Acronis

3 Gründe **warum Backup strategisch** sein sollte

Dieses Whitepaper beschreibt drei wesentliche Gründe, warum Backup ein strategisches Element Ihres IT-Plans sein sollte – und warum es für Ihr Unternehmen sehr wichtig ist, eine Strategie zu entwickeln und umzusetzen, mit der Ihre Daten vollständig geschützt werden.

Inhaltsverzeichnis

Einführung

Sie sind Mitglied eines kleinen IT-Teams in einem mittelständischen Unternehmen, und ein Feuer zerstört Ihre Firmeneinrichtung (inkl. Datencenter). Unglücklicherweise fehlten Ihnen jedoch Zeit und Ressourcen, um einen Disaster Recovery-Plan zu entwerfen und umzusetzen. Sie hatten bisher noch nicht einmal eine Backup-Strategie entwickelt und angewandt, um Ihre Systeme zu schützen.

Backup ist von strategischer Bedeutung für Ihren Geschäftsbetrieb, weil auch Ihre Daten es sind.

Damit sind Sie aber nicht alleine. Viele kleine bis mittlere Unternehmen verfügen über keine effektiven Backup- und Disaster Recovery-Maßnahmen. Gemäß einer von Acronis in Auftrag gegebenen IDC-Studie vom Mai 2014 zum Thema „Disaster Recovery" konnten 70% der Befragten der Aussage „Unsere Backup- und Disaster Recovery-Aktionen werden gut geplant und umgesetzt" nicht wirklich zustimmen.

Jetzt jedoch, da Ihr Datencenter zerstört ist, stehen Sie auch noch vor dem Problem, wie Sie Ihrem Management-Team vermitteln, dass die meisten Ihrer Unternehmensdaten wie Finanzunterlagen, Rechnungsdaten, laufende Aufträge, Kundendaten und Verträge dauerhaft verloren sind.

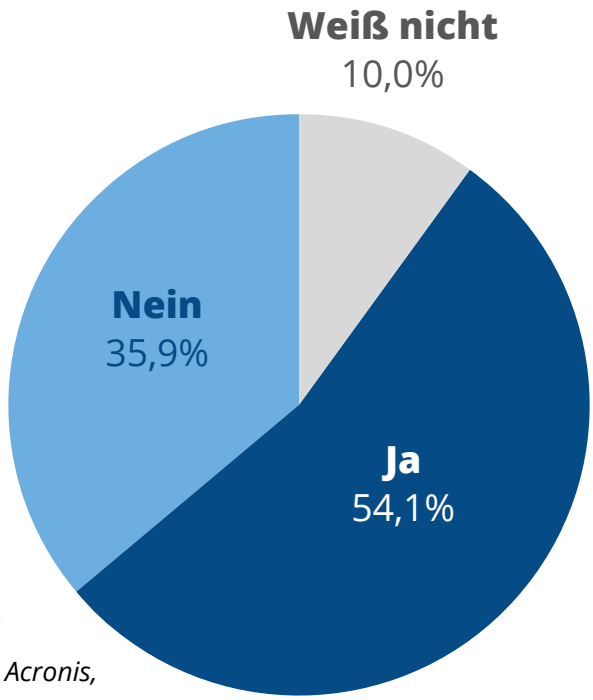
Wenn man also bedenkt, wie sehr die Existenz Ihres Unternehmens von Ihrer Backup-Strategie abhängt, stellt sich die Frage, warum das Thema Datensicherung in Ihrem Planungsprozess immer erst nachträglich behandelt wird. Systeme und Netzwerk haben Sie sorgfältig geplant, entworfen und umgesetzt – die „Backup-Diskussion" sowie die entsprechende Umsetzung wurden jedoch verschoben.

- Gartner schätzt, dass bei nur 35% der kleinen bis mittleren Unternehmen ein umfassender Disaster Recovery-Plan vorhanden ist.

