

# Phasenplan

## Hochverfügbares-Rechenzentrum





## IN 10 PHASEN ZUM AUSFALLSICHEREN RECHENZENTRUM

Ausfallzeiten in der IT kosten mehr als eingeschränkte Datenzugriffe. Ungeplante Ausfälle gefährden die Geschäftsprozesse, die heute mehr denn je von der IT-Basis abhängen. Bares Geld kann hier gespart werden, indem eine zentrale und hochverfügbare IT-Struktur zum Einsatz kommt. In nur zehn einfach planbaren Schritten lässt sich dies erfolgreich umsetzen.

Image, Umsatzzahlen, Kundenvertrauen und sozio-wirtschaftliche Reputation zählen zu den Indikatoren eines erfolgreichen Unternehmens. Abhängig sind diese nicht nur von den einzelnen Mitarbeitern, sondern auch von der Technik, die die Geschäftsprozesse stützt und gewährleistet. Das Bild des „einfachen“ Systemausfalls ist eine Illusion. In den meisten Fällen bedeutet eine solche Störung Datenverlust, beispielsweise sensibler Kunden- oder Vertragsinformationen. Schlimmer noch, die täglichen Arbeitsabläufe müssen dann unterbrochen werden, im günstigsten Fall nur für Stunden; über Tage oder eine Woche hinweg kann sich das keine

Firma leisten. Und somit entspricht ein Systemausfall eben immer einem Umsatzverlust, vielleicht verliert der Betrieb auch Kunden, Aufträge oder öffentliches Ansehen.

Betrachtet der EDV-Verantwortliche seine IT-Struktur einmal tiefer, so wird ihm auffallen, wie abhängig das jeweilige Geschäft von der IT ist. Da die heutige schnelllebige Zeit wirtschaftliche Ausfälle nicht verzeiht, muss ein Unternehmen an der IT-Basis ansetzen, um langfristige Prosperität und Wirtschaftlichkeit zu gewährleisten. Hauptansatzpunkte sind Ausfallzeiten, Datenverlust und nahezu unverwaltbares Datenwachstum. Um diese zu einem Höchstmaß zu verhindern und somit die stete Geschäftstätigkeit zu garantieren, sollte der IT-Manager die Installation eines hochverfügbaren Rechenzentrums überdenken. Oft sind dazu nur Modernisierungs-, Erweiterungs- beziehungsweise Konsolidierungsmaßnahmen nötig. Der vorliegende 10-Phasenplan zeigt auf, welche Schritte dazu notwendig sind.



## DIE 10 PHASEN

### Phase 1 – Application Cluster

Die erste Phase beschreibt die Bündelung aller eingesetzten Anwendungen auf einem oder mehreren virtuellen Maschinen auf den VM Hosts. Diese sind mittels Fibre-Channel(FC)-Host-Bus-Adapter mit einem FC-Switch verbunden. Der Switch gewährleistet die Anbindung an den so genannten „Shared Storage“ (Speicher mit verteilten Zugriffen). Hier werden die VM Hosts beispielsweise durch VMware High Availability und VMotion Fault Tolerance gesichert. Der Cluster über die VMs kann Microsoft Cluster Services (MSCS), Novell Cluster Services (NCS), Oracle Real Application Cluster (ORAC) und Storage Foundation HA (SFHA) umfassen. Ausfallsicherheit auf dieser Ebene schaffen die virtuellen Maschinen sowie die Software-Tools für deren Speicherung.

### Phase 2 – Stretched Cluster

In der zweiten Phase erfährt das oben beschriebene Cluster eine Erweiterung, um die Ausfallsicherheit zu erhöhen. Den bestehenden VM Hosts werden weitere VM

Hosts in einem anderen Brandabschnitt zugefügt. Auch diese sind mittels entsprechenden Controllern über den Switch mit dem Speichersystem verbunden. Fällt ein VM Host aus, übernimmt ein anderer Clusternode dessen Funktion. Der Ausfall kann vom Anwender unbemerkt behoben werden. Das „Umschalten“ auf das Zweitsystem erfolgt transparent und automatisch. Durch diese Installation sind Hardware-Störungen abgesichert, die gerade bei VM Hosts zahlreiche Applikationen zum Erliegen bringen könnten.

