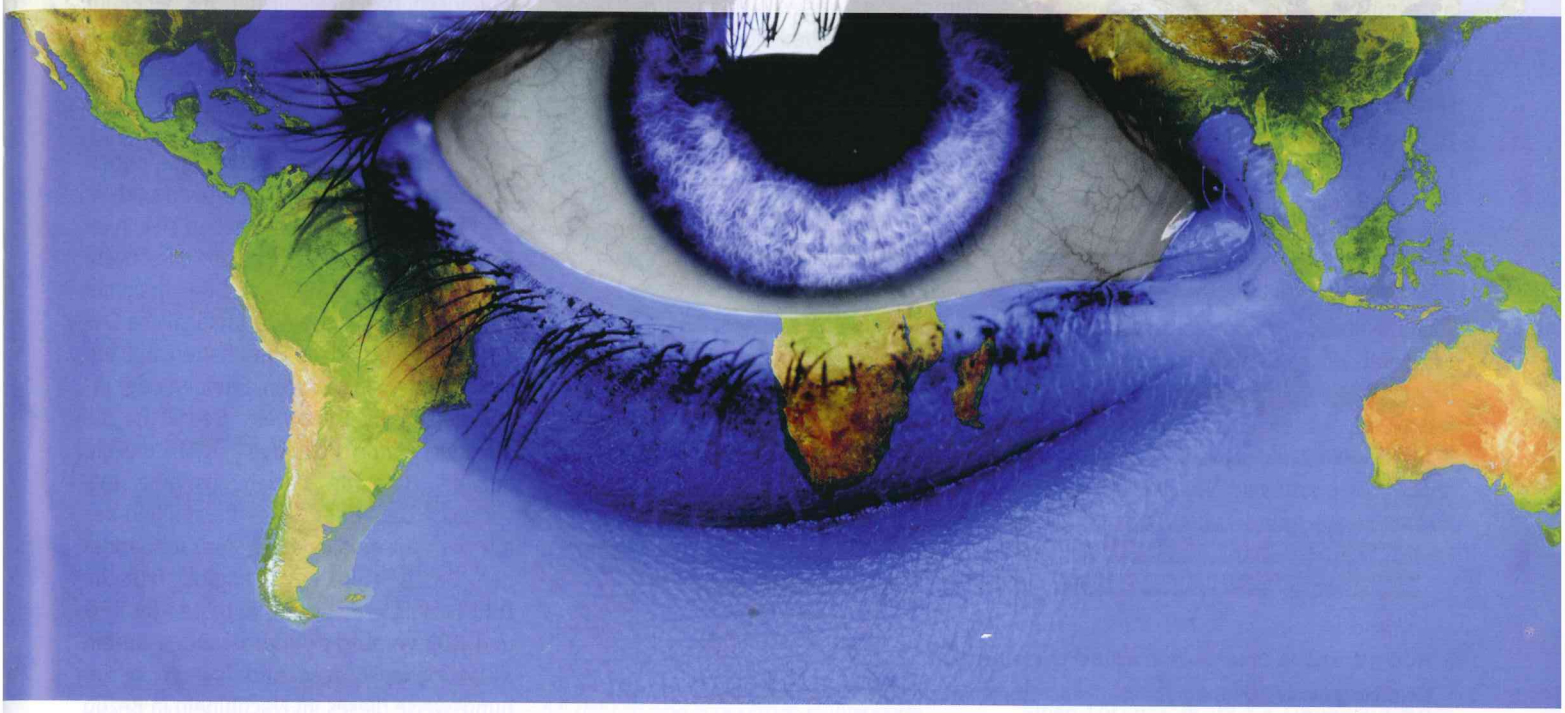
Die gesamte Applikationslandschaft im Blick

Datenkonsistenz im Katastrophenfall



Je mehr Applikationen im Unternehmen als geschäftskritisch eingestuft werden, desto wichtiger ist es, deren individuelle Ausfallzeiten so gering wie möglich und deren Daten zueinander konsistent zu halten. Kritische Applikationen werden typischerweise mit verschiedenen Hardware- und Softwarebasierenden Desaster-Recovery-Lösungen gegen Katastrophenfälle geschützt. Doch nur selten schaffen es diese Lösungen, Daten tatsächlich auch übergreifend für eine gesamte Applikationslandschaft konsistent wiederherzustellen.

