arcserve®

WHITE PAPER

Hochverfügbarkeit ist kein Luxus.

Ausfallzeiten vermeiden in Mittelstandsunternehmen

Die Informationstechnologie (IT) bietet kleinen und mittleren Unternehmen enormen Nutzen, stellt allerdings auch eine gewaltige Schwachstelle dar. Angesichts weltweiter Märkte arbeiten Beschäftigte rund um die Uhr, und die Unternehmen sind quasi immer irgendwo online. Jede Unterbrechung der Anwendungsverfügbarkeit kann schnell Umsatzverluste, Produktivitätseinbußen, Verlust an Markenwert und rechtliche Implikationen zur Folge haben. Eine längere Ausfallzeit kann im Extremfall sogar den Bestand Ihres Unternehmens gefährden.

Wie also soll Ihr Unternehmen mit dieser Art von existenzieller Bedrohung umgehen? Die traurige Realität sieht leider so aus, dass die meisten Unternehmen es schlichtweg ignorieren.

Business Continuity – also die Planung, Vorbereitung und Implementierung ausfallsicherer Geschäftssysteme im Vorgriff auf ungeplante Ausfallzeiten – wird nicht selten als IT-Problem betrachtet. Deshalb überlassen es die meisten Unternehmen auch der IT-Abteilung, eine Lösung dafür zu finden. Dies führt zwangsläufig dazu, dass unterschiedliche taktische Lösungen bereitgestellt werden, die sich aber nicht an einer übergeordneten Strategie orientieren. Tatsächlich ist Business Continuity aber ein Problem des Unternehmens, und deshalb erfordert es auch einen unternehmensorientierten Lösungsansatz.

Die folgende Checkliste zeigt Ihnen, ob Ihr Business Continuity-Plan Sie schützt oder nicht. Wenn Sie die Punkte bejahen, sind Sie einem Risiko ausgesetzt:

- **Ihr Plan erfordert in großem Umfang manuelles Eingreifen.**
- **Ihr Plan nimmt bei einem Ausfall Datenverluste in kritischen Systemen von mehr als ein paar Sekunden in Kauf.**
- **Sie können mit Ihrem Plan den Zugriff auf kritische Systeme nicht innerhalb von Minuten wiederherstellen.**
- **Ihr Plan stützt sich auf eine 30 Jahre alte Datensicherungs- und Wiederherstellungstechnologie.**

Datensicherung und Wiederherstellung waren 30 Jahre lang für die Absicherung von IT-Systemen die bevorzugte Methode. Sie wurden allerdings in viel einfacheren Zeiten entwickelt. Bei der Sicherung von Daten auf Band oder Festplatte, oder bei der Erfassung von Snapshots – die moderne Entsprechung einer Datensicherung–, wird ein punktuelles Abbild der Anwendungsdaten erstellt. Erfolgt die Wiederherstellung jedoch auf Basis einer punktuellen Kopie, erhalten Sie nie aktuellere Daten als die zum Zeitpunkt der letzten Sicherung. Ganz gleich, ob Ihre Kopie 15 Minuten oder zwei Tage alt ist – die Wiederherstellung der Sicherung geht immer mit Datenverlust und entsprechenden Folgen einher. Für einige Systeme mag das akzeptabel sein. Für viele Ihrer erfolgskritischen Geschäftsanwendungen hätte dies aber katastrophale Folgen.

Die Sicherungs- und Wiederherstellungstechniken wurden für relativ unkomplizierte Computing-Prozesse entwickelt, und in einer Zeit, in der noch regelmäßige Zeitfenster eingeplant wurden, in denen niemand das System nutzen würde. Die Geschäftsanwendungen, auf die die Unternehmen heute ihren Tagesbetrieb stützen, müssen immer online sein. Deshalb ist eine Technologie vonnöten, die eine ununterbrochene Systemverfügbarkeit gewährleistet und das Risiko von Datenverlusten ausräumt, ohne auf bestimmte Backup-Fenster angewiesen zu sein.

