

Wiederanlauf braucht Tests

Um bestmöglich für den „Fall der Fälle“ gerüstet zu sein, bedarf es neben einer sorgsamem Planung auch regelmäßiger Übungen zum Wiederanlauf. Für eine möglichst störungsarme Umsetzung solcher Tests empfiehlt unser Autor ein stufenweises Konzept.

Von Bernd Ewert, Hamburg

Eine Planung des Wiederanlaufs nach Notfällen ist im Eigeninteresse und aufgrund der Gesetzeslage inzwischen in vielen Unternehmen erfolgt. Natürlich will niemand von einem Notfall betroffen sein und zum Glück ereignet er sich auch nicht allzu häufig. Was aber geschieht mit einem Plan, der nie in die Tat umgesetzt wird?! Wer wirklich wissen will, ob er beziehungsweise seine IT einen Notfall tatsächlich überleben würden, der muss nicht nur über die notwendigen Ressourcen und Pläne für den Wiederanlauf verfügen, sondern diese auch regelmäßig testen. Dabei ist besonderes

Augenmerk darauf zu legen, ob der Wiederanlauf nicht nur überhaupt, sondern auch so schnell wie vorgesehen erfolgen kann, da die Wiederherstellungszeit üblicherweise ein besonders kritischer Faktor ist.

Ein Wiederanlaufstest bildet den Ablauf im Notfall ab. Zum Glück muss man jedoch weder einen Notfall erzeugen noch ihn stets vollständig simulieren, um gegen ihn gewappnet zu sein – Aufwand und Kosten hierfür wären auch nicht angemessen. Stattdessen genügt es, Teilaspekte des Notfallplans in aufeinander aufbauenden Stufen zu testen (vgl. Abb. 1).

Test-Stufen

Alarmtest

Ein Alarmtest prüft die folgenden Punkte eines Wiederanlaufverfahrens:

- _____ Entdecken einer Notfallsituation,
- _____ Alarmierung und Benachrichtigung von geschultem Fachpersonal,
- _____ erste Einschätzung des Notfallumfangs,
- _____ Eskalation an die Entscheidungsebene,
- _____ Entscheidung über das Vorliegen eines Notfalls und
- _____ den anschließenden Aufbau der Organisation zur Notfallbewältigung.

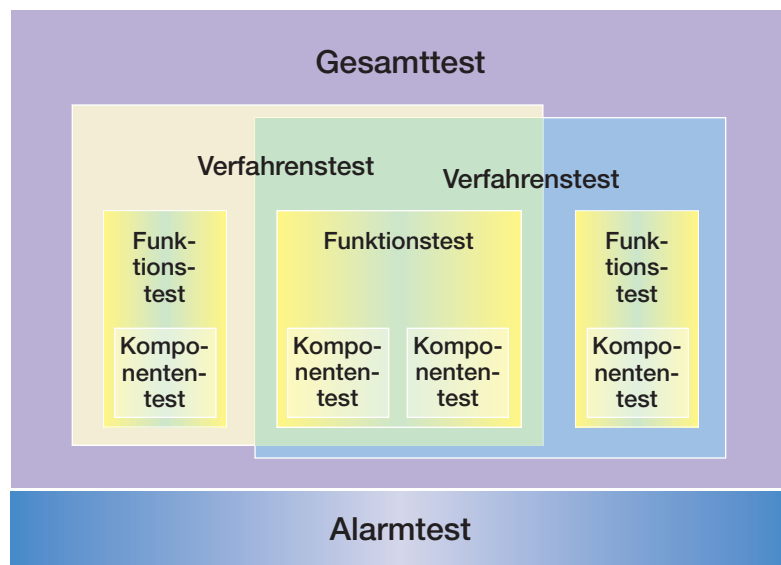
Die wesentlichen Punkte beim Alarmtest sind also das Durchlaufen der festgelegten Alarmketten und die Konfrontation des Personals mit einem Notfallszenario. Man weiß danach, wie schnell und gezielt mit den ersten Maßnahmen zur Notfallbewältigung begonnen werden kann. Teamstrukturen, die im Notfall greifen sollen, können bis hin zur Arbeitsfähigkeit der Teams verfolgt werden; dies umfasst auch die Verfügbarkeit notwendiger Arbeitsgrundlagen wie Schlüssel oder Pläne.

