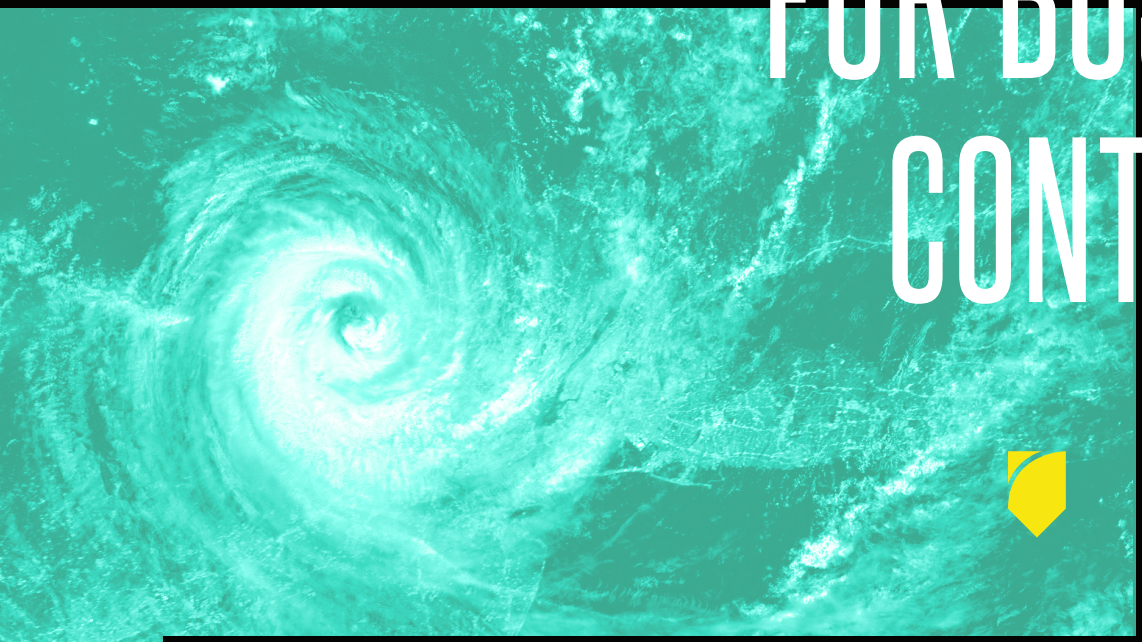
arcserve®

eBook

Ein IT Überlebensleitfaden

INTELLIGENTE STRATEGIEN FÜR BUSINESS CONTINUITY



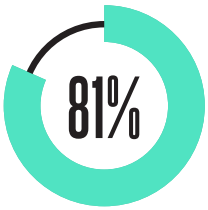
7 ENTSCHEIDENDE FRAGEN AN SIE SELBST ÜBER DIE ÜBERWINDUNG VON DATENVERLUST UND AUSFALLZEITEN - UND UM SICHERZUSTELLEN, DASS IHR BUSINESS CONTINUITY PLAN NICHT VOR IHREN AUGEN EXPLODIERT.

Angst. Verwirrung. Verzweiflung. Es erscheint wie ein Alptraum, nur dass es tatsächlich an Ihrem Arbeitsplatz passiert: Sie erfüllen Ihre alltäglichen IT-Aufgaben, und werden plötzlich von einer sich anbahnenden Datenverlustkatastrophe überrascht. Sie müssen gequält erkennen, dass Sie nicht in der Lage sein werden, Ihre Systeme schnell genug wiederherzustellen, um die dringendsten Bedürfnisse Ihres Unternehmens zu erfüllen.

Es kann eine schreckliche Erfahrung sein - eine, die alles bedroht, wofür Sie gearbeitet haben und was Sie erreichen wollten. Denn wenn Sie Daten verlieren, wie es in allen Unternehmen passieren kann, können Sie extreme Verzögerungen in der Geschäftsabwicklung erleiden, ein Vermögen an Produktivität und Umsatz verlieren und hilflos zusehen, wie Kunden durch die schlechte Erfahrung frustriert werden und woandershin abwandern.