Moderne Hochverfügbarkeitstechnologie (High Availability, HA) überträgt Anwendungs- und Datenänderungen kontinuierlich an einen dezentralen Standort. Im Notfall, z. B. bei Erdbeben, Stromausfällen oder einer fehlgeschlagenen Softwareinstallation, erfolgt sofort und vollkommen automatisch ein Failover zu einer aktuellen Kopie Ihres Systems. HA eliminiert Ausfallzeiten und somit auch Datenverluste.

Hochverfügbarkeit für alle

HA ist die ideale Lösung, wenn Sie Ihre Systeme vor Ausfallzeiten und Datenverlusten schützen möchten. Jahrelang genoss HA allerdings einen schlechten Ruf. Man hielt die Technologie für zu komplex und zu teuer für kleine und mittlere Unternehmen. Man war allgemein der Ansicht, dass nur große Unternehmen mit umfangreichem Budget und unerschöpflichen IT-Ressourcen realistischerweise in der Lage wären, HA-Lösungen bereitzustellen. Bis vor Kurzem hielt sich dieses Vorurteil noch.

Bei HA wird in der Regel eine Kombination aus Replikations- und Server-Heartbeat-Technologie verwendet, damit die IT-Systeme am dezentralen Standort mit den Anwendungen im Hauptrechenzentrum synchron gehalten werden können. Früher bedeutete dies dedizierte Netzwerke mit hoher Bandbreite zwischen zwei physischen Standorten sowie redundante Kopien der Server-, Speicher- und Netzwerkhardware, mit speziellen Anwendungen und spezieller Betriebssoftware. Aufgrund der Kosten für diese Redundanz blieb HA für kleinere Unternehmen stets unerreichbar.

Heute sind kostengünstige Netzwerke mit hoher Bandbreite allgegenwärtig – sie sind inzwischen sogar zu einer betriebswirtschaftlichen Notwendigkeit geworden. Darüber hinaus ist es dank zahlreicher Service Provider problemlos möglich, virtuelle Server On-Demand und zu sehr geringen Kosten einzurichten. Diese Fortschritte bei der Infrastruktur bedeuten, dass die HA-Technologie heute mehr Unternehmen zu einem weitaus erschwinglicheren Preis zur Verfügung steht.

Der drastische Rückgang bei den HA-Infrastrukturkosten hat dazu geführt, dass die Business Continuity-Pläne vieler Unternehmen nun neu überdacht werden. Unkoordinierte, sich vielfach überschneidende Backup-Lösungen gibt es im Rechenzentrum zuhauf. Wenn Sie in der Vergangenheit in puncto Business Continuity auf Backup und Wiederherstellung gesetzt haben, wissen Sie wahrscheinlich, dass diese isolierten Lösungen der reinste Wartungsalbtraum sind, die Produktivität hemmen und, was noch wichtiger ist, die Disaster Recovery deutlich verkomplizieren. Moderne HA-Lösungen bieten einen universellen Ansatz für Business Continuity, der die Kosten für Datensicherung senkt, die Disaster Recovery vereinfacht sowie Datenverluste und Ausfallzeiten beseitigt.

