arcserve®

WHITE PAPER

Komplexität fraß einfach mein Budget auf

Wie zusammengewürfelte Datensicherungs-lösungen in gemischten Umgebungen Chaos und erhöhte Kosten erzeugen

Alles Woche für Woche hören wir von unseren Channel-Partnern oder unseren gemeinsamen Kunden, welchen neuen Herausforderungen sie sich in puncto Datensicherung stellen müssen. Nicht, dass die Welt untergegangen wäre (was dann ja auch niemanden mehr kümmern würde) oder dass ihre Rechenzentren oder Bürogebäude in Schutt und Asche lägen. NEIN, in den meisten Fällen geht es einfach darum, wie komplex es werden kann, etwas zu tun, das jede Firma schon immer getan hat: furchtbar langweiliges Backup. Allerdings ist das vor dem Hintergrund des anhaltenden und scheinbar unkontrollierbaren Datenwachstums wahrlich keine leichte Aufgabe! Aber das ist lange noch nicht alles. Es geht nicht allein um die Datensicherung, sondern um die Fähigkeit zur Wiederherstellung - ganz egal unter welchen Umständen. Von einfacher Datenbeschädigung, Datenverlust aufgrund von Benutzerfehlern (Sie glauben ja nicht, was ich mit meinem Laptop alles anstellen kann) bis hin zu Migrationen und, ja, klar, ... auch ungeplante Ausfälle.

Wir haben ein Monster geschaffen

Was gegenwärtig zu einem gravierenden, wenn nicht sogar dem gravierendsten betrieblichen Problem wird, ist die Komplexität der Datensicherungs-Infrastruktur. Sie könnten jeden Moment zu jeder Zeit unterschiedlichste Backup-Schemata in Ihrer IT-Umgebung laufen lassen.
Vorsicht ist besser als Nachsicht? Falsch! Konsequenz ist besser als Nachsicht.
Und machen Sie es bitte nicht zu kompliziert. Nehmen wir zunächst eine kleine Selbsteinschätzung vor (eine Masche, damit Sie weiterlesen, aber spielen Sie einfach mit):

1. Zu viele Daten, und sie sind schwer zu sichern.
2. Ich nutze verschiedene Anbieter/Anwendungen/Prozesse.
3. Meine Anwendungen haben verschiedene Wiederherstellungsanforderungen.
4. Wir sind uns nicht einig, was eine unternehmenskritische Anwendung ist.
5. Ich kenne mein Recovery Point Objective nicht für alles.
6. Ich kenne mein Recovery Time Objective so irgendwie.

7. Bei uns laufen zu viele VMs und das macht mich wahnsinnig.
8. Ich habe kein Budget/Geld/Personal.
9. Niemand mag mich (aber lassen wir das ...).
10. Ich habe meinen Business Continuity-Plan eine Weile nicht getestet und ehrlich gesagt, ich möchte das auch lieber nicht.

Wenn Sie die meisten dieser Fragen mit Ja beantwortet haben, sind Sie ... normal! Aber nicht unbedingt aus dem Schneider. Die ständige Weiterentwicklung Ihrer Infrastruktur addiert gleichzeitig immer mehr Schichten aus Hardware, Software und unausgegorenen Datensicherung-„Lösungen" – ironischerweise vielleicht sogar eher „Probleme"?

Darüber hinaus haben die rasche Einführung und Ausbreitung von Servervirtualisierungs-technologien eine völlig neue Welt geschaffen, in der die effektive Sicherung von Daten unter ganz neuen Regeln läuft. Manche Anbieter möchten uns glauben machen, dass nur noch virtuelle Umgebungen von Bedeutung sind, weil sie die Infrastruktur betreiben ... falsch! Als Dienstleister im Bereich der Datensicherung muss man alles sichern, was von Bedeutung ist, virtuell und physisch. Nicht alles ist virtuell oder in der Cloud!

Die Cloud, dieses nebulöse und amorphe Gebilde, in der/über die Sie alles laufen lassen sollen, kann recht verschwommen sein. Und auf wessen Kosten? Wo passt sie in Ihre geplante Datensicherungsstrategie hinein, denn sie könnte tatsächlich eine Rolle spielen.

Und, amüsieren Sie sich?