### Phase 3 – Redundanz durch Duale Pfade

In der dritten Phase wird die Ausfallsicherheit durch redundante Datenpfade auf ein höheres Niveau gesetzt. Dabei erhalten die VM Hosts zunächst eine Dual-Controller-Ausstattung. Darüber hinaus wird ein weiterer FC-Switch ins Netzwerk integriert, der ebenso an das Speichersystem angeschlossen ist. Die VM Hosts können nun mittels der redundanten HBAs ihre Daten an beide Switche versenden. Damit lässt sich zum einen



Loadbalancing einrichten, zum anderen lassen sich die Datenpfade absichern. Sollte ein HBA oder gar Switch ausfallen, so gelangen die gesamten Daten über die verbleibenden Verbindungen auf das Speichersystem. Somit sind nach Abschluss der dritten Phase VM Hosts, Controller, Datenpfade und Switches redundant und hochverfügbar.

#### **Phase 4 – Spiegelung / Replikation**

Mit der vierten Phase beginnt die Absicherung des eigentlichen Speichers, hier durch Speicherspiegelung oder die so genannte Replikation. Dabei wird in einem anderen Brandabschnitt des Unternehmens ein weiteres Speichersystem eingerichtet, das ebenso mit beiden Switches verbunden wird. Mittels dedizierter Replikationssoftware schreiben nun alle Rechner die Daten in den primären Speicherbereich. Die Replikationssoftware spiegelt diese dann auf den sekundären Speicher im anderen Brandabschnitt. Sollte ein Primärspeicher eine Störung haben, so kann das zweite Sys-

tem nach einer kurzen Umschaltzeit dessen Aufgaben übernehmen. Dies ist noch kein echter synchroner Spiegel.

#### **Phase 5 – Storage Virtualisierung für Disaster Recovery**

Um den Speicher optimal zu nutzen und mit hoher Funktionalität auszustatten, wird in Phase fünf die Storage Virtualisierung genutzt. Dadurch lässt sich zudem eine Disaster-Recovery-Strategie umsetzen. Über Appliances wird der gesamte Speicher im Storage Area Network (SAN) virtualisiert und zu einem Speicherpool zusammengefasst, auch über getrennte Standorte hinweg. Nun kann eine echte synchrone Spiegelung erfolgen, die einen transparenten Failover im Falle einer Störung garantiert. Die Daten sind in dieser Phase gegen einzelne Systemausfälle in den jeweiligen Brandabschnitten und gegen den Ausfall einer gesamten Seite gesichert. Trotzdem bestehen noch Risiken des Datenverlustes, die sich durch weitere Schritte eliminieren lassen.



### **Phase 6 – Backup-to-Tape**

Die Primärsysteme gewährleisten den ständigen Zugriff auf die digitalen Informationen. In der sechsten Phase erhalten diese eine Absicherung über ein Backup auf Band. Dabei wird ein Backup-Server sowie eine Tape Library oder auch ein Autoloader in einem der Brandabschnitte in die bestehende Installation integriert. Eine Bandbibliothek bietet den Vorteil, zahlreiche Medien vorhalten zu können und somit auch Kapazitäten im Petabyte-Bereich vor Ort zu verwahren.

Müssen nun Daten wieder hergestellt werden, so können diese vom Band zurück geschrieben werden. Der EDV-Verantwortliche sollte hier genaues Augenmerk auf die einzusetzende Technologie werfen, denn je nach Format variieren Kapazität und Datendurchsatz. Das derzeit meist gewählte Format ist LTO, das in den Generationen 3, 4 und 5 recht hohe Leistungswerte bieten kann. Darüber hinaus sind die Backup-Intervalle und die Datenmenge entscheidend für

ein erfolgreiches Recovery.

### **Phase 7 – Backup-to-Disk**

Phase sieben unterstützt das Backup-to-Tape nicht nur, sondern kann zudem dem Restore-Prozesse erleichtern und beschleunigen. In diesem Schritt wird ein Disk-Backup-System dem SAN hinzugefügt, in einem anderen Brandabschnitt allerdings. Im Falle eines notwendigen Restores lassen sich die Dateien in kürzester Zeit wieder herstellen. Zudem erlauben diese Arrays eine höhere Funktionalität und Flexibilität als reiner Bandspeicher. Mit Backup-to-Disk ermöglichen wir auch das Streamen der LTO Laufwerke, was für einen flüssigeren, sicheren und zügigeren Datensicherungsprozess sorgt.

### **Phase 8 – Datenduplizierung**

In der achten Phase geht es um die optimale Ausnutzung der Speichersysteme. Ebenso lässt sich damit der unkontrollierte Datenwildwuchs beherrschen, wenn auch nicht zur Gänze stoppen.



