Uptime ist in, Downtime ist out !

Nicht nur durch ständig wachsende Anforderungen wie Basel II, den Sarbanes-Oxley Act (SOX) und das Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG) nimmt die Bedeutung von Hochverfügbarkeits-Lösungen stetig zu: Seit der vollständigen Integration der IT in die Hauptgeschäftsprozesse eines Unternehmens wird das Thema IT-Hochverfügbarkeit zum wichtigen Wettbewerbsvorteil für viele Firmen. Ebenso zwingt die fortschreitende Globalisierung – verbunden mit der explosionsartigen Ausbreitung des Internets – viele Unternehmen beim Kampf um Marktanteile und Umsatzwachstum zu einer Rund-um-die-Uhr-Präsenz im Netz und bei E-Mails.

Doch was ist eigentlich Hochverfügbarkeit und wie viel davon benötigt man wirklich? Welche Anforderungen und Notwendigkeiten ergeben sich daraus für die Geschäftstätigkeit und die Prozesse?

Fest steht: Jedes Unternehmen hat unterschiedliche Anforderungen an die Hochverfügbarkeit, jede Lösung ist somit individuell. Die Notwendigkeit für die hochverfügbare, redundante Auslegung der IT-Systeme in kommerziellen Geschäftsbereichen wird u.a. forciert durch

- Gesetzliche Anforderungen (Transparente Bilanzierung, Langzeitarchivierung, elektronische Lesbarkeit, Datensicherheit, Datenschutz, Datenkompatibilität)
- Geschäftliche Anforderungen zu Partnern und Lieferanten (Geschäftsprozesse, B2B, B2C, Umsatzausfall, Imageschaden, mittelbare Folgeschäden)

Es bestehen für jede Branche unterschiedliche Anforderungen für die Absicherung eines Ausfalls und zur Vermeidung von Folgeschäden pro Zeiteinheit. Die Kosten, die durch die Nichtverfügbarkeit eines Dienstes („Downtime“) entstehen, hängen sehr stark von der jeweiligen Anwendung und vom Geschäftsfeld ab. Für ein Unternehmen – und vor allem für die Unternehmensführung – ist es besonders wichtig, diese Auswirkungen auf die Kosten und Arbeitszeit zu kennen.

Viele Unternehmen kennen jedoch noch nicht einmal die Kosten ihrer geplanten Downtimes, geschweige denn der Auswirkungen von ungeplanten Downtimes, obwohl diese eine wichtige Entscheidungsgrundlage bei der Auswahl der Verfügbarkeitsstrategien sind.

Während Finanzinstitute und Handelsunternehmen sehr hohe Anforderungen an die Verfügbarkeit ihrer Systeme stellen müssen, sind die Anforderungen bei manchen Dienstleistern oder Handwerkern sicher geringer.

Dabei gilt es, die Gesamtkosten des Ausfalls, also sowohl die Kosten während eines Ausfalls als auch die Kosten nach einem Ausfall zu betrachten.

Die Notwendigkeit für Hochverfügbarkeit ist dabei unmittelbar mit den Folgekosten eines Ausfalls gekoppelt:

- Interne Kosten: Personalkosten bei System- und Arbeitsstillstand nach einem Ausfall, Umsatzverlust durch fehlende Geschäftsfähigkeit
- Externe Kosten: Schadenersatzanforderungen, Konventionalstrafen, Höhere Kreditzinsen (Basel II, zudem bei Versicherungsunternehmen: Solvency II)
- Indirekte Folgen bei Nichtbeachtung (Haftungsrisiken, Freiheitsstrafen bei inkorrekter oder nicht vorhandener Bilanzierung (SOX - nur bei an US-Börsen notierten Unternehmen oder mit diesen geschäftlich verbunden, z.B. Konzern, Lieferant), bei inkorrekter Behandlung von Daten, Datenverlust oder Datenmanipulation: Gefährdung der Existenz von Firmen und auch Einzelpersonen
- Gefährdung der allgemeinen Sicherheit Dritter
- Verlust der Glaubwürdigkeit und Zuverlässigkeit
- Verlust von Marktanteilen und Image
- Minderung der Wettbewerbsfähigkeit
- Mögliche Haftung für Folgeschäden von Partnern und Lieferanten

Gegen welche Gefahren muss sich ein Unternehmen schützen?

Aus den gewonnenen Erkenntnissen über den individuellen Verfügbarkeitsbedarf eines Unternehmens und die damit verbundenen Folgekosten lassen sich verschiedene Gefährdungspotentiale identifizieren. Nur wenn dieses Potential bekannt ist, kann man sich adäquat schützen bzw. eine Gefährdung als Restrisiko wissentlich in Kauf nehmen.

Prinzipiell werden die Gefährdungen in 5 Kategorien unterteilt:

Höhere Gewalt	Organisatorische Mängel	Menschliche Fehlhandlungen	Technisches Versagen	Vorsätzliche Handlungen
▪ Personalausfall ▪ Ausfall eines IT-Systems ▪ Staub, Verschmutzung	▪ Unzureichende Kontrolle der IT-Sicherheitsmaßnahmen ▪ Fehlende oder unzureichende Wartung ▪ Fehlendes oder unzureichendes Test- und Freigabeverfahren ▪ Unzureichende Leitungskapazität	▪ Fahrlässige Zerstörung von Daten und Geräten ▪ Gefährdung durch Reinigungs- und Fremdpersonal	▪ Ausfall der Stromversorgung ▪ Ausfall von Netzkomponenten ▪ Datenverlust bei mobilen Einsätzen	▪ Diebstahl ▪ Vandalismus ▪ Spyware, Viren und Würmer ▪ Sabotage

Ein Unternehmen muss die für sich relevanten Gefährdungen kennen. Das heißt nicht zwingend, dass alle oben aufgeführten Gefährdungen auf jedes Unternehmen zutreffen. Eine individuelle Betrachtung ist unumgänglich.