Die Risiken für die Unternehmens-IT sind dieselben wie eh und je. Allerdings macht sich in vielen Rechenzentren eine gewisse Sorglosigkeit breit, weil Hardware und/oder Virtualisierung in vielen Fällen Schutz gegen Störungen des IT-Betriebs vermitteln. Typischerweise werden Sicherheit und Hochverfügbarkeit von Daten, Datenbanken und Dateisystemen herstellerabhängigen Verfahren anvertraut, zum Beispiel auf Basis vorhandener Hardware-Mittel wie SANs oder RAID (innerhalb der Laufwerkseinheiten), Virtualisierungslösungen und Snapshots (in verschiedenen Ausprägungen). Bei vielen Unternehmen mangelt es aber bereits an der angemessenen Reaktionsmöglichkeit bei Ausfall eines zentralen Rechenzentrums, was in der Regel durch einfache Spiegelmechanismen in eigene oder dienstleisterbetriebene Notfallrechenzentren realisiert werden kann.

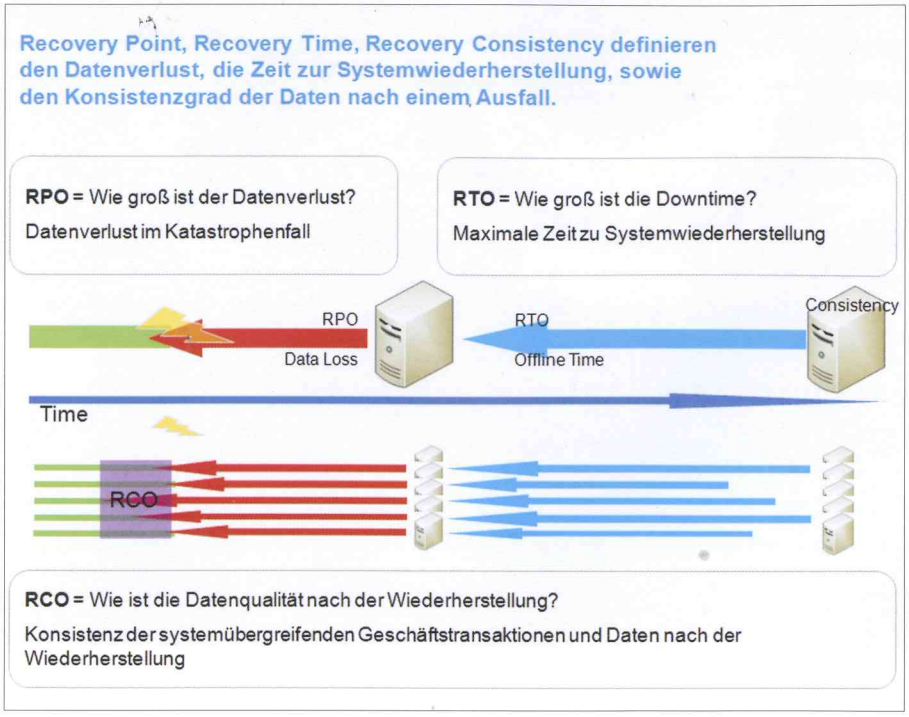
Darüber hinaus haben sich – nicht zuletzt durch den Preisverfall bei Speichermedien – regelmäßige Backups inzwischen auch in mittleren und kleineren IT-Umgebungen mit nur wenigen Servern und Nutzerarbeitsplätzen zumindest als Grundsicherung durchgesetzt, sodass nach einem Katastrophenfall ein gewisser Datenbestand wiederhergestellt werden kann. Wiederherstellaufwände, -zeiträume und -punkte speziell für unternehmenskritische Applikationen sollten hierbei aber besser nicht bewertet werden. Sauber implementiert können diese Verfahren aber auf jeden Fall wirksam bei technischen Fehlern schützen.

