Information und Bildungsarbeit von und für die SAP®-Commu

Backup & Restore

Michael Scherf, Mitglied der Geschäftsleitung von All for One Steeb, Martin Finkbeiner, Geschäftsführer von Grandconsult, einem Tochterunternehmen von All for One Steeb, und Alexander Wallner, Geschäftsführer NetApp Deutschland, (v.l.n.r.) erklären, warum jeder SAP-Bestandskunde für sein Backup und Restore einen Schutzbrief haben sollte, denn Datensicherheit gilt nur bei vollständiger Datenverfügbarkeit!

Ab Seite 58

Datenverfügbarkeit und Datensicherheit auch aus der Cloud und für Hana von NetApp und All for One Steeb

Backup & Restore

Eine Datensicherung machen viele – vielleicht alle. Aber ist damit die Datenverfügbarkeit garantiert? Datensicherheit ist erst am Ende gegeben, wenn die Rücksicherung erfolgreich abgeschlossen ist. NetApp, All for One Steeb und Grandconsult haben Lösungen für Backup und erfolgreiches Restore erarbeitet: Die Kombination aus Technologie und Organisation ist entscheidend.

Mit Alexander Wallner, NetApp-Geschäftsführer Deutschland, Michael Scherf, Mitglied der Geschäftsleitung All for One Steeb und Martin Finkbeiner, Geschäftsführer von Grandconsult, ein Tochterunternehmen von All for One Steeb, sprach E-3 Chefredakteur Peter Färbinger. Eine von NTT Communications durchgeführte internationale Studie „Disaster Recovery and Business Continuity Readiness Survey" zeigt, dass nur knapp mehr als 50 Prozent der befragten Unternehmen über einen IT-Notfallplan verfügen. „Aus eigener Erfahrung lässt sich sagen, dass diese Angaben je nach Branche und Geschäftsmodell durchaus realistisch sind", bestätigt Alexander Wallner zu beginn des Gesprächs die Ist-Situation. Untersuchungen zeigen auch, dass die Notfallplänen leider nicht einmal das Papier wert sind, auf dem sie ausgedruckt sind. Michael Scherf von All for One Steeb unterscheidet somit auch zwischen IT und Organisation: „Wer einen IT-Notfallplan entwickelt, wird dort auch regelmäßige Testdurchläufe definieren. Hiermit wird die Funktionsfähigkeit und Konsistenz der Restore-Daten geprüft. Es sollten aber auch die organisatorischen Abläufe rund um die Datenwiederherstellung getestet und trainiert werden. Insbesondere in Branchen, die hohe Mengen an Transaktionen durchführen oder eng getaktet in Lieferketten eingebunden sind, beispielsweise große Online-Händler oder Unternehmen der Automobilzulieferindustrie, zählt im Notfall jede Minute. Da bleibt keine Zeit darüber zu diskutieren, wer nun welchen Handgriff im Detail erledigen soll."Backup sowie Business Continuity sind im Grunde in jeder IT-Organisation ein zentrales Thema und der CIO hat hierbei die Aufgabe, die Datensicherheit und Datenverfügbarkeit sicherzustellen. „So weit der Status Quo", meint Alexander Wallner. „Was sich jedoch ändert, sind die Geschäftsabläufe und zunehmend sogar die Geschäftsmodelle und damit wesentliche Rahmenbedingungen. So haben sich Daten in den vergangenen Jahren immer mehr zu einem zentralen Produktionsfaktor entwickelt. Die digitale Transformation mit ihren durchgängigen digitalen Prozessketten sowie stark datenzentrierte Geschäftsmodelle, die zum Beispiel das Kundenverhalten analysieren, führen dazu, dass auch in der Unternehmensleitung die Botschaft angekommen ist, dass die IT-Systeme ausfallsicher funktionieren müssen." Sollten sie doch einmal ausfallen, müssen sie sehr schnell wiederhergestellt werden können. IT-Leiter müssen aber gegenüber dem Management nicht nur wirksame Business Continuity-Strategien aufzeigen, auch für die Compliance zur Einhaltung von Datenschutzvorschriften sind wirksame Maßnahmen notwendig. „Wer diese Hintergründe kennt, sollte eigentlich davon ausgehen, dass bei 100 Prozent aller Unternehmen detaillierte Notfallpläne für Business Continuity vorliegen müssten, richtig?", fragt Wallner. Die Praxis sieht jedoch deutlich anders aus.

Der K-Fall

Alle Vorhersagen sind schwierig, besonders wenn sie die Zukunft betreffen. Somit ist wahrscheinlich die beste Vorsorge für den K-Fall das Einüben von Standards und Prozessen. „Mit manchen Unternehmen führen wir solche Tests einmal pro Quartal durch, wodurch sich bereits eine hohe Sicherheit ergibt, dass Daten und Abläufe eine sichere Wiederherstellung ermöglichen. Wer jedoch eine lebendige SAP-Landschaft betreibt, die regelmäßig erweitert wird oder in die kontinuierlich Updates eingespielt werden, sollten solche Trainings auch öfters durchgeführt werden", mahnt Martin Finkbeiner von Grandconsult, ein Tochterunternehmen der All fo One Steeb. Hat die Datenwiederherstellung im Ernstfall mit dem letzten Backup nicht funktioniert, müssen ältere Versionen herangezogen werden. Unter Umständen wird auch das Einspielen älterer Systempatches notwendig bis hin zum Rückbau von Hardware-Komponenten, um eine Kompatibilität der IT-Umgebung zu den alten Backup-Daten herzustellen. „Im Ernstfall ist es dazu jedoch oftmals zu spät", weiß Finkbeiner aus seiner beruflichen Praxis. „Daher sollte stets ausreichend Vorsorge getroffen werden, dass auch im nie ganz auszuschließenden K-Fall möglichst vieles auf Anhieb glatt läuft bei der Datenwiederherstellung." Umfragen haben gezeigt, dass die häufigsten Ursachen für einen Datenverlust ein Hardware- oder Software-Defekt ist. Das

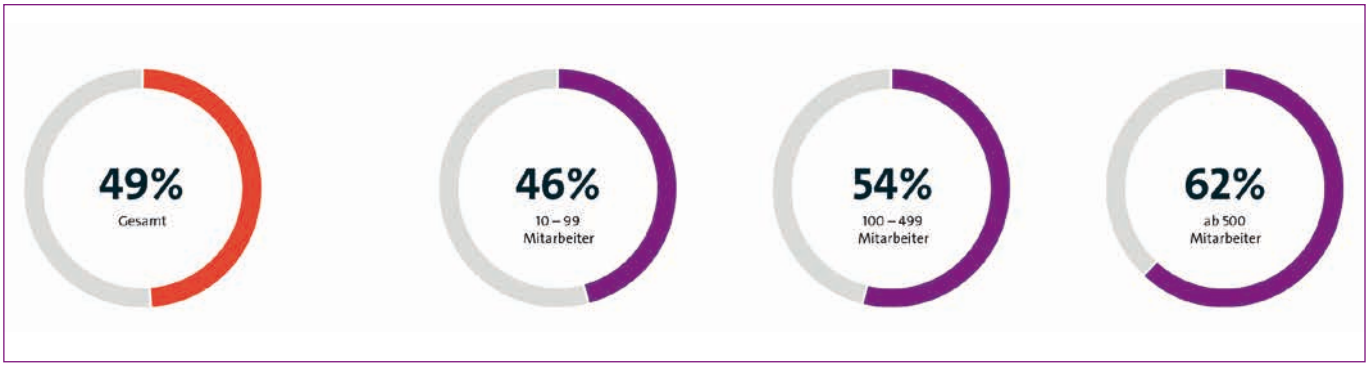
Michael Scherf, Mitglied der Geschäftsleitung All for One Steeb, Martin Finkbeiner, Geschäftsführer von Grandconsult und Alexander Wallner, NetApp-Geschäftsführer Deutschland (v.l.n.r.).

kann der Ausfall einer Festplatte oder eines Storage-Controllers sein, aber auch eine vorübergehend fehlerhafte Anwendung, die ihre Daten nicht ganz korrekt abspeichert. Ebenfalls sehr häufig kommen Bedienfehler vor oder ein Datenverlust durch plötzlichen Stromausfall, ohne dass die Notstromversorgung rechtzeitig einspringen konnte. Schad-Software wie Viren oder Naturgewalten wie Feuer und Wasser finden sich deutlich seltener als Grund für einen Datenverlust. „Das Statistische Bundesamt nennt in einer internationalen Umfrage Fehler in IT-Komponenten als führenden Grund für Datenverluste, gefolgt von menschlichen Fehlern, Stromausfällen und durch Wetter erzeugt Ausfälle“, erklärt Alexander Wallner von NetApp. Kann man den K-Fall üben oder automatisieren? „Die Kann-Frage stellt sich gar nicht“, sagt NetApp-Manager Wallner. „Es ist vielmehr ein Muss, die operativen und organisatorischen Abläufe eines IT-Ausfalls inklusive der Datenwiederherstellung zu trainieren.“ Im IT-Grundschutz-Katalog des BSI (Bundesamt für Sicherheit in der Informationstechnik) sind „Übungen zur Datenrekonstruktion“ vorgeschrieben. Die Ausgestaltung in der Praxis kann unterschiedlich sein. „Manche IT-Organisation testen ihre Notfallpläne in bis zu vier Testläufen pro Jahr“, ergänzt Michael Scherf von All for One Steeb. Er weiß aber auch, dass die Realität leider so aus sieht, dass man sich zumindest einmal jährlich dazu aufrafft, die notwendigsten Schritte durchzuführen. „Im Katastrophenfall führt diese Haltung jedoch zu operativem Chaos und deutlich verzögerten Anlaufzeiten“, warnt Scherf.

