Dieses Kapitel führt Sie in die Entwicklung einer Sicherungs- und Wiederherstellungsstrategie ein. Die wichtigsten Sicherungsmethoden werden erläutert und ihre Vor- und Nachteile genannt. Mit diesen Informationen können Sie ein geeignetes Sicherungskonzept für Ihr SAP-System erarbeiten.

6 Sicherung und Wiederherstellung

Der wichtigste Aspekt im Rahmen des Betriebs eines SAP-Systems ist eine effektive Sicherungs- und Wiederherstellungsstrategie; Ziel ist es, nach einem Systemausfall, einer Notsituation (siehe Kapitel 7, »Disaster Recovery«) oder einem Hardware- oder Softwarefehler eine möglichst schnelle, vollständige oder teilweise Wiederherstellung der Datenbank zu erreichen.

Die Informationen in diesem Kapitel sollen Ihnen dabei helfen, ein Konzept zur optimalen kontinuierlichen Sicherung Ihrer Daten zu entwickeln, mit dem Sie im Notfall Ihre Datenbank rasch und effizient wiederherstellen können. Dazu werden zunächst die Aspekte Sicherung und Wiederherstellung behandelt, anschließend wird die Performance angesprochen. Details zu den einzelnen Datenbanken werden in Kapitel 8, »Datenbankverwaltung«, behandelt.

Ziel der Sicherungsstrategie ist es, den Datenverlust im Notfall zu minimieren, also keine oder nur die während eines möglichst kurzen Zeitraums erfassten Daten zu verlieren. Um das zu erreichen, sollte Ihre Sicherungsstrategie so klar definiert wie möglich sein. Eine unnötig komplizierte Strategie kann die Sicherung und Wiederherstellung auch unnötig kompliziert gestalten. Zudem sollten Sie beachten, dass das Verfahren sowie die Problembehandlung gut dokumentiert werden; die Sicherungsstrategie sollte sich darüber hinaus nicht negativ auf die Tagesgeschäfte auswirken.

6.1 Sicherung

Eine Systemsicherung dient dazu, auf den darin gespeicherten Datenstand des Systems im Notfall zugreifen und ihn zurückspielen zu können. Sie dient

in der Regel nur der Absicherung, da Sie eine Sicherung nur brauchen, wenn Sie Ihr System wiederherstellen müssen – es sei denn, Sie planen beispielsweise, ein Qualitätssicherungssystem aus einer Systemsicherung neu aufzubauen. Dies sollte jedoch nicht dazu führen, die Sicherung zu bagatellisieren. Ganz im Gegenteil: Führen Sie sich vor Augen, in welchem Maß durch einen Systemausfall Daten verloren gehen können und welche Auswirkungen das für Ihr Unternehmen hat. Bereits der Verlust von Bestelldaten einer Stunde oder eines Tages kann zu enormen wirtschaftlichen Schäden führen.

6.1.1 Was muss gesichert werden?

Es gibt drei Kategorien von Daten, die gesichert werden müssen:

- Datenbank
- Transaktionsprotokolle
- Betriebssystemdateien

Sie benötigen möglicherweise unterschiedliche Tools zur Sicherung der unterschiedlichen Daten. Mit SAP-Werkzeugen können Sie z.B. nur eine oder zwei der Dateikategorien sichern: Der DBA-Einplanungskalender (Transaktion DB13, siehe auch Kapitel 8, »Datenbankverwaltung«) kann nur die Datenbank und die Transaktionsprotokolle, nicht aber die Betriebssystemdateien sichern.

Datenbank

Die Datenbank ist der Kern Ihres SAP-Systems. Ohne Sicherung der Datenbank können Sie Ihr System nicht wiederherstellen. Die Häufigkeit, mit der eine vollständige Datenbanksicherung vorgenommen wird, bestimmt, wie weit Sie bei einer Wiederherstellung des Systems in der Zeit zurückgehen:

- Wenn täglich eine vollständige Sicherung durchgeführt wird, benötigen Sie für eine Wiederherstellung die vollständige Sicherung des gestrigen Tages sowie die Transaktionsprotokolldateien eines oder eines halben Tages.
- Wenn wöchentlich eine vollständige Sicherung durchgeführt wird, benötigen Sie die vollständige Sicherung der vergangenen Woche. Sie müssen nun aber bereits die Protokolldateien mehrerer Tage wiederherstellen, um das System zu aktualisieren.

Durch tägliche Sicherung verringern Sie das Risiko, die aktuelle Datenbank aufgrund nicht verwendbarer Protokolldateien nicht wiederherstellen zu können.

Wird keine tägliche Sicherung vorgenommen, müssen Sie das System mit zahlreichen Protokolldateien aktualisieren. Dieser Schritt zieht zum einen das Wiederherstellungsverfahren aufgrund der Menge der Dateien in die Länge, zum anderen erhöht sich das Risiko, die Datenbank aufgrund einzelner defekter Transaktionsprotokolle nicht auf den aktuellen Stand bringen zu können.

Wöchentliche Sicherung [zB]

Eine Wiederherstellung mithilfe der vollständigen Sicherung der letzten Woche, die vor vier Tagen durchgeführt wurde:

- Pro Tag werden zehn Protokolldateien erstellt.
- Das System muss also mit 40 Dateien (zehn Protokolldateien mal vier Tage) aktualisiert werden.
- Sie benötigen 120 Minuten, um die Protokolldateien vom Band auf die Festplatte zu laden (40 Dateien mal drei Minuten pro Datei).
- Sie benötigen 200 Minuten, um die Datenbank mit den Protokolldateien zu aktualisieren (40 Dateien mal fünf Minuten pro Datei).

Die Gesamtzeit für die Wiederherstellung beträgt also – ohne die eigentlichen Datenbankdateien – 320 Minuten (5,3 Stunden).

Tägliche Sicherung [zB]

Eine Wiederherstellung mithilfe der vollständigen Sicherung der letzten Nacht:

- Pro Tag werden maximal zehn Protokolldateien erstellt.
- Sie benötigen 30 Minuten, um die Protokolldateien vom Band auf die Festplatte zu laden (zehn Dateien mal drei Minuten pro Datei).
- Sie benötigen 50 Minuten, um die Datenbank mit den Protokolldateien zu aktualisieren (zehn Dateien mal fünf Minuten pro Datei).

Die Gesamtzeit für die Wiederherstellung beträgt also – ohne die eigentlichen Datenbankdateien – 80 Minuten (1,3 Stunden).

Wie Sie an diesen Beispielen sehen können, benötigen Sie bei einer wöchentlichen Sicherung wesentlich mehr Zeit für die Wiederherstellung als bei einer täglichen Sicherung. Die Beispiele zeigen auch, dass die Zeit, die für die Wiederherstellung der Protokolldateien benötigt wird, von der Größe der Dateien sowie von der Zahl der Tage abhängt, die seit der letzten voll-

ständigen Sicherung vergangen sind. Bei großen Protokolldateien (wie z.B. 100 MB oder mehr pro Stunde) wird dies schnell unpraktisch. Wenn Sie die Häufigkeit der Durchführung vollständiger Datenbanksicherungen erhöhen (wenn Sie also weniger Tage zwischen den einzelnen Sicherungen verstreichen lassen), verringern Sie automatisch die Wiederherstellungszeit.

Sie müssen daher abwägen, ob eine tägliche Vollsicherung der Datenbank mit wenigen Protokolldateien bei dem in Ihrem System anfallenden Transaktionsvolumen wirtschaftlicher ist als z.B. eine wöchentliche Vollsicherung mit entsprechend mehr zurückzuladenden Transaktionsprotokollen. Diese Entscheidung hängt natürlich auch von der Bedeutung des SAP-Systems für die Geschäftsprozesse Ihres Unternehmens ab.

[+] **Tägliche Vollsicherung der Datenbank**

Sie sollten nur dann auf eine tägliche Sicherung der Produktivdatenbank verzichten, wenn schwerwiegende Gründe dagegen sprechen (beispielsweise wenn die Datenbank so groß ist, dass sie nicht über Nacht gesichert werden kann). Die Kosten für Speicherplatz sind in den letzten Jahren so stark gesunken, dass eine Sicherungsstrategie auf Basis einer täglichen Vollsicherung längst nicht mehr unerschwinglich ist. SAP empfiehlt eine tägliche Vollsicherung der Produktivdatenbank sowie die Speicherung der letzten 28 Sicherungen.

Transaktionsprotokolle

Transaktionsprotokolle sind ein Teil der Datenbanksicherung und für deren Wiederherstellung von entscheidender Bedeutung. Die Protokolle enthalten alle Änderungen, die an der Datenbank vorgenommen wurden. Hierdurch können diese Änderungen wieder rückgängig gemacht werden, oder die Datenbank kann nach einem Ausfall auf den letzten Stand zurückgebracht gebracht werden. Es ist sehr wichtig, dass Sie über eine lückenlose Sicherungskopie aller Transaktionsprotokolle verfügen. Wenn Sie eine Wiederherstellung vornehmen müssen und nur ein Protokoll nicht brauchbar ist, kann die Datenbank ab dem unbrauchbaren Protokoll nicht mehr wiederhergestellt werden.

[zB] **Beschädigte Protokolldateien**

Ein Protokoll vom Dienstag wird beschädigt. Das System bricht zwei Tage später, also am Donnerstag, zusammen. Sie können die Datenbank nur bis zum letzten fehlerfreien Protokoll vom Dienstag wiederherstellen. Beginnend mit dem beschädigten Protokoll, sind alle weiteren Transaktionen verloren.

Auch die Häufigkeit der Protokollsicherungen ist eine kaufmännische Entscheidung, die von folgenden Faktoren abhängt:

- Transaktionsvolumen
- kritische Perioden für das System
- Menge der Daten, deren Verlust das Management zu tolerieren bereit ist
- Ressourcen, die zur Sicherung nötig sind

[+] **Zeitabstände zwischen Protokollsicherungen**

Auch hier gilt: Je höher Ihr Transaktionsvolumen ist, desto kürzer sollten die Zeitabstände zwischen den einzelnen Protokollsicherungen sein. Hierdurch wird automatisch die Menge der Daten verringert, die bei einem potenziellen Katastrophenfall im Rechenzentrum verloren gehen kann.

So sichern Sie Transaktionsprotokolle:

1. Sichern Sie das Transaktionsprotokoll auf Festplatte.
2. Kopieren Sie diese Sicherung auf einen Sicherungsdateiserver, der sich nicht an Ihrem Standort befindet. Wenn Sie Ihre Protokolle über ein Netzwerk sichern, sollten Sie immer mit Verifikationen arbeiten.

   Der Sicherungsdateiserver sollte sich idealerweise in einem anderen Gebäude oder in einer anderen Stadt befinden. Der entfernte Standort erhöht die Chancen, dass die Sicherung bei einer Zerstörung des primären Rechenzentrums (mit den SAP-Servern) erhalten bleibt.
3. Sichern Sie die Transaktionsprotokollsicherungen von beiden Servern (SAP-Server und Sicherungsdateiserver) zusammen mit den anderen Dateien auf Betriebssystemebene jeden Tag auf Band.

[!] **Datenbankstopp bei vollem Sicherungsverzeichnis**

Transaktionsprotokolle werden in einem Verzeichnis gespeichert, das genügend Speicherplatz zur Verfügung haben muss. Wenn der verfügbare Speicherplatz vollständig mit Transaktionsprotokollen belegt ist, stoppt die Datenbank. Kommt es zu keiner Weiterbearbeitung in der Datenbank, stoppt damit auch das gesamte SAP-System. Hier ist es wichtig, vorausschauend zu handeln und die Transaktionsprotokolle regelmäßig zu sichern.

Steht Ihnen kein Sicherungsdateiserver an einem separaten Standort zur Verfügung, sichern Sie die Transaktionsprotokollsicherungen nach jedem Protokollsicherungsvorgang auf Band, und schicken Sie die Bänder gegebenenfalls regelmäßig an einen anderen Standort.

[!] **Keine Sicherung im Append-Modus**

Sichern Sie die Protokolle nicht im *Append-Modus* auf Band. Hierbei werden mehrere Sicherungen auf dasselbe Band geschrieben. Im Katastrophenfall gehen dann alle Sicherungen auf diesem Band verloren.

Dateien auf Betriebssystemebene

Auch Dateien auf Betriebssystemebene müssen gesichert werden:

- Konfiguration der Betriebsumgebung (z.B. System- und Netzwerkkonfiguration)
- SAP-Dateien (z.B. Kernel)
- Systemprofile
- Spool-Dateien
- Transportdateien
- andere Anwendungen mit SAP-Bezug
- Schnittstellen- oder Add-on-Produkte, die ihre Daten oder Konfigurationen außerhalb der SAP-Datenbank speichern

Die Datenmenge dieser Dateien ist im Vergleich zur SAP-Datenbank relativ klein. Je nachdem, wie Ihr System arbeitet, sollte die Sicherung der genannten Dateien nur einige Hundert Megabyte bis einige Gigabyte umfassen. Zusätzlich kann es sich bei einigen Daten um statische Daten handeln, die monatelang unverändert bleiben.