Technische Lösungen decken nicht alle Fehler ab

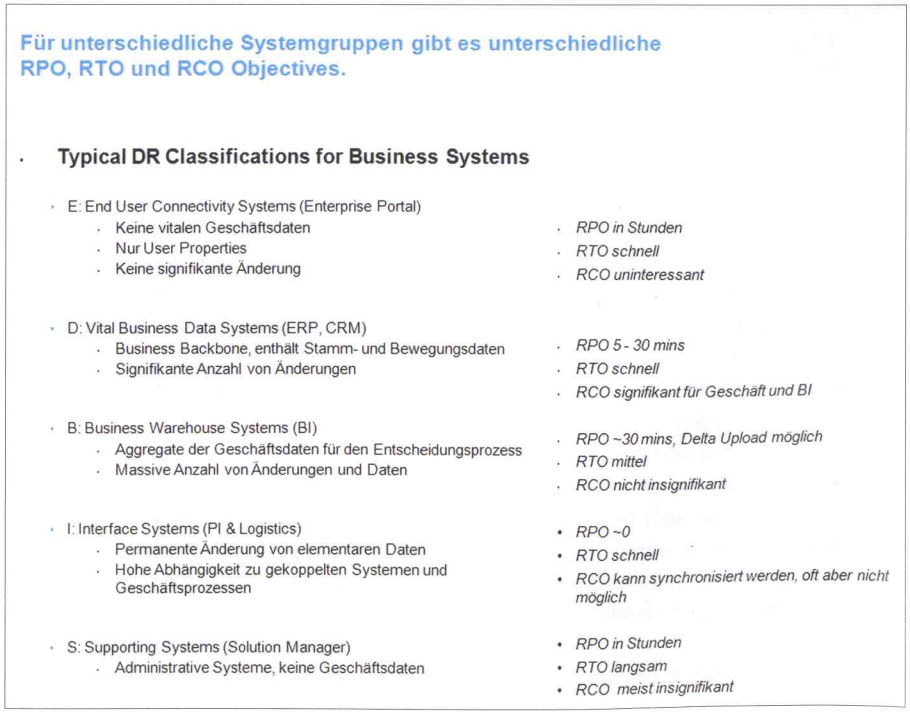
Lösungen für Hochverfügbarkeit und Desaster Recovery (DR) der Daten orientieren sich aber eben allzu oft ausschließlich am Schutz gegen rein technische Ausfälle. Dass Daten sicher sind, glauben dennoch viele Rechenzentrumsverantwortliche. Das ist auch zutreffend, solange die Daten nicht gegen logische Fehler geschützt werden sollen. Jedoch sind logische Fehler durchaus eine Bedrohung für die IT-Umgebungen. Zu den logischen Fehlern gehören hierbei unter anderem das fehlerhafte Verändern von Daten durch Benutzerfehler oder Probleme in der automatisierten Datenverarbeitung sowie das irrtümliche oder mutwillige Löschen von Daten. Diese Probleme werden dann auch „works as designed" typischerweise über alle virtuellen Laufwerke oder in den Snapshots „gesichert", das DR-Konzept somit logisch kompromittiert.

Ein weiteres Handicap neben der Technologie sind auf Seiten der Ablauforganisation fehlende Prozesse zur Alarmierung und zur Einleitung von Maßnahmen des IT-Katastrophenschutzes. Zusätzlich zur reinen Lehre des Business Continuity Management zeigen sich in der gelebten Praxis immer wieder ähnliche Problemstellungen beim Wiederanlauf der Applikationslandschaft: Neben den reinen Daten müssen auch Applikationen, Einstellungsdateien und vor al-

lem Schnittstellen und Dateisysteme konsistent und übergreifend über die gesamte Landschaft wiederhergestellt werden. Hardware-basierende Lösungen sind hier vielfach überfordert und auch Datenbankhersteller-spezifische Lösungen (auch wenn sie eine asynchrone Datenbankspiegelung darstellen) bieten keinen ausreichenden Katastrophenschutz, wenn gleichzeitig Datenbanken unterschiedlicher Hersteller im Einsatz sind oder relevante Abhängigkeiten zwischen Datenbanken und Dateisystemen bestehen.