Laut einer aktuellen ITIC-Studie geben

98% der Unternehmen an, dass eine einzelne Stunde Ausfallzeit sie 100.000 Dollar oder mehr kostet(1),



während 81% angeben, dass die Kosten pro Stunde 300.000 Dollar oder mehr betragen(2).

Und das sind nur Durchschnittswerte: Die tatsächliche Dauer und die Kosten eines Ausfalls können selbst für kleine und mittlere Unternehmen weitaus höher sein und erreichen oft Millionen von Dollar pro Vorfall.

ACHTEN SIE DARAUF, DASS "DISASTER RECOVERY" AUF IHR UNTERNEHMEN UND NICHT AUF IHRE KARRIERE ZUTRIFFT.

Standardmesswerte, unzureichende Ergebnisse.

Datensicherung konzentriert sich traditionell auf zwei Schlüsselmesswerte - RTO (Recovery Time Objective), welcher die Zeit misst, die für die Wiederherstellung Ihrer Daten benötigt wird, und RPO (Recovery Point Objective), der misst, wie viel Daten Sie bei einem Ausfall bereit sind zu verlieren.

Im Laufe der Jahre haben sich IT-Profis oft auf RTO konzentriert, um sicherzustellen, dass ein Unternehmen wieder zur Normalität zurückfindet. Viele Unternehmen können jetzt ihre Daten enorm schnell wieder online abrufen - und zwar in wenigen Minuten statt in Stunden oder Tagen.

Problem gelöst? Happy End? Nicht unbedingt. Denn auch das andere Schlüsselelement - das Alter Ihrer Daten - spielt eine entscheidende Rolle bei der Wiederherstellung nach einer Katastrophe. Sicher, mit Ihrem beeindruckenden RTO sind Sie im Handumdrehen wieder einsatzbereit. Aber was ist, wenn Ihr letztes Backup 10 Stunden zurückliegt und Sie daher keine Kundenaufträge, die während dieser Zeitspanne erteilt wurden, wiederherstellen oder ausführen können? Sie würden Einnahmen verlieren, die bereits ein "gemachter Deal" waren, ohne jemals zu wissen, wer die verlorenen Aufträge platziert hat oder ob es eine Chance gibt, sie in langfristige Kunden umzuwandeln, die einen signifikanten Wert auf Dauer bieten würden. Es wird Zeit, den Panikknopf zu drücken. Und verschärfen Sie Ihr RPO.

Budgetsorgen, eine kostensenkende Zwangsjacke.

Natürlich wissen Sie im Prinzip, dass Sie die RTOs und RPOs festlegen müssen, die für Ihre Systeme und Anwendungen geeignet sind. Aber das Budget ist immer ein Faktor. In Bezug auf RPO haben Sie möglicherweise nicht die notwendigen Finanzmittel für Ihre IT-Abteilung zur Verfügung, um alle Ihre Daten so oft wie nötig erfolgreich zu sichern. Infrastruktur- und Personalkosten können die Kosten schnell in die Höhe treiben und so die Ressourcen begrenzen die Sie für eine Backup-Lösung einsetzen können, die in der Lage ist, RPOs von Minuten zu unterstützen.

Um diese Budgetrestriktionen zu erfüllen, sind viele Organisationen leider gezwungen, die Leistungsfähigkeit hintenan zu stellen. Es ist ein typischer Fall des „am falschen Ende sparens" bei einer Katastrophe. Wenn die Geldbörse geschmählert wird, sind Sie oft gezwungen, sich mit unzureichenden Backup- und Wiederherstellungswerkzeugen und -methoden zu begnügen, die Sie, wenn Sie selbst entschieden hätten, gar nicht erst gewählt hätten.

Zunehmende Komplexität, nicht aufrechtzuhaltender Status quo.