Wir/Sie haben ein Monster erschaffen, bestehend aus Ebenen großartiger Datensicherungs-technologie. Grossartig ist sie, wenn man alles einzeln betrachtet, aber zusammengetragen ist es ein heilloses Durcheinander.
Sehen wir uns das einfache Beispiel eines aktuellen Kunden aus dem Mittelstand an:

1. Desktop-Backup: Online-Lösung (vielleicht zwei ... wir wissen es nicht genau)
2. Exchange-Backup: Festplatte und Band von Anbieter A
3. NAS-Backup: Legacy-Backup B (NDMP)
4. Oracle: Oracle Utilities mit Replikation
5. VMs: Anbieter C
6. Laptop-Backup: Die Benutzer sind angehalten, wichtige Dateien in einen „Box"-Service (Cloud) zu kopieren
7. Ein wenig Clustering auf Linux und Windows, aber nicht für alle
8. Ein Backup-Gerät pro Abteilung (am Standort)
9. Die Richtlinien zur Datenspeicherung sind je nach Abteilung/Benutzer unterschiedlich ... einige Bänder befinden sich aus Compliance-Gründen an einem anderen Standort ... so langsam bekommen Sie ein Bild, oder?

Trotz der Verwendung von APIs und eines gewissen Levels an Branchenstandards ist es unmöglich zu erwarten, dass man eine klare Vorstellung dessen bekommt, was wirklich passiert und, was noch wichtiger ist, wie aktuell die eigenen Daten jeweils sind.

Warum sollte mich das kümmern?

- **Katastrophen kann es immer geben.** Nehmen wir an, es kommt zu einem Ausfall, und Sie brauchen einen „guten" Zeitpunkt, um alles wieder zum Laufen zu bekommen. Wie bestimmen Sie diesen Zeitpunkt? Wie stellen Sie eine Datenkonsistenz in allen Bereichen sicher?
- **Geld.** Datensicherung in verteilten Umgebungen verursacht immense Kosten, es ist einfach ineffizent. Und womöglich gelingt es Ihnen nicht, die nötigen Fachkenntnisse, die für den Betrieb unterschiedlichster Datensicherungs-anwendungen erforderlich sind, immer auf dem neuesten Stand zu halten.
- **Transparenz.** Niemand interessiert sich für Backups, und Backups verursachen Kosten. Aber alle interessieren sich für Verfügbarkeit und Wiederherstellung von Daten und Anwendungen, Und dreimal dürfen Sie raten, wer am Ende schuld ist?
- **Hype.** Viele Spezialisten sind genau in einem Betriebssystem oder Bereich sehr gut, aber nur wenige können alle Ihre Anforderungen erfüllen.
- **Und noch einmal Geld.** Es ist Ihr Budget, und wenn Sie lieber einfach nur ausgeben als wirklich investieren, erwirtschaften Sie keine Erträge.

Das sollte schon ausreichen, um Ihnen schlaflose Nächte zu bescheren. Doch wäre das so, als würde man das sprichwörtliche halbleere Glas betrachten. Dahinter steckt nämlich mehr.

RPO, SLA und die Buchstabensuppe

Man könnte argumentieren, dass die Nutzung vieler verschiedener Technologien schlicht zum IT-Alltag dazugehört. Letzten Endes wird es eine Lösung geben, die sich herausbildet und der natürliche, technologische Entwicklungsprozess wird die besseren von den unbedeutenderen Datensicherungstechnologien aussortieren. In der Zwischenzeit reparieren Sie ein altes Auto, solange es noch fährt, aber damit wird es nicht besser. Ich weiß. Ist mir auch schon passiert, aber zum Glück nur bei einem Auto, nicht bei einer Backup-Infrastruktur.

Hier geht es um die Wichtigkeit von Anwendungen, die vor dem Hintergrund eines straffen Budgets gegen Anwendungs- bzw. Datenwiederherstellungs-SLAs festgelegt werden müssen. Klingt doch gut, oder? Aber was bedeutet das konkret, und wie erreichen Sie das?