Die RCO, Recovery Consistency Objective, berücksichtigt die Qualität der wiederhergestellten Daten nach einer Katastrophe oder menschlichem Versagen. (Grafik: Libelle AG)



Systeme werden im Katastrophenschutzkonzept entsprechend ihrer Rolle für die Aufrechterhaltung der Unternehmensaufgaben vorqualifiziert, wobei die DR-Klassen zur Anwendung kommen. (Grafik: Libelle AG)

Um die Wirksamkeit eines übergreifenden DR-Konzepts im Vorfeld zu planen und im Nachhinein zu beurteilen, haben sich zwei Begriffe durchgesetzt: Mit der „Recovery Point Objective" (RPO) wird der maximal erlaubte beziehungsweise tatsächliche Datenverlust nach dem Umschalten auf ein Notfallsystem in Minuten, Stunden oder Tagen gemessen. Der zweite Begriff ist die „Recovery Time Objective" (RTO), die die maximal erlaubte beziehungsweise tatsächliche Dauer der Wiederherstellung des mit dem ausgefallenen System verbundenen Geschäftsprozesses angibt. Typische DR-Konzepte versuchen, mithilfe von RPO und RTO vorab die Anforderungen an ein Katastrophenkonzept zu definieren, beziehungsweise dieses im Nachhinein in Bezug auf seine Effektivität zu beurteilen.

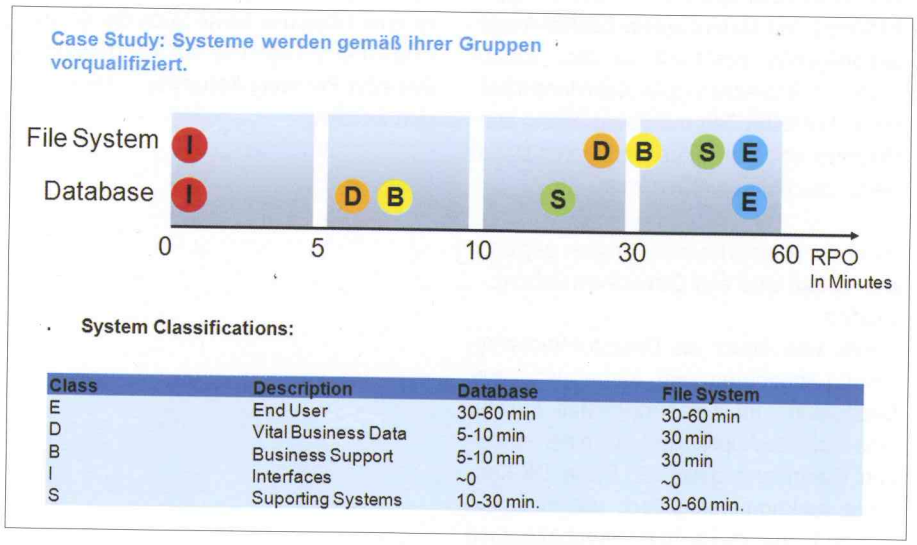
RCO misst Konsistenz wiederhergestellter Daten

Ein wesentlicher Aspekt bleibt bei dieser Betrachtung jedoch unberücksichtigt. Neben der Zeit der Wiederherstellung und des Umfangs des realen Datenverlustes, spielt die Konsistenz der wiederhergestellten Daten eine ganz entscheidende Rolle: Daten und Systeme müssen nicht nur schnell und möglichst vollständig, sondern auch im richtigen Zusammenhang und mit den richtigen Querverweisen wiederhergestellt werden – die Daten der einzelnen Applikationen sollen nach dem Wiederanlauf logisch zueinander passen, um zeitintensives manuelles Nacharbeiten zum „Glattziehen" der Systemlandschaft zu vermeiden. Es muss somit ein weiterer Faktor für die Beurteilung eines Disaster-Recovery-Konzepts beachtet werden: die Recovery Consistency Objective – RCO. Die RCO beschreibt die systemübergreifende Konsistenz der Daten und Geschäftstransaktionen nach einer Wiederherstellung.