Die vielleicht größte Veränderung im Datenschutz in den letzten Jahren ist der Grad der Komplexität in Ihrer IT-Umgebung. Genug um jeden im Kopf schwindlig zu machen. Das liegt daran, dass es jetzt so viele, sich verändernde Komponenten gibt, dass Verwirrung und Probleme zwangsläufig zunehmen, was zu hässlichen Verzögerungen bei Wiederherstellung führt. Beachten Sie Folgendes:

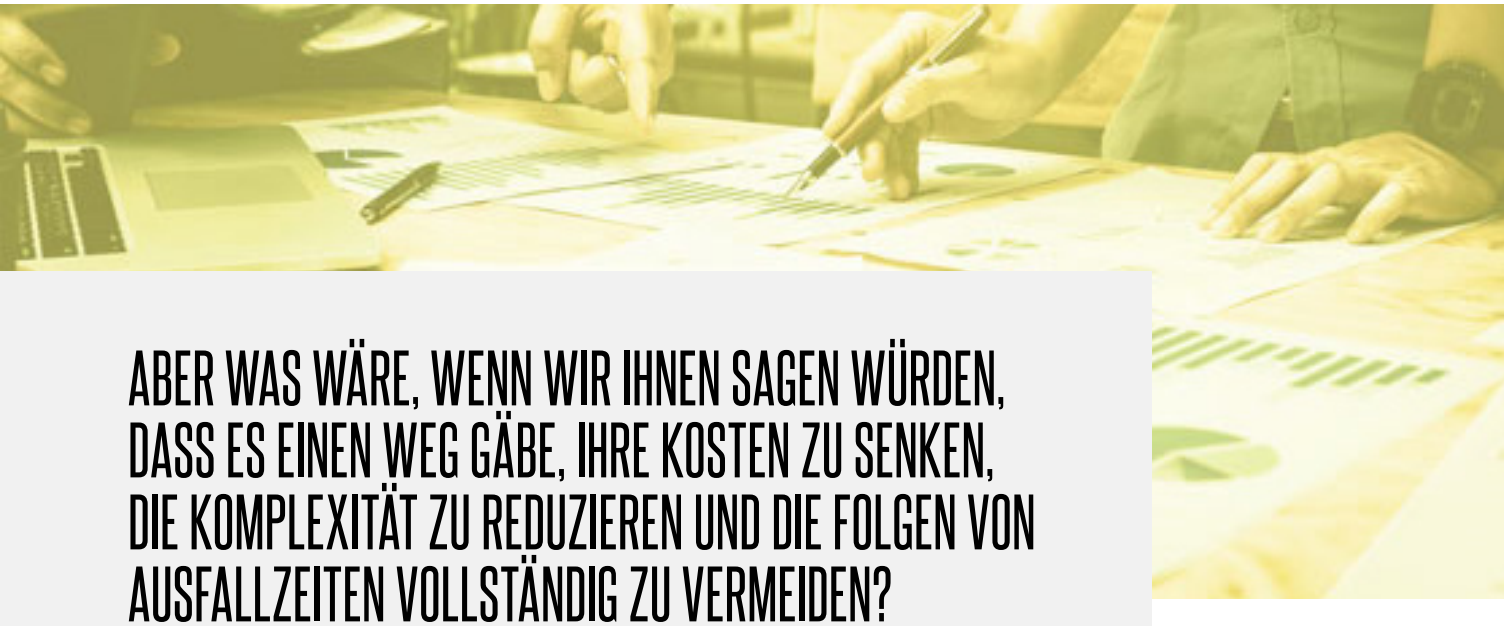
Vielfalt ist überall. Heute haben Sie es mit lokalen, Cloud-, hybriden und virtuellen Umgebungen sowie mit großen Datenmengen, Videos und Fotos zu tun – alles auf mobilen Geräten auf der ganzen Welt verteilt. Und das alles muss geschützt werden, höchstwahrscheinlich mit unterschiedlichen Service Level Agreements (SLAs).

Mehr Backup-Mechanismen und Anbieter bedeuten mehr Ärger. Sicher, Sie können ein großartiges lokales Backup-System haben, aber es kann vielleicht nicht mit der Cloud verbunden werden. Oder das Cloud-Backup wird evtl. von einem anderen Anbieter als dem, der Ihr Rechenzentren betreibt, verwaltet. Mobile Backups? Schauen Sie sich die einzelnen App-Anbieter an. Und so weiter und so fort. Gartner berichtet, dass durchschnittliche mittelständische Unternehmen mindestens 3 verschiedene Backup-Lösungen als Teil ihrer dezentralen Betriebsabläufe nutzen, wobei ein Viertel davon den Anbieter so schnell wie möglich wechseln möchten.