Dateneduplizierung durchsucht Byte-Stränge nach Redundanzen und eliminiert diese. Gesichert werden so nur die einzigartigen Daten sowie die darauf verweisenden Links. Die Dateneduplizierung selbst kann an unterschiedlichen Stellen im Netzwerk erfolgen, direkt am Client, auf dem Mediaserver oder an einer Deduplizierungsappliance.

Die Deduplizierung direkt am Client erfolgt per Software und eliminiert bereits in der VM doppelt vorliegende Informationen. Dieser Datenbestand wird auch auf dem Disk-Backup-System gesichert. Das Bandsystem zeichnet die gesamten Datenbestände auf. Beim Einsatz eines Mediaserver sortiert dieser die Redundanzen aus und sichert die verringerte Datenmenge sowohl auf das Band- als auch das Festplattensystem. Kommt eine dedizierte Deduplizierungsappliance zum Einsatz, so geschieht hier die Datenreduktion und wird auch auf ihr gespeichert. Auch hier sichert das Band-Backup weiterhin alle digitalen Informationen.

### **Phase 9 – Auslagerung**

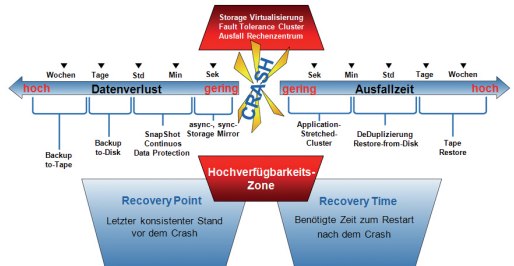
Das in Phase sechs aufgesetzte Band-Backup erfährt durch die neunte Phase eine Erweiterung. Durch die Auslagerung der Bänder erhöht sich der Schutz der Daten im Falle eines physischen Schadens am Brandabschnitt, zum Beispiel durch Wasser oder Feuer. Die Informationen werden durch eine Backup-Software auf den Bändern gesichert, beispielsweise NetBackup von Symantec. Bei einem solchen Prozess wirft die Bandbibliothek beschriebene und gelabelte Bänder automatisch aus. Danach geschieht die Auslagerung an einen anderen Standort, entweder durch einen Mitarbeiter oder externen Dienstleister. Die Software vermerkt die Aufzeichnungen, Standorte sowie das Verfallsdatum der Bänder. Im Falle eines Datenausfalls versendet die Software eine Nachricht an die externe Lagerstätte und fordert die Bänder an, die für die Wiederherstellung benötigt werden. Von den zurückgelieferten Bändern erfolgt dann das Restore mittels der Bandbibliothek.



## Phase 10 – Verschlüsselung

Die zehnte Phase ist ein Erweiterungspunkt zu Phase neun. Der Backup-Client, der Media-Server oder das Bandsystem verschlüsselt mittels Software die Daten auf den Bändern. Nun sind selbst im Falle eines Diebstahls oder anderen ungewollten Zugriffs auf die ausgelagerten Medien die Informationen geschützt. Ein Missbrauch durch unautorisierte Hände ist so nicht möglich.

**Ziel: kein Datenverlust – keine Ausfallzeit**



## Modernisieren, Konsolidieren: Geschäftssicherheit und mehr gewinnen

In zehn Schritten lässt sich ein hochverfügbares und Disaster-Recovery-taugliches Rechenzentrum zusammen stellen. Oft sind einzelne Phasen schon in Betrieb, ergeben aber noch nicht den umfassenden Schutz, den Unternehmen heute benötigen. Neben einem hohen Sicherheitsniveau kann die Firma weitere positive „Nebeneffekte“ erreichen. So ergibt sich beispielsweise durch Cluster, Virtualisierung und Deduplizierung erhebliches Konsolidierungs- und Sparpotenzial, sei es bei der Hardware, den Stromkosten oder den Klimawerten.

Ein genauer Serverraumcheck klärt ab, wie Ausfälle optimal verhindert werden und mit welchen Mitteln des 10-Phasen-Plans sich dies umsetzen lässt. Damit erreicht man eine zentrale, stabile und stets verfügbare IT-Basis, die nicht nur IT-technisch, sondern auch klimatechnisch zukunftstauglich ist.



**TargoSoft IT-Systemhaus GmbH**

Amsinckstraße 65

D-20097 Hamburg

Tel. +49 (0) 40 / 23 51 22 0

Fax +49 (0) 40 / 23 51 22 40

info@targosoft.de

www.targosoft.de

powered by