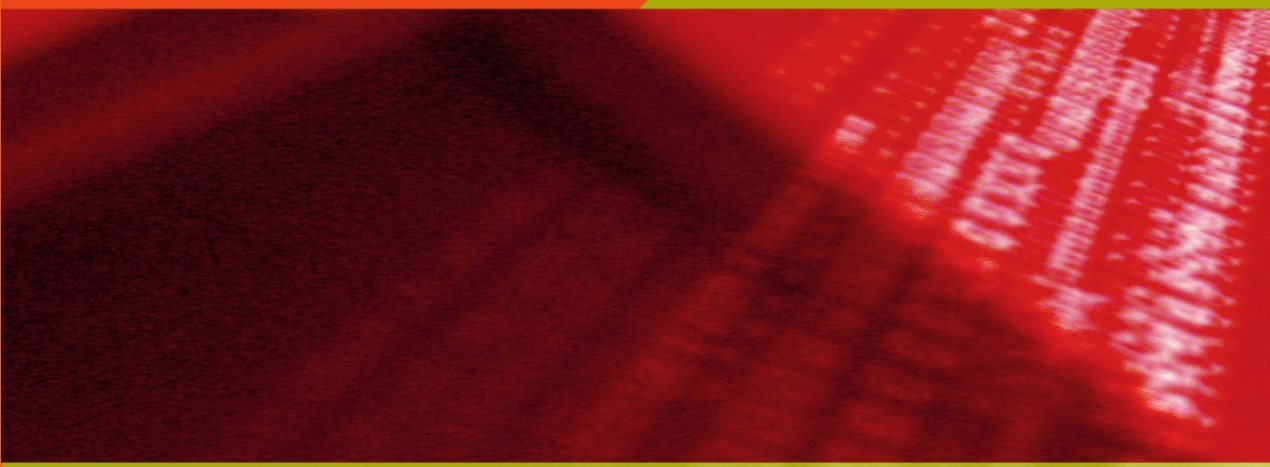
Gerhard Klett | Klaus-Werner Schröder | Heinrich Kersten

IT-Notfallmanagement mit System

Notfälle bei der Informationsverarbeitung sicher beherrschen

PRAXIS



VIEWEG+ TEUBNER

‹kes›

Gerhard Klett | Klaus-Werner Schröder | Heinrich Kersten

IT-Notfallmanagement mit System

Gerhard Klett | Klaus-Werner Schröder | Heinrich Kersten

IT-Notfallmanagement mit System

Notfälle bei der Informationsverarbeitung sicher beherrschen

Mit 17 Abbildungen und 14 Tabellen

PRAXIS

VIEWEG+
TEUBNER

Bibliografische Information der Deutschen Nationalbibliothek
Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der
Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über
<http://dnb.d-nb.de> abrufbar.

Höchste inhaltliche und technische Qualität unserer Produkte ist unser Ziel. Bei der Produktion und Auslieferung unserer Bücher wollen wir die Umwelt schonen: Dieses Buch ist auf säurefreiem und chlorfrei gebleichtem Papier gedruckt. Die Einschweißfolie besteht aus Polyäthylen und damit aus organischen Grundstoffen, die weder bei der Herstellung noch bei der Verbrennung Schadstoffe freisetzen.

1. Auflage 2011

Lektorat: Christel Roß | Maren Mithöfer

Vieweg+Teubner Verlag ist eine Marke von Springer Fachmedien.
Springer Fachmedien ist Teil der Fachverlagsgruppe Springer Science+Business Media.
www.viewegteubner.de

Umschlaggestaltung: KünkelLopka Medienentwicklung, Heidelberg
Druck und buchbinderische Verarbeitung: AZ Druck und Datentechnik, Berlin
Gedruckt auf säurefreiem und chlorfrei gebleichtem Papier
Printed in Germany

ISBN 978-3-8348-1288-9

Vorwort

Viele Organisationen (Unternehmen, Behörden,...) haben die Notwendigkeit eines Sicherheitsmanagements für ihre Informationsverarbeitung erkannt und bereits wichtige Schritte unternommen: Es wurden mögliche Sicherheitsvorfälle nach Eintrittshäufigkeit und Schadenhöhe analysiert und daraus Risiken für die Organisation abgeleitet, klassifiziert und bewertet. Zumindest höhere Risiken wurden durch geeignete *präventive* Maßnahmen unter eine noch akzeptable Grenze gedrückt.