Die drei Begriffe RPO, RTO und RCO lassen sich leicht daran veranschaulichen, wie die verschiedenen Systeme eines Unternehmens im Katastrophenfall eingestuft werden. Die Einstufung reicht von der schnel-

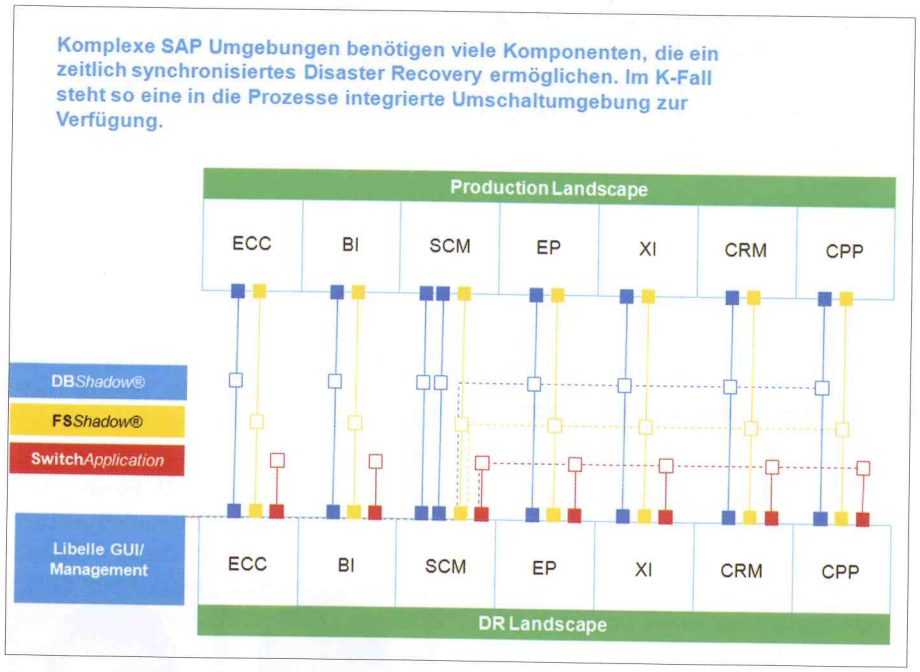
len Wiederverfügbarkeit der Hardware unter Inkaufnahme von Datenverlusten bis hin zur Sicherstellung höchstmöglicher Datenkonsistenz über unterschiedliche voneinander abhängige Systeme hinweg.

Die Definition von RPO, RTO und RCO sollte je Geschäftsprozess abgeleitet werden. Eine hohe Konsistenz der wiederhergestellten Daten ist beispielsweise bei unternehmenskritischen Applikationen wie ERP (Enterprise Resource Planning) und CRM (Customer Relationship Management) sinnvoll. Andererseits könnten bei unterstützenden Systemen erst bei größeren Störungen überhaupt weitergehende Maßnahmen ergriffen werden. Zum Beispiel können unter den Gesichtspunkten des Desaster Recovery bei einem Web-Shop noch nicht übermittelte Daten durchaus verloren gehen, jedoch sollte die User-Sitzung möglichst rasch fortgesetzt werden, damit der Anwender nicht abspringt und zu einem anderen Angebot wechselt.



Class	Description	Database	File System
E	End User	30-60 min	30-60 min
D	Vital Business Data	5-10 min	30 min
B	Business Support	5-10 min	30 min
I	Interfaces	~0	~0
S	Suporting Systems	10-30 min.	30-60 min.