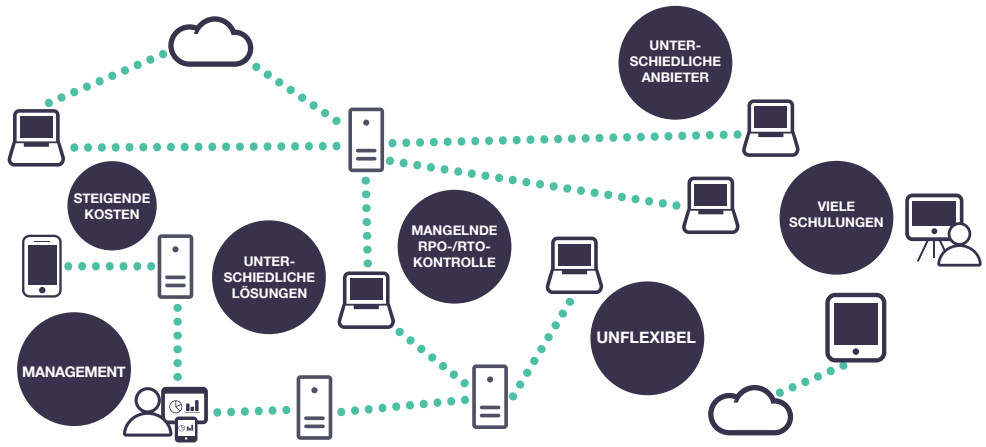

Abbildung 1: Die verborgenen Komplexitätsrisiken beim Einsatz isolierter Backup-Lösungen

HA mag sich für Ihr Unternehmen zwar anbieten, ohne eine detaillierte Analyse der Geschäftssysteme mit den zugehörigen Anforderungen an die Wiederherstellung wissen Sie allerdings nicht, welche Anwendungen davon profitieren werden. Gewiss ist auf jeden Fall, dass die früheren Einschränkungen bezüglich HA-Bereitstellungen nicht mehr gelten. Folglich können Sie sich nun anderen Problemen zuwenden, die Ihren Business Continuity-Plänen im Wege stehen könnten.

Die zehn wichtigsten Fallstricke bei der Business Continuity

Alle sprechen darüber, wie Disaster Recovery richtig geht. Ebenso hilfreich ist es jedoch zu wissen, welche Stolpersteine einen erwarten, wenn Disaster Recovery nicht richtig durchgeführt wird. Deshalb haben wir eine Liste der zehn wichtigsten Fallstricke bei der Planung von Disaster Recovery und Business Continuity erstellt.

1 Es geht um das Unternehmen, nicht um Technologie!

Disaster Recovery, Hochverfügbarkeit, Datensicherung und Wiederherstellung, Business Continuity – wie auch immer man es bezeichnen mag, das Ziel ist immer das gleiche: der Geschäftsbetrieb des Unternehmens ist unter allen Umständen aufrechtzuerhalten. Allzu oft lassen die Unternehmen es zu, dass die Technologie zu sehr in den Vordergrund gerät. Oft gerät aus dem Blick, dass es bei Disaster Recovery darum geht, eine geschäftliche Anforderung zu erfüllen. Deshalb müssen den Überlegungen auch geschäftliche Anforderungen zugrunde gelegt werden. Bevor Sie versuchen herauszufinden, wie Sie Disaster Recovery implementieren sollten, müssen Sie nach dem „Warum" fragen. Sprechen Sie mit Führungsverantwortlichen in Ihrem Unternehmen, um zu verstehen, was für sie wichtig ist. Für einige wird das E-Mail sein, für andere das System für die Online-Auftragserfassung und für wieder andere Microsoft SharePoint. Der springende Punkt ist, dass Sie nicht wissen können, welche Systeme die wichtigsten sind, wenn Sie nicht die Anwender im Unternehmen fragen. Wenn Sie die Anforderungen des Unternehmens verstehen, können Sie entsprechende Prioritäten festlegen, die Sie zudem bei der Auswahl der Disaster Recovery-Technologie unterstützen.

2 Es kann eine Katastrophe sein – muss aber nicht

Wenn Sie an Disaster Recovery denken, haben Sie wahrscheinlich Wirbelstürme, Überschwemmungen, Terrorangriffe und Ähnliches vor Augen, nicht aber, dass ein Software-Upgrade aufgrund eines nicht gut durchdachten Rollback-Verfahrens schief geht oder dass ein Hardware-Fehler in einer kritischen Netzwerkkomponente auftritt. Für gewöhnlich wird für ein Worst-Case-Szenario geplant und für triviale alltägliche Fehler vorgesorgt. Bei Ihrer Disaster Recovery-Planung müssen Sie alle Eventualitäten berücksichtigen – vom alltäglichen bis zum katastrophalen Ereignis.