Die Häufigkeit der Sicherungen auf Betriebssystemebene hängt von der jeweiligen Anwendung ab. Wenn diese Anwendungsdateien mit dem SAP-System synchron gehalten werden müssen, müssen sie auch mit der gleichen Häufigkeit gesichert werden wie die Protokolle.

[zB] **Synchronität zwischen Anwendungsdateien und SAP-System**

Ein Beispiel für eine solche Situation wäre ein Steuerprogramm, das die Umsatzsteuerdaten außerhalb des SAP-Systems speichert. Diese Dateien müssen genau mit den Kundenaufträgen im System übereinstimmen.

Eine einfache und schnelle Methode, Betriebssystemdateien zu sichern, besteht im Kopieren aller Dateien auf die Festplatte eines zweiten Servers. Auf dem Markt existiert eine Reihe von Produkten, die Daten auf Betriebs-

systemebene sichern. Vom zweiten Server aus können Sie alle gewünschten Dateien auf Band sichern. Dieser Vorgang minimiert Dateiausfallzeiten.

6.1.2 Sicherungsarten

Die möglichen Arten einer Datenbanksicherung lassen sich anhand von drei Aspekten differenzieren:

- was gesichert wird: vollständig oder inkrementell?
- wie gesichert wird: online oder offline?
- wann gesichert wird: geplant oder nach Bedarf?

Grundsätzlich sind die Optionen dieser drei Dimensionen miteinander kombinierbar. Alle Varianten haben jeweils ihre Vor- und Nachteile, die im Folgenden erläutert werden.

Was gesichert wird

Bezüglich des Umfangs der Datenbanksicherung haben Sie die Wahl zwischen einer vollständigen oder einer teilweisen Sicherung.

- **Vollständige Datenbanksicherung**
  Folgende Aspekte sind hier zu beachten:
  - *Vorteile*
    Die Datenbank wird als Ganze gesichert, wodurch auch die Wiederherstellung der Datenbank einfacher und schneller vonstattengeht. Es sind weniger Transaktionsprotokolle zum Aktualisieren der Datenbank notwendig.
  - *Nachteile*
    Die vollständige Sicherung dauert länger als die inkrementelle Sicherung. Aufgrund der längeren Sicherungsdauer werden die Benutzer länger bei der Arbeit gestört. Eine Vollsicherung sollte deshalb immer nur außerhalb der regulären Geschäftszeiten stattfinden.
- **Inkrementelle Sicherung mittels Transaktionsprotokollen**
  Folgende Aspekte sind hier zu beachten:
  - *Vorteile*
    Sehr viel schneller als eine vollständige Datenbanksicherung. Wegen der kürzeren Sicherungsdauer werden die Benutzer weniger lang und in der Regel kaum spürbar bei der Arbeit beeinträchtigt.

- *Nachteile*
  Zur Wiederherstellung der Datenbank ist eine vollständige Sicherung als Grundlage nötig. Die Wiederherstellung der Datenbank mithilfe inkrementeller Transaktionsprotokolle dauert wesentlich länger und ist komplizierter als die Wiederherstellung anhand einer vollständigen Sicherung. Die letzte vollständige Sicherung muss für die Wiederherstellung herangezogen und anschließend muss das System mit allen Protokollen seit der vollständigen Sicherung aktualisiert werden. Wenn seit der letzten Vollsicherung mehrere Tage vergangen sind, müssen bei einem Absturz sehr viele Protokolle wiederhergestellt werden. Kann ein Protokoll nicht wiederhergestellt werden, können alle darauffolgenden Protokolle auch nicht wiederhergestellt werden.

- **Differenzielle Sicherung**
  Abhängig von Ihrer Datenbank und Ihrem Betriebssystem, haben Sie möglicherweise eine dritte Option (siehe Tabelle 6.1), die differenzielle Sicherung. Dabei wird nur das gesichert, was sich seit der letzten vollständigen Sicherung geändert hat. Eine gängige Lösung umfasst eine vollständige Sicherung am Wochenende und differenzielle Sicherungen während der Woche.

  - *Vorteile*
    Die Gefahr einer unvollständigen Wiederherstellung durch beschädigte Protokollsicherungen wird reduziert. Eine differenzielle Sicherung sichert alle Änderungen an der Datenbank, die seit der letzten vollständigen Sicherung vorgenommen wurden.
  - *Nachteile*
    Wie bei der inkrementellen Sicherung ist auch hier zur Wiederherstellung der Datenbank eine vollständige Sicherung als Grundlage nötig. Eine differenzielle Sicherung kann mehr Zeit in Anspruch nehmen als die Sicherung der Transaktionsprotokolle. Direkt zu Anfang ist sie kürzer (nach der vollständigen Sicherung) und wird immer länger, je mehr Daten geändert wurden.

[!] Vollsicherung als Basis der inkrementellen Sicherung

Beachten Sie, dass eine inkrementelle Sicherung stets aus einer Vollsicherung *und* den darauffolgenden Transaktionsprotokollen besteht. Problematisch wird eine Wiederherstellung anhand inkrementeller Sicherungen, sobald die zugrunde liegende vollständige Sicherung oder einzelne Transaktionsprotokolle beschädigt oder verloren gegangen sind.

Wie gesichert wird

Bei den Sicherungsmodi wird zwischen *offline* und *online* unterschieden, was sich auf den Systemstatus des SAP-Systems und der Datenbank bezieht. Um eine Offline-Sicherung durchzuführen, wird das SAP-System von der Datenbank getrennt, und es kann nicht im SAP-System gearbeitet werden. Die Online-Sicherung wird durchgeführt, während Datenbank und SAP-System normal laufen.

- **Offline**
  Vorteile
  - Eine Offline-Sicherung erfolgt schneller als eine Online-Sicherung.
  - Während der Sicherung kommt es nicht zu Komplikationen durch Datenänderungen in der Datenbank.
  - Alle Dateien werden zur gleichen Zeit gesichert und ergeben ein konsistentes Abbild des Systems; die zugehörigen Betriebssystemdateien entsprechen der SAP-Datenbank.
  - Während einer Offline-Sicherung können Sie eine binäre Verifizierung durchführen. Hierdurch verdoppelt sich allerdings die Sicherungszeit.
  - Das SAP-System muss nicht gestoppt werden, um mit einer Offline-Sicherung zu beginnen. Hierdurch bleibt der SAP-Puffer erhalten.

  Nachteile
  - Das SAP-System steht während der Offline-Sicherung nicht zur Verfügung.
  - Wenn die Datenbank gestoppt wird, wird auch der Datenbankpuffer entleert. Dieser Vorgang wirkt sich nachteilig auf die Performance aus, und zwar so lange, bis der Puffer wieder mit Daten belegt wird.

- **Online**
  Vorteile
  - Das SAP-System steht den Benutzern während der Sicherung zur Verfügung. Dies ist notwendig, wenn das System dauerhaft und rund um die Uhr genutzt wird.
  - Die Puffer werden nicht entleert. Dadurch kommt es nach der Sicherung nicht zu nachteiligen Auswirkungen auf die Performance.

  Nachteile
  - Eine Online-Sicherung erfolgt langsamer als eine Offline-Sicherung. Die Sicherungszeit verlängert sich, da die Sicherung neben dem normalen Betrieb gleichzeitig läuft und Systemressourcen in Beschlag nimmt.

- Die Online-Performance lässt während der Sicherung nach.
- Daten in der Datenbank können sich ändern, während die Datenbank gesichert wird. Daher sind Transaktionsprotokolle für eine erfolgreiche Wiederherstellung besonders wichtig.
- Zugehörige Dateien auf Betriebssystemebene stimmen möglicherweise nicht mehr mit der SAP-Datenbank überein.

[!] **Transaktionsprotokolle bei Online-Sicherung**

Wenn Sie mit Online-Sicherungen arbeiten, sind Transaktionsprotokolle für eine erfolgreiche Wiederherstellung besonders wichtig.

Wann gesichert wird

Der Zeitpunkt einer Datenbanksicherung kann anhand eines Sicherungsplans festgelegt sein oder nach Bedarf spontan aus einer bestimmten Situation heraus gewählt werden. Mehr zu den im Folgenden genannten Tools und Transaktionen erfahren Sie in Kapitel 8, »Datenbankverwaltung«.

- **Geplant**
  Geplante Sicherungen werden regelmäßig durchgeführt, etwa täglich oder wöchentlich. Für den Normalbetrieb können Sie mit dem DBA-Einplanungskalender (Transaktion DB13) einen automatisierten Sicherungsplan für die Datenbank und die Transaktionsprotokolle konfigurieren. Mithilfe dieses Kalenders können Sie Sicherungszyklen einrichten und prüfen. Es gibt auch die Möglichkeit, wichtige Datenbankprüfungen und Aktualisierungen der Statistiken durchzuführen. Der Status der Sicherungen kann im DB-Sicherungsmonitor (Transaktion DB12) angezeigt werden.
- **Bedarfsgerecht**
  Bedarfsgerechte Sicherungen werden spontan vorgenommen, z.B. vor größeren Systemänderungen, in Vorbereitung auf ein SAP-Upgrade oder nach einer strukturellen Änderung der Datenbank (z.B. durch Hinzufügen einer Datendatei). Sicherungen, die direkt vom Bediener überwacht werden oder bedarfsgerecht erfolgen, können entweder auch mithilfe des DBA-Einplanungskalenders oder auf der Datenbank- oder der Betriebssystemebene initiiert werden.

Sie können den DBA-Einplanungskalender nicht nur für periodisch geplante, sondern auch für spontane Sicherungen verwenden. Für die bedarfsgerechte Sicherung werden allerdings häufiger Tools auf Datenbankebene eingesetzt, wie das SQL Server Management Studio für Microsoft SQL Server oder die BR*Tools unter Oracle.

Unabhängig von der gewählten Sicherungsmethode, sollten Sie sich die folgenden Ziele setzen:

- Erzeugen Sie eine verlässliche Sicherung, die zur Wiederherstellung der Datenbank herangezogen werden kann.
- Verwenden Sie eine einfache Sicherungsstrategie.
- Reduzieren Sie die Anzahl der Abhängigkeiten untereinander, die für den Betrieb erforderlich sind.
- Versuchen Sie, die Geschäftsbereiche möglichst wenig oder gar nicht bei ihrer Arbeit mit dem SAP-System zu beeinträchtigen.

Wägen Sie zwischen den Bedürfnissen Systemsicherheit und Performance ab, um aus dem Fundus der gegebenen Möglichkeiten die optimale Sicherungsstrategie zu entwickeln.

Datenbanksystemabhängige Terminologie

Die folgende Tabelle vergleicht die Terminologie, die im Rahmen der Sicherung von den verschiedenen Datenbanksystemen verwendet wird, für die in den vorangehenden Abschnitten erläuterten Methoden. Je nachdem, mit welcher Datenbank Ihr System arbeitet, tragen die Sicherungsvorgänge und -jobs unterschiedliche Namen. Das Prinzip ist jedoch im Grunde immer gleich. Ziehen Sie im Zweifel Ihren Datenbankadministrator oder die Dokumentation Ihres Datenbanksystems zu Rate.

	Vollständige Datenbank-sicherung	Inhalt	Teilweise Datenbank-sicherung	Protokoll-sicherung
DB2 UDB	vollständige Datenbank-sicherung in TSM (Tivoli Storage Manager)	Offline-/Online-Tablespace-Sicherung in TSM	inkrementelle Datenbank-sicherung mit DB2 UDB in TSM	Archivieren inaktiver Log-Dateien in TSM
	vollständige Datenbank-sicherung auf Gerät	Offline-/Online-Tablespace-Sicherung auf Gerät	inkrementelle Datenbank-sicherung mit DB2 UDB auf Gerät	Archivieren inaktiver Log-Dateien auf Gerät

Tabelle 6.1 Terminologie in Bezug auf die Sicherung

	Vollständige Datenbank-sicherung	Inhalt	Teilweise Datenbank-sicherung	Protokoll-sicherung
	vollständige Datenbank-sicherung mit Lieferanten-bibliothek	Offline-Tablespace-Sicherung mit Lieferanten-bibliothek	inkrementelle Datenbank-sicherung mit DB2 UDB und Lieferanten-bibliothek	Ein-Schritt-Archivierung in Speicher-software
SQL Server	vollständige Datenbank-sicherung		differenzielle Datenbank-sicherung	Transaktions-protokoll-sicherung
Oracle	vollständige Datenbank offline und erneute Proto-kollsicherung	Offline-Voll-sicherung der Datenbank	Offline-Teil-sicherung der Datenbank	erneute Proto-kollsicherung
	vollständige Datenbank online und erneute Proto-kollsicherung	Online-Voll-sicherung der Datenbank	Online-Teil-sicherung der Datenbank	

Tabelle 6.1 Terminologie in Bezug auf die Sicherung (Forts.)