Prioritäten im Blick

Rein technologisch gibt es beim Backup keine Hürden. Selbst für größte SAP Hana-Szenarien mit Hadoop-Cluster gibt es sichere und effiziente Backup-Systeme. Um die notwendigen Abläufe innerhalb der IT-Organisation aufzusetzen, liefern Anbieter teilweise kostenlose Best Practice-Beispiele und Tipps im Internet. „Die größte Gefahr ist im Grunde die tägliche Projektarbeit in der IT sowie der Effizienz- und Kostendruck“, warnt Martin Finkbeiner. „Dies führt dazu, dass die unproduktiven Tätigkeiten wie das Backup in der Prioritätenliste nach ganz unten rutschen.“ Datensicherung macht jeder – oder? „Eine Datensicherung wird in der einen oder anderen Form in der Tat so gut wie von jedem Unternehmen vorgenommen“, ist Martin Finkbeiner von Grandconsult überzeugt. Allerdings nimmt man eine Datensicherung aus dem Grund vor, um im Notfall die gesicherten Daten sehr schnell und gleichzeitig fehlerfrei wieder einspielen zu können, sodass der Geschäftsbetrieb möglichst wenig beeinträchtigt wird. „Erst beim Restore zeigt sich oft jedoch, wie wirkungsvoll die Backup-Strategie tatsächlich ist“, betont Finkbeiner das Wiederherstellen, auf das es letztendlich wirklich ankommt. „Gründe für ein Scheitern der Wiederherstellung gibt es viele“, weiß sein Kollege Michael Scherf. Technische Probleme können dazu führen, dass Daten auf einem Speichermedium nicht mehr lesbar sind oder ein Backup nicht konsistent gesichert wird. In modernen Backup-Umgebungen von NetApp wird zum Beispiel längst ganz auf Magnetbänder verzichtet. Besonders heikel sind zudem Datensicherungen, die zwar rein technisch sauber durchgelaufen sind, deren Wiederherstellung jedoch unbrauchbare Ergebnisse liefern, etwa bei Fehlern oder sich gegenseitig ungünstig beeinflussenden Faktoren auf Seite der Anwendungslandschaft. „Auch solche Restore-Probleme kommen in der Praxis immer wieder vor. Es sind also ganz unterschiedliche Faktoren, die zu einem fehlerhaften Restore führen können“, ergänzt Alexander Wallner.

Falsche Sicherheit? Mit redundanter Datenspeicherung, Notfallrechenzentren mit Datenspiegelung etc. sind die Daten meistens sehr sicher. Wozu dann noch sichern? „Je nach Geschäftsmodell und Branche fallen die Anforderungen an die Datenverfügbarkeit ganz unterschiedlich aus, daher sind trotz redundanter Storage-Systeme und Business Continuity-Konzepte immer noch Backup-Lösungen notwendig“, betont Alexander Wallner im E-3 Gespräch mit Nachdruck. Darüber hinaus übernimmt das Backup auch die Rolle einer Archivierung und erfüllt damit gesetzliche Vorschriften. „Daher benötigen Unternehmen immer ein mehrstufiges Konzept für aktuelle operative Daten bis hin zur Langzeitarchivierung“, erklärt Wallner. Michael Scherf ergänzt: „Damit etwa ein Notfallrechenzentrum im Ernstfall sofort einspringen kann, ist je nach Anforderung des Geschäftsbetriebs eine mehr oder weniger permanente Daten-



Notfallmanagement? Fehlanzeige! Laut einer Bitkom-Studie von 2015 verfügen nur knapp die Hälfte aller deutschen Unternehmen über ein Notfallmanagement bei digitaler Wirtschaftsspionage, Sabotage oder Datendiebstahl. Umso wichtiger sind gut funktionierende Backup- und Restore-Prozesse.

sicherung erforderlich." Oft müssen zudem mehrere Generationen von Datensicherungen wiederherstellbar vorgehalten werden, um etwa selektiv ganz bestimmte Teile einer Gesamtdatensicherung wiederherzustellen.

Nicht überall Zero Downtime

„Immer häufiger verträgt der Geschäftsbetrieb nur noch eine geringe Downtime", beschreibt Michael Scherf das sich ändernde Business. „Das Fenster für den Wiederanlauf der IT wird daher immer enger. Die passenden Lösungen hierfür sind alles andere als trivial, unter Einbezug eines spezialisierten externen Dienstleisters lassen sie sich dennoch wirtschaftlich abbilden." Online Backup, per Snapshots ohne Beeinträchtig des laufenden IT Betriebs und sehr schnelle und gezielte Wiederherstellbarkeit sind wichtige Eckpunkte. Scherf kennt die Praxis: „Schnell wird im Tagesgeschäft einmal eine SAP-Tabelle zerschossen und nur diese soll aus der letzten Datensicherung wiederhergestellt werden." Klassische Magnetbänder oder Tape Roboter sind daher für moderne Backup-Aufgaben klar auf dem Rückzug. IT-Experten bevorzugen heute High Availability Backup-Netzwerke. Das Zeitfenster für Backup und Wiederherstellung bei gleichzeitig starkem Anstieg der Datenvolumina gelten als die entscheidenden Kenngrößen für ein wirkungsvolles Datensicherungssystem. NetApp bietet für klassische Datenbanken den SnapManager oder den SnapCreator an. Beide Produkte nutzen die Snapshot-Technologie für schnelle und performance-neutrale Backups. Diese Backup-Tools nutzen unter anderem die SAP-Backint-Schnittstelle und sind somit in das SAP-Backup-Management und Monitoring (DB12/DB13) integriert. „Pauschale Datensicherungskonzepte gibt es nicht, da Kunden unterschiedlichste SLAs haben", betont Alexander Wallner." „Wichtig ist stets, das Datensicherungskonzept konsequent von den Anforderungen des Geschäftsbetriebs her abzuleiten", beschreibt Scherf das Szenario und wirft einige Fragen auf: Wie lange darf die IT ausfallen, ohne dass mein Geschäft nicht mehr vertretbar beeinträchtigt wird? In welchem Umfang sind für mich Datenverluste akzeptabel, weil ich sie notfalls auch manuell nachfahren kann? Welche Anwendungen sind absolut geschäftskritisch und allenfalls sogar für Zero Downtime auszulegen, welche nicht? Wann greifen welche Sanktionen meiner Kunden, wenn ich etwa Lieferplanabrufe als Zulieferunternehmen der Automobilindustrie nicht mehr zeitgerecht bedienen kann? Mit welchen Umsatzverlusten muss ich rechnen, wenn meine Handelsplattform

Kurzinterview: Die drei von der Datensicherung

Wie kam es zu der Zusammenarbeit zwischen All for One und NetApp?

Michael Scherf, All for One Steeb: Mit unseren Managed Services sowie mit unseren Technologie Consulting-Aktivitäten verzeichnen wir ein anhaltend starkes Wachstum. Das liegt auch mit daran, dass wir die gesamte Wertschöpfungskette abdecken. So übernehmen wir die SAP-Betriebsverantwortung für Kunden aus unseren Rechenzentren heraus. Gleichzeitig betreuen wir viele Unternehmen direkt in ihren eigenen Rechenzentren, vor Ort wie auch Remote. Immer häufiger auch alles zusammen. In dieser konsequenten Ausrichtung nimmt die Partnerschaft mit NetApp seit vielen Jahren bereits eine Schlüsselrolle bei uns ein. Mit NetApp lassen sich die Anforderungen unserer Kunden an Business Continuity am besten realisieren.