Daten sind gespeichert und sehr unterschiedlich. In Anbetracht der vielen oben genannten Umgebungen werden die Daten Ihres Unternehmens wahrscheinlich an vielen Orten gespeichert – im eigenen Rechenzentrum, in der Public Cloud, an einem entfernten Standort und so geht die Liste weiter. Aber Daten werden nicht nur nach dem Ort, an dem sie gehostet werden, sondern auch nach dem Grad ihrer Bedeutung getrennt. Ihr IT-Team sollte besser in der Lage sein POS-Daten innerhalb weniger Minuten wiederherzustellen, während die Wiederherstellung der Präsentation einer Marketingkonferenz von vor zwei Jahren eine weitaus geringere Priorität hat. Sie müssen vorbereitet sein einen Aktionsplan nach Prioritätsstufen auszuführen, wenn Ausfallzeiten und kritische Datenverluste drohen. Viel einfacher gesagt als getan.

Bei so viel Komplexität in der heutigen Computing-Umgebung kann man sagen, dass wir in eine neue Datenverarbeitungsära eingetreten sind. Es ist jedoch wahrscheinlich, dass Ihre Business Continuity -Pläne während der vorangegangenen Ära eingeführt wurden - als der Weg zur Datenwiederherstellung klarer und einfacher war.

Das bringt Sie in Gefahr. Denn wenn Sie immer noch ein altes Modell verwenden, das der Wiederherstellung ein geringen Betrag zuweist, ohne das tatsächliche finanzielle Risiko von Ausfallzeiten und Datenverlusten richtig zu bestimmen, stellen Sie sich auf ein Problem ein. Denken Sie daran, wie bereits erwähnt, die durchschnittliche Ausfallzeit kann einem mittelständisches Unternehmen bis zu 300.000 Dollar pro Stunde oder mehr an direkten Kosten verursachen. Und das beinhaltet noch nicht einmal die indirekten Kosten, die den Kundenumsatz und den Verlust des Kundenvertrauens beinhalten.



ABER WAS WÄRE, WENN WIR IHNEN SAGEN WÜRDEN, DASS ES EINEN WEG GÄBE, IHRE KOSTEN ZU SENKEN, DIE KOMPLEXITÄT ZU REDUZIEREN UND DIE FOLGEN VON AUSFALLZEITEN VOLLSTÄNDIG ZU VERMEIDEN?

Bevor wir herausfinden, wie man dorthin gelangt, sollten wir uns zunächst die Ursachen dieser Störungen ansehen und Ihr Wissen über die Bedrohungen bewerten.

Stellen Sie sich die folgenden Fragen, um herauszufinden, inwieweit Ihr Unternehmen gefährdet ist, und dann zeigen wir Ihnen, wie Sie eine erschwingliche Business Continuity-Strategie einführen können, die vorhersehbar, nachhaltig und zuverlässig ist.

Wie verteidigen Sie sich gegen die Ursachen von Datenverlust und Ausfallzeiten - und die Verwüstung, die sie bringen können?

BEGINNEN SIE DAMIT, SICH DIESE 7 SCHLÜSSELFRAGEN ZU STELLEN - EIN WICHTIGER ERSTER SCHRITT IN DIE RICHTIGE RICHTUNG.

1 Sind Sie durch einen veralteten Business Continuity-Plan belastet, der Sie anfällig macht für Ransomware-Angriffe (die können demnächst fast alle 14 Sekunden passieren)?

Sie haben viel von ihnen gehört, vielleicht sogar selbst erlebt.: Ransomware-Angriffe. Sie können sich als katastrophal für Ihr Unternehmen erweisen, indem sie Ihnen den Zugriff auf Ihre eigenen Daten verwehren und Sie dem Risiko aussetzen, die Daten selbst zu verlieren.