6.1.3 Sicherungsstrategie

In der Sicherungsstrategie werden alle Maßnahmen zur Sicherung des Systems gebündelt und festgehalten, zu welchem Zeitpunkt und in welchen Intervallen welche Sicherungsmethode zum Einsatz kommt. Diese Strategie sollten Sie in Form einer *Sicherungshäufigkeitstabelle* in einem Sicherungskonzept dokumentieren und mit den Bedürfnissen des Managements und der Fachbereiche abstimmen.

Die *Sicherungsstrategie* setzen Sie mit geeigneten Sicherungstools um. Letztlich ist es jedoch gleichgültig, welches Werkzeug Sie zur Umsetzung der Strategie verwenden – seien es die bereits genannten SAP-internen Tools oder die Bordmittel Ihres Datenbank- bzw. Betriebssystems. Entscheidungskriterien sollten Handhabbarkeit, Zuverlässigkeit und die vorhandenen Überwachungsmöglichkeiten sein.

So entwickeln Sie Ihre Sicherungsstrategien:

1. **Ermitteln Sie Ihre Wiederherstellungsanforderungen und Ihren Toleranzbereich bei einem Systemausfall.**
   Es ist nicht möglich, eine allgemein tolerierbare Ausfallzeit zu definieren, da dieser Zeitraum stark vom jeweiligen Unternehmen abhängig ist. Die Kosten eines Ausfalls umfassen den Produktionsausfall sowie die für die Wiederherstellung notwendigen Aufwendungen wie Zeit, Geld etc. Diese Kosten sollten ähnlich wie bei einer Versicherung gestaffelt werden: Je mehr Deckung Sie benötigen, desto teurer wird die Versicherung. Übertragen auf die Wiederherstellung, bedeutet dies: Je schneller die Wiederherstellung abgeschlossen sein soll, desto teurer wird die Lösung.
2. **Ermitteln Sie, welche Kombination aus Hardware, Software und Prozessen die gewünschte Lösung bieten kann.**
   Bessere Hardware macht eine Sicherung und Wiederherstellung schneller, bessere Software macht sie komfortabler, wohldefinierte Prozesse machen sie effizienter. Das alles hat freilich seinen Preis und unterliegt wirtschaftlichen Abwägungen von Kosten und Nutzen. Noch wichtiger jedoch ist, dass Ihre Methode zuverlässig ist.
3. **Testen Sie Ihr Sicherungsverfahren, indem Sie die Hardware implementieren und die tatsächlichen Laufzeiten und Testergebnisse überprüfen.**
   Stellen Sie sicher, dass Sie Ergebnisse von allen Sicherungsarten erhalten, die in Ihrer Umgebung eingesetzt werden können, nicht nur von denen, die Sie einzusetzen gedenken. Diese Information wird zukünftige Evaluierungs- und Kapazitätsplanungsentscheidungen unterstützen und bei Bedarf nützliche Vergleichsmöglichkeiten bieten.
4. **Testen Sie Ihr Wiederherstellungsverfahren, indem Sie verschiedene Ausfallsituationen simulieren.**
   Dokumentieren Sie alle Aspekte der Wiederherstellung, einschließlich der Fragen, wer welche Aufgaben übernimmt, wer benachrichtigt werden soll etc. (siehe auch Kapitel 7, »Disaster Recovery«). Denken Sie daran, dass eine Wiederherstellung genau dann notwendig werden kann, wenn Sie am wenigsten damit rechnen. Die Tests sollten kontinuierlich erfolgen, mit zusätzlichen Tests bei Änderungen von Hardware- und Softwarekomponenten.

Planen Sie neben Ihren täglichen und wöchentlichen Sicherungszyklen zusätzliche Sicherungen an bestimmten Tagen ein (z. B. Monatsende, Jahresende). Diese sind zwar eigentlich nicht notwendig, können aber z. B. für den Katastrophenfall besonders archiviert werden (siehe auch Kapitel 7, »Disaster Recovery«).

6.1.4 Strategieempfehlungen

Im Folgenden geben wir Ihnen noch einige Hinweise und Empfehlungen für die Entwicklung einer Sicherungsstrategie.

Datenbank

Wie schon erläutert, empfehlen wir, wenn der Aufwand vertretbar ist, eine tägliche vollständige Sicherung der Datenbank. Bei Datenbanken, die für eine tägliche Sicherung zu groß sind, sollte einmal pro Woche eine vollständige Sicherung erfolgen.

Sicherungen prüfen

Sicherungen müssen regelmäßig geprüft werden. Hierzu müssen Sie das System wiederherstellen und dann testen, ob die Wiederherstellung zu Ihrer Zufriedenheit verlaufen ist. Solange Sie die Sicherung nicht geprüft haben, können Sie nie wissen, ob auch tatsächlich alles auf Band oder Festplatte gesichert wurde.

[zB] **Notwendigkeit der Sicherungsprüfung**

Die Sicherung verschiedener Dateien wurde ausgeführt, doch wurde der Append-Schalter für die zweite Datei und alle nachfolgenden Dateien nicht richtig gesetzt. Als Konsequenz wurde nicht eine Datei nach der anderen auf Band gesichert. Vielmehr wurde das Band nach jeder gesicherten Datei zurückgespult und anschließend die nächste Datei gesichert. Bis auf die letzte gesicherte Datei wurden also alle vorangegangenen Dateien überschrieben.

[!] **Sicherungen erst zum Schluss prüfen**

Eine Sicherung darf erst geprüft werden, nachdem *alle* Dateien gesichert wurden. Wenn die Prüfung nach jeder einzelnen Datei durchgeführt wird, kann das System nicht erkennen, dass die vorherige Datei eventuell überschrieben wurde.

Datenbankintegrität

Um sicherzugehen, dass die Datenbank keine beschädigten Blöcke enthält, muss die Integrität der Datenbank regelmäßig geprüft werden. Defekte Blöcke könnten sonst während der Sicherung unbemerkt bleiben. Führen Sie möglichst wöchentlich außerhalb der Geschäftszeiten eine Integritätsprüfung durch. Sie können sie mithilfe des DBA-Einplanungskalenders planen.

Transaktionsprotokolle

Die Sicherung der Transaktionsprotokolle ist äußerst wichtig. Wenn der zur Speicherung der Transaktionsprotokolle verfügbare Speicherplatz belegt ist, stoppt die Datenbank und damit auch das SAP-System.

Beobachten Sie daher das Aufkommen an Transaktionsprotokollen in Ihrem System, und definieren Sie ausgehend von diesen Erkenntnissen ein geeignetes Sicherungsintervall, z.B. stündlich. Die Zeitabstände zwischen den Sicherungen entsprechen der maximalen Datenmenge, deren Verlust Sie tolerieren. Für ein Unternehmen mit hohem Transaktionsvolumen ist auch das Risiko höher. Hier wäre es beispielsweise ratsam, halbstündlich eine Sicherung vorzunehmen. Wenn Sie über eine Versandabteilung verfügen, die die Arbeit um 03:00 Uhr morgens aufnimmt, oder über eine Produktionsstrecke, die erst um 22:00 Uhr Feierabend macht, sollten Sie entsprechend früher mit der Sicherung beginnen bzw. später aufhören. Die Transaktionsprotokollsicherung kann während des normalen Betriebs ausgeführt werden, ohne dass es zu einer Störung der Benutzer kommt.

Dateien auf Betriebssystemebene

Die Häufigkeit der Sicherungen auf Betriebssystemebene hängt von der jeweiligen Anwendung ab. Wenn die Anwendungsdateien mit dem SAP-System synchron gehalten werden sollen, müssen sie auch mit der gleichen Häufigkeit gesichert werden wie Datenbank und Protokolle. Ist eine exakte Entsprechung weniger wichtig, können die Anwendungsdateien auch weniger häufig gesichert werden.

Sicherungsstrategie-Checkliste

Für die Sicherung wertvoller Systemdaten muss eine angemessene Vorgehensweise entwickelt werden. Sie sollten so früh wie möglich eine entsprechende Strategie definieren, um möglichem Datenverlust vorzubeugen. Vor dem Go Live sollten Sie die Checkliste mit sicherungsrelevanten Themen abgearbeitet haben (siehe Tabelle 6.2).

Frage, Aufgabe oder Entscheidung	Erledigt
Entscheiden Sie, wie häufig Sie eine vollständige Datenbanksicherung vornehmen möchten.	
Entscheiden Sie, ob teilweise oder differenzielle Sicherungen nötig sind.	
Entscheiden Sie, ob Sie automatische Sicherungen nutzen möchten. Wenn ja, entscheiden Sie, wo dies erfolgen soll (im DBA-Einplanungskalender oder anderswo).	
Entscheiden Sie, wie häufig die Transaktionsprotokolle gesichert werden sollen.	
Legen Sie fest, welche Sicherungsmedien (Festplatten, Bänder etc.) Sie verwenden möchten.	
Sorgen Sie dafür, dass Sie eine Tagesmenge an Protokollen auf dem Server speichern können.	
Sorgen Sie für ausreichend Speicherplatz im Verzeichnis für Transaktionsprotokolle.	
Richten Sie die erforderlichen Berechtigungen für das SAP-System, das Betriebssystem und die Datenbank ein.	
Überlegen Sie, ob Sie den DBA-Einplanungskalender zur Einplanung der Sicherung von Transaktionsprotokollen nutzen möchten.	
Erarbeiten Sie Richtlinien für Datenträgerbeschriftungen, um einen reibungslosen Ablauf zu gewährleisten.	
Entscheiden Sie sich für eine Sicherungs-Aufbewahrungsfrist.	
Beschaffen Sie die notwendige Hardware (Festplatten) bzw. legen Sie die Größe des benötigten Bandpools fest (pro Tag benötigte Bänder × Aufbewahrungsfrist + 20 %).	
Berücksichtigen Sie zukünftiges Wachstum und spezielle Anforderungen.	
Initialisieren Sie die Bänder.	
Legen Sie eine Lagerungsstrategie für die Bänder fest.	
Dokumentieren Sie die Sicherungsprozeduren in einem Betriebshandbuch.	
Schulen Sie die Bediener in den Sicherungsprozeduren.	
Implementieren Sie eine Sicherungsstrategie.	
Führen Sie eine Sicherung und Wiederherstellung zu Testzwecken durch.	
Definieren Sie einen Notfallplan, und entscheiden Sie, wer in einem Notfall kontaktiert werden soll.	

Tabelle 6.2 Sicherungsstrategie – Checkliste

6.2 Wiederherstellung

Normalerweise wird eine Wiederherstellung aus folgenden Gründen vorgenommen:

- Disaster Recovery nach einer Notsituation (siehe Kapitel 7)
- Testen Ihres Disaster-Recovery-Plans (siehe Kapitel 7)
- Kopieren Ihrer Datenbank in ein anderes System (siehe Kapitel 2, »SAP-Systemverwaltung«)

Bei einer Systemwiederherstellung wird auf die regelmäßig angefertigten Sicherungen zurückgegriffen. Im Rahmen einer Disaster Recovery werden in der Regel die Datenbank und – falls nötig – das Betriebssystem mithilfe der letzten vollständigen Sicherung neu aufgesetzt. Anschließend werden die seit der Vollsicherung erstellten Transaktionsprotokolle eingelesen. Nach erfolgreichem Abschluss dieser Prozedur hat das System den Stand, den es zum Zeitpunkt der letzten fehlerfreien Protokollsicherung hatte. Entscheidend ist, wie lange eine solche Wiederherstellung dauert. Dass sie möglichst schnell erfolgen soll, liegt darin begründet, das System nach einem Ausfall rasch wieder einsatzbereit zu haben, damit der Geschäftsablauf möglichst wenig unterbrochen wird.

Bei einer *Datenbankkopie* (z.B. beim regelmäßigen Aktualisieren des Qualitätssicherungssystems anhand einer Kopie des Produktivsystems) wird meist entweder die letzte Vollsicherung eingespielt oder per Stream eine Live-Kopie erzeugt. Transaktionsprotokolle werden in der Regel nicht berücksichtigt.

Analog zur Systemsicherungsstrategie sollten Sie für den Notfall eine *Wiederherstellungsstrategie* in petto haben. Folgende Faktoren können eine Wiederherstellungsstrategie beeinflussen:

- Geschäftskosten, die durch Systemausfallzeiten verursacht werden
- operative Zeitpläne
- globale oder lokale Benutzer
- Anzahl der Transaktionen pro Stunde
- Budget

Die Entwicklung einer Wiederherstellungsstrategie wird ausführlich in Kapitel 7, »Disaster Recovery«, behandelt. Der eigentliche Prozess zur Wiederherstellung des SAP-Systems und der Datenbank wird in diesem Buch nicht

betrachtet, da diese Aufgabe sehr stark vom jeweiligen System und der Datenbank abhängig ist. Wenden Sie sich im Zweifel an einen Spezialisten (z.B. Ihren Datenbankadministrator oder einen externen Basis-Berater), der Sie operativ bei diesem kritischen Prozess unterstützen kann. Arbeiten Sie mit Ihrem Datenbankadministrator oder Berater auch zusammen, um den Wiederherstellungsprozess für Ihr System zu testen und zu dokumentieren. Anhand dieses Wissenstransfers werden Sie bald in der Lage sein, die Wiederherstellung selbst vorzunehmen.