Dies heißt natürlich *nicht*, dass die entsprechenden Sicherheitsvorfälle nicht mehr eintreten können: Präventive Maßnahmen können Sicherheitsvorfälle nicht gänzlich ausschließen – und verursachen zudem Kosten. Aus den gewählten Kompromissen zwischen Sicherheit und Wirtschaftlichkeit resultieren somit stets unterschiedlich hohe *Restrisiken*, die es weiter zu behandeln gilt. Behandeln kann dabei z. B. heißen, Risiken auf Dritte zu verlagern oder zu versichern.

Nimmt man sich die Ergebnisse der Risikoanalyse und -bewertung vor, so erkennt man schnell, welche Risiken bei ihrem Eintritt einen *gravierenden oder sogar existenzbedrohenden Schaden* nach sich ziehen können – womit wir im Grunde auch schon die Definition des Wortes *Notfall* festgelegt haben: Der Eintritt eines Vorfalls dieser Kategorie stellt in der Regel den klassischen *Notfall* dar.

Dort, wo es ein Sicherheitsmanagement der skizzierten Art nicht gibt, wird man im Zuge der *Unternehmensvorsorge* mögliche Sicherheitsvorfälle mit mindestens gravierenden Auswirkungen auf die Geschäftstätigkeit erfassen, analysieren und einer geeigneten Behandlung zuführen. Dies umschreibt die Aufgabe eines *separaten* Notfallmanagements.

Um welche Vorfälle handelt es sich in diesen kritischen Kategorien? Dazu einige Beispiele:

– Beim Ausfall wichtiger IT-Anwendungen und IT-Systemen geht es darum, möglichst schnell wieder in einen *Normalzustand* zu kommen, ggf. auch mithilfe einer Überbrückung durch einen *Notbetrieb*.

- Manipulationen an Daten und Anwendungen durch einen Innentäter sind erkannt worden; Ziel muss es sein, dessen Aktivitäten so schnell wie möglich zu unterbinden und auf einen *sicheren früheren Stand* der Daten und Anwendungen aufzusetzen.
- Bei Ausfall eines Dienstleisters (z. B. Netzwerk-Provider) sollen durch "Umschaltung" auf einen anderen Dienstleister *Verluste und Ausfallzeiten minimiert* werden.
- Durch bekannt gewordenen Diebstahl vertraulicher Informationen wird das Image der Organisation massiv gefährdet; hier kann es nur darum gehen, kurzfristig Sicherheitslücken zu stopfen und durch entsprechende *präventive Maßnahmen* erneut Vertrauen bei den Kunden aufzubauen.
- Wird aufgrund fehlender Compliance bei einem Rechenzentrum z. B. von einer Aufsichtsbehörde eine Betriebseinstellung verfügt, geht es um eine möglichst schnelle, nachweisbare *Wiederherstellung der Compliance*, so dass der Betrieb fortgesetzt werden kann.

Solche Vorfälle können bei ihrem Eintritt bereits *Notfälle* darstellen oder sich innerhalb kurzer Zeit dazu auswachsen. Somit kommt es darauf an, durch schnelle sachgerechte Entscheidungen und trainierte Vorgehensweisen die Auswirkungen auf die Geschäftstätigkeit und die Verluste der Organisation zu begrenzen.

Dieses *reaktive* Vorgehen ist eine zentrale Aufgabe des *Notfallmanagements*. Es dient dazu, eingetretene Notfälle beherrschen zu können.

Im vorliegenden Buch behandeln wir die *präventiven* genauso wie die *reaktiven* Verfahren des (IT-)Notfallmanagements.

Um einen breiten Kreis von Lesern zu erreichen, setzen wir die Existenz eines normgerechten Sicherheitsmanagements in der Organisation *nicht* voraus, sondern werden diese Thematik ebenfalls (im Überblick) behandeln.

Ziel ist es, für das Notfallmanagement

- die erforderlichen Organisationsstrukturen, Prozesse und Dokumente sowie
- die wesentlichen Methoden (Risikoanalyse, Business Impact Analysis, Kritikalitätsanalyse)

im Zusammenhang und praxisnah darzustellen.

