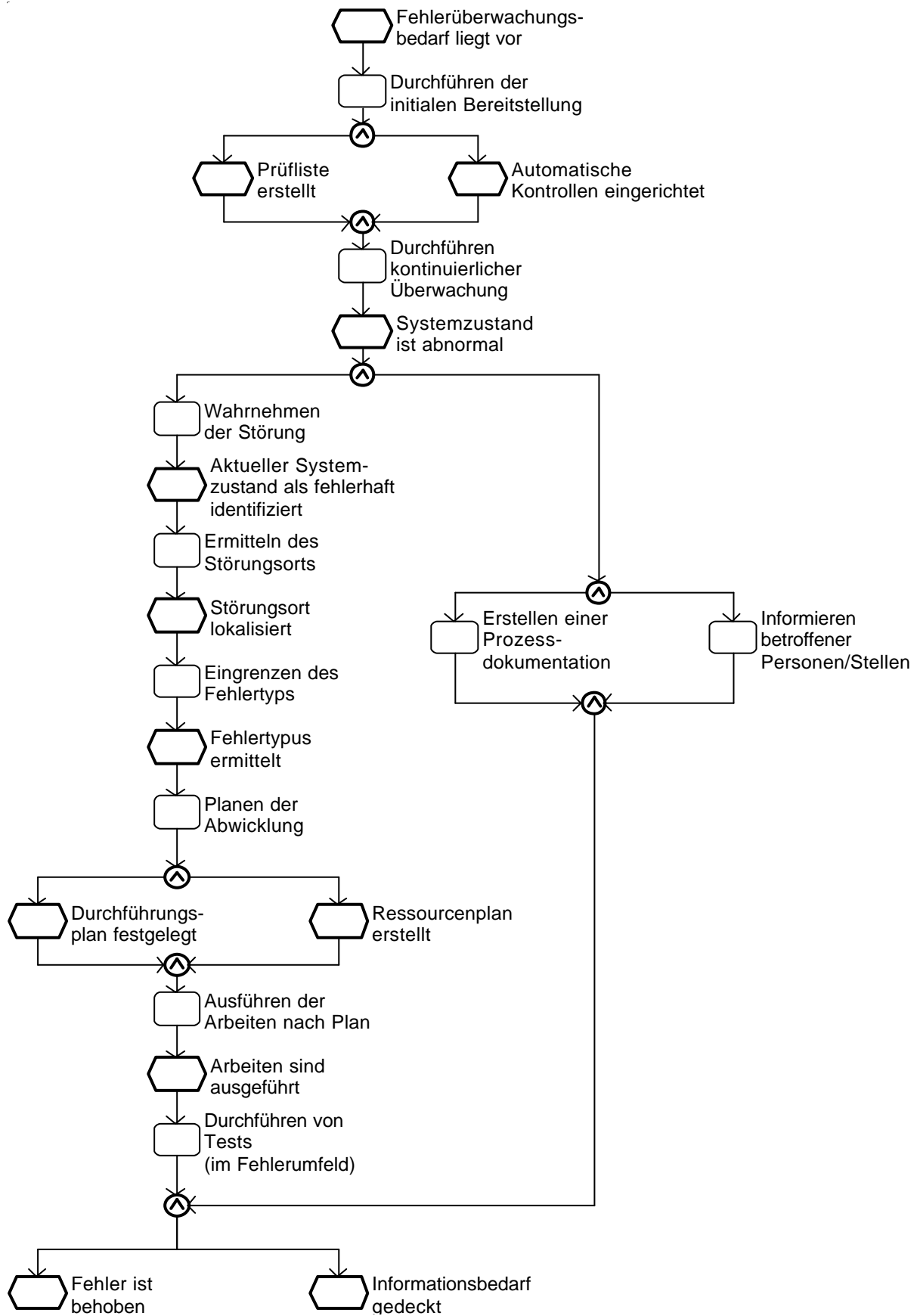


Abbildung 17: Referenzprozess Fault-Management

### **3.2.2 Prozesskompass Fault-Management**

Zusammenfassend sind folgende Teilprozesse im Referenzprozess Fault-Management enthalten:

1. Durchführen der initialen Bereitstellung
2. Durchführen kontinuierlicher Überwachung
3. Wahrnehmen der Störung
4. Ermitteln des Störungsorts
5. Eingrenzen des Fehlertyps
6. Planen der Abwicklung
7. Ausführen der Arbeiten nach Plan
8. Durchführen von Tests (im Fehlerumfeld)
9. Erstellen einer Prozessdokumentation
10. Informieren betroffener Personen/Stellen

### 3.2.2.1 Durchführen der initialen Bereitstellung

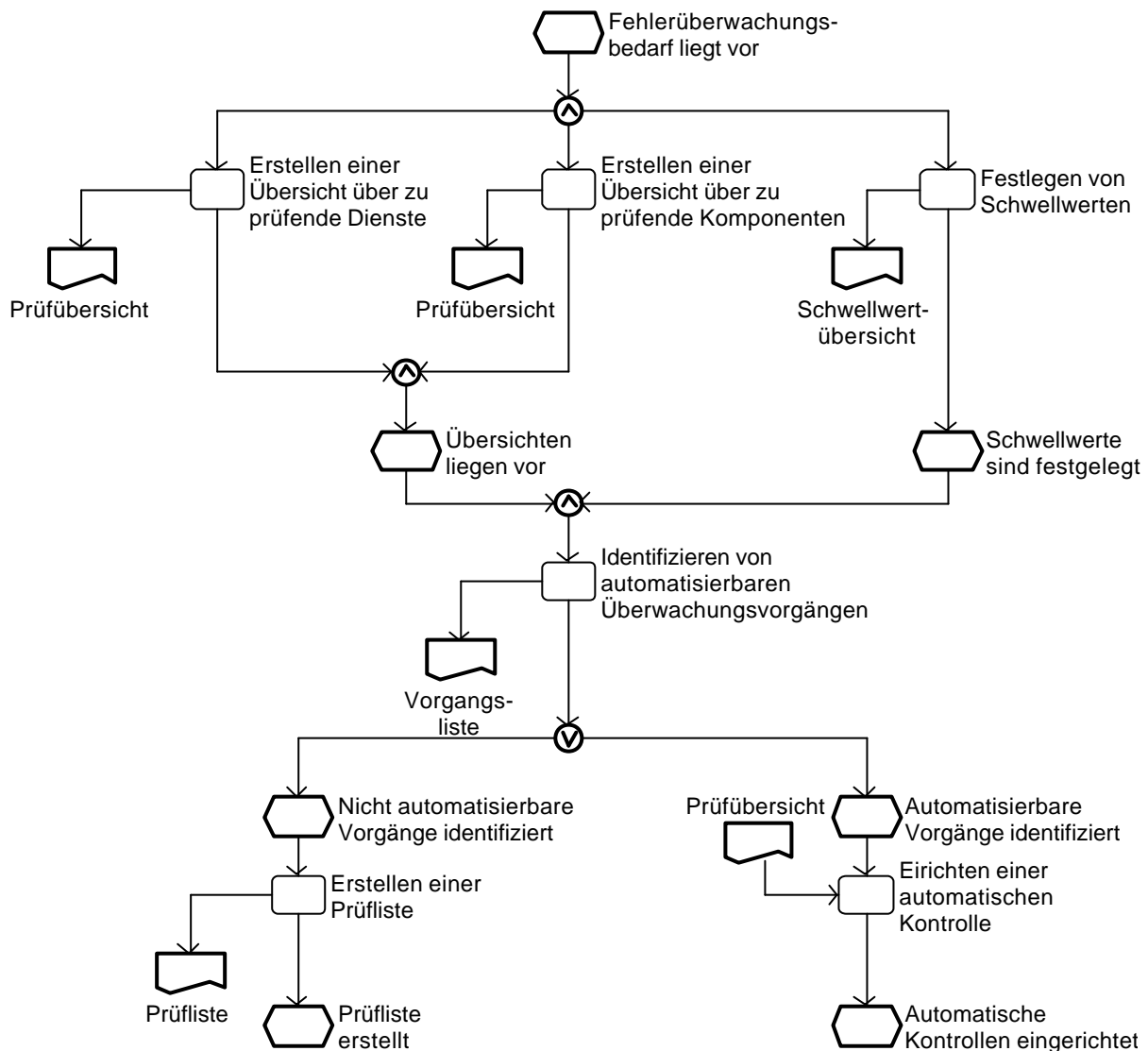


Abbildung 18: Durchführen der initialen Bereitstellung

Um ein Fault-Management durchführen zu können, muss erst einmal festgelegt werden, welche Komponenten und Dienste überwacht werden sollen und wie man eventuell den Überwachungsvorgang automatisieren kann. Außerdem müssen Schwellwerte definiert werden, deren Überschreitung ein Fehler des Systems signalisieren. Als Ergebnis dieses Teilprozesses erhält man eine Prüfliste und es wird eine automatische Kontrolle eingerichtet.

#### 3.2.2.1.1 Tätigkeiten: Durchführen der initialen Bereitstellung

Um die initiale Bereitstellung für das Fault-Management sicherzustellen, muss der IT Systems Administrator folgende Tätigkeiten durchführen:

- Erstellen einer Übersicht über zu prüfende Dienste
- Erstellen einer Übersicht über zu prüfende Komponenten
- Festlegen von Schwellwerten
- Identifizieren von automatisierbaren Überwachungsvorgängen
- Erstellen einer Prüfliste
- Einrichten einer automatischen Kontrolle

### 3.2.2.1.2 **Kompetenzfelder: Durchführen der initialen Bereitstellung**

#### Fähigkeiten/Fertigkeiten

- Übersichten erstellen können
- Übersichten über zu prüfende Dienste erstellen können
- Übersichten über zu prüfende Komponenten erstellen können
- Schwellwerte festlegen können
- Automatisierbare Vorgänge identifizieren können
- Prüflisten erstellen können
- Automatische Kontrollen einrichten können
- Dokumentieren können

#### Wissen

- Betriebsarten von Systemen und benutzen Hardware kennen
- Grundlegende Kenntnisse in der Netzwerktechnik und in Netzwerktopologien
- Kenntnisse von Datenübertragungssystemen und –techniken sowie der verwendeten Hardwareschnittstellen kennen
- Kenntnisse über die sich im Einsatz befindenden System- und Kommunikationsarchitekturen
- Kenntnisse über die sich im Einsatz befindenden Netzwerk- und Kommunikationsprotokollen sowie der Dienste und der verwendeten Schnittstellen zu anderen Systemen und Softwaresystemen
- Vorgehensmodelle bei der Erstellung eines Prüfverfahrens für das sich im Einsatz befindende IT-System
- Kenntnisse in der Auswertung von Systemmitteilungen durch Skriptsprachen
- Kenntnisse über informationstechnische und elektrische Leistungsgrößen
- Messverfahren kennen
- Kenntnisse über die sich im Einsatz befindenden Adapter und Hardwarecontroller
- Kenntnisse im Umgang mit Fernzugriffsverfahren und –software
- Kenntnisse in der Rationalisierung von Arbeitsschritten und deren Organisation in Bezug auf das Management von Fehlerzuständen des Systems
- Kenntnisse im Umgang mit Standards der Dokumentation bei Prävention und der Fehlerbeseitigung

#### Werkzeuge

- Systemmonitore
- Betriebssystemeigene Werkzeuge
- Skripteditoren
- Diagnosesoftware
- Fernzugriffssoftware

### 3.2.2.1.3 **Beispiel: Durchführen der initialen Bereitstellung**

Hier dient ebenfalls das Beispiel aus dem Kapitel 3.1 ff. Change-Management. Nachdem das System im Ganzen installiert und in Betrieb genommen wurde, müssen Vorbereitungsmaßnahmen getroffen werden, die einen fehlerfreien Betrieb gewährleisten können. Dazu müssen alle relevanten Dienste wie Mail, Replikation zwischen den Servern etc. aufgelistet werden und in eine Checkliste übernommen werden. Da es neben der Software auch bei der Hardware zu Ausfällen kommen kann, muss auch hier eine Übersicht erstellt werden. Diese wird aus dem Systemhandbuch entnommen. Hier werden unter anderem die einzelnen RAID-Controller mit den dort angeschlossenen Festplatten, die USV, die Prozessoren etc. ebenfalls in einer Checkliste aufgenommen. Für die einzelnen Dienste und Hardwarekomponenten werden Grenzwerte festgelegt. Wenn diese unter- bzw. überschritten werden, ist mit einem fehlerhaften oder nicht mehr den Anforderungen nach performanten System auszugehen.

In diesen Arbeitsschritten überlegt man sich, welche Dienste und Hardwarekomponenten sich über automatische Kontrollmeldungen überwachen lassen. Für die Hardware wird nun noch nachträglich Software installiert, die den Systemstatus dieser Komponenten überwachen kann und eventuell eine Mitteilung an den Systemadministrator senden kann. Für die Dominodienste wird das Überwachungstool eingesetzt, welches mit der Software mitgeliefert wurde. So können Mail- und Replikationsdienste automatisch überwacht werden. Neben diesen automatisierbaren Überwachungsvorgängen lassen sich eine Reihe von nicht automatisierbaren Vorgängen identifizieren. So kann die gekaufte USV nicht selbstständig ihren Sta-

tus überprüfen oder die Dominoserver können nicht von sich aus eventuelle Abstürze melden. Diese und eine Reihe weiterer nicht durch Automatismen abfangbaren Vorgänge werden in die Checkliste aufgenommen und es wird festgelegt, in welchen Zeiträumen eine Funktionsüberprüfung stattfinden muss.

### 3.2.2.2 Durchführen kontinuierlicher Überwachung

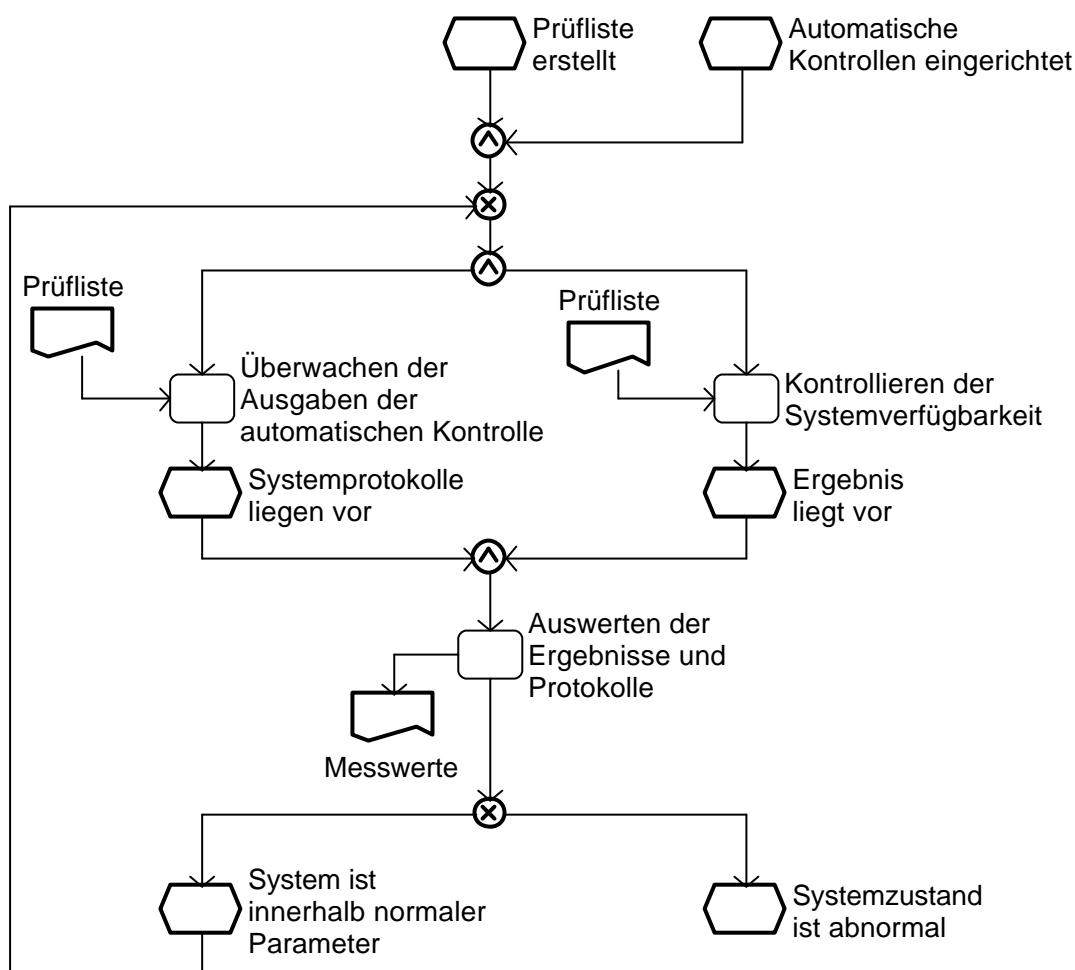


Abbildung 19: Durchführen kontinuierlicher Überwachung

Hat man sich Gedanken gemacht, was man mit welcher Vorgehensweise überwachen will, kann man kontinuierliche Messungen durchführen. Hier werden die Ausgaben der zuvor erstellten bzw. eingerichteten automatischen Kontrolle und die Kontrolle der Systemverfügbarkeit überwacht und ausgewertet. Tritt dabei eine Überschreitung eines vorher festgelegten Schwellwertes auf oder werden in den Ergebnissen oder Protokollen Fehler vermerkt, arbeitet das System nicht mehr einwandfrei. Wenn keine Überschreitung zu beobachten ist oder die Ergebnisse und Protokolle keine Fehler vermerken, führt man die kontinuierlichen Messungen weiter fort.

#### 3.2.2.2.1 Tätigkeiten: Durchführen der kontinuierlichen Überwachung

Durch folgende Tätigkeiten führt der IT Systems Administrator die kontinuierlichen Messungen durch:

- Überwachen der Ausgaben der automatischen Kontrolle
- Kontrollieren der Systemverfügbarkeit
- Auswerten der Ergebnisse und Protokolle

#### 3.2.2.2.2 Kompetenzfelder: Durchführen der kontinuierlichen Überwachung

Fähigkeiten/Fertigkeiten

- Ausgaben der kontinuierlichen Kontrolle auswerten können
- Ergebnisse und Protokolle interpretieren können
- Systemverfügbarkeiten prüfen können
- Dokumentieren können

#### Wissen

- Kenntnisse und Erfahrungen bei der Auswertung von Logdateien der verwendeten Betriebssysteme und Systemsoftware
- Kenntnisse in der Auswertung von Systemmitteilungen durch Skriptsprachen
- Betriebsarten von Systemen und benutzten Hardware kennen
- Grundlegende Kenntnisse in der Netzwerktechnik und in Netzwerktopologien
- Kenntnisse von Datenübertragungssystemen und –techniken sowie der verwendeten Hardwareschnittstellen besitzen
- Kenntnisse über die sich im Einsatz befindenden System- und Kommunikationsarchitekturen
- Kenntnisse über die sich im Einsatz befindenden Netzwerk- und Kommunikationsprotokollen sowie der Dienste und der verwendeten Schnittstellen zu anderen Systemen und Softwaresystemen
- Vorgehensmodelle bei der Erstellung eines Prüfverfahrens für das sich im Einsatz befindende IT-System kennen
- Kenntnisse über informationstechnische und elektrische Leistungsgrößen
- Messverfahren kennen
- Kenntnisse über die sich im Einsatz befindenden Adapter und Hardwarecontroller
- Kenntnisse im Umgang mit Fernzugriffsverfahren und –software
- Kenntnisse in der Rationalisierung von Arbeitsschritten und deren Organisation in Bezug auf das Management von Fehlerzuständen des Systems
- Kenntnisse im Umgang mit Standards der Dokumentation bei Prävention und der Fehlerbeseitigung

#### Werkzeuge

- Fernzugriffssoftware
- Systemmonitore
- Skripteditoren
- Diagnosesoftware
- Betriebssystemeigene Werkzeuge

#### **3.2.2.2.3 Beispiel: Durchführen kontinuierlicher Überwachung**

Während des Betriebs der Dominoserver werden ständig die Verfügbarkeitsstatistiken überprüft und sowie die Checklisten regelmäßig durchgegangen, um so im Vorfeld bereits auftretende Fehler zu identifizieren. Eventuell werden neue Dienste und Komponenten in die Checkliste aufgenommen, die entweder über automatische Kontrollen oder manuell überprüft werden müssen.



### 3.2.2.3 Wahrnehmen der Störung

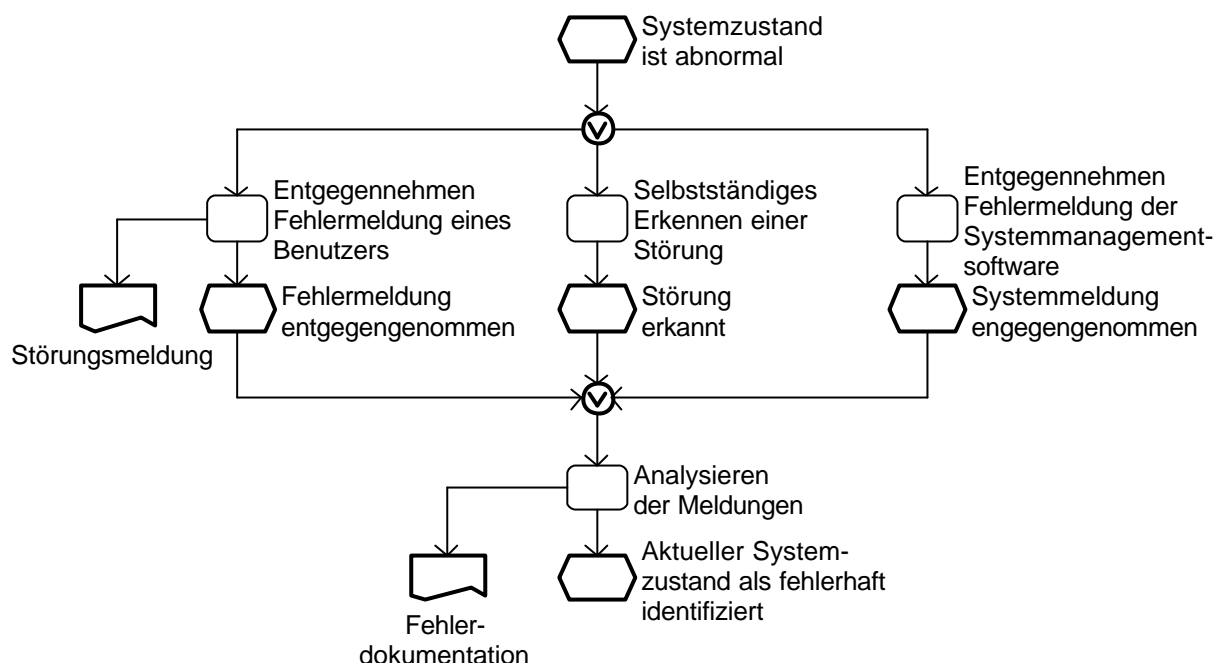


Abbildung 20: Wahrnehmen der Störung

Ergibt die Überwachung, dass der aktuelle Systemzustand abnormal ist, kann eine genauere Information zum Störungsbestand z. B. über die Systemmanagementsoftware und/oder durch eine Meldung von Benutzern beschrieben werden. Möglich ist hier auch, dass der IT Systems Administrator die Störung selbst erkennt. Im Anschluss müssen die Störungsmeldungen mit dem Ergebnis interpretiert werden, dass der aktuelle Systemzustand als fehlerhaft erkannt wird. Dies wird in einer Fehlerdokumentation festgehalten.

#### 3.2.2.3.1 Tätigkeiten: Wahrnehmen der Störung

Der IT Systems Administrator muss bei der Wahrnehmung einer Störung des Systems folgende Tätigkeiten durchführen:

- Entgegennehmen Fehlermeldung eines Benutzers
- Selbstständiges Erkennen einer Störung
- Entgegennehmen Fehlermeldung der Systemmanagementsoftware
- Analysieren der Meldungen

#### 3.2.2.3.2 Kompetenzfelder: Wahrnehmen der Störung

Fähigkeiten/Fertigkeiten

- Fehlermeldungen aus der Systemmanagementsoftware abrufen können
- Fehlermeldungen von Benutzern verstehen können
- Störung selbstständig erkennen können
- Meldungen bzw. erkannte Störungen interpretieren und analysieren können
- Dokumentieren können

Wissen

- Kenntnisse und Erfahrungen bei der Auswertung von Logdateien der verwendeten Betriebssysteme und Systemsoftware
- Erfahrungen bei der Identifikation und Interpretation von Fehlerzuständen des Systems besitzen
- Betriebsarten von Systemen und benutzter Hardware kennen
- Grundlegende Kenntnisse in der Netzwerktechnik und in Netzwerktopologien
- Kenntnisse von Datenübertragungssystemen und -techniken sowie der verwendeten Hardwareschnittstellen kennen
- Kenntnisse über die sich im Einsatz befindenden System- und Kommunikationsarchitekturen

- Kenntnisse über die sich im Einsatz befindenden Netzwerk- und Kommunikationsprotokollen sowie der Dienste und der verwendeten Schnittstellen zu anderen Systemen und Softwaresystemen
- Vorgehensmodelle bei der Erstellung eines Prüfverfahrens für das sich im Einsatz befindende IT-System kennen
- Kenntnisse über informationstechnische und elektrische Leistungsgrößen
- Messverfahren kennen
- Kenntnisse über die sich im Einsatz befindenden Adapter und Hardwarecontroller
- Kenntnisse im Umgang mit Fernzugriffsverfahren und –software
- Kenntnisse in der Rationalisierung von Arbeitsschritten und deren Organisation in Bezug auf das Management von Fehlerzuständen des Systems
- Kenntnisse im Umgang mit Standards der Dokumentation bei der Identifikation des Fehlerzustandes

#### Werkzeuge

- Fernzugriffssoftware
- Systemmonitore
- Systemmanagementsoftware
- Betriebssystemeigene Werkzeuge

#### **3.2.2.3.3 Beispiel: Wahrnehmen der Störung**

Über den durchgeführten Service (siehe 3.6.2.7) gehen innerhalb kürzester Zeit aus mehreren Abteilungen Meldungen ein, dass der Zugriff auf die Datenbanken auf dem Applikations-server nicht möglich ist. Anhand dieser Meldungen wird nun analysiert, wo die Störung aufgetreten ist. Sind alle Abteilungen oder ist nur ein Teil betroffen? Kann ein Ausfall des Servers ausgeschlossen werden? Fällt die Störung eventuell mit Arbeiten am System oder in der näheren Umgebung zusammen? Handelt es sich dabei eventuell um eine Netzwerkstörung und muss dann somit der Network Administrator angerufen werden? Diese Vermutungen werden zusammen mit der eingetroffenen Meldung in einer Fehlerdokumentation erfasst, welches später als Protokoll dienen soll.

### 3.2.2.4 Ermitteln des Störungsorts

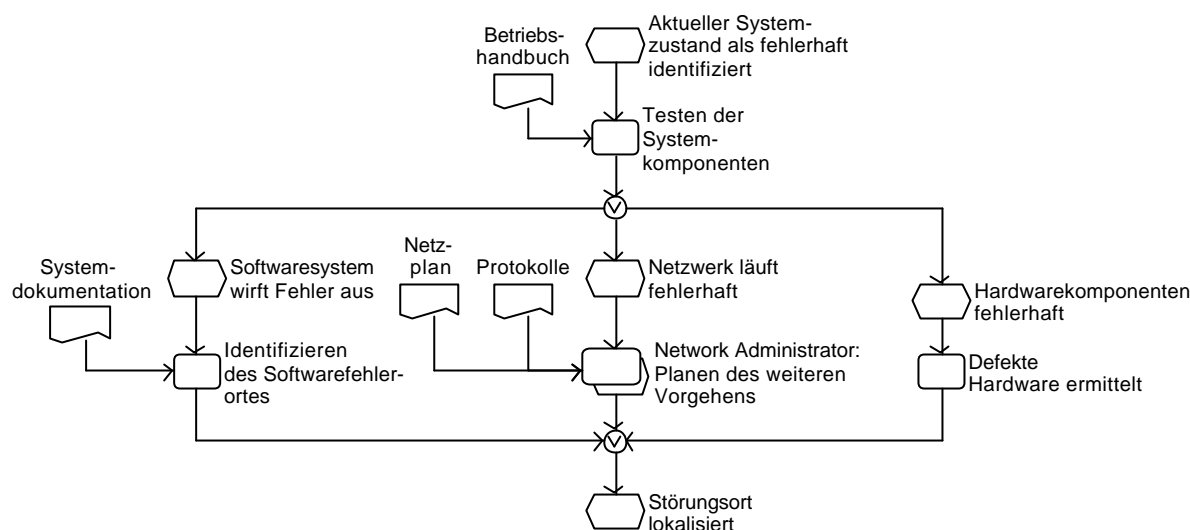


Abbildung 21: Ermitteln des Störungsorts

Wurde der aktuelle Systemzustand als fehlerhaft erkannt, werden die Systemkomponenten getestet. Dabei legt die Reihenfolge der zu testenden Komponenten immer der angenommene Fehler fest. Im Ergebnis wird die fehlerhafte Komponente identifiziert. Tritt der Fehler jedoch wegen eines Netzwerkproblems auf oder ist der Fehler ein Netzwerkproblem, wird dies dem Network Administrator kommuniziert und zusammen mit ihm das weitere Vorgehen zur Beseitigung besprochen. Ergebnis dieses Prozesses ist die Ermittlung des Störungsortes.

#### 3.2.2.4.1 Tätigkeiten: Ermitteln des Störungsortes

Durch folgende Tätigkeiten lokalisiert der IT Systems Administrator den Ort der Störung:

- Testen der Systemkomponenten

Falls das Softwaresystem den Fehler auswirft:

- Identifizieren des Softwarefehlerortes

Falls ein Hardwarefehler vorliegt:

- Ermitteln der defekten Hardware

Falls es sich um einen Netzwerkfehler handelt oder der Fehler durch einen Netzwerkfehler verursacht wird:

- Zusammen mit dem Network Administrator: Planen des Weiteren Vorgehens

#### 3.2.2.4.2 Fähigkeiten: Ermitteln des Störungsortes

Fähigkeiten/Fertigkeiten

- Systemkomponenten hinsichtlich von Fehlerursachen testen können
- Fehlerhafte Teilstücke des Systems diagnostizieren können
- Fehler im Netzwerk erkennen und untersuchen können
- Fehlerhafte Softwarekomponenten identifizieren können
- Vorgänge koordinieren können
- Dienste und deren Abhängigkeiten kennen
- Fehlerhafte Hardwarekomponenten identifizieren können
- Aus Erfahrungen lernen können
- Pragmatisches und systematisches Vorgehen besitzen
- Dokumentieren können

Wissen

- Erfahrungen bei Ortsbestimmung von Fehlerzuständen des Systems und Kenntnisse über deren Zusammenhänge besitzen

- Betriebsarten von Systemen und benutzter Hardware kennen
- Kenntnisse von Datenübertragungssystemen und –techniken sowie der verwendeten Hardwareschnittstellen kennen
- Kenntnisse über die sich im Einsatz befindenden System- und Kommunikationsarchitekturen
- Kenntnisse über die sich im Einsatz befindenden Netzwerk- und Kommunikationsprotokollen sowie der Dienste und der verwendeten Schnittstellen zu anderen Systemen und Softwaresystemen
- Messverfahren kennen
- Kenntnisse über die sich im Einsatz befindenden Adapter und Hardwarecontroller
- Kenntnisse im Umgang mit Fernzugriffsverfahren und –software
- Kenntnisse in der Rationalisierung von Arbeitsschritten und deren Organisation in Bezug auf das Management von Fehlerzuständen des Systems
- Kenntnisse im Umgang mit Standards der Dokumentation bei der Identifikation des Fehlerzustandes

#### Werkzeuge

- Datenbanken
- Informationsquellen wie Newsgroups, Zeitschriften, Mailinglisten, Herstellerinformationen
- Testprogramme
- Testgeräte

#### **3.2.2.4.3 Beispiel: Ermitteln des Störungsorts**

Bei der eingeleiteten Routineprüfung stellt sich heraus, dass das Betriebssystem zwar reagiert, aber nicht der Applikationsserver. Zunächst wird der Dominoserver selbst gestartet. Dieser fährt fehlerfrei hoch. Auf die Datenbanken kann weiterhin nicht zugegriffen werden. Deshalb wird ein kompletter Neustart des Systems durchgeführt, da einige Festplatten nicht zur Verfügung stehen. Diese können sich auf nicht nachvollziehbare Weise vom RAID-Controller abgemeldet haben.