Was sind die Vorteile dieser Verbindung für den SAP-Bestandskunden?

Scherf: Kunden erhalten so von uns ein sehr genau auf ihre spezifische Geschäftsanforderung hin abgestimmtes Gesamtangebot aus Technologie, Implementierung, Service, Betrieb und Innovation. Dazu betreiben wir zusammen unter anderem ein Research & Development Center bei SAP in Walldorf und haben so auch SAP selbst direkt mit ihm Boot.

Wie wird sich dieses Service weiterentwickeln und wer kommt dafür jetzt und zukünftig als potenzieller Anwender in Frage?

Martin Finkbeiner, Grandconsult: Im Zuge von Big Data, Industrie 4.0 und IoT wird Business Continuity einen deutlich akzentuierten Stellenwert erhalten. Die Bewertung vieler Business Cases dürfte mit Blick auf Datensicherung und Verfügbarkeit bald deutlich anders ausfallen, als bisher, einfach, weil sich die Geschäftsabläufe und Modelle sowie deren Risikoprofile grundlegend ändern werden.

Was ist Ihr interessantestes Erfolgserlebnis bezüglich Datenwiederherstellung?

Alexander Wallner, NetApp: Viele Anwender zeigen sich heute geradezu begeistert darüber, wie schnell und präzise sich in modernen Umgebungen etwa versehentlich gelöschte SAP-Tabellen oder andere Files wiederherstellen lassen. Solche Erfolgserlebnisse motivieren auch die Service-Teams in den Unternehmen wie beim Provider enorm.

ausfällt? Wieviel Zeit bleibt mir überhaupt, um die Verluste später durch entsprechend mehr Transaktionen wieder reinzuholen? Ist meine IT-Landschaft überhaupt darauf ausgelegt, die Mehrtransaktionen zu bewältigen? „Nur wenn der Business Case klar und belastbar umrissen ist, lässt sich aus den Business Continuity-Anforderungen auch die passende Strategie für die IT Service Continuity ableiten", ergänzt sein Kollege Martin Finkbeiner. Wichtig, meint Finkbeiner: Die vorgenannten Grundfragen zu den Anforderungen des Geschäftsbetriebs sollten periodisch neu gestellt werden. Gerade in Zeiten der digitalen Transformationen und ihrer enormen Geschäftsdynamik werden dieselben Fragen ein Jahr später grundlegend anders beantwortet, so die Erfahrungen. „Datensicherung wird insbesondere dann komplex, wenn die Menge der Daten zunimmt und die Anzahl der parallel zu sichernden Systeme wächst, also beispielsweise bei SAP Landschafts-Backups", weiß NetApp-Manager Wallner aus seiner beruflichen Praxis. Dazu kommen noch die langen Backup-Laufzeiten, welche den Systembetrieb belasten. Mit Hilfe von Storage-basierten Sicherungsmethoden können Backup-Laufzeiten minimiert, Performance-Einbußen fast gänzlich neutralisiert und das gleichzeitige Sichern einer kompletten SAP-Landschaft realisiert werden. „Wer ohne großen administrativen Aufwand die Backup-Strategie optimieren möchte, setzt beispielsweise ein Cloud Storage Gateway ein", meint Alexander Wallner.

Cloud-Backup

Die von NetApp angebotene Lösung AltaVault ist als physische Appliance oder virtuelle Maschine verfügbar und übernimmt den Datentransfer der eigenen Backup-Daten zu beliebigen Cloud-Providern oder auch in eine Private Cloud. AltaVault ist in beliebigen SAP-Landschaften einsetzbar und funktioniert mit den gängigen Backup-Anwendungen. Technologisch ermöglicht AltaVault der Cloud ähnliche Zugriffe wie bei einem Netzlaufwerk: Protokolle wie CIFS (Common Internet File System) und NFS (Network File System) bilden die Basis dafür, dass die IT bestehende Abläufe und Software für die Datensicherung direkt weiterverwenden kann. Dies sichert bereits getätigte Investitionen und beschleunigt die Implementierung. „Darüber hinaus ist die Lösung mit Public Clouds wie beispielsweise AWS, Azure oder Softlayer einsetzbar", ist Alexander Wallner stolz auf die NetApp-Kompetenz. Backup-Services aus der Cloud, die sich an Unternehmen richten, werden von IT-Dienstleistern in unterschiedlichen Ausprägungen und Qualitätsstufen angeboten. „Das Problem hierbei ist die Vergleichbarkeit der Leistungen, da CIOs beim Einkauf von Cloud-Services beispielsweise auch auf die SLAs achten müssen", betont Wallner im E-3 Gespräch. So ist es für die IT-Abteilung recht aufwändig, verschiedene Anbieter zu evaluieren. Vor diesem Hintergrund ist das Angebot „Backup as a Service" entstanden. Auf Basis von NetApp-Technologien bieten autorisierte Service Provider die komplette Leistung des Backups in die Cloud. Die Besonderheit hierbei: NetApp zertifiziert den Service der IT-Dienstleister, übernimmt also praktisch die Qualitätskontrolle für die

>> Backup optimieren mit Cloud Storage Gateway. <<

Alexander Wallner,
NetApp-Geschäftsführer
Deutschland.

Unternehmenskunden. „Darüber hinaus dürfen die Partner für BaaS nur Rechenzentren in Deutschland einsetzen", erklärt Wallner. Heute bieten bereits zehn Partner in Deutschland ihre Dienstleistungen für BaaS an, die sich natürlich auch perfekt für SAP-Kunden eignen.

Hana-Backup

Anders als bei herkömmlichen Datenbanken, die ihre Daten primär von Festplatte oder Flash lesen, halten In-memory-Computing-Systeme wie SAP Hana die Daten weitgehend komplett im Hauptspeicher. „Dies führt zu neuen Anforderungen an die Backup-Infrastruktur, da erheblich mehr Daten zu sichern sind", kennt Alexander Wallner die neuen, technologischen Herausforderungen. Das Sichern dieser Daten erfolgt typischerweise als fortlaufendes Streaming auf ein Backup-System, da hier klassische Verfahren mit täglichen Deltasicherungen schon aufgrund der Datenmengen nicht mehr funktionieren. Bei einer Datensicherung im TByte-Bereich kann das Sichern auf Disk und anschließend auf Tape einige Stunden dauern. Ähnlich viel Zeit verschlingt die Wiederherstellung der Daten. „Daher arbeiten viele Unternehmen heute mit dem Konzept von Snapshots", weiß Wallner. „Hierbei werden Sicherungskopien des operativen SAP-Systems fortlaufend erstellt und gesichert, ohne die produktiven Systeme zu belasten. Ein Recovery erfolgt dadurch erheblich schneller." Die von NetApp entwickelten Storage-Systeme FAS oder AFF erstellen diese Snapshots für das Hana-Backup in nur wenigen Sekunden. Wie eine von NetApp unter Hana-Bestandskunden durchgeführte Analyse gezeigt hat, liegt die Zeit für ein Hana Snapshot-Backup bei durchschnittlich 19 Sekunden. Selbst komplexe Datensicherungen laufen bei Kunden nicht länger als eine Minute.

„SAP-Lösungen sind meistens geschäftskritisch", ergänz Michael Scherf von All for One Steeb. „Durch den verstärkten Einsatz von Hana ändert sich zudem die technologische Basis, die zudem vermehrt auch dazu genutzt wird, bisherige Geschäftsabläufe oder gar Geschäftsmodelle neu zu designen." Dieses veränderte „Big Picture" beeinflusst auch die Organisation der Datensicherung und Datenwiederherstellung. Dazu kommt, dass der temporäre Einbezug von Ressourcen aus der Public Cloud, etwa Compute-Leistung, ganz neue Skalierungsmöglichkeiten bietet. „Unser Vorgehensmodell beim Restore Schutzbrief reicht daher von der Überprüfung der Anforderungen aus dem konkreten Business Case, über die Analyse und den Abgleich mit den bereits bestehenden Backup-Prozesse und -Technologien, der Bewertung von geeigneten Soll-Szenarien bis hin zu deren Realisierung und vor allem den Ongoing-Services im laufenden Betrieb", erklärt Scherf das erarbeitete, ganzheitliche Backup- und Restore-Modell.