Danksagung

Für die Unterstützung bei der Herstellung dieses Buch bedanken wir uns bei Frau Dr. Roß und dem Lektorat des Vieweg+Teubner Verlags.

Im April 2011
Gerhard Klett, Klaus-Werner Schröder, Heinrich Kersten

Inhaltsverzeichnis

Anhänge:

1 Praxisbericht

IT-unterstütztes Management von Lieferketten (Supply Chain Management, SCM) zählt in vielen Unternehmen zu den wesentlichen Ressourcen, deren Ausfall ohne geeignetes Notfallmanagement hohe Kosten und Risiken nach sich zieht. In diesem Praxisbericht wird die Notfallvorsorge sowie das Notfallmanagement eines Supply Chain Management-Systems beschrieben, welches sich zur Darstellung des Zustandes der Lieferkette in Echtzeit der Erfassung der Betriebsdaten entlang der Kette der Übergabe-Punkte mit Barcode Readern bedient.

Zur besseren Übersichtlichkeit gliedert sich der Praxisbericht in zwei Teile:

- Im ersten Teil wird das Notfallmanagement auf Seiten des *Service Providers*, der das übergeordnete Supply Chain Management-System betreibt, vorgestellt.
- Der zweite Teil des Praxisberichts beinhaltet die Notfallmaßnahmen in der nachgelagerten *Betriebsdatenerfassung*, die bei einem Ausfall des Supply Chain Management-Systems mit seiner Zustandserfassung für eine konsistente Speicherung und Verarbeitung der erfassten Daten nach dem Wiederanlauf des Supply Management-Systems zu sorgen hat.

1.1 Notfallmanagement für ein Supply Chain Management-System

In diesem Kapitel wird von folgendem Szenario ausgegangen:

- Das Supply Chain Management-System wird von einem Anbieter als Dienst angeboten (Application Service Provider, ASP).
- Der Eigentümer des damit abgebildeten Prozesses (Process Owner) gehört zu der Organisation des Anwenders des Dienstes.
- Die Basisdienste des Supply Chain Management-Systems wie Installation, Konfiguration, Systemüberwachung (Monitoring), Wartungen und Updates sind Aufgabe des Dienste-Anbieters.

G. Klett. et al., *IT-Notfallmanagement mit System*,
DOI 10.1007/978-3-8348-8226-4_1,

– Die Administration mit Verwaltung der Endbenutzer, Zustandserfassung und Ermittlung von Kennzahlen wird ebenfalls in der Organisation des Anwenders erbracht.

Wir betrachten den Fall, dass das Supply Chain Management-System ausfällt, d.h. keine Anmeldungen und Administration von Benutzern möglich sind, keine Betriebsdaten verbucht werden können, keine Reports über Wareneinn- und Warenausgänge etc. erstellt werden.

Dieser Fall kann – trotz Einhaltung des Durchlaufens der dreistufigen Kette aus Test, Qualitätssicherung und Produktionsumgebung – beispielsweise die Folge eines missglückten Updates oder einer fehlerhaften Umstellung auf ein neues Software Release sein.

Planung und Realisierung der Notfallmaßnahmen

Zunächst werden in Koordination mit dem Anwender vorbeugende Maßnahmen im Rahmen der Notfallvorsorge zur Reduzierung der Eintrittswahrscheinlichkeit von Notfällen definiert. Dazu gehören beispielsweise Kennwerte über Auslastung von Datenbanken sowie deren Optimierung, Wartung der Hardware und ihrer Betriebsumgebung, die konsequente Anwendung einer Qualitätssicherungskette mit Dokumentation der Ergebnisse bei bevorstehenden Updates und Release-Wechsel sowie die dokumentierte Verwendung eines revisionssicheren Change Managements mit Business Impact Analysis, Risikoabschätzung von bevorstehenden Systemänderungen und Rollback-Verfahren (geordnete Rückkehr zum Systemzustand vor der Änderung).