Alarmtests lassen sich gut mit Übungen im Rahmen des Arbeitsschutzes kombinieren. Ihre Auswirkung auf den laufenden Geschäftsbetrieb ist nur gering. Ein Alarmtest sollte pro Notfallszenario einmal im Jahr angesetzt werden.

Komponententest

Ein Komponententest soll die Ein- oder Ersetzbarkeit einzelner Ressourcen im Notfall prüfen. Er ist insbesondere anlassbezogen bei größeren Veränderungen und darüber hinaus regelmäßig für zentrales IT-Equipment wichtig. Oft können zudem Verfahren, die sich im Rah-

Abbildung 1:
Da eine Nachbildung vollständiger Notfallszenarien riskant und nicht immer notwendig ist, empfiehlt es sich, Teilaspekte des Notfallplans in aufeinander aufbauenden Stufen zu testen.



men von Installationen oder Betriebsstörungen ergeben, ebenfalls als Komponententest (aus-)gewertet werden. Beispiele sind das Unterbrechen von Verbindungen, das Ausschalten einzelner Geräte oder das Einspielen gesicherter Daten. Auch externe Dienstleistungen (z. B. die schnelle Lieferung von Ersatzressourcen) können im Rahmen von Komponententests überprüft werden; die Möglichkeit dazu sollte vertraglich abgesichert sein.

Pro Jahr sind in einer üblichen Arbeitsumgebung eine ganze Reihe von Komponententests durchzuführen. Durch sie wird punktuell geprüft, ob die Verlässlichkeit wesentlicher Pfeiler des Wiederanlaufkonzepts gegeben ist. Die Auswirkungen auf den laufenden Geschäftsbetrieb werden möglichst gering gehalten, indem man beispielsweise Zeiten wählt, an denen die zu testende Ressource nicht produktiv benötigt wird.

Funktionstest

Ein Funktionstest überprüft das Zusammenspiel verschiedener Ressourcen innerhalb einer Organisationseinheit, beispielsweise einer Abteilung. Es wird getestet, ob diese Einheit nach einem Notfall in der geplanten Zeit und im veranschlagten Ausmaß leistungsfähig ist. Besonders wichtig ist dies für Bereiche, die unternehmenskritische Funktionen gegenüber dem Markt ausüben oder von denen andere Funktionen in zeitkritischer Weise abhängig sind. Letzteres gilt vor allem für die Gewährleistung der Infrastruktur, also Gebäude- und Informationstechnik.

Ein typischer Funktionstest ist daher der Wiederanlauf der gesamten IT eines Unternehmens. Gerade hier ist das Zusammenspiel der Komponenten wichtig: beispielsweise die Erreichbarkeit über Daten-

netze, die Steuerung des Zugriffsschutzes und die Synchronität der Datensicherungen. Einen Funktionstest der Gesamt-IT sollte man natürlich so planen, dass Anwender möglichst wenig davon betroffen sind. Es ist jedoch nicht immer vermeidbar, dass er den laufenden Geschäftsbetrieb (negativ) beeinflusst; aber auch hier können Beeinträchtigungen über einen geeigneten Testzeitpunkt auf das geringstmögliche Maß begrenzt werden.

Andere Einheiten als die (Gesamt)-IT üben im Rahmen von Funktionstests eher temporäre Ersatzverfahren ohne die Verwendung der gewohnten Arbeitsumgebung, um besonders eilige Tätigkeiten schon während des Wiederanlaufs zu erledigen. So können beispielsweise Transaktionen im Börsenhandel über Tickets und die Ein- und Auslagerung von Waren in nichtchaotische Lager über Listen abgewickelt werden.