Zum Schluss: Was würde diese Gesprächrunde einem SAP-Bestandskunden raten bezüglich der Überprüfung seiner Datensicherung? „Hier empfehlen wir auf einen Dienstleister zu setzen, der die Überprüfung und Validierung der Backups vornimmt", antwortet Martin Finkbeiner für alle. „Für diesen Zweck haben wir unser Angebot für den Restore-Schutzbrief entwickelt. Der Grundgedanke ist: Backup ist nicht alles, denn ohne Validierung der wiederhergestellten Datensicherung ist alles nichts. Also kein Backup ohne gesicherte Validierung des Restores."

Neue Betreibermodelle für den SAP-Betrieb

Sicher durch die Wolke

Während die Nutzung der Public Cloud für den Core-SAP-Betrieb derzeit noch keine echte Option ist, sind es gerade die Projekte im Testing und Development sowie die Integration der Cloud in die Backup- und Disaster Recovery-Strategie, die für Unternehmen besonders relevant sind, um die Effizienz und Datensicherheit zu verbessern.

Von Thomas Herrmann, NetApp

Für ihre SAP-Lösungen benötigen Unternehmen eine extrem flexibel einsetzbare Speicherinfrastruktur, die eine Vielzahl von IT-Systemen unterstützt. Die Cloud ist hier eine wertvolle IT-Ressource, um die Leistung der SAP-Systeme gezielt zu steigern und die Anforderungen der Fachbereiche schneller zu erfüllen.

Die Anforderungen an das Datenmanagement in SAP-Umgebungen sind sehr vielfältig: Technologien wie die In-memory-Plattform SAP Hana, Echtzeitanalysen für Fachabteilungen und immer wieder Ad-hoc-Anfragen nach mehr Speicherkapazität für Test- und Entwicklungssysteme sorgen dafür, dass IT-Verantwortliche hohen Wert auf ein möglichst effizientes und flexibles Storage-Management legen. Gleichzeitig gilt es die Datenschutzbestimmungen zu beachten, die nach dem Safe Harbor-Urteil eine noch genauere Analyse verlangen, welche Daten an welchen Standorten verarbeitet werden.

Darüber hinaus bringt das kontinuierliche Datenwachstum von SAP-Landschaften inkrementelle Backup-Strategien mit Tape-Libraries oder klassische Backups sehr schnell an ihre Grenzen. Wer die Datenverfügbarkeit einer SAP-Landschaft organisationsweit verbessern möchte, muss darüber hinaus noch die ganz unterschiedlichen Datenquellen in die Backup-Strategie einbinden, wie beispielsweise für Drittsysteme oder das Open Source-Framework Hadoop.

Ergänzend zu diesen eher allgemeinen Entwicklungen rund um die Unternehmens-IT bringt die neue Generation von SAP-Lösungen ebenfalls ihre speziellen Anforderungen an die Storage-Infrastruktur mit.

Digitale Transformation schafft neue Daten

Die kürzlich vorgestellte In-memory-Lösung SAP Hana Vora für Hadoop und Spark ist beispielsweise eine leicht einsetzbare Technologie, um selbst größte Big Data-Bestände zu analysieren – wodurch Fachbereiche sehr schnell wieder neue Datenmengen generieren. Darüber hinaus ist damit zu rechnen, dass sich das In-memory-Konzept als der kommende Datenbankstandard für SAP-Anwendungen durchsetzt – so ist bei S/4 Hana die In-memory-Technologie bereits fest verankert. Das heißt für den CIO: hier kommen hohe Anforderungen nach schnellem Storage und mehr Speicherkapazität auf das Rechenzentrum zu. Auf Ebene der Geschäftsstrategie zeigt sich, dass Geschäftsmodelle immer datenzentrierter werden. Die digi-

Thomas Herrmann ist bei NetApp als Business Development Manager SAP für die Region DACH verantwortlich und seit über 20 Jahren in der IT-Industrie tätig.

tale Transformation der Unternehmen führt zu hoher Business-Agilität bis hin zu Echtzeitprozessen.

Wer einen Webshop oder eine Internet-Buchungsplattform betreibt, kann sich Aufgrund der Konkurrenzsituation keine Ausfälle der IT erlauben. Ein mehrstündiger Systemstillstand wegen Datenverlusten führt zu verärgerten Kunden bis hin zu Umsatzeinbußen. Für die Entwicklung von SAP-Landschaften bedeutet dies, dass CIOs künftig deutlich mehr Hochverfügbarkeit und Sicherheit für ihre Storage-Infrastruktur benötigen.

Angst vor zu viel Abhängigkeit

Wie die Erfahrung zeigt, haben so manche CIOs immer noch Bedenken, wenn es um die Nutzung von Cloud-Ressourcen geht. Es sind aber weniger die technologischen Fragen, die für Diskussionen sorgen, denn alle Cloud-Provider verfügen über Standard-Schnittstellen. Vielmehr werden Bedenken geäußert, sich dauerhaft an einen Cloud-Anbieter binden zu müssen. Eine im Januar von IDC veröffentlichte Umfrage unter deutschen Unternehmen hat ergeben, dass 36 Prozent der Befragten eine Abhängigkeit von externen Cloud-Anbietern vermeiden möchten. 39 Prozent äußerten Sicherheitsbedenken bei der Cloud-Nutzung. Trotzdem schreitet die Cloud-Integration weiter voran: Eine Umfrage der Analysten von ESG ergab im Jahr 2015, dass 49 Prozent der befragten Unternehmen die Cloud bereits für Backup und Archivierung einsetzen. Wer einmal große Datenbestände in die Cloud kopiert hat, wird feststellen, dass sich diese nur sehr schwer zu einem anderen Service-Provider transferieren lassen.

Datenbremse Data Gravity

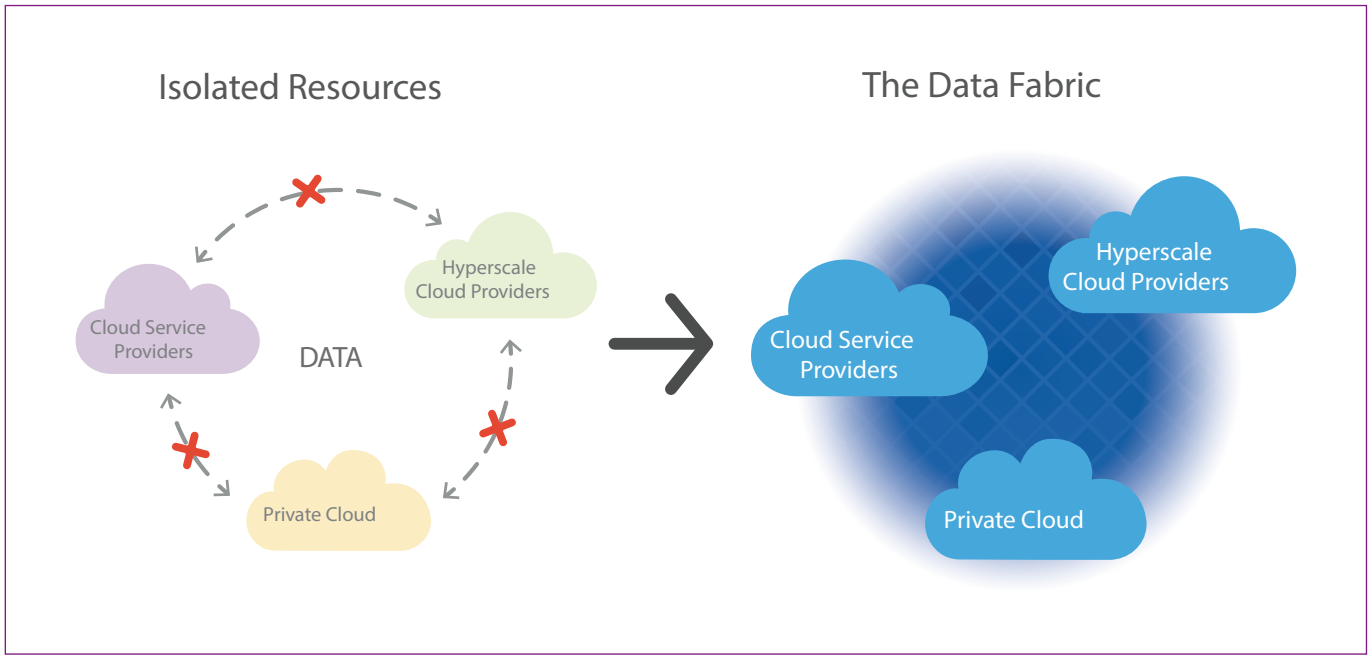
Hier wird der Effekt der Data-Gravity spürbar: Diese bremst IT-Modernisierungsvorhaben aus, da auch Bits und Bytes im übertragenen Sinne den Gesetzen der Schwerkraft unterliegen. Sie haben nämlich die Tendenz, sich an eine bestehende Infrastruktur zu heften. Diese Trägheit wird dadurch erzeugt, dass Daten Eigenschaften wie beispielsweise ihre Größe oder eine bestimmte Sicherheitsklasse besitzen. Wer zum Beispiel eine Storage-Infrastruktur im Petabyte-Bereich aufbaut, wird diese aufgrund der riesigen Datenmenge nur sehr schwer auf eine neue Plattform migrieren können.