### 3.2.2.5 Eingrenzen des Fehlertyps

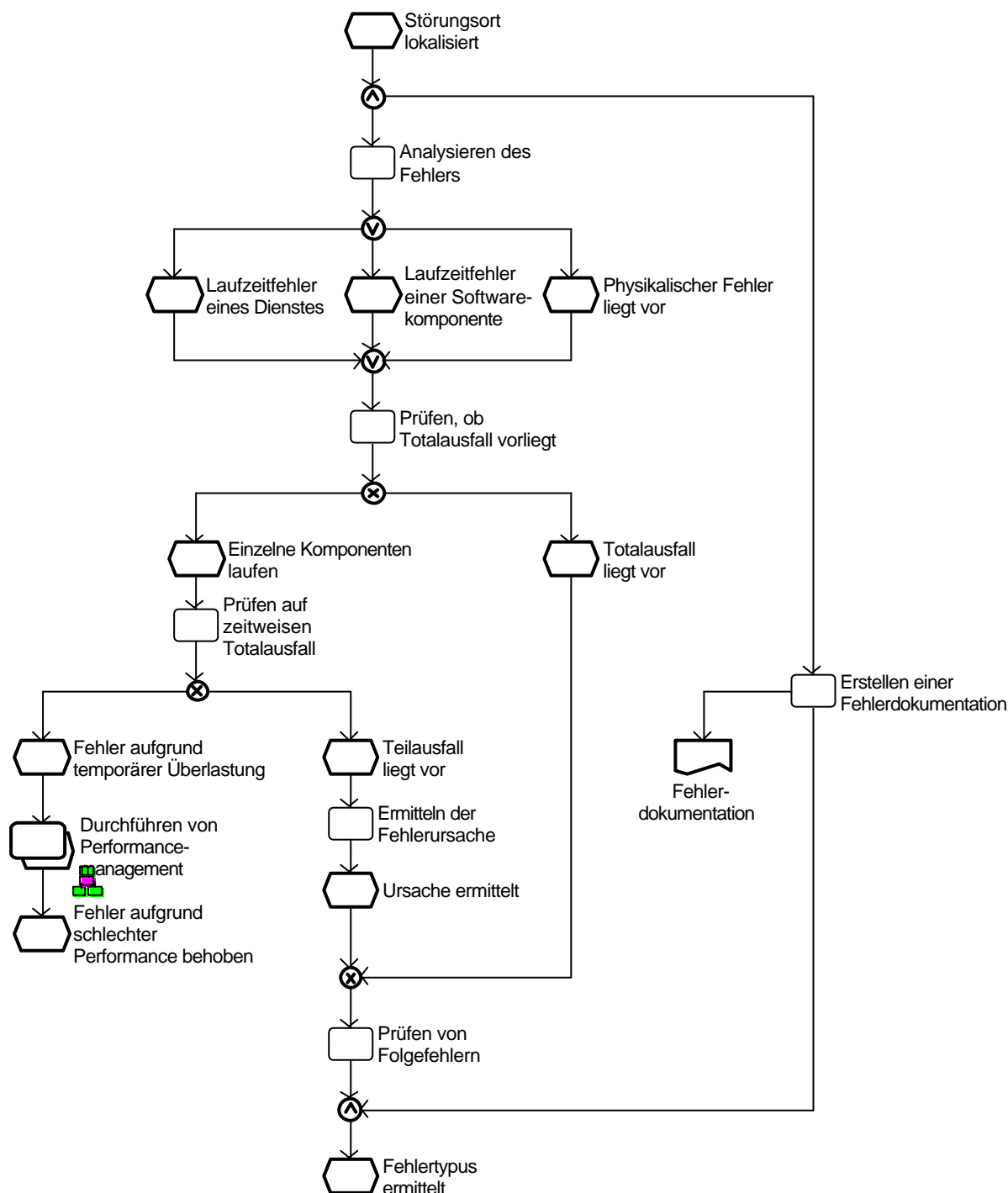


Abbildung 22: Eingrenzen des Fehlertyps

Ist der Störungsort ermittelt, wird der Fehlertyp bestimmt. Ist dieser ermittelt, wird überprüft, ob ein Totalausfall der betroffenen Komponenten vorliegt. Liegt kein Totalausfall vor, wird auf zeitweisen Totalausfall geprüft. Handelt es sich um einen zeitweisen Teilausfall, werden die Fehlerursachen ermittelt. In jedem Fall erfolgt noch die Ermittlung von Folgefehlern. Ergebnis dieses Prozesses ist die Ermittlung des Fehlertyps. Zusammenfassend werden die eingegrenzten Fehler in der Prozessdokumentation eingefügt. Handelt es sich jedoch bei diesem Teilausfall um ein Performanceproblem der identifizierten Komponenten, wird der Prozess des Performance-Management (siehe Abschnitt 3.3ff.) vom IT Systems Administrator durchgeführt.

### **3.2.2.5.1 Tätigkeiten: Eingrenzen des Fehlertyps**

Um den Fehlertyp eingrenzen zu können, muss der IT Systems Administrator folgende Tätigkeiten durchführen:

- Analysieren des Fehlers
- Prüfen, ob Totalausfall vorliegt

Falls noch einige Komponenten laufen:

- Prüfen auf zeitweisen Totalausfall

Falls ein Teilausfall vorliegt:

- Ursache ermitteln

Auf jeden Fall:

- Prüfen von Folgefehlern
- Erstellen einer Fehlerdokumentation

Falls der Fehler aufgrund einer temporären Überlastung verursacht wurde:

- Durchführen Performance-Management

### **3.2.2.5.2 Fertigkeiten: Eingrenzen des Fehlertyps**

Fähigkeiten/Fertigkeiten

- Fehler analysieren können
- System auf Totalausfall prüfen können
- Auf zeitweisen Totalausfall prüfen können
- Fehlerursachen ermitteln können
- Folgefehler identifizieren können
- Performance-Management durchführen können
- Dienstabhängigkeiten kennen
- Funktionen der Dienste kennen
- Dokumentieren können

Wissen

- Erfahrungen bei Arten von Fehlerzuständen des Systems und Kenntnisse über deren Zusammenhänge besitzen
- Betriebsarten von Systemen und benutzter Hardware kennen
- Kenntnisse von Datenübertragungssystemen und -techniken sowie der verwendeten Hardwareschnittstellen
- Kenntnisse über die sich im Einsatz befindenden System- und Kommunikationsarchitekturen
- Kenntnisse über die sich im Einsatz befindenden Netzwerk- und Kommunikationsprotokollen sowie der Dienste und der verwendeten Schnittstellen zu anderen Systemen und Softwaresystemen
- Messverfahren kennen
- Kenntnisse über die sich im Einsatz befindenden Adapter und Hardwarecontroller
- Kenntnisse im Umgang mit Fernzugriffsverfahren und -software
- Kenntnisse in der Rationalisierung von Arbeitsschritten und deren Organisation in Bezug auf das Management von Fehlerzuständen des Systems
- Kenntnisse im Umgang mit Standards der Dokumentation bei der Fehlerursachenbestimmung haben

Werkzeuge

- Diagnosewerkzeuge

### **3.2.2.5.3 Beispiel: Eingrenzen des Fehlertyps**

Nach dem durchgeführten Reset lässt sich das System nicht neu starten. Das BIOS des RAID-Controller meldet, dass eins der beiden RAID-Arrays ausgefallen ist. Um den Fehler genauer zu lokalisieren, wird ein Test des RAID-Systems mithilfe des Diagnoseprogramms des Herstellers durchgeführt. Der durchgeführte Test ergibt, dass alle Platten eines Arrays

ausgefallen sind. Anhand der Prüfung wird vermutet, dass einer der SCSH-Kanäle ausgefallen ist.

### 3.2.2.6 Planen der Abwicklung

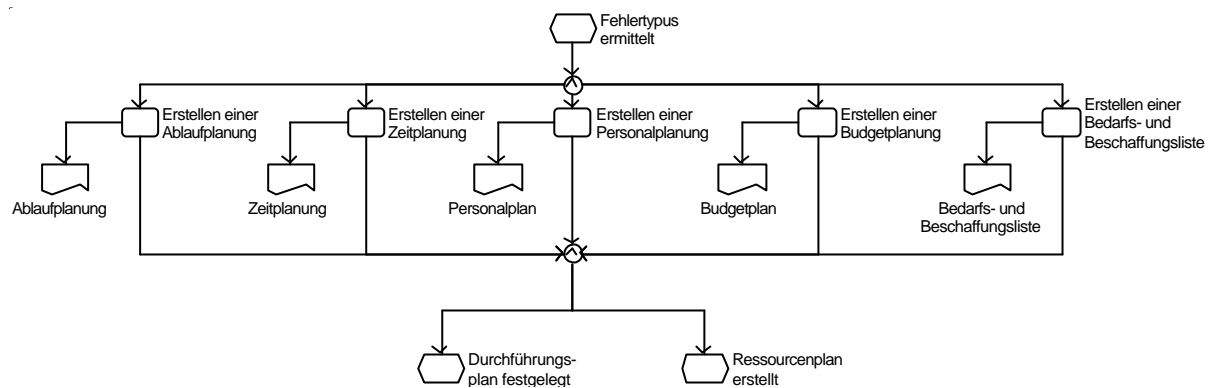


Abbildung 23: Planen der Abwicklung

Ist der Typ des Fehlers bekannt, werden die Ressourcen und das Vorgehen geplant. Im Anschluss daran liegen ein Durchführungs- und ein Ressourcenplan vor (für weitere Erläuterungen siehe 3.1.2.3 Planen der Abwicklung).

#### 3.2.2.6.1 Tätigkeiten: Planen der Abwicklung

Folgende Tätigkeiten muss ein IT Systems Administrator bei der Planung der Abwicklung durchführen:

- Erstellen einer Zeitplanung
- Erstellen einer Ablaufplanung
- Erstellen einer Bedarfs- und Beschaffungsliste
- Erstellen einer Personalplanung
- Erstellen einer Budgetplanung

#### 3.2.2.6.2 Kompetenzfelder: Planen der Abwicklung

Fähigkeiten/Fertigkeiten

- Planen können
- Zeitplanung erstellen können
- Beschaffungsliste erstellen können
- Zukünftigen Bedarf ermitteln können
- Sich selbst und eventuell Mitarbeiter beurteilen und einschätzen können
- Personalplanung erstellen können
- Budgetplanung erstellen können
- Ablaufplanung erstellen können
- Spezielle Anforderungen verstehen können
- Kaufmännisches Rechnen durchführen können
- Zukünftige Aufwände kalkulieren und prognostizieren können
- Dokumentieren können
- Rechtliche Rahmenbedingungen einhalten

Wissen

- Kenntnisse bei der Planung von Prozessen und Projekten sowie über organisatorische Auswirkungen
- Kenntnisse in der Rationalisierung von Arbeitsschritten und deren Organisation in Bezug auf die Beseitigung von Fehlerzuständen des Systems
- Standards der Dokumentation für die Planungsabläufe von Projekten kennen
- Betriebswirtschaftliche Grundkenntnisse in der Kosten- und Nutzenanalyse

Werkzeuge

- Projektmanagementsoftware
- Kaufmännische Software
- Tabellenkalkulation



**3.2.2.6.3 Beispiel: Planen der Abwicklung**

Da die Wartung der Controller im Servicevertrag durch den Hersteller erfolgt, wird die Servicehotline angerufen. Die Prüfung soll durch einen Techniker eines ortsansässigen Systemhauses, welches im Namen des Herstellers Serviceleistungen anbieten kann, durchgeführt werden. Die Behebung der Störung wird auf ca. vier Stunden geschätzt. Eventuell können auch die Festplatten selbst betroffen sein. Eine erste Aufwandseinschätzung der zu ersetzenden Hardware sowie die Personalkosten des Technikers werden dem Vorgesetzten gemeldet. Dieser gibt sein Okay für die auszuführenden Tätigkeiten.

### 3.2.2.7 Ausführen der Arbeiten nach Plan

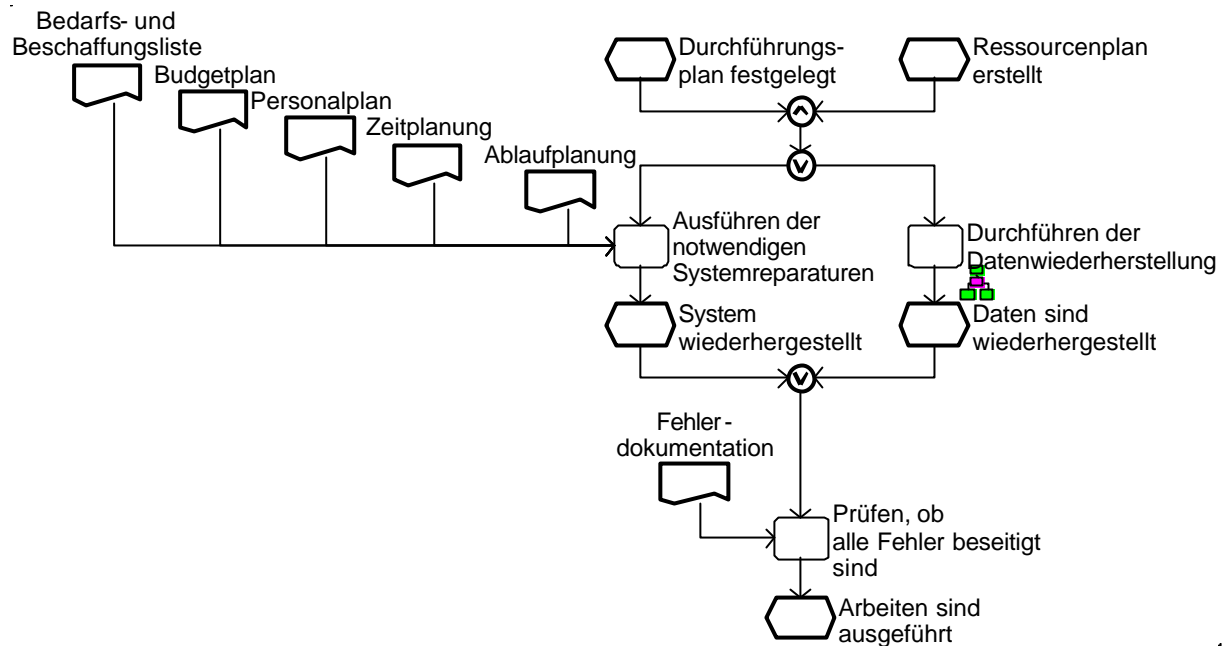


Abbildung 24: Ausführen der Arbeiten nach Plan

Steht der Durchführungsplan fest und ist der Ressourcenplan erstellt, wird die Fehlerbeseitigung durchgeführt. Dann beginnt die Ausführung der für die Störungsbeseitigung notwendigen Reparaturen und falls mit dem Auftreten Daten verloren oder zerstört wurden, werden diese so weit wie möglich (Stand der letzten Datensicherung) wiederhergestellt. Der Prozess endet damit, dass anhand der angefertigten Fehlerdokumentation im ersten Zug überprüft wird, ob alle Fehler beseitigt wurden.

#### 3.2.2.7.1 Tätigkeiten: Ausführen der Arbeiten nach Plan

Um eine Fehlerbeseitigung durchführen zu können, muss der IT Systems Administrator folgende Tätigkeiten durchführen:

- Ausführen der notwendigen Systemreparaturen
- Durchführen der Datenwiederherstellung
- Prüfen, ob alle Fehler beseitigt sind

#### 3.2.2.7.2 Kompetenzfelder: Ausführen der Arbeiten nach Plan

Fähigkeiten/Fertigkeiten

- Systemreparaturen selbstständig durchführen können
- Daten wiederherstellen können
- Nach Bedarf andere Prozesse des IT Systems Administrator für die Ausführung heranziehen können
- Überprüfen können, ob Arbeiten vollständig ausgeführt wurden

Wissen

- Kenntnisse über die konkrete Art und den Ort des Fehlers sowie der daraus resultierenden Tätigkeiten
- Kenntnisse in der Rationalisierung von Arbeitsschritten und deren Organisation in Bezug auf die Beseitigung von Fehlerzuständen des Systems
- Standards der Dokumentation in Bezug auf Nachvollziehbarkeit von Tätigkeiten

Werkzeuge

- Konfigurationsmanagementsoftware

### 3.2.2.7.3 **Beispiel: Ausführen der Arbeiten nach Plan**

Der Servicetechniker baut wie vereinbart den neuen RAID-Controller ein und will die vorhandenen Konfigurationen auf den neuen Controller einspielen. Jedoch lässt sich das Konfigurationsmenü des Controllers nicht aufrufen. Der Techniker vermutet als zusätzliche Fehlerquelle ein Defekt auf dem Mainbord. Er baut den alten Controller wieder ein und fährt zurück zum Systemhaus, um einen neuen RAID-Controller zu holen. Wenig später ruft er an, dass derzeit kein neuer Controller bei ihnen auf Lager ist und erst am Montag wieder geliefert werden kann. Dies wird dem Vorgesetzten gemeldet. Um nun einen weiteren Arbeitsausfall zu vermeiden, wird mit dem Techniker vereinbart, dass der Controller direkt vom Hersteller per UPS noch heute (Freitag) bestellt werden soll und der Einbau über das Wochenende zu erfolgen hat.

Der defekte Controller wird durch den neuen Controller ersetzt. Beim Versuch, die Konfiguration des RAID-Systems zurück auf den neuen Controller zu lesen, tritt der gleiche Fehler auf, wie beim ersten Austauschversuch. Auch dieses mal ist es nicht möglich, das Konfigurationsprogramm zu starten. Nach mehrmaliger Rücksprache mit der Herstellerhotline kann das Problem nicht behoben werden.

Schließlich vermutet der IT Systems Administrator, dass eventuell ein Tastaturproblem vorliegt, weil das Konfigurationsprogramm des Controllers über eine bestimmte Tastenkombination aufgerufen wird. Nach einem Austausch der Servertastatur lässt sich das Konfigurationsprogramm ohne Probleme aufrufen und die Konfiguration auf den neuen Controller zurückschreiben.

Über den neuen Controller kann wieder auf beide Plattenarrays zugegriffen werden. Im zweiten Array wird jedoch eine fehlerhafte Platte erkannt, diese wird ebenfalls getauscht und eine Reorganisation des Arrays durchgeführt. Das bei Wartungsarbeiten durch die vom Hersteller vorgeschriebenen Firmware-Upgrades nach dem Tausch der Platte misslingt. Es werden mehr als die Hälfte der Platten als „Replace“ markiert. Ein erneuter Anruf bei der Servicehotline des Herstellers ergibt, dass sämtliche betroffenen Platten ausgetauscht werden müssen. Diese müssen am Montag neu bestellt werden. Um einen weiteren Arbeitsausfall zu vermeiden, werden die Plattenarrays auf aktiv gesetzt. So können die defekten Platten im laufenden Betrieb gewechselt werden. Anschließend wird eine Wiederherstellung der Daten durchgeführt und über das Transaktionsprotokoll der Zustand nach der letzten Datensicherung wiederhergestellt.

Nachdem die Platten eingetroffen sind, werden die als „Replace“ markierten Platten ausgetauscht. Nach dem Abschluss der Arbeiten werden alle Platten als fehlerfrei erkannt und das RAID-System meldet den Status „stable“.

### 3.2.2.8 Durchführen von Tests (im Fehlerumfeld)

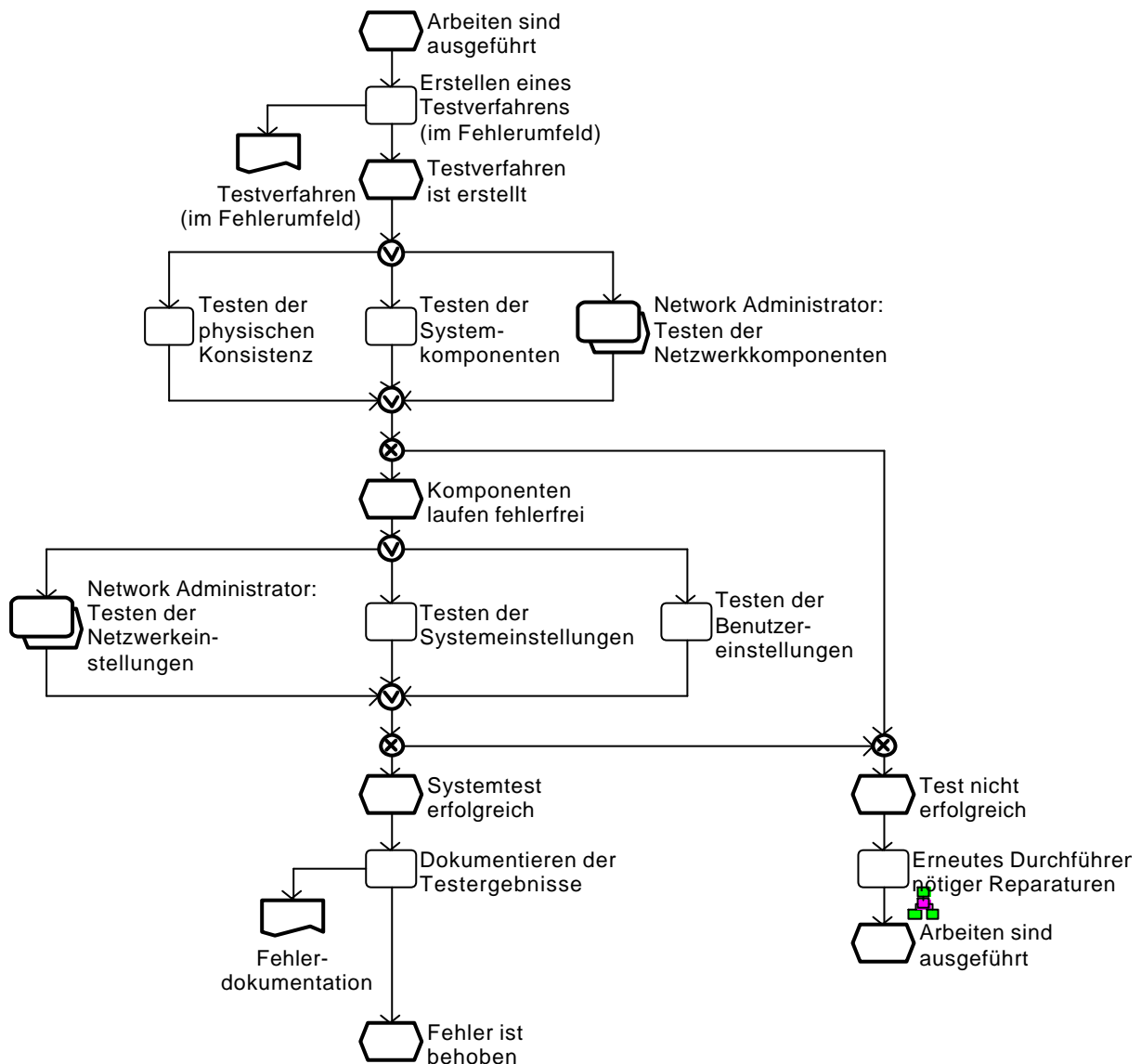


Abbildung 25: Durchführen von Tests (im Fehlerumfeld)

Wird angenommen, dass der Fehler behoben ist, wird das Gesamtsystem zu Testzwecken in Betrieb genommen. Dazu werden im Kontext des Testverfahrens die physische Konsistenz, die Systemkomponenten und, zusammen mit dem Network Administrator die Netzwerkkomponenten auf einwandfreie Funktion und Stabilität geprüft. Laufen die Komponenten fehlerfrei, werden die System- und Benutzereinstellungen und zusammen mit dem Network Administrator die Netzwerkeinstellungen überprüft. Sollten hier oder beim Testen der Einzelkomponenten erneut Fehler auftreten, wird das Fault-Management mit diesen neuen Erkenntnissen erneut durchgeführt. Waren die Tests jedoch erfolgreich, werden abschließend die Testergebnisse der Fehlerdokumentation beigefügt. Der aufgetretene Fehler ist somit behoben und das System funktioniert wieder einwandfrei. Der IT Systems Administrator kann mit der kontinuierlichen Überwachung fortfahren.

#### 3.2.2.8.1 Tätigkeiten: Durchführen von Tests (im Fehlerumfeld)

Um einen Test im Fehlerumfeld durchzuführen, muss der IT Systems Administrator folgende Tätigkeiten ausführen:

- Erstellen eines Testverfahrens (im Fehlerumfeld)
- Testen der physischen Konsistenz
- Testen der Systemkomponenten
- Zusammen mit dem Network Administrator: Testen der Netzwerkkomponenten

Laufen die Komponenten stabil:

- Zusammen mit dem Network Administrator: Testen der Netzwerkeinstellungen
- Testen der Systemeinstellungen
- Testen der Benutzereinstellungen

War der Systemtest erfolgreich:

- Dokumentieren der Testergebnisse

War der Komponenten- oder Systemtest nicht erfolgreich:

- Erneutes Durchführen der nötigen Reparaturen

### **3.2.2.8.2 Kompetenzfelder: Durchführen von Tests (im Fehlerumfeld)**

Fähigkeiten/Fertigkeiten

- Datenleitungen testen können
- Netzwerkkomponenten und Netzwerkeinstellungen zusammen mit dem Network Administrator überprüfen können
- Zielgerichtete Gespräche führen können
- Systemeinstellungen testen können
- Benutzereinstellungen testen können
- Bei Tests systematisch vorgehen können
- Testverfahren erstellen und weiterentwickeln können
- Testverfahren kennen
- Systemanforderungen verstehen und umsetzen können
- Systemeigene Werkzeuge kennen und nutzen können
- Ergebnis- und Fehlerprotokolle interpretieren können
- Dienste kennen und deren Laufzeit beobachten und überprüfen können
- Anforderungsdefinitionen verifizieren können
- Vorhandene Informationsquellen aus Herstelldokumentationen, Systembeschreibungen etc. effektiv nutzen können
- Informationsquellen erschließen können
- Aus Erfahrungen planen können
- Testergebnisse fehlerfrei dokumentieren können
- Dokumentieren können

Wissen

- Über grundlegende Kenntnisse in der Organisation und Komponenten von Netzwerken verfügen
- Kenntnisse über die verwendeten Systemarchitekturen, Betriebssysteme und Softwaresysteme
- Erfahrungen mit Hardwaretests in wesentlichen Betriebsarten
- Verwendete Schnittstellenfunktionen zu anderen Systemen und innerhalb des eigenen Systems kennen
- Kenntnisse der Funktion von Kommunikations- und Netzwerkprotokollen sowie der verwendeten Dienste und Komponente
- Testverfahren und ihre Referenzmodelle kennen
- Erfahrungen in der Verwendung von Protokollen für Tests und Konfigurationen
- Funktionsweise von Datenübertragungssystemen und -techniken sowie von Systemsoftware
- Standards von Testverfahren
- Standards der Dokumentation in Bezug auf Nachvollziehbarkeit von Fehlerzuständen und getesteten Systembereichen

Werkzeuge

- Ereignismonitore
- Performancemonitore (im Testumfeld)
- Diagnosesoftware
- Testsoftware
- Textverarbeitung

#### **3.2.2.8.3 Beispiel: Durchführen von Tests**

Für den Ausfall von Hardware, insbesondere von Festplatten, wurde im Vorfeld ein Stress-test entworfen. Dieser wird durch ein firmeneigenes Script durchgeführt, welches ununterbrochen Daten auf Festplatten schreibt und diese anschließend überprüft. Des Weiteren kann aufgrund der Checkliste überprüft werden, ob alle Hard- und Softwarekomponenten fehlerfrei laufen.

Der Stresstest wird über Nacht durchgeführt. Am nächsten Tag wird der Erfolg überprüft. Da es zu keinen weiteren Fehlern gekommen ist, wird der Vorgesetzte in Kenntnis gesetzt, dass das Hardwareproblem gelöst und der Server wieder in Betrieb genommen werden kann. Nachdem überprüft wurde, dass alle Dienste fehlerfrei laufen, kann zur kontinuierlichen Überwachung übergegangen werden. Die Testergebnisse werden in die Fehlerdokumentation übertragen.

### 3.2.2.9 Erstellen einer Prozessdokumentation

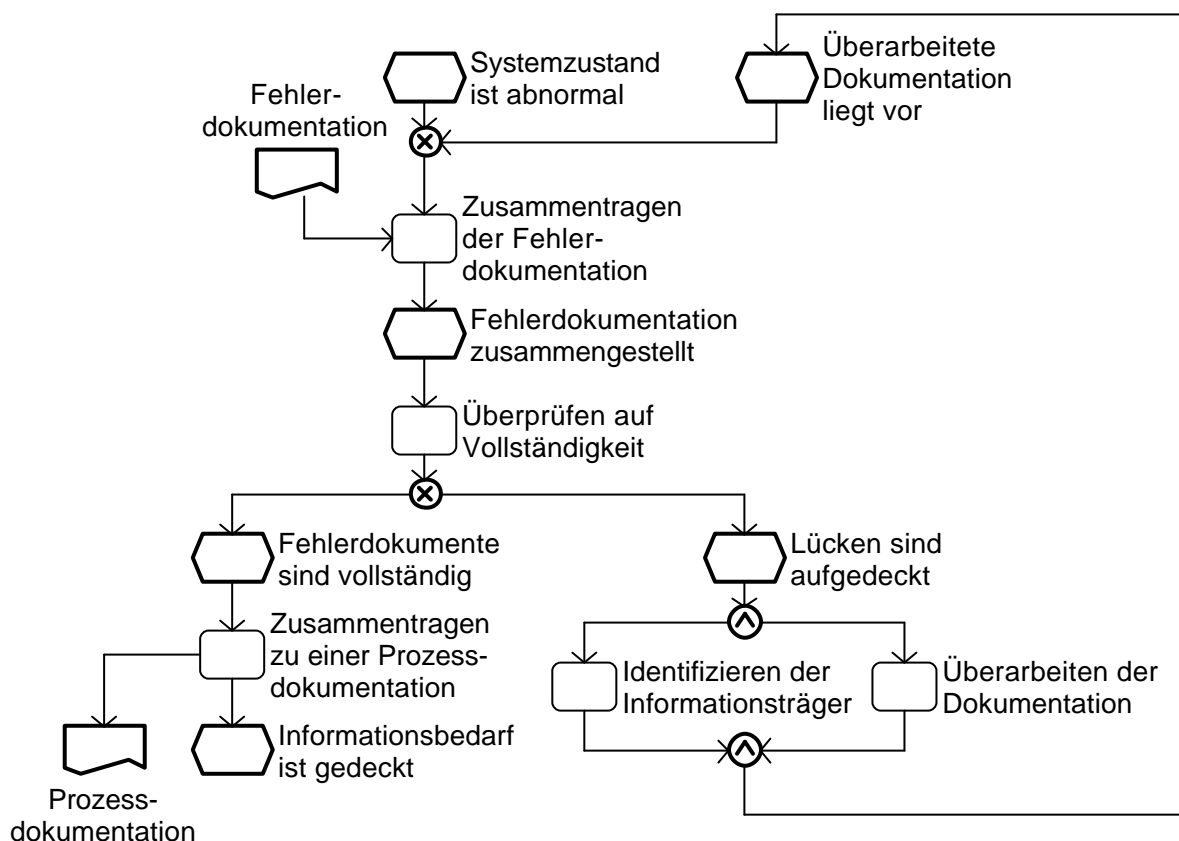


Abbildung 26: Erstellen einer Prozessdokumentation

Der Teilprozess „Erstellen einer Prozessdokumentation“ setzt sich aus einer kontinuierlichen Prozessdokumentation und Dokumentationen zu einzelnen Teilprozessen zusammen. Es ist sowohl das Vorgehen als auch die aufgetretenen Fehler und die daraus resultierten Handlungen zu dokumentieren. Hier fällt die Tätigkeiten „Erstellen einer Fehlerdokumentation“ und „Dokumentieren der Testergebnisse“ hinein. Diese einzelnen Dokumente werden zusammengetragen, danach auf Vollständigkeit überprüft und zu einer abschließenden Prozessdokumentation zusammengefügt.

Ziel dieses Prozesses ist es den kontinuierlichen Informationsbedarf zu decken. D. h. zum einen, dass einmal erarbeitete Prozessschritte mit der Dokumentation für Dritte nachvollziehbar werden und nicht erneut erarbeitet werden müssen, was die Effizienz im betrieblichen Alltag steigert. Zum anderen soll die Prozessdokumentation als Grundlage für eventuell zu erstellende Verfahrenshandbücher oder Best Practices dienen.

#### 3.2.2.9.1 Tätigkeiten: Erstellen einer Prozessdokumentation

Um eine Prozessdokumentation im Fault-Management durchführen zu können muss der IT Systems Administrator, meist parallel zu den Tätigkeiten der anderen Teilprozesse, folgende Tätigkeiten durchführen:

- Zusammentragen der Fehlerdokumentation
- Überprüfen auf Vollständigkeit

Falls die einzelnen Fehlerdokumentationen Lücken aufweisen

- Identifizieren der Informationsträger
- Überarbeiten der Dokumentation

Auf jeden Fall:

- Zusammentragen zu einer Prozessdokumentation

### **3.2.2.9.2 Kompetenzfelder: Erstellen einer Prozessdokumentation**

#### Fähigkeiten/Fertigkeiten

- (Parallel zur Ausarbeitung) den gesamten Prozess dokumentieren können
- Übertragen können von Tätigkeiten in Betriebshandbücher und Verfahrensanweisungen
- Betriebsvereinbarungen beachten können
- Sicherheitsrelevantes einschätzen und vor widerrechtlichen Zugriffen schützen können
- Informationslücken entdecken können

#### Wissen

- Standards der Dokumentation in Bezug auf das Nachvollziehen von Prozessschritten kennen
- Rechtliche Auswirkungen in Bezug auf Dokumentationslücken kennen

#### Werkzeuge

- Textverarbeitung

### **3.2.2.9.3 Beispiel: Erstellen einer Prozessdokumentation**

Während der Durchführung der Fehlerbeseitigung wird eine Fehlerdokumentation durchgeführt. Die soll zum einen die durchgeführten Tätigkeiten am RAID-System aufzeichnen und zum anderen die bisherigen Verfahrensanweisungen überprüfen.

So wurde während der Projektdurchführung festgestellt, dass bisherige Serviceverträge nicht schnell genug aufgefunden wurden und es deshalb zu unnötigen Verlängerungen der Reparaturmaßnahmen über das Wochenende hinaus kam. Des Weiteren kam es zu Schnittstellenproblemen zwischen den betroffenen Abteilungen und der Serviceabteilung des Herstellers, die maßgeblich zur Verlängerung der Reparaturmaßnahmen und somit zu zusätzlichen Kosten führten.