Da Ausfälle jedoch nicht gänzlich zu verhindern sind, besteht der nächste Schritt bei der Planung der Notfallmaßnahmen auf Seiten des Anbieters des Dienstes für Supply Chain Management in der Ermittlung und vertraglichen Vereinbarung von mindestens drei zeitlichen Kennwerten mit dem Anwender des Systems:

– Verfügbarkeit des Systems
  meist in Prozent einer zeitlichen Spanne angegeben (zum Beispiel 99,5% der Gesamtstunden eines Jahres)
– Reaktionszeit nach gemeldetem Systemausfall
  zum Beispiel 4 Stunden; spätestens nach Ablauf dieser Zeit hat der ASP – revisionssicher dokumentiert für den Anwender – reagiert und mit Maßnahmen für Fehlerermittlung und Wiederanlauf begonnen

– Reparaturzeit nach Feststellung der (wahrscheinlichen) Fehlerursache (zum Beispiel 8 Stunden)

Für Störungen bei und Fehler von Hardware, Zugangsnetzwerk, Betriebsumgebung (Energieversorgung, Klimatisierung, etc.), die zum Ausfall des Supply Chain Management führen können, sind vom ASP Prozesse mit ihren Rollen sowie Maßnahmen zur Fehlerbehebung und Störungsbeseitigung definiert und dokumentiert worden.

Folgende Rollen wurden definiert:

– Es gibt einen *Eigentümer* des Prozesses Notfallmanagement für das Supply Chain Management-System. Er verantwortet die Definition der Notfallmaßnahmen in Koordination mit dem Anwender, die Auditierung und die regelmäßigen Übungen.

– Der *Notfallmanager in Rufbereitschaft* (Manager on Duty) ist ein Entscheider innerhalb der Organisation des Service-Anbieters, der weiterführende Maßnahmen autorisiert, die Einfluss auf den Betrieb der Infrastruktur des Dienstleisters haben können (wie zum Beispiel das Öffnen von Firewalls für bestimmte Dienste).

– Der *Notfallkoordinator* unterstützt den Eigentümer des Notfallmanagement-Prozesses bei dessen Ausführung. Er ist das Bindeglied zum Operating des Dienstleisters.

– Die *Verantwortlichen für kritische Ressourcen* sind im Wesentlichen die Administratoren für die Betriebssysteme, das Netzwerk, die Datenbanken usw., die in die einzelnen Schritte des Notfallprozesses mit einzubeziehen sind.

Die Notfallmaßnahmen sind in einem Dokumentenmanagement-System nach folgendem Schema dokumentiert:

– Ziel der Notfallmaßnahme

– konkrete Beschreibung der Lösung

– chronologische Spezifikation für jeden Schritt

– genaue Reihenfolge der Schritte

– Zuordnung der Aktivitäten zu jedem Schritt

– Information über die Ausführung der Schritte an das ausführende Personal

– Benennung der Verantwortlichen für die Implementierung der Lösung

Es versteht sich, dass es für die Dokumentation der Notfallmaßnahmen ein gedrucktes, aktuelles Exemplar geben muss, da der Notfall (beispielsweise bei Ausfall des Zugangsnetzwerks) auch ein Zugriff auf das Dokumentenmanagement-System verhindern könnte.

Zusätzlich zu den Notfallmaßnahmen existieren Alarmierungspläne, denen zu entnehmen ist, wer innerhalb der Organisation des Dienstleisters vom Ausfall des Systems und den derzeitigen Aktivitäten zum Wiederanlauf zu unterrichten ist (Geschäftsführung, Kundenbetreuer etc.). Vorbereitete Schemata für Informationen und Erklärungen unterstützen die konsistente Kommunikation mit den Anwendern und deren Hierarchie.

Für den Ausfall von Hardware gibt es dokumentierte Ersatzbeschaffungspläne mit

- genauer Bezeichnung der Komponente inkl. Beschaffungsdatum und Seriennummer,
- Hersteller, Lieferant, Lieferzeit, Lagerort und Dauer der Re-Installation.

Alle diese Rollen, Prozesse und Maßnahmen werden in Absprache mit dem Anwender mindestens einmal jährlich einer Übung und einer Revision unterzogen. Die Ergebnisse dabei werden dokumentiert und fließen in die Risikoanalyse, die der Anwender erstellt, sowie in etwaige Änderungen der Dienstleistungsverträge (Service Level Agreements, SLA) zwischen dem Dienstleister und dem Anwender des Supply Chain Managements ein.