3 Wie können Sie Budgets verteilen, ohne die Kosten für Systemausfälle zu kennen?

Zu oft weisen Unternehmen ein Budget für die Disaster Recovery-Planung zu, bevor sie überhaupt das finanzielle Risiko von Ausfallzeiten und Datenverlusten für das Unternehmen ermittelt haben. Wenn Sie nicht beziffern können, wie viel Geld Sie durch einen Ausfall kritischer Systeme verlieren können, wird es schwierig sein zu ermitteln, wie viel Sie ausgeben sollten, um diese Verluste zu verhindern. Ihr Ansatz für Disaster Recovery muss an den Anforderungen des Unternehmens ausgerichtet sein. Und dies heißt, dass die Kosten für einen Ausfall vor Budgetzuteilung bewertet werden müssen. Vergessen Sie bei Ihren Kostenberechnungen für Ausfallzeiten auch die Einhaltung von Vorschriften nicht. Für nicht erfüllte gesetzliche Vorgaben drohen häufig empfindliche Geldstrafen.

4 Abschätzen der Risiken

Welche Ereignisse als Katastrophe eingestuft werden, ist in jedem Unternehmen unterschiedlich, nicht selten sogar von Abteilung zu Abteilung. Einige Ereignisse, beispielsweise Erdbeben, können so katastrophale Folgen haben, dass sich das Unternehmen ganz offensichtlich davor schützen muss. Andere Ereignisse scheinen zunächst nichts Besonderes zu sein, z. B. eine ausgefallene Netzwerk-Hardware. Dennoch können sie enorme finanzielle Auswirkungen haben. Wenn Sie an Disaster Recovery denken, sollten Sie sich unbedingt folgende Fragen stellen: Wogegen sollen wir uns schützen? Übersehen Sie auch das augenscheinlich Banale nicht. Geringfügige Verluste aufgrund alltäglicher Probleme können sich schnell summieren.

5 Haben Sie einen Plan?

Wenn Ihr Disaster Recovery-Plan nur eine Haftnotiz auf den Backup-Bändern unter dem Bett Ihres Systemadministrators ist, haben Sie ein Problem. Es klingt zwar erstaunlich, aber eine überraschend große Anzahl Unternehmen hat keinen Disaster Recovery-Plan. Wichtig ist, dass Sie ein formales Dokument ausarbeiten, in dem alle Anwendungen, Hardware, Anlagen, Service Provider, Mitarbeiter und Prioritäten aufgeführt sind. Und Sie müssen von allen Stakeholdern im Unternehmen entsprechende Unterstützung einholen. Der Plan muss alle funktionalen Bereiche umfassen und klare Richtlinien dahingehend enthalten, was vor, während und nach einem Notfall zu geschehen hat.

6 Wir haben einen Plan, aber den haben wir nie getestet

Ein Disaster Recovery-Plans ist nur dann sinnvoll, wenn er auch funktioniert. Und dies lässt sich nur sicherstellen, indem Sie ihn testen. Den Plan unter simulierten Notfallbedingungen zu testen, ist zwar wichtig, kann aber auch eine Herausforderung darstellen. Disaster Recovery-Tests sind kostspielig und ziehen wichtige Zeit- und Personalressourcen aus dem Tagesbetrieb ab. Es bleibt aber dabei: Ohne vollständig auf Anwendungsebene getestete Wiederherstellung stehen Sie bei einem echten Notfall vor einem Problem. Halten Sie Ausschau nach Datensicherungslösungen, die es Ihnen ermöglichen, Umgebungen für unterbrechungsfreie Tests Ihrer Disaster Recovery-Pläne einzurichten.