So wurde vereinbart, dass relevante Daten aller Serviceverträge digitalisiert gespeichert werden. Alle externen Stellen sollen ab sofort in einer Datenbank erfasst werden.



### **3.2.2.10 Informieren betroffener Personen/Stellen**

#### **3.2.2.10.1 Tätigkeiten: Informieren betroffener Stellen/Personen**

In diesem Abschnitt werden die Kommunikationsmaßnahmen als kontinuierliche, den gesamten Prozess begleitende Teilprozesse beschrieben.

Solche Ad-hoc-Kommunikationsmaßnahmen werden durchgeführt, wenn bestimmte Personen oder Stellen über den aktuellen Stand der Bearbeitung informiert werden müssen. Dazu zählen aber auch die Einweisung der Nutzer nach dem erfolgreichen durchgeführten Fehlermanagement sowie ausführlichere Nutzerschulungen zu neu installierten Systemen.

Diese Tätigkeiten werden kumuliert im Referenzprozess „Benutzerberatung und Organisation“ (siehe Abschnitt 3.6ff.) durchgeführt. In diesen fallen auch die konkrete Schulung und Einweisung in das System.

#### **3.2.2.10.2 Kompetenzfelder: Informieren betroffener Stellen/Personen**

Fähigkeiten/Fertigkeiten

- Schulungen organisieren und durchführen können (siehe Abschnitt 3.6.2.4 Einweisen der Benutzer)
- Erklären können
- Dokumentieren können

Wissen

- Je nach Informationsbedarf Kenntnisse über relevante Themen, die den Nutzer betreffen können, besitzen

Werkzeuge

- Informationsverteiler

#### **3.2.2.10.3 Beispiel: Informieren betroffener Stellen/Personen**

Bei vielen Störungen muss meist externes Personal hinzugezogen werden. Diese müssen rechtzeitig und im Rahmen von abgeschlossenen Service- oder Wartungsverträgen informiert werden. Des Weiteren müssen betroffene Stellen über die voraussichtliche Dauer der Störung (4 Stunden) informiert werden. Die Meldefrist wird in einer Serviceumfangsbeschreibung festgelegt (siehe dazu 3.6.2.2ff. Erstellen eines Vorschlag für Servicestrukturen). In diesen sind auch die internen Schnittstellen festgelegt, d. h. welche Mitarbeiter und Abteilung über eine Störung informiert werden müssen.



### 3.3 Performance-Management

---

Die Überwachung der Performance dient der Qualitätskontrolle der durch den Administrator angebotenen Leistungen, des Aufdeckens von Systemengpässen und zur Erfassung von Nutzungsdaten/Logs im Sinne des Accounting Managements.

Dieser Prozess verläuft im wesentlichen analog zum Referenzprozess „Fault-Management“ nur mit anderen Schwerpunkt. Es wird ein Aufzeichnungskonzept erstellt und umgesetzt. Im Falle eines Ereignisses, wie eine Schwellwertüberschreitung oder einer externen Meldung, werden Ort und Ursache ermittelt und eingegrenzt.

Anschließend wird das Ereignis analysiert. Handelt es sich nicht um ein temporäres, einmaliges Problem, wird ein Handlungskonzept unter der Berücksichtigung von sowohl technischen als auch wirtschaftlichen Aspekten entwickelt, um derartige Engpässe zukünftig zu vermeiden. Gegebenfalls wird unter der Zuhilfenahme des Referenzprozesses „Change-Management“ eine Systemänderung durchgeführt.

### 3.3.1 Der Referenzprozess Performance-Management

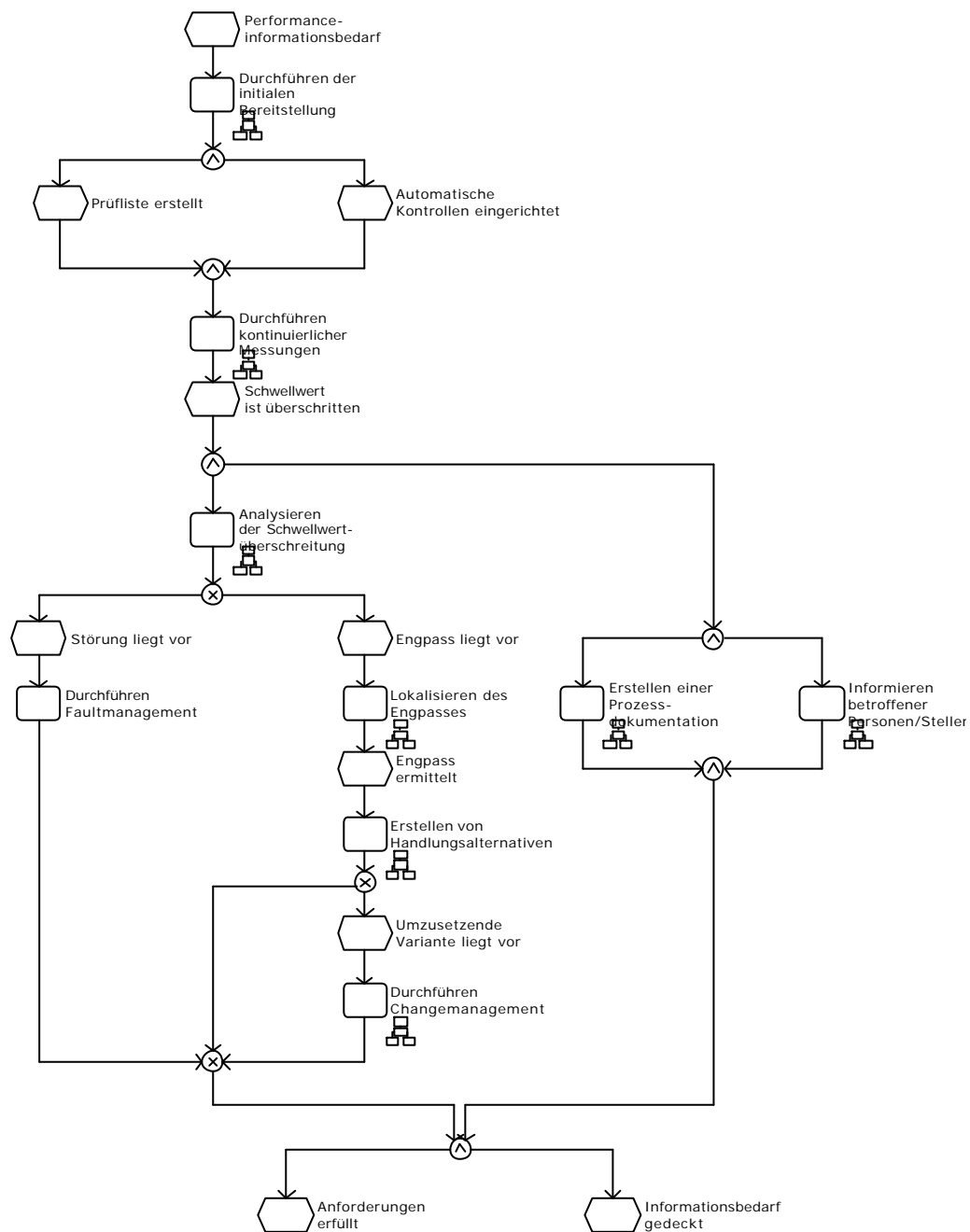


Abbildung 27: Referenzprozess Performancemanagement

### **3.3.2 Prozesskompass Performance-Management**

Zusammenfassend sind folgende Teilprozesse im Referenzprozess Performance-Management enthalten:

1. Durchführen der initialen Bereitstellung
2. Durchführen kontinuierlicher Messungen
3. Analysieren der Schwellwertüberschreitung
4. Lokalisieren des Engpasses
5. Erstellen von Handlungsalternativen
6. Durchführen Fault-Management
7. Durchführen Change-Management
8. Erstellen einer Prozessdokumentation
9. Informieren betroffener Personen/Stellen

### 3.3.2.1 Durchführen der initialen Bereitstellung

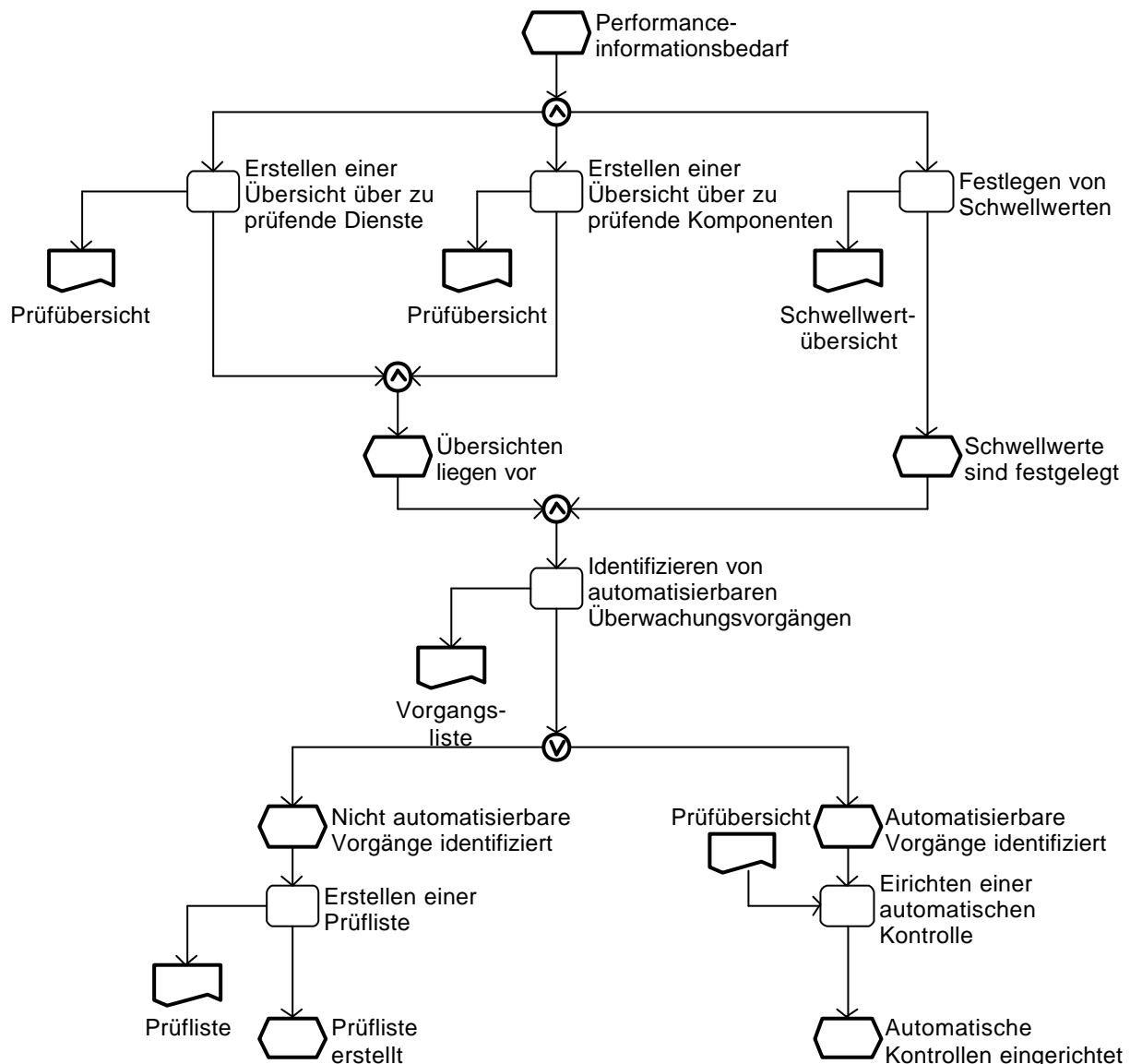


Abbildung 28: Durchführen der initialen Bereitstellung

Um ein Performance-Management durchführen zu können, muss erst einmal festgelegt werden, welche Komponenten und Dienste überwacht werden sollen und wie man eventuell den Überwachungsvorgang automatisieren kann. Außerdem müssen Schwellwerte definiert werden, deren Überschreitung eine Abnormalität des Systems signalisieren. Als Ergebnis dieses Teilprozesses erhält man eine Prüfliste und es wird eine automatische Kontrolle eingerichtet.

#### 3.3.2.1.1 Tätigkeiten: Durchführen der initialen Bereitstellung

Um die initiale Bereitstellung für das Performance-Management sicherzustellen, muss der IT Systems Administrator folgende Tätigkeiten durchführen:

- Erstellen einer Übersicht über zu prüfende Dienste
- Erstellen einer Übersicht über zu prüfende Komponenten
- Festlegen von Schwellwerten
- Identifizieren von automatisierbaren Überwachungsvorgängen
- Erstellen einer Prüfliste
- Einrichten einer automatischen Kontrolle

### 3.3.2.1.2 **Kompetenzfelder: Durchführen der initialen Bereitstellung**

#### Fähigkeiten/Fertigkeiten

- Übersichten erstellen können
- Übersichten über zu prüfende Dienste erstellen können
- Übersichten über zu prüfende Komponenten erstellen können
- Schwellwerte festlegen können
- Automatisierbare Vorgänge identifizieren können
- Prüflisten erstellen können
- Automatische Kontrollen einrichten können
- Dokumentieren können
- Service Level Agreements für das Performance-Management interpretieren können

#### Wissen

- Betriebsarten von Systemen und benutzen Hardware kennen
- Grundlegende Kenntnisse in der Netzwerktechnik und in Netzwerktopologien
- Kenntnisse von Datenübertragungssystemen und –techniken sowie der verwendeten Hardwareschnittstellen kennen
- Kenntnisse über die sich im Einsatz befindenden System- und Kommunikationsarchitekturen
- Kenntnisse über die sich im Einsatz befindenden Netzwerk- und Kommunikationsprotokollen sowie der Dienste und der verwendeten Schnittstellen zu anderen Systemen und Softwaresystemen
- Vorgehensmodelle bei der Erstellung eines Prüfverfahrens für das sich im Einsatz befindende IT-System kennen
- Kenntnisse in der Auswertung von Systemmitteilungen durch Skriptsprachen
- Kenntnisse über informationstechnische und elektrische Leistungsgrößen
- Messverfahren kennen
- Kenntnisse über die sich im Einsatz befindenden Adapter und Hardwarecontroller
- Kenntnisse im Umgang mit Fernzugriffsverfahren und –software
- Kenntnisse in der Rationalisierung von Arbeitsschritten und deren Organisation in Bezug auf das Management von Fehlerzuständen des Systems
- Kenntnisse im Umgang mit Standards der Dokumentation bei Prävention und der Erhaltung einer Performanzqualität

#### Werkzeuge

- Systemmonitore
- Betriebssystemeigene Werkzeuge
- Skripteditoren
- Diagnosesoftware
- Fernzugriffssoftware

### 3.3.2.1.3 **Beispiel: Durchführen der initialen Bereitstellung**

Hier dient ebenfalls das Beispiel aus dem Kapitel 3.1ff. Change-Management. Nachdem das System im Ganzen installiert und in Betrieb genommen wurde, müssen Vorbereitungsmaßnahmen getroffen werden, die einen fehlerfreien Betrieb gewährleisten können. Dazu müssen alle relevanten Dienste wie Mail, Replikation zwischen den Servern etc. aufgelistet werden und in eine Checkliste übernommen werden. Da es neben softwareseitigen auch zu hardwareseitigen Performanzbeeinträchtigungen kommen kann, muss auch hier eine Übersicht erstellt werden. Diese kann zum größten Teil aus dem Systemhandbuch und den einzelnen technischen Hardwarebeschreibungen entnommen werden. Für die identifizierten Dienste und Hardwarekomponenten werden Grenzwerte festgelegt. Wenn diese unter- bzw. überschritten werden, ist mit einem fehlerhaften oder nicht mehr den Anforderungen nach performanten System auszugehen.

In diesen Arbeitsschritten überlegt man sich, welche Dienste und Hardwarekomponenten lassen sich über automatische Kontrollmeldungen überwachen. Für die Hardware wird nun noch nachträglich Software installiert, die den Systemstatus dieser Komponenten überwachen kann und eventuell eine Mitteilung an den Systemadministrator senden kann. Für die Dominodienste wird das Überwachungstool eingesetzt, welches mit der Software mitgeliefert wurde. So können Mail- und Replikationsdienste automatisch überwacht werden.

Neben diesen automatisierbaren Überwachungsvorgängen lassen sich eine Reihe von nicht automatisierbaren Vorgängen identifizieren. So kann die eventuelle Nichtverfügbarkeit des externen Mailservers zum einen am Server selbst liegen, zum anderen aber auch, weil die DSL-Leitung nicht zur Verfügung steht. Diese und eine Reihe weiterer nicht durch Automatismen abfangbaren Vorgängen werden in die Checkliste aufgenommen und sollten in regelmäßigen Abständen getestet werden.

Über das Überwachungstool, welches die Mailauslastung misst und kontrolliert, wurde ein 80%-Auslastungsschwellwert eingepflegt. Wird dieser Wert länger als eine Stunde überschritten, erzeugt der entsprechende Mailserver von einem eigens dafür geschriebenen Agenten eine Warnung, die per Email an den Administrator weitergeleitet wird.



### 3.3.2.2 Durchführen kontinuierlicher Messungen

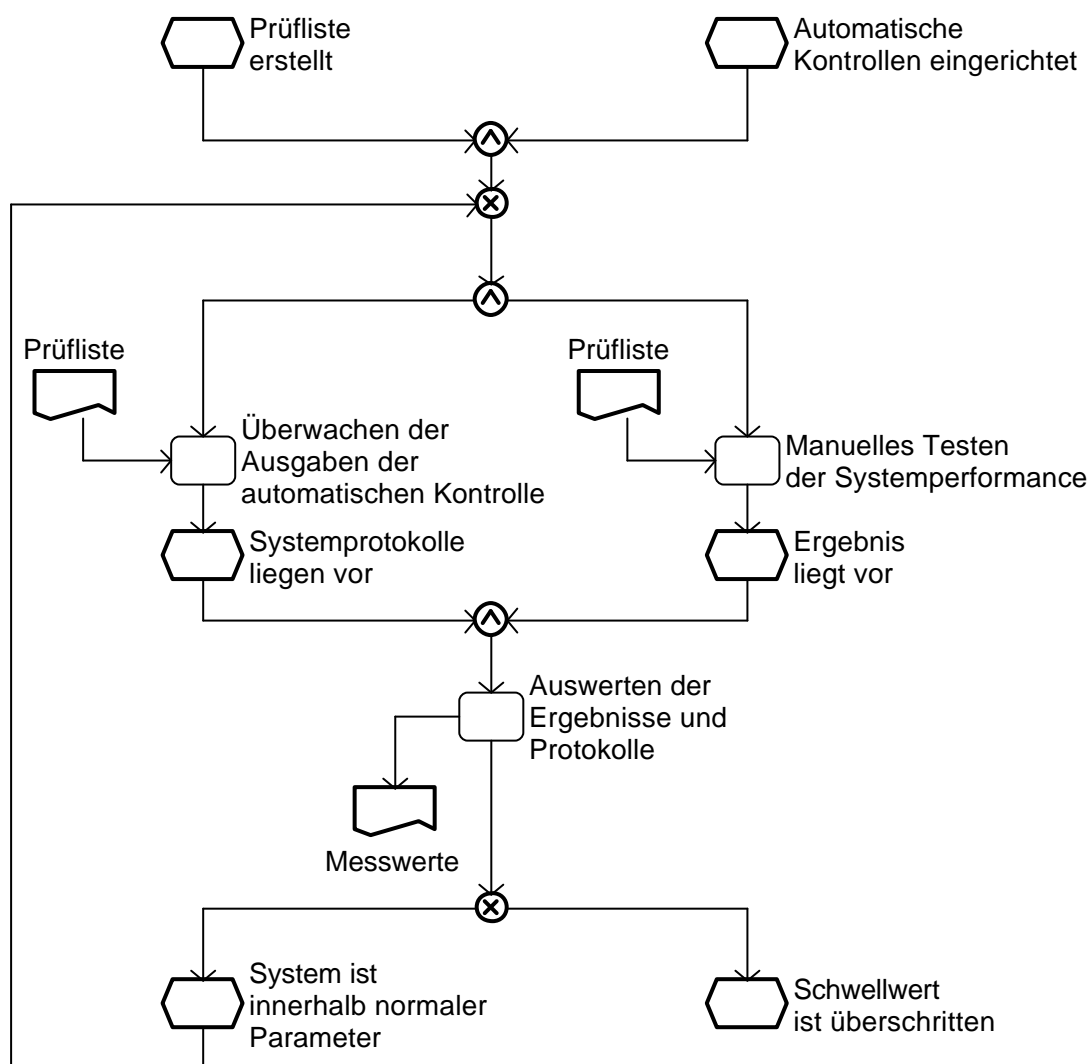


Abbildung 29: Durchführen kontinuierlicher Messungen

Liegt die Vorgehensweise der Überwachung vor, können die kontinuierlichen Überwachungen der Systemperformance beginnen. Hier werden die Ausgaben der zuvor erstellten bzw. eingerichteten automatischen Kontrolle und die allgemeine Systemperformance überwacht und ausgewertet. Tritt dabei eine Überschreitung eines vorher festgelegten Schwellwertes auf, fährt man im nächsten Schritt weiter, in dem diese Überschreitung analysiert wird. Wenn keine Überschreitung zu beobachten ist, führt man die kontinuierlichen Messungen weiter fort.

#### 3.3.2.2.1 Tätigkeiten: Durchführen kontinuierlicher Messungen

Durch folgende Tätigkeiten führt der IT Systems Administrator die kontinuierlichen Messungen durch:

- Überwachen der Ausgaben der automatischen Kontrolle
- Manuelles Testen der Systemperformance
- Auswerten der Ergebnisse und Protokolle

#### 3.3.2.2.2 Kompetenzfelder: Durchführen kontinuierlicher Messungen

Fähigkeiten/Fertigkeiten

- Ausgaben der automatischen Kontrolle auswerten können
- Ergebnisse und Protokolle interpretieren können

- Systemperformance manuell prüfen können
- Dokumentieren können

#### Wissen

- Kenntnisse und Erfahrungen bei der Auswertung von Logdateien der verwendeten Betriebssysteme und Systemsoftware
- Kenntnisse in der Auswertung von Systemmitteilungen durch Skriptsprachen
- Betriebsarten von Systemen und benutzen Hardware kennen
- Grundlegende Kenntnisse in der Netzwerktechnik und in Netzwerktopologien
- Kenntnisse von Datenübertragungssystemen und –techniken sowie der verwendeten Hardwareschnittstellen kennen
- Kenntnisse über die sich im Einsatz befindenden System- und Kommunikationsarchitekturen
- Kenntnisse über die sich im Einsatz befindenden Netzwerk- und Kommunikationsprotokollen sowie der Dienste und der verwendeten Schnittstellen zu anderen Systemen und Softwaresystemen
- Vorgehensmodelle bei der Erstellung eines Prüfverfahrens für das sich im Einsatz befindende IT-System kennen
- Kenntnisse über informationstechnische und elektrische Leistungsgrößen
- Messverfahren kennen
- Kenntnisse über die sich im Einsatz befindenden Adapter und Hardwarecontroller
- Kenntnisse im Umgang mit Fernzugriffsverfahren und –software
- Kenntnisse in der Rationalisierung von Arbeitsschritten und deren Organisation in Bezug auf das Management von Fehlerzuständen des Systems
- Kenntnisse im Umgang mit Standards der Dokumentation bei Prävention und der Erhaltung einer Performanzqualität

#### Werkzeuge

- Fernzugriffssoftware
- Systemmonitore
- Skripteditoren
- Diagnosesoftware
- Betriebssystemeigene Werkzeuge

#### **3.3.2.2.3 Beispiel: Durchführen kontinuierlicher Überwachung**

Während des Betriebs der Dominoserver werden ständig die Auslastungsstatistiken überprüft, die Checklisten regelmäßig durchgegangen, um so im Vorfeld bereits auftretende Engpässe zu identifizieren. Eventuell werden neue Dienste und Komponenten in die Checkliste aufgenommen, die entweder über automatische Kontrollen oder manuell überprüft werden müssen.

### 3.3.2.3 Analysieren der Schwellwertüberschreitung

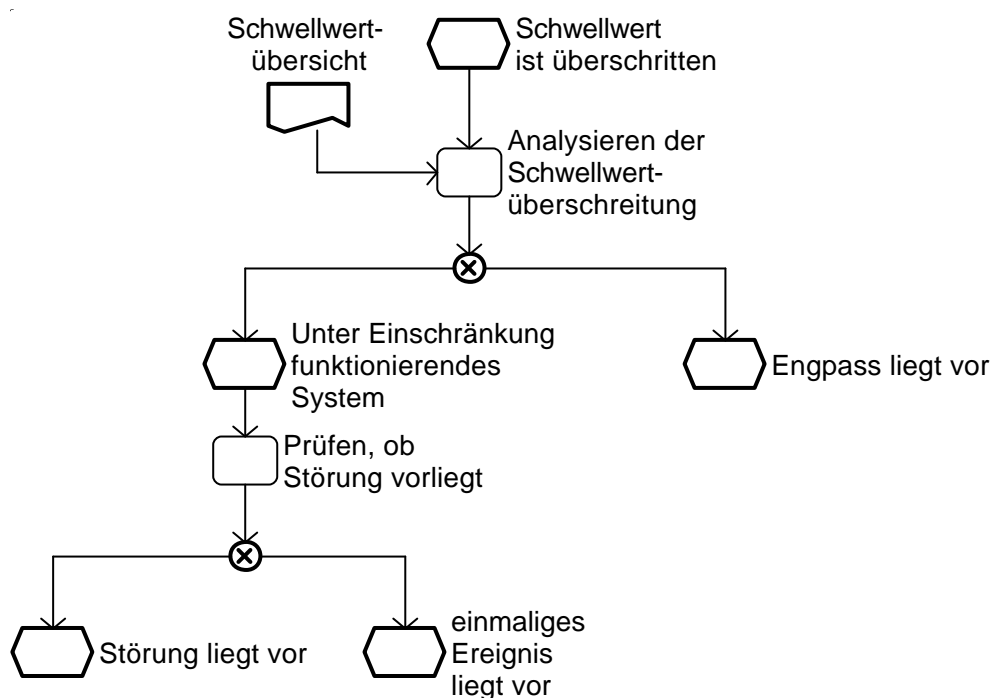


Abbildung 30: Analysieren der Schwellwertüberschreitung

Ergibt die kontinuierliche Überwachung, dass ein oder mehrere Schwellwerte überschritten sind, kann eine genauere Information über den Grund für die Schwellwertüberschreitung notwendig sein. Dazu ist zu prüfen, ob ein Ausfall oder Absturz vorliegt oder nicht. Liegt ein Ausfall/Absturz vor, ist zu prüfen, ob die Störung reproduzierbar ist. Wenn dem so ist, wird der Fault-Managementprozess (siehe 3.2ff.) durchgeführt, andernfalls handelt es sich um ein einmaliges Ereignis und es sind keine Handlungen notwendig. Hat die Analyse der Überschreitung ergeben, dass gar keine Störung vorliegt, handelt es sich tatsächlich um einen Engpass.

#### 3.3.2.3.1 Tätigkeiten: Analysieren der Schwellwerte

Der IT Systems Administrator muss bei der Analyse einer Schwellwertüberschreitung folgende Tätigkeiten durchführen:

- Analysieren der Schwellwertüberschreitung
- Prüfen, ob Störung vorliegt.

#### 3.3.2.3.2 Kompetenzfelder: Analysieren der Schwellwerte

Fähigkeiten/Fertigkeiten

- Schwellwertüberschreitungen analysieren können
- Auf Reproduzierbarkeit einer Störung prüfen können
- Ganzheitliche Sichtweise über das System besitzen
- Dokumentieren können

Wissen

- Kenntnisse und Erfahrungen bei der Auswertung von Logdateien der verwendeten Betriebssysteme und Systemsoftware
- Kenntnisse über auftretende Schwellwerte der benutzten Hard- und Software
- Kenntnisse im Umgang mit Systemmanagementsysteme
- Kenntnisse in Standards der Dokumentation in Bezug auf die Nachvollziehbarkeit der potentiellen Schwellwertüberschreitung

Werkzeuge

- Betriebsinterne Informationssysteme
- Systemmonitore
- Betriebssystemeigene Werkzeuge

#### **3.3.2.3.3 Beispiel: Analysieren der Schwellwertüberschreitung**

Der Agent versendet eine Email, die eine Überlastung des Mailservers des zentralen Domino-servers anzeigt. Da es sich mittlerweile um die dritte Email handelt (jede Stunde wird eine solche Überlastungsmeldung vom Agenten versendet), kann von einem einmaligen Ereignis abgesehen werden. Weitere Beobachtungen des Email-Verkehr zeigt an, dass der Zustand sich seit einiger Zeit nur knapp unterhalb des definierten Schwellwertes befand und nun weiter ansteigt. Es wird prognostiziert, dass es in spätestens zwei Wochen zu Zustellungsengpässen von Emails kommen kann. Dies wird dem Vorgesetzten gemeldet. In diesem Gespräch erfährt der Administrator, dass es aufgrund eines neuen langfristigen Projektes auch in der Zukunft zu einem immer stärker ansteigenden Verkehr kommen wird, weil größere Daten mit den externen Projektpartnern ausgetauscht werden müssen.

### 3.3.2.4 Lokalisieren des Engpasses

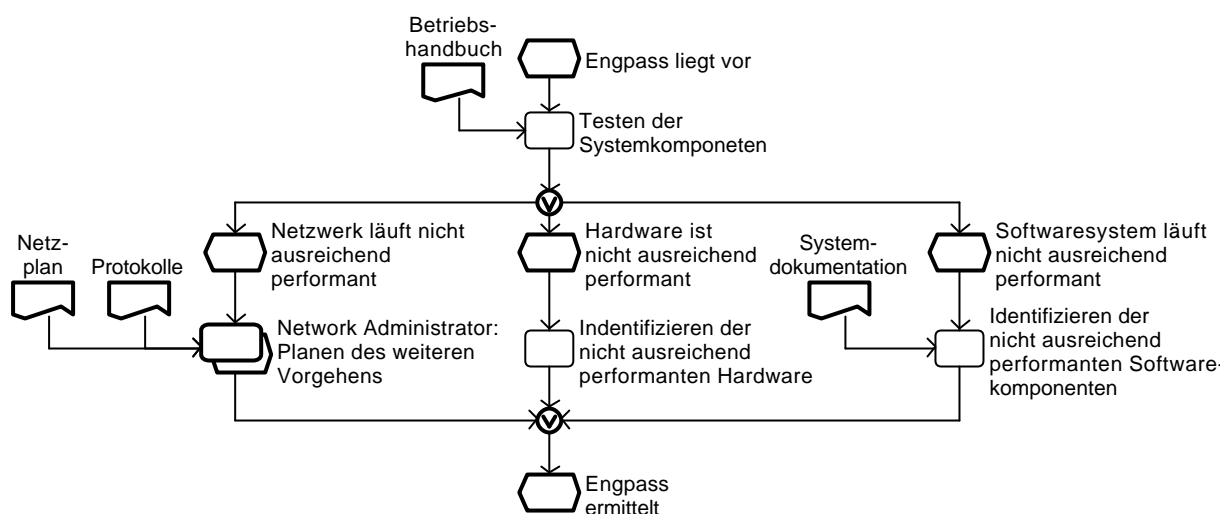


Abbildung 31: Lokalisieren des Engpasses

Wurde ein Engpass erkannt, werden die Systemkomponenten getestet. So wird festgestellt, ob es sich bei der nicht ausreichend performanten Komponente um eine Hardware- oder Softwarekomponente handelt. Handelt es sich jedoch um eine Netzwerkkomponente, muss zusammen mit dem Network Administrator das weitere Vorgehen besprochen werden. Im Ergebnis liegt der Ort des Engpasses vor.

#### 3.3.2.4.1 Tätigkeiten: Lokalisieren des Engpasses

Durch folgende Tätigkeiten lokalisiert der IT Systems Administrator den Engpass:

- Testen der Systemkomponenten

Falls Softwarekomponenten nicht ausreichend performant sind:

- Identifizieren der nicht ausreichend performanten Softwarekomponenten

Falls Hardware nicht ausreichend performant ist:

- Identifizieren der nicht ausreichend performanten Hardware

Falls das Netzwerk nicht ausreichend performant läuft:

- Zusammen mit dem Network Administrator: Planen des Weiteren Vorgehens

#### 3.3.2.4.2 Kompetenzfelder: Lokalisieren des Engpasses

Fähigkeiten/Fertigkeiten

- Systemkomponenten hinsichtlich ihrer Performanz testen können
- Nicht ausreichend performante Teilstücke diagnostizieren können
- Netzwerkkomponenten hinsichtlich ihrer Performanz prüfen können
- Nicht ausreichend performante Hardwarekomponenten identifizieren können
- Nicht ausreichend performante Softwarekomponenten identifizieren können
- Vorgänge koordinieren können
- Dienste und deren Abhängigkeiten kennen
- Dokumentieren können

Wissen

- Erfahrungen bei Engpassbestimmung des Systems und Kenntnisse über deren Zusammenhänge besitzen
- Betriebsarten von Systemen und benutzer Hardware kennen
- Kenntnisse von Datenübertragungssystemen und -techniken sowie der verwendeten Hardwareschnittstellen
- Kenntnisse über die sich im Einsatz befindenden System- und Kommunikationsarchitekturen

- Kenntnisse über die sich im Einsatz befindenden Netzwerk- und Kommunikationsprotokollen sowie der Dienste und der verwendeten Schnittstellen zu anderen Systemen und Softwaresystemen
- Messverfahren kennen
- Kenntnisse über die sich im Einsatz befindenden Adapter und Hardwarecontroller
- Kenntnisse im Umgang mit Fernzugriffsverfahren und –software
- Kenntnisse in der Rationalisierung von Arbeitsschritten und deren Organisation in Bezug auf das Management von Fehlerzuständen des Systems
- Kenntnisse im Umgang mit Standards der Dokumentation bei der Ermittlung des Engpasses

Werkzeuge

- Datenbanken
- Informationsquellen

#### **3.3.2.4.3 Beispiel: Lokalisieren des Engpasses**

Nachdem die verfügbaren Herstellerdokumentationen studiert wurden, stellt sich heraus, dass der zentrale Server in der derzeitigen Ausstattung den zu erwartenden Mailverkehr nicht hinreichend unterstützen kann. Dieser Server ist der einzige, der die Emails nach außen leitet und nach innen auf die entsprechenden Mailserver mit ihren Postfächern verteilt. Bei den beiden Mailservern, in denen ebenfalls ein Schwellwert von 80% festgelegt wurde, ist zur Zeit nur eine Auslastung von durchschnittlich 40-50% gegeben und diese wird sich aufgrund des Projektes auch nicht in der Nähe von 80% bewegen.