1.2 Notfallmanagement der Betriebsdatenerfassung

Wie in dem vorgehenden Kapitel erwähnt, wollen wir nun die Notfallmaßnahmen bei der Betriebsdatenerfassung des Supply Chain Management-Systems näher betrachten.

Zur Darstellung des Zustandes der Lieferkette in Echtzeit werden die Betriebsdaten entlang der Kette der Übergabe-Punkte mit Barcode Readern und RFID-Scannern erfasst. Im Wesentlichen werden von diesen Handgeräten die Identifikationsnummern für Produktions- und Versandobjekte gelesen.

Diese Daten werden zu Beginn der Erfassungskette nach der Freigabe des Prozessauftrages als Barcode-Etikett beziehungsweise als RFID-Label angelegt und auf den Versandbehälter aufgebracht. Danach erfolgt im nächsten Schritt das Einscannen der Identifikationsnummer zur Bestätigung des Prozessauftrages.

Nach der Produktion und dem internen Transport findet nach der Einlieferung in eines der Lagerzentren der nächste Scan-Vorgang zur Buchung des Wareneinganges statt. Vor der Auslieferung zum Kunden wird beim Warenausgang nochmals die Identifikationsnummer des Versandobjektes mit den Scannern gelesen.

Zur Verdeutlichung des Vorganges der Betriebsdatenerfassung dient folgende Abbildung:

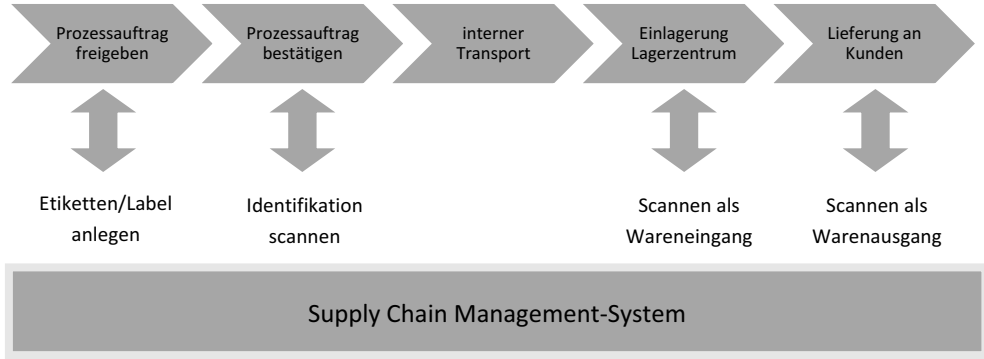


Abbildung 1: Betriebsdatenerfassung an Übergabestationen

Wir werden nun im Detail die Notfallmaßnahmen für den völligen Ausfall des übergeordneten Supply Chain Management-Systems vorstellen.

Planung und Realisierung der Notfallmaßnahmen

Wie bereits im vorgehenden Kapitel erwähnt, ist eine wesentliche Komponente in der Planung der Notfallmaßnahme die vertragliche Beschränkung der Ausfallzeit des Supply Chain Management-Systems. Dazu ist mit dem Anbieter dieses Dienstes eine gesamte maximale Ausfallzeit von 24 Stunden vertraglich festgelegt worden. *Gesamte maximale Ausfalldauer* bedeutet hier die Zeit von der ersten Störungsmeldung bis zur Wiederaufnahme des Normalbetriebes des Gesamtsystems. Andernfalls drohen empfindliche Vertragsstrafen, die gestaffelt nach der tatsächlichen Überschreitung der vereinbarten Ausfallzeit fällig werden.

Damit Produktion und Transport unterbrechungsfrei und unabhängig von dem übergeordneten System für die vereinbarte Ausfallzeit weiterlaufen können, wurde das Software Interface zwischen Handerfassungsgeräten und Supply Chain Management-

System redundant und mit einem Pufferspeicher für die erfassten Daten versehen.

