Acronis®
COMPUTE WITH CONFIDENCE
WWW.ACRONIS.DE

Acronis® Guide für Backup und Recovery in kleinen und mittleren Unternehmen

Freier Journalist – Alan Stevens

Sie sind der Meinung, dass harte Arbeit sich auf jeden Fall lohnt? Das trifft leider nicht zu, wenn Ihre IT versagt. In diesem Fall kann die ganze Arbeit, Zeit und Mühe, die Sie in den Aufbau und die Führung Ihres kleinen Unternehmens investiert haben, völlig umsonst gewesen sein.

Dabei spielt es keine Rolle, wodurch der Systemausfall verursacht wird. Dies kann beispielsweise ein Virus, ein Software-Fehler oder ein Hardware-Absturz sein. Das Ergebnis ist immer gleich. Sie können Stunden oder sogar Tage nicht auf Ihre IT zugreifen und verlieren eventuell viel Arbeit. Verfügen Sie jedoch über ein aktuelles Backup und einen wohlüberlegten Plan für die Wiederherstellung, sind die Folgen für die Finanzen und die Produktivität Ihres Unternehmens nicht ganz so schlimm.

Selbstverständlich kostet es ein wenig Zeit und Mühe, eine entsprechende Backup- und Recovery-Strategie auszuarbeiten. Möglicherweise hat diese Aufgabe für Sie keine besondere Priorität, insbesondere dann, wenn Sie mit der Entwicklung und Führung Ihres Unternehmens voll ausgelastet sind. Acronis ist sich dieses Dilemmas bewusst und unterstützt Sie deshalb mit einem übersichtlichen und informativen Guide, damit Sie herausfinden können, wie sich ein Systemausfall für Ihr Unternehmen konkret auswirken würde.

Welche Bereiche müssen unbedingt geschützt werden?

Zuallererst sollten Sie sich fragen, welche Bereiche Ihres Unternehmens besonders geschützt werden müssen. Dabei ist es noch wichtiger zu wissen, wie schnell diese Bereiche nach einem Ausfall wieder betriebsbereit sein müssen. Sie können sich vielleicht noch damit arrangieren, dass Ihr Lohnabrechnungssystem ein paar Tage ausfällt. Was passiert aber, wenn Sie mehrere Stunden keine Aufträge mehr eingeben und keine Rechnungen mehr stellen können? Dies hätte einen unmittelbaren negativen Einfluss auf die Finanzkraft Ihres Unternehmens.

Ebenso müssen Sie entscheiden, welche Systeme innerhalb jeder Unternehmensfunktion vorzugsweise geschützt werden und höchste Priorität haben sollen, um den größten Nutzen zu erzielen. Treffen Sie die Entscheidung, sämtliche Personaldaten zu sichern oder möchten Sie Zeit sparen, indem Sie ausschließlich Dokumente und Daten schützen? Dies setzt allerdings voraus, dass Sie Windows und alle anderen Anwendungen immer neu installieren können. Des Weiteren sollten Sie sich fragen, ob ein Backup eines einzelnen PCs überhaupt sinnvoll ist, wenn die Anwender ihre Dateien auf einem gemeinsamen Server oder einem anderen Storage-Medium speichern (und Sie Backups von diesen Servern erstellen).

Nur Sie können entscheiden, welche Lösung für Ihr Unternehmen am besten ist. Generell sind zu viele Backups besser als zu wenige. Denn aus den verschiedensten Gründen speichern nicht alle Anwender ihre Arbeit auf dem Server. Viele Mitarbeiter verfügen über lokale Kopien, um offline arbeiten zu können. Dies trifft insbesondere auf Mitarbeiter zu, die häufig geschäftlich unterwegs sind. Andere Anwender wiederum sichern ihre Dateien lokal, weil ihnen die Serverleistung nicht ausreicht oder sie dem Server einfach nicht vertrauen. Da es sich hier logischerweise immer um die aktuellsten Dateien handelt, ist die Wiederherstellung im Falle eines Verlusts besonders kritisch. Diese Problematik sollten Sie auf keinen Fall unterschätzen, da schätzungsweise 60 % der Unternehmensdaten auf Workstations gespeichert sind.