7 Wer ist für was verantwortlich?

Ein echtes Notfallereignis läuft immer chaotisch ab und stiftet viel Verwirrung. Wenn wichtige Mitarbeiter nicht wissen, welche Zuständigkeiten sie im Notfall haben, dauert die Wiederherstellung unnötig lange und geht mit zahlreichen Schwierigkeiten einher. In Ihrem Disaster Recovery-Plan müssen die Rollen und Verantwortlichkeiten jeder beteiligten Person klar dargelegt sein. Dies beinhaltet auch, was zu tun ist, wenn zuständige Mitarbeiter nicht verfügbar sind. Diese Personen müssen außerdem an den Tests Ihres Disaster Recovery-Plans beteiligt werden.

8 Was ist RPO? Und was ist RTO?

Es ist von entscheidender Bedeutung, zu wissen, wie anfällig jeder Bereich Ihres Unternehmens für Ausfallzeiten und Datenverluste ist. Diese Informationen helfen Ihnen bei der Auswahl der richtigen Disaster Recovery-Technologie, bilden die Grundlage für Ihre Disaster Recovery-Planung und geben Aufschluss über die Konsequenzen eines Ausfalls, um jede Geschäftsanwendung wiederherzustellen. Es werden zwei Messdaten verwendet, um die Toleranz einer Anwendung bezüglich Ausfallzeit und Datenverlust zu messen: Recovery Point Objective (RPO) und Recovery Time Objective (RTO). Beide Metriken werden in Zeit gemessen. RPO geht bis zum Zeitpunkt des Notfalls zurück, während RTO in die Zukunft gerichtet ist.

RPO ist ein Messwert für Datenverlust. Je größer der RPO, desto mehr Datenverlust wird innerhalb einer Anwendung toleriert, bevor es für das Unternehmen problematisch wird. Stellen Sie ihn sich als Zeitpunkt vor, bis zu dem Sie Daten erfolgreich wiederherstellen können. Alle Daten zwischen diesem Punkt und dem Eintritt des Notfalls sind verloren.

RTO ist ein Messwert für die Bedeutung einer Anwendung für den laufenden Geschäftsbetrieb. Je geringer der RTO, desto schneller muss die Anwendung wiederhergestellt sein, bevor das Unternehmen bedeutende Verluste erleidet.

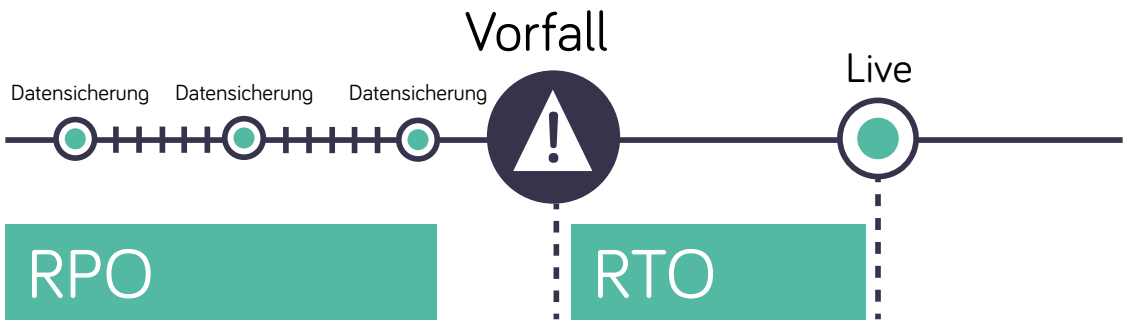

Abbildung 2: Wichtiger Bestandteil Ihres Business Continuity-Plans ist das Wissen, wie oft Ihre unterschiedlichen Anwendungen und Datenquellen gesichert werden sollten (Recovery Point Objective – RPO) und wie schnell Sie sie wieder brauchen (Recovery Time Objective – RTO).

Wenn Sie RPO und RTO für jede Anwendung nicht kennen, werden Sie bei der Disaster Recovery im Dunkeln tappen. Was auch immer Sie tun, um nach einem Notfall für Wiederherstellung zu sorgen, ist reine Spekulation. Mit RPO und RTO können Sie Service-Level definieren, die Sie erreichen müssen.