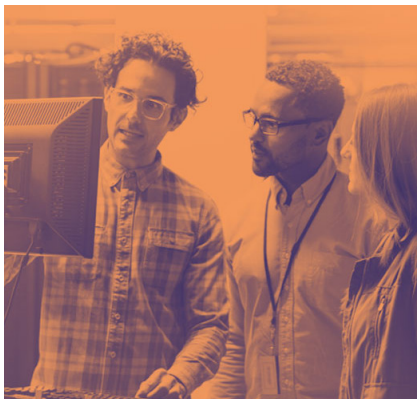
Ohne Zugriff auf Ihre Daten können Sie keine Bestellungen ausführen oder verfolgen. Keine Kunden bedienen, den Vertrieb koordinieren, Ihre Lieferkette verwalten oder eine große Anzahl anderer wichtigen Geschäftsfunktionen tätigen. Sie könnten sogar Ihr Geschäft verlieren.

Außerdem, wie ZDnet meldet, halten neue Ransomware-Stämme nicht nur Dateien als Geiseln, sondern sind sogar noch zerstörerischer, indem sie in betrieb befindliche Systemdateien verdampfen und einen kompletten Neuaufbau erfordern, bevor Sie fortfahren können(3).

Schlimmer noch, ein Lösegeldangriff kann große Unternehmen, mittelständische Unternehmen und kleine Unternehmen gleichermaßen treffen. Kein Wunder, dass Ransomware-Stämme wie WannaCry und Petya die Herzen von IT-Entscheidern auf der ganzen Welt in Angst und Schrecken versetzen. Und es ist nicht verwunderlich, dass der Schaden enorm ist. Der Report von Cybersecurity Ventures besagt, dass Ransomware-Angriffe bis 2019(4) weltweit 11,5 Milliarden Dollar Schaden anrichten könnten, ein sprunghafter Anstieg von den bereits erlittenen 2,0 Milliarden Dollar an Schäden im Jahr 2017(5). Und bis Ende 2019 wird es schätzungsweise alle 14 Sekunden einen Ransomware-Angriff auf ein Unternehmen geben(6)!

Das ist eine beängstigende Beschleunigung der Angriffe. Es zeigt, dass die Art der Ransomware-Gefahr schnell wächst und mutiert. Es stellt sich auch die Frage: Wenn Ihr Business Continuity-Plan ein paar Jahre alt ist und Gefahr läuft, veraltet zu sein, ist dann auch die verheerende Verwüstunge möglich, die durch die sich rasant entwickelnde Ransomeware-Bedrohung angerichtet werden kann?

2 Sind Sie im Falle einer Cyberattacke Kollegen ausgeliefert, die bereit sind, mit dem Finger auf Sie zu zeigen?



Um sich vor Datenverlust und Ausfallzeiten zu schützen, ist es wichtig, den richtigen Datenschutz zu haben. Es ist genau das, was Sie brauchen, um sich vor einer der schlimmsten Bedrohungen zu schützen - der Cyberattacke.

Eine professionell gestartete Cyberattacke kann Sie mit Distributed Denial of Service (DDoS) in großem Maßstab treffen, Ihre Geräte beschädigen, Daten unzugänglich machen und Sie gegenüber dem Management und den Kunden für Sicherheitsverletzungen und Schäden haftbar machen.

Laut einer aktuellen Umfrage von Neustar und Harris, gaben ganze 92% der Unternehmen an, dass sie bei einem DDoS-Angriff ebenfalls einen erheblichen Datenverlust erlitten haben(7). Und selbst wenn der DDoS-Angriff relativ klein ist, kann er immer noch als Vorwand für ein ehrgeizigeres Ziel dienen: Daten zu stehlen, Malware zu installieren, die Schwachstellen eines Netzwerks abzubilden und Ransomware zu installieren, was, wie bereits erwähnt, zu katastrophalen Datenverlusten und Ausfallzeiten führen kann.

Nehmen Sie als Beispiel für die Gefahren die Gesundheitsbranche, in der Leben buchstäblich auf dem Spiel stehen, wenn eine Cyberattacke Schaden anrichtet. Anfang 2018 erlitt ein Krankenhaus im Westen New Yorks eine Cyberattacke, die zu einem Ausfall der EHR (Electronic Health Record) führte, der zwei Wochen dauerte(8) - und damit den Kern der Einrichtung traf um Patienteninformationen abzurufen.