### 3.3.2.5 Erstellen von Handlungsalternativen

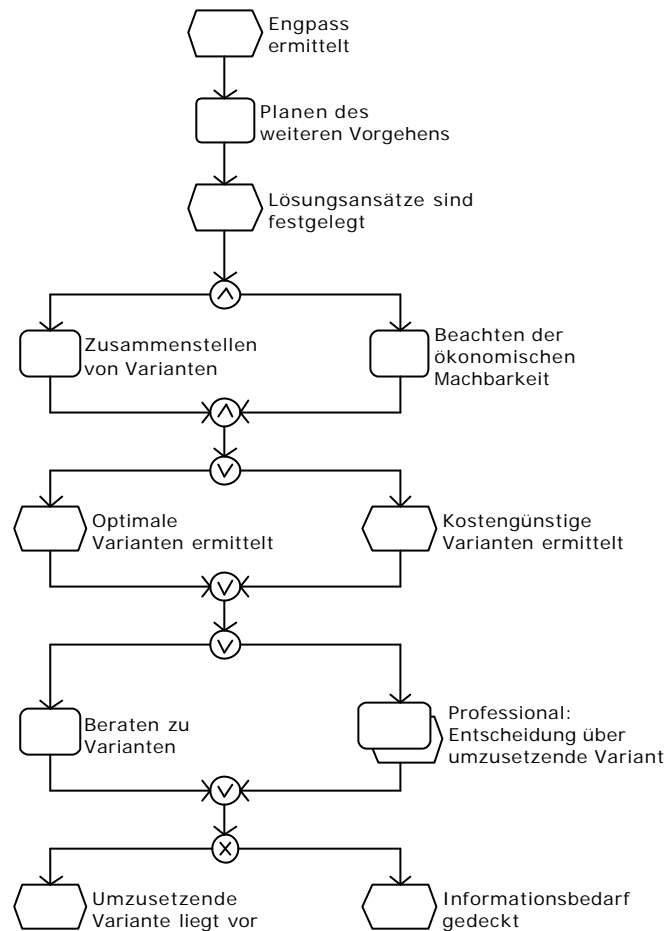


Abbildung 32: Erstellen von Handlungsalternativen

Ist der Ort des Engpasses erst einmal ermittelt, muss das weitere Vorgehen geplant werden. Im Ergebnis werden Lösungswege festgelegt. Diesem folgen ein Variantenvergleich unter der Beachtung der ökonomischen Machbarkeit. Hier wird zwischen den kostengünstigen und den wirksamen optimalen Varianten unterschieden. Sind diese bestimmt, erfolgt (sofern nötig) die Abstimmung mit dem Entscheidungsträger. Entschieden wird, welche Variante durchgeführt wird, bzw. ob überhaupt etwas an der bisherigen Situation geändert werden muss, wenn das System im Prinzip weiterhin funktionsfähig ist.

#### 3.3.2.5.1 Tätigkeiten: Erstellen von Handlungsalternativen

Für die Erstellung von Handlungsalternativen muss der IT Systems Administrator folgende Tätigkeiten durchführen:

- Planen des Weiteren Vorgehens
- Zusammenstellen von Varianten
- Beachten der ökonomischen Machbarkeit
- Beraten zu Varianten

Falls notwendig:

- Professional: Entscheidung über umzusetzende Variante

Falls etwas an der derzeitigen Situation geändert werden soll und die Entscheidung vom Professional vorliegt:

- Durchführen Change-Management

### **3.3.2.5.2 Kompetenzfelder: Erstellen von Handlungsalternativen**

#### Fähigkeiten/Fertigkeiten

- Planen können
- Zukünftige Anforderungen abschätzen können
- Varianten zusammenstellen können
- Ökonomische Machbarkeit beachten können
- Wirtschaftlichkeitsbetrachtungen durchführen können
- Zwischen kostengünstigen und wirksamen Varianten differenzieren können
- Varianten vergleichen können
- Kompetenzen zu anderen Organisationseinheiten kennen
- Change-Management durchführen können
- Dokumentieren können

#### Wissen

- Kenntnisse über die sich im Einsatz befindenden System- und Kommunikationsarchitekturen
- Kenntnisse der Funktionsweise der sich im Einsatz befindenden Betriebssysteme, Softwarekomponenten und Dienste sowie deren Beziehung zueinander
- Kenntnisse in der Erstellung von Kosten- und Nutzenvergleiche
- Kenntnisse im Umgang mit Standards der Dokumentation in Bezug auf die Erstellung eines Anforderungskatalogs für die Durchführung eines Change-Managementprozesses

#### Werkzeuge

- Kaufmännische Software

### **3.3.2.5.3 Beispiel: Erstellen von Handlungsalternativen**

Dem Administrator stehen nun eine Reihe von Alternativen zur Verfügung. So kann zunächst überlegt werden, ob der Server mit weiterer Hardware ausgestattet werden soll. Nun ist es zum Beispiel möglich, dass jeder Mailserver seine Emails, die er nach außen sendet auch gleich von sich aus tut und sie nicht erst zum zentralen Server versendet. Eine weitere Möglichkeit ist, dass man einen weiteren Durchgangsserver aufsetzt und schon bevor die Mailserver die Mail versenden, klar ist, zu welchem Server sie die entsprechende Mail senden sollen. Eine andere Möglichkeit ist, dass man ein Cluster aufbaut und so ein Lastenausgleich zwischen den einzelnen Servern erreicht.

Für diese Alternativen werden jeweils Entscheidungsdokumente für den Vorgesetzten erstellt, die neben der Kostenaufstellung, einer Empfehlung auch einen Umsetzungsplan mit den zu erwartenden Kosten für die Soft- und Hardware, als auch für das für die Umsetzung benötigte Personal und ein Zeitplan für die Umsetzung enthalten. Dabei stellt sich heraus, dass die Variante „Hardwareaufrüstung“ die kostengünstigste Variante ist. Diese jedoch nur temporär das Performanceproblem beheben würde. Die „Cluster“-Lösung stellt sich als die nachhaltigste Lösung dar. Alle Alternativen werden in einer Präsentation zusammengetragen und dem Vorgesetzten vorgestellt. Der Vorgesetzte weist den Administrator an, die „Cluster“-Lösung umzusetzen. Dies lässt einen neuen Change-Managementprozess starten.



#### **3.3.2.6 Durchführen Fault-Management**

Wurde kein Engpass sondern eine Störung identifiziert, muss der IT Systems Administrator diese beheben. Er bedient sich in diesem Fall dem Fault-Management (siehe Abschnitt 3.2ff.).

#### **3.3.2.7 Durchführen Change-Management**

Wurde vom Entscheider eine umzusetzende Variante festgelegt, muss der IT Systems Administrator diese ggf. ausführen. Er bedient sich in diesem Fall des Change-Management (siehe Abschnitt 3.1ff.).

### **3.3.2.8 Erstellen einer Prozessdokumentation**

#### **3.3.2.8.1 Tätigkeiten: Erstellen einer Prozessdokumentation**

Der Teilprozess „Erstellen einer Prozessdokumentation“ setzt sich aus einer kontinuierlichen Prozessdokumentation und Dokumentationen zu einzelnen Teilprozessen zusammen. Hier sollen alle aufgetretenen Engpässe für eine spätere Auswertung erfasst werden, die für die Modifikation und Neufestlegung von Schwellwerten dienen kann.

Da diese Arbeit parallel und eng verknüpft mit dem Gesamtprozess des Performance-Managements verläuft und oben verbal beschrieben ist, was der Inhalt dieser Prozessdokumentation ist, bedarf es hier keiner Prozessabbildung.

#### **3.3.2.8.2 Kompetenzfelder: Erstellen einer Prozessdokumentation**

Fähigkeiten/Fertigkeiten

- Dokumentieren können

Wissen

- Standards der Dokumentation in Bezug auf das Nachvollziehen von Prozessschritten kennen
- Rechtliche Auswirkungen in Bezug auf Dokumentationslücken kennen

Werkzeuge

- Textverarbeitung

#### **3.3.2.8.3 Beispiel: Erstellen einer Prozessdokumentation**

Die anfallenden Messergebnisse, die zusammengetragenen Alternativen und eine Voraussage über die zukünftige Entwicklung der Performanz des zentralen Servers müssen in solch einer Form zusammengefasst werden, dass es für den Vorgesetzten als Entscheidungsgrundlage dienen kann. Dabei müssen die Informationen komprimiert und auf das Wesentliche reduziert werden. Eventuell müssen weitere Informationen recherchiert werden, um derzeit nicht vorhandene Informationen, wie Grenzwerte der Auslastung des Mailservers zu erfahren.

### **3.3.2.9 Informieren betroffener Personen/Stellen**

#### **3.3.2.9.1 Tätigkeiten: Informieren betroffener Stellen/Personen**

In diesem Abschnitt werden die Kommunikationsmaßnahmen als kontinuierliche, den gesamten Prozess begleitende Teilprozesse beschrieben.

Solche Ad-hoc-Kommunikationsmaßnahmen werden durchgeführt, wenn bestimmte Personen oder Stellen über den aktuellen Stand der Bearbeitung informiert werden müssen. Dazu zählen aber auch die Einweisung der Nutzer nach dem erfolgreich durchgeführten Performance-Management sowie ausführlichere Nutzerschulungen zu neu installierten Systemen.

Diese Tätigkeiten werden kumuliert im Referenzprozess „Benutzerberatung und Organisation“ (siehe Abschnitt 3.6ff.) durchgeführt. In diesem fallen auch die konkrete Schulung und Einweisung in das System.

#### **3.3.2.9.2 Kompetenzfelder: Informieren betroffener Stellen/Personen**

Fähigkeiten/Fertigkeiten

- Schulungen organisieren und durchführen können (siehe Abschnitt 3.6.2.4 Einweisen der Benutzer)
- Erklären können
- Dokumentieren können

Wissen

- Je nach Informationsbedarf Kenntnisse über relevante Themen, die den Nutzer betreffen können, besitzen

Werkzeuge

- Informationsverteiler

#### **3.3.2.9.3 Beispiel: Informieren betroffener Stellen/Personen**

Nachdem die Performanzprobleme entdeckt wurden, müssen die betroffenen Personen oder die Abteilungen in Kenntnis gesetzt werden. Dies führt zu einem transparenten Service. Des Weiteren müssen im Rahmen der eigenen Verantwortung Präventivmaßnahmen getroffen werden. Falls die notwendigen Handlungen und Veränderungen am IT-System nicht ausreichen, muss mit dem Vorgesetzten das Gespräch gesucht werden. Je nach dem Ausmaß des Problems müssen weitere Gespräche zum Beispiel mit dem Network Administrator geführt werden, um so zum einen den Problembereich abstecken zu können und zum anderen dem Vorgesetzten die wichtigen Informationen zukommen zu lassen.



### **3.4 Security-Management**

---

IT Systems Administrator setzen die Sicherheitskonzepte des IT Security Coordinator im praktischen Betrieb um, wobei sie auf der einen Seite für die physische Sicherheit wie Zutrittsbeschränkungen zu Servern, Klimatisierung, Pufferung der Energieversorgung, auf der anderen Seite für die Datenintegrität und –vertraulichkeit verantwortlich sind.

So sorgen die IT Systems Administrator, meist zusammen mit dem Network Administrator, während des Betriebs für das Schließen bekannt gewordener Sicherheitslöcher, erkennen Angriffe von außen und von innen und reagieren angemessen darauf. Dabei sorgen sie gegebenenfalls für die rechtliche Beweissicherung. Dies geschieht in Abstimmung mit dem IT Security Coordinator.

### 3.4.1 Der Referenzprozess Security-Management

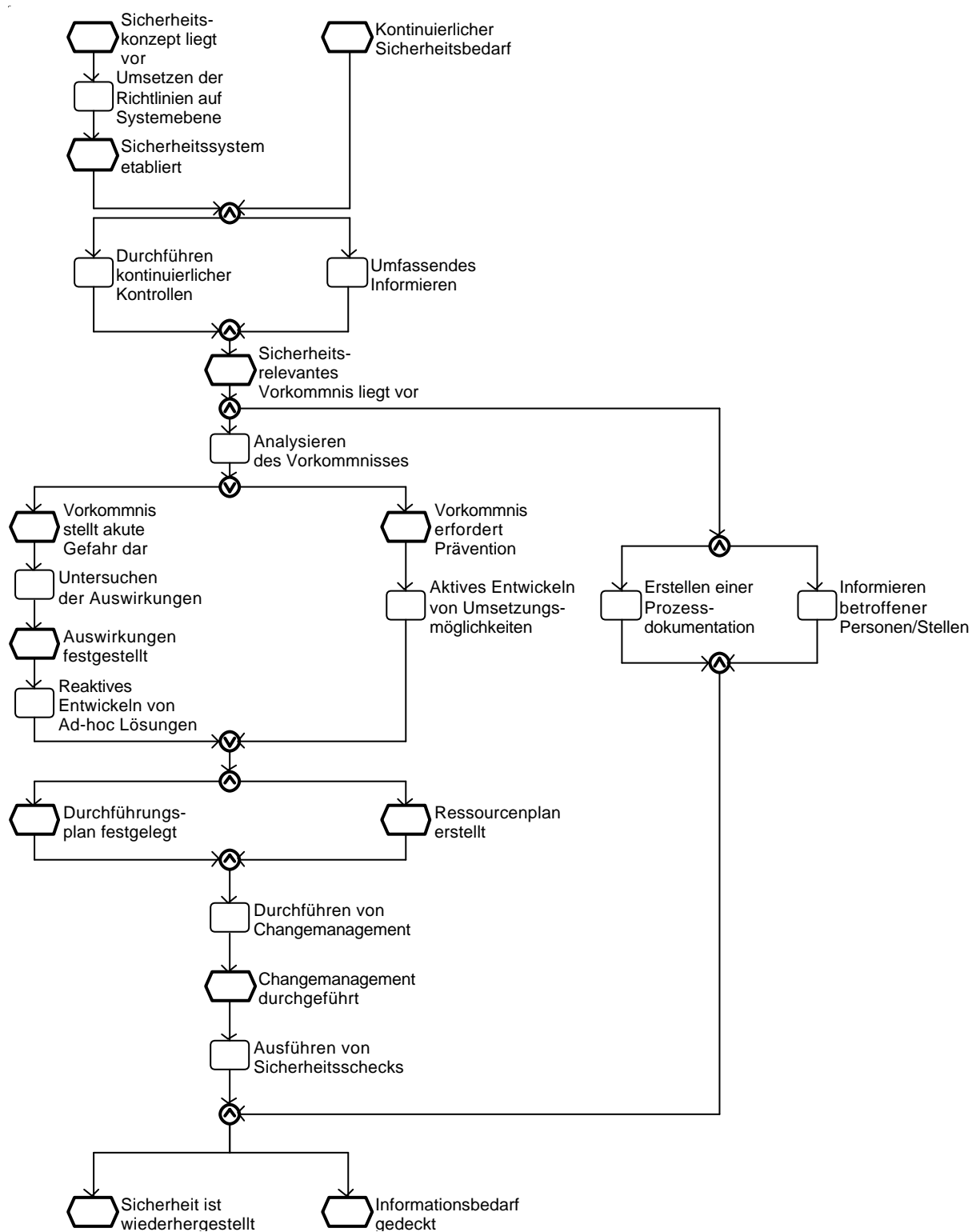


Abbildung 33: Referenzprozess Security-Management

### **3.4.2 Prozesskompass Security-Management**

Zusammenfassend sind folgende Teilprozesse im Referenzprozess Security-Management enthalten:

1. Umsetzen der Richtlinien auf Systemebene
2. Durchführen kontinuierlicher Kontrollen
3. Umfassendes Informieren
4. Analysieren des Vorkommnisses
5. Untersuchen der Auswirkungen
6. Reaktives Entwickeln von Ad-hoc-Lösungen
7. Aktives Entwickeln von Umsetzungsmöglichkeiten
8. Durchführen Change-Management
9. Ausführen von Sicherheitsschecks
10. Erstellen einer Prozessdokumentation
11. Informieren betroffener Personen/Stellen



### 3.4.2.1 Umsetzen der Richtlinien auf Systemebene

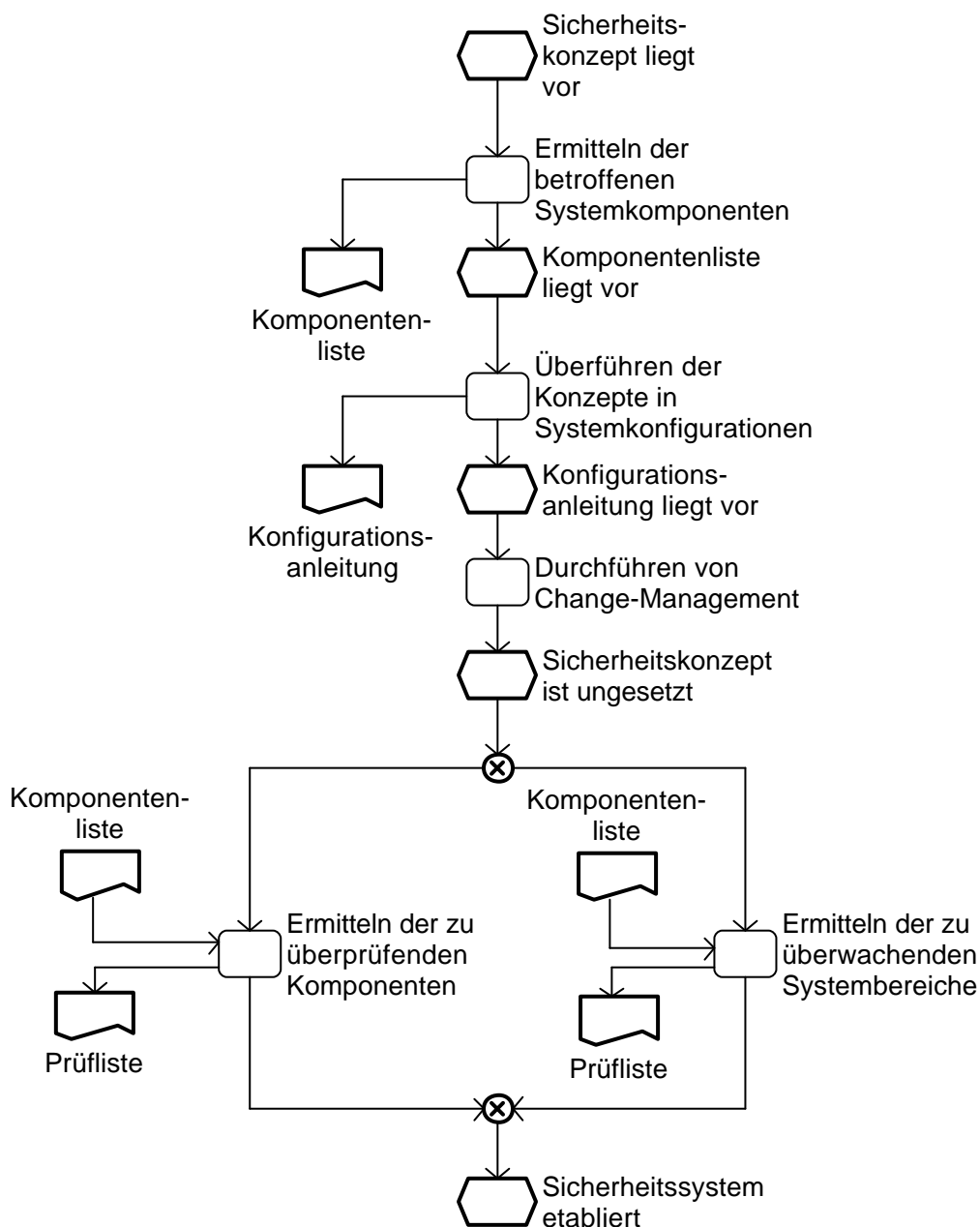


Abbildung 34: Umsetzen der Richtlinien auf Systemebene

Eine jede Organisation stellt Richtlinien auf, die den Umgang mit sicherheitsrelevanten Daten und Objekten regeln. Diese Richtlinien müssen auf Systemebene umgesetzt werden. Dazu müssen betroffene Systemkomponenten ermittelt werden und für diese Komponenten eine entsprechende Konfiguration aus dem allgemeinen Sicherheitskonzept abgeleitet werden. Um das umzusetzen, bedient sich der IT Systems Administrator des Change-Managements. Somit ist das Sicherheitskonzept umgesetzt. Im Anschluss daran werden zu überprüfende Komponenten und zu überwachende Systembereiche identifiziert. Ist dies geschehen, ist das Sicherheitssystem etabliert.

#### 3.4.2.1.1 Tätigkeiten: Umsetzen der Richtlinien auf Systemebene

Um die geforderten Richtlinien auf die Systemebene umzusetzen, führt der IT Systems Administrator folgende Tätigkeiten durch:

- Ermitteln der betroffenen Systemkomponenten
- Überführen der Konzepte in Systemkonfigurationen
- Durchführen Change-Management

- Ermitteln der zu überprüfenden Komponenten
- Ermitteln der zu überwachenden Systembereiche

### **3.4.2.1.2 Kompetenzfelder: Umsetzen der Richtlinien auf Systemebene**

#### Fähigkeiten/Fertigkeiten

- Betroffene Systemkomponenten ermitteln können
- Konzepte in konkrete Konfigurationen überführen können
- Change-Management ausführen können
- Zu überprüfende Komponenten ermitteln können
- Zu überwachende Systembereiche ermitteln können
- Dokumentieren können

#### Wissen

- Betriebsarten von Systemen und benutzer Hardware kennen
- Grundlegende Kenntnisse in der Netzwerktechnik und in Netzwerktopologien
- Kenntnisse von Datenübertragungssystemen und –techniken sowie der verwendeten Hardwareschnittstellen kennen
- Kenntnisse über die sich im Einsatz befindenden System- und Kommunikationsarchitekturen
- Kenntnisse über die sich im Einsatz befindenden Netzwerk- und Kommunikationsprotokollen sowie der Dienste und der verwendeten Schnittstellen zu anderen Systemen und Softwaresystemen
- Methoden bei der Erstellung eines Sicherheitsmodells für das sich im Einsatz befindende IT-Systeme
- Kenntnisse der Funktionsweise von Scanner und Sniffer
- Kenntnisse der Funktionsweise und der Chancen und Risiken von Firewalls und Proxys
- Kenntnisse der Funktionsweise von Würmern, Viren, Trojanern und Hybriden
- Kenntnisse der Funktionsweise gängiger Hacking Software
- Kenntnisse im Umgang mit Fernzugriffsverfahren und –software
- Kenntnisse in der Rationalisierung von Arbeitsschritten und deren Organisation in Bezug auf das Management von Systemsicherheit
- Kenntnisse im Umgang mit Standards der Dokumentation bei Prävention von Sicherheitsvorfällen und der Erstellung von Anforderungen für das zu erfolgende Change-Management

#### Werkzeuge

- Betriebssystemeigene Werkzeuge

### **3.4.2.1.3 Beispiel: Umsetzen der Richtlinien auf Systemebene**

In der Firma werden alle Webaufrufe mit dynamischen Inhalten und Datenbankanbindungen über den Applikationsserver (siehe Beispiel aus Kapitel 3.1ff. Change-Management) gehostet. Wenn dieser Server ausfallen oder für eine Weile nicht erreichbar sein sollte, wird nach Aussagen der Geschäftsleitung ein beträchtlicher Schaden entstehen, da auch hier der gesamte Shopaufruf der Firma gehostet ist. Aus diesem Grund muss der Server ausfallsicher gemacht werden und eine hinreichende Internetsicherheit gewährleisten.

Zunächst werden die betroffenen Server identifiziert. Da sowohl der zentrale Servercluster, der Applikationsserver als auch die beiden Mailserver direkt Zugang zum Internet haben, besteht hier ein hohes Risiko, dass diese Opfer eines Angriffes von Außen werden können. Nach innen ist der Zugriff auf die Server über eine Zugriffskontrollliste beschränkt. Die Server selbst stehen in einem angeschlossenen Raum und können nur über eine Tür mit PIN erreicht werden. Vom Systemadministrator wird vorgeschlagen, alle Server durch eine Firewall zu sichern und so eine DMZ (Demilitarisierte Zone) zu schaffen. Des Weiteren wird empfohlen, die Webpräsenz auf einen separaten Server zu hosten und diesen über einen kontrollierten Zugang (Replikation) durch die Firewall mit dem Applikationsserver zu verbinden. Zusätzlich sollte ein Paketfilter auf der Firewall eingerichtet. Dies wird der Geschäftsleitung präsentiert, welche danach auch die Umsetzung dieses Konzeptes beschließt. Nachdem der neue Server installiert und konfiguriert wurde (inklusive der herstellerspezifischen Sicherheitsupdates) und ein ausgiebiger Test durchgeführt wurde werden IDSs (Intrusion

Detection System) installiert. Diese dienen neben der hostbasierten auch der netzwerkba-  
sierten Überwachung.

### 3.4.2.2 Durchführen kontinuierlicher Kontrollen

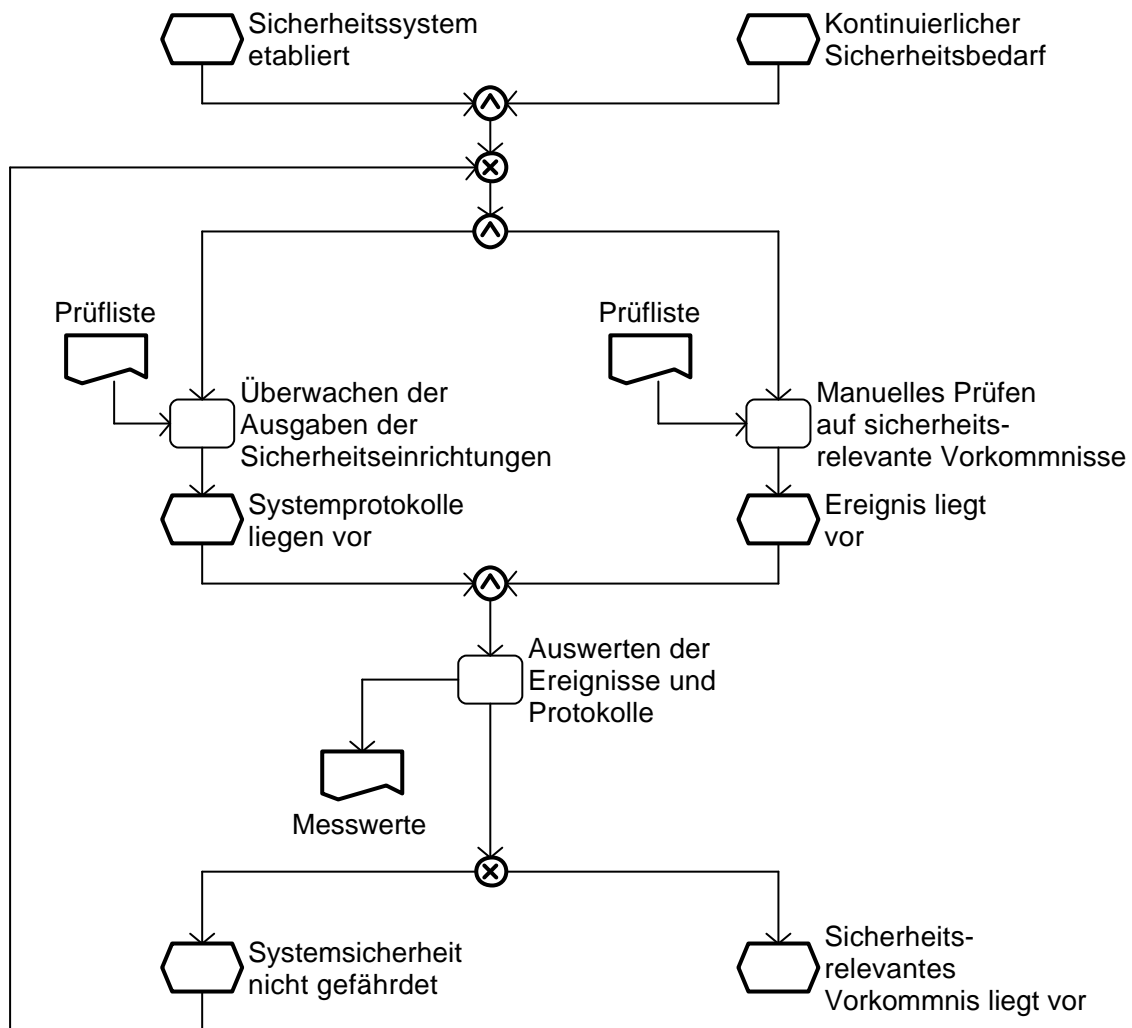


Abbildung 35: Durchführen kontinuierlicher Kontrollen

Verfügt man über ein Sicherheitssystem, hat Komponenten (Hard- und Software) und Systembereiche (Unternehmens- und Benutzerdaten) identifiziert und liegt ein Bedarf an Systemsicherheit vor, kann man eine kontinuierliche Kontrolle des Systems anstreben. Dazu überwacht der IT Systems Administrator die Ausgaben der Sicherheitseinrichtungen bzw. prüft manuell auf ungewöhnliche Vorkommnisse. Die Ergebnisse und Protokolle der Prüfung bzw. der Ausgabe werden dann ausgewertet und auf ihre Relevanz hin geprüft. Diese Überprüfung ergibt, ob es sich um ein sicherheitsrelevantes Vorkommnis handelt oder nicht.

#### 3.4.2.2.1 Tätigkeiten: Durchführen kontinuierlicher Kontrollen

Folgende Tätigkeiten muss der IT Systems Administrator durchführen, um kontinuierliche Kontrollen durchzuführen:

- Überwachen der Ausgaben der Sicherheitseinrichtungen
- Manuelles Prüfen auf sicherheitsrelevante Vorkommnisse
- Auswerten der Ergebnisse und Protokolle

#### 3.4.2.2.2 Kompetenzfelder: Durchführen kontinuierlicher Kontrollen

Fähigkeiten/Fertigkeiten

- Auf ungewöhnliche Vorkommnisse (manuell) prüfen können
- Ausgaben der Sicherheitseinrichtung überwachen können
- Ergebnisse und Protokolle auswerten und interpretieren können

- Dokumentieren können

#### Wissen

- Betriebsarten von Systemen und benutzter Hardware kennen
- Grundlegende Kenntnisse in der Netzwerktechnik und in Netzwerktopologien
- Kenntnisse von Datenübertragungssystemen und –techniken sowie der verwendeten Hardwareschnittstellen kennen
- Kenntnisse über die sich im Einsatz befindenden System- und Kommunikationsarchitekturen
- Kenntnisse über die sich im Einsatz befindenden Netzwerk- und Kommunikationsprotokollen sowie der Dienste und der verwendeten Schnittstellen zu anderen Systemen und Softwaresystemen
- Kenntnisse der Funktionsweise von Scanner und Sniffer
- Kenntnisse der Funktionsweise und der Chancen und Risiken von Firewalls und Proxys
- Kenntnisse der Funktionsweise von Würmern, Viren, Trojanern und Hybriden
- Kenntnisse der Funktionsweise gängiger Hacking Software
- Kenntnisse im Umgang mit Fernzugriffsverfahren und –software
- Kenntnisse in der Rationalisierung von Arbeitsschritten und deren Organisation in Bezug auf das Management von Systemsicherheit
- Kenntnisse im Umgang mit Standards der Dokumentation bei Prävention von Sicherheitsvorkommnissen

#### Werkzeuge

- Betriebssystemeigene Werkzeuge
- Fernzugriffssoftware
- Diagnosesoftware
- Sicherheitssoftware

#### **3.4.2.2.3 Beispiel: Durchführen kontinuierlicher Überwachung**

Neben der Überwachung der Protokolle der IDS werden in regelmäßigen Abständen die Anfälligkeit des Systems bei bekannten Angriffsarten überprüft.

Bei dieser täglichen Routineuntersuchung der Protokolle des IDS wurde ein „synflood“ Angriff entdeckt. Synflood Angriffe können gesamte Dienste für mehrere Stunden unerreichbar machen. Es wird in einer neuen Akte dieser Vorfall dokumentiert. So wird zunächst festgehalten, wann dieser Angriff zum ersten mal, nach Protokoll des IDS, aufgetreten ist. Die Meldung erhält der Systemadministrator per SMS auf sein Handy.