[!] **Unvollständige oder fehlerhafte Wiederherstellung**

Wenn die Wiederherstellung nicht korrekt oder nicht vollständig durchgeführt wurde, kann sie misslingen und muss von Neuem gestartet werden, da sonst einige Dateien nicht berücksichtigt werden können. Sie müssen besondere Daten über Ihre Datenbank erfassen, um sie später wiederherstellen zu können. Arbeiten Sie mit einem Spezialisten zusammen, um diese Daten zu identifizieren und zu dokumentieren.

Da der Wiederherstellungsprozess eine der wichtigsten Aufgaben im SAP-System darstellt, muss die Wiederherstellung der Datenbank in regelmäßigen Abständen getestet werden. Auch hierzu bietet Ihnen Kapitel 7, »Disaster Recovery«, weitere Hinweise.

6.3 Performance

Das wichtigste Ziel der Datenbankwiederherstellung ist neben der möglichst vollständigen Wiederherstellung die Minimierung der Zeit, die dafür benötigt wird. Für das Unternehmen ist entscheidend, wie lange das SAP-System nicht für die Benutzer zur Verfügung steht und damit bestimmte Unternehmensabläufe nicht stattfinden können. Deshalb ist die Systemperformance bei der Wiederherstellung ein bedeutender Faktor.

Die Sicherungsperformance ist ebenfalls wichtig, besonders wenn das System global eingesetzt und rund um die Uhr genutzt wird. Während einer Sicherung gilt es, die Auswirkungen auf die Benutzer so gering wie möglich zu halten. Das Ziel besteht daher einerseits in der Reduzierung der Sicherungszeit (insbesondere bei Offline-Sicherungen) und andererseits darin, genügend Systemreserven für einen akzeptablen Betrieb während einer Online-Sicherung bereitzuhalten.

Sicherungs- und Wiederherstellungsperformance werden hauptsächlich durch den Datendurchsatz Ihrer Geräte bestimmt. Um sie zu verbessern, müssen Sie den Engpass oder das Gerät, das den Durchsatz begrenzt, ermitteln und eliminieren bzw. austauschen. Dieser Prozess ist Wirtschaftlichkeitsüberlegungen unterworfen, denn zusätzliche Performance durch weitere oder modernere Geräte ist natürlich auch ein Kostenfaktor.

Dieser Abschnitt gibt Ihnen Tipps, wie Sie durch gezielte Maßnahmen die Performance Ihrer Datensicherungen und Wiederherstellungen positiv beeinflussen können.

6.3.1 Performancefaktoren

Drei Hauptvariablen beeinflussen sowohl die Performance der Sicherung als auch der Wiederherstellung:

- **Größe der Datenbank**
  Je größer die Datenbank, desto länger dauert die Sicherung.
- **Hardwaredurchsatz**
  Diese Variable bestimmt, wie schnell die Sicherung vonstattengeht. Der Durchsatz wird vom jeweils schwächsten Glied der Sicherungskette bestimmt, so z.B. vom:
  - Datenbanktreiber-Array
  - verwendeten Eingabe-/Ausgabekanal (E/A-Kanal)
  - Festplatten- oder Bandlaufwerk
- **Sicherungszeitpunkt**
  Dabei handelt es sich um den Zeitpunkt bzw. -raum, der Ihnen zur regelmäßigen Sicherung des Systems zur Verfügung steht. Das Ziel hierbei besteht darin, die Benutzer möglichst wenig zu behindern.
  - *Online-Sicherung*
    Der Sicherungszeitpunkt für diese Art der Sicherung liegt in Perioden mit niedriger Systemaktivität, üblicherweise früh am Morgen.
  - *Offline-Sicherung*
    Der Sicherungszeitpunkt für diese Art der Sicherung liegt in Perioden, in denen das SAP-System heruntergefahren werden kann, üblicherweise am Wochenende.

  Bei Systemwiederherstellungen ist der Zeitpunkt weniger entscheidend, da das System in einem solchen Fall ohnehin nicht läuft.

[+] **Zeitverschiebung an Unternehmensstandorten beachten**

Berücksichtigen Sie die Zeitverschiebungen an anderen Standorten Ihres Unternehmens. Zum Beispiel ist 12:00 Uhr mittags in Mitteleuropa 06:00 Uhr morgens in New York.

6.3.2 Sicherungsperformance

Für die folgenden Ansätze zur Verbesserung der Sicherungsperformance wird davon ausgegangen, dass Sie Ihre Sicherung lokal auf dem Datenbankserver vornehmen. Eine Sicherung über ein Netzwerk ist zwar technisch machbar, hängt bezüglich der Performance aber wesentlich von Netztopologie, Overhead und Datenverkehr ab – die Durchsatzwerte der Plattensysteme treten in den Hintergrund. Die volle Kapazität des Netzwerks steht ohnehin nur selten zur Verfügung. Wenn eine Sicherung über das Netzwerk vorgenommen wird, sinkt zudem die Netzwerkleistung für andere Benutzer. Das kann dazu führen, dass auch andere Unternehmensanwendungen gebremst werden.

Sicherung auf schnelleren Geräten

Alle Optimierungsansätze zielen darauf ab, einen Engpass am Sicherungsgerät zu verhindern. Das Sicherungsgerät, üblicherweise eine Festplatte oder ein Bandlaufwerk, ist das Gerät, das den Durchsatz begrenzt. Folgende Aspekte sind in diesem Zusammenhang zu berücksichtigen:

- **Vorteile**
  Schnellere Festplatten oder Bandlaufwerke ermöglichen es Ihnen, eine ganze Datenbank in vertretbarer Zeit zu sichern.
- **Nachteile**
  Schneller Speicher kostet mehr Geld. Festplatten oder Bandgeräte mit hohem Datendurchsatz erfordern eine gewisse Investitionsbereitschaft.

Parallele Sicherung

Die parallele Sicherung auf mehrere Laufwerke verwendet ein RAID-0-Array (RAID = Redundant Array of Independent Disks), bei dem gleichzeitig mehrere Medien (Festplatten/Bänder) beschrieben werden. In einigen Umgebungen, wie beispielsweise Oracle, werden einzelne Tablespaces oder Dateien gleichzeitig auf separate Laufwerke gesichert. Dadurch ist die Gesamtperformance wesentlich höher, als wenn Sie nur ein einziges Laufwerk verwenden.

Mit einer genügend großen Anzahl paralleler Laufwerke kann der Engpass von den Laufwerken auf eine andere Komponente verschoben werden. Sie müssen daher auch die Performance der anderen Untersysteme berücksichtigen, wenn Sie die parallele Sicherung nutzen möchten. Diese Untersysteme umfassen Controller, CPU und E/A-Bus. In vielen Konfigurationen ist der Controller oder Bus der limitierende Faktor.

[!] **Wiederherstellung einer parallelen Sicherung**

Wenn Sie eine parallele Sicherung wiederherstellen, müssen alle Medien des Sets lesbar sein. Ist ein Band beschädigt, können Sie die Sicherung nicht verwenden. Je mehr Bänder ein Set enthält, desto größer ist die Chance, dass eines davon beschädigt ist.

Sicherung auf Festplatten, dann auf Magnetband

Die Sicherung zunächst auf Festplatten und anschließend auf Band ist die schnellste Methode, um eine Datenbank zu sichern. Die Sicherung auf Festplatten ist normalerweise schneller als die Sicherung auf Band. Sie können schnell mehrere identische Kopien auf Festplatten speichern und beispielsweise einige an Fremdlagerorten, andere an eigenen Unternehmensstandorten lagern.

Sobald die Sicherung auf Festplatte erfolgt ist, ist die Systemperformance nur minimal beeinträchtigt. Da die Sicherung auf Band von der bereits angefertigten Kopie auf der Festplatte gezogen wird und nicht von der Produktivdatenbank, gibt es kein Konkurrieren um Ressourcen zwischen Sicherung und Datenbankaktivitäten. Während einer Disaster Recovery kann im Optimalfall die Wiederherstellung von der Sicherung auf Festplatte erfolgen. Diese Methode hat aber auch einige Nachteile:

- Sie benötigen zusätzlichen Festplattenplatz in der Größe der Datenbank. Bei einer größeren Datenbank kann dies zu immensen zusätzlichen Kosten führen.
- Bis die Sicherung auf Band abgeschlossen ist, sind Sie potenziellen Katastrophenfällen im Rechenzentrum schutzlos ausgeliefert. In einer Disaster-Recovery-Situation müssen Sie zuerst die Dateien auf der Festplatte wiederherstellen und dann die Wiederherstellung der Datenbank von der Festplatte ausführen.

Es gibt noch andere Optionen für schnellere Sicherungen, wie etwa *Hochverfügbarkeit* (High Availability, HA) oder moderne *Snapshot-Verfahren*, deren Erläuterung allerdings den Rahmen dieses Buches überschreiten würde.

6.3.3 Wiederherstellungsperformance

Die Performanceanforderungen für eine Wiederherstellung sind wichtiger als die für eine Sicherung. Die Wiederherstellungsperformance bestimmt, wann das System wieder zur Verfügung steht und wie schnell die Geschäfte wieder aufgenommen werden können. Das Ziel ist, die Datenbank und zugehörige Dateien rasch wiederherzustellen und das System schnell wieder allgemein verfügbar zu machen.

Die genannten Maßnahmen zur Verbesserung der Sicherungsperformance führen im Grunde gleichzeitig zu einer Verringerung der Wiederherstellungszeit. Insofern können Sie diese Vorschläge sowohl unter dem Gesichtspunkt der Sicherung als auch der Wiederherstellung anwenden, beispielsweise:

- **Dedizierte Laufwerke**
  Zusammen mit der parallelen Sicherung beschleunigt die Wiederherstellung von Dateien und Tablespaces auf einzelne dedizierte Laufwerke den gesamten Prozess erheblich. Es wird jeweils nur ein Tablespace oder eine Datei auf das Laufwerk geschrieben. Hierdurch wird das Konkurrieren um Laufwerkressourcen vermieden.
- **RAID-Systeme**
  RAID 0+1 ist schneller als RAID5, aber diese Geschwindigkeit hängt von der jeweiligen Hardware ab. In den meisten Fällen nimmt die Berechnung der Paritätsdaten für das Paritätslaufwerk (RAID5) mehr Zeit in Anspruch als das zweimalige Schreiben der Daten (RAID 0+1). Diese Option ist kostspielig, da die nutzbare Kapazität nur 50 % der totalen Kapazität beträgt – signifikant weniger als bei RAID5:
  - *RAID 0+1 = [single_drive_capacity × (number_of_drives ÷ 2)]*
  - *RAID5 = [single_drive_capacity × (number of drives – 1)*]
- **Laufwerke mit höherer Schreibperformance**
  Von moderneren Laufwerken mit einer höheren Schreibperformance können Sie Daten in der Regel auch schneller auslesen. Die bessere Leseleistung verringert die Wiederherstellungszeit.
- **Laufwerk-Array-System mit höherer Schreibperformance**
  Der Vorteil schnellerer Einzellaufwerke gilt auch für Laufwerk-Arrays: In der Regel verbessert sich mit der Schreibperformance auch die Lesegeschwindigkeit, was zu einer Verkürzung der Wiederherstellungszeit führt.

Maßnahmen zur Verbesserung der Sicherungsperformance werden seitens des Managements oft nicht mit besonders hoher Dringlichkeit gewürdigt.

Das liegt daran, dass Sicherungen meist außerhalb der Kernzeiten stattfinden und sich eine bessere Performance in der Regel bei den Anwendern nicht bemerkbar macht. Entsprechend schwierig kann es werden, zusätzliche Mittel für modernere Technik zu bekommen.

Wenn Sie jedoch damit argumentieren, dass bei der Wiederherstellung deutliche Zeiteinsparungen möglich wären, finden Sie vielleicht eher Gehör: Immerhin steht das System nach einem Havariefall umso schneller wieder zur Verfügung.

6.4 Fazit

Die Ausführungen in diesem Kapitel sollen Sie dabei unterstützen, eine Sicherungsstrategie für Ihre SAP-Systeme zu entwerfen, die von den betriebswirtschaftlichen Rahmenbedingungen Ihres Unternehmens ausgeht. Mithilfe einer Kombination aus vollständigen und inkrementellen Datenbanksicherungen, ergänzt durch das Speichern von Transaktionsprotokollen und Betriebssystemdateien, sichern Sie sich gegen ein Worst-Case-Szenario ab. Ihr Ziel sollte sein, das System im Fall der Fälle komplett und innerhalb kürzester Zeit wiederherstellen zu können, um zum geregelten Betrieb zurückzukehren.