Berücksichtigt werden sollten des Weiteren die für die Wiederherstellung der Daten benötigte Wiederanlaufzeit, die als Recovery Time Objective (RTO) bezeichnet wird. Wenn beispielsweise Ihr Web-, E-Mail- oder Hauptdatenbankserver ausfällt, ist es für Ihr Unternehmen lebenswichtig, dass das System innerhalb von Minuten wieder läuft. Es dauert viel zu lange, wenn

Wie kostspielig sind Ausfallzeiten wirklich

Die durch Ausfallzeiten verursachten Kosten lassen sich nur sehr schwer genau berechnen. Fest steht aber, dass sie auf jeden Fall zu hoch sind und vor allem in wirtschaftlich unsicheren Zeiten gering gehalten werden sollten. Sehen Sie sich hierzu die folgenden drei Beispiele an:

- ***Der Web-Server fällt vielleicht eine Stunde aus** – Aufträge gehen verloren, Kunden schauen sich Websites von Wettbewerbern an und der Ruf Ihres Unternehmens ist ruiniert.*
- ***Stürzt der Windows Exchange Server ab, verschwinden wichtige E-Mail-Datensätze** – es dauert Tage, alte Papierdokumente zu finden und neu einzugeben, die Mailing-Listen neu zu generieren und den Status vor dem Absturz wiederherzustellen. Kunden und Partner sind verärgert und Mitarbeiter frustriert, weil sie nicht effektiv arbeiten können.*
- ***In den Kassensystemen Ihrer Geschäfte hat sich ein Trojaner eingeschlichen und die Software muss neu installiert werden** – die Supportmitarbeiter müssen Überstunden leisten, um das Problem zu lösen, und vernachlässigen dabei andere Projekte. Die Mitarbeiter sind gezwungen manuell zu arbeiten und die Kundenloyalität wird extrem strapaziert.*

Ein Backup ist keineswegs nur die Wiederherstellung von Daten, die versehentlich im Papierkorb gelandet sind. Es geht vielmehr um die Wiederherstellung Ihrer Systeme nach einem beispielsweise durch einen Virus, einen Software-Fehler oder einen Hardware-Absturz verursachten Ausfall, um die Auswirkungen für Ihr Unternehmen schnell zu minimieren.

Image-basiertes Backup

Normalerweise werden bei einem Backup alle Dokumente und Dateien einzeln vom Server oder PC auf das Backup-Medium kopiert. Dies hängt jedoch vom jeweiligen Host-Dateisystem ab. Die Bearbeitung dieser Dateien, auf die auch andere Anwendungen zugreifen, erfordert eine spezielle Software und kann sehr zeitintensiv sein.

Die Disk Imaging-Technologie wurde ursprünglich zum „Klonen" von PCs entwickelt und vermeidet dieses Problem durch die Erstellung eines Snapshots oder „Images" von einer Festplatte. Das auf Blockebene erstellte Image ist unabhängig von der Dateiebene und kann daher viel schneller als die herkömmliche Datei auf Dateiebene sein. Da offene Dateien kein Problem mehr darstellen, ist auch das Disaster Recovery viel einfacher.

Image-basierte Backups sind sehr beliebt und bieten einen optimalen Schutz. Sie bleiben weiterhin völlig flexibel und können zum Beispiel auch nur eine gelöschte Datei wiederherstellen.

Sie erst das Betriebssystem und das Backup-Programm laden müssen, bevor Sie überhaupt die Wiederherstellung starten können. Daher ist es ratsam, den gesamten Server zu sichern, um die Wiederherstellung jederzeit abrufen zu können.