- Nur 2 Prozent der befragten Firmen sichern 100% ihrer Daten per Backup. *(Quelle: Umfrage Disaster Recovery Studie, IDC und Acronis, Mai 2014)*

- 36% der befragten Firmen räumten ein, dass sie von virtuellen Servern seltener Sicherungen erstellen als von ihren physischen Servern. *(Quelle: Umfrage Disaster Recovery Studie, IDC und Acronis, Mai 2014)*

Sichert Ihre Organisation virtuelle Server genauso häufig wie physische Server?



Quelle: Umfrage Disaster Recovery Studie, IDC und Acronis, Mai 2014

Backup ist von strategischer Bedeutung für Ihren Geschäftsbetrieb, weil auch Ihre Daten es sind. Ohne Sicherung setzen Sie Ihr Unternehmen einem hohen Risiko aus. Backup ist Ihr Versicherungsschutz, und nichts – weder eine andere Technologie noch ein manueller Prozess – kann Backup ersetzen. Keine Datensicherung zu machen und deswegen Daten zu verlieren ist vergleichbar mit dem Verlust eines physischen Inventars, das Sie nicht versichert haben!

Dieses Whitepaper berschreibt drei wesentliche Gründe, warum Backup ein strategisches Element Ihres IT-Plans sein sollte – und warum es für Ihr Unternehmen sehr wichtig ist, eine Strategie zu entwickeln und umgehend umzusetzen, mit der Ihre Daten vollständig geschützt werden.

#1: Nur Backup kann Ihre Geschäftsdaten wirklich schützen

Das Leben ist voller Unwägbarkeiten, und auch Ihr Geschäftsbetrieb ist davon nicht ausgenommen. Naturkatastrophen (Erdbeben, Überschwemmungen), von Menschen verursachte Störfälle (Computerviren, Sicherheitsverstöße) sowie Soft- oder Hardware-Fehler können zu Datenverlust führen. Daten gehen viel öfter verloren, als wir gemeinhin wahrhaben oder zugeben wollen. Bedenkt man die Vielzahl interner und externer Faktoren, die Ihr System und Ihre Daten beeinflussen, lautet die Frage tatsächlich nicht mehr ‚ob', sondern ‚wann' auch Sie Daten verlieren werden.

In erster Linie sollte Backup für Sie strategisch sein, weil das die einzig wirklich effektive Möglichkeit ist, wichtige Daten zu schützen. Bedenken Sie, welche Folgen es für Ihr Unternehmen haben würde, wenn Sie die Daten von Verkauf, Kundenverwaltung, Entwicklungsabteilung oder Buchhaltung verlieren sollten. Unersetzliche Daten zu verlieren kann zu Umsatzeinbußen, Vertragsstrafen, Rechtstreitigkeiten, Compliance-Problemen und rückläufigen Börsenkursen führen. Im schlimmsten Fall zwingt Sie ein solcher Datenverlust sogar in den Konkurs.

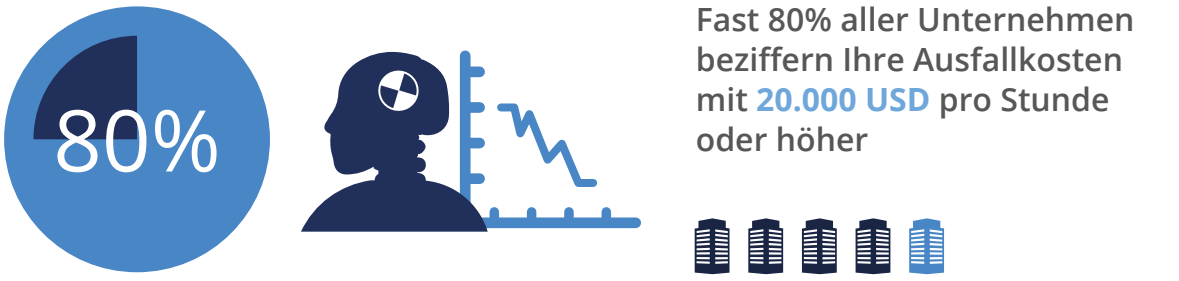
Dem IBHS (Institute for Business and Home Safety) gemäß können ca. 25% der Unternehmen, die ein schweres Daten-Desaster erlebt haben, ihren Geschäftsbetrieb nicht mehr fortsetzen. Abgesehen von einer Katastrophe können Daten auch noch auf andere Art verloren gehen:

- In den USA gehen beispielsweise wöchentlich 140.000 Festplatten kaputt. *(Quelle: National Archives & Records Administration in Washington)*
- Auf 6% aller PCs kommt es pro Jahr zu einem Datenverlust. *(Quelle: The Cost of Lost Data, David. M. Smith)*
- 31% aller PC-Anwender haben schon einmal alle Dateien durch ein Ereignis verloren, das sie nicht beeinflussen konnten.

Um die beste Vorgehensweise für Ihr Unternehmen zu bestimmen, sollten Sie zuerst den Wert und die benötigte Verfügbarkeit Ihrer verschiedenen Datenbestände ermitteln. Die Ergebnisse dieser Analyse müssen dann in Ihren IT-Plan einfließen.

Denn nicht alle Daten in Ihrer IT-Umgebung sind gleich. Einige Daten ändern sich sehr schnell und sind sehr wichtig für Ihr Unternehmen. Diese Daten sollten Sie häufig sichern, um die Datenmenge, die Sie schlimmstenfalls verlieren könnten, möglichst gering zu halten. Da diese Daten besonders wertvoll für Ihre Geschäftsvorgänge sind, sollten Sie auch mehr Geld und Ressourcen bereitstellen, um sicher zu stellen, dass diese Daten vollständig gesichert und auch schnell wiederhergestellt werden können. Sie sollten erwägen, einen vielschichtigen Backup-Plan zu implementieren – beispielsweise alle paar Stunden eine Sicherung durchführen und die entstandenen Backup-Dateien so vorbereiten, dass Sie Ihre Systeme jederzeit als virtuelle Maschinen (VMs) wiederherstellen können. Und zwar sowohl am ursprünglichen wie auch an einem anderen, entfernten Einsatzort.

Andere Daten sind vielleicht ebenfalls wichtig, ändern sich jedoch nicht so häufig. Und Ihr Unternehmen benötigt darauf keinen sofortigen Zugriff. Für diese Daten empfiehlt sich die Umsetzung eines einfacheren Backup-Plans. Sie können beispielsweise täglich eine Kopie erstellen und die entstandenen Backup-Dateien auf preisgünstigen Medien (z. B. Magnetband) oder auf einem günstigen Langzeit-Cloud-Storage speichern.



Quelle: Umfrage Disaster Recovery Studie, IDC und Acronis, Mai 2014

Dies ist ein wesentlicher Grund, warum Sie Backup unbedingt als strategisches Element in Ihren IT-Plan aufnehmen sollten. Sie können Ihre IT-Architektur und Systeme damit passend dazu ausrichten, um Ihre Backup-Anforderungen nach der jeweiligen Wichtigkeit, Änderungshäufigkeit oder der vorgegebenen Wiederherstellungszeit optimieren zu können.

#2: Kein Disaster Recovery-Plan funktioniert ohne Backup

Disaster Recovery stellt die Kontinuität Ihres Geschäftsbetriebs im Desaster-Fall oder bei anderen unvorhersehbaren Ereignissen sicher und besteht zumeist aus einem primären und einem sekundären Standort, der entweder kontinuierlich aufrechterhalten oder schnell als Standby-System aufgesetzt wird. Daten, Betriebssysteme, Applikationen, Dateien und Ordner werden zwischen den Systemen repliziert und in der Regel kreuzweise gesichert, um Ihre Systeme in einem betriebsbereiten Zustand wiederherzustellen und dabei Datenverlust und Ausfallzeit soweit wie möglich zu minimieren. Sicherungen sind dabei der wesentlichste Bestandteil einer wirksamen Disaster Recovery-Strategie.