Das folgende Kapitel 7, »Disaster Recovery«, gibt noch einmal spezielle Hinweise für ein Katastrophenszenario. In Kapitel 8, »Datenbankverwaltung«, lernen Sie die SAP-internen Datenbankwerkzeuge kennen, mit denen Sie Sicherungen automatisiert durchführen.

Auch den sorgfältigsten Systemadministrator kann es ereilen: Systemausfall, Datenverlust, Zerstörung durch Naturkatastrophen. In solchen Situationen ist es gut, einen Plan zu haben und nicht völlig überrascht zu werden. Dieses Kapitel gibt Ihnen Anregungen, wie Sie sich auf den Havariefall und eine Systemwiederherstellung vorbereiten können.

7 Disaster Recovery

Geschäftsprozesse finden täglich zu Tausenden statt, und normalerweise kommt es dabei nicht zu Problemen. Der kleinste Systemstörfall kann jedoch zu einer schwerwiegenden Unterbrechung der Geschäftsprozesse und damit zum Verlust von Zeit, Geld und Ressourcen führen. Daher ist es ratsam, sich Pläne für den Notfall zurechtzulegen, damit man solchen Problemen, ungeachtet ihrer Größe und Komplexität, nicht hilflos gegenübersteht.

Gegenstand dieses Kapitels ist die wohl wichtigste Aufgabe eines Systemadministrators: *Disaster Recovery*. Disaster Recovery ist eine Form der Systemwiederherstellung, wie sie in Kapitel 6, »Sicherung und Wiederherstellung«, beschrieben wird.

7.1 Vorüberlegungen

Das Ziel der Disaster Recovery ist es, das System nach einer *Notsituation* so weit wiederherzustellen, dass das Unternehmen mit seinen Geschäftsabläufen fortfahren kann. Da nicht nur während des Systemausfalls selbst die Geschäftsprozesse zum Erliegen kommen, sondern auch noch während der Wiederherstellung, muss eine Disaster Recovery möglichst schnell durchgeführt werden. Umso wichtiger ist es, die Wiederherstellung gut geplant und erprobt zu haben. Je früher Sie mit der Planung beginnen, desto besser sind Sie im Fall eines tatsächlichen Notfalls vorbereitet.

Hinweis zu den folgenden Erläuterungen [!]

Dieses Kapitel ist keine Anleitung zur Disaster Recovery! Es dient dazu, Ihr Bewusstsein für dieses Thema zu schärfen und Ihnen zu verdeutlichen, wie wichtig es ist, einen Plan zu entwickeln.

Eine Notsituation ist alles, was zu einer Schädigung oder zum Ausfall des SAP-Systems führt. Hierzu gehören Schädigungen der Datenbank (z.B. das versehentliche Laden von Testdaten in das Produktivsystem), schwere Hardwareausfälle oder auch der vollständige Verlust des SAP-Systems und der Infrastruktur (z.B. durch eine Naturkatastrophe oder einen Gebäudebrand). Im Fall einer solchen Notsituation besteht die wichtigste Aufgabe des Systemadministrators darin, das SAP-System erfolgreich wiederherzustellen. Er sollte jedoch vor allem Sorge dafür tragen, dass es erst gar nicht zu einem solchen Notfall kommt.

Ein Systemadministrator sollte für das Schlimmste gerüstet sein und entsprechende »Notfallpläne« bereithalten. Während der Disaster Recovery sollte nichts zum ersten Mal getan werden, denn unerfreuliche Überraschungen könnten den gesamten Recovery-Prozess zunichte machen.

Stellen Sie sich zu Beginn Ihrer Planung folgende Fragen:

- Fällt mit dem SAP-System auch der gesamte Geschäftsprozess aus?
- Wie hoch ist der Ertragsausfall, und wie hoch sind die entstehenden Kosten während eines Systemausfalls?
- Welche wichtigen Geschäftsfunktionen können nicht mehr ausgeführt werden?
- Wie werden die Kunden unterstützt?
- Wie lange kann das System ausfallen, bis das Unternehmen geschäftsunfähig wird?
- Wer koordiniert und verwaltet die Disaster Recovery?
- Was tun die Benutzer, solange das SAP-System nicht funktioniert?
- Wie lange wird das System ausfallen?
- Wie lange wird es dauern, bis das SAP-System wieder zur Verfügung steht?
- Welche Komponenten des SAP-Systems müssen mindestens wiederhergestellt werden, damit eine Fremd-Recovery möglich ist?

Wenn Sie sorgfältig planen, stehen Sie im Fall einer Notsituation weniger unter Druck: Sie wissen bereits, dass das System wiederhergestellt werden kann und wie lange dies voraussichtlich dauern wird.

Sollten Sie feststellen, dass die für eine Wiederherstellung notwendige Zeit zu lang und der damit verbundene Schaden zu hoch ist, sollte das Management zusätzliche Investitionen in Geräte, Einrichtungen und Personal in

Betracht ziehen. Eine *High-Availability-Lösung* (Hochverfügbarkeit) ist zwar oft kostspielig, allerdings sind die Kosten unter Umständen nicht annähernd so hoch wie der mögliche Verlust im Havariefall.

7.2 Für eine Notsituation vorplanen

Das Erstellen eines Disaster-Recovery-Plans ist ein Großprojekt, da Entwicklung, Tests und Dokumentation viel Zeit beanspruchen und über ein Jahr dauern können. Allein die Dokumentation kann bereits äußerst umfangreich werden und möglicherweise mehrere Hundert Seiten umfassen.

Ziehen Sie einen Experten zu Rate, wenn Sie nicht wissen, wie Sie für den Notfall vorplanen sollen: Ein Plan, der nicht funktioniert, ist schlimmer, als gar keinen Plan zu haben, denn der schlechte Plan vermittelt ein trügerisches Gefühl der Sicherheit. Disaster-Recovery-Berater und -Lieferanten von Drittseite können Sie bei Ihrer Planung unterstützen.

7.2.1 Welche Maßgaben gelten für die Disaster Recovery?

Die Anforderungen an die Disaster Recovery lassen sich direkt von den Anforderungen an die Systemverfügbarkeit ableiten, die seitens des Managements aufgestellt werden. Die Vorgaben für die notwendige Systemverfügbarkeit ergeben sich z.B. aus der Berechnung des Schadens für das Unternehmen im Fall einer Systemhavarie. Der monetäre Schaden wird meist vom Management berechnet und als ein Wert in Euro pro Zeiteinheit angegeben. Die Höhe der Ausfallkosten ist abhängig vom Unternehmen bzw. von der Branche (z.B. Industrie/öffentliche Verwaltung), aber auch von der Sparte, in der die Software eingesetzt wird (z.B. Produktion/Einkauf).

In der Regel wird die gewünschte Systemverfügbarkeit in *Service Level Agreements* (SLA) vereinbart, die Sie als Administrator erfüllen müssen. Deshalb ist es aus Ihrer Sicht wichtig zu wissen, welche Investitionen (z.B. für technische Ausrüstung oder Servicepersonal) notwendig sind, um für das jeweilige System einen bestimmten Grad an Verfügbarkeit gewährleisten zu können. Dabei gilt, dass die Kosten einer Recovery umso höher sind, je weniger Zeit sie in Anspruch nehmen soll. Durch Prävention (siehe Kapitel 10, »Sicherheitsverwaltung«) und einen guten Recovery-Plan können Sie die Kosten jedoch beeinflussen.

Aus Sicht der fachlichen Unternehmenseinheiten ist zu bedenken, dass Hochverfügbarkeit ihren Preis hat. Wird hier am falschen Ende gespart, gibt

es oft ein böses Erwachen. Die Kosten müssen entsprechend im Verwaltungs- oder IT-Budget eingeplant werden.

[zB] **Finanzielle Auswirkungen eines Havariefalls**

Im Folgenden geben wir Ihnen drei Beispiele dafür, wie die finanziellen und unternehmerischen Auswirkungen für einen Havariefall berechnet werden können.

- **Beispiel 1:** Bei der Hochrechnung des monetären Schadens bei einem Systemausfall hat Ihr Unternehmen festgelegt, dass Transaktionsdaten nur für den Zeitraum von einer Stunde verloren gehen dürfen. Die entstehenden Kosten gehen von 1.000 verlorenen Transaktionen pro Stunde aus, die in das SAP-System eingegeben werden und nicht wiederhergestellt werden können. Ein solcher Transaktionsverlust kann zu Umsatzverlusten und verärgerten Kunden führen. Wenn Aufträge verloren gehen, auf deren rasche Ausführung ein Kunde angewiesen ist, kann die Situation kritisch werden. In diesem Fall müssen Sie Ihren Sicherungsrhythmus entsprechend kurz auslegen, z.B. durch eine stündliche Sicherung der Transaktionsprotokolle.
- **Beispiel 2:** In Ihrem Unternehmen wurde festgelegt, dass ein System nicht länger als drei Stunden offline sein darf. Die entstehenden Kosten (beispielsweise wurden 20.000 EUR pro Stunde berechnet) resultieren daraus, dass keine Verkäufe verbucht werden können. In diesem Fall benötigen Sie eine entsprechend effiziente Notfallstrategie bzw. -infrastruktur, um das System innerhalb von drei Stunden wieder in Betrieb zu nehmen.
- **Beispiel 3**: Bei einem Notfall, wie etwa dem Verlust des Gebäudes mit dem SAP-Rechenzentrum, kann das Unternehmen nur eine Ausfallzeit von zwei Tagen zulassen. Nach zwei Tagen wenden sich die ersten Kunden ab. Es muss also eine alternative Methode gefunden werden, um das Geschäft weiterzuführen, z.B. wird ein Ausweichrechenzentrum aufgebaut oder ein Notfallvertrag mit einem externen Dienstleister abgeschlossen.

7.2.2 Wann sollte das Disaster-Recovery-Verfahren beginnen?

Für jeden Disaster-Recovery-Plan muss anhand eindeutiger Kriterien festgelegt werden, ab wann er in Kraft tritt und ab wann das Verfahren beginnt. Stellen Sie sich folgende Fragen:

- Aus welchen Merkmalen besteht eine Notsituation?
- Wurden diese Merkmale in der vorliegenden Situation erfüllt?
- Wer muss zu Rate gezogen werden, um die Situation zu bewerten? Die entsprechende Person sollte sowohl Kenntnisse von den Auswirkungen des Ausfalls auf den Geschäftsablauf als auch von der Problematik der Recovery haben.

Ergebnis dieser Überlegungen sollte sein, dass Sie sich jederzeit sofort darüber im Klaren sein können, ob Sie Ihr Disaster-Recovery-Verfahren initiieren müssen oder nicht. Alternativ definieren Sie ein Gremium, das alle für eine Entscheidung notwendigen Informationen innerhalb kürzester Zeit zusammentragen und bewerten sowie eine Entscheidung über das Einleiten des Recovery-Verfahrens treffen kann.

7.2.3 Zu erwartende Ausfallzeit

Die *Ausfallzeit* ist der Zeitraum, in dem das System nicht zur Verfügung steht. Sie können die Ausfallzeit nur schätzen. In der Regel liegt sie etwas höher als die Wiederherstellungszeit, da nach einer Wiederherstellung z.B. einige Tests durchgeführt, Benutzerstammsätze entsperrt und Benachrichtigungen versandt werden müssen. Umso bedeutsamer ist es, dass Sie die benötigte Wiederherstellungszeit möglichst genau kennen.

Während der Ausfallzeit können z.B. keine Aufträge bearbeitet und keine Produkte versandt werden. Der daraus entstehende Schaden ist nur ein Teil der Kosten, die für eine Disaster Recovery anfallen. Um eine Unterbrechung der Geschäfte so weit wie möglich zu verhindern, müssen alternative Prozesse geprüft werden, die genutzt werden können, während das SAP-System wiederhergestellt wird.

Folgende Faktoren führen bei Ausfallzeiten zu Kosten:

- Die Zeitspanne, in der das SAP-System nicht genutzt werden kann. Je länger das System nicht arbeitet, desto länger dauert es im Nachhinein, die Verluste nach erfolgreicher Recovery wieder aufzuholen. Die Transaktionen aus den alternativen Prozessen, die während der Ausfallzeit genutzt wurden, müssen in das System eingespeist werden, um es zu aktualisieren. In einer Umgebung mit umfangreichen Transaktionen kann die Situation problematisch werden.
- Ein ausgefallenes System verursacht mehr Kosten als ein laufendes System, da zusätzliche Technik oder weiteres Personal eingesetzt werden muss.
- Kunden, die nicht bedient oder unterstützt werden können, wandern möglicherweise zur Konkurrenz ab.
- Eventuell kommen auch Folgeprozesse zum Erliegen, die zu Regressansprüchen Ihrer Kunden führen.

Die Dauer einer akzeptablen Ausfallzeit variiert je nach Unternehmen und der Art der Geschäfte.