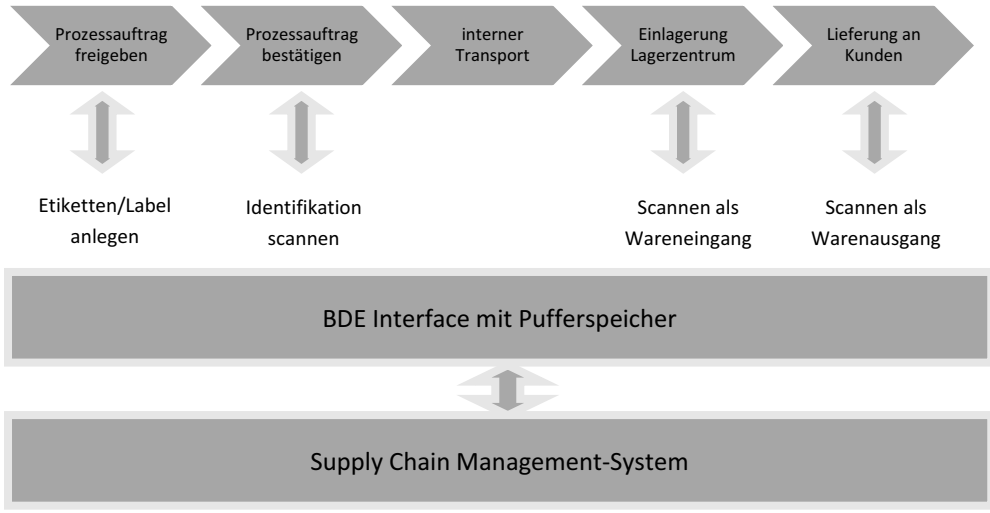


Abbildung 2: Betriebsdatenerfassung mit Pufferspeicher

Zur Vereinfachung der Datenerfassung und deren späteren Weiterverarbeitung werden einige nicht zeitkritische und eher selten benötigte Prozesse wie zum Beispiel Behälter- und Verpackungsverwaltung während des Ausfalls nicht unterstützt. Sie können bis nach dem Wiederanlauf nach maximal 24h verschoben werden.

Als weitere Notfallmaßnahme ist beim Ausfall des Systems die Notfallmannschaft in der Zeit von 6 bis 22 Uhr vor Ort und befindet sich in der restlichen Zeit in Rufbereitschaft.

Für die Überwachung der Notfallprozesse bei der Betriebsdatenerfassung und dem Wiederanlauf des Supply Chain Management-Systems beim Anbieter dieses Dienstes sind vom Anwender Prozesse mit ihren Rollen sowie Maßnahmen zur Synchronisierung mit dem übergeordneten System nach dem Wiederanlauf definiert und dokumentiert worden.

Die Rollen für den Notfallbetrieb bei der Betriebsdatenerfassung sind wie folgt definiert:

- Es gibt einen *Eigentümer* des Prozesses Notfallbetrieb für die Betriebsdatenerfassung. Er verantwortet die Definition der Notfallmaßnahmen in Koordination mit den ebenfalls betroffenen Anwendern und Kunden. Er ist für die Auditierung und die regelmäßige Übung des Notfallbetriebes verantwortlich.
- Der *Notfallmanager in Rufbereitschaft* (Manager on Duty) ist ein Entscheider innerhalb der Organisation des Anwenders, der weiterführende Maßnahmen autorisiert, die Einfluss auf den Betrieb der Infrastruktur des Anwenders haben können.
- Der *Notfallkoordinator* unterstützt den Eigentümer des Notfallmanagement-Prozesses bei dessen Ausführung. Er ist das Bindeglied zum Notfallteam des Dienstleisters.

Die Notfallmaßnahmen sind in einem Dokumentenmanagement-System nach dem im vorigen Kapitel aufgeführten Schema dokumentiert:

- Ziel der Notfallmaßnahme
- konkrete Beschreibung der Lösung
- chronologische Spezifikation für jeden Schritt
- genaue Reihenfolge der Schritte
- Zuordnung der Aktivitäten zu jedem Schritt
- Information über die Ausführung der Schritte an das ausführende Personal
- Benennung der Verantwortlichen für die Implementierung der Lösung

Es existieren ebenfalls Alarmierungspläne mit den Informationen, wer innerhalb der Organisation des Anwenders vom Notfallbetrieb der Betriebsdatenerfassung und dem derzeitigem Stand der Aktivitäten zum Wiederanlauf beim Dienstleister zu unterrichten ist (Abteilungsleiter, Kunden etc.). Wie zuvor auf der Seite des Dienstleisters unterstützen auch hier vorbereitete Schemata für Informationen und Erklärungen die konsistente Kommunikation mit den Kunden und deren Hierarchie.