Es gibt viele Methoden, mit denen Unternehmen ihre Daten nach einem Systemfehler oder Desaster wiederherstellen. Aber jede Methode beruht auf Backup. Wenn beispielsweise ein Server plötzlich ausfällt, kann eine Failover-Lösung die Serverlast ohne menschliches Eingreifen auf einen anderen bereitstehenden Server, ein anderes System oder Netzwerk verlegen. Dafür müssen Sie die Daten aber auf dem zweiten Server replizieren und danach auch sichern.

Hochverfügbarkeit ermöglicht Redundanz, durch die Sie Ausfallzeiten minimieren oder eliminieren können und sicher stellen, dass kritische Systeme immer und üblicherweise innerhalb weniger Minuten verfügbar sind. Hochverfügbarkeit ist eine Einzellösung und arbeitet mit nur einem Satz an Daten. Es ist Ihre Entscheidung, ob Sie die Daten replizieren oder nicht – aber Sie müssen sie unbedingt sichern.

Im Desasterfall können Sie ein System dadurch wiederherstellen, dass Sie ein neues System aufsetzen. Dazu müssen Sie entweder alle erforderliche Software neu installieren oder ein Image des alten Systems auf das neue übertragen. In jedem Fall benötigen Sie aber zumindest ein Backup der betreffenden Daten.

Unter Migration versteht man einen Prozess, bei dem ein Betriebssystem, Applikationen, Daten, Dateien, Ordner etc. auf ein neues (und möglicherweise abweichendes) System übertragen werden. Systeme werden aus den unterschiedlichsten Gründen migriert, z.B. wenn Server gewartet, repliziert oder per Upgrade aktualisiert werden müssen, Systemressourcen

optimiert, physische Maschinen in virtuelle Umgebungen verschoben, Daten nach einem Desaster wiederhergestellt oder IT-Infrastrukturen geändert werden sollen (etwa bei einem Firmenzusammenschluss, einer Firmenübernahme oder starkem Firmenwachstum).

Es gibt viele unterschiedliche Arten von Migrationen einschließlich Datenmigration, Applikationsmigration und Cloud-Migration. Um ein System migrieren zu können, benötigen Sie mindestens eine Backup-Kopie der Daten und Applikationen.

Failover, Hochverfügbarkeit, fehlertolerante Systeme, Systemwiederherstellung und Migration sind mögliche Bestandteile eines Disaster Recovery-Plans, mit denen man auf bestimmte unterschiedliche Ereignisse reagieren kann. Jede dieser Methoden beruht auf einer gut durchdachten Backup-Strategie, die immer vor und nicht nach Eintritt eines solchen Ereignises geplant werden sollte.

Eine weitere wichtige Komponente Ihres Disaster Recovery-Plans ist die Überlegung, wie viele Backup-Kopien benötigt und wo diese Kopien gespeichert werden sollen. Acronis versucht diese Aufgabe für Sie zu vereinfachen und empfiehlt dazu eine 3-2-1-Backup-Methode:

- Verwalten Sie alle Daten an *drei* Speicherorten, beispielsweise auf produktiven Systemen und Sicherungen auf NAS-Systemen und in der Cloud.

- Speichern Sie Ihre Backup-Kopien auf *zwei* Arten von Medien (beispielsweise auf Festplatten und in der Cloud).

- Bewahren Sie *eine* Kopie Ihrer Backup-Daten ‚offsite' (an einem externen Ort) auf.

Eine Sicherung lokal verfügbar zu halten ist dann besonders sinnvoll, wenn bei einem primären System ein Hard- oder Software-Fehler auftritt (z. B. durch eine Sicherheitsverletzung oder einen Computervirus). In solchen Fällen ist ein lokales Backup (im Vergleich zu anderen Optionen) üblicherweise die schnellste Möglichkeit, um die Systeme eines Unternehmens wieder einsatzbereit zu bekommen.