Die Vorteile überwiegen

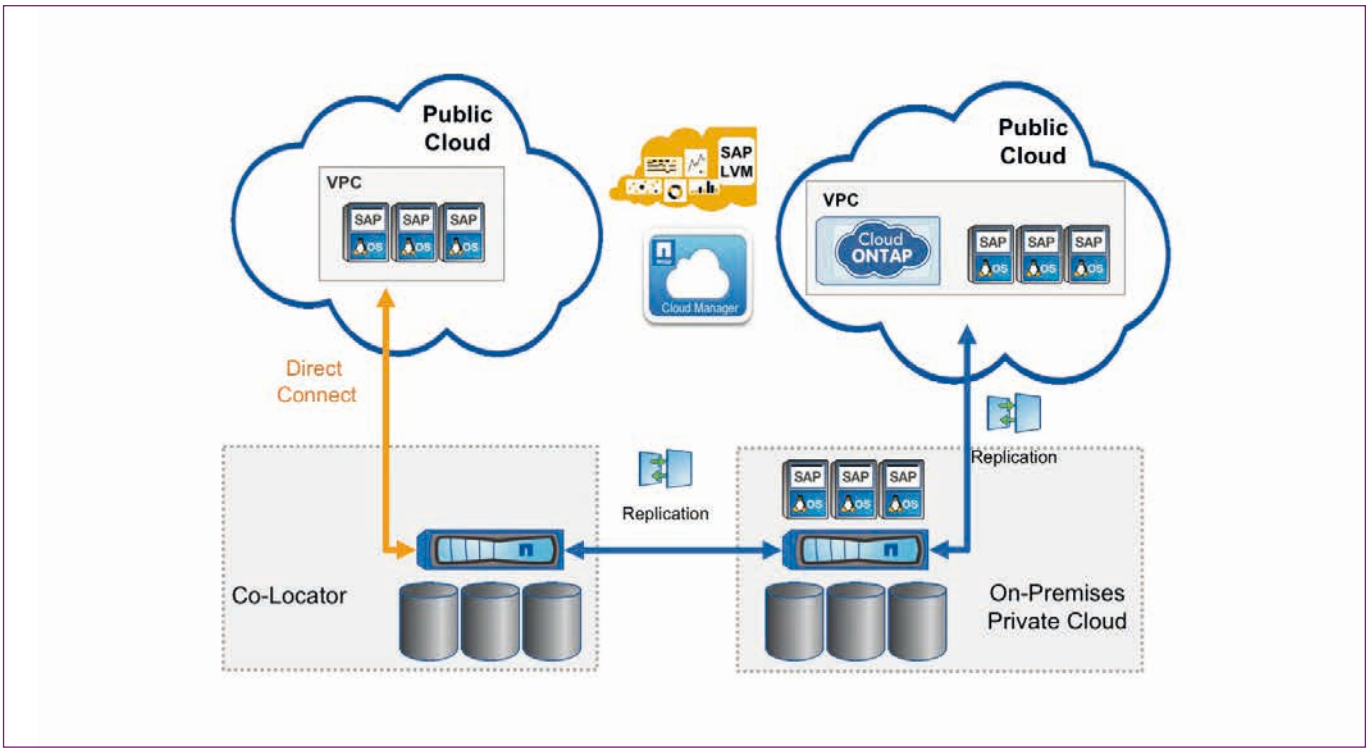
Ist die SAP-Landschaft einmal soweit umgesetzt, dass die SAP-Systeme in einer hybriden Cloud-Infrastruktur laufen könnten, stehen dem CIO zahlreiche Optionen offen, um den laufenden Betrieb zu verbessern, die Ausfallsicherheit zu steigern und Kosten zu sparen. Eine schnell realisierbare Möglichkeit ist die Integration von weiteren Hyperscale-Cloud-Providern wie Amazon, Microsoft oder Softlayer, zum Beispiel zur Bereitstellung von Test- und Anwendungsszenarien. Hier kann die IT-Abteilung den

Mit NetApp-Technologien verschieben SAP-Anwenderunternehmen ihre Daten zwischen Cloud-Ressourcen und Service-Anbietern in beide Richtungen. So müssen sie sich nicht auf einen Cloud-Anbieter festlegen, können Ressourcen aus AWS, Azure oder SoftLayer beliebig kombinieren und vermeiden ein Vendor Lock-in.

Fachbereichen vollkommen automatisiert das Einrichten, Betreiben, Entfernen und Abrechnen von SAP-Instanzen in der Cloud ermöglichen. Dies macht vor allem dann Sinn, wenn per Replizierungs-Mechanismus (Snapshot) auch die Backups in die Cloud gespeichert werden. Basierend auf diesen Snapshots lassen sich in Sekundenschnelle die Testumgebun-



Data Fabric ist das von NetApp entwickelte Konzept, mit dem IT-Verantwortliche eine Multi-Cloud-Infrastruktur realisieren.



Die technologischen Grundlagen für die flexible Nutzung der Cloud schaffen die Lösungen NetApp Private Storage sowie NetApp Cloud ONTAP. Mit SAP LVM und NetApp Cloud Manager erfolgt die Administration und Integration der Cloud-Ressourcen.

gen für SAP einrichten, beispielsweise als Projekt- oder Sandbox-Systeme für Demozwecke oder für Schulungen. Ein weiterer Vorteil von Multi-Cloud-Umgebungen: hiermit gelingt die Integration von Drittsystemen und Storage-Silos zu einer Gesamtlösung, wodurch die Wirksamkeit von Big Data-Strategien erhöht wird. Ganz wichtig hierbei: um das Datenmanagement insgesamt für den SAP-Betrieb zu vereinfachen, sollte die Steuerung von Cloud-Ressourcen, On-Premise-Systemen sowie eventuell vorhandenen Storage-Silos über nur eine zentrale Management-Oberfläche erfolgen.

Notfall-Rechenzentrum in der Cloud

Die Nutzung der Cloud als Backup-Plattform erlaubt das Einrichten weiterer Services, um so die Datenverfügbarkeit zu steigern. Beispielsweise kann die IT die Cloud als Notfallrechenzentrum nutzen, falls im eigenen Rechenzentrum Komponenten ausfallen. Die gesamte Palette von Backup, Cloning und Disaster Recovery lässt sich heute mit geeigneten Software-Lösungen vollständig in der Cloud abbilden.

Wie eine mögliche Lösung für die oben aufgeführten Anforderungen inklusive der Cloud-Integration aussieht, zeigt NetApp mit seinen Technologien, die für SAP-Systeme einen deutlichen Mehrwert gegenüber dem Einsatz von SAP-Bordwerkzeugen liefern. Von NetApp ist zum Beispiel mit Data ONTAP ein Speicherbetriebssystem verfügbar, das verschiedene Storage-Protokolle in einem Gesamtsystem vereint und hierbei auch Cloud-Ressourcen ansteuert.

SAP-Storage-Infrastruktur im Griff

Das Betriebssystem steht auch als Cloud ONTAP zur Verfügung, besitzt den gleichen Funktionsumfang und ist virtualisiert einsetzbar in HyperScaler-Umgebungen – Unternehmen erhalten sich mit dieser einheitlichen Datenmanagementplattform die Flexibilität, ihre Daten auf beliebigen On-Premise- oder Cloud-Plattformen mit einheitlicher Technologie zu betreiben. Damit werden Effekte wie die Data Gravity sowie ein möglicher Cloud Vendor Lock-in wirksam bekämpft.