Technologien wie Continuous Data Protection sind unverzichtbar, um sicherzustellen, dass diese Ziele erfüllt werden können.

9 Die Wiederherstellung dauert länger, als Sie gedacht haben

Für viele Unternehmen endet die Sorge um Disaster Recovery in dem Moment, wenn die Backup-Bänder das Rechenzentrum verlassen. Es ist allerdings entscheidend zu wissen, wie lange die Wiederherstellung wichtiger Unternehmenssysteme dauert und wie viel kritische Geschäftsdaten nach einem Notfall verloren sind. Auch wenn Sie auf ausgelagerte Backup-Kopien zugreifen können, heißt dies nicht, dass Sie die Anwendungen rechtzeitig wiederherstellen können. Haben Sie Zugriff auf Hardware, die die Daten lesen kann? Können Daten und Anwendungen dem Anwender schnell genug zur Verfügung gestellt werden? Verfügen Sie über ausreichend Bandbreite, um Daten von einem Cloud Service Provider wiederherzustellen? Wenn Sie wissen, wie lange die Wiederherstellung von Anwendungen dauert und welche Folgen der Ausfall auf das Unternehmen hat, entscheiden Sie sich vielleicht für eine andere Technologie.

10 Wieder auf dem Produktionssystem

Bei der Disaster Recovery-Planung wird eine Komponente häufig vernachlässigt: die Rückkehr zum Produktionssystem nach einem Failover zu einem Notfallstandort. Der Grund liegt auf der Hand. Wenn wir an einen Notfall denken, geht es uns dabei primär darum, unsere wertvollen Assets zu schützen. Wir verschwenden wenig Gedanken daran, was mit diesen Assets passiert, nachdem das Notfallereignis vorbei ist.

Die Fähigkeit des Failback zu den Produktionssystemen ist ebenso wichtig wie die Fähigkeit zum Failover. Sofern es nicht sorgfältig geplant wurde, verfügt ein Backup-Rechenzentrum voraussichtlich nicht über dieselbe Kapazität oder Performance wie der Produktionsstandort.

Ohne Failback-Plan führen Sie zwar vielleicht einen erfolgreichen ersten Failover durch, fahren dann aber zunehmend Verluste ein, wenn Ihr Unternehmen seinen Betrieb wochenlang auf der Basis eines unzulänglich ausgelegten Backup-Standorts aufrechterhalten muss.

Die Risiken kennen

Mit Ausnahme von E-Mail ist es fast unmöglich zu wissen, welche Anwendungen für Ihr Unternehmen das größte Ausfallrisiko darstellen, ohne Informationen von den Mitarbeitern aus den jeweiligen Fachbereichen einzuholen. RPO und RTO bieten Messdaten, um dieses Risiko zu bestimmen. Sie geben auch Aufschluss darüber, welche Anwendungen bei Ihren Disaster Recovery-Bemühungen an oberster Stelle stehen sollten.

Sowohl RPO als auch RTO sind kontinuierliche Größen. Stellen Sie sich eine Zeitleiste mit dem Ausfallereignis in der Mitte vor. Der RPO-Punkt liegt hinter dem Ausfallereignis und gibt die Menge an Datenverlusten an, die für eine Anwendung akzeptabel ist. Je mehr sich der Punkt vom Ausfallereignis weg bewegt, desto mehr nimmt der Datenverlust zu, und die potenziellen Kosten für das Unternehmen steigen.

Der RTO-Punkt liegt an der gegenüberliegenden Seite der Zeitachse. Der RTO-Punkt zeigt die Länge der Ausfallzeit an, die eine Anwendung tolerieren kann, bevor sich die Verluste für das Unternehmen akkumulieren. Mit anderen Worten: wie schnell Sie nach dem Ausfall dafür sorgen müssen, dass die Anwendung wieder betriebsbereit ist.

