Retrospect

Planung für Disaster Recovery

Ein Best-Practice-Dokument für Retrospect-Partner

Aspekte der Katastrophenvorsorge

Eine 'Disaster Recovery' und deren Implikationen für ein Computer-System zu berücksichtigen (zum Beispiel dazu in der Lage zu sein, ein 'Bare Metal Restore' durchzuführen, nachdem es zu einem Ausfall der Festplatte gekommen ist), ist ein vergleichsweise enger Rahmen, wenn man über die Katastrophenvorsorge für ein ganzes Business nachdenkt, d.h. sicherstellt, dass ein Business wieder normal läuft, kurz nachdem es zu einem Feuer, einer Flut, einem Diebstahl oder einem anderen Umstand gekommen ist. Fragen a la “Wo werden die Mitarbeiter sich treffen und arbeiten”, und “Wie werden wir Computer zur Verfügung stellen, ohne darauf zu warten, dass uns ein Versicherungsunternehmen einen Scheck zusendet” stellen berechtigte Bedenken dar, wenn es darum geht, einen Plan zu entwickeln, um eine katastrophale Lage in den Griff zu bekommen.

Die Planung der Katastrophenvorsorge in Ihre Dienstleistungen integrieren

Katastrophenvorsorge ist tatsächlich ein so breites und komplexes Thema, dass ganze Unternehmen für das Angebot solcher Dienstleistungen errichtet worden sind. Obwohl die Darstellung der Aufgaben, die dazu erforderlich sind, um solchen Unternehmen nachzueifern, den Rahmen dieses Dokuments sprengt, ist eines klar: IT-Service-Provider befinden sich in der besten Position, um ihre Kunden dazu zu bringen, darüber nachzudenken, was für das Überleben ihrer Unternehmen getan werden muss, und um Dienstleistungen für die Sicherstellung laufender IT-Funktionen anzubieten.

Zumindest sollten Sie – auch wenn es nur darum geht, dass Sie sich und Ihr Business vor unerwartetem Datenverlust schützen, wenn Sie mit den Systemen von Kunden arbeiten- über ein umfassendes Backup und einen Wiederherstellungsplan für jeden Ihrer Kunden verfügen. Erheben Sie einen solchen Plan zur Pflicht, und führen Sie darin Folgendes im Detail auf:

- Erste Planung und Implementierung
- Tagesgeschäft (Ausführen von Backups und Wiederherstellungen, Überprüfen von E-Mail-Benachrichtigungen)
- Regelmäßige Wartung und Tests (Archivierung, Verifizieren von partiellen und kompletten Wiederherstellungen)
- Neubewertung, falls erforderlich (Systemkapazität, Leistung, Technologie, Methodik, usw.)

Die oben aufgeführten Aufgaben führen im Zeitablauf zu signifikanten Einnahmen aus Dienstleistungen, und etwa 70-90% eines Backups und Wiederherstellungsprozesses können von der Umgebung eines Kunden in die eines anderen dupliziert werden, was dies zu einem größtenteils wiederholbaren Prozess macht. Entscheiden Sie, was funktioniert, und sorgen Sie dann für den Erfolg Ihrer Kunden (sowie für Ihren eigenen!).

Best Practices für Backup- und Disaster-Recovery-Pläne

Erstellen und formalisieren Sie einen Plan

Wir empfehlen, dass Sie für jeden Ihrer Kunden einen Backup- und Wiederherstellungsplan formalisieren. Darin sollten Punkte wie Ihre Dienstleistungsvereinbarung mit Antwortzeiten

enthalten sein, die Sie einhalten können, sowie Ihre und deren Verantwortungsbereiche, Messgrößen für den Erfolg, und die Art der laufenden Dienstleistungen, die angeboten werden.

Offsite-Backup-Speicherung und Wiederherstellung

Lokale Backups stellen die erste Verteidigungslinie gegen Datenverlust dar, aber es ist entscheidend, zumindest eine Kopie der Unternehmensdaten sicher offsite zu speichern - vorzugsweise an einem Ort, der sich mehrere Meilen entfernt befindet. Hier sind ein paar Dinge, die bezüglich Offsite-Backups zu beachten sind:

- Für welche Daten muss ein Offsite-Backup durchgeführt werden? Können bestimmte Daten—wie z.B. Cache-Dateien—ausgeschlossen werden?
- Sollten die Daten verschlüsselt sein?
- Wo werden die Offsite-Daten gespeichert?
- Wie werden sie dorthin gelangen? (Optionen: Cloud-Backups, physischer Transport von Backup-Medien)
- Wer wird dafür verantwortlich sein, physische Medien an eine externe Location zu transportieren?
- Wann werden wir einen Zugang zu den physischen Medien haben, falls wir diesen benötigen?
- In welchem Zeitabstand wird die Offsite-Speicherung aktualisiert?
- Für welchen Zeitraum werden ältere Daten archiviert?