Schritt 1: Ermitteln Sie wichtige Anwendungen

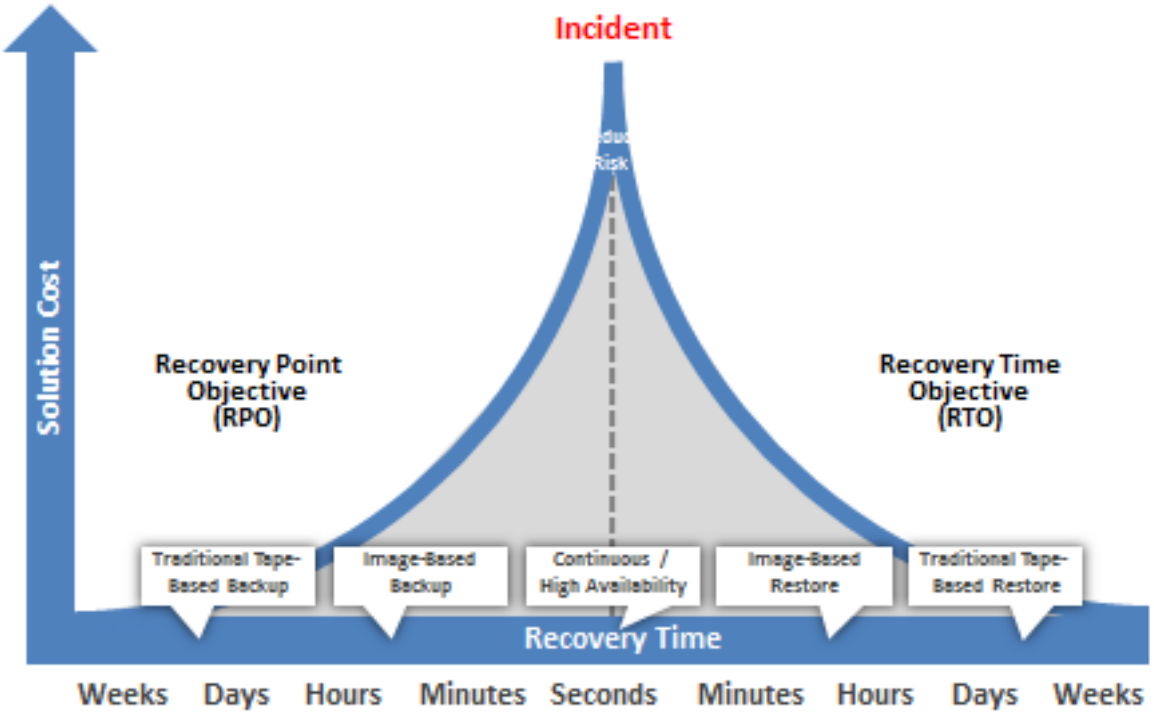
Achtung: Es kann sein, dass Sie dies zunächst mit Kollegen oder einer Ihnen nahestehenden Person in einer Gruppentherapie ausdiskutieren müssen. Was ich sagen will, ist: Nicht alle Anwendungen sind von vornherein gleichgewichtig ins Leben gerufen worden, und was die Priorität von Geschäftsanwendungen betrifft, herrscht eine gewisse Dynamik.

Anders ausgedrückt, alles befindet sich in ständigem Wandel, und jeder Anspruchsberechtigter konzentriert sich auf genau das, was ihm in dem Moment am wichtigsten ist.

Im Endeffekt ist das Entscheidende die Erfassung Ihrer fünf wichtigsten Anwendungen, ob auf virtuellen Servern gehostet oder nicht. Das sind wahrscheinlich die Anwendungen, die Ihr Unternehmen am Laufen halten. Somit unterscheidet sich hier das Investment in Datensicherung hinsichtlich Technologie, Personal, Prozess und Geld von dem in eine Back-Office-Anwendung (bei der das Recovery Point Objective viele Stunden oder Tage betragen kann, gegenüber Minuten oder Sekunden).

Geschäftskritische Anwendungen sind typischerweise voneinander abhängig und werden von anderen Anwendungen „gefüttert". Auch diese müssen gesichert werden. Und übrigens: Diese können sich auch auf Ihren herkömmlichen, physischen Servern befinden. Wenn Sie der Meinung sind, dass es ausreicht, nur „virtuellen" Kram zu sichern, wünsche ich Ihnen viel Glück!