Und dann war da noch der Fall des großen Mid-Atlantic Gesundheitssystems, das in den letzten drei Jahren 76 medizinische Vorfälle im Zusammenhang mit Ausfallzeiten (nicht nur durch Cyberattacken, sondern auch durch andere Ursachen) meldete, die seine Laborkennzeichnung und -verfolgung, die Medikamentenverwaltung und die Fähigkeit, die Versorgung ohne Verzögerungen zu gewährleisten, unterbrachen(9).

Aber selbst wenn Ihre Branche nicht die auf Leben und Tod Dringlichkeit der Gesundheitsfürsorge hat, kann Ihre Karriere durch diese Art von Störungen immer noch erheblichen Schaden erleiden: Kollegen könnten Sie zum Sündenbock machen. Wütende Kunden könnten Sie schlechtreden. Und wie viele sehr erfahrene IT-Profis könnten Sie sogar selbst Ihre eigene Leistung in Frage stellen. Aber wie wehrt man sich?

3 Wird menschliches Versagen ein Missverhältnis zwischen Ihren RTOs und RPOs aufdecken?

Ja, es ist eine Tatsache, dass Ihre Mitarbeiter die Ursache für menschliches Versagen sind. Jeder macht Fehler, ohne Ausnahme - männlich oder weiblich, erfahren oder unerfahren, fleißig oder uninteressiert -, alle neigen dazu, manchmal fehlgeleitete (oder einfach nur dumme oder leichtsinnige) Dinge zu tun, die zu Ausfallzeiten, Datenverlust und Datenverstößen führen können. Auch Ihre IT-Kollegen können ein großer Teil des Problems sein.

Die Statistiken variieren, wie häufig menschliche Fehler am Arbeitsplatz auftreten. Aber ob Ihre Mitarbeiter versehentlich ein freigegebenes Verzeichnis oder einen Ordner löschen, einen Design- oder Codierungsfehler machen, verdächtige Programme oder Dokumente herunterladen oder einen Vanille-Milchshake in den Serverraum bringen - die Auswirkungen können verheerend sein.

Sie können auch eine gefährliche Trennung zwischen Ihren RTOs und RPOs aufdecken. Wenn Ihre Server beispielsweise in Vanille getränkt werden, können Sie einen DR-Plan haben, der es Ihnen ermöglicht, Ihre unternehmenskritischen Daten in nur 15 Minuten wiederherzustellen - oder mit anderen Worten, eine 15-minütige RTO zu erreichen. Sie werden ziemlich schnell wieder einsatzbereit sein.

Aber passt Ihr anderer wichtiger Richtwert - Ihr RPO - zum beeindruckenden RTO? Ist Ihr RPO auch auf 15 Minuten eingestellt, oder ist er länger, vielleicht sogar stundenlang? Tatsache ist, dass Ihre 15-minütige Wiederherstellunggszeit Ihnen nicht viel nützt, wenn Ihr RPO 10 Stunden beträgt. Sie könnten keine Daten von Kundenbestellungen wiederherstellen, die während des vorangegangenen 10-Stunden-Fensters aufgegeben wurden, und Sie würden nie erfahren, wer in dieser Zeit welche Ware oder Dienstleistung gekauft hat oder zu welchem Preis.

In diesem Fall gibt es ein ernsthaftes Missverhältnis zwischen Ihrem RPO und RTO. Ja, dieser Unterschied kann während der Betriebszeit eines typischen Arbeitstages verdeckt sein oder unerheblich erscheinen . Aber wenn ein menschlicher Fehler oder eine andere Katastrophe Ihre Systeme zum Einsturz bringt, wird die unangenehme Wahrheit dieses Missverhältnisses aufgedeckt - und Ihr Unternehmen wird den Preis dafür zahlen. (Aber es gibt auch eine Lösung, wie wir zeigen werden.)