Der Notfallbetrieb der Betriebsdatenerfassung sieht im Einzelnen wie folgt aus:

- Bei Ausfall des Supply Chain Management-Systems werden die Scanner des Datenerfassungssystems auf den Pufferbetrieb im Interface zum Supply Chain Management-System umgeschaltet.
- Alle erfassten Daten zur Produktion, zur Lagerung werksintern und zur Umlagerung werksübergreifend wie z. B. freigegebene Prozessaufträge, Plandaten, Lagerart, Ladestelle, Materialmenge, Produktionsort etc. werden im Puffer gespeichert.
- Nach dem Wiederanlauf des Supply Chain Management-Systems werden die erfassten Prozessaufträge aus der Pufferliste an das SCM zurückgemeldet und danach aus der Pufferliste gelöscht. Ebenso werden die Warenausgänge aus der Pufferliste verbucht.
- Zurückgestellte, weniger zeitkritische Prozesse, werden im SCM initiiert und mit benötigten Daten aus der Pufferliste synchronisiert.

Für die Implementierung dieser Notfallmaßnahmen entstehen zusätzliche Kosten:

- Zusätzliche Synchronisationssoftware wird benötigt.
- Der Aufwand für die Schnittstellen und deren redundantem Betrieb erhöht sich.
- Erhöhter Personalaufwand für das Umschaltszenario mit Datensicherung ist erforderlich.
- Die Lagerkapazität wird zur Zwischenlagerung von Produktionsgütern erhöht.

Alle diese Rollen, Prozesse und Maßnahmen werden in Absprache mit dem Dienstleister mindestens einmal jährlich einer Übung und einer Revision unterzogen. Die Ergebnisse dabei werden dokumentiert und fließen in die Risikoanalyse, die der Anwender erstellt, sowie in etwaige Änderungen der Dienstleistungsverträge (Service Level Agreements, SLA) zwischen dem Dienstleister und dem Anwender des Supply Chain Managements ein.

1.3 Fazit

Als Fazit lässt sich hier festhalten, dass der Anteil am Notfallmanagement für den Anbieter dieser Dienstleistung weitaus größer ist als für den Bezieher. Diese Reduktion des Aufwandes für den

Bezieher der Dienstleistung ist ein gewünschter Aspekt für ein Outsourcing. In unserem Beispiel hat der Anwender des Supply Chain Managements auf seiner Seite im Wesentlichen für eine ausreichende Anzahl funktionstüchtiger Handscanner zur Weiterführung der Betriebsdatenerfassung, für die Organisation seiner Notfallmannschaft und die Überwachung sowie Überprüfung der Synchronisation der BDE-Daten nach dem Wiederanlauf des Systems zu sorgen. Alles andere ist Aufgabe des Anbieters.

Allerdings müssen die Notfallpläne und deren Übungen von beiden Parteien abgestimmt und durchgeführt werden. Ergebnisse aus diesen Übungen müssen ausführlich gemeinsam bewertet werden. Es ist darauf zu achten, dass der Informationsfluss zwischen Anbieter und Kunde gewährleistet ist. Ergebnisse aus den Übungen müssen gegebenenfalls zeitnah Änderungen in den Service Level Agreements zur Folge haben. Gerade heute bei der in immer größerem Ausmaß praktizierten Kombination von Outsourcing und Virtualisierung ist die vertragliche Abstimmung über die gemeinsamen Notfallpläne und deren Tests eine oft unterschätzte Herausforderung.

2 Methodischer Einstieg

2.1 Begriffliche Abgrenzung

Natürlich fängt alles mit der Erkenntnis an, dass man eine Art „Notfallmanagement“ in der Organisation benötigt, weil Notfälle bereits vorgekommen sind oder aber als mehr oder weniger realistische Drohung im Raum stehen.