7.2.4 Wiederherstellungszeit

Als *Wiederherstellungszeit* wird die für die Wiederherstellung der verlorenen Daten und der Betriebsfähigkeit des Systems notwendige Zeit verstanden. Unterschiedliche Notfallszenarien haben unterschiedliche Wiederherstellungszeiten, die von den betrieblichen Notwendigkeiten (z.B. Umfang der wiederherzustellenden Daten) abhängig sind.

Die Wiederherstellungszeit muss an die Unternehmenserfordernisse angepasst sein. Wenn die aktuelle Wiederherstellungszeit das Zeitlimit dieser Maßgaben überschreitet, muss dieses Missverhältnis den zuständigen Managern oder Führungskräften mitgeteilt werden. Ein Missverhältnis kann folgendermaßen beseitigt werden:

- durch Investition in Geräte, Prozesse und Einrichtungen, die die Wiederherstellungszeit verkürzen
- durch eine Änderung der Unternehmenserfordernisse, sodass längere Wiederherstellungszeiten möglich werden

[zB] Wiederherstellungszeit durch zusätzliche Ressourcen vermindern

In einem Unternehmen würde die Wiederherstellung des Systems eine Woche dauern, wenn ein einziger Mitarbeiter mit dieser Aufgabe betraut wäre. Das Unternehmen kann sich die daraus entstehenden Kosten und Ertragsverluste nicht leisten: Während dieses Zeitraums würden Kunden zur Konkurrenz abwandern, Lieferantenrechnungen würden zur Zahlung fällig, und Rechnungen würden nicht beglichen. In einer solchen Situation müsste das Management zusätzliche Ressourcen bereitstellen, um die Wiederherstellung auf ein akzeptables Zeitmaß zu reduzieren.

Wenn Sie Ihr Recovery-Verfahren nicht testen (siehe Abschnitt 7.8, »Testen des Disaster-Recovery-Verfahrens«), bleibt die benötigte Wiederherstellungszeit nur ein Schätzwert. Sorgen Sie durch gründliche Tests dafür, dass Sie im Notfall, ausgehend von einer breiten Erfahrungsbasis, möglichst genau sagen können, wie viel Zeit eine Wiederherstellung in Anspruch nehmen wird. Dadurch können Sie auch gegenüber den Anwendern genauere Aussagen über die zu erwartende Ausfallzeit machen.

7.2.5 Kommunikation im Havariefall

Ein Teil Ihrer Notfallplanung sollte ein Kommunikationskonzept sein. Auch wenn sich ein Systemausfall in der Regel recht deutlich bemerkbar macht, ist es für die Anwender mindestens ärgerlich, wenn sie über ihre Situation im Unklaren gelassen werden.

In bestimmten Unternehmensbereichen kann ein Systemausfall dazu führen, dass der gesamte Betrieb zum Erliegen kommt. Die Verantwortlichen können nicht angemessen reagieren, wenn ihnen nicht mitgeteilt wird, wann das System voraussichtlich wieder zur Verfügung steht.

Überlegen Sie gegebenenfalls auch in Zusammenarbeit mit den Fachanwendern Folgendes:

- Wer ist von einem Systemausfall betroffen?
- Welche Folgen hat der Systemausfall für die Fachbereiche bzw. welche besonderen Abhängigkeiten bestehen?
- Innerhalb welches Zeitraums muss über den Systemausfall informiert werden?
- Welche Informationen sollen gegeben werden (z.B. Art, Ursache und Umfang der Störung, voraussichtliche Ausfallzeit)?
- Welche Ansprechpartner sollen informiert werden?
- Wie werden die Informationen weitergegeben bzw. wie sehen die Kommunikationsketten aus?
- Welche Kommunikationswege stehen im Havariefall noch zur Verfügung? Wie wird kommuniziert, wenn z.B. das E-Mail-System ebenfalls ausgefallen ist?
- Wie wird nach der Systemwiederherstellung darüber informiert, dass das System wieder verfügbar ist?
- In welchem Umfang wird über die Analyse und Aufarbeitung des Vorfalls informiert?

Planen Sie die Kommunikation aktiv in Ihren Recovery-Plan mit ein, und stimmen Sie sich mit den Fachabteilungen ab. Eine gute Kommunikation wirkt in einer Notfallsituation deeskalierend. Sie müssen sich nicht um das Abwehren von Beschwerden kümmern, sondern können sich auf die Systemwiederherstellung konzentrieren.

7.3 Recovery-Team und Rollenverteilung

An einer Systemwiederherstellung sind im Normalfall mehrere Personen beteiligt, das sogenannte *Recovery-Team*. Um die Disaster Recovery möglichst schnell und effizient abwickeln zu können, muss die Koordination des Teams optimal laufen. In einem Recovery-Team gibt es vier Schlüsselrollen:

- **Recovery-Manager**
  Der Recovery-Manager ist für die komplette technische Wiederherstellung verantwortlich, alle Aktivitäten sollten von ihm koordiniert werden.
- **Kommunikationsbeauftragter**
  Der Kommunikationsbeauftragte betreut die Benutzer (per Telefon, E-Mail etc.) und unterrichtet das Topmanagement vom aktuellen Wiederherstellungsstatus. Übernimmt eine Person die gesamte Kommunikation, kann der Rest der Gruppe sich ohne Unterbrechungen dem eigentlichen Recovery-Verfahren widmen.
- **Technisches Recovery-Team**
  Dieses Team arbeitet an der Wiederherstellung des Systems. Im Lauf der Recovery müssen die ursprünglichen Pläne vielleicht geändert werden. Das technische Recovery-Team muss die Änderungen verwalten und die technische Wiederherstellung des Systems koordinieren.
- **Test- und Abnahmemanager**
  Nach erfolgter Recovery koordiniert und plant der Test- und Abnahmemanager die Testverfahren und -abnahmen.

Die Anzahl der Mitarbeiter, die diese Rollen übernehmen, variiert je nach Unternehmensgröße. In einem kleinen Unternehmen können z. B. Recovery-Manager und Kommunikationsbeauftragter ein und dieselbe Person sein. Die Bezeichnungen und Aufgabenbereiche variieren vermutlich je nach Bedarf Ihres Unternehmens.

Strukturieren Sie Ihr Disaster-Recovery-Konzept so, dass für jedes Teammitglied bzw. für jede Rolle klar definiert ist, welche Aufgaben zu welchem Zeitpunkt auszuführen sind. Beschreiben Sie die Abhängigkeiten und Abstimmungsprozesse zwischen den Rollen, und erstellen Sie Checklisten für jeden Teil des Teams.

[+] **Statusaushang**

Um Störungen der Mitarbeiter zu vermeiden, die an der Recovery arbeiten, empfiehlt es sich, einen Statusaushang zu erstellen. Darauf sollten Schlüsselpunkte des Recovery-Plans sowie Schätzungen verzeichnet sein, wann das System wiederhergestellt und einsatzfähig sein wird.

Berücksichtigen Sie auch, dass wichtige Mitarbeiter zum Zeitpunkt des Notfalls nicht verfügbar sein könnten, z. B. wegen Urlaub oder Krankheit. Das Team muss auch ohne diese Personen eine erfolgreiche Recovery durchführen können. In einer tatsächlichen Notsituation kann diese Frage sehr dringlich werden.

[!] **Planen Sie mit Mitarbeitern von außen**

Wenn es sich bei dem Notfall um eine größere Naturkatastrophe handelt, werden sich Ihre Mitarbeiter vor Ort größere Sorgen um ihre Familien als um das Unternehmen machen. Bei manchen Szenarien kann es auch dazu kommen, dass wichtige Mitarbeiter verletzt oder gar getötet werden. Sie sollten sich auch auf solche Situationen einrichten und Pläne erarbeiten. Planen Sie ein, dass Mitarbeiter aus anderen Standorten eingeflogen und in das Recovery-Team integriert werden müssen.

7.4 Arten der Disaster Recovery

Disaster-Recovery-Szenarien lassen sich in zwei Arten unterteilen:

- **Eigen-Recovery**
  Eigen-Recovery ist Disaster Recovery, die Sie selbst an Ihrem Unternehmensstandort durchführen. Die eigene Infrastruktur muss dazu weitgehend intakt geblieben sein, was meist der Fall ist. Im Optimalfall wird die Recovery an der Originalhardware vorgenommen, im schlimmsten Fall muss die Originalhardware durch ein Sicherungssystem ersetzt werden.
- **Fremd-Recovery**
  Fremd-Recovery ist Disaster Recovery, die an einem speziellen Disaster-Recovery-Standort durchgeführt wird. Bei diesem Szenario sind die komplette Hardware und Infrastruktur durch Feuer, Überschwemmung, Erdbeben oder Ähnliches vernichtet worden. Die neuen Server müssen von Grund auf konfiguriert werden.

Berücksichtigen Sie im Fall der Fremd-Recovery unbedingt, dass eine zweite Wiederherstellung des Systems am ursprünglichen Standort stattfinden muss, sobald die ursprüngliche Einrichtung wieder aufgebaut worden ist. Planen und terminieren Sie die zweite Wiederherstellung so, dass möglichst wenige Benutzer behindert werden, denn auch während dieser Wiederherstellung ist das System natürlich nicht einsatzbereit.

7.5 Notfallszenarien

Viele Notfallszenarien sind denkbar, und es ist unmöglich, für alle möglichen Szenarien Pläne zu entwickeln. Um die Aufgabe überschaubar zu halten, sollten Sie sich daher auf drei bis fünf wahrscheinliche Szenarien beschränken. Tritt ein Notfall ein, können Sie sich an das Szenario halten, das dem tatsächlichen Notfall am ehesten entspricht. Ein Notfallszenario besteht aus folgenden Punkten:

- Beschreibung der Notsituation
- Planung der Hauptaufgaben auf hoher Ebene
- geschätzte Ausfallzeit

So gestalten Sie die Vorbereitung auf den Ernstfall mit Notfallszenarien am sinnvollsten:

1. Nutzen Sie Abschnitt 7.5.1, »Beschädigte Datenbank«, bis Abschnitt 7.5.3, »Vollständiger Verlust oder Zerstörung der Servereinrichtung«, als Ausgangspunkt, und bereiten Sie drei bis fünf Szenarien vor, die eine möglichst große Bandbreite der denkbaren Notsituationen abdecken.
2. Erstellen Sie für jedes Szenario einen Plan der Hauptaufgaben auf hoher Ebene.
3. Testen Sie die geplanten Szenarien, indem Sie unterschiedliche Notfälle simulieren und prüfen, ob Ihre Szenarien auf die tatsächliche Notsituation anwendbar wären.
4. Ist dies nicht der Fall, ändern Sie die Szenarien ab oder entwickeln neue.
5. Wiederholen Sie den Prozess.

Die folgenden drei Beispiele sind nach steigendem Schweregrad angeordnet. Beachten Sie, dass die genannten Ausfallzeiten dabei nur Beispiele sind. Sie sollen lediglich illustrieren, welche Situationen auf Sie zukommen können. Ihre eigene Ausfallzeit wird von diesen Angaben abweichen. Sie müssen also die Beispielausfallzeit durch eine Ausfallzeit ersetzen, die auf Ihre Umgebung zutrifft. Es soll verdeutlicht werden, dass abhängig von der konkreten Notsituation unterschiedlich umfangreiche Maßnahmen zu ergreifen sind und dass auch bei vermeintlich geringfügigen Schäden massive Ausfallzeiten entstehen können.

7.5.1 Beschädigte Datenbank

Eine Beschädigung der Datenbank kann z.B. entstehen, wenn irrtümlich Testdaten in das Produktivsystem geladen wurden oder ein fehlerhafter Transport von Daten in das Produktivsystem zu einem Absturz führt. Bei einem solchen Störfall müssen die SAP-Datenbank und die zugehörigen Betriebssystemdateien wiederhergestellt werden. Die Ausfallzeit beträgt beispielsweise vier Stunden.

7.5.2 Hardwareausfall

Die folgende Hardware kann ausfallen:

- Prozessoren
- Festplatten oder deren Steuereinheit
- RAID-Controller, wodurch es zu einem Ausfall des Arrays kommt

Bei einem solchen Ausfall sind folgende Schritte erforderlich:

1. die ausgefallene Hardware ersetzen
2. gegebenenfalls den Server neu aufbauen (Betriebssystem und Programme)
3. SAP-Datenbank und zugehörige Dateien wiederherstellen

Die Ausfallzeit beträgt beispielsweise drei Tage und umfasst:

- zwei Tage zur Beschaffung von Ersatzhardware
- einen Tag zum Neuaufbau des Servers (durch eine Person), das heißt acht Stunden Arbeitszeit

Ersatz des Produktivservers planen **[+]**

Planen und testen Sie den Einsatz Ihres Testsystems (QAS) als Sicherungsserver, wenn der Produktivserver (PRD) ausfällt.