Schnelle Vollsicherung

Für SAP-Umgebungen sind von NetApp spezielle Lösungen verfügbar, um schnell SAP-Kopien zu erstellen und so Projektlaufzeiten generell zu beschleunigen. Mit dem NetApp-Backup werden innerhalb weniger Sekunden konsistente Vollsicherungen der aktuellen SAP Hana-Daten erzeugt. Die Backup-Funktionen von NetApp sind nahtlos in das SAP Hana Studio integriert. Außerdem beeinträchtigt dieser Backup nicht die Leistung der Hana-Server. Eine unter SAP-Hana-Bestandskunden durchgeführte Analyse hat ergeben, dass Kunden durchschnittlich nur 19 Sekunden für ein Hana Snapshot-Backup benötigen (siehe auch E-3 Magazin Dezember 2015, „Auf der Überholspur“, Seite 92). Darüber hinaus bietet diese Technologie weitere Funktionen wie das Cloning einer Systemumgebung, um somit Backups auf ihre Datenintegrität zu testen. Dies kann über ein Repairsystem erfolgen, das sich auf Basis eines geclonten Backups in Sekundenschnelle einrichten lässt und zum Testen der Datenintegrität nutzbar ist.

Weiterhin unterstützt NetApp mit seinem Data Fabric-Konzept den Aufbau und laufenden Betrieb von hybriden Cloud-Umgebungen, sodass sich die Backups automatisiert und sicher in die Cloud transferieren lassen. Schließlich wurden die NetApp-Lösungen eng ins SAP LVM integriert, wodurch zum Beispiel eine hohe Automatisierung beim Anlegen von SAP-Systemkopien möglich wird.

Bitte beachten Sie auch den Community-Info-Eintrag ab Seite 99

NetApp®

So steigern Unternehmen mit der Cloud die Verfügbarkeit ihrer SAP-Lösungen

Restore-Restore-Schutzbrief Schutzbrief

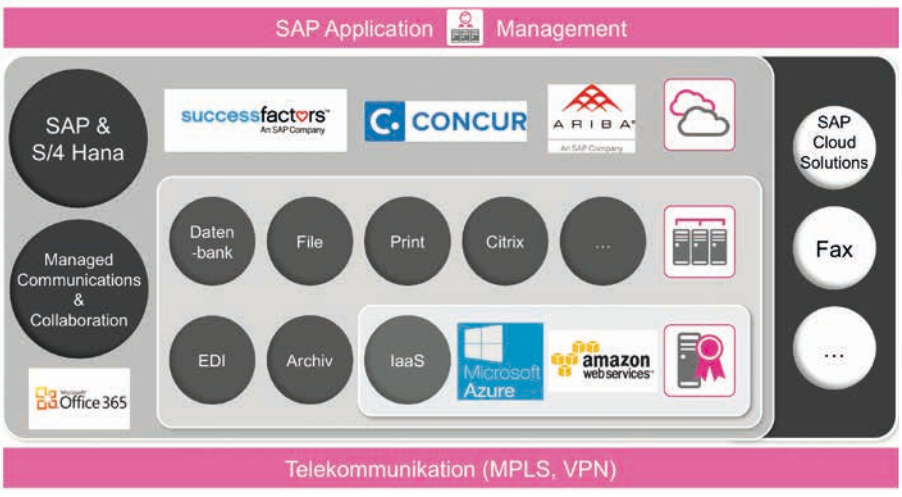
SAP-Anwendungen sind geschäftskritisch und müssen sofort nahtlos wieder anlaufen, sollten sie einmal ausfallen. Regelmäßig per Restore validierte Backups sind dazu unerlässlich. Genau hier setzt ein neues umfassendes Dienstleistungspaket von Grandconsult, All for One Steeb und NetApp an.

Von Martin Finkbeiner, Grandconsult, und Michael Scherf, All for One Steeb

Beim ersten Mal ging noch alles glatt. Das Backup ist sauber durchgelaufen. Auch ein Restore der gerade frisch aufgesetzten SAP-Produktivsysteme lieferte blitzsaubere Resultate. „Alles gut", stand unter dem Report und das Backup wanderte ins Archiv. Ein Jahr später jedoch war der Ernstfall eingetreten – nur ein Restore konnte jetzt noch helfen. Zunächst sah alles gut aus. Zumindest waren bei den regelmäßigen Backups zuvor keinerlei Auffälligkeiten zu beobachten. Auf den erstmals wieder durchgeführten Restore folgte jedoch prompt das böse Erwachen. Bei den Datensicherungen hatten sich kleine Fehler eingeschlichen und über die Zeit fortgeschrieben. Am Ende passte nichts mehr sauber zusammen. Teile der wiederhergestellten Stamm- und Bewegungsdaten zu Kunden, Preisen, Aufträgen und Lieferzeiten waren gleichermaßen unbrauchbar geworden. An einen Geschäftsbetrieb war nicht mehr zu denken. In solchen Fällen werden häufig externe SAP-Experten gerufen: Die Berater von Grandconsult waren zusammen mit ihren Kollegen von All for One Steeb von Freitag bis Sonntag damit beschäftigt, die fehlerhaften Datenbestände wieder herzustellen. Das ganze Wochenende über wurde fieberhaft analysiert, nachgefahren, getestet und nachgerechnet, ehe pünktlich am Montagmorgen der operative Geschäftsbetrieb wieder starten konnte.

Backup ist nicht alles

Solche Ereignisse sind keinesfalls Einzelfälle aus einem bewegten Beraterleben. Zwar gehören Backups zum kleinen Einmaljedes IT-Betriebs, genauso übrigens, wie die regelmäßige Überprüfung der durchgeführten Datensicherungen. Die Praxis hingegen zeichnet ein deutlich anderes Bild. Weniger beim Backup, vor allem jedoch beim Restore. Fehlende Ressourcen, etwa bei Personal, Compute oder Storage, neue Technologien wie Hana, erweiterte Anwendungslandschaften und vor allem „Big Data", der massive Anstieg des täglichen Datenvolumens, sorgen immer häufiger dafür, dass die entscheidenden Schritte, die Validierung der laufenden Datensicherungen, unter den Tisch fallen. Weder CEO, noch CFO oder CIO wollen naturgemäß gerne an solche wunde Punkte erinnert werden. „Augen zu und durch, wird schon gutgehen", lautet allzu oft noch die Devise. Und wenn dann doch einmal etwas passiert, wird meist nur hinter vorgehaltener Hand darüber gesprochen – wenn überhaupt. Solche Ausfälle dürfen nicht in die Öffentlichkeit durchdringen, entsprechend rar sind belastbare Zahlen über die Häufigkeit solcher Ereignisse. Die Gründe für derart viel, nennen wir es, „Diskretion", sind mit weichen Faktoren wie Reputationsverlust alleine nicht erklärt. Es geht zunehmend um Handfesteres. Immer genauer müssen etwa Finanzinstitute die IT-Ausfallsicherheit ihrer kreditsuchenden Unternehmenskunden ins Visier nehmen. Basel 2 verlangt das geradezu. Wer hier Schwächen offenbaren muss, dem winken empfindlich höhere Kosten bei der Unternehmensfinanzierung.



Zunächst kommen die bisherigen Backup-Prozesse auf den Prüfstand, ehe für jeden Geschäftsbetrieb und jede Software-Landschaft der passende Restore-Schutzbrief abgeschlossen wird.

Regelmäßige Validierung

Backup alleine ist jedoch nicht alles, denn ohne entsprechende Validierung ist aller Backup im Ernstfall wertlos. In Phasen des „Durchtauchens" benötigen auch naheliegende Erkenntnisse ihre Zeit, ehe sie ihren festen Platz im IT Service-Betrieb gefunden haben. Zusammen mit NetApp wurden Ursachen, Wirkungszusammenhänge, Erkenntnisse und Erfahrungen solcher Noteinsätze genau analysiert und die passenden Lösungen dazu jetzt in einen Restore-Schutzbrief gegossen.

Michael Scherf verantwortet in der Geschäftsleitung von All for One Steeb die Managed-Services-Aktivitäten, die sich immer mehr in Richtung Orchestrierung von IT-Betriebslösungen etwa für Hana in Private Cloud, Public Cloud und On Premise entwickeln.

Martin Finkbeiner ist Geschäftsführer der All for One Steeb Tochter Grandconsult. Der Data Fabric-Experte berät Großkonzerne und mittlerweile verstärkt auch den Mittelstand bei der Ausrichtung ihrer Rechenzentren hin zu einem industrialisierten IT-Betrieb etwa für Hana.

Der Grundgedanke ist einfach: Kein Backup ohne regelmäßige Validierung, denn nur so lässt sich ein IT-Betrieb wirkungsvoll absichern. So umfasst der Restore-Schutzbrief drei aufeinander abgestimmte Leistungsstufen: „Consult & Design“, „Build & Implement“ sowie „Run“.