### 3.4.2.3 Umfassendes Informieren

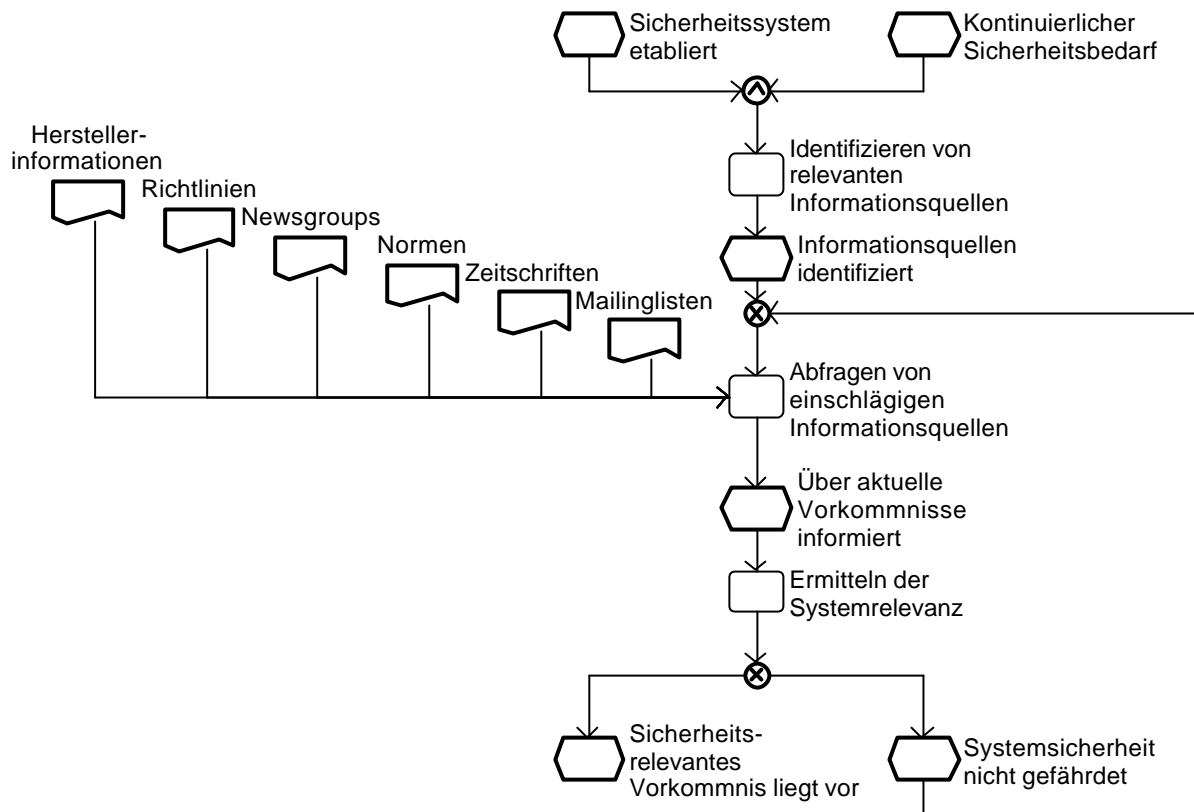


Abbildung 36: Umfassendes Informieren

Parallel zu den kontinuierlichen Kontrollen werden einschlägige Informationsquellen nach aktuellen Sicherheitsbedenken abgefragt. Die Bedeutung dieser Recherche muss der IT Systems Administrator für das eigene System hin überprüfen. Diese Überprüfung ergibt, ob es sich um ein sicherheitsgefährdendes Ereignis handelt oder nicht.

#### 3.4.2.3.1 Tätigkeiten: Umfassendes Informieren

Um sich umfassend zu informieren, muss der IT Systems Administrator folgende Tätigkeiten durchführen:

- Identifizieren von relevanten Informationsquellen
- Abfragen von einschlägigen Informationsquellen
- Ermitteln der Systemrelevanz

#### 3.4.2.3.2 Kompetenzfelder: Umfassendes Informieren

Fähigkeiten/Fertigkeiten

- Selbstständiges recherchieren können
- Informationsquellen nach sicherheitsrelevanten Themen durchsuchen können
- Informationsquellen themenspezifisch abfragen können
- Informationen analysieren können
- Bedeutung für das eigene System abschätzen können
- Dokumentieren können

Wissen

- Kenntnisse über gängige Informationsquellen in Bezug auf Sicherheitsthemen
- Kenntnisse in Rechercheverfahren
- Kenntnisse im Umgang mit Standards der Dokumentation in Bezug auf Sammeln relevanter Informationen für die Minimierung von Sicherheitsrisiken des IT-Systems

#### **3.4.2.3.3 *Beispiel: Umfassendes Informieren***

Um es erst gar nicht zu Sicherheitslücken im System kommen zu lassen, werden zunächst alle möglichen Informationsquellen zusammengestellt. Da die Anzahl der zu Verfügung stehenden Informationen zu groß ist und der Systemadministrator für die Erfassung von relevanten Informationen zu viel Zeit benötigen würde, installiert er einen Filter, der die einschlägigen Herstellerseiten, Newsgroups etc. nach von ihm vorgegebenen Schlüsselworten durchsucht. So kann er sich zielgerichtet informieren und dann abschätzen, ob die Information eine für sein zu betreuendes System Relevanz besitzt.

### 3.4.2.4 Analysieren des Vorkommnisses

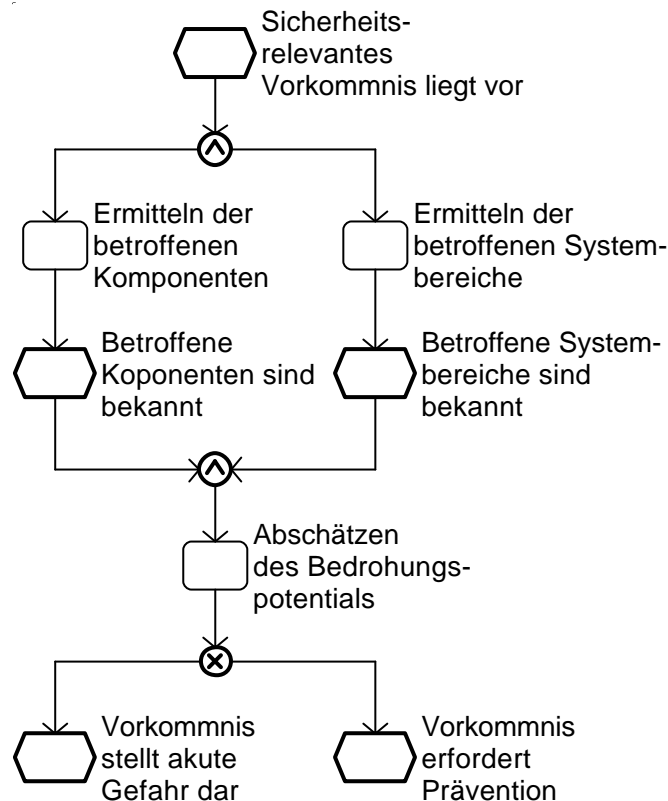


Abbildung 37: Analysieren des Vorkommnisses

Wurde durch die Kontrolle bzw. das Informieren ein sicherheitsrelevantes Vorkommnis für das System identifiziert, werden zunächst die betroffenen Systemkomponenten und Systembereiche identifiziert. Sind diese bekannt, muss der IT Systems Administrator das Bedrohungspotential abschätzen. Hier muss er entscheiden, ob es sich um eine akute Gefährdung handelt oder ob dem Vorkommnis präventiv begegnet werden muss.

#### 3.4.2.4.1 Tätigkeiten: Analysieren des Vorkommnisses

Der IT Systems Administrator muss folgende Tätigkeiten bei der Analyse des Vorkommnisses durchführen:

- Ermitteln der betroffenen Komponenten
- Ermitteln der betroffenen Systembereiche
- Abschätzen des Bedrohungspotentials

#### 3.4.2.4.2 Kompetenzfelder: Analysieren des Vorkommnisses

Fähigkeiten/Fertigkeiten

- Betroffene Systemkomponenten identifizieren können
- Betroffene Systembereiche identifizieren können
- Bedrohungspotential (für das eigene System) abschätzen können
- Dokumentieren können

Wissen

- Betriebsarten von Systemen und benutzter Hardware kennen
- Grundlegende Kenntnisse in der Netzwerktechnik und in Netzwerktopologien
- Kenntnisse von Datenübertragungssystemen und -techniken sowie der verwendeten Hardwareschnittstellen kennen
- Kenntnisse über die sich im Einsatz befindenden System- und Kommunikationsarchitekturen



- Kenntnisse über die sich im Einsatz befindenden Netzwerk- und Kommunikationsprotokollen sowie der Dienste und der verwendeten Schnittstellen zu anderen Systemen und Softwaresystemen
- Kenntnisse der Funktionsweise von Scanner und Sniffer
- Kenntnisse der Funktionsweise und der Chancen und Risiken von Firewalls und Proxys
- Kenntnisse der Funktionsweise von Würmern, Viren, Trojanern und Hybriden
- Kenntnisse der Funktionsweise gängiger Hacking Software
- Kenntnisse im Umgang mit Fernzugriffsverfahren und –software
- Kenntnisse in der Rationalisierung von Arbeitsschritten und deren Organisation in Bezug auf das Management von Systemsicherheit
- Kenntnisse im Umgang mit Standards der Dokumentation in Bezug auf das Festhalten von Beweismitteln für spätere rechtliche Folgemaßnahmen

#### Werkzeuge

- Betriebssystemeigene Werkzeuge
- Fernzugriffssoftware
- Diagnosesoftware
- Sicherheitssoftware

#### **3.4.2.4.3 Beispiel: Analysieren des Vorkommnisses**

Durch die Analyse der Protokolldateien aller beteiligten Systeme muss die Auswirkung auf das Gesamtsystem und einzelner Systeme erkannt werden. Des Weiteren muss die Ausfallzeit bestimmt werden. Hinzu kommt, dass der Webadministrator und der Netzwerkadministrator informiert werden muss, weil zum einen der Webserver als auch eventuell die Firewall betroffen sein kann. Bei der Analyse wird ein DDOS (Distributed Denial of Service) Angriff identifiziert. Der Angriff hat um 18 Uhr stattgefunden und dauerte weniger als eine Sekunde. Die aufgezeichneten Pakete treffen auf eine Firewallregel zu und wurden von dieser zum Teil verworfen und protokolliert. Die eingehenden Pakete stammten von einem Universitätsserver in Deutschland. Ansonsten sind keine Unregelmäßigkeiten aufgetreten. Die angebotenen Dienste waren zum Teil stark beeinträchtigt worden. So stand der Internetshop für zwei Stunden nicht zur Verfügung. Für das weitere Vorgehen werden die zusammengetragenen Informationsquellen konsultiert. Es wird ein weiteres Tool „Shaft“ identifiziert, welches Angriffe dieser Art analysieren kann. Nach der Installation und Auswertung der Protokolle kann mit diesem Tool das Ereignis 100%ig als Shaft Synflood identifiziert werden. Ein Fehlalarm ist somit ausgeschlossen.

### 3.4.2.5 Untersuchen der Auswirkungen

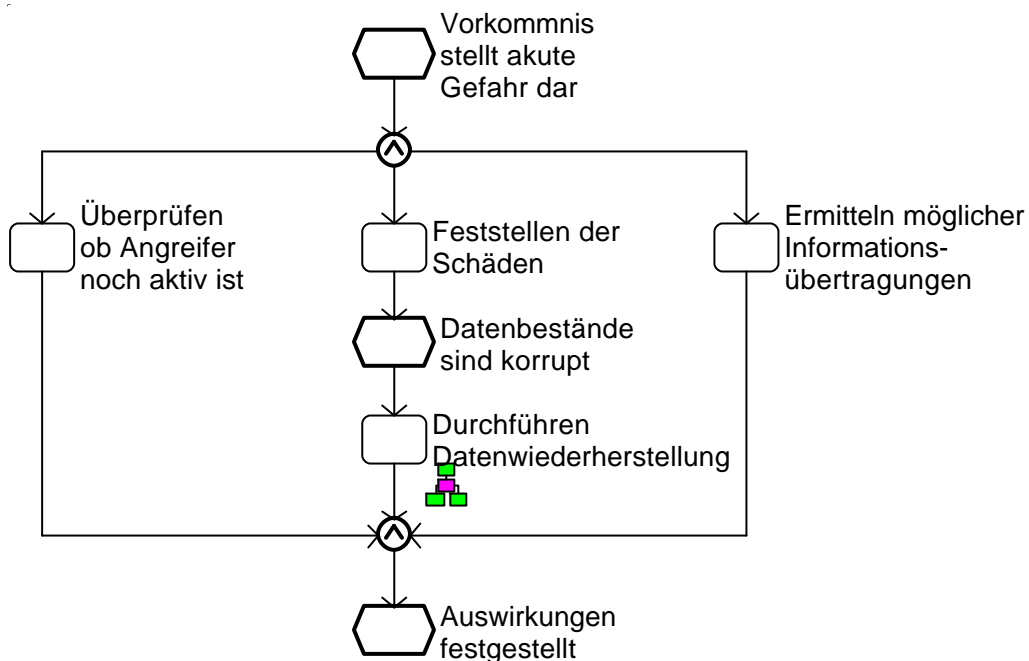


Abbildung 38: Untersuchen der Auswirkungen

Geht von dem Vorkommnis eine akute Gefährdung für das System aus, so muss der IT Systems Administrator prüfen, ob der Angreifer noch aktiv ist, die Schädigung feststellen und ermitteln, ob es zu einer Informationsübertragung gekommen ist. Wird dabei festgestellt, dass Datenbestände verändert oder gelöscht wurden, führt der IT Systems Administrator die Datenwiederherstellung durch. Im Ergebnis sind die Auswirkungen des Vorkommnisses festgestellt.

#### 3.4.2.5.1 Tätigkeiten: Untersuchen der Auswirkungen

Um die Auswirkungen des sicherheitsrelevanten Vorkommnisses zu untersuchen, muss der IT Systems Administrator folgende Tätigkeiten durchführen:

- Überprüfen, ob Angreifer noch aktiv ist
- Feststellen der Schäden
- Eventuell: Durchführen Datenwiederherstellung
- Ermitteln möglicher Informationsübertragungen

#### 3.4.2.5.2 Kompetenzfelder: Untersuchen der Auswirkungen

Fähigkeiten/Fertigkeiten

- Aktivitäten von Angreifern überprüfen können
- Schädigungen feststellen können
- Mögliche Informationsübertragungen ermitteln können
- Datenwiederherstellung durchführen können
- Dokumentieren können

Wissen

- Betriebsarten von Systemen und benutzter Hardware kennen
- Grundlegende Kenntnisse in der Netzwerktechnik und in Netzwerktopologien
- Kenntnisse von Datenübertragungssystemen und –techniken sowie der verwendeten Hardwareschnittstellen kennen
- Kenntnisse über die sich im Einsatz befindenden System- und Kommunikationsarchitekturen
- Kenntnisse über die sich im Einsatz befindenden Netzwerk- und Kommunikationsprotokollen sowie der Dienste und der verwendeten Schnittstellen zu anderen Systemen und Softwaresystemen
- Kenntnisse der Funktionsweise von Scanner und Sniffer

- Kenntnisse der Funktionsweise und der Chancen und Risiken von Firewalls und Proxys
- Kenntnisse der Funktionsweise von Würmern, Viren, Trojanern und Hybriden
- Kenntnisse der Funktionsweise gängiger Hacking Software
- Kenntnisse im Umgang mit Fernzugriffsverfahren und –software
- Kenntnisse in der Rationalisierung von Arbeitsschritten und deren Organisation in Bezug auf das Management von Systemsicherheit
- Kenntnisse im Umgang mit Standards der Dokumentation in Bezug auf das Festhalten von Beweismitteln für spätere rechtliche Folgemaßnahmen

#### Werkzeuge

- Fernzugriffssoftware
- Systemmonitore
- Sicherheitssoftware
- Datenwiederherstellungssoftware
- Diagnosesoftware
- Betriebssystemeigene Werkzeuge

#### **3.4.2.5.3 Beispiel: Untersuchen der Auswirkungen**

Der DDOS-Angriff betraf ausschließlich den Server, der außerhalb der DMZ stand. Es gab gemäß der Protokolle keinen Datentransfer zwischen den Angreifer und dem Server. Da der Angreifer bereits offline ist und das IDS keine weiteren Angriffe verzeichnet, kann davon ausgegangen werden, dass der Angriff eingestellt wurde. Aufgrund der durch den DOS-Angriff verursachten Überlastung wurden einige Domino-Dienste und Anwendungen mit Fehlern angehalten. Dies verursachte, neben dem Ausfall des Shopsystems, auch den Verlust wichtiger Kunden-, Transaktions- und Bestelldaten. Nachdem die Geschäftsleitung über den entstandenen Schaden informiert und eine erste Hochrechnung über den entgangenen Gewinn erstellt wurde, wird der Systemadministrator beauftragt, weitere Schäden und Angriffe vorzubeugen.

### 3.4.2.6 Reaktives Entwickeln von Ad-hoc-Lösungen

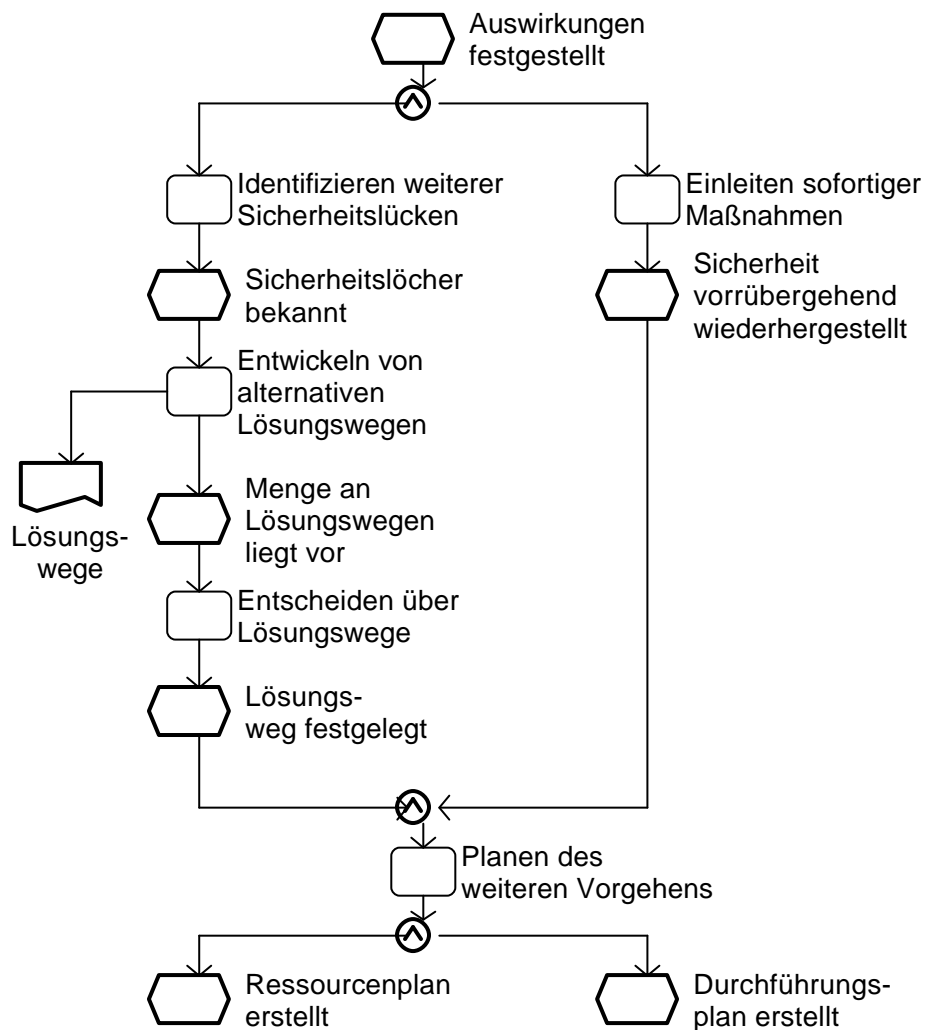


Abbildung 39: Reaktives Entwickeln von Ad-hoc-Lösungen

Sind die Auswirkungen festgestellt, muss zunächst, um weitere Schäden zu vermeiden, sofort der Gefahr entgegengewirkt und dann (alternative) Lösungswege entwickelt werden, über deren Verwirklichung der IT Systems Administrator entscheiden muss. Dazu müssen zunächst alle Sicherheitslücken, die mit diesem Vorkommnis entstanden sind, identifiziert werden. Nachdem dann Lösungswege vorgeschlagen sind und über diese entschieden worden ist, muss der IT Systems Administrator die Umsetzung (inkl. Ressourcen- und Durchführungsplan) planen (siehe auch „Planen der Abwicklung“ Abschnitt 3.1.2.3).

#### 3.4.2.6.1 Tätigkeiten: Reaktives Entwickeln von Ad-hoc-Lösungen

Um Ad-hoc-Lösungen reaktiv zu entwickeln, muss der IT Systems Administrator folgende Tätigkeiten durchführen:

- Einleiten sofortiger Maßnahmen
- Identifizieren weiterer Sicherheitslücken
- Entwickeln von alternativen Lösungswegen
- Entscheiden über Lösungswege
- Planen des Weiteren Vorgehens

#### 3.4.2.6.2 Kompetenzfelder: Reaktives Entwickeln von Ad-hoc-Lösungen

Fähigkeiten/Fertigkeiten

- Auf Sicherheitsverletzungen angemessen reagieren können
- Weitere Sicherheitslücken identifizieren können

- Lösungswege entwickeln können
- Alternativen untereinander abwägen können
- Zeitplanung erstellen
- Beschaffungsliste erstellen können
- Zukünftigen Bedarf ermitteln können
- Sich selbst und eventuell Mitarbeiter beurteilen und einschätzen können
- Personalplanung erstellen können
- Budgetplanung erstellen können
- Ablaufplanung erstellen können
- Planungen zusammenführen können
- Spezielle Anforderungen verstehen können
- Kaufmännisches Rechnen durchführen können
- Zukünftige Aufwände kalkulieren und prognostizieren können
- Dokumentieren können

#### Wissen

- Erfahrungen im Umgang mit Sicherheitsverletzungen im IT-System
- Betriebsarten von Systemen und benutzter Hardware kennen
- Kenntnisse über die sich im Einsatz befindenden System- und Kommunikationsarchitekturen und deren Abhängigkeiten untereinander
- Kenntnisse der Funktionsweise von Scanner und Sniffer
- Kenntnisse der Funktionsweise und der Chancen und Risiken von Firewalls und Proxys
- Kenntnisse der Funktionsweise von Würmern, Viren, Trojanern und Hybriden
- Kenntnisse der Funktionsweise gängiger Hacking Software
- Kenntnisse über die potentielle Sicherheitslücke und deren Auswirkungen auf das sich in Betrieb befindende IT-System
- Kenntnisse im Umgang mit Fernzugriffsverfahren und –software
- Kenntnisse in der Rationalisierung von Arbeitsschritten und deren Organisation in Bezug auf das Management von Systemsicherheit
- Kenntnisse in der Planung und Kostenbestimmung weiterer Tätigkeiten
- Kenntnisse im Umgang mit Standards der Dokumentation in Bezug auf zu erfolgende Änderungen am IT-System durch einen Change-Managementprozess

#### Werkzeuge

- Projektmanagementsoftware
- Kaufmännische Software
- Diagnosesoftware
- Tabellenkalkulation

#### **3.4.2.6.3 Beispiel: Reaktives Entwickeln von Ad-hoc-Lösungen**

Da der Paketfilter der Firewall einige Pakete verworfen hat, muss diese so konfiguriert werden, dass bei einem eventuell ähnlichen Angriff von „shaft“ diesen bereits im Vorfeld abwehren. Die Einstellungen in der DMZ waren zu diesem Zeitpunkt ausreichend.

Um den Server noch in einem höheren Maße ausfallsicher zu machen, werden für eine Entwicklung eines Lösungsplans typische DOS-Angriffe analysiert und daraufhin werden zunächst alle bekannten Ports, die ein Shaft-Angriff benutzt gesperrt. So kann dieser Server selbst nicht als Slave oder Reflector für andere Angriffe benutzt werden. Des Weiteren werden die TCP und UDP Ports für diesen Server weiter eingeschränkt, da typische Angriffe immer über 1024 erfolgen.

Um eine weitere Ausfallsicherheit zu gewährleisten, wird vorgeschlagen, dass auf dem Server ein Fernwartungstool installiert wird, welches dem Systemadministrator erlaubt, notfalls auch von zu Hause auf eine Meldung einer Sicherheitsverletzung zu reagieren.

Diese Vorschläge werden der Geschäftsleitung vorgestellt, die daraufhin dessen Durchführung beschließt.

### 3.4.2.7 Aktives Entwickeln von Umsetzungsmöglichkeiten

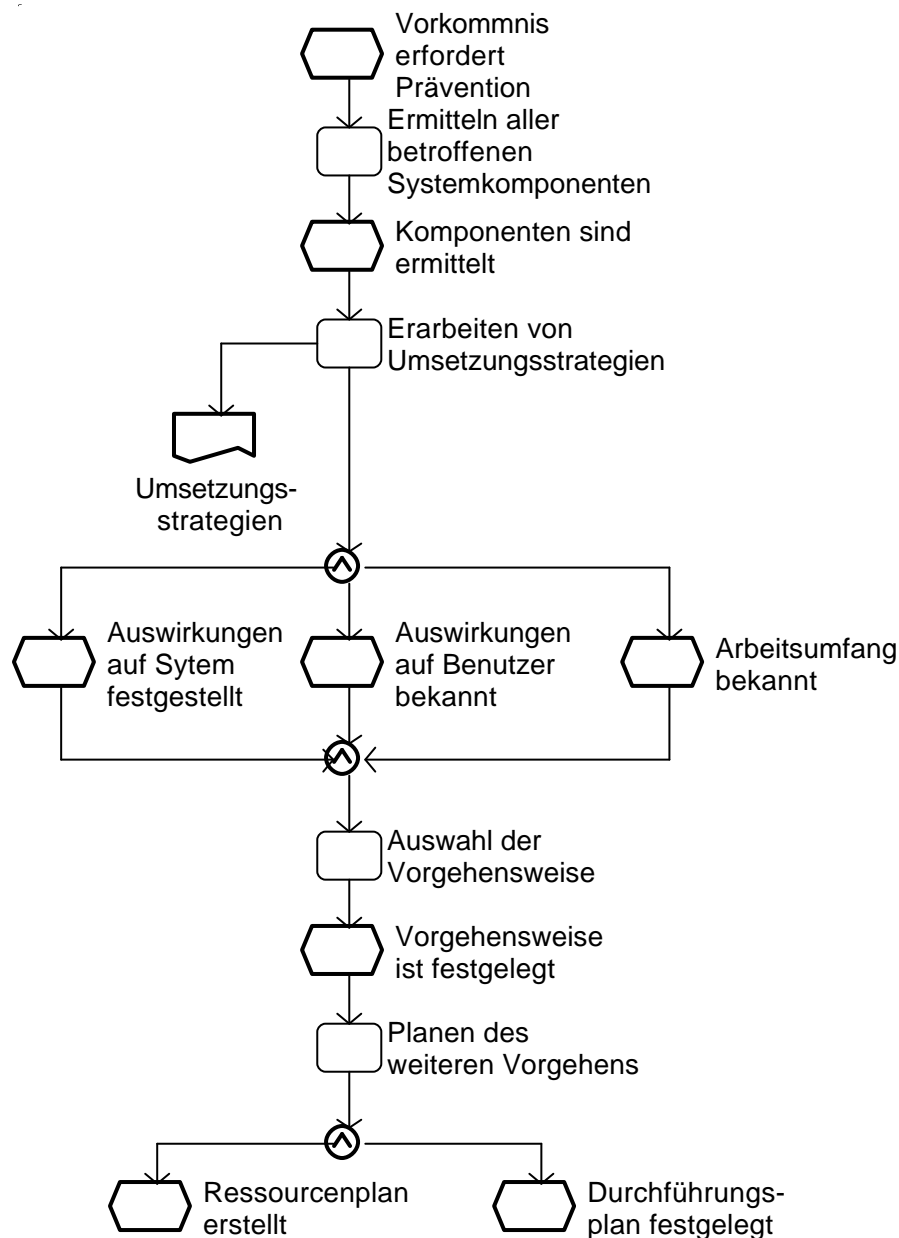


Abbildung 40: Aktives Entwickeln von Umsetzungsmöglichkeiten

Soll dem Vorkommnis präventiv begegnet werden, muss der IT Systems Administrator alle betroffenen Systemkomponenten ermitteln. Sind diese bekannt, muss er Umsetzungsstrategien zur Prävention entwickeln. Dabei werden Auswirkungen auf das laufende System und die Benutzern festgestellt sowie der Arbeitsumfang ermittelt. Aus der Vielzahl der möglichen Umsetzungsstrategien, wird eine Vorgehensweise ausgewählt und das weitere Vorgehen geplant. Im Ergebnis liegen wiederum ein Ressourcen- und Durchführungsplan vor (siehe auch „Planen der Abwicklung“ Abschnitt 3.1.2.3).

#### 3.4.2.7.1 Tätigkeiten: Aktives Entwickeln von Umsetzungsmöglichkeiten

Um aktiv Umsetzungsmöglichkeiten zu entwickeln, muss der IT Systems Administrator folgende Tätigkeiten durchführen:

- Ermitteln aller betroffenen Systemkomponenten
- Erarbeiten von Umsetzungsstrategien
- Auswahl der Vorgehensweise
- Planen des Weiteren Vorgehens

### 3.4.2.7.2 **Kompetenzfelder: Aktives Entwickeln von Umsetzungsmöglichkeiten**

#### Fähigkeiten/Fertigkeiten

- Betroffene Systemkomponenten ermitteln können
- Umsetzungsstrategien erarbeiten können
- Auswirkungen auf das System feststellen können
- Auswirkungen auf Benutzer erkennen können
- Arbeitsumfang der einzelnen Umsetzungsstrategien ermitteln und abschätzen können
- Alternativen abwägen können
- Planen können
- Zeitplanung erstellen
- Beschaffungsliste erstellen können
- Zukünftigen Bedarf ermitteln können
- Sich selbst und eventuell Mitarbeiter beurteilen und einschätzen können
- Personalplanung erstellen können
- Budgetplanung erstellen können
- Ablaufplanung erstellen können
- Spezielle Anforderungen verstehen können
- Kaufmännisches Rechnen durchführen können
- Zukünftige Aufwände kalkulieren und prognostizieren können
- Dokumentieren können

#### Wissen

- Betriebsarten von Systemen und benutzter Hardware kennen
- Kenntnisse über die sich im Einsatz befindenden System- und Kommunikationsarchitekturen und deren Abhängigkeiten untereinander
- Kenntnisse der Funktionsweise von Scanner und Sniffer
- Kenntnisse der Funktionsweise und der Chancen und Risiken von Firewalls und Proxys
- Kenntnisse der Funktionsweise von Würmern, Viren, Trojanern und Hybriden
- Kenntnisse der Funktionsweise gängiger Hacking Software
- Kenntnisse über die potentielle Sicherheitslücke und deren Auswirkungen auf das sich in Betrieb befindende IT-System
- Kenntnisse im Umgang mit Fernzugriffsverfahren und –software
- Kenntnisse in der Rationalisierung von Arbeitsschritten und deren Organisation in Bezug auf das Management von Systemsicherheit
- Kenntnisse in der Planung und Kostenbestimmung weiterer Tätigkeiten
- Kenntnisse im Umgang mit Standards der Dokumentation in Bezug auf zu erfolgende Änderungen am IT-System (Anforderungskatalog)

#### Werkzeuge

- Projektmanagementsoftware
- Kaufmännische Software
- Tabellenkalkulation

### 3.4.2.7.3 **Beispiel: Aktives Entwickeln von Umsetzungsmöglichkeiten**

Nicht immer liegt eine konkrete Sicherheitsverletzung des Systems vor. Oft werden die Ports gescannt, um eventuell Sicherheitslücken zu identifizieren.

Beim Studium der zusammengetragenen Informationsquellen wurde festgestellt, dass der Webservice des Dominoservers eine Sicherheitslücke aufweist, der den unberechtigten Zugriff auf Datenbanken zulässt. Da alle Server in einer DMZ stehen, kann die Sicherheitsverletzung ausschließlich von innen erfolgen. Eine längere Recherche auf den Herstellerseiten konnten keine Sicherheitspatches identifizieren. Aus diesem Grund wird der Hersteller angerufen, um mit ihm das weitere Vorgehen zu besprechen. Diesem war die Lücke auch erst vor einigen Tagen bekannt geworden. Er empfiehlt für die Zeit die Schreibzugriffe zu beschränken.

Der Systemadministrator entzieht den Nutzern vorübergehend das Recht Dokumente zu löschen. So können nicht unberechtigt Daten vernichtet werden. Die betroffenen Benutzer werden zum einen über die entzogenen Rechte in Kenntnis gesetzt, zum anderen erklärt der Systemadministrator auch den Grund der Beschränkung. Der Vorgesetzte wird in-

formiert, dass zur Zeit eine Sicherheitslücke im System besteht, der Hersteller jedoch noch kein geeignetes Patch anbietet. Der Systemadministrator empfiehlt eine enge Kooperation mit dem Hersteller zu suchen und vorübergehend eine interne Firewall zu installieren bis das Patch vorliegt.



#### **3.4.2.8 Durchführen Change-Management**

Wurde ein Durchführungs- und Ressourcenplan für das Schließen der Sicherheitslöcher entwickelt, muss der IT Systems Administrator mithilfe des Change-Managementprozesses diese Arbeiten ausführen (siehe 3.1ff.).