Komplexe SAP-Umgebungen benötigen viele Komponenten, die ein zeitlich synchronisiertes Desaster Recovery ermöglichen. Im Katastrophenfall steht so eine in die Prozesse integrierte Umschaltumgebung zur Verfügung. (Grafik: Libelle AG)



Libelle BusinessShadow ist eine Datenspiegelungs-Lösung, die auch für WAN-Katastrophenschutzkonzepte genutzt werden kann und zudem Schutz gegen logische Fehler bietet. (Bild: Libelle AG)

Neben RPO und RTO kann die Recovery Consistency Objective (RCO) Verantwortlichen helfen, DR-Konzepte auf praxisrelevante Schwachstellen hin zu überprüfen, wobei letztlich die Bedeutung jedes Systems für die Weiterführung der kritischen Geschäftsprozesse und somit der Unternehmensziele ausschlaggebend ist.

Lösungsansatz zur Verbesserung der RCO

Einen Lösungsansatz zur Optimierung des RCO und zum Schutz gegen logische Fehler wie das irrtümliche oder mutwillige Verändern und Löschen von Informationen bieten asynchrone Applikations-, Datenbank- und Dateisystemspiegelungen. Das Funktionsprinzip ist denkbar einfach: Änderungen im Produktivsystem werden zyklisch zu einem oder mehreren lokalen oder entfernten Spiegelsystemen übertragen und dort in einem Zwischenspeicher abgelegt, der „Trichter" genannt wird. Physisch befindet sich der Trichter immer auf dem Spiegelsystem, damit er auch beim vollständigen Ausfall des Produktivsystems zugänglich ist. Der Umfang des Zwischenspeichers beziehungsweise die Zeitspanne, in der die Veränderungsinformationen im Trichter bleiben, lässt sich gemäß der spezifischen Anforderungen der Fachbereiche beliebig einstellen und verändern. Erst nach Ablauf dieser Zeitspanne werden die Daten aus dem Zeittrichter auch logisch im Spiegelsystem aktiviert. Das heißt, das Spiegelsystem läuft dem Produktivsystem um den eingestellten Zeitversatz hinterher, außerdem liegen alle übertragenen Produktivveränderungen aber bereits physikalisch im Zeittrichter auf der Spiegelseite. Im Falle einer Störung oder Datenkorruption wird das Spiegelsystem, oder im Sinne der RCO die gesamte Spiegelsystemlandschaft, mit einem frei wählbaren Daten-Zeitpunkt

Für Abonnenten ist dieser Artikel auch digital auf www.datakontext.com verfügbar

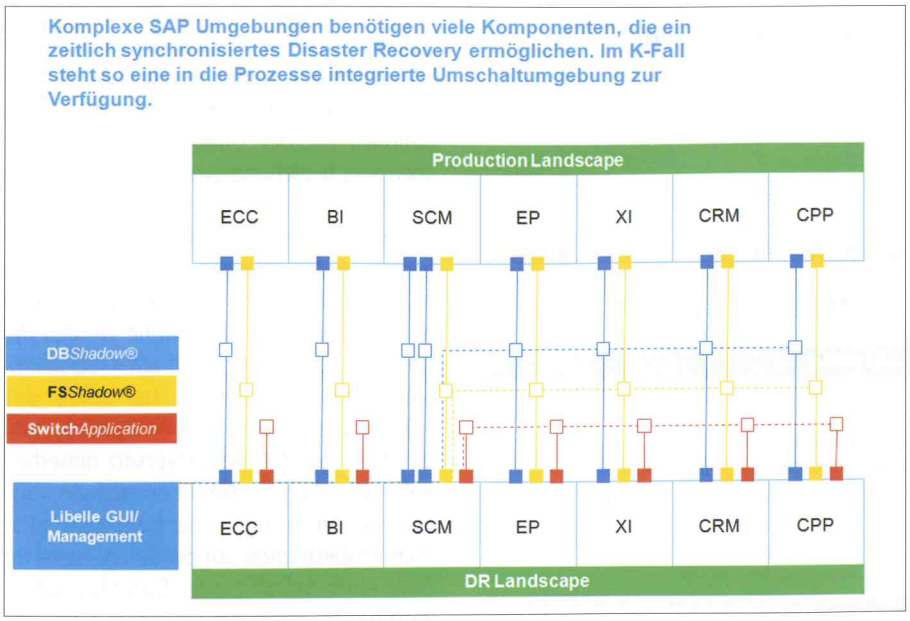
Weitere Artikel/News zum Schwerpunkt unter www.datakontext.com/ausfall