Wenn Informationen in dem betroffenen System von anderen Quellen wieder neu erstellt werden können, ist der Verlust von einigen Daten während eines Notfalls zwar unangenehm, stellt unter Umständen aber kein allzu großes Problem dar. Fehlende Rechnungen im Kreditorensystem beispielsweise lassen sich neu erstellen, indem man die Lieferanten bittet, Zahlungsaufforderungen erneut zu übermitteln. Wenn sich die Daten allerdings nicht so einfach rekonstruieren lassen, z. B. bei Online-Bestellungen von Kunden, kann sich der Verlust dieser Informationen direkt auf den Umsatz, die Anwenderproduktivität, den Ruf und die Marke Ihres Unternehmens sowie auf die Einhaltung von Vorschriften auswirken.

Ähnlich haben nicht kritische Unternehmenssysteme, z. B. Monatsberichte von einer Business Analytics-Anwendung, nicht die gleichen Auswirkungen auf das Unternehmen wie tagesgeschäftsrelevante Systeme, beispielsweise Point-of-Sale-Anwendungen. RTO misst die geschäftlichen Auswirkungen der Ausfallzeit einer Anwendung und hilft Ihnen zu ermitteln, welche Disaster Recovery-Tools für die Anwendung am besten geeignet sind. Regelmäßige Datensicherung mag für eine Business Analytics-Anwendung ausreichen, da POS-Systeme für das Unternehmen aber erfolgsentscheidender sind, erfordern diese eine Hochverfügbarkeitslösung.

Die Differenz zwischen den RPO- und RTO-Messdaten und den tatsächlichen Ergebnissen regulärer Disaster Recovery-Tests ist ein Indikator dafür, ob eine Lücke hinsichtlich der Verfügbarkeit von Anwendungen besteht. Dabei sollte man sich vergegenwärtigen, dass eine Verfügbarkeitslücke nicht immer darauf schließen lässt, dass für Business Continuity ein falscher Ansatz verfolgt wird. Unternehmen haben oft zahlreiche Disaster Recovery-Technologien von unterschiedlichen Anbietern im Einsatz, von denen viele Überschneidungen aufweisen, doppelte Funktionen enthalten und die Wiederherstellung noch komplizierter machen. Durch Tests lassen sich Probleme und Inkonsistenzen bei den vorhandenen Business Continuity-Technologien beseitigen. Zudem können sie auf die Bereiche aufmerksam machen, in denen durch eine Konsolidierung auf einem einzelnen Ansatz oder Lösungsanbieter die RTO-Werte verbessert werden können.

Wie sieht ein erfolgreicher HA-Ansatz aus?

Es ist kein Geheimnis, wie ein erfolgreiches HA-Konzept aussehen sollte: null Ausfallzeiten und Datenverluste bei Anwendungen. Ist dies aber für Mittelstandsunternehmen realistisch?

Die HA-Technologie ist kein so komplexer, „esoterischer" Ansatz für Business Continuity mehr wie früher. Große Unternehmen greifen bereits seit Jahren auf HA-Technologie zurück, um ihre bedeutendsten Geschäftsanwendungen zu schützen. Die Technologie wurde vielfach getestet und hat sich in der Praxis bewährt. So wird sie inzwischen weitgehend als Standardtool zur Vermeidung von Notfällen akzeptiert. Sie ist einfach, wiederholbar, messbar und automatisiert. Technologien wie Continuous Data Protection, Replikation und automatisches Failover und Failback sind nicht mehr wegzudenken.

Die Tatsache, dass die HA-Produkte inzwischen so ausgereift sind, hat sie nun auch für kleine und mittlere Unternehmen erschwinglich gemacht. Dies, in Kombination mit den niedrigeren Infrastrukturkosten – Breitband, Servervirtualisierung, mehrere Service Provider – und der deutlich verbesserten Anwenderfreundlichkeit, macht aus HA eine echte Business Continuity-Alternative für Unternehmen jeder Größe.