Erstellen Sie Ihre Systemwiederherstellungs-Toolbox

Jeder IT-Service-Provider sollte ein Arsenal von nützlichen Tools führen. Halten Sie zumindest die folgenden jederzeit bereit:

- Brennen Sie eine Retrospect-Notfall-Wiederherstellungs-Disc für Windows-Systeme.
    - Am besten ist die Lizenzierung mit dem Retrospect-Dissimilar-Hardware-Restore-Add-on (Add-on zur Wiederherstellung nicht identischer Hardware)
    - Beachten Sie spezifische Hardware-Anforderungen (wie RAID und Netzwerk-HBAs)
- Erstellen Sie eine bootbare Tools-Disk für OS X-Systeme.
    - Fügen Sie die Retrospect-Anwendung, Engine, und den Client mit ein
    - Fügen Sie favorisierte Mac-Hilfsprogramme hinzu (Disk Warrior, Tech Tool Pro, usw.)
- Falls Offsite-Backups auf Band gespeichert werden, stellen Sie sicher, dass Sie umgehend ein Laufwerk beschaffen können, um diese Bänder zu lesen, falls das wichtigste Band-Backup-Laufwerk aus irgendeinem Grund unbrauchbar geworden sein sollte.
- Stellen Sie sicher, dass Sie Zugang zu allen erforderlichen Passwörtern und Schlüsseln haben! Falls die Post-it™-Notiz, die Ihr Backup-Set-Passwort enthält, sich unter ihrem Keyboard befand, das gerade mit dem Rest des Büros in Flammen aufgegangen ist, haben Sie ein Problem, wenn Sie dieses Passwort nicht anderweitig sicher gespeichert haben!

Testen, testen, testen

Selbst gut durchdachte Disaster-Recovery-Pläne müssen getestet werden. Es gibt kaum etwas, das mehr weh tut, als festzustellen, dass die Dinge nicht wie erwartet laufen, wenn Sie eine kritische

Wiederherstellung laufen lassen. Das Design von Retrospect beinhaltet eine einzigartige Datenverifizierungsmethode, die tatsächlich die gleichen Abläufe verwendet wie in den Fällen, in denen eine Wiederherstellung läuft. Das ist klasse, wenn es darum geht, sicherzustellen, dass die Backup-Daten lesbar sind und exakt mit den ursprünglichen Daten übereinstimmen, aber der beste Weg, um das Vertrauen in das System aufrechtzuerhalten, besteht stets darin, eine echte Wiederherstellung zu testen.

Erstellen Sie einen Plan, um Wiederherstellungen mindestens vierteljährlich für jeden Ihrer Kunden zu testen. Wenn Sie derartige Testvorgänge durchführen, gibt es mehrere Tests, die nicht übersehen werden sollten:

- Suchen Sie eine Datei und führen Sie die Wiederherstellung durch
- Stellen Sie einen Ordner in seiner früheren Version wieder her
- Stellen Sie einen gesamten Datenträger wieder her und sorgen Sie dafür, dass er bootet, die Anwendungen wie erwartet laufen usw.
- Überprüfen Sie kritische Business-Anwendungsfunktionen (Rechnungswesen, E-Mail, usw.) im Anschluss an eine Wiederherstellung
- Führen Sie eine Wiederherstellung von Offsite-Backups durch

Neben der Sicherstellung der Zuverlässigkeit des Backup-Systems sorgt das Testen von Wiederherstellungen dafür, dass Sie in regelmäßigen Abständen vor Ihre Kunden treten und erhält *deren Vertrauen in Sie* aufrecht. Es ist ein Win-Win-Prozess.

Starten Sie umgehend; perfektionieren Sie es im Zeitablauf

Was auch immer Sie tun, warten Sie nicht damit, Ihren Kunden Offsite-Backups zu bieten, bis Sie einen perfekten Plan erarbeitet haben. Lagern Sie etwas JETZT aus. Es liegt in der Natur der Dinge, dass sowohl Naturkatastrophen als auch solche, die vom Menschen hervorgerufen werden, nur schwer vorherzusagen oder zu verhindern sind. Es ist am besten, wenn Sie zumindest eine Kopie der Backups Ihrer Kunden umgehend sicher offsite speichern. Danach können Sie sich im Laufe der Zeit ein System überlegen und implementieren, dass ein Dienstleistungsniveau bietet, welches den Umständen und Bedürfnissen Ihrer Kunden am besten gerecht wird.

* Retrospect, Inc. duldet nicht, dass Passwörter auf eine nicht-sichere bzw. nicht-geschützte Art und Weise gespeichert werden.