7.5.3 Vollständiger Verlust oder Zerstörung der Servereinrichtung

Folgende Komponenten können in einem Katastrophenfall zerstört werden:

- die Server
- die gesamte stützende Infrastruktur
- die gesamte Dokumentation und die Materialien im Gebäude
- das Gebäude selbst

Ein vollständiger Einrichtungsverlust kann das Resultat von Naturkatastrophen wie Feuer, Überschwemmungen, Orkanen oder von durch Menschen verursachten Katastrophen sein. In einem solchen Katastrophenfall sind folgende Schritte erforderlich:

1. die zerstörten Einrichtungen ersetzen
2. die zerstörte Infrastruktur ersetzen
3. die zerstörte Hardware ersetzen
4. den Server und die SAP-Umgebung neu aufbauen (Hardware, Betriebssystem, Datenbank etc.)
5. die SAP-Datenbank und zugehörige Dateien wiederherstellen

Die Ausfallzeit beträgt beispielsweise acht Tage und umfasst folgende Aspekte:

- Mindestens fünf Tage zur Beschaffung der Hardware. Wenn es sich um eine regionale Katastrophe handelt, kann die Beschaffung auch länger dauern, da auch die Lieferanten betroffen sein könnten.

[+] **Überregionale Lieferanten**

Wenden Sie sich an überregionale Lieferanten mit mehreren regionalen Verteilzentren. Als zusätzliche Sicherung sollten Sie nach alternativen Lieferanten in entfernteren Regionen Ausschau halten.

- zwei Tage zum Neuaufbau des Servers (durch eine Person), das heißt 16 Stunden Arbeitszeit
- Während die Hardware beschafft und der Server neu aufgebaut wird, muss eine Alternativeinrichtung arbeiten, in der ein minimales Notfallnetzwerk konstruiert werden kann. Die Integration in das Notfallnetzwerk kann z.B. einen Tag dauern.

Ein vollständiger Verlust erfordert eine Wiederherstellung in einer neuen Einrichtung bzw. einem Ausweichgebäude. Je nach Unternehmensgröße, Bedeutung des SAP-Systems für die Geschäftsabläufe und regionalem Risiko von Naturkatastrophen ist eventuell der Aufbau eines redundanten Rechenzentrums sinnvoll. Wenn eines Ihrer Rechenzentren zerstört wurde, könnte der Betrieb der Systemlandschaft schnell in das zweite Rechenzentrum umgeschaltet werden. Die beiden Rechenzentren müssen dafür jedoch mindestens mehrere Kilometer voneinander entfernt aufgebaut sein. Sind sie in demselben Gebäude untergebracht, würden bei einer Havarie mit hoher Wahrscheinlichkeit beide Rechenzentren ausfallen.

Sollte Ihr Unternehmen nicht die Mittel für ein redundantes Rechenzentrum haben oder einsetzen wollen, können Sie auch einen Vertrag über einen Disaster-Recovery-Standort mit einem externen Dienstleister abschließen. Im Havariefall können Sie die Hardware dieses Dienstleisters für den Notbetrieb nutzen.

[!] **Recovery-Standort im Ernstfall**

Nur weil Sie einen Vertrag für einen Disaster-Recovery-Standort haben, ist dies noch keine Garantie dafür, dass dieser Standort im Ernstfall auch zur Verfügung stehen wird. Bei einer Katastrophe, die eine ganze Region in Mitleidenschaft zieht, werden viele andere Unternehmen auf dieselben Disaster-Recovery-Standorte zurückgreifen wollen wie Sie. In einer solchen Situation könnte es sein, dass Sie ohne Recovery-Standort auskommen müssen, da andere diesen Standort vor Ihnen gebucht haben.

Ein Disaster-Recovery-Standort oder ein Notfallrechenzentrum ist unter Umständen nicht mit Geräten vom gleichen Leistungsgrad wie Ihr Produktivsystem ausgestattet. Berücksichtigen Sie in Ihrer Planung also auch eine verringerte Performance und begrenzte Transaktionen. Reduzieren Sie z.B. Hintergrundjobs auf das Nötigste, oder lassen Sie nur Benutzer mit wirklich essenziellen Geschäftsaufgaben auf dem Recovery-System zu.

7.6 Recovery-Skript

Ein Recovery-Skript ist ein Dokument, das Schritt-für-Schritt-Anweisungen für folgende Aspekte beinhaltet:

- das Verfahren zur Wiederherstellung des SAP-Systems
- die für jeden Schritt zuständigen Personen
- bei langwierigen Schritten der geschätzte Zeitaufwand
- die Abhängigkeiten zwischen den Schritten

Ein Skript hilft Ihnen dabei, geeignete Schritte zur Wiederherstellung des SAP-Systems einzuleiten, und vermeidet das Auslassen von Schritten. Wenn Sie einen wichtigen Schritt versehentlich auslassen, müssen Sie unter Umständen das gesamte Verfahren von vorn beginnen, wodurch sich die Wiederherstellung natürlich verzögert.

Folgendes ist zur Erstellung eines Recovery-Skripts notwendig:

- eine Checkliste für jeden Schritt
- ein Dokument mit Screenshots zur Erklärung der Anweisungen (bei Bedarf)
- Flussdiagramme, wenn die Abfolge der Schritte oder Aktivitäten komplex oder verwirrend ist

Ist die für die Recovery hauptverantwortliche Person nicht verfügbar, unterstützt ein Recovery-Skript ihre Stellvertreter bei der Erfüllung dieser Aufgabe. Deshalb muss das Skript alle Aufgaben vollständig und möglichst leicht verständlich beschreiben.

Wichtige Schritte des Recovery-Verfahrens

Um den Recovery-Prozess zu verkürzen, können Sie ein Verfahren definieren, bei dem so viele Aufgaben wie möglich parallel erledigt werden. Fügen Sie für jeden Schritt einen Zeitplan hinzu. Die wichtigsten Schritte sind:

1. Während einer Notsituation können Sie die Recovery unterstützen, indem Sie Folgendes tun:
   - Fakten sammeln
   - die letzten Sicherungsbänder vom Fremdlagerort zurückfordern
   - das Crash Kit bereithalten (siehe Abschnitt 7.7, »Crash Kit«)
   - alle benötigten Mitarbeiter benachrichtigen (hierzu gehören das interne SAP-Team, betroffene wichtige Benutzer, Infrastruktur-Support, IT, Einrichtungen, Berater auf Abruf etc.)
   - Funktionsorganisationen (Vertrieb, Buchhaltung und Versand) auf alternative Verfahren für wichtige Geschäftstransaktionen und -verfahren vorbereiten
   - Nicht-SAP-Systeme, die über Schnittstellen von und zum SAP-System verfügen, über den Systemausfall informieren
2. Minimieren Sie die Auswirkungen des Ausfalls durch folgende Maßnahmen:
   - alle zusätzlichen Transaktionen in das System anhalten (z. B. Schnittstellen aus anderen Systemen)
   - Transaktionsbelege sammeln, die erneut manuell eingegeben werden müssen

3. Starten Sie den Planungsprozess mit folgenden Maßnahmen:
   - das Problem analysieren
   - die Szenarienpläne auswählen, die dem eingetretenen Notfall am ehesten entsprechen
   - die Pläne bei Bedarf ändern
4. Entscheiden Sie, wann das Disaster-Recovery-Verfahren beginnen soll:
   - Anhand welcher Kriterien wurde das Eintreten einer Notsituation bestimmt? Wurden diese Kriterien erfüllt?
   - Wer trifft die endgültige Entscheidung darüber, ob eine Notsituation eingetreten ist?
5. Stellen Sie das Eintreten eines Notfalls fest.
6. Führen Sie das Recovery-Verfahren durch.
7. Lassen Sie das wiederhergestellte System testen, und nehmen Sie es ab. Das Testen sollten wichtige Benutzer übernehmen. Diese Benutzer verwenden eine Checkliste, um abzuklären, ob das System zufriedenstellend wiederhergestellt wurde.
8. Aktualisieren Sie das System mit den Transaktionen, die während des Ausfalls von alternativen Prozessen übernommen wurden. Sobald dieser Schritt abgeschlossen ist, sollte das Ergebnis erneut abgenommen werden.
9. Benachrichtigen Sie die Benutzer, dass das System wieder einsatzbereit ist.
10. Führen Sie eine Nachbesprechung zu dem Störfall durch, um die Gründe der Havarie zu ermitteln.
11. Werten Sie die Erfahrung der Systemwiederherstellung im Recovery-Team aus, und optimieren Sie Ihre Disaster-Recovery-Pläne.

Das Recovery-Skript muss im Havariefall schnell zugänglich sein. Es darf nicht nur auf einem Server abgelegt sein, der eventuell durch einen Netzwerkausfall nicht mehr erreichbar ist. Ein Papierexemplar kann durch einen Brand zerstört worden sein. Bereiten Sie sich auf diese Notfallszenarien vor, und hinterlegen Sie das Recovery-Skript entsprechend redundant. Sorgen Sie dafür, dass der Ablageort allgemein bekannt und im Notfall für die Verantwortlichen zugänglich ist.

Abhängigkeit von anderen Anwendungen

Ihr SAP-System ist in der Regel über Schnittstellen mit anderen vor- oder nachgelagerten Systemen verbunden. Fällt das SAP-System aus, können

Vorsysteme unter Umständen ebenfalls zum Stillstand kommen, weil RFC-Aufrufe massenweise auflaufen und nicht abgearbeitet werden können. Folgesysteme können nicht arbeiten, weil Ihr SAP-System die notwendigen Daten nicht zur Verfügung stellt. So kann leicht eine Kettenreaktion mit weitreichenden Folgen für Systemlandschaft und Geschäftsprozesse entstehen.

Berücksichtigen Sie darum in Ihrem Recovery-Skript die Kommunikation mit den Verantwortlichen der verbundenen Anwendungen. Lassen Sie die Schnittstellen stoppen, oder halten Sie sie selbst an. Halten Sie fest, wie nach einer Systemwiederherstellung die Daten neu synchronisiert werden.

7.7 Crash Kit

Ein *Crash Kit* enthält alles, was Sie benötigen, um die SAP-Server neu aufzubauen, das SAP-System neu zu installieren und die SAP-Datenbank mitsamt den dazugehörigen Dateien wiederherzustellen. Sie müssen daher in einem oder mehreren Behältern – physisch, also in Form von Sicherungsbändern, Hardware und Dokumenten, und/oder digital – alles zusammentragen, was Sie benötigen, um Ihre SAP-Umgebung wiederherstellen zu können. Wenn Ihr Standort evakuiert werden muss, werden Sie keine Zeit mehr haben, um in letzter Minute noch schnell alles zusammenzusuchen.

Sie sollten Ihr Crash Kit regelmäßig durchsehen und prüfen, ob noch alle Elemente aktuell und einsatzbereit sind. Ein Servicevertrag ist ein gutes Beispiel für einen Bestandteil des Crash Kits, bei dem eine solche Prüfung notwendig ist: Ist der Vertrag nicht mehr gültig, weil er nicht rechtzeitig verlängert wurde, können Sie im Notfall eventuell nicht auf die Hilfe externer Dienstleister zurückgreifen oder müssen erst Verhandlungen aufnehmen.

[!] **Crash Kit aktualisieren**

Wenn an einer Komponente (Hardware oder Software) auf dem Server eine Änderung vorgenommen wird, ersetzen Sie die nicht mehr aktuellen Bestandteile in Ihrem Crash Kit durch aktuelle und getestete Elemente.

Das Crash Kit sollte räumlich getrennt von den Servern aufbewahrt werden. Wenn es sich im Serverraum befindet, wird bei Verlust der Server auch das Crash Kit in Mitleidenschaft gezogen. Beispiele für geeignete Lagermöglichkeiten sind:

- kommerzieller Lager- und Datenspeicherort außerhalb des eigenen Standorts
- andere Unternehmensstandorte
- ein anderer sicherer Gebäudetrakt

Im Folgenden nennen wir die wichtigsten Artikel, die in einem Crash Kit enthalten sein sollten. Je nach Ihrer speziellen Umgebung können Sie Artikel hinzufügen oder weglassen. Die Inventarliste ist nach Dokumentation und Software geordnet.

Dokumentation

Die folgende Dokumentation muss im Crash Kit enthalten sein:

- Disaster-Recovery-Skript
- Test- und Verifikationsskript für funktionale Benutzergruppen, anhand dessen die Funktionsfähigkeit des wiederhergestellten Systems festgestellt wird
- Installationsanweisungen:
  - Betriebssystem
  - Datenbank
  - SAP-System
- spezielle Installationsanweisungen für:
  - Treiber, die manuell installiert werden müssen
  - Programme, die auf eine bestimmte Weise installiert werden müssen
- Kopien von:
  - SAP-Lizenzen aller Instanzen
  - Servicevereinbarungen (mit Telefonnummern) für alle Server

Gültigkeit der Servicevereinbarungen prüfen [!]

Überzeugen Sie sich davon, dass die Servicevereinbarungen noch gültig sind. Sie sollten diese Prüfung regelmäßig durchführen.

- Anweisungen zum Abruf von Sicherungsbändern aus Fremd-Datenspeichern außerhalb des eigenen Standorts
- Eine Liste der Personen, die zum Abruf von Sicherungsbändern aus Datenspeichern außerhalb des eigenen Standorts autorisiert sind. Diese Liste muss der Liste entsprechen, die beim externen Datenspeicher vorliegt.