Abb. 1: Das Verhältnis zwischen Recovery Point Objective und Recovery Time Objective und eine grundlegende Kartierung der Datensicherungstechnologien, die zum Erreichen der jeweiligen Vorgaben üblicherweise verwendet werden



Schritt 2: Bestimmen Sie Ihr RPO

Dies ist ein Zahlenspiel, bei dem Ihre Fähigkeit, Ihre wichtigsten Datensicherungszahlen zu identifizieren, den entscheidenden Unterschied macht. Leider finden Sie dies nicht in einem Glückskeks, auch wenn das überaus praktisch wäre. Sie wissen ja, dass die Geschäftsführung Zahlen liebt, und etwas, das nicht meßbar ist, können Sie auch nicht kontrollieren oder verbessern. Die Einschätzung von Datenverlust oder dem Risiko dafür läuft auf einige wenige Schlüsselwerte hinaus. Das Recovery Point Objective ist einer der wichtigsten. Welche Menge an Daten können Sie sich wirklich leisten zu verlieren?

Vor Kurzem las ich Data Protection for Virtual Data Centers von IT-Experte, Autor und Analyst Jason Buffington. Seine Definition gefiel mir gut, deshalb möchte ich Sie gern mit Ihnen teilen:

„Wenn Ihre Unternehmensziele besagen, dass Sie nicht mehr als zwei Stunden an Daten verlieren dürfen, dann ist das Ihr RPO – Ihr Ziel dafür, wie oft Sie einen zuverlässigen Wiederherstellungspunkt benötigen."

Diese Definition zeigt deutlich, warum die Kontrolle des Recovery Point Objective unser Anliegen sein sollte: Sie ist ein Unternehmensziel. Letztlich muss die Technologie (oder die Technologien),

die Sie zur Implementierung Ihrer RPO-Strategie einsetzen, alle geschäftskritischen Anwendungen und mehr abdecken, und das konsistent und vorhersagbar.

Schritt 3: Bestimmen Sie die RTO- Abhängigkeiten

Recovery Time Objective ist die Zeit, die es braucht, bis Ihre Systeme samt Daten, Anwendungen usw. wieder laufen. Es ist die Zeit, die es braucht, bis Sie wieder „auf den Beinen" sind.

Es ist ein Ziel, keine Garantie!

Ich wurde kürzlich in eine interessante Diskussion darüber verwickelt, warum ich persönlich glaube, dass das Recovery Time Objective eigentlich keine Frage der Technologie ist. Die Definition weiter oben unterstützt meine Ansicht. Natürlich gehe ich ein wenig an die Grenzen, wenn man berücksichtigt, dass viele Technologien ins Spiel kommen, wenn es darum geht, ein Unternehmen oder eine Abteilung wieder zum Laufen zu bekommen.
Wie beim Recovery Point Objective geht es auch beim Recovery Time Objective um Ziele, doch die Abhängigkeit von der Technologie reduziert sich hier aufgrund von ... Menschen. Es sind Menschen, Prozesse und Technologien im Spiel, wohingegen im anderen Fall nur die richtige Infrastruktur gestaltet und die richtigen Datensicherungstechnologien ausgewählt wurden.

Dieses Thema wurde von vielen äußerst intelligenten Leuten bis zum Abwinken behandelt, deshalb werde ich für Sie nur zusammenfassen, was der Unternehmer in mir denkt:

1. RTO ist ein Ziel – keine Realität.
2. Das Testen Ihres Business Continuity-/Disaster Recovery-Plans und die gleichzeitige Validierung Ihres RPO sind essenziell.
3. Das Testen Ihres derzeitigen RTO-Plans ist absolut entscheidend.
4. Der menschliche Faktor steht im Weg.
5. Technologien wie Virtualisierung haben den Prozess weiter verkompliziert.

Menschen neigen dazu, bei einer Katastrophe fluchtartig nach Hause zu stürzen ... deshalb sorgen Sie besser für einen Failover in eine Region, in der sicher gearbeitet wird. Überlegen Sie einfach, was Sie tun würden. Kann ich Ihnen jetzt ein wenig Hochverfügbarkeit verkaufen?