Die Wiederherstellung einer einzelnen Workstation wird vielleicht als nicht so wichtig angesehen. Es ist jedoch erstaunlich, wie lange ihre Wiederherstellung dauert, wenn kein entsprechendes Backup für sie vorliegt. Allein die Neuinstallation von Windows kann eine Stunde oder länger dauern. Außerdem benötigen Sie Zeit, die Installations-CDs für Office und weitere Anwendungen zu finden, die Lizenzschlüssel zu suchen, die Kennwörter für die verschiedenen Accounts einzugeben und die entsprechenden Einstellungen zu ändern. Sind die Techniker Stunden oder sogar Tage damit beschäftigt, abgestürzte PCs wieder ans Laufen zu bekommen, wirkt sich dies sehr nachteilig aus und kann genauso kostspielig wie der Ausfall eines Servers sein. Ohne Zugriff auf seinen PC kann der betroffene Mitarbeiter auch mehrere Tage nicht produktiv arbeiten.

Wie häufig sollten Backups erstellt werden?

Sie sollten nicht nur darüber nachdenken, was Sie sichern möchten, sondern auch festlegen, wie oft Sie ein Backup erstellen. Über die Jahre hat sich die Durchführung eines täglichen Backups bewährt, normalerweise nachts, da dann nur selten auf die Systeme zugegriffen wird. Auf diese Weise entstehen keine Konflikte mit geöffneten Dateien und anderen laufenden Prozessen. Dieser Ansatz ist jedoch oft nicht mehr anwendbar, da die heutigen IT-Systeme auf längere Arbeitszeiten und mehr Leistung ausgelegt sind. Darüber hinaus können Backups, die über Nacht erstellt wurden, 24 Stunden zu alt sein. Das würde bedeuten, dass Sie zum Beispiel wegen einer simplen Spannungsschwankung einen ganzen Tag Arbeit verlieren könnten.

Das heißt aber nicht, dass nachts jetzt überhaupt keine Backups mehr laufen sollten. Schließlich bieten sie einen grundsätzlichen Schutz, der sich auf jeden Fall bezahlt macht. Moderne Backup-Anwendungen basieren jedoch auf Technologien, die auch mehrmalige Backups zulassen und sowohl die Leistung als auch den für das Ablegen der Kopien erforderlichen Speicherbedarf minimal beeinflussen.

Dank Disk Imaging und anderen Technologien können Sie jetzt zum Beispiel stündlich Backups erstellen.

Womit sollten Sie beginnen?

Es gibt keine genauen und festen Regeln. Aber im Allgemeinen sollten Sie bei der Ausarbeitung einer Backup-Strategie für ein kleines Unternehmen folgende Punkte berücksichtigen:

Shared resources (Geteilte Ressourcen) – Beginnen Sie mit den Servern und weiteren geteilten Ressourcen, wie zum Beispiel Storage-Geräte. Selbst wenn sie für das Unternehmen nicht lebensnotwendig sind, kann eine Ausfallzeit doch zahlreiche Anwender betreffen. Deshalb ist es im Falle eines Problems wichtig, dass die Server und Anwendungen schnell wieder laufen. Und machen Sie keine halben Sachen. Sofern möglich, erstellen Sie ein Backup von dem gesamten Server oder Gerät. Bei der Wiederherstellung erspart Ihnen dies viel wertvolle Zeit.

Netzwerk-Desktops – Die Verwaltung des Backup-Prozesses ist wesentlich einfacher, wenn Anwender ihre Dateien auf gemeinsamen Storage-Medien speichern. Versuchen Sie darüber hinaus Desktop-PCs vorzugsweise mithilfe von zentral und automatisch verwalteten Tools in das Backup-System einzubinden. Überlassen Sie dies nicht den Anwendern selbst, da diese es dann meistens nicht tun.

Es muss nicht unbedingt alles gesichert werden. Daten lassen sich aber wesentlich schneller wiederherstellen, wenn Sie alles gesichert haben. Entscheiden Sie sich für ein selektives Backup, sollten Sie Ihre E-Mails besonders schützen. Laden Anwender ihre E-Mails in einen lokalen Nachrichtenspeicher auf der Festplatte ihres PCs herunter, ist dies extrem wichtig.