Backup-Kopien auf zwei unterschiedlichen Medienarten vorzuhalten ist wichtig, um sich vor dem Ausfall der Medien zu schützen. 34% aller Firmen *(Quelle: Boston Computing Networks)* führen keine Tests ihrer Bandsicherungen durch – und 77% derer, die es doch tun, entdecken dabei Fehler.

59%

der Unternehmen sehen es als gefährlich an, nur eine Backup-Kopie vorzuhalten

Quelle: eine Umfrage des Redmond Magazine

Eine Backup-Kopie offsite vorzuhalten schützt vor dem Fall, dass ein Desaster sowohl Ihre Systeme als auch Ihre lokalen Sicherungen zerstört. Wenn Sie einen zweiten Standort in Betrieb nehmen müssen, können Sie dafür die extern aufbewahrte Backup-Kopie verwenden. Sicherungen in der Cloud zu speichern, schützt vor allen unvorhergesehenen Ereignissen (insbesondere einem Desaster). Größere Unternehmen speichern ihre Backup-Kopien sowohl in privaten wie öffentlichen Clouds, während kleine bis mittlere Unternehmen ihre Kopien eher in öffentlichen Clouds aufbewahren.

Falls Sie die Kontinuität Ihres Geschäftsbetriebs ohne Disaster Recovery- und Backup-Plan nicht sicherstellen können, können Sie es sich auch nicht leisten, die Entwicklung eines Disaster Recovery-Plans hinauszuschieben. Dies muss, zusammen mit Ihrer Backup-Strategie, ein wesentlicher Bestandteil Ihres IT-Plans sein.

#3: Backup ist eine wichtige Voraussetzung, um Compliance einhalten zu können

Fast alle Anforderungen zur Einhaltung rechtlicher Bestimmungen beinhalten, dass Unternehmen ihre Daten schützen und sichern müssen. Nachfolgend einige Beispiele weltweiter gängiger Compliance-Richtlinien, die Datensicherung notwendig machen.

HIPAA (U.S.) – Falls Ihre Organisation Krankenakten in elektronischer Form aufbewahrt, verlangt der HIPAA (Health Information Portability & Accountability Act), dass Ihre Organisation über Kontroll-Möglichkeiten verfügt, um Datenintegrität, Authentifizierung, Sicherheit, Notfallplanung, Zugriffs- und Prüfvorgänge zu verwalten. Die Sicherung der Patientendaten ist eine wesentliche Maßnahme, um diese Anforderungen zu erfüllen. Ähnlich strenge Bestimmungen gelten auch für Patientendaten in Deutschland.

BDSG (D) – Zweck des Bundesdatenschutzgesetzes ist es, den einzelnen Büger davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird. Gemäß §9 sind alle Stellen, welche personenbezogene Daten verarbeiten, erheben oder nutzen verpflichtet, technische und/oder organisatorische Maßnahmen zu treffen, um zu gewährleisten, dass die Sicherheits- und Schutzanforderungen des BDSG erfüllt sind. Die Spezifizierung dieser Anforderungen ergibt sich aus der Anlage (zu §9 Satz 1) BDSG. Dort steht unter dem Punkt Verfügbarkeitskontrolle: „Es muss sichergestellt werden, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt werden." Als Maßnahme dafür findet man u.a. das Vorhandensein eines Backup-Konzepts. Nur Backup kann sicherstellen, dass Daten nicht verloren gehen, selbst wenn sie versehentlich gelöscht oder zerstört werden.