Virtualisierung hat mein Leben echt kompliziert gemacht

Server- und Desktop-Virtualisierung sind mittlerweile beherrschend in den meisten Organisationen, nicht nur in Wirtschaftsunternehmen. Während die Akzeptanz je nach Branche, Unternehmensgröße und Neigung zur Bereitstellung von IT-Technologien variieren kann, steht fest, dass die Zeiten der Virtualisierung für „Test/Dev" auf Serverseite lange vorbei sind. Auch die Desktop-Virtualisierung verbreitet sich zusehends, bietet sie der IT doch viele neue Möglichkeiten.

Niemand zweifelt daran, dass Servervirtualisierung zahlreiche Vorteile hat, Geld spart, mehr Flexibilität bietet etc. Außerdem kann sie in Disaster Recovery-Szenarien hilfreich sein und sogar einen gewissen Level an Hochverfügbarkeit bieten. Viele Analystenberichte bestätigen diese Punkte, und Kundenbeispiele gibt es im Überfluss.

Doch wenn es um Datensicherung geht, müssen wir uns einige wichtige Faktoren vor Augen

halten, die Ihre Gleichung ein ganzes Stück komplexer machen. Sie denken intuitiv sicher, dass Virtualisierung gut sei zur Datensicherung/Data Recovery, aber das ist sie keineswegs. Ich will damit nur sagen, dass sie einiges an Komplexität verschleiert, was Ihre Datensicherungs-Infrastruktur wiederum verkompliziert.
Und zwar:

1. Sie haben Anwendungen auf VMs laufen, und diese müssen gesichert werden. Sie haben also wichtige Anwendungen … Sie haben aber auch wichtige VMs.
2. Es besteht quasi ein Wildwuchs an VMs und Anwendungen (in gewaltigem Ausmaß).
3. Die geschäftsbedingten Messdaten für Recovery Point Objective und Recovery Time Objective gelten nach wie vor.
4. Anwendungs- und Datenwiederherstellung soll granular möglich sein.
5. Nicht alles wurde von physisch auf virtuell migriert.
6. Sie benötigen echte Fachkenntnisse, um die Umgebung bereitzustellen und zu verwalten.
7. Die physikalischen Komponenten, die die Virtualisierung unterstützen, sind nicht immun gegen Ausfälle … im Gegenteil. Verlieren Sie ein System, können Sie dutzende virtueller Maschinen verlieren: Betriebssystem, Anwendungen und Benutzerzugriff. Sie könnten also möglicherweise sogar mehr auf einmal „verlieren".
8. Sie müssen den Speicherbedarf optimieren, den alle Images von Betriebssystemen benötigen – schließlich ist Speicherplatz nicht billig!

Natürlich können und sollten Sie zwecks höherer Verfügbarkeit clustern. Sie haben nun also einige wichtige Cluster, auf denen wichtige VMs laufen, auf denen wichtige Anwendungen laufen … ich will es nur erwähnt haben.

Für all diese Anwendungen, darunter einige kritische (plus entsprechende Daten), benötigen Sie immer noch einen Disaster Recovery-Standort – also muss alles repliziert werden, falls Ihr primärer Standort ggfls. nicht verfügbar ist. Und erschwerend kommt hinzu …

Greifen Sie auf mehr als eine Virtualisierungstechnologie zurück? VMware? Hyper-V? XenServer? RedHat KVM? Sicherungstechniken sind nicht gleich Sicherungstechniken. Tatsächlich gibt es da ziemliche Unterschiede.

Sie haben immer noch einige physische Server, die Sie entweder nicht migriert haben oder nicht migrieren wollen, und dann haben wir da noch die Cloud-Sache. Einige Daten und VMs sind in der Cloud, was die Planung betrieblicher Wiederherstellung erschwert. Wie gesagt, nicht unbedingt eine schlechte Methode, aber sie bringt mehr Komplexität.

Vergessen Sie nicht, dass Sie im Fall von logischer Datenbeschädigung (Datenintegrität/-konsistenz) immer noch punktuelle Backups brauchen, also wie differenziert ist Ihr Backup? Gibt es Hierarchien? Wie integrieren Sie neue VMs in Ihr Schema? Wer entscheidet?

Ich will darauf hinaus, dass es beim Einsatz der Virtualisierung zu deutlich mehr Komplexität im Hinblick auf Datensicherung kommt. Das ist nicht unbedingt schlecht, doch Sie müssen es verstehen und planen. Sonst verlieren Sie die Kontrolle. Die größere Frage ist die, welche Art Datensicherungs-Infrastruktur Sie benötigen, um diese Komplexität zu vereinfachen und dennoch Ihre Service Level Agreements zu erfüllen. Zusammengewürfelte Lösungen für die Datensicherung sind nicht die Antwort, da sie die Komplexität nur verstärken.