Mobile Desktops – Für Anwender, die viel Zeit außerhalb ihres Büros arbeiten, ist es nicht immer praktisch alles an einem gemeinsamen Speicherort abzulegen. In diesem Fall empfiehlt es sich, das Backup und Disaster Recovery offline durchzuführen. Hierbei müssen zwei Anforderungen erfüllt werden: Der Prozess sollte für den Notebook-Nutzer einfach zu handhaben sein (ideal wäre, wenn er nichts damit zu tun hätte oder besser noch nicht einmal etwas davon merken würde). Außerdem sollten die zu verwendenden Datenträger ausgewählt werden. Auf diesen Punkt wird später näher eingegangen.

Virtuelle Ressourcen – Das Backup von virtuellen Desktops und Servern dürfen Sie nicht vernachlässigen. Die Durchführung eines Backups eines physikalischen Host Servers ist schon mal ein guter Start. Für einen umfassenden Schutz und für die Wiederherstellung einzelner virtueller Maschinen benötigen Sie jedoch spezielle, für virtuelle Technologien konzipierte Tools. Ansonsten sind die Überlegungen ähnlich wie bei den „realen" Ressourcen. Sie sollten am besten alles sichern, um im Schadensfall den Status schnell und komfortabel wiederherstellen zu können.

Hosted Ressourcen – Einer der Vorteile eines hosted Services, wie beispielsweise Google Apps oder einem Hosted Exchange Service, besteht darin, dass alle Backups für Sie ausgeführt werden. Sie sollten sich aber niemals komplett darauf verlassen. Schauen Sie sich die Vertragsbedingungen sorgfältig an, damit Sie keine Überraschungen erleben. In Bezug auf die Wiederherstellung ist dies besonders wichtig, da die „besten Bemühungen" des Dienstleistungsanbieters möglicherweise nicht mit Ihren Erwartungen von einer zeitnahen Wiederherstellung übereinstimmen.

Welche Medien eignen sich zur Speicherung der Backups?

Sie wissen jetzt, welche Systeme vorrangig gesichert werden müssen und bis zu welcher Ebene Sie sichern möchten. Als nächstes sollten Sie die verschiedenen Lösungen auf dem Markt vergleichen und herausfinden, welche Ihren Anforderungen am besten entspricht. Zahlreiche unterschiedliche Technologien und Produkte stehen zur Auswahl und haben jeweils spezifische Vorteile, die im Folgenden näher erläutert werden. Beachten Sie jedoch, dass ein einziges Produkt möglicherweise nicht die Antwort auf alles sein kann. Eventuell benötigen Sie für Ihren Ansatz eine Kombination aus allen angebotenen Lösungen.

Für Backup-Medien trifft dies ganz besonders zu. Das Band ist schon lange nicht mehr die einzige erschwingliche Option. Es ist zwar immer noch beliebt, wird aber zunehmend von der CD abgelöst. Die CD, die die auf ihr gespeicherten Daten direkt statt linear abgreift, ist nicht nur schneller, sondern auch kostengünstiger, da keine komplexen Bandbibliotheken zum Schutz moderner Server und Workstations mehr notwendig sind.

Neben vielen unterschiedlichen CDs gibt es weitere Backup-Medien, deren Vor- und Nachteile in der folgenden Tabelle aufgelistet werden.

Sie sollten das Risiko am besten streuen, indem Sie Backups auf mehreren Medien speichern. Für kurzfristige Sicherungen empfehlen sich lokale Backups oder Backups auf einer Festplatte im Netzwerk. Für eine langfristige Archivierung dagegen sollten Sie auf Tapes oder optische Medien (CD/DVD) zurück greifen. Sie können Backups gleichzeitig auf zwei Medien, beispielsweise im Netzwerk und im Online-Speicher, durchführen, um noch sicherer und flexibler zu sein.