Die nächste Frage ist, welche Aufgaben das Notfallmanagement übernehmen soll. Fragt man in Arbeitsgruppen oder auch Seminaren mit Notfallverantwortlichen nach diesem Punkt, so erhält man eine Reihe interessanter, nicht immer ganz ernst gemeinter Ausführungen:

- Wir planen, wie wir Notfälle vermeiden.
- Wir planen, wie wir Notfälle als harmlose Störungen ausgeben können.
- Wir planen, wie wir notfalls ohne IT auskommen.
- Wir planen die Behandlung von Notfällen.
- Wir planen die Überbrückung von Notfällen.
- Wir planen, welche Ereignisse wir als Notfälle betrachten.
- Wir planen, welche Notfälle wir tolerieren.
- Wir planen, wie wir die Verantwortung für einen Notfall auf andere schieben.
- Wir planen, wie wir nach einem Notfall zum Normalzustand zurückfinden.

Analysiert man diese Statements, stellt man fest, dass eigentlich allen etwas Bedenkenswertes anhaftet – aber möglicherweise noch einige Aspekte fehlen oder konkretisiert werden müssen.

Organisation

Im Folgenden sprechen wir oft von der *Organisation* und meinen damit die Institution (Unternehmen, Behörde…), die ein Notfallmanagement aufsetzen will oder bereits betreibt.

Geschäftsprozesse

Eine solche Organisation hat bestimmte (Fach-)Aufgaben zu bewältigen, die sich in aller Regel als *Geschäftsprozesse* betrachten lassen.

G. Klett. et al., *IT-Notfallmanagement mit System*,
DOI 10.1007/978-3-8348-8226-4_2,

Darunter verstehen wir eine geplante, gesteuerte Abfolge von einzelnen Arbeitsschritten, die manuell von Personen und / oder automatisiert abgewickelt werden. Die Arbeitsschritte laufen im einfachsten Fall sequenziell ab; vielfach handelt es sich aber um ein Netz von parallelen, vielfältig miteinander verknüpften Einzelaktivitäten.

Das Ziel eines solchen Prozesses ist stets, ein Ergebnis zu produzieren oder eine Dienstleistung zu erbringen.

Ein solcher Geschäftsprozess kann sich in einer gegebenen Infrastruktur in vielfältiger Weise der Ressource *Information*, organisatorischer und personeller Ressourcen sowie Mitteln der Informationstechnik (Systeme, Netzwerke, Anwendungen) bedienen. Soweit es um datenverarbeitende (Teil-)Prozesse geht, können diese so charakterisiert werden, dass sie bestimmte Eingabedaten miteinander verknüpfen und daraus Ausgabedaten produzieren.

Der mittels IT abgewickelte Teil eines Geschäftsprozesses wird meist IT-Verfahren (gelegentlich auch: IT-Anwendung) genannt.

Einige wichtige weitere Begriffe, die wir zur Diskussion des Notfallthemas benötigen, wollen wir uns detaillierter anschauen.

Normalbetrieb

Als *Normalbetrieb* (bzw. *Normalzustand*) bezeichnen wir eine zeitliche Phase (bzw. Zustand), in der ein Geschäftsprozess seine Funktion korrekt und innerhalb der geplanten Parameter (Kennzahlen für Leistung / Antwortzeiten, maximale Ausfallzeiten,...) erbringt.

Innerhalb des Normalbetriebs werden die genannten Parameter und weitere Größen in einem Sollbereich liegen bzw. einen Sollzustand einhalten.

Störung

Eine *Störung* liegt vor, wenn – unabhängig von der Ursache – eine Größe sich nicht mehr innerhalb des Sollbereichs bewegt bzw. eine Abweichung von einem Sollzustand auftritt.

Nehmen wir das Beispiel der Temperaturmessung. Hier wird der Sollbereich meist durch einen Temperaturbereich (z. B. von 15°C bis 35°C) festgelegt. Fällt die Temperatur unter den Wert 15°C oder steigt sie über 35°C, liegt eine Störung vor. Die Auswirkungen dieser Störung können banal sein oder aber den Einstieg in eine Katastrophe darstellen.

Somit sind für jeden kritischen Gegenstand

- der zulässige Temperaturbereich,
- die Notwendigkeit einer Alarmierung (einschließlich möglicher Alarmschwellen) und