Als Ausgangspunkt dient regelmäßig die genaue Aufnahme der bisher praktizierten Datensicherungsverfahren. Daraus werden die Anforderungen an den genauen Leistungsumfang des Restore-Schutzbriefes abgeleitet und im Detail die Soll-Prozesse für Backup und Restore konzipiert. Zur „Consult & Design“-Phase gehört optional die Auswahl eines geeigneten Providers, der die benötigte Backup- und Restore-Betriebsumgebung gewissermaßen schlüsselfertig aus seiner Cloud als Service bereitstellt. In der Praxis lassen sich so erhebliche Kosten-, Qualitäts- und Skalierungsvorteile erzielen. Mit Orchestrierungskompetenz, die sich über On-Premise, Private und Public-Cloud-Ressourcen erstreckt, lassen sich zudem in dieser Phase bereits rasch Demo-Umgebungen aufbauen, die eine gute Basis für die anschließenden „Build & Implement“-Schritte liefern.

Fokus Restore-Prozesse

Je nach Kundenanwendung stehen hier Leistungen wie die Bereitstellung der IT-Infrastruktur, das Setup für den erstmaligen Datentransfer, die Einrichtung einer kontinuierlichen Backup-Replikation in der festgelegten Periodizität und vor allem die eigentliche Implementierung der Restore-Prozesse im Vordergrund. Auf ihrer Basis, erfolgreich durchgeführte Tests eingeschlossen, wird der Restore-Schutzbrief später auch formal abgenommen und in den Regelbetrieb überführt. In dieser „Run Phase“ übernehmen externe Dienstleister wie Grandconsult zusammen mit All for One Steeb die regelmäßige Durchführung und Validierung der Restore-Prozesse. Diese erfolgt zweistufig: Für die rein systemseitige Rücksicherung werden stets zunächst die Backup- und Log-Dateien in die Restore-Umgebung übertragen. Im gleichen Arbeitsschritt erfolgt das „Deployment“ der Log-Files. Damit werden gleichzeitig die Grundlagen für die anwendungsseitige Validierung geschaffen. Ist der „Datenbank Verify“ wirklich ok? Lässt sich der „System LogOn“ auf dem testweise wiederhergestellten System erfolgreich absetzen? Liefern ausgewählte Transaktionen und Reports dieselben Ergebnisse wie auf den Produktiv-Systemen? Erst wenn alle diese Fragen klar mit „ja“ beantwortet sind, erfolgt die Freigabe. Je nach Schutzbriefvereinbarung werden diese Schritte regelmäßig wiederholt. Die Häufigkeit, mit der die Validierungen durchgeführt werden, richtet sich nach individuellen Erfordernissen. Die Ergebnisse werden in einem gesonderten Reporting festgehalten. Die Wartung der Restore-Umgebung erfolgt, genauso wie Anpassungen an neue Anforderungen, ebenso in dieser Phase. Technologisch basieren die Backup- und Restore-Umgebungen auf Lösungen von NetApp, etwa SnapVault und SnapMirror. Damit lassen sich parallel und ohne Beeinträchtigung des IT-Betriebs während des laufenden Tagesgeschäfts Datensicherungen per Snapshot durchführen, auslagern und wiederherstellen. Zur Validierung des Backups kommen NetApp Private Store, Cloud ONTAP, Flex Clone und FlexClone Split zum Einsatz.

Welches Betriebsszenario?

Die Backup-Umgebung vor Ort im eigenen Rechenzentrum ausbauen? Auslagerung des Backups zum Service Provider in die Private Cloud mit oder ohne zusätzlichen Einbezug von Public Cloud-Ressourcen? Oder gar eine dynamische Kombination von allem? Die jeweils beste Betriebslösung erfordert stets eine eingehende Bewertung der Ausgangslage. Diese ist naturgemäß individuell. Generell lässt sich folgendes festhalten: Ausbau, Betrieb und Anpassungen einer eigenen Backup-Umgebung samt regelmäßig validiertem Restore binden dauerhaft erhebliche personelle Ressourcen. Dazu kommen fixe Kosten. Dies alles entfällt bei der Auslagerung an einen externen Provider. Hier erfolgt die Abrechnung „On Demand“, also nutzungsbezogen. Zudem garantieren regelmäßig belastbare Service Level-Vereinbarungen die zugesicherten Leistungen.

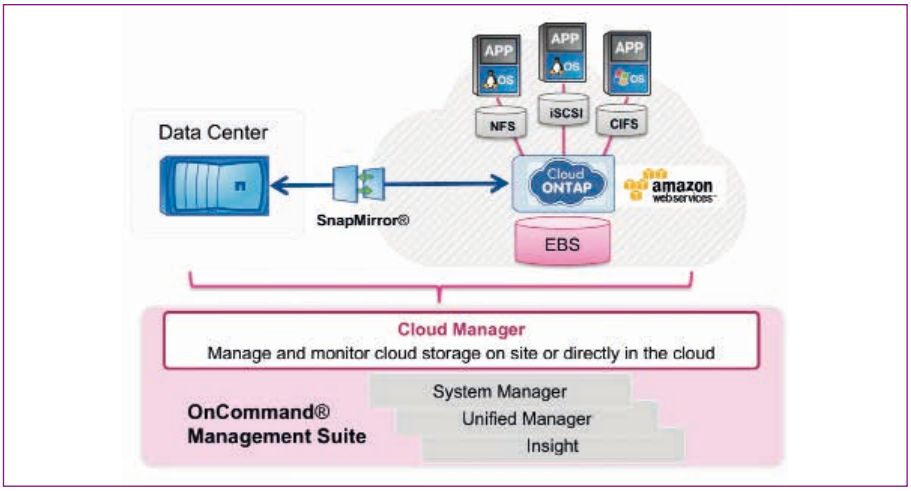
Ganz neue Wege eröffnen Service Provider mit der Orchestrierung von dynamischen IT-Szenarien. Solche Betriebslösungen zielen auf ein Zusammenwirken zwischen dem IT-Betrieb vor Ort, etwa im Rechenzentrum des Kunden, und dem IT-Betrieb aus der Private Cloud, z.B. aus dem All-for-One-Steeb-Datacenter. Dabei werden für bestimmte Einsatzzwecke au-

Backup unter neuen Vorzeichen

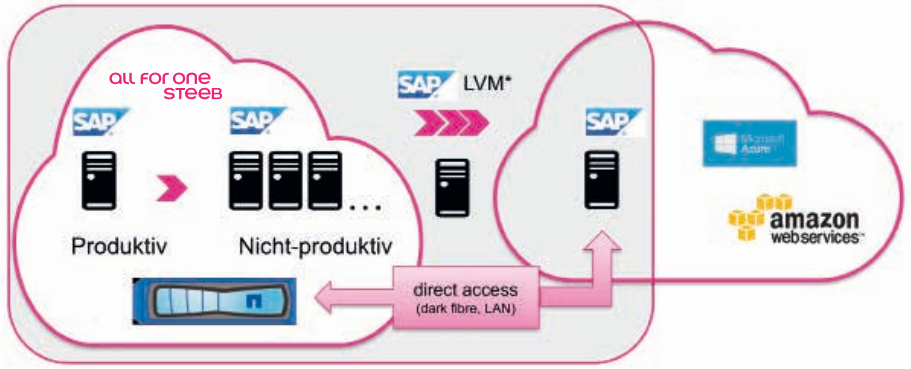
Das Voranschreiten von Hana und SAP Cloud Solutions im Verbund mit herkömmlichen SAP-Landschaften wird für viele herkömmliche IT-Betriebslösungen zur Nagelprobe. Durchgängige Virtualisierung, Automatisierung und Skalierung innerhalb eines industrialisierten IT-Betriebs aus der Private Cloud beherrschen unter den vielen neuen Vorzeichen beim genauen Hinschauen bis dato jedoch nur wenige Top-Spezialisten. Was zunächst bei Großkonzernen begann, hält zudem vermehrt im Mittelstand Einzug. Entsprechend stark wächst der Beratungsbedarf. Besonders gefragt sind daher „Trusted Advisor" mit einem ganzheitlichen Beratungsansatz in strategischen Technologiefragen, etwa die Konzeption, Virtualisierung, Flexibilisierung und Orchestrierung spezifischer Referenzarchitekturen für den Betrieb von Hana, On-Going-Betreuung des IT-Betriebs mit Service Level Agreements sowie zusätzlich Management- und Prozessberatung. Während Grandconsult namhafte Großkonzerne in deren Rechenzentren berät und dazu mit Partnern wie NetApp und Cisco ein „Joint Research & Development Lab" bei SAP in Walldorf betreibt, zählt All for One Steeb im Managed Services-Markt zu den führenden Private Cloud Providern für den SAP-Betrieb.