### 3.4.2.9 Ausführen von Sicherheitschecks

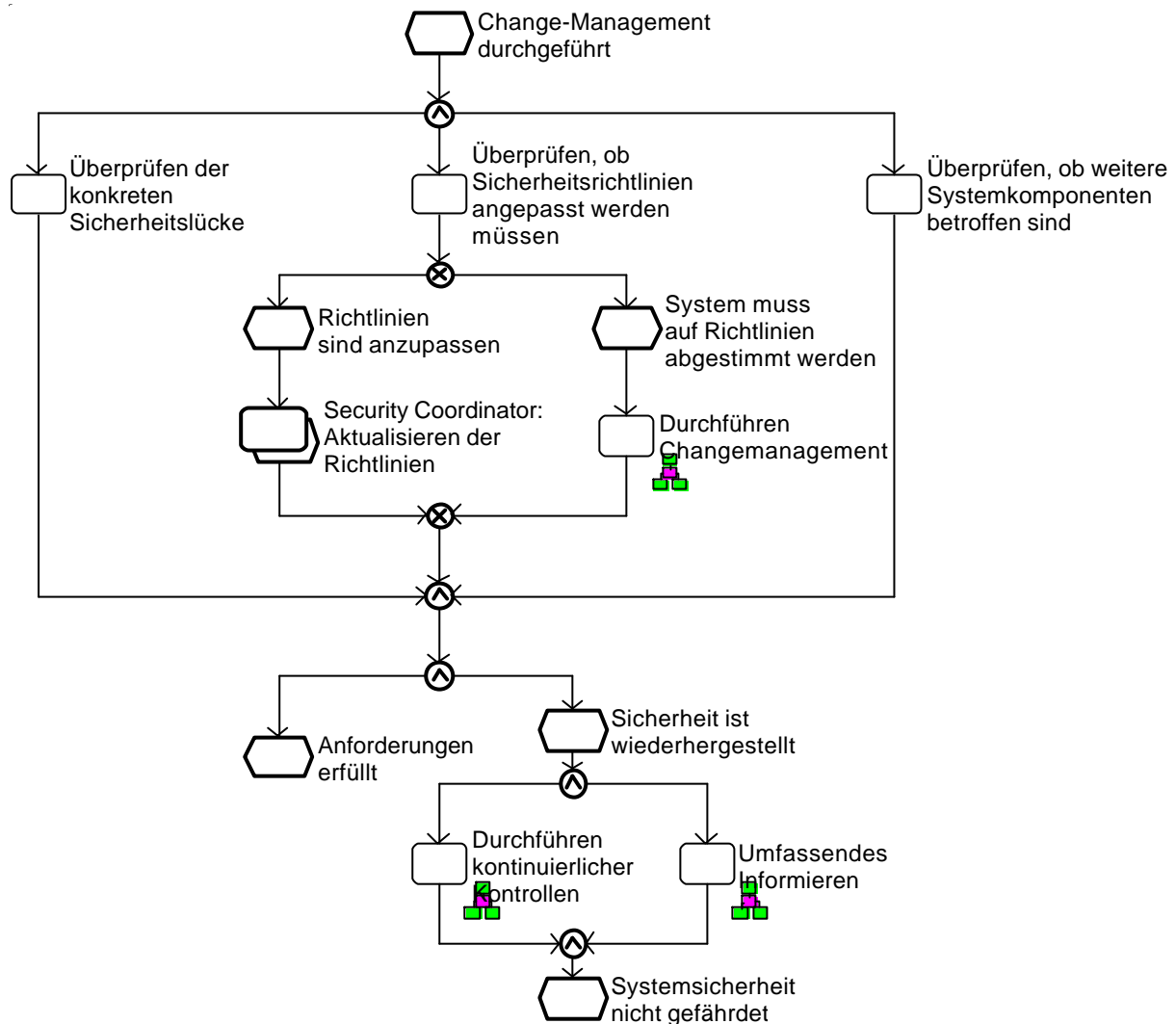


Abbildung 41: Ausführen von Sicherheitschecks

Ist das Change-Management vollzogen, führt man einen abschließenden Sicherheitscheck durch, um sicherzugehen, dass die identifizierten Sicherheitslücken tatsächlich geschlossen worden sind. Dazu prüft der IT Systems Administrator die konkrete Sicherheitslücke sowie die durch diese Lücke verursachten weiteren Sicherheitslücken anderer Komponenten. Außerdem prüft er, ob nach der Veränderung des Systems nach dem Change-Management die Sicherheitsrichtlinien noch eingehalten werden oder ob diese angepasst werden müssen. Sind die Sicherheitsrichtlinien nicht eingehalten worden, so müssen entweder diese auf der Grundlage der neuen Anforderung an die Systemsicherheit angepasst werden oder das System muss auf die Richtlinien abgestimmt werden, was einen erneuten Change-Managementprozess nach sich zieht. Im Ergebnis sind die Anforderungen, die die Sicherheitsrichtlinien vorschreiben, erfüllt und die Systemsicherheit wiederhergestellt. Der IT Systems Administrator kehrt wieder in die kontinuierliche Kontrolle des Systems (siehe Abschnitt 3.4.2.2) und des umfassenden Informierens (siehe Abschnitt 3.4.2.3) zurück.

#### 3.4.2.9.1 Tätigkeiten: Ausführen von Sicherheitschecks

Um die nötigen Sicherheitsschecks durchzuführen, muss der IT Systems Administrator folgende Tätigkeiten durchführen:

- Überprüfen der konkreten Sicherheitslücke
- Überprüfen, ob Sicherheitsrichtlinien angepasst werden müssen
- Überprüfen, ob weitere Systemkomponenten betroffen sind
- Zusammen mit dem Security Coordinator: Aktualisieren der Richtlinien
- Durchführen Change-Management

- Durchführen kontinuierlicher Kontrollen
- Umfassendes Informieren

### 3.4.2.9.2 **Kompetenzfelder: Ausführen von Sicherheitsschecks**

#### Fähigkeiten/Fertigkeiten

- Konkrete Sicherheitslücke auf Sicherheit überprüfen können
- Sicherheitsrichtlinien auf deren Anpassung an neue Anforderungen überprüfen können
- Weitere Systemkomponenten auf Sicherheitsvorkommnisse überprüfen können
- Sicherheitsrichtlinien zusammen mit dem Security Coordinator auf die neuen Anforderungen anpassen können
- Change-Management durchführen können
- Kontinuierliche Kontrollen durchführen können
- Sich umfassend informieren können
- Dokumentieren können

#### Wissen

- Betriebsarten von Systemen und benutzter Hardware kennen
- Kenntnisse über die sich im Einsatz befindenden System- und Kommunikationsarchitekturen und deren Abhängigkeiten untereinander
- Kenntnisse der Funktionsweise von Scanner und Sniffer
- Kenntnisse der Funktionsweise und der Chancen und Risiken von Firewalls und Proxys
- Kenntnisse der Funktionsweise von Würmern, Viren, Trojanern und Hybriden
- Kenntnisse der Funktionsweise gängiger Hacking Software
- Kenntnisse über die potentielle Sicherheitslücke und deren Auswirkungen auf das sich in Betrieb befindende IT-System
- Kenntnisse im Umgang mit Fernzugriffsverfahren und –software sowie Sicherheits(test)software
- Kenntnisse in der Rationalisierung von Arbeitsschritten und deren Organisation in Bezug auf das Management von Systemsicherheit
- Kenntnisse in der Planung und Kostenbestimmung weiterer Tätigkeiten
- Kenntnisse im Umgang mit Standards der Dokumentation in Bezug auf getestete Systembereiche
- Grundlegende Kenntnisse in der Organisation, Dimensionierung, Topologien und Komponenten von Netzwerken
- Kenntnisse im methodischen Vorgehen von Tests in Bezug auf Sicherheitsschecks
- Standards von Testverfahren

#### Werkzeuge

- Ereignismonitore
- Testsoftware
- Sicherheitssoftware
- Betriebssystemeigene Werkzeuge

### 3.4.2.9.3 **Beispiel: Ausführen von Sicherheitsschecks**

Nachdem die Firewall etabliert (siehe Abschnitt 3.4.2.7.3 Beispiel: Aktives Entwickeln von Umsetzungsmöglichkeiten) bzw. die Server neukonfiguriert und die Fernwartungssoftware auf den Servern installiert ist (siehe Abschnitt 3.4.2.6.3 Beispiel: Reaktives Entwickeln von Ad-hoc-Lösungen), wird die bekannte Sicherheitslücke über einen simulierten Angriff getestet. Dieser Angriff wird protokolliert durchgeführt und im Vorfeld mit der Geschäftsleitung abgesprochen. Nachdem die Sicherheitslücke beseitigt wurde, kehrt man zur regelmäßigen Kontrolle der Protokolle zurück und es werden die derzeitigen System- und Sicherheitsrichtlinien einer gründlichen Prüfung unterzogen, eventuell werden Empfehlungen für eine Änderung ausgesprochen, Benutzerrichtlinien angepasst oder Sicherheitssoftware installiert.

### 3.4.2.10 Erstellen einer Prozessdokumentation

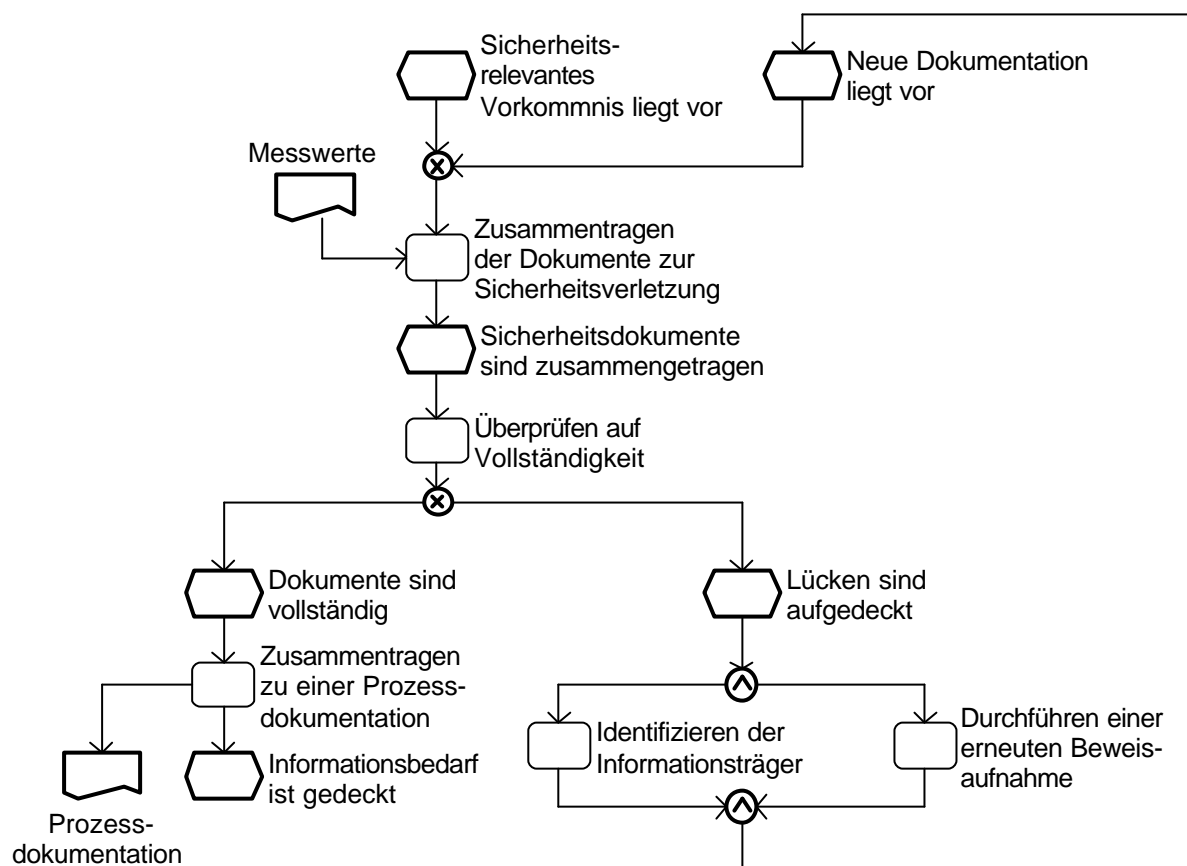


Abbildung 42: Erstellen einer Prozessdokumentation

Der Teilprozess „Erstellen einer Prozessdokumentation“ setzt sich aus einer kontinuierlichen Prozessdokumentation und Dokumentationen zu einzelnen Teilprozessen und der Beweissicherung zusammen. Es ist sowohl das Vorgehen, als auch die identifizierten Sicherheitsverletzungen zur späteren Beweisführung zu dokumentieren. Diese einzelnen Dokumente werden zusammengetragen und zu einer abschließenden Prozessdokumentation zusammengefügt.

Ziel dieses Prozesses ist es sowohl den kontinuierlichen Informationsbedarf zu decken als auch eine Beweismappe über entstandene (wirtschaftliche) Schäden anzulegen. So sollen zum einen erarbeitete Prozessschritte mit der Dokumentation für Dritte nachvollziehbar und nicht erneut erarbeitet werden. Zum anderen soll damit für Dritte der Hergang der Sicherheitsverletzung nachvollziehbar werden.

#### 3.4.2.10.1 Tätigkeiten: Erstellen einer Prozessdokumentation

Um eine Prozessdokumentation im Security-Management durchführen zu können, muss der IT Systems Administrator, meist parallel zu den Tätigkeiten der anderen Teilprozesse, folgende Tätigkeiten durchführen:

- Zusammentragen der Dokumente zur Sicherheitsverletzung
- Überprüfen auf Vollständigkeit

Falls die einzelnen Dokumente der Sicherheitsverletzung Lücken aufweisen:

- Identifizieren der Informationsträger
- Durchführen einer erneuten Beweisaufnahme

Auf jeden Fall:

- Zusammentragen zu einer Prozessdokumentation

### **3.4.2.10.2 Kompetenzfelder: Erstellen einer Prozessdokumentation**

#### Fähigkeiten/Fertigkeiten

- (Parallel zur Ausarbeitung) den gesamten Prozess dokumentieren können
- Übertragen der Tätigkeiten in Beweismappen
- Sicherheitsrelevante Vorkommnisse für eine spätere Verwendung durch Dritte dokumentieren können
- Sicherheitsrelevantes einschätzen und vor widerrechtlichen Zugriffen schützen können
- Dokumentationslücken entdecken können

#### Wissen

- Standards der Dokumentation in Bezug auf das Nachvollziehen von Prozessschritten kennen
- Rechtliche Auswirkungen in Bezug auf Dokumentationslücken kennen

#### Werkzeuge

- Textverarbeitung

### **3.4.2.10.3 Beispiel: Erstellen einer Prozessdokumentation**

Seitdem der Angriff auf das System festgestellt wurde, müssen alle relevanten Dokumente für eine spätere Beweisführung zusammengetragen und geeignet archiviert werden. Des Weiteren soll die komplette Beseitigung der Sicherheitslücke dokumentiert werden, so dass der Systemadministrator nicht selbst verdächtigt werden kann, die Sicherheit des Systems verletzt oder das System korrumpiert zu haben.

Die einzelnen Dokumente werden zeitlich geordnet und daraus können Handlungsalternativen abgeleitet werden, die in späteren Fassungen von Sicherheitsrichtlinien eingepflegt werden müssen.

### **3.4.2.11 Informieren betroffener Personen/Stellen**

#### **3.4.2.11.1 Tätigkeiten: Informieren betroffener Stellen/Personen**

In diesem Abschnitt werden die Kommunikationsmaßnahmen als kontinuierliche, den gesamten Prozess begleitende Teilprozesse beschrieben.

Solche Ad-hoc-Kommunikationsmaßnahmen werden durchgeführt, wenn bestimmte Personen oder Stellen über den aktuellen Stand der Bearbeitung informiert werden müssen. Dazu zählen aber auch die Einweisung der Nutzer nach dem erfolgreich durchgeführten Security-Management sowie ausführlichere Nutzerschulungen zu neuen Sicherheitsrichtlinien.

Diese Tätigkeiten werden kumuliert im Referenzprozess „Benutzerberatung und Organisation“ (siehe Abschnitt 3.6ff.) durchgeführt. In diesen fallen auch die konkrete Schulung und Einweisung in das System.

#### **3.4.2.11.2 Kompetenzfelder: Informieren betroffener Stellen/Personen**

Fähigkeiten/Fertigkeiten

- Schulungen organisieren und durchführen können (siehe Abschnitt 3.6.2.4 Einweisen der Benutzer)
- Erklären können
- Dokumentieren können

Wissen

- Je nach Informationsbedarf Kenntnisse über relevante Themen, die den Nutzer betreffen können, kennen

Werkzeuge

- Informationsverteiler

#### **3.4.2.11.3 Beispiel: Informieren betroffener Stellen/Personen**

Um die eigene Arbeit abzusichern, steht der Systemadministrator im ständigen Kontakt mit dem Vorgesetzten oder bei Bedarf mit der Geschäftsleitung. Des Weiteren muss der Systemadministrator die zusammengetragenen Dokumente so kommunizieren, dass sie als Entscheidungsgrundlage für Handlungsalternativen dienen können. Die meist komplexen Sachverhalte, zum Beispiel wie Angriffe erfolgen, welchen Schaden sie anrichten können und wie hoch das daraus resultierende Bedrohungspotential für die eigenen Server ist, muss vom Systemadministrator so kommuniziert werden, dass ein Sicherheitsbewusstsein bei den informierten Personen entsteht. Es sollte jedoch nicht das Risiko übertrieben werden, da sonst die Kosten der Behebung der Sicherheitslücke den zu erwartenden Schaden bei Weiterem übersteigen kann.



### 3.5 Datensicherung

---

Durch technisches Versagen, versehentliches Löschen oder durch Manipulation können gespeicherte Daten unbrauchbar werden bzw. verloren gehen. Um dem entgegenzuwirken, muss eine Datensicherung gewährleisten, dass durch einen redundanten Datenbestand der IT-Betrieb kurzfristig wieder aufgenommen werden kann. Des Weiteren kann aufgrund zu vieler Daten eine Beeinträchtigung der Systemleistung erfolgen.

Sobald eins der oben genannten Ereignisse aufgetreten ist, bedienen sich IT Systems Administrator dieses Teilprozesses. Aufgrund der Komplexität der Konzeption einer angemessenen und funktionstüchtigen Datensicherung sowie der Vorgaben des Security-Managements, bedarf es einer geordneten Vorgehensweise. Um den IT-Grundschutz zu realisieren, müssen IT Systems Administrator zunächst (nach den Empfehlungen des Bundesamts für Sicherheit in der Informationstechnik) ein Datensicherungskonzept erarbeiten. In diesem werden auch Archivierungsregeln festgelegt.

Um dieses Konzept in die Praxis umsetzen zu können, müssen Hard- und Softwarevoraussetzungen geschaffen werden. IT Systems Administrator etablieren selbstständig die notwendigen Geräte und Anlagen. Sind die Komponenten beschafft, kann die eigentliche Datensicherung beginnen. Bei einer erfolglosen Datensicherung muss diese erneut durchgeführt werden. Eine erfolgreiche Datensicherung muss auf jeden Fall gewährleistet sein. Werden vom Benutzer der Verlust oder die Manipulation von Daten gemeldet, werden diese vom IT Systems Administrator wiederhergestellt.

Die im Datensicherungskonzept definierte Notfallvorsorge sollte neben der eigentlichen Datensicherung in regelmäßigen Abständen erfolgen. Eine genaue Überprüfung beendet den Prozess der Datensicherung.



### 3.5.1 Der Referenzprozess Datensicherung

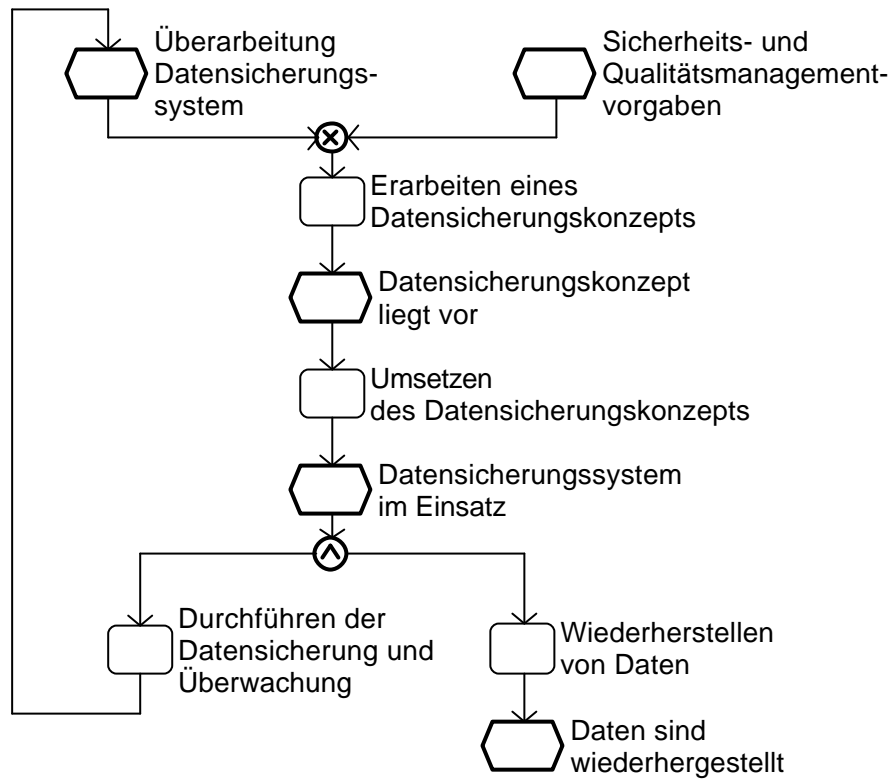


Abbildung 43: Referenzprozess Datensicherung

### **3.5.2 Prozesskompass Datensicherung**

Zusammenfassend sind folgende Teilprozesse im Referenzprozess Datensicherung enthalten:

1. Erarbeiten eines Datensicherungskonzepts
2. Umsetzen des Datensicherungskonzepts
3. Durchführen der Datensicherung und Überwachung
4. Wiederherstellen von Daten

### 3.5.2.1 Erarbeiten eines Datensicherungskonzepts

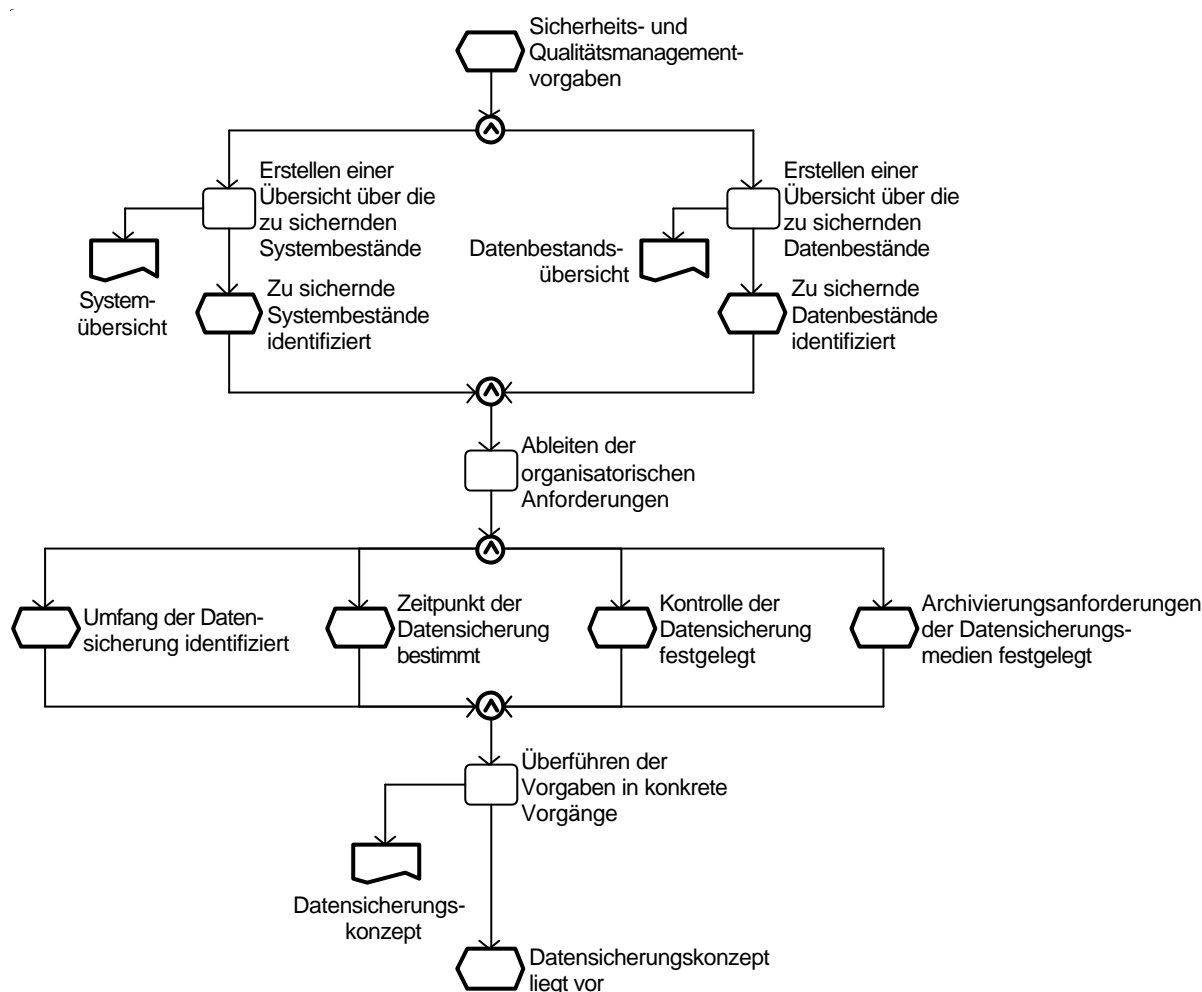


Abbildung 44: Erarbeiten eines Datensicherungskonzepts

Jeder Prozess der Datensicherung beginnt mit der Erarbeitung eines Datensicherungskonzepts. Dabei werden zunächst Übersichten über zu sichernde Systembestände und über zu sichernde Datenbestände erstellt. Aus diesen Übersichten werden spezielle organisatorische Anforderungen abgeleitet, um die Datensicherung in den Produktionsbetrieb einzusetzen. So wird der Umfang der zu sichernden Daten identifiziert (Speicherplatz), der Zeitpunkt, wann die Datensicherung durchgeführt werden soll sowie Kontrollmechanismen, die den Erfolg oder Misserfolg einer Datensicherung bestimmen, und die Anforderungen der Archivierung an die Datensicherungsmedien festgelegt. Diese Vorgaben werden in konkrete Vorgänge für die Umsetzung überführt. Im Ergebnis liegt ein Datensicherungskonzept vor.

#### 3.5.2.1.1 Tätigkeiten: Erarbeiten eines Datensicherungskonzepts

Um ein Datensicherungskonzept für das System zu erarbeiten, muss der IT Systems Administrator folgende Tätigkeiten durchführen:

- Erstellen einer Übersicht über die zu sichernden Systembestände
- Erstellen einer Übersicht über die zu sichernden Datenbestände
- Ableiten der organisatorischen Anforderungen
- Überführen der Vorgaben in konkrete Vorgänge

#### 3.5.2.1.2 Kompetenzfelder: Erarbeiten eines Datensicherungskonzepts

Fähigkeiten/Fertigkeiten

- Übersichten über zu sichernde System- und Datenbestände erstellen können
- Spezielle organisatorische Anforderungen an das System ableiten können

- Datenumfänge abschätzen können
- Datensicherungszeitpunkt festlegen können
- Anforderungen an die Datensicherungsmedien bestimmen können
- Kontrollen einrichten können
- Vorgaben in konkrete Vorgänge überführen können
- Dokumentieren können

#### Wissen

- Kenntnisse über gängige Datensicherungsverfahren und der Verwendung von Datensicherungsmedien und Sicherungsformen
- Techniken der Datensicherung kennen
- Kenntnisse über die verwendeten Systemarchitekturen, Betriebssysteme und Softwaresysteme
- Kenntnisse bei der Verwendung von Referenzmodellen der Sicherung von Datenzuständen
- Kenntnisse bei der Planung von Prozessen und über organisatorische Auswirkungen
- Datensicherungshandbuch der Organisation
- Standards der Dokumentation in Bezug auf das Entwerfen von Richtlinien für die Datensicherung und die spätere Nachvollziehbarkeit von Datensicherungen

#### Werkzeuge

- Betriebssystemeigene Datensicherungswerkzeuge

### **3.5.2.1.3 Beispiel: Erarbeiten eines Datensicherungskonzepts**

Hier wird das Beispiel aus Kapitel 3.1ff. Change-Management aufgegriffen. Für das neue System wird nun eine Datensicherung eingeführt.

Zunächst werden alle Daten identifiziert, die für den fehlerfreien Betrieb notwendig sind. So müssen die notes.ini, names.nsf, die cert.id, server.id, desktop.dsk, catalog.nsf, mail.box und user.id (ID des Administrator), die Transaktionsprotokollierung und die Datenbanken im shared Data-Verzeichnis gesichert werden.

Da die Server ausschließlich während der Geschäftszeiten benutzt werden, wird das Backup in der Nacht durchgeführt. Zusätzlich wird ein Logbuch angelegt, in dem jede Datensicherung einzutragen ist. Hier wird auch der Erfolg oder der Misserfolg einer Datensicherung erfasst.

Für das Backup wird der auftretende Speicherbedarf ermittelt. Die Server und die Klienten sollen einmal täglich gesichert werden. Dabei werden ausschließlich Datenbanken, bei denen Veränderungen erfolgen, berücksichtigt. Einmal wöchentlich wird ein Gesamtbackup durchgeführt und dieses in einem Schließfach außerhalb der Gebäude der Firma hinterlegt. Diese Maßnahmen werden in einem Datensicherungskonzept zusammengetragen und allen Mitarbeitern zur Verfügung gestellt.

### 3.5.2.2 Umsetzen des Datensicherungskonzepts

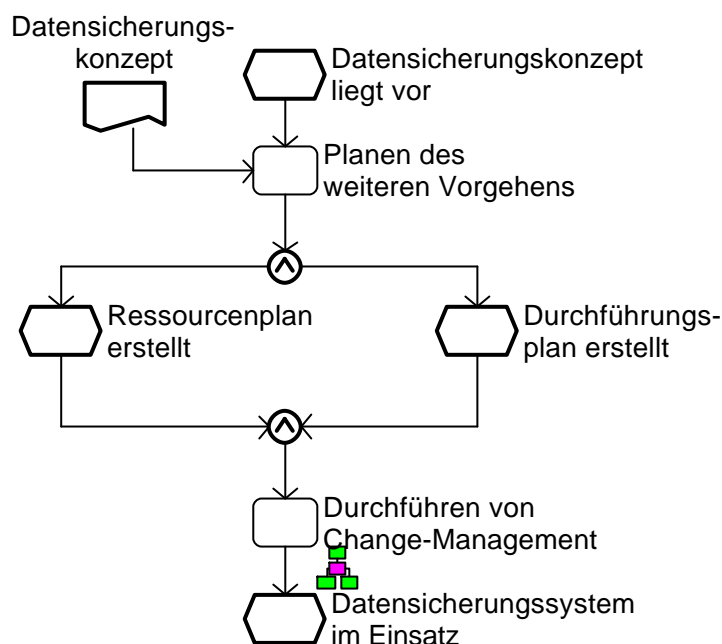


Abbildung 45: Umsetzen des Datensicherungskonzepts

Nachdem das Datensicherungskonzept vorliegt, muss es vom IT Systems Administrator umgesetzt werden. Dazu plant er zunächst das weitere Vorgehen und leitet daraus einen Ressourcen- und Durchführungsplan ab. Mit diesen Anforderungen setzt er mithilfe des Change-Managementprozesses das Konzept in den Produktionsbetrieb um. Im Ergebnis ist das Datensicherungssystem im Einsatz.

#### 3.5.2.2.1 Tätigkeiten: Umsetzen des Datensicherungskonzepts

Folgende Tätigkeiten muss der IT Systems Administrator durchführen, um das Datensicherungskonzept umzusetzen:

- Planen des Weiteren Vorgehens
- Durchführen Change-Management

#### 3.5.2.2.2 Kompetenzfelder: Umsetzen des Datensicherungskonzepts

Fähigkeiten/Fertigkeiten

- Vorgehen planen können
- Ressourcenplan erstellen können
- Zukünftigen Bedarf ermitteln können
- Sich selbst und eventuell Mitarbeiter beurteilen und einschätzen können
- Durchführungsplan erstellen können
- Kaufmännisches Rechnen durchführen können
- Zukünftige Aufwände kalkulieren und prognostizieren können
- Change-Management durchführen können
- Dokumentieren können

Wissen

- Kenntnisse über gängige Datensicherungsverfahren und der Verwendung von Datensicherungsmedien und Sicherungsformen
- Techniken der Datensicherung kennen
- Kenntnisse über das einzusetzende Datensicherungskonzepts
- Kenntnisse über die verwendeten Systemarchitekturen, Betriebssysteme und Softwaresysteme
- Kenntnisse bei der Verwendung von Referenzmodellen zur Sicherung von Datenzuständen
- Kenntnisse bei der Planung von Prozessen und über organisatorische Auswirkungen

- Datensicherungshandbuch der Organisation
- Standards der Dokumentation in Bezug auf das Entwerfen von Richtlinien für die Datensicherung und das spätere Nachvollziehen von Datensicherungen
- Betriebswirtschaftliche Grundkenntnisse in der Kosten- und Nutzenanalyse und der Kalkulation von Tätigkeiten

#### Werkzeuge

- Projektmanagementsoftware
- Kaufmännische Software
- Tabellenkalkulation
- Datensicherungswerkzeuge

#### **3.5.2.2.3 Beispiel: Umsetzen des Datensicherungskonzeptes**

Für die Datenarchivierung wird zur Zeit der Tivoli Storage Manager eingesetzt. Von dieser Firma wird auch ein Backup und Archivklient für Lotus Domino und für Lotus Notes angeboten. Dieser ist für den Betrieb von Dominoumgebungen entwickelt und optimiert worden. Im ersten Zug sollen alle Klienten und die Server mit diesem Klienten versehen werden. Dazu müssen die notwendigen Lizenzen gekauft, die Rechner mit dem Backup und Archivklienten versehen werden und diese nach den Vorgaben des Datensicherungskonzeptes konfiguriert werden. Dies beinhaltet neben dem Einstellen des Datensicherungszeitpunkts, des Backup-Servers auch die Konfiguration einer Include/Exclude-Liste. Die Planung wird mit der Geschäftsleitung durchgesprochen und nach deren Zustimmung durchgeführt.