Um die Kontrolle über ein virtualisiertes Rechenzentrum aufrechtzuerhalten, müssen Administratoren die Planung und Durchführung von Datensicherung aus einer ganzheitlichen Betrachtung heraus angehen.
Unterm Strich bedeutet das, dass vorhandene Richtlinien überprüft und angepasst werden müssen, um wahrscheinlich eine hybride Infrastruktur aus physischer , virtueller und Cloud-Umgebung zu sichern.

Wo geht das Geld hin?

Jetzt, da ich Sie an Dinge erinnert habe, die Sie bereits wussten, womöglich aber so lange ignorieren wollten, bis sie wirklich akut sind (was wahrscheinlich zu spät wäre), sollten wir über das deprimierende Thema „Wovon es bei IT-Budgets gegenwärtig nicht genug gibt" sprechen: Budget.

Wenn Sie sich ansehen, wie komplex heute Ihre Datensicherungs-Infrastruktur ist, könnte es sinnvoll sein, eine simple Einstufung der Kosten vorzunehmen, die Ihre Ressourcen, Ihre Zeit, Ihr Maintenance-Budget und vor allem Ihre Fähigkeit, Service Level Agreements einzuhalten, verschlingen. Also das, wofür Sie bezahlt werden.

Es folgt meine kurze Checkliste der Bereiche, (meine persönlichen Kommentare inklusive!)

Sie erhebt keinen Anspruch auf Vollständigkeit, sondern ist eher als Ausgangspunkt für eine weiterführende Diskussion gedacht. Einige dieser Kosten sind direkte Kosten, andere hingegen indirekte Kosten. (Ich bin kein Wirtschaftsprüfer, das wird also keine wissenschaftlich Abhandlung dazu.) Zudem sind viele dieser Kosten miteinander verknüpft und haben einen Einfluss auf Sie oder auf Ihre Datensicherungsorganisation. Wenn Sie also Ihre Gesamtbetriebskosten betrachten, berücksichtigen Sie bitte diese Faktoren:

1. Administratoren/Personal - Sie leisten gute Arbeit! Aber Sie benötigen Tools, durch die Sie mit weniger Arbeit mehr erreichen können, und auch Sie müssen mal ausspannen.
2. Schulungen – haben Sie wirklich einen Kurs besucht? Na gut. Aber im Ernst: Viele Kosten stehen in direktem Zusammenhang mit Technologiekomplexität bzw. fehlender Schulung.
3. Lizenzen – immer ein heikles Thema. Fragen Sie mal Ihren Einkauf.
4. Bandbreite/Netzwerk: ziemlich wichtig, wenn Sie sich die Menge an Daten ansehen, die Sie hin und her kopieren, vor allem über große Entfernungen. Das kann alles hinfällig machen , wenn es um Service Level Agreements mit einem Recovery Point Objective von null geht (Failover; Replikation).
5. Speichermedium und- platz (Band, Festplatte, Appliances): Tolle Sache, aber Sie müssen ein Gleichgewicht herstellen zwischen Performance, Kapazitäten, Kosten, Zukunftsfähigkeit ... Ein Zuviel kann sich hier rächen.
6. Energie: Wenn Sie sie nicht unbedingt durch Fahrradfahren selbst erzeugen möchten, ist das ein wichtiger Faktor in der Rechnung.
7. Einhaltung von Vorschriften: Personal, Prozesse, Audits, Anwälte, zusätzliche Backups und entsprechende Medien ... auch an einem anderen Standort.

8. Unterbrechung des Unternehmensablaufs: Läuft auf die Frage nach dem Recovery Point Objective hinaus – wie viel kostet Sie ein Datenverlust? Er kann zu Umsatzeinbußen führen, die sich sowohl direkt als auch indirekt in der Rechnung finden.
9. Produktivitätsverlust: Passiert nur den anderen, oder?