Wesentlich ist, dass ein Unternehmen sich gegen die Gefährdungen schützt, die im konkreten Fall eine hohe Wahrscheinlichkeit des Eintretens haben oder einen immensen Schaden hervorrufen können.

Die Maßnahmen müssen individuell geplant erfolgen und dürfen nicht nach dem „Gießkannen-Prinzip“ eingesetzt werden. Nur so können die Risiken effektiv minimiert werden.

Wie sollte sich ein Unternehmen schützen?

Um die individuellen notwendigen Schutzmaßnahmen zu bestimmen, empfiehlt sich folgende prinzipielle Vorgehensweise:

- Gefährdungsanalyse
- Definition der individuellen Anforderungen an der Verfügbarkeit
- Ermittlung der Ausfallkosten
- Auswahl der individuellen technischen Maßnahmen

Eine Analyse der Gefährdungen sollte wie oben beschrieben immer individuell für das Unternehmen geschehen. Parallel und teilweise aufbauend auf der Gefährdungsanalyse muss im Unternehmen der benötigte Schutzbedarf, d.h. der notwendige Grad der Verfügbarkeit, definiert werden. Dazu sollten zunächst die nachfolgend aufgeführten Fragen beantwortet werden:

- In welchem Zeitraum muss die Anwendung wieder zur Verfügung stehen?
  RTO (Recovery Time Objective)
- Wie groß ist der maximal tolerierbare Datenverlust?
  RPO (Recovery Point Objective)
- In welchem Zeitraum muss die Anwendung wieder über das Netzwerk zugreifbar sein?
  NRO (Network Recovery Objective)
- Über welchen Zeitraum kann die Anwendung im eingeschränkten Betrieb (z.B. langsamere Antwortzeiten) betrieben werden?
  DOO (Degraded Operations Objective)

Die angenommenen Ausfallzeiten etc. sind nun monetär zu bewerten, d.h. die Ausfallkosten werden berechnet, indem alle mit einem Ausfall zusammenhängenden Kostenfaktoren berücksichtigt werden. Schematisch dargestellt kann die Bewertung wie folgt erfolgen:

Kosten während des Ausfalls	Verlorene Endnutzer-produktivität	=	Stundenkosten der beeinflussten Nutzer	x	Downtime-Stunden	
	Verlorene IT-Produktivität	=	Stundenkosten der beeinflussten IT-Mitarbeiter	x	Downtime-Stunden	
	Verlorener Umsatz	=	Umsatzeinbuße pro Stunde	x	Downtime-Stunden	
Kosten nach dem Ausfall	Weitere Geschäfts-ausfälle	=	Imageschaden (Kundenservice)	+	Überstunden-kosten	
			Verpasste Termine	+	Vertragsstrafen oder Gebühren	

Die Ausfall-Kosten können je nach Anwendung und Industrie schnell inakzeptable Größenordnungen annehmen und sogar das IT-Budget übersteigen.

Durch diese Schadenspotenzialanalyse lässt sich die Höhe der Investitionen ermitteln, die eine optimale Kosten-Nutzen-Relation gewährleisten.

Die gestellten Fragen adressieren sowohl die Hochverfügbarkeit (High Availability) wie auch die Wiederanlauffähigkeit nach einem Katastrophenfall (Disaster Recovery). In einer Hochverfügbarkeits-Implementierung wird versucht, durch möglichst automatisierte Fail-Over-Mechanismen den Ausfall von Komponenten abzufedern und damit die Anwendung mit möglichst geringen Einschränkungen für den Endbenutzer verfügbar zu halten. Desaster-Recovery-Lösungen dagegen greifen, wenn der Katastrophenfall eintritt.

Hochverfügbarkeits- und Desaster-Recovery-Lösungen sollten gemeinsam als Maßnahmen gesehen werden, Schaden von dem Unternehmen abzuwenden und sich inhaltlich nicht widersprechen. Sie sollten sich vielmehr ergänzen und aufeinander aufbauen.

Weiterführende Informationen:

Planungshilfe Betriebsichere Rechenzentren
www.bitkom.org/de/themen_gremien/36795_34464.aspx

Bundesamt für Sicherheit in der Informationstechnik
www.bsi.de/

BITKOM AK Server- und Betriebskonzepte
www.bitkom.org/gremien/Server

BITKOM AK Betriebsicheres Rechenzentrum & Infrastruktur
www.bitkom.org/gremien/rechenzentrum

BITKOM AK Speichertechnologien
www.bitkom.org/gremien/Speichertechnologien

Ihr Ansprechpartner:

Dr. Ralph Hintemann
Bundesverband Informationswirtschaft,
Telekommunikation und neue Medien e.V.
Albrechtstraße 10
10117 Berlin-Mitte
Tel: ++49 (0)30/27 576-250
Fax: ++49 (0)30/27 576-409
E-Mail: r.hintemann@bitkom.org
www.bitkom.org

Hochverfügbare Informationstechnik

Unverzichtbar für den Geschäftserfolg

BITKOM