SOX (U.S.) – Alle amerikanischen Unternehmen und Prüfungsgesellschaften, auch ausländische Prüfungsgesellschaften und Unternehmen mit einer amerikanischen Börsennotierung, unterliegen dem Sarbanes-Oxley Act von 2002, der strenge Anforderungen bezüglich Aufbewahrung, Änderung und Zerstörung von Unterlagen bzw. Daten beinhaltet. Die Sicherung der Finanz- und

Geschäftsdaten ist ein wesentlicher Bestandteil, um diese Anforderungen zu erfüllen. Durch die extraterritoriale Wirkung dieses US-Gesetzes gibt es inzwischen in den meisten Ländern entsprechende nationale Vorschriften wie z. B. die Richtlinie 2006/43/EG des Europäischen Parlaments und des Rats.

Basel II und Basel III (Global) – Neben anderen Anforderungen verlangen Basel II und III, dass Finanzinstitute ihre Daten immer unter Kontrolle haben und Backup-Pläne für die Systeme vorhanden sein müssen.

WpHG (D) – §16 des Gesetzes über den Handel mit Wertpapieren regelt die Aufzeichnungspflichten von Wertpapierdienstleistungsunternehmen sowie Unternehmen mit Sitz im Inland, die an einer inländischen Börse zur Teilnahme am Handel zugelassen sind. Diese müssen bestimmte Angaben zur Durchführung von Aufträgen aufzeichnen und mindestens 6 Jahre aufbewahren sowie sie gemäß §257 des HGB in dieser Zeit verfügbar halten und jederzeit innerhalb angemessener Frist lesbar machten können.

PCI (Global) – Der PCI 3.0 DSS (Payment Card Industry's Data Security Standard) 12.10.1 verlangt von Händlern, einen Reaktionsplan für Störfälle zu erstellen, der zum Schutz vor Sicherheitsverletzungen implementiert wird. Der Plan muss auch einen Prozess zur Datensicherung umsetzen.

GLBA (U.S.) – Die FFIEC-Bundesbehörden (Federal Financial Institutions Examination Council, entspricht der Bundesanstalt für Finanzdienstleistungsaufsicht, kurz BaFin) und die FTC (Federal Trade Commission, Wettbewerbsbehörde bzw. Kartellamt) beaufsichtigen Finanzinstitute, die dem GLBA (Gramm-Leach-Bliley Act) unterliegen. Beide Behörden verlangen, dass Finanzinstitute über Notfallpläne verfügen, um ihre Systeme bzw. Daten bei einem Notfall oder einer Katastrophe wiederherstellen zu können. Diese Bestimmungen erfordern u. a. Pläne für Datensicherung, Disaster Recovery und einen Notfallbetrieb. Ähnliche Bestimmungen für Unternehmen, die von der BaFin beaufsichtigt werden, finden Sie auch in unterschiedlichen deutschen Gesetzgebungen.

Warum Acronis die optimale Lösung für eine Backup-Strategie in kleinen bis mittleren Unternehmen ist

Derzeit sind drei Grundtypen von Backup-Lösungen auf dem Markt verfügbar:

- Die traditionelle ‚Eine-für-alles'-Plattform, die einen intelligenten Backup Server bereitstellt, um eine einheitliche Datensicherung der kompletten IT-Umgebung durchzuführen und zu verwalten (egal ob physisch oder virtuell).

- Einzelne separate Produkte oder Tools, die unterschiedliche Datentypen, Betriebssysteme und Applikationen schützen.