Um dem wachsenden Speicherbedarf gerecht zu werden, wird ein weiteres Bandlaufwerk und Bänder bestellt und in die bestehende Backupinfrastruktur integriert. Ein erstes Backup wird anschließend durchgeführt, um neben dem ersten Datenbestand zu sichern auch die Funktionsfähigkeit zu überprüfen. Die erste Sicherung wird ins Datensicherungslogbuch eingetragen.

### 3.5.2.3 Durchführen der Datensicherung und Überwachung

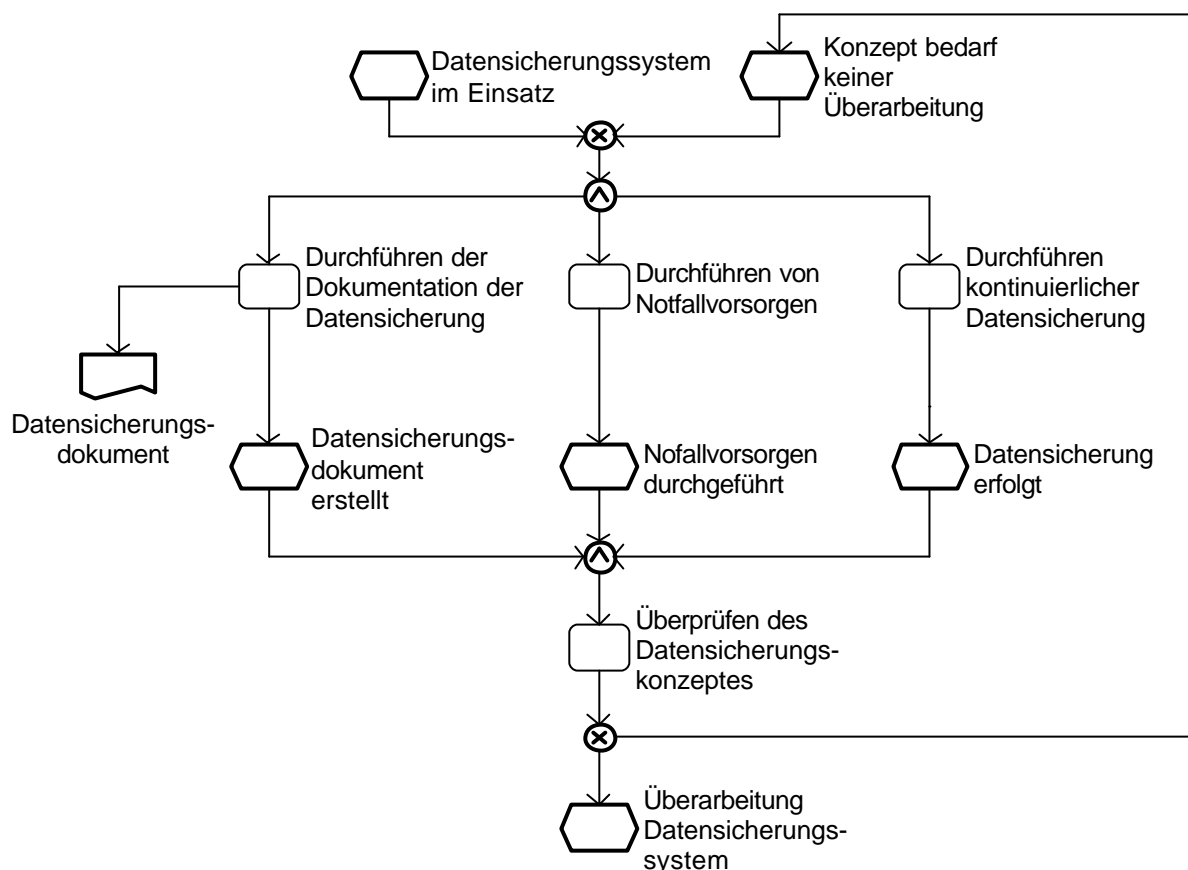


Abbildung 46: Durchführen der Datensicherung und Überwachung

Nachdem das Datensicherungssystem im Einsatz ist, muss der IT Systems Administrator kontinuierlich die Datensicherung nach den Vorgaben des Datensicherungskonzepts durchführen. Parallel dazu führt er regelmäßig Notfallvorsorgen durch, d.h. er übt ständig bei einem Ausfall der Datensicherung, welche Tätigkeiten dann durchzuführen sind, um die Datensicherung wieder in Betrieb zu nehmen. Begleitend zur kontinuierlichen Datensicherung und dem Durchführen von Notfallvorsorgen, dokumentiert der IT Systems Administrator die Datensicherung. Falls die kontinuierliche Datensicherung fehlerhaft verläuft, muss dies vom IT Systems Administrator erkannt werden und erneut angestoßen werden. Der Prozess endet mit der regelmäßigen Überprüfung des Datensicherungskonzepts.

#### 3.5.2.3.1 Tätigkeiten: Durchführen der Datensicherung und Überwachung

Um eine Datensicherung und deren Überwachung durchführen zu können, muss der IT Systems Administrator folgende Tätigkeiten durchführen:

- Durchführen kontinuierlicher Datensicherung
- Durchführen von Notfallvorsorgen
- Durchführen der Dokumentation der Datensicherung
- Überprüfen des Datensicherungskonzepts

#### 3.5.2.3.2 Kompetenzfelder: Durchführen der Datensicherung und Überwachung

Fähigkeiten/Fertigkeiten

- Kontinuierliche Datensicherung durchführen können
- Notfallvorsorgen durchführen können
- Datensicherungskonzept überprüfen können
- Zeitgerechtes Handeln beschreiben können
- Dokumentieren können

Wissen

- Kenntnisse über gängige Datensicherungs- und Archivierungsverfahren und der Verwendung von Datensicherungsmedien und Sicherungsformen
- Techniken der Datensicherung kennen
- Kenntnisse über das einzusetzende Datensicherungskonzept
- Kenntnisse über die verwendeten Systemarchitekturen, Betriebssysteme und Softwaresysteme
- Kenntnisse bei der Verwendung von Referenzmodellen der Sicherung von Datenzuständen
- Kenntnisse bei der Planung von Prozessen und über organisatorische Auswirkungen
- Datensicherungshandbuch der Organisation
- Standards der Dokumentation in Bezug auf das Entwerfen von Richtlinien für die Datensicherung und das spätere Nachvollziehen von Datensicherungen
- Kenntnisse über verschiedene gängige Notfallvorsorgen
- Erfahrungen und Kenntnisse über datensicherungsstörende Ereignisse

Werkzeuge

- Betriebssystemeigene Datensicherungswerkzeuge
- Datensicherungssoftware
- Archivierungswerkzeuge

### **3.5.2.3.3 Beispiel: Durchführen der Datensicherung und Überwachung**

Um den Ausfall der Datensicherung so gering wie möglich zu halten, werden verschiedene Situationen am System getestet. So wird der Zugriff auf Datenbeständen einer zu sichern- den Datenbank während des Backups simuliert, um zu überprüfen, ob die Datensicherung abbricht oder fehlerfrei ausgeführt wird. Dann wird getestet ob die konfigurierte selbstständige Verzögerung der Datensicherung bei den Backupklienten einspringt, wenn der Backupserver zum Datensicherungszeitpunkt nicht zur Verfügung steht. Diese „Feuerwehübungen“ werden ebenfalls im Logbuch festgehalten. Da die Datensicherung automatisch abläuft, wird regelmäßig der Erfolg über die Logdateien der Datensicherung überprüft.



### 3.5.2.4 Wiederherstellen von Daten

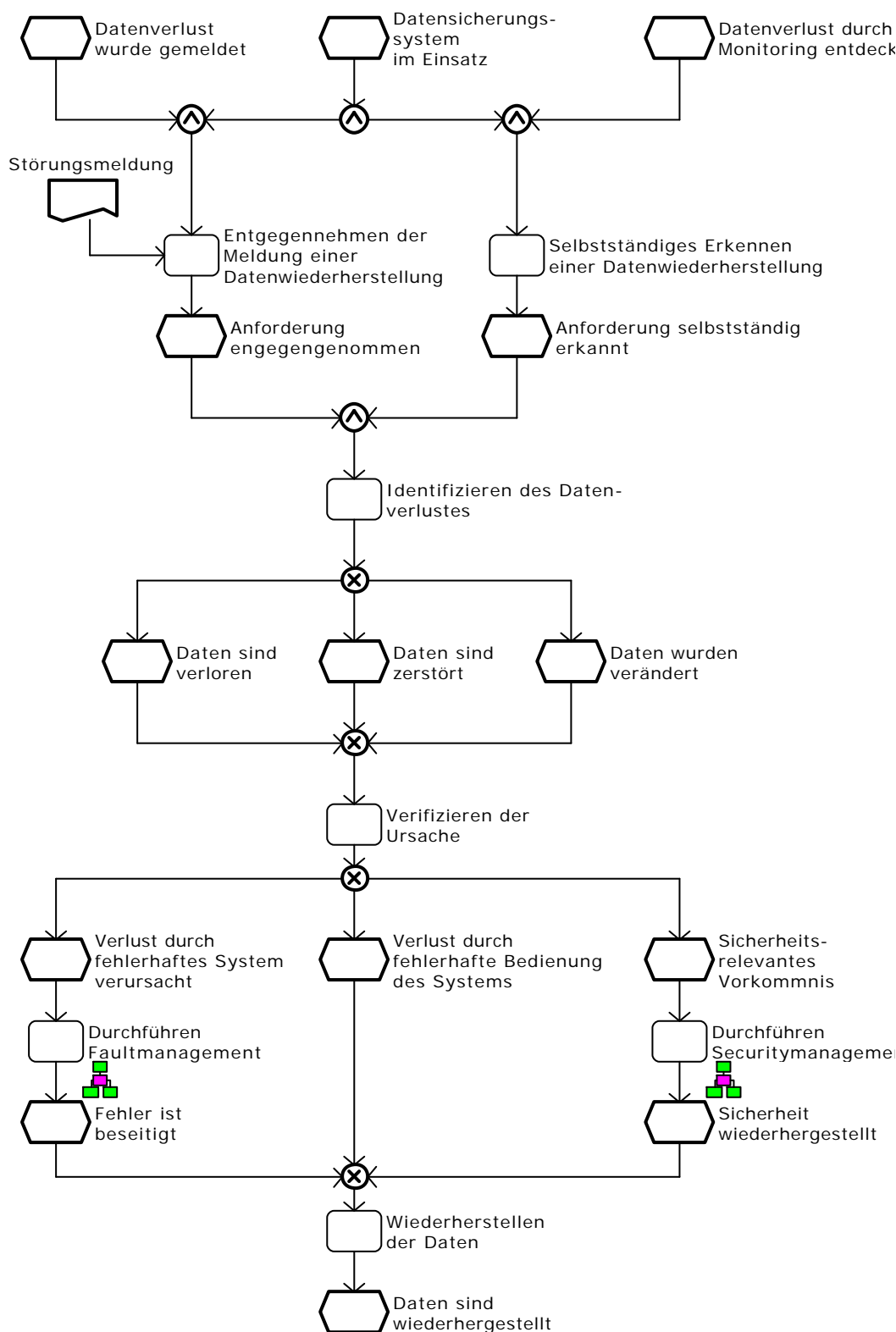


Abbildung 47: Wiederherstellen von Daten

Ist ein Datenverlust aufgrund eines Fehlers im System oder einer Sicherheitsverletzung aufgetreten oder hat ein Nutzer einen Verlust seiner Daten gemeldet, muss der IT Systems Administrator diesen zunächst analysieren. Ist die Art des Verlustes (Daten sind verloren, zerstört oder geändert worden) festgestellt, wird die Ursache bestimmt. Entstand der Verlust durch einen Fehler im oder am IT-System, stößt der IT Systems Administrator hierbei selbstständig das Fault-Management an und beseitigt somit die Fehlerursache (siehe auch 3.2ff.). Ist der Verlust durch ein sicherheitsrelevantes Vorkommnis entstanden, bedient sich der IT

Systems Administrator des Security-Managements (siehe 3.4ff.) und beseitigt das identifizierte Sicherheitsloch. In jedem Fall werden die Daten auf dem System wiederhergestellt.

#### **3.5.2.4.1 Tätigkeiten: Wiederherstellen der Daten**

Um eine Wiederherstellung der Daten durchführen zu können, muss der IT Systems Administrator folgende Tätigkeiten durchführen:

- Entgegennehmen der Meldung einer Datenwiederherstellung oder
- Selbstständiges Erkennen einer Datenwiederherstellung
- Identifizieren des Datenverlusts
- Verifizieren der Ursache

Ist der Verlust aufgrund eines fehlerhaften Systems entstanden:

- Durchführen Fault-Management

Ist der Verlust durch ein sicherheitsrelevantes Vorkommnis verursacht worden:

- Durchführen Security-Management

Auf jeden Fall:

- Wiederherstellen der Daten

#### **3.5.2.4.2 Kompetenzfelder: Wiederherstellen der Daten**

Fähigkeiten/Fertigkeiten

- Meldungen von Benutzern und System verstehen können und in prozessbezogenen Kontext bringen
- Art des Datenverlusts bestimmen können
- Ursachen eines Datenverlusts aufdecken können
- Security-Management durchführen können
- Fault-Management durchführen können
- Daten wiederherstellen können
- Dokumentieren können

Wissen

- Kenntnisse über gängige Datensicherungs- und Archivierungsverfahren und der Verwendung von Datensicherungsmedien und Sicherungsformen
- Techniken der Datensicherung kennen
- Kenntnisse über das einzusetzende Datensicherungskonzepts
- Kenntnisse über die verwendeten Systemarchitekturen, Betriebssysteme und Softwaresysteme
- Kenntnisse bei der Verwendung von Referenzmodellen zur Sicherung von Datenzuständen
- Kenntnisse bei der Planung von Prozessen und über organisatorische Auswirkungen
- Datensicherungshandbuch der Organisation
- Kenntnisse über wichtige Ursachen von Datenverlusten
- Standards der Dokumentation in Bezug auf das spätere Nachvollziehen von Datenwiederherstellungen
- Erfahrungen und Kenntnisse über datensicherungsstörende Ereignisse

Werkzeuge

- gängige Datenwiederherstellungssoftware und -hardware
- Diagnosesoftware

#### **3.5.2.4.3 Beispiel: Wiederherstellen der Daten**

Der Service der Systemadministration wird von einem Benutzer angerufen, dass seine Daten auf dem Server nicht mehr vorhanden sind. Der Systemadministrator nimmt den Hinweis zunächst auf und informiert über eine Rundmail, dass eventuell Daten von einem gemeinsamen Laufwerk vorübergehend nicht zur Verfügung stehen. Nach erneutem Nachfragen, wo sich die Daten ursprünglich befanden, stellt sich heraus, dass es sich um Daten des Applikationsservers (siehe Beispiel aus Kapitel 3.1ff: Change-Management) handelt. Der Sys-

temadministrator überprüft das Transaktionsprotokoll. Der letzte schreibende Zugriff stammt vom vorherigen Tag und seitdem wurde nicht wieder versucht die Datei zu öffnen. Nach einem Check des Festplattensystems stellt sich heraus, dass eine Festplatte Fehler in bestimmten Festplattensektoren hat und das automatische Korrekturprogramm eventuell diese Datei gelöscht hat. Es wird eine neue Platte aus dem Lager genommen und die fehlerhafte Platte ausgetauscht. Nachdem das System wieder hochgefahren ist, wird ein Backup auf die Platte gespielt. Danach wird mithilfe des Transaktionsprotokolls der Stand der Datei wie nach dem letzten Zugriff wiederhergestellt.

### **3.6 Benutzerverwaltung und Organisation**

---

Die Benutzerverwaltung beinhaltet zum einen die Erstellung und Pflege von Benutzerkonten und deren Rechte, die Umsetzung der Organisationsstruktur sowie der Richtlinien aus dem Security-Management, als auch die technische Beratung von nicht fachlichen Projektleitern bei der Projektplanung und dem Projektmanagement in den Bereichen des IT-Systems.

Zu den organisatorischen Aufgaben der IT Systems Administrator gehören zum einen der Aufbau und die Führung eines Supports und zum anderen die Organisation der gekauften Softwarelizenzen.

### 3.6.1 Der Referenzprozess „Benutzerverwaltung und Organisation“

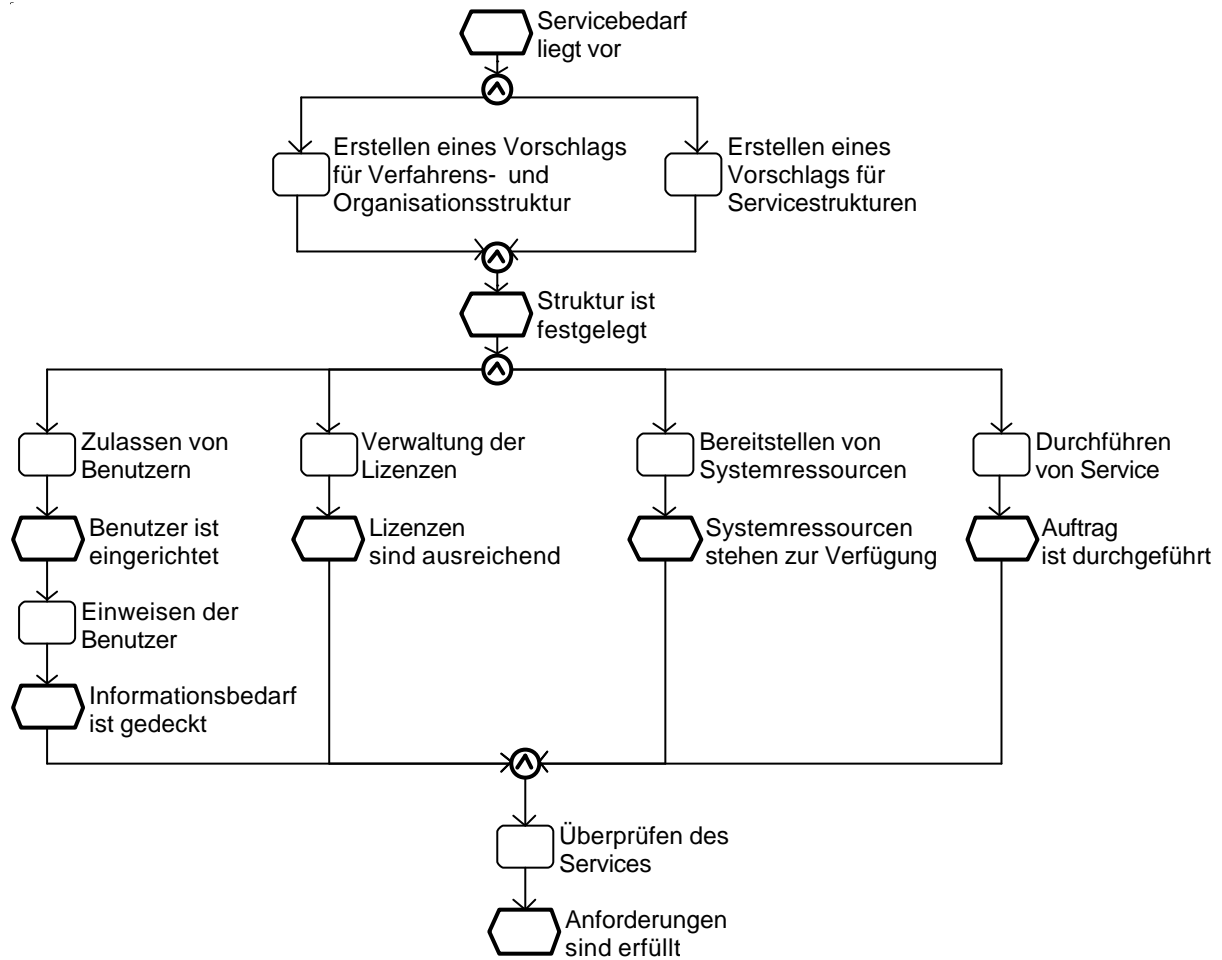


Abbildung 48: Referenzprozess Benutzerverwaltung und Organisation

### **3.6.2 Prozesskompass Benutzerverwaltung und Organisation**

Zusammenfassend besteht der Referenzprozess Benutzerverwaltung und Organisation aus den folgenden Teilprozessen:

1. Erstellen einer Verfahrens- und Organisationsstruktur
2. Erstellen eines Vorschlags für Servicestrukturen
3. Zulassen von Benutzern
4. Einweisen der Benutzern
5. Verwaltung der Lizenzen
6. Bereitstellen von Systemressourcen
7. Einrichten von Servicestrukturen
8. Sicherstellen der Servicequalität

### 3.6.2.1 Erstellen eines Vorschlages für Verfahrens- und Organisationsstrukturen

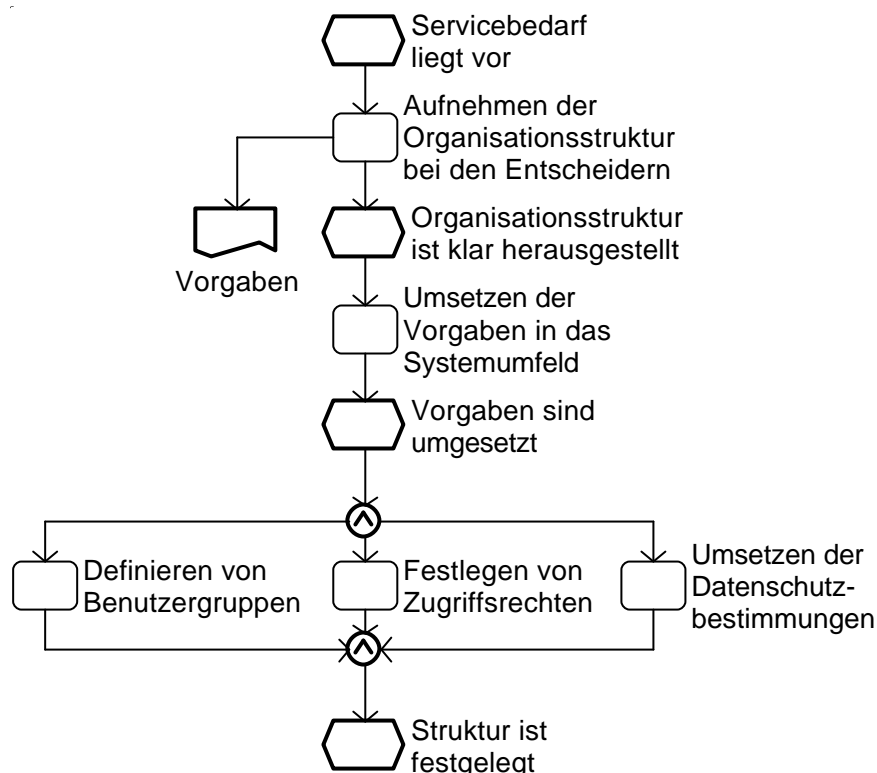


Abbildung 49: Erstellen eines Vorschlags für Verfahrens- und Organisationsstrukturen

Jeder Prozess der Organisation und Benutzerberatung beginnt mit der Erstellung eines Vorschlags für die Festlegung von Verfahrens- und Organisationsstrukturen im Systembetrieb. Dazu werden die Anforderungen an die Organisationsstruktur im IT-System bei den Entscheidern aufgenommen. Die daraus resultierenden Vorgaben werden in die Systemlandschaft umgesetzt. Dabei wird die Organisation auf personeller und systemspezifischer Ebene abgebildet. Daraus werden die notwendigen Benutzergruppen, die aus den Vorgaben resultierenden Zugriffsrechten abgeleitet und eingerichtet und die Datenschutzbestimmungen umgesetzt. Im Ergebnis ist die Struktur im Systemumfeld festgelegt.

#### 3.6.2.1.1 Tätigkeiten: Erstellen eines Vorschlags für Verfahrens- und Organisationsstrukturen

Um einen Vorschlag für Verfahrens- und Organisationsstrukturen für das IT-System zu erstellen, muss der IT Systems Administrator folgende Tätigkeiten durchführen:

- Aufnehmen der Organisationsstruktur bei den Entscheidern
- Umsetzen der Vorgaben in das Systemumfeld
- Definieren von Benutzergruppen
- Festlegen von Zugriffsrechten
- Umsetzen der Datenschutzbestimmungen
- Einrichten von Verzeichnisstrukturen

#### 3.6.2.1.2 Kompetenzfelder: Erstellen eines Vorschlags für Verfahrens- und Organisationsstrukturen

Fähigkeiten/Fertigkeiten

- Neue Bedürfnisse bei den Entscheidern aufnehmen können
- Bedürfnisse verstehen und in Verfahrens- oder Organisationsstrukturen übertragen können
- Vorgaben in das Systemumfeld übertragen können
- Benutzergruppen aus den Vorgaben ableiten können
- Zugriffsrechte aus den Vorgaben ableiten können
- Verzeichnisstrukturen anlegen können

- Datenschutzbestimmungen in das Systemumfeld umsetzen können
- Dokumentieren können

#### Wissen

- Kenntnisse bei der Planung von Prozessen und über organisatorische Auswirkungen
- Kenntnisse über Datenschutzbestimmungen
- Kenntnisse der betriebssystemeigenen Vergabe von Zugriffsrechten und deren Besonderheiten in der Einrichtung von Verzeichnisstrukturen
- Kenntnisse in der Verwendung von Standards der Dokumentation in der Erstellung von Vorgaben und Strukturen

#### Werkzeuge

- Textverarbeitung
- Informationsverteiler

### **3.6.2.1.3 Beispiel: Erstellen eines Vorschlags für Verfahrens- und Organisationsstrukturen**

Hier dient ebenfalls das Beispiel auf dem Kapitel 3.1ff. Change-Management: Nachdem die Server und die Klienten installiert und konfiguriert wurden, müssen die Vorgaben aus dem vorliegenden Organigramm umgesetzt werden. Aus diesem wird ein Rechtediagramm abgeleitet, welches später in den einzelnen Zugriffskontrolllisten der Domino-Anwendungen übertragen werden muss. Da jeder Mitarbeiter einen eigenen Bereich für seine Korrespondenzen erhalten soll, andere Kollegen jedoch immer auf dem laufenden sein müssen, werden diese Rechte ebenfalls zunächst im Rechtediagramm eingepflegt. Des Weiteren soll für die reibungslose Kommunikation und Kooperation ein Gruppenkalender für jede Abteilung eingerichtet werden.

Aus diesen Anforderungen werden Benutzergruppen abgeleitet. So wird für jede Abteilung eine separate Gruppe angelegt, dann werden die Abteilungsleiter in einer Gruppe zusammengefasst und zum Schluss werden Benutzer Gruppen nach ihrer Funktion zugeordnet. Diesen Gruppen werden Rechte zugeordnet, die den ausschließlich berechtigten Datenzugriff sowie das Ausführen von Agenten, das Erstellen von Repliken auf dem Server und auf dem Klienten und das Ändern von Gestaltungselementen in den einzelnen Datenbanken sicherstellen bzw. verweigern sollen. Für kritische Anwendungen werden neben den erlaubten Zugriffen auch Negativlisten erstellt, die aus dem Rechtediagramm abgeleitet wurden.



### 3.6.2.2 Erstellen eines Vorschlag für Servicestrukturen

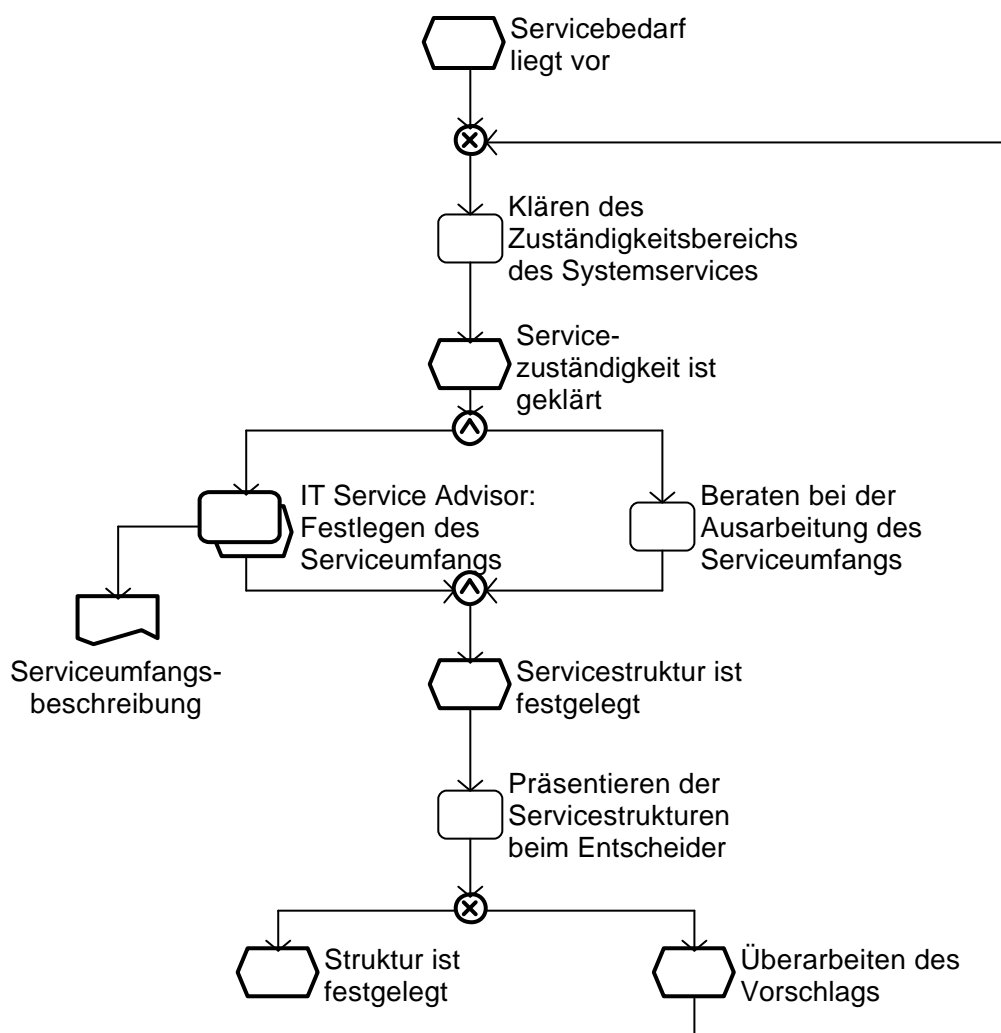


Abbildung 50: Erstellen eines Vorschlags für Servicestrukturen

Neben dem Prozess „Erstellen eines Vorschlags für Verfahrens- und Organisationsstrukturen“ beginnt jede Benutzerberatung und Organisation mit der Erstellung eines Vorschlag für die Einrichtung von Servicestrukturen. Dazu müssen die Zuständigkeiten für den Systemservice geklärt werden. In Zusammenarbeit mit dem IT Service Advisor wird der Umfang des zu leistenden Services festgelegt. Nachdem diese Festlegung erfolgt ist, wird der Vorschlag für die Servicestrukturen den Entscheidern präsentiert. Im Ergebnis ist die Servicestruktur festgelegt.

#### 3.6.2.2.1 Tätigkeiten: Erstellen eines Vorschlags für Servicestrukturen

Um einen Vorschlag für die Servicestrukturen zu erstellen, muss der IT Systems Administrator folgende Tätigkeiten durchführen:

- Klären des Zuständigkeitsbereichs des Systemservices
- Zusammen mit dem IT Service Advisor: Festlegen des Serviceumfangs
- Beraten bei der Ausarbeitung des Serviceumfangs
- Präsentieren der Servicestrukturen beim Entscheider

#### 3.6.2.2.2 Kompetenzfelder: Erstellen eines Vorschlags für Servicestrukturen

Fähigkeiten/Fertigkeiten

- Zuständigkeitsbereich des Systemservices abschätzen und bestimmen können
- Serviceumfang mit IT Service Advisor festlegen können

- Präsentieren können
- Dokumentieren können

Wissen

- Kenntnisse bei der Planung von Prozessen und über organisatorische Auswirkungen
- Kenntnisse und Erfahrungen bei der Vorbereitung und Durchführung von Präsentationen
- Kenntnisse in der Verwendung von Standards der Dokumentation in der Erstellung von Vorgaben und Strukturen

Werkzeuge

- Präsentationssoftware

### **3.6.2.2.3 Beispiel: Erstellen eines Vorschlags für Servicestrukturen**

Parallel wird initial ein Vorschlag von eventuell durchzuführenden Serviceaufträgen erstellt. Dabei müssen verbindliche Vereinbarungen formuliert werden, welcher IT-Dienst in welcher Qualität, zum Beispiel hinsichtlich Verfügbarkeit, Bandbreiten, Reaktionszeiten und Event-Management, zu welchen Kosten erbracht werden soll. Diese werden in sogenannte Service Level Agreements (SLA) zusammengetragen. Dabei wird aktiv auf die Fachabteilungen zugegangen und mit den Abteilungsleitern gesprochen, um so die Wünsche der Benutzer zu erforschen. Daraus werden die Anforderungen an die Leistungen formuliert und an den Erfordernissen der Serviceabnehmer (Benutzer) ausgerichtet. Zusammen mit der Geschäftsleitung wird ein akzeptabler Kompromiss zwischen den Forderungen der Benutzer und der wirtschaftlichen Machbarkeit ihrer Realisierung erarbeitet.