Und ... Fehler bei der Einhaltung von Vorschriften: Geldstrafen, Gefängnis, Anwaltskosten und dann der obligatorische Brief an alle Ihre Kunden, in dem es heißt, dass ihre persönlichen Daten möglicherweise preisgegeben wurden, weil jemand das Backup-Band verloren hat. So sind Sie zwar in aller Munde.....aber tolles Marketing.

Schauen wir uns dies von einer anderen Seite an: Was sind die Risiken? Eine Gefahrenminderung ist entscheidend für das Unternehmen, und wenn wir uns auf IT-Risiken konzentrieren, gibt es einige Bereiche, deren Überprüfung durchaus lohnenswert ist.
Ein sehr guter Anfang ist es, sich Bedrohungen des Systems anzusehen, etwa Hardwarefehler, Netzwerkprobleme, Softwareprobleme, Datenbeschädigung, Störungen usw. Dann gibt es weitere Risikobereiche, etwa externe Bedrohungen durch Hacker oder Probleme mit der Energieversorgung. Aber es ist wichtig, auch Risiken einzubeziehen, die mit der zunehmenden wechselseitigen Abhängigkeit unserer Anwendungen zu tun haben (Stichwort „Wertschöpfungskette"). Wir alle wissen, zu was die Natur fähig ist, und dass sie eine nicht zu unterschätzende Quelle für Bedrohungen darstellt, insbesondere durch extreme Wetterereignisse als Folge der Erderwärmung.

Diese Bedrohungen sollten klassifiziert werden und können zur Entwicklung einer vollständigen Risikobewertung Ihrer Datensicherungs- oder IT-Infrastruktur genutzt werden. So ist die kombinierte Betrachtung von Kosten und Risiken der Schlüssel, vor allem im Zusammenhang mit Disaster Recovery-Planung, aber auch ganz allgemein zum Nutzen des Unternehmens.

Fazit

IT-Infrastrukturen befinden sich in ständigem Wandel, um an das Jahr für Jahr exponentielle Datenwachstum angepasst zu werden. Das hat direkte Auswirkungen auf Datensicherungs-Infrastrukturen, denn es hat sie mit der Zeit immer komplexer gemacht hat. Viele Lösungen sind aufgetaucht, um der Vielfalt an Plattformen, Anwendungen und Datensätzen gerecht zu werden .

Während Virtualisierung sich als großartige Technologie für mehr Produktivität und Flexibilität erwiesen hat, ist es wichtig, die versteckten Kosten der Virtualisierung und ihre Auswirkungen auf Datensicherungsstrategien zu verstehen, damit Sie auch weiterhin Ihre Service Level Agreements einhalten können ... und das Meiste aus Ihrem Budget herausholen. Es ist an der Zeit, das Monster, das wir erschaffen haben, zu zähmen!

Mehrfachlösungen in der Datensicherung sind nicht die passende Antwort, da sie das Chaos nur erhöhen und Ihre Fähigkeit, konsistente Service Level Agreements zu bieten, beeinträchtigen. Die Antwort besteht wahrscheinlich in einer ganzheitlicheren Sicht auf die Infrastruktur. Eine, die die Datensicherungsschemata vereinheitlicht, indem sie bei Ihren Geschäftsanforderungen ansetzt, und das mit einem tiefgreifenden Verständnis der Anwendungen und Daten, die es zu sichern gilt. Wie ein Branchen-Star es formulierte: Backup funktioniert nicht mehr1.

Lassen Sie uns das reparieren.

1 Gartner: „The Broken State of Backup" von Dave Russell

Der Autor

Christophe Bertrand ist Leiter des Produktmarketings für arcserve. Seine umfangreichen Erfahrungen im Software- und Hardwarebereich innerhalb der Storage-Branche beinhalten die Verantwortung für das Produktmarketing in Unternehmen wie Legato Systems (jetzt Teil von EMC), VERITAS (jetzt Teil von Symantec), Maxtor, Hitachi Data Systems und DataDirect Networks. Bertrand hat einen doppelten Bachelor in Betriebswirtschaftslehre und ist Alumnus der Middlesex University (MBA).

arcserve®

assured recovery™

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

CA Deutschland GmbH, Marienburgstr 35, 64297 Darmstadt, +49 6151 949 663 , AT +43 1 917797 939, CH +41 44 8047 849, germanychannel@ca.com www.arcserve.com/de