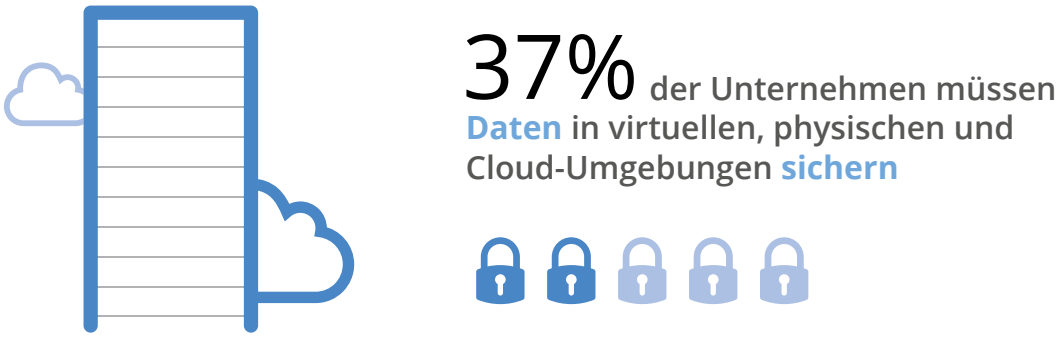
- Ein integriertes Paket von Produkten, das einheitliche Steuerung, Verwaltung und Reporting für Ihre komplette IT-Umgebung bereitstellt – unabhängig von der Größe Ihres Unternehmens, der Anzahl unterschiedlicher Datentypen sowie Anzahl und Arten von Betriebssystemen und Applikationen.

Eine traditionelle Plattform unterstützt eine große Anzahl und viele Datentypen, Betriebssysteme und Applikationen. Eine Plattform bedeutet, dass man auch nur mit einem einzigen Anbieter umgehen muss. Das bedeutet weit weniger Komplexität, als sich bei der Handhabung und Verwaltung mehrerer Anbieter ergeben würde. Der Erwerb einer traditionellen Lösung ist meist eine strategische Entscheidung.

Leider sind traditionelle Data Protection-Plattformen für kleine bis mittlere Organisationen üblicherweise zu teuer. Die Anschaffung einer solchen Plattform verursacht signifikante Vorlaufkosten (etwa für Lizenzen, dedizierte Hardware, Netzwerkkomponenten für den zentralen Betrieb, Wartungskosten). Eine traditionelle Data Protection-Plattform benötigt außerdem einen oder mehrere geschulte, zertifizierte Vollzeit-Systemadministratoren – eine Ressource, die sich viele kleine bis mittlere Unternehmen nicht leisten können.

Sie können sich aber auch dafür entscheiden, einzelne separate Backup-Produkte und Tools bei Bedarf anzuschaffen. Dies wäre eine eher taktische Vorgehensweise, um Ihre Backup-Bedürfnisse System für System und Applikation für Applikation anzugehen. Zwar vereinfacht dies vielleicht die anfängliche Kaufentscheidung (da jede dieser Applikationen günstiger als eine traditionelle Plattform ist), allerdings müssen Sie in diesem Fall aber oft unterschiedliche Backup-Hersteller für unterschiedliche Betriebssysteme und Applikationsplattformen handhaben.

Der Nachteil: Mehrere Produkte und Anbieter erhöhen auch Faktoren wie Schulungsbedarf sowie den Aufwand für Verwaltung, Installation, Überwachung und Reporting, da jedes Produkt unterschiedlich ist. Mit dem Wachstum Ihrer Organisation beginnen sich die Kosten für weitere separate Produkte/Tools aufzusummieren. Mit einer zunehmenden Zahl von Betriebssystemen und Applikationen in Ihrem Unternehmen müssen Sie auch immer mehr IT-Administratoren anstellen. Dies erhöht wiederum Personal- und IT-Schulungsbedarf.



Quelle: Umfrage Disaster Recovery Studie, IDC und Acronis, Mai 2014

Als kleines bis mittleres Unternehmen ist der Erwerb eines integrierten Produktpakets die optimale Entscheidung, weil Sie dann nur noch eine einzige Backup-Lösung für all Ihre Betriebssysteme und Applikationen im Einsatz haben. Oder anders ausgedrückt: Damit können Sie Ihre bisherigen Einzellösungen zu einer einzigen Gesamtlösung integrieren. Dank einer integrierbaren Produkt-Suite müssen Sie nur noch einen Anbieter handhaben. Die Komplexität und der Zeitaufwand für die Verwaltung von Lösungen mehrerer Anbieter entfällt also. Weil eine Produkt-Suite zudem auch nur ein Installationsmenü und eine Verwaltungskonsole für alle Produktkomponenten verwendet, werden die Anforderungen an Ihre IT-Mitarbeiter vereinfacht und die IT-Schulungskosten gesenkt.