Webinare: Mehr erfahren über den Restore-Schutzbrief

Backup alleine ist nicht alles, denn ohne entsprechende Validierung ist aller Backup im Ernstfall wertlos. Genau hier setzt der Restore-Schutzbrief von Grandconsult und All for One Steeb an. Mehr über typische Einsatzszenarien im eigenen Rechenzentrum, in der Private und in der Public Cloud liefert eine Webinar-Reihe. Termine und Anmeldungen unter www.all-for-one.com/events



SAP-Betrieb On Demand mit NetApp Cloud ONTAP in der hybriden Cloud



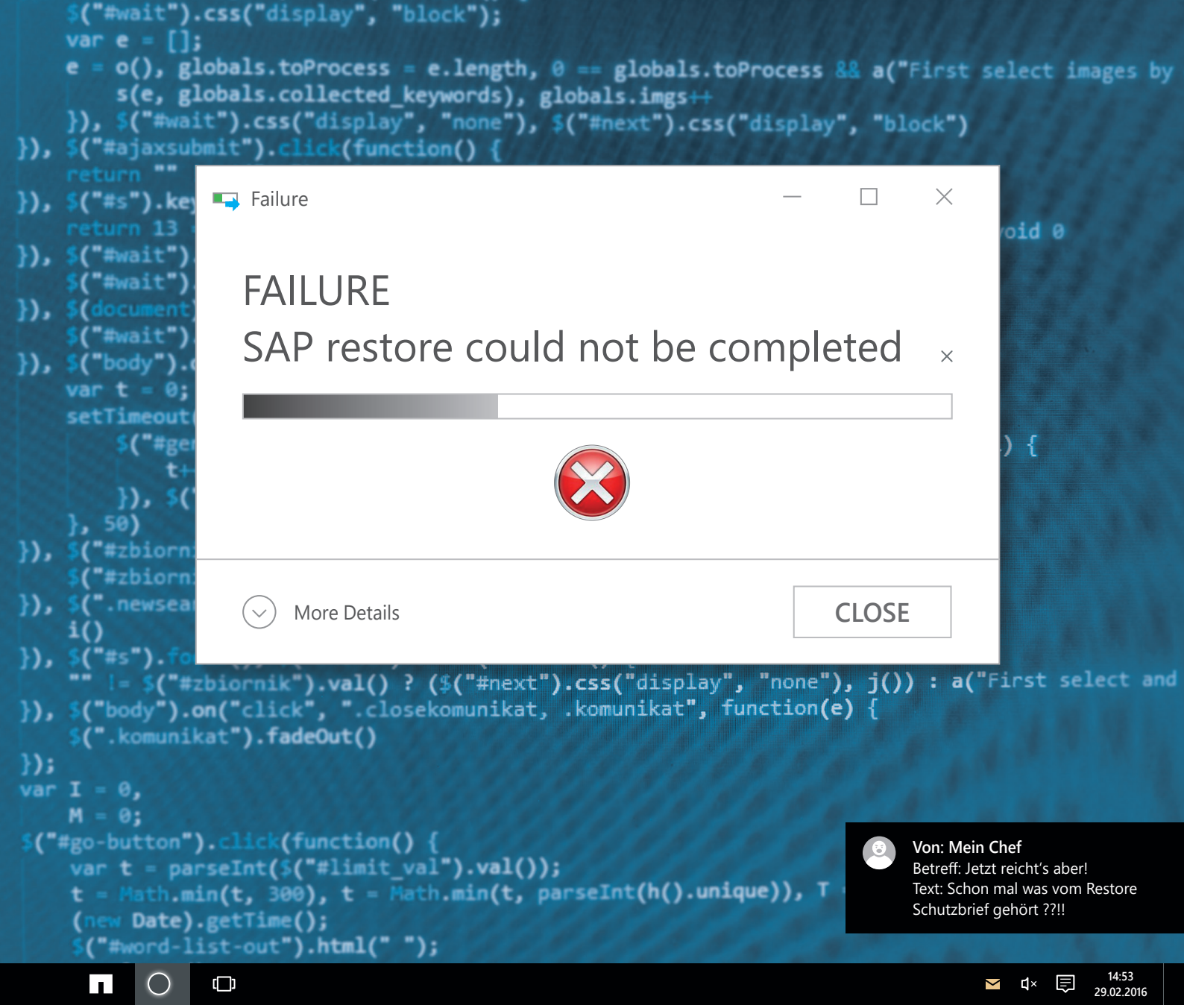
SAP-Betrieb in der Hybride Cloud mit NetApp Private Storage: Private und Public Cloud beim gleichen Co-Locator, Daten verbleiben in der Private Cloud, Compute-Leistung aus der Public Cloud.

ßerhalb des geschäftskritischen SAP-Applikationsbetriebs verstärkt Public Cloud-Ressourcen mit dazu geschaltet. Im Dunstkreis von Ereignissen wie der NSA-Affäre oder aktuell Safe Harbor mag das überraschen. Fragen zur Datenhoheit, Datenautonomie oder Datensicherheit, etwa zur Abwehr von Cyberkriminalität, sind stets fester Bestandteil einer jeden Gesamtbetrachtung über den Wertbeitrag, den jeder CIO mit seinem Team zur Geschäftsentwicklung in Zeiten der digitalen Transformation leisten muss. Sicherheitsaspekte werden daher zunehmend nüchtern und analytisch im Rahmen einer qualifizierten technischen wie juristischen Diskussion überprüft. Als Hintergrund dient hier ein in Deutschland besonders gut ausgeprägter Rechtsrahmen. Der gesamte Datenbestand liegt etwa in der Private Cloud, also in den Rechenzentren eines besonders vertrauenswürdigen Service Providers. Ihr Schutzniveau übersteigt, aufgrund aufwändiger Zertifizierungen wie ISAE 3402 Typ II oder ISO 27001, häufig den IT-Sicherheitslevel des Eigenbetriebs. Die selektiv aus der Public Cloud dazu geschalteten Compute-Ressourcen halten keinerlei Daten dauerhaft. Solche Ressourcen werden nur temporär zur Laufzeit benutzt. So lassen sich etwa Datenbanken wiederherstellen, Applikationen hochfahren und Konsistenzchecks durchführen. Die Datenhoheit bleibt so unangetastet und stets beim Kunden. Public Cloud-Provider haben in puncto Sensibilität bei Datensicherheit mächtig zugelegt. IT-Produktionsstätten vor Ort in Deutschland sind auch hier zunehmend an der Tagesordnung. In derart dynamischen IT-Betriebsmodellen lassen sich aus der Cloud viele weitere Services nutzen. Das Spektrum reicht von sehr schnell zu- und abschaltbaren Systemen etwa für Repair, Projekt, Sandbox, Test, Demo oder Schulungszwecke bis hin zu Backup Insurance-Systemen, die im Disaster Recovery-Fall als Rückfallposition dienen, sodass Ausfallzeiten für die IT-Systeme wirksam minimiert werden.

Bitte beachten Sie auch den Community-Info-Eintrag ab Seite 99

all for one steeb

www.grand-consult.com



Wenn Sie Ihren Job mögen, werden Sie unseren Restore Schutzbrief lieben.

Backup ist nicht alles, denn ohne restorefähigen Backup ist alles nichts. Daher kein Backup mehr, ohne regemäßig validierten Restore. Nur von uns mit Brief und Siegel, nach eingehender Analyse, Konzeption und Beratung: Der Restore Schutzbrief, damit Ihre SAP Landschaft auch dann weiterläuft, wenn sie einmal ausfällt.

Regelmäßig validiert
Backup plus Restore als Service

Individuell
On Premise, Private Cloud mit/ohne Public Cloud, Hybrid Cloud

Robust und belastbar
Passgenaue Service Level Agreements

Posteingang

Carsten Müller
Grandconsult GmbH
carsten.mueller@grand-consult.com

Sie wollen mehr über unsere Restore Schutzbrief-Garantie erfahren? Rufen Sie mich dazu gerne an!

Telefon +49 (0)40-360 976 035

CeBIT 2016: Halle 4, bei SAP

NetApp® all for one steeb Grandconsult