Funktionstests sollten für alle zeitkritisch operierenden Organisationseinheiten jährlich stattfinden. Sie weisen die Machbarkeit kompletter Abschnitte des Wiederanlaufplans nach und gehen deutlich über den Nachweis von Einzelverfügbarkeiten hinaus. Auf der anderen Seite fehlt auch hier noch die Integration in den Gesamtzusammenhang.

Verfahrenstest

Erst ein Verfahrenstest prüft das Zusammenspiel mehrerer organisatorischer Einheiten, sodass auch übergreifende Prozessketten dargestellt werden können. Typische Verfahrenstests sind die Durchführung geschäftlicher Transaktionen oder die Abwicklung ganzer Geschäftsvorfälle unter Notfallbedingungen.

Der Verfahrenstest ist überall dort erforderlich, wo erhebliche Abhängigkeiten zwischen verschiedenen Geschäftsfunktionen bestehen, vor allem bei der IT-Nutzung. Nach dem Wiederanlauf steht die IT im Notfall oft nur in eingeschränktem Ausmaß zur Verfügung; den Umgang der Anwender mit dieser Konstellation zu proben ist Aufgabe von Verfahrenstests. Dabei ist auch zu prüfen, ob die IT-Anwendungen im Notbetrieb von den Anwendern ausreichend performant nutzbar sind und korrekte Ergebnisse liefern.

Verfahrenstests unter Einbeziehung der gesamten IT sollten etwa einmal im Jahr durchgeführt werden. Störungen des laufenden Geschäftsbetriebs sind dabei kaum zu vermeiden, können aber meist gering gehalten werden. Wichtig ist, dass die teilnehmenden Personen jederzeit wissen, ob sie sich in einer Produktions- oder in einer Testumgebung befinden.

Gesamttest

Der Gesamttest umfasst den Wiederanlauf aller zeitkritischen

Einheiten und Prozesse, die von einem Notfallszenario betroffen sind (z. B. nach Zerstörung eines Gebäudes); er bildet den gesamten für die erste Zeit nach dem Notfall geplanten Betrieb ab. Gesamttests dienen der Prüfung aller technischen und organisatorischen Vorkehrungen sowie der Übung aller Tätigkeiten, die im Notfall durchzuführen sind. Sie integrieren alle Teilverfahren und ermöglichen damit auch die Prüfung aller Schnittstellen.

Gesamttests erfordern eine extrem sorgfältige Planung und müssen zuvor mit der Unternehmensleitung und den Leitern aller Geschäftsfunktionen abgestimmt werden. Ein Gesamttest setzt unbedingt voraus, dass die relevanten Einheiten und Prozesse vorher Verfahrens- und Funktionstests unterzogen wurden.

Aufgrund des hohen Aufwands und eines beträchtlichen Risikos werden Gesamttests nur selten durchgeführt. Oft ist absehbar, dass die erzielbaren Aussagen sich von denen aus Verfahrenstests nicht signifikant unterscheiden. Daher kann auf Gesamttests bisweilen sogar völlig verzichtet werden.

Test-Umgebung

Die Ressourcen für Tests sind grundsätzlich gemäß dem Wiederanlaufkonzept bereitzustellen. Mögliche Verfahren im Notfall sind _____ die Nutzung redundanter Ressourcen, _____ die Umwidmung von für andere Zwecke genutzten Ressourcen, _____ der Einsatz von speziell für den Notfall vorgehaltenen Ressourcen, _____ die Hinzuziehung bestehender externer Ressourcen und _____ die Neubeschaffung von Ressourcen.

Je stärker die betroffenen Ressourcen in den laufenden Geschäftsbetrieb integriert sind, umso schwieriger ist es natürlich, sie für

Tests bereitzustellen, ohne den Betrieb zu beeinträchtigen. Wo möglich, sollte mit dem Test auf betriebliche Ruhezeiten ausgewichen werden. Bei einem 7-Tage-24-Stunden-Betrieb geht das nicht – verschiedene Möglichkeiten können dann die Beeinträchtigungen minimieren helfen:

_____ Man kann speziell für den Test Ressourcen beschaffen, die im Notfall nicht vorgesehen sind. Mit jeder Abweichung vom Wiederanlaufplan wird jedoch die Aussagefähigkeit des Tests reduziert.