Zusammenfassung

IT-Profis sollten das Thema „Backup“ niemals hinauszögern. Tatsächlich sollten Backup und Disaster Recovery fortlaufende Dikussionspunkte über den gesamten IT-Planungsprozess hinweg sein. Datensicherungen sind geschäftskritisch – ja, strategisch entscheidend – für Ihr Unternehmen, weil …

… Ihr Geschäftsbetrieb letztendlich auf Ihren Daten basiert, und nur Backup diese wirklich schützen kann.
Kein Backup = keine Daten = kein Unternehmen

… Backup eine wesentliche Komponente eines Disaster Recovery-Plans ist.
Kein Backup = kein Disaster Recovery = kein Unternehmen

… viele Compliance-Richtlinien von Unternehmen verlangen, dass sie ihre Daten sichern.
Kein Backup = Compliance-Verstoß = die Gefahr zivil- oder strafrechtlicher Sanktionen

Acronis bietet kleinen bis mittleren Unternehmen die einzig erschwingliche strategische Lösung an, um Daten jeder Art in beliebigen IT-Umgebungen und an beliebigen Speicherorten schützen zu können. Acronis Backup-Produkte basieren auf der Acronis AnyData Engine – einer Sammlung einzigartiger, leistungsstarker Technologien für Data Protection der neuen Generation, um Daten in virtuellen, physischen und Cloud- Umgebungen erfassen, speichern, wiederherstellen und verwalten zu können. Sie können, je nach Ihren Unternehmensanforderungen, einzelne Acronis-Produkte einsetzen oder diese bei Bedarf problemlos zu einer einheitlichen Gesamtlösung integrieren, die Daten jeder Art in beliebigen IT-Umgebungen und an beliebigen Speicherorten schützt.

Sie können, unabhängig von Ihrer IT-Umgebung, dieselbe einheitliche Konsole verwenden, um jedes Produkt zu konfigurieren, zu installieren und zu verwalten. Für eine größere Anzahl von Systemen bietet Acronis den Acronis Management Server (AMS) an. Dieser ermöglicht mit nur einer Oberfläche, die Verwaltung der Sicherungen und Wiederherstellungen aller Daten über mehrere Acronis Backup Advanced-Produkte hinweg. Die Acronis-Technologie für Data Protection der neuen Generation wurde für Unternehmen entwickelt, die eine umfassende, effiziente und einfach zu bedienende Lösung benötigen. Sie vereinfacht die Durchführung von Backup und Disaster Recovery sowie den sicheren Zugriff auf Ihre geschäftskritischen Daten und hilft dabei, Datenverlust zu vermeiden sowie den IT-Verwaltungsaufwand und die Gesamtbetriebskosten (TCO) zu reduzieren.

Acronis

Über Acronis

Acronis setzt Standards für Data Protection der neuen Generation. Mit seinen Lösungen für Backup, Disaster Recovery und sicheren Zugriff, basierend auf der AnyData Engine, und dem Vorsprung durch seine Imaging-Technologie, bietet Acronis einfaches, umfassendes und sicheres Backup für Dateien, Applikationen und Betriebssystem in beliebiger Umgebung – virtuell, physisch, Cloud oder mobil.

Acronis wurde 2002 gegründet und schützt Daten von über 5 Millionen Nutzern und 300.000 Unternehmen in über 130 Ländern. Acronis-Produkte beinhalten mehr als 100 Patente und wurden u.a. zum besten Produkt des Jahres gewählt von Network Computing, TechTarget und IT Professional.

Die Produkte decken eine große Bandbreite von Funktionen ab (z.B. Migration, Klonen und Replizierung).

Weitere Informationen finden Sie unter **www.acronis.de**.

Folgen Sie Acronis auf Twitter: **twitter.com/acronis_de/**.