So wird eine Helpdesk eingerichtet, die unter anderem Fragen und Fehlfunktionen im Dominosystem aufnimmt und an die entsprechenden Administratoren weiterleitet. Um den erforderlichen Gesamtüberblick zu wahren, werden sogenannte Frameworks eingesetzt. Diese bieten gegenüber den für die Überwachung einzelner Komponenten den Vorteil, dass sie Statusinformationen über das gesamte Netz liefern können. Flankierend werden, um den Implementierungsaufwand zu minimieren, zusätzlich Third-Party-Lösungen integriert.

### 3.6.2.3 Zulassen von Benutzern

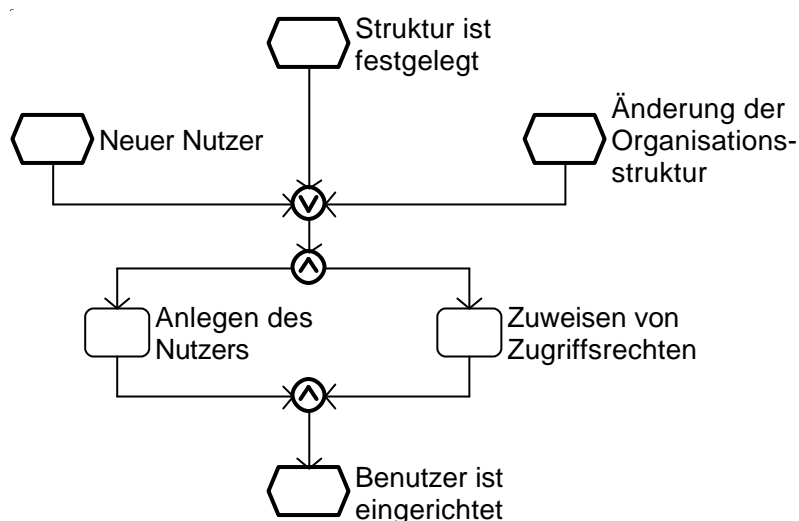


Abbildung 51: Zulassen von Benutzern

Tritt ein neuer Benutzer in die Organisation ein oder wird diese neu strukturiert, muss der IT Systems Administrator die Zugriffsrechte neu anpassen und (bei einem neuen Benutzer) den neuen Nutzer anlegen und ihn nach den Vorgaben der Verfahrens- und Organisationsstruktur in die entsprechende Benutzergruppe oder dem Profil eintragen. Im Ergebnis ist der neue Benutzer eingerichtet bzw. sind die neuen Vorgaben in der Rechteverwaltung des Systems umgesetzt.

#### 3.6.2.3.1 Tätigkeiten: Zulassen von Benutzern

Um einen neuen Benutzer zuzulassen, muss der IT Systems Administrator folgende Tätigkeiten durchführen:

- Anlegen des Nutzers
- Zuweisen von Zugriffsrechten

#### 3.6.2.3.2 Kompetenzfelder: Zulassen von Benutzern

Fähigkeiten/Fertigkeiten

- Neue Nutzer anlegen können
- Zugriffsrechte zuweisen können
- In erforderliche Benutzergruppe eintragen können
- Eventuell Verzeichnisse aktualisieren können
- Neue organisatorische Anforderungen in die Benutzerverwaltung übertragen können
- Dokumentieren können

Wissen

- Kenntnisse und Erfahrungen in der Verwendung von Verfahrens- und Organisationsstrukturen
- Kenntnisse bei der Planung von Prozessen und über organisatorische Auswirkungen
- Kenntnisse im Einsatz von Anmeldeskripten
- Kenntnisse im Entwurf von Profilen für die Zugriffsvergabe
- Kenntnisse in der Verwendung von Standards der Dokumentation in der Erstellung von Vorgaben und Strukturen

Werkzeuge

- Verzeichnisse
- Verwaltungswerkzeuge

#### **3.6.2.3.3 Beispiel: Zulassen von Benutzern**

Dass die Benutzer sich am Domino-Server anmelden können, muss zunächst für jeden Benutzer eine sogenannte ID erzeugt werden. Um den Migrationsaufwand so gering wie nötig zu halten, wird die Active-Directory-Struktur der Windows 2000 Domäne importiert. Da zu diesem Zeitpunkt feststeht, welche Benutzergruppe Zugriff zu welchen Datenbanken haben soll, wird über ein Template die jeweilige Vorlage direkt bei der Registrierung eingebunden. Aus Sicherheitsgründen wird die Laufzeit der ID zunächst auf zwei Jahre gesetzt. Da der reibungslose Zugriff auf alle Domino-Server gewährleistet werden kann, werden die einzelnen Benutzer-IDs mit den Zertifizierungsschlüsseln der anderen Server gegenzertifiziert. Für die persönliche Maildatenbank erhalten sie Managerrechte.

Um einen Wildwuchs von Datenbanken auf den Servern zu vermeiden, werden nur berechnigte Benutzer über eine separate Benutzergruppe das Recht zugesprochen, Repliken und neue Datenbanken auf den Servern zu erstellen. Alle anderen Benutzer werden in eine Negativliste aufgenommen, die explizit keine weiteren Datenbanken erzeugen kann.

### 3.6.2.4 Einweisen der Benutzer

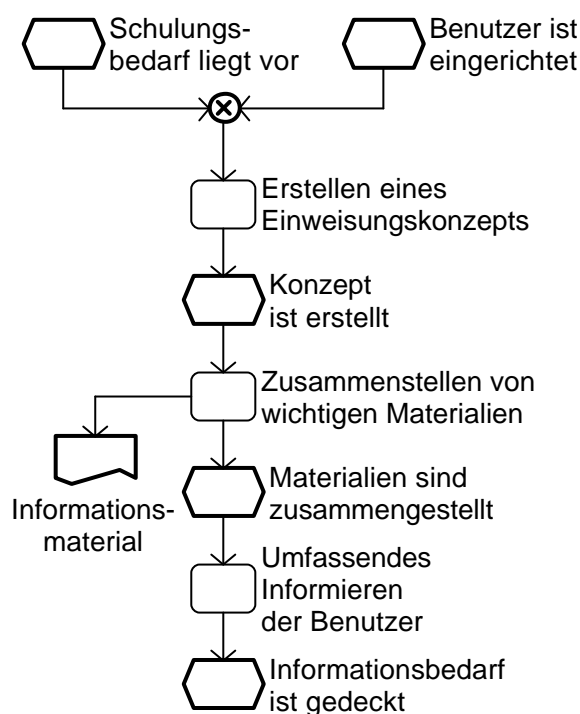


Abbildung 52: Einweisen der Benutzer

Dieser Prozess ist als prozessbegleitende Tätigkeit zu verstehen, die alle anderen Referenz- und Teilprozesse parallel begleitet und dort unter dem Namen „Informieren betroffener Stellen/Personen“ läuft. Benutzer müssen immer dann geschult bzw. informiert werden, wenn Änderungen am IT-System, bei den Richtlinien und bei Störungen des Geschäftsbetriebes erfolgten. Handelt es sich dabei um grundlegende Änderungen oder muss ein neuer Nutzer in das bestehende System eingeführt werden, erstellt der IT Systems Administrator einen Schulungsplan, trägt danach die benötigten Unterlagen zusammen und führt im Anschluss dazu eine Einweisung oder Schulung durch. Erst wenn der Benutzer alle Informationen besitzt, die er für den täglichen Arbeitsablauf benötigt, ist der Prozess beendet.

#### 3.6.2.4.1 Tätigkeiten: Einweisen der Benutzer

Um Benutzer in das Systemumfeld einzuweisen, muss der IT Systems Administrator folgende Tätigkeiten durchführen:

- Erstellen eines Schulungsplans
- Zusammenstellen von wichtigen Materialien
- Umfassendes Informieren der Benutzer

#### 3.6.2.4.2 Kompetenzfelder: Einweisen der Benutzer

Fähigkeiten/Fertigkeiten

- Schulungsplan erstellen können
- Relevante Schulungsunterlagen identifizieren und zusammenstellen können
- Schulungen durchführen können

Wissen

- Kenntnisse bei der Planung von Prozessen und über organisatorische Auswirkungen
- je nach Informationsbedarf Kenntnisse über relevante Themen, die den Nutzer betreffen können

#### **3.6.2.4.3    *Beispiel: Einweisen der Benutzer***

Um den Serviceaufwand so gering wie nur irgend möglich zu halten, wird eine FAQ-Liste in das Intranet gestellt, die die häufigst gestellten Fragen in der Bedienung von Lotus Notes beantworten soll. Des Weiteren werden regelmäßige Schulungen im Umgang mit Lotus Notes angeboten und eine kurze Bedienungsanleitung erstellt. Den Mitarbeitern, die in der Außenstelle arbeiten wird noch der Umgang mit Repliken erklärt, da diese nicht immer einen direkten Zugriff zum zentralen Domino-Server besitzen.

### 3.6.2.5 Verwaltung der Lizenzen

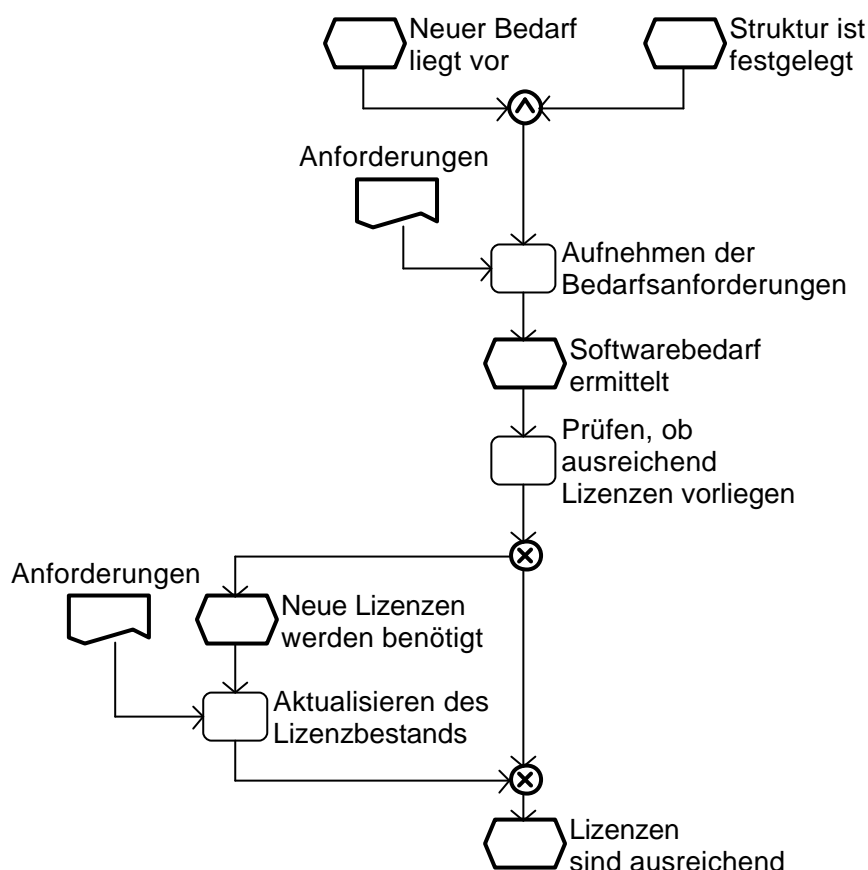


Abbildung 53: Verwaltung der Lizenzen

Während das System in Betrieb ist, bei einer Veränderung der Organisationsstruktur, bei der Durchführung des Change-Managements oder beim Eintreten eines neuen Benutzers in die Organisation, entsteht ein neuer Bedarf an Softwarelizenzen. Diese neuen Anforderungen werden vom IT Systems Administrator aufgenommen. Danach überprüft er, ob noch ausreichend Lizenzen für die entsprechenden Softwarekomponenten vorhanden sind. Werden weitere Lizenzen benötigt, besorgt er diese und aktualisiert den Lizenzbestand. Im Ergebnis liegt eine ausreichende Anzahl von Lizenzen vor.

#### 3.6.2.5.1 Tätigkeiten: Verwaltung der Lizenzen

Folgende Tätigkeiten muss der IT Systems Administrator durchführen, um Lizenzen für sein zu administrierendes System zu verwalten:

- Aufnehmen der Bedarfsanforderungen
- Prüfen, ob ausreichend Lizenzen vorliegen

Falls neue Lizenzen benötigt werden

- Aktualisieren des Lizenzbestands

#### 3.6.2.5.2 Kompetenzfelder: Verwaltung der Lizenzen

Fähigkeiten/Fertigkeiten

- Bedarfsanforderungen aufnehmen können
- Auf ausreichendes Vorhandensein von Lizenzen prüfen können
- Neue Lizenzen besorgen können
- Lizenzbestand aktualisieren können
- Zukünftigen Bedarf abschätzen können
- Dokumentieren können

Wissen

- Kenntnisse bei der Planung von Prozessen und über organisatorische Auswirkungen
- Kenntnisse über die eingesetzten Softwarelizenzbestimmungen
- Standards der Dokumentation in Bezug auf das Nachvollziehen von Prozessschritten kennen und der daraus resultierenden Beschaffungsmaßnahmen neuer Lizenzen

#### **3.6.2.5.3 Beispiel: Verwaltung der Lizenzen**

Für den reibungslosen Betrieb sind eine Reihe von Lizenzen nötig. Die Abwicklung wird über das IBM eigene Passport II Programm abgewickelt. Damit wurden in der Vergangenheit bereits gute Erfahrungen gesammelt.

Für die Mailserver ist jeweils ein Messaging-Server, für den Servercluster jeweils ein Enterprise-Server und für den Domino-Server, der sich außerhalb der DMZ befindet ein Applikationsserver notwendig. Des Weiteren müssen für die Benutzer jeweils eine Lotus-Notes-Klienten-Lizenz besorgt werden. Für die Systemadministration jeweils eine Lotus-Dominio-Lizenz (die eine Lotus-Notes-Klient-Lizenz enthält) und für die Lotus-Notes-Entwickler eine Domino-Designer-Lizenz (die ebenfalls eine Lotus-Notes-Klient-Lizenz enthält). Diese werden in die bereits vorhandene Lizenzdatenbank eingetragen. Über den Dienst im Domino-Server lassen sich die Verwendung der Lizenzen überwachen und eventuell können daraus neue Bedarfsanforderungen abgeleitet werden. Für den zu erwartenden Neuzugang von Mitarbeitern wird bereits eine ausreichende Anzahl von Lizenzen besorgt.



### 3.6.2.6 Bereitstellen von Systemressourcen

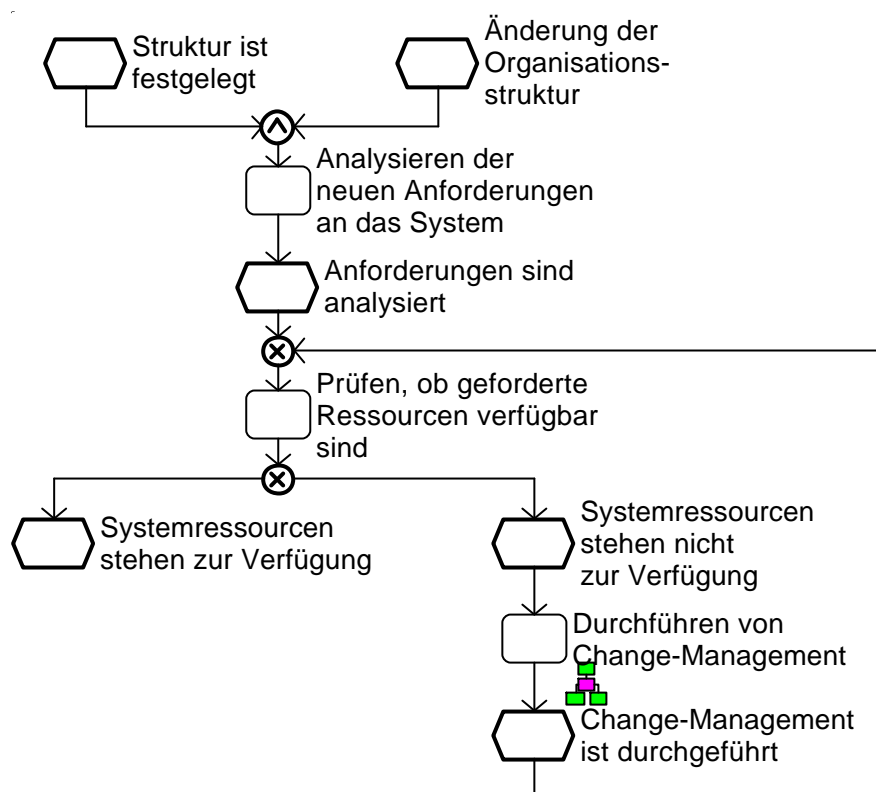


Abbildung 54: Bereitstellen von Systemressourcen

Treten neue Anforderungen an das System auf, müssen diese zunächst vom IT Systems Administrator analysiert werden. Danach wird von ihm geprüft, ob diese Anforderungen mit den derzeit zur Verfügung stehenden Ressourcen erfüllbar sind. Sind diese Anforderungen mit den existierenden Ressourcenangebot nicht realisierbar, muss der IT Systems Administrator ein Change-Management durchführen, um die notwendigen Ressourcen bereitzustellen.

#### 3.6.2.6.1 Tätigkeiten: Bereitstellen von Systemressourcen

Um die notwendigen Systemressourcen bereitzustellen, muss der IT Systems Administrator folgende Tätigkeiten durchführen:

- Analysieren der neuen Anforderungen an das System
- Prüfen, ob geforderte Ressourcen verfügbar sind

Stehen die Systemressourcen nicht zur Verfügung:

- Durchführen Change-Management

#### 3.6.2.6.2 Kompetenzfelder: Bereitstellen von Systemressourcen

Fähigkeiten/Fertigkeiten

- Anforderungen an das System analysieren können
- Zukünftigen Bedarf abschätzen können
- Ressourcenverfügbarkeit prüfen und beurteilen können
- Change-Management durchführen können
- Dokumentieren können

Wissen

- Betriebsarten von Systemen und benutzter Hardware kennen
- Kenntnisse über die sich im Einsatz befindenden System- und Kommunikationsarchitekturen und deren Abhängigkeiten untereinander

- Grundlegende Kenntnisse in der Organisation, Dimensionierung, Topologien und Komponenten von Netzwerken
- Besonderheiten von Datenübertragungssystemen und –techniken sowie der verwendeten Hardwareschnittstellen
- Kenntnisse von Hardwarestandards und Standards der Konfiguration von Hardwaresystemen
- Kenntnisse bei der Planung von Prozessen und über organisatorische Auswirkungen
- Kenntnisse über die verwendeten Systemarchitekturen, Betriebssysteme und gängiger Datensicherungstechniken
- Standards der Dokumentation in Bezug auf die Verwaltung von zur Verfügung stehenden Systemressourcen und den eventuell daraus resultierenden Anforderungen für eine Ausweitung der Ressourcen
- Kenntnisse bei der Planung von Prozessen und Projekten sowie über organisatorische Auswirkungen
- Standards der Dokumentation für die Planungsabläufe von Projekten kennen
- Betriebswirtschaftliche Grundkenntnisse in der Kosten- und Nutzenanalyse und der Bedarfsschätzung

#### Werkzeuge

- Kaufmännische Software
- Diagnose- und Prognosesoftware
- Kalkulationssoftware

#### **3.6.2.6.3 Beispiel: Bereitstellen von Systemressourcen**

Wie im Beispiel 3.1ff. des Changemanagement beschrieben, müssen für den Betrieb der Lotus-Domino-Domäne eine Reihe von Anschaffungen getätigt werden. Diese dienen der Bereitstellung aller Funktionen des neuen Systems.

Nachdem das System installiert, konfiguriert und ausgiebig getestet wurde, wird abschließend überprüft, ob die Anforderungen erfüllt wurden und alle Ressourcen den Benutzern zur Verfügung stehen.

### 3.6.2.7 Durchführen von Service

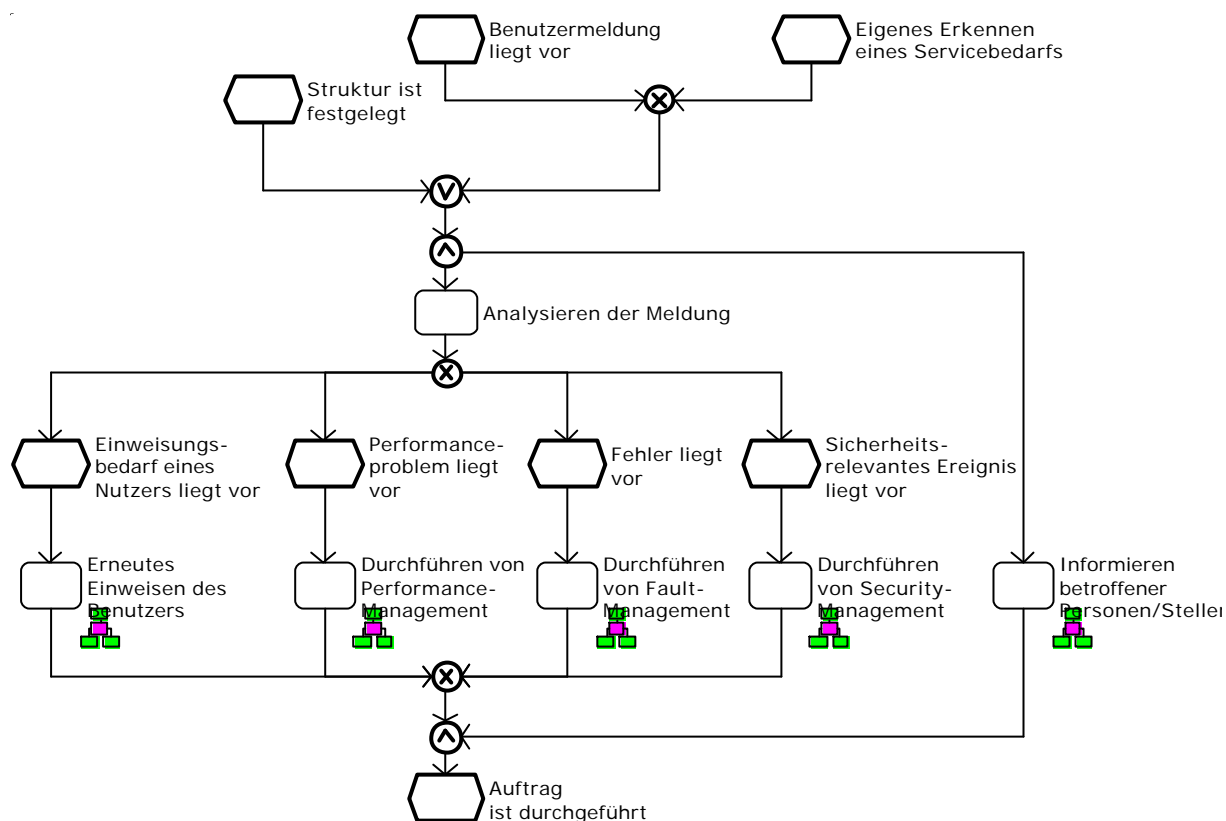


Abbildung 55: Durchführen von Service

Nachdem die Strukturen für den Service festgelegt sind, werden diese in konkrete Handlungen umgesetzt. Im laufenden Betrieb kann es zu Beeinträchtigungen der Verfügbarkeit von Ressourcen im IT-System kommen. Diese werden durch den IT Systems Administrator selbst identifiziert, können aber auch durch eine Meldung eines Benutzers angezeigt werden.

Zunächst informiert der IT Systems Administrator alle betroffenen Stellen und Personen bzw. die gesamte Organisation über den derzeitigen Umfang der zu erwartenden Störung, über den Zustand des Systems und eventuell über zu erfolgende Tätigkeiten. Als nächstes analysiert er die Meldung und identifiziert entweder ein Performanzproblem, einen Systemfehler oder ein sicherheitsrelevantes Ereignis. Daraufhin führt er Performance-, Fault- oder Security-Management durch und informiert erneut die betroffenen Stellen und Personen über den Erfolg der durchgeführten Tätigkeiten und den eventuell daraus resultierenden Änderungen für die Ressourcenverfügbarkeit. Im Ergebnis ist der Service durchgeführt und es ergeben sich eventuell neue Anforderungen an die bestehenden Servicestrukturen.

#### 3.6.2.7.1 Tätigkeiten: Durchführen von Service

Um den Service durchführen zu können muss der IT Systems Administrator folgende Tätigkeiten durchführen:

- Analysieren der Meldung

Hat der Benutzer das System falsch bedient:

- Erneutes Einweisen des Benutzers

Liegt ein Performanceproblem vor:

- Durchführen von Performance-Management

Liegt ein Fehler vor:

- Durchführen von Fault-Management

Liegt ein sicherheitsrelevantes Ereignis vor:

- Durchführen von Security-Management

Auf jeden Fall:

- Informieren betroffener Personen/Stellen

#### **3.6.2.7.2 Kompetenzfelder: Durchführen von Service**

Fähigkeiten/Fertigkeiten

- Servicebedarf erkennen
- Informationsbedarf von Personen und Stellen erkennen und deren Bedarf decken können
- Benutzeranliegen verstehen können
- Service durchführen können, im Speziellen je nach Bedarf Performance-, Fault- oder Security-Management durchführen können
- Dokumentieren können

Wissen

- Grundkenntnisse einer Qualitätssicherung und – management
- Erfahrungen und Kenntnisse in der Interpretation von Benutzer- und Systemmeldungen
- je nach Servicebedarf Kenntnisse über wichtige Themen, die den Service betreffen

Werkzeuge

- Trouble-Ticket-Systeme
- Betriebssystemeigene Werkzeuge
- Geräte für den Empfang von Meldungen, wie Pager, SMS oder Telefon
- Informationsverteiler

#### **3.6.2.7.3 Beispiel: Durchführen von Service**

- Wie im 3.2.2.3 Beispiel: Durchführen kontinuierlicher Überwachung beschrieben, geht eine Fehlermeldung beim Service über die Helpdesk ein. Nach eingehender Recherche der Statusmeldungen und weiterer Nachfragen bei den betroffenen Benutzern, wird von einem Hardwarefehler ausgegangen, welcher im o.g. Beispiel behoben wird. Und wie in 3.2.2.10 Beispiel: Informieren betroffener Stellen/Personen beschrieben, werden die für die Behebung der Störung benötigte externe Personal angerufen und die betroffenen Stellen im Unternehmen informiert.

### 3.6.2.8 Überprüfen des Services

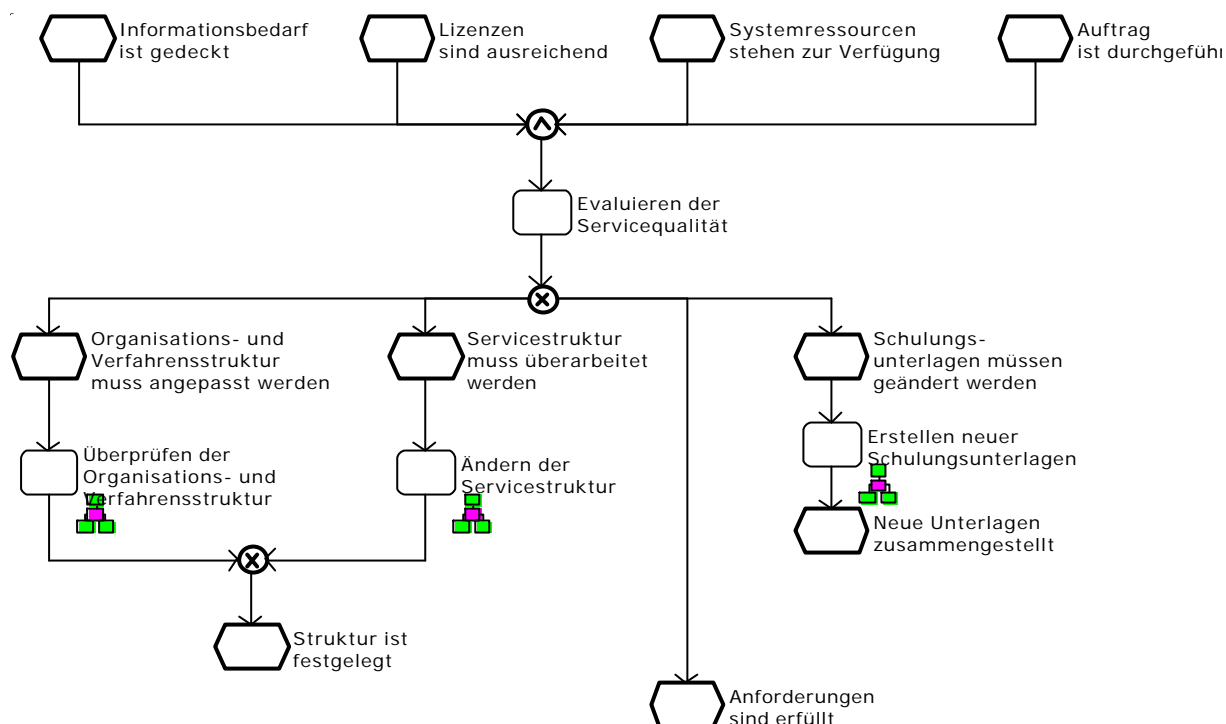


Abbildung 56: Überprüfen des Services

Wurde der Service durchgeführt, sollte er auf seine Qualität regelmäßig überprüft werden. Durch die Evaluation müssen entweder die neuen Anforderungen an die bestehende Organisations-, Verfahrens- und Servicestruktur umgesetzt werden, die vorhandenen Schulungsunterlagen überarbeitet werden oder es bedarf keiner Änderung und alle Anforderungen sind erfüllt.

#### 3.6.2.8.1 Tätigkeiten: Überprüfen des Services

Um den Service zu überprüfen, muss der IT Systems Administrator folgende Tätigkeiten durchführen:

- Evaluieren der Servicequalität

Wenn die vorhandene Organisations- und Verfahrensstruktur angepasst werden muss:

- Überprüfen der Organisations- und Verfahrensstruktur

Wenn die vorhandene Servicestruktur angepasst werden muss:

- Ändern der Servicestruktur

Wenn Schulungsunterlagen geändert werden müssen:

- Erneutes Zusammenstellen von Informationsmaterialien

#### 3.6.2.8.2 Kompetenzfelder: Überprüfen des Services

Fähigkeiten/Fertigkeiten

- Servicequalität evaluieren können
- Vorhandene Organisations- und Verfahrensstruktur überprüfen können
- Vorhandene Servicestruktur überprüfen können
- Relevante Schulungsunterlagen identifizieren und zusammenstellen können
- Dokumentieren können

Wissen

- Kenntnisse gängiger Qualitätssicherungsmaßnahmen
- Kenntnisse und Erfahrung in der Durchführung von Schulungen und Einweisungen in das eingesetzte IT-System

- Kenntnisse der Planung von Prozessen und der Auswirkung auf die Organisation
- Kenntnisse der Verwendung von Dokumentationsstandards in Bezug auf die Ermittlung des zukünftigen Bedarfs innerhalb der Benutzerberatung und der Organisation

#### **3.6.2.8.3 Beispiel: Überprüfen des Services**

Da die Behebung des Festplattenfehlers zu lang gedauert hat, wird über eine Revision der derzeitigen Servicestrukturen nachgedacht.

So werden, wie im 3.2.2.9 Beispiel: Erstellen einer Prozessdokumentation beschreiben, alle Dokumente und Serviceverträge mit externen Partnern digitalisiert, um so einen schnelleren Zugriff zu gewährleisten. Des Weiteren werden Festplatten auf Lager gekauft, um schnell auf Festplattenausfälle reagieren zu können.

Die Informationen, die die Mitarbeiter von der Systemadministration während des Vorfalls erhielten, waren zu spärlich und es dauerte entschieden zu lang. Dies war unter anderem durch ein Personalmangel in der Systemadministration verursacht worden. Im Gespräch mit der Geschäftsleitung wurden zwei Alternativen abgewogen. Zum einen soll durch das Neueinstellen eines weiteren Systemadministrators die Antwortzeiten verkürzt werden oder zum anderen müssen die SLA's verändert werden. Die Geschäftsleitung entscheidet sich zunächst für die Änderung der SLA's und will somit für einen bestimmten Zeitraum diese Maßnahme überprüfen, bevor sie sich für eine Neueinstellung entschließt.

Auf jeden Fall wird, für das schnellere Melden von Fehlern am Domino-System ein Trouble-Ticket-System implementiert. Um die Fehlerdiagnose zu vereinfachen, müssen die Benutzer bereits im Vorfeld festlegen, welche Fehlerart eventuell vorliegt. Dazu werden im Trouble-Ticket-System Kategorien vorgegeben.