Im Notfall müssen Sie unbedingt auf Ihre Backups zugreifen können. Legen Sie Ihre Backup-Tapes oder CDs/DVDs deshalb nicht einfach in einen Schrank und lassen Sie diese auch nicht während der Ausführung des Backup-Programms im Server. Sorgen Sie dafür, dass die Datenträger entsprechend gekennzeichnet und an einem sicheren Ort aufbewahrt werden. Nur so können Sie diese immer schnell wieder finden. Sofern möglich, bewahren Sie ein paar Kopien auch an einem anderen Ort außerhalb des Unternehmens auf. Wenn Sie ein Storage-Gerät sichern, sollten Sie von diesem auch ein Backup auf zweiter Ebene durchführen und an einem anderen Ort aufbewahren.

Datendeduplizierung

Bei der Durchführung von Backups sind Kompromisse unvermeidlich. Wenn Sie alles speichern, haben Sie bald nicht mehr genug Speicherplatz zur Verfügung. Gehen Sie dagegen selektiv vor, können wiederum entscheidende Daten fehlen.

Eine Komprimierung ist zwar hilfreich, kann aber nicht mit den Vorteilen einer Datendeduplizierung mithalten. Mit dieser innovativen Technologie werden Ihre Daten immer nur einmal kopiert, ganz gleich, wie oft sie vorkommen. Die meisten der zum Beispiel für Windows erforderlichen Dateien sind auf jedem PC die gleichen. Deshalb ist es überhaupt nicht sinnvoll, ein Backup von jeder einzelnen Kopie anzulegen. Viel besser legt die Backup-Software nur eine Kopie von jeder Datei an und verweist in nachfolgenden Backups auf diesen Ort.

Immer mehr Backup-Lösungen unterstützen jetzt die Deduplizierung auf Dateiebene sowie in einigen Fällen auf Blockebene. Storage-Kosten sind dadurch geringer und Backups lassen sich schneller durchführen. Bei Bedarf können sowohl einzelne Dateien oder komplette Systeme wiederhergestellt werden.

Tabelle: Backup- und Recovery-Medien im Vergleich

Speicher-medium	Positiv	Negativ	Geeignet für	Nicht geeignet für
Tape	Tape Cartridges sind relativ günstig. Sie können nicht einfach überschrieben werden.	Langsamer linearer Zugriff. Automatisierte Band-bibliotheken können sehr kostspielig sein.	Automatisches Backup großer Datenserver. Langfristige Archivierung.	Backup einzelner Workstations und PCs. Schnelle Wiederherstellung.
CD/DVD	Direkter Zugriff. Erschwinglich. Fast jeder PC verfügt über einen CD/ DVD-Brenner.	Begrenzte Speicher-kapazität, d. h. zum Speichern großer. Datenmengen benöti-gen Sie mehrere CDs/ DVDs.	Offline-Backup einzelner PCs und Notebooks. Bootfähige Wiederherstellungs-CDs/DVDs. Langfristige Archivierung.	Server-Backup.
Memory Card/Stick	Einfaches Handhaben und Speichern. Abgesehen von USB- und Memory Card-Anschlüssen ist keine spezielle Hardware erforderlich.	Leicht überschreibbar, sehr fehleranfällig und eingeschränkte Speicherkapazität.	Kurzfristiges Backup wichtiger Dokumente und Daten.	Regelmäßiges Backup von Servern oder PCs/ Notebooks.
Externe Festplatte	Schneller, direkter Zugriff. Hohe Speicher-kapazität. Geringe Kosten.	Leicht überschreibbar. Schlecht zu transportieren.	Automatisches Backup von Server und Network Workstation.	Backup großer Datenserver. Langfristige Archivierung.
Netzwerk-Speicher	Schneller, direkter Zugriff. Hohe Speicher-kapazität. Geringe Kosten.	Leicht überschreibbar.	Automatisches Backup von Server und Network Workstation.	Langfristige Archivierung.
Online-Speicher	Externe Verwaltung.	Backup-/Recovery-Leistung abhängig vom Breitband-Internetzugang.	Backup mobiler Notebooks.	Backup/Recovery von Servern.