_____ Man kann die Störung auf weniger kritische Geschäftsfunktionen beschränken, indem man deren Ressourcen dem Betrieb entnimmt. Die entstehende Störung ist der Bedeutung des Tests gegenüberzustellen.

Die Nutzung von Ressourcen aus dem laufenden Betrieb ist

überdies dann mit besonderem Aufwand verbunden, wenn sich ihr Zustand durch den Test verändert. So können beispielsweise Möbel ad hoc umgenutzt werden, bei Datenbeständen muss nach dem Test jedoch erst der vorherige Zustand wiederhergestellt werden, bevor man wieder mit dem Normalbetrieb beginnen kann.

Solcher Aufwand und gleichzeitig die Mehrarbeit der beteiligten Anwender ist manchmal vermeidbar, indem die während des Tests getätigten Eingaben als Produktionsdaten behandelt werden. In zwei Fällen ist dies jedoch *nicht* möglich:

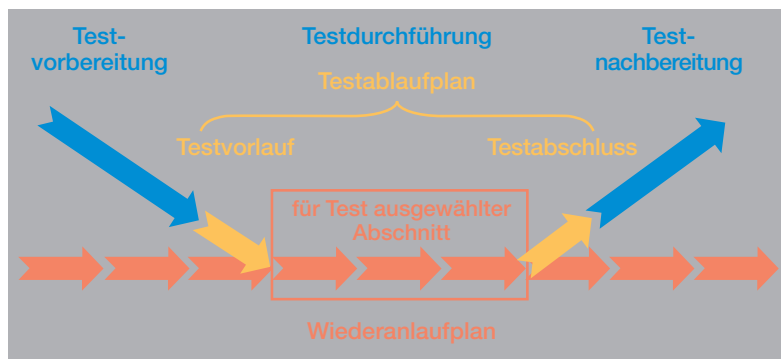
_____ Meist ist nur ein Teil der Ressourcen für den Notfall relevant, sodass der andere Teil auch beim Test nicht eingesetzt wird. Bei Abhängigkeiten zwischen beiden Teilen können dann Asynchronitäten zwischen genutzten und ungenutzten Ressourcen auftreten.

_____ Oft wird im Notfall ein Datenverlust in Kauf genommen, beispielsweise durch Einspielen der letzten synchronen Datensicherung. Im Test wird man einen solchen Datenverlust aber nicht hinnehmen wollen, sodass ein für den Notfall geplantes Verfahren des Aufbaus von Datenbeständen im Test nicht nutzbar ist.

Test-Ablauf

Ein Wiederanlauftest simuliert einen in sich abgeschlossenen Abschnitt des gesamten Wiederanlaufplans. Die darin geplanten Aktivitäten setzen auf einem Zustand auf, der im Notfall nach Eintritt eines Szenarios und dem Durchlaufen der vor dem Abschnitt gelegenen Aktivitäten eintritt. Diesen Zustand muss man daher auch für den Test zunächst herstellen, bevor die erste Aktivität aus dem Wiederanlaufplan gestartet werden kann.

Abbildung 2:
Zu einem Wiederanlauf-
test gehören
auch umfangreiche
Vor- und Nach-
arbeiten.



Um vom Betrieb in den Test und wieder zurück zu kommen, sind deshalb exakt geplanter Vorlauf und entsprechende Nacharbeiten notwendig. Diese müssen gleichzeitig dafür sorgen, dass der laufende Geschäftsbetrieb nicht nachhaltig beeinträchtigt wird. Daher ist ein ausführlicher Testablaufplan notwendig: Er umfasst die gesamte Durchführung vom Vorlauf über den ausgewählten Abschnitt des Wiederanlaufplans bis zu den Nacharbeiten.