Ausfallzeiten und Datenverluste gehören für jedes Unternehmen, das sich auf IT stützt, zum Geschäftsrisiko dazu. Wie dieses Risiko mit der richtigen Technologie eliminiert werden kann, sollte bereits ganz früh bei Software-Entwicklung und Bereitstellungsprozess überlegt werden. Wenn Sie die von jeder Anwendung benötigte Schutzebene kennen, können Sie auch die entsprechenden Ressourcen zuweisen. Sobald eine Anwendung von den Anwendern im Unternehmen produktiv genutzt wird, müssen die zugehörigen RPO- und RTO-Werte klar identifiziert und die richtigen Business Continuity-Lösungen implementiert werden, um bei einem Ausfall die Wiederherstellung garantieren zu können.

Jeder Ansatz für Business Continuity, der nicht null Ausfallzeit und Datenverlust garantiert, hat nichts mit Hochverfügbarkeit zu tun. Es gibt eine Vielzahl an Lösungen, die versprechen, die Disaster Recovery zu verbessern. Wenn sie aber nicht die damit zusammenhängenden Risiken beseitigen, sind sie nicht HA.

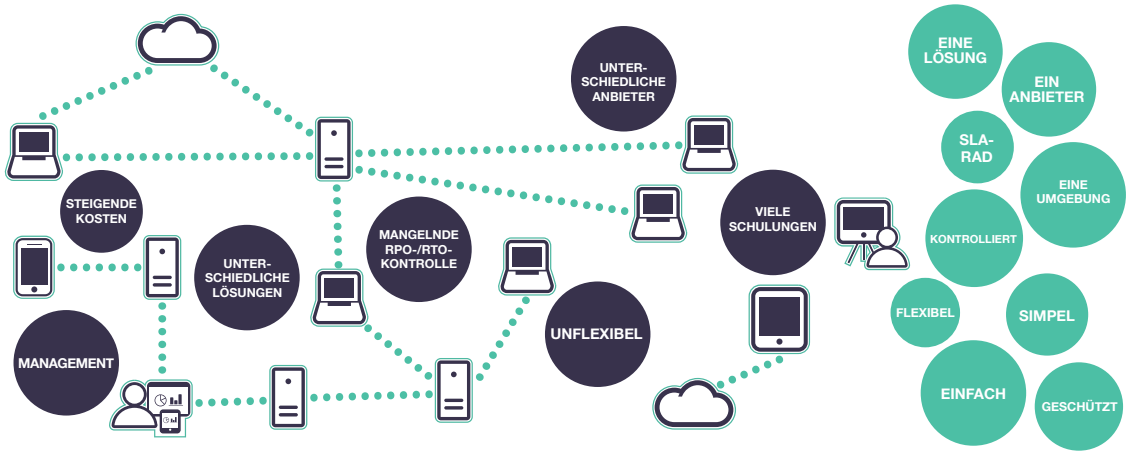

Abbildung 3: Eine einheitliche Business Continuity-Lösung

arcserve®

WHITE PAPER

Über Arcserve® Unified Data Protection

Seit über 20 Jahren bietet Arcserve Unternehmen in aller Welt Schutz mit null Ausfallzeit. Jetzt stellt Arcserve® Unified Data Protection (UDP) eine Komplettlösung für all Ihre Anforderungen im Bereich Datensicherung und Hochverfügbarkeit bereit. Mit einer zentralisierten Steuerung vereinheitlicht Arcserve® UDP den Schutz durch Backup, Snapshot, Replikation und Deduplikation für Ihre virtuellen und physischen Anwendungen sowie für On-Premise- und Cloud-basierte Anwendungen. Arcserve® UDP Assured Recovery™ bietet einen umfassenden Testprozess zur Vorbereitung auf den Notfall in Echtzeit, mit dem Sie Business Continuity-Pläne prüfen können, ohne dass Ihr Geschäftsbetrieb unterbrochen wird. Weitere Informationen zu Arcserve® Unified Data Protection (UDP) und unserer 30-Tage-Testversion finden Sie unter: http://arcserve.com/availability

Weitere Informationen zu Arcserve UDP **finden Sie unter** **arcserve.com/de**