Was ist als nächstes zu tun?

Als nächstes müssen Sie entscheiden, mit welchen Backup-Produkten Sie arbeiten möchten. Wegen der sehr großen Auswahl ist es auf jeden Fall sinnvoll, sich Demonstrationen oder noch besser Testversionen anzusehen. So können Sie sich am besten von ihrer Benutzerfreundlichkeit überzeugen und nachprüfen, ob sie den von Ihnen gewünschten Anforderungen an Sicherheit und Wiederanlaufzeiten (RTO) entsprechen.

Jetzt müssen Sie nur noch die von Ihnen gewählten Produkte installieren und anwenden. Wir haben noch eine paar letzte Tipps für Sie. Testen Sie zuerst Ihre Backups, um sicherzugehen, dass sie auch wirklich funktionieren. Die Erstellung eines Backups bedeutet nicht automatisch, dass die Daten nach einem Ausfall auf jeden Fall wiederhergestellt werden können. So ist es nicht ungewöhnlich, dass Unternehmen gewissenhaft ihre täglichen Backups erstellt haben, um dann beim Versuch der Wiederherstellung feststellen zu müssen, dass diese entweder unbrauchbar oder noch schlimmer komplett leer sind.

Außerdem sollten Sie Ihre Backup und Recovery-Strategie und alle damit verbundenen Prozeduren dokumentieren. Verlassen Sie sich nicht auf einzelne Personen, die Bescheid wissen. Kommt es zu einem Ausfall, ist die für die Backups verantwortliche Person grundsätzlich krank oder in Urlaub. Schreiben Sie detailliert auf, wie Backups durchzuführen sind und welche Medien dafür genutzt werden sollen. Legen Sie Namenskonventionen, Speichermedien, Speicherort usw. fest. Führen Sie die gleichen Schritte für die Wiederherstellung durch und sorgen Sie dafür, dass diese auch von den zuständigen Personen gelesen werden. Verteilen Sie die Informationen an möglichst viele Mitarbeiter. Stellen Sie die Anweisungen sowohl auf Papier als auch elektronisch zur Verfügung. Es reicht nicht, diese einfach nur in einem Ordner auf dem Server abzulegen. Zum einen schaut dort niemand nach und zum anderen könnte der Server schließlich abstürzen – genau aus diesem Grund haben Sie das Backup ja überhaupt erst erstellt...

Über Acronis®

Acronis ist ein führender Hersteller hoch entwickelter und skalierbarer Software-Lösungen für Onsite- wie auch Offsite-Backup Acronis ist ein führender Hersteller hoch entwickelter und skalierbarer Software-Lösungen für Onsite- wie auch Offsite-Backup und Restore, Disaster Recovery, Deployment, System-Migration und Security. Unternehmen und Privatkunden können mit patentierten Acronis Technologien für Disk Imaging und Disk Management ihre digitalen Systeme in und zwischen physischen und virtuellen Umgebungen migrieren, verwalten und pflegen. Digitale Informationen werden zuverlässig abgesichert, eine hohe Verfügbarkeit, Geschäftskontinuität und Integrität der Unternehmensdaten sowie der IT-Infrastruktur gewährleistet und Ausfallzeit minimiert. Acronis Software wird in mehr als 180 Ländern vertrieben und ist in 13 Sprachen verfügbar. Mehr Informationen können auf der Website abgerufen werden: www.acronis.de.

Acronis®
COMPUTE WITH CONFIDENCE
WWW.ACRONIS.DE

Für weitere Informationen besuchen Sie http://www.acronis.de

Acronis Germany GmbH

Balanstr. 59, 81541
München
Tel. +49 89 613 72 84-0

Fax +49 89 613 72 84-99
info-de@acronis.com
http://www.acronis.de