Beispiel

Die betrachtete Unternehmens-IT sei auf zwei Standorte verteilt, die Datenbestände teilweise gespiegelt. Der beispielhafte Test geht von der Nichtverfügbarkeit eines der Standorte aus und umfasst den Aufbau der IT-Umgebung für den Notbetrieb am anderen Standort sowie den Aufruf von Anwendungen.

Im Vorlauf müssen die Spiegel aufgetrennt und weitere Platten, die sonst zu anderen Zwecken (z. B. Entwicklung) eingesetzt werden, zum Restore nicht-gespigelter Datenbestände von Sicherungen auf Kassetten bereitgestellt werden. Dafür sind Daten dieser zusätzlichen Platten vorher zu sichern.

Die Testaktivitäten nach Wiederanlaufplan enthalten das Einspielen der Datensicherung, sodass ein synchroner Gesamtdatenbestand für die Anwendungen entsteht. Während des Tests werden die Daten im Testsystem verändert.

Im Nachgang muss der Spiegel neu aufgesetzt werden. Die zusätzlichen Platten werden gelöscht, mit ihren ursprünglichen Daten bestückt und wieder ihrer ursprünglichen Verwendung zugeführt.

Die Test-Durchführung wird natürlich noch von der Vor- und Nachbereitung eingerahmt: Hier sind die Planungs- und Kommunikationsprozesse angesiedelt, die für den Test erforderlich sind. Dazu gehören unter anderem die Benennung des Test-Personals, Vor- und Nachbesprechungen, die Verteilung von Test-Plänen und die Vereinbarung gemeinsamer Berichtsformate.

Für ein Gesamtprotokoll und die Bewertung sollte ein Test-Koordinator sorgen. Bei der Bewertung sind der Test selbst sowie der Status der Wiederanlauffähigkeit zu unterscheiden. Bewertungsskalen für beide Beurteilungen müssen vorher festliegen, sonst kann im Nachhinein leicht ein Streit über das Ziel des Tests entbrennen.

Test-Konzept

Die Grundbedingungen für Wiederanlauftests sollte man in einem übergreifenden Testkonzept festlegen. Dieses berücksichtigt zwei Phasen:

den anfänglichen Aufbau der Wiederanlauffähigkeit und den langfristigen Erhalt der Wiederanlauffähigkeit.

In der ersten Phase werden im Zuge des Aufbaus der Wiederanlauffähigkeit alle wesentlichen Voraussetzungen mithilfe der genannten hierarchischen Teststufen geprüft. Am Ende stehen Gesamttests oder zumindest umfangreiche Verfahrenstests.

In der zweiten Phase müssen organisatorische und technische Änderungen nachvollzogen werden, die im Unternehmen stattfinden, zum Beispiel die Einführung neuer IT-Anwendungen oder die Neustrukturierung von Geschäftsprozessen. Die anzuwendenden Teststufen werden dabei von der Tragweite der Änderungen bestimmt. Parallel dazu sollte man aber auch Bereiche ohne ersichtliche Änderungen in regelmäßigen Abständen testen.

Es ist ratsam, die durchzuführenden Tests für mindestens ein Jahr im Voraus zu planen, um die Verfügbarkeit aller notwendigen Ressourcen abzusichern. Das Konzept und im Detail die Jahresplanung bestimmen das Ziel für die vorgesehenen Wiederanlauftests. Mit der Frage, was auf Wiederanlauffähigkeit überprüft werden soll, sind auch gekoppelt:

die Auswahl der Test-Stufe und des Szenarios beziehungsweise der zu testenden Komponenten, die Auswahl der Test-Umgebung und der beteiligten Organisationseinheiten sowie die Auswahl von Termin und Ort des Tests.

Ein umfassendes Testkonzept mit dem richtigen Mix sorgt dafür, dass das durchführende Unternehmen die Gratwanderung zwischen ausreichender Sicherheit und Minimierung des Aufwands schafft.

Bernd Ewert ist Geschäftsführer der consequa GmbH.