transaktionsinteger in der Datenbank, im Dateisystem und über alle Schnittstellen zu verbundenen Systemen hinweg zur Produktivumgebung erklärt. Wurde beispielsweise zum Zeitpunkt x eine Datenbanktabelle per fehlerhaftem EDI (Electronic Data Interchange) irrtümlich mit leeren Einträgen beschrieben, kann das Spiegelsystem – beziehungsweise die gesamte Landschaft – transaktionsinteger mit dem Datenzeitpunkt x-1 zum Produktivsystem erklärt werden. Fällt hingegen das komplette Produktivsystem aufgrund eines Hardware- oder Rechenzentrum-Ausfalls aus, wird ganz einfach der letzte, aktuellste Datenstand aktiviert.

Aus diesem Verfahren ergeben sich mehrere grundsätzliche Vorteile: Neben dem Schutz gegen technische Störungen entsteht zum einen eine echte Reaktionsmöglichkeit auf logische Fehler. Zum anderen ist das Einspielen der gültigen Transaktionen aus dem Trichter sehr schnell. Dadurch werden die Zeit bis zum Umschalten auf das wiederhergestellte System (RTO) und der Datenzeitpunkt (RPO) sowie die Konsistenz der Informationen auf dem wiederhergestellten System (applikationsinternes RCO) gegenüber Verfahren wie Backup/Restore und den auf einer Virtualisierung von Speicherplatz basierenden Lösungen erheblich verbessert. Ein weiterer Vorteil ist, dass dieses Verfahren der asynchronen Datenspiegelung mit einem Zeittrichter auch für eine interkontinentale Sicherung der Systeme genutzt werden kann. Und im Sinne der RCO im Rahmen eines Desaster-Recovery-Konzepts ganz entscheidend: Die Wiederherstellungspunkte einzelner Applikationen und Datenbanken können transaktionsgenau gesteuert werden, sodass auch in komplexen Applikationslandschaften in kürzester Zeit mit übergreifend konsistenten und transaktionsintegeren Daten weitergearbeitet werden kann.

Hochverfügbarkeitslösungen gegen den K-Fall und auf Datenkonsistenz prüfen

Vieles, was heute als Desaster-Recovery-Lösung angeboten wird, ist bei genauerer Betrachtung im Katastrophenfall nur für eine isolierte Applikation mit einer einzelnen Datenbank geeignet. Diese DR-Konzepte funktionieren jedoch nur in einem Verbund von meist herstellerabhängigen Lösungen, die sowohl Hardware- als auch Software-basierende Werkzeuge und die entsprechenden Eskalationsprozeduren umfassen. Das Ziel eines Desaster-Recovery-Konzepts für geschäftskritische Umgebungen muss aber über die reine Wiederherstellung einzelner Systeme hinausgehen und vor allem die Konsistenz der Daten und der Schnittstellen zu beteiligten Systemen innerhalb der kritischen Geschäftsprozesse berücksichtigen. Nur so kann sichergestellt werden, dass mit der Wiederverfügbarkeit der Systeme auch die Applikationsumgebung mit den korrekten Datenstrukturen wiederhergestellt werden kann. Neben der Recovery Point Objective und dem Recovery Time Objective sollte auch die Recovery Consistency Objective zur Beurteilung der Desaster-Recovery-Konzepte herangezogen werden. ■



Die RCO definiert, wie konsistent die unterschiedlichen Systeme im Fehlerfall sein müssen. (Grafik: Libelle AG)

Lars Albrecht, Vorstandsvorsitzender Libelle AG, **Stuttgart**

Peter Höroldt, Account Manager Libelle AG, Stuttgart