- Eine Teileliste, die genügend Details enthält, um eine neue Hardware zu kaufen oder zu leasen, wenn der Server zerstört wurde. Nach einer gewissen Zeit können Originalteile nicht mehr erhältlich sein. Sie sollten dann eine alternative Teileliste entwerfen. Zu diesem Zeitpunkt sollten Sie auch über eine Aktualisierung der Ausrüstung nachdenken.
- Layout des Dateisystems
- Layout der Hardware
- Telefonnummern von:
  - wichtigen Benutzern
  - Mitarbeitern des Informationsservices
  - Einrichtungspersonal
  - anderem Infrastrukturpersonal
  - Beratern (SAP, Netzwerk etc.)
  - SAP-Hotline
  - Datenspeichern außerhalb des eigenen Standorts
  - Sicherheitsabteilung oder -mitarbeitern
  - Kontakten im Rahmen von Servicevereinbarungen
  - Hardwarelieferanten

Software

Alle Softwarebestandteile, die für einen vollständigen Wiederaufbau des Servers benötigt werden, sollten das Crash Kit enthalten.

- Betriebssystem:
  - Installations-Kit
  - Treiber für Hardware, die nicht im Installations-Kit enthalten ist, wie etwa Netzwerkkarten oder SCSI-Controller
  - Service Packs, Updates und Patches
- Datenbank:
  - Installations-Kit
  - Service Packs, Updates und Patches
  - Recovery-Skript zur Automatisierung der Datenbankwiederherstellung
- SAP-System:
  - neue Installationsdateien des verwendeten SAP-Releases und der Datenbank

  - aktuell installierter Kernel
  - Systemprofildateien
  - Datei *tpparam*
  - Datei *saprouttab*
  - Dateien *saplogon.ini* (für SAP GUI)
- andere Programme, die im SAP-System integriert sind (z.B. ein Steuerpaket)
- andere Software für die SAP-Installation:
  - Hilfsprogramme
  - Sicherung
  - Steuerprogramm USV
  - Hardwaremonitor
  - FTP-Client
  - Remote-Control-Programm
  - Systemmonitore

Crash-Kit-Inventar [+]

Die Person, die das Crash Kit versiegelt, sollte auch eine Inventarliste zusammenstellen und diese mit Datum und Unterschrift versehen. Wenn das Siegel gebrochen wurde, wurden vermutlich auch Artikel entfernt oder geändert, die das Kit in Notfällen nutzlos machen könnten.

7.8 Testen des Disaster-Recovery-Verfahrens

Indem Sie eine Disaster Recovery simulieren, können Sie sicherstellen, dass Sie Ihr System auch tatsächlich wiederherstellen und alle Aufgaben ausführen können, die im Disaster-Recovery-Plan vorgesehen sind. Durch die Simulation können Sie Folgendes feststellen:

- ob Ihr Disaster-Recovery-Verfahren funktioniert
- ob es Änderungen gegeben hat, Schritte nicht dokumentiert oder erforderliche Aktualisierungen nicht durchgeführt wurden
- ob einige Schritte zusätzlicher Erläuterung bedürfen
- ob Schritte, die der dokumentierenden Person vollkommen klar sind, für andere Personen ebenso nachvollziehbar sind
- ob ältere Hardware nicht länger verfügbar ist

Trifft einer dieser Fälle zu, überarbeiten Sie Ihren Recovery-Plan. Sie müssen vielleicht ein Upgrade der Hardware durchführen, damit sie mit den zurzeit verfügbaren Geräten kompatibel ist. Entwerfen Sie auch eine alternative Vorgehensweise, um auf bislang unbemerkte Unstimmigkeiten im Ernstfall reagieren zu können.

Da die tatsächliche Recovery-Zeit von vielen Faktoren beeinflusst wird, kann sie letztlich nur durch Tests bestimmt werden. Sobald Sie anstelle von Schätzungen über tatsächliche Zeitwerte verfügen, gewinnt Ihre Notfallplanung an Glaubwürdigkeit. Wenn das Verfahren oft geübt wird, weiß in einer Notsituation jeder sofort, was zu tun ist. Auf diese Weise kann möglicherweise das Schlimmste verhindert werden.

Gehen Sie folgendermaßen vor, um Ihr Disaster-Recovery-Verfahren zu testen:

1. Führen Sie Ihren Disaster-Recovery-Plan in einem Sicherungssystem oder an einem Fremdstandort aus.
2. Generieren Sie ein zufälliges Notfallszenario.
3. Führen Sie Ihren Notfallplan aus, um zu sehen, ob er in einer solchen Situation greift.
4. Nehmen Sie die Disaster Recovery an demselben Standort vor, an dem sie auch im Ernstfall erfolgen wird. Wenn Sie mehrere Recovery-Standorte haben, führen Sie die Tests an jedem dieser Standorte aus. Die Geräte, Einrichtungen und Konfigurationen können an jedem Standort unterschiedlich sein. Dokumentieren Sie alle Schritte, die an dem jeweiligen Standort ausgeführt werden müssen. So sind Sie davor gefeit, im Ernstfall feststellen zu müssen, dass Sie das System an einem bestimmten Standort nicht wiederherstellen können. Andere Optionen für Standorte, an denen Sie Ihr Disaster-Recovery-Szenario testen können, sind:
   - ein Sicherungsserver an Ihrem Standort
   - ein anderer Unternehmensstandort
   - ein anderes Unternehmen, mit dem Sie eine gegenseitige Support-Vereinbarung haben
   - ein Unternehmen, das Disaster-Recovery-Standorte und -Dienstleistungen anbietet

Während einer realen Disaster Recovery werden die Aufgaben von Ihrem Stammpersonal übernommen. Sie sollten aber Vorkehrungen für den Fall

treffen, dass während der Disaster Recovery einige der wichtigsten Mitarbeiter nicht verfügbar sind. Ein Testverfahren kann daher auch die zufällige Auswahl einer Person beinhalten, die dann als nicht verfügbar gilt und nicht am Testverfahren teilnimmt. Diese Vorgehensweise spiegelt eine reale Situation wider, in der ein wichtiger Mitarbeiter abwesend ist oder z. B. schwer verletzt wurde.

Zusätzlich sollten auch Mitarbeiter von anderen Standorten an den Tests teilnehmen. Integrieren Sie diese Personen in die Tests, da Sie sie auch während einer realen Disaster Recovery benötigen könnten. Diese Mitarbeiter können die Lücken füllen, die durch nicht verfügbares Personal entstehen.

Die Disaster Recovery sollte mindestens einmal im Jahr vollständig durchgespielt werden. Die tatsächliche Häufigkeit ist jedoch eine kaufmännische Entscheidung, die unter Berücksichtigung der entstehenden Kosten getroffen werden sollte.

Betreuung des Produktivsystems [!]

Beachten Sie, dass während des Disaster-Recovery-Tests immer noch Mitarbeiter benötigt werden, die das reale Produktivsystem betreuen.

7.9 Ausfallrisiko minimieren

Das Risiko eines Ausfalls kann auf vielerlei Weise minimiert werden. Einige der hier aufgeführten Vorschläge mögen offensichtlich erscheinen, in der Realität werden sie aber häufig außer Acht gelassen.

7.9.1 Risiko des menschlichen Versagens minimieren

Viele Notsituationen werden durch menschliches Versagen ausgelöst, beispielsweise durch einen Fehler oder durch einen übermüdeten Bearbeiter. Für potenziell gefährliche Aufgaben (wie das Löschen der Testdatenbank, das Verschieben einer Datei oder das Formatieren eines neuen Laufwerks) sollte ein Skript mit Checkliste erstellt werden, mit deren Hilfe die einzelnen Schritte verifiziert werden können.

Eigene Fähigkeiten kritisch bewerten [+]

Führen Sie keine gefährlichen Aufgaben aus, wenn Sie sich müde fühlen. Wenn Sie es dennoch tun müssen, holen Sie eine zweite Meinung ein, bevor Sie beginnen.

7.9.2 Single Points of Failure minimieren

Single Point of Failure bedeutet, dass der Ausfall einer einzigen Komponente den Ausfall des gesamten Systems nach sich zieht. So minimieren Sie das Risiko:

- Ermitteln Sie Umstände, in denen ein Single Point of Failure auftreten kann.
- Erstellen Sie eine Prognose darüber, was geschieht, wenn diese Komponente oder dieser Prozess versagt.
- Eliminieren Sie so viele Single Points of Failure wie möglich.

Single Points of Failure können Folgendes einschließen:

- Der Sicherungs-SAP-Server befindet sich in demselben Rechenzentrum wie der produktive SAP-Server. Wird das Rechenzentrum zerstört, wird damit auch der Sicherungsserver zerstört.
- Alle SAP-Server sind an denselben Stromkreis angeschlossen. Wenn der Stromkreis unterbrochen wird, werden alle Geräte in diesem Stromkreis in Mitleidenschaft gezogen. Das bedeutet, alle Server stürzen ab.

Kaskadenausfälle

Ein *Kaskadenausfall* liegt dann vor, wenn ein Ausfall weitere Ausfälle nach sich zieht, wodurch die Komplexität des Problems steigt. Die Recovery umfasst dann die koordinierte Lösung vieler Probleme.

[zB] **Kaskadenausfall**

Folgendes Beispiel soll einen Kaskadenausfall verdeutlichen:

- Ein Stromausfall in der Klimaanlage kann zu einem Ausfall der Klimakontrolle im Serverraum führen.
- Ohne Kühlung steigt die Temperatur im Serverraum über die zulässige Betriebstemperatur der Geräte.
- Die Überhitzung bewirkt einen Hardwareausfall im Server.
- Der Hardwareausfall führt zu einer Beschädigung der Datenbank.
- Zusätzlich kann die Überhitzung noch viele weitere Geräte und Systeme in Mitleidenschaft ziehen, wie etwa Netzwerkgeräte, das Telefonsystem und andere Server.

Die Wiederherstellung nach einem Kaskadenausfall kann sich komplex gestalten, z.B. weil bei der Lösung eines Problems andere Probleme oder andere beschädigte Geräte entdeckt werden oder einige Geräte nicht getestet oder repariert werden können, bevor andere Geräte nicht wieder einsatzbereit sind. Bezogen auf unser Beispiel, würde in einem solchen Fall ein System gute Dienste leisten, das die Klimaanlage oder die Temperatur des Serverraums überwacht und bei Überschreiten eines bestimmten Grenzwertes die zuständigen Mitarbeiter benachrichtigt.

7.10 Geschäftsfortführung während der Systemwiederherstellung

Während die Disaster Recovery durchgeführt wird, müssen die betroffenen Geschäftsprozesse möglichst fortgeführt werden, um finanzielle Schäden im Unternehmen zu vermeiden bzw. zu minimieren. Überlegen Sie sich, mit welchen alternativen Verfahren Sie die wichtigsten Unternehmensprozesse bei einem Ausfall des SAP-Systems aufrechterhalten können, z.B.:

- Einziehung von Barmitteln
- Auftragsbearbeitung
- Produktversand
- Rechnungsbegleichung
- Lohn- und Gehaltsabrechnung
- alternative Standorte zur Fortführung der Geschäfte

Ohne einen alternativen Prozess wird Ihr Geschäftsbetrieb zurückgehen oder völlig zum Erliegen kommen. Folgende Probleme können entstehen:

- Aufträge können nicht eingegeben werden.
- Produkte können nicht versandt werden.
- Barmittel können nicht eingezogen werden.

Alternative Prozesse sind denkbar in Form von:

- manueller Datenerfassung auf Papierbasis (z.B. handgeschriebene Bestellungen)
- Arbeit an selbstständigen PC-Systemen

Planen Sie in Zusammenarbeit mit den Fachanwendern, wie bestimmte Geschäftsprozesse während der Wiederherstellung weiterlaufen können.

Legen Sie fest, ab welchem Zeitpunkt oder bei welcher erwarteten Ausfallzeit ein alternativer Prozess in Kraft tritt. Darüber hinaus ist zu überlegen, wie die Daten, die über den Notprozess entstehen, nach der Systemwiederherstellung in das SAP-System übernommen werden können.

7.11 Fazit

Die Disaster Recovery als Spezialfall der Systemwiederherstellung muss gut vorbereitet sein. Ein profundes Konzept, die notwendigen Utensilien sowie geplante, regelmäßige Übungen bereiten Sie auf den Notfall vor. Dieses Kapitel hilft Ihnen dabei, alles Nötige zu bedenken.

Kalkulieren Sie für Ihr Unternehmen und Ihre Systeme, welche Kosten ein Systemausfall verursachen würde bzw. wie viel Schaden eine Stunde Nichtverfügbarkeit bedeutet. Konkrete Zahlen führen Ihnen und Ihrem Management am leichtesten vor Augen, wie wichtig es ist, in die Disaster Recovery zu investieren.