4 Was ist ein sicherer Weg, um Ihre SLAs in Müll zu verwandeln? (Tipp: veraltete Technik passt perfekt.)

Nennen Sie es ein verstaubtes Altsystem. Oder ein schrulliges altes Stück Hardware. Oder irgendeine andere Beschreibung für antike Relikte, die Sie sich vorstellen können. Welche Worte Sie auch immer wählen, die alternde Technologie fügt Ihrem Unternehmen ein riesiges Element an Unvorhersehbarkeit hinzu, oft im falschen Moment, genau dann, wenn die Dinge (trügerischerweise) so reibungslos zu laufen scheinen.

Wenn diese alte Technologie verrückt spielt - und Sie gezwungen sind, Ausfallzeiten aufgrund alternder Serverlaufwerke, Netzwerk-Switches oder anderer Schuldiger zu ertragen - werden Sie herausfinden das Sie eine ganze Reihe von Problemen haben. Eines davon könnten Ihre Service Level Agreements (SLAs) sein, die bis zur Grenze der Belastbarkeit gestreckt und vielleicht nicht eingehalten werden.

Das wirkt sich negativ auf Sie und Ihr gesamtes IT-Team aus, egal wie ungerecht die Umstände auch sein mögen. Allzu oft bekommen Technologie-Führungskräfte wie Sie nicht den Anteil des Budgets, den sie für neue Ersatzressourcen benötigen, aber man ist sicher bereit, Ihnen eine ganze Menge Vorwürfe zu machen, wenn Fehler auftreten.

5 Kann etwas so Einfaches wie ein Stromausfall Ihre hochkomplexe IT-Umgebung über den Haufen werfen?

Es ist eine Tatsache: Stromausfälle sind eine wachsende Bedrohung für das heutige Business, wie die Tatsache zeigt, dass sich die Zahl der von Ausfällen betroffenen Personen zwischen 2016 und 2017(10) mehr als verdoppelt hat, wobei die durchschnittliche Dauer eines Ausfalls jetzt 81 Minuten beträgt(11). Und obwohl ein Stromausfall oft der Nebeneffekt bei einer Naturkatastrophe ist (siehe Frage 7), kann es auch ein anderer Vorfall sein, der den Energieversorger und Ihre Organisation im Alleingang zu Fall bringt.

So oder so, Sie werden alle Folgen von Datenverlust und Ausfallzeiten erleben, einschließlich einer, die besonders herausfordernd ist: Die Beherrschung einer komplexen Umgebung, die gleichermaßen (oder ungleich) aus On-Premise, Virtual, Cloud und Hybrid besteht. In diesem Mix wird von Ihnen erwartet, dass Sie mehrere Anbieter, unterschiedliche SLAs, separate Speicher, weitreichende Standorte und abgestufte Datenprioritäten im Griff haben, während Sie gleichzeitig sicherstellen, dass die Wiederherstellung wie geplant durchgeführt wird und das mit weniger zur Verfügung stehenden Zeit und Ressourcen.

Das ist eine große Aufgabe - egal, ob Sie im Dunkeln nach einem Stromausfall arbeiten oder im kühlen Licht eines Rechenzentrums, in dem eine Downtime-Katastrophe eintritt.

6 Wie kann ein Ausfall plötzlich Ihre IT-Zeitpläne und Aktionspläne zerschlagen?

Dinge gehen irgendwann kaputt! Und während Sie vielleicht versucht sind, die Schuld für den Ausfall veralteten IT-Systemen zu geben (siehe Frage 4), ist die Realität, dass jedes Element Ihrer IT-Infrastruktur anfällig für Ausfälle ist, unabhängig davon, wie lange es bereits in Betrieb ist.

Da liegt das Problem bei einem plötzlichen Ausfall - die gelegentlich überraschend auftretende Fehlfunktion. Wir alle haben zahlreiche Beispiele gesehen – wie der berühmte Fall einer Festplatte, die in einem Exchange-Server explodierte(12). Zeugen der Explosion hörten ein krachendes und kratzendes Geräusch vom Server, der sofort die Arbeit einstellte, was zu einer 13-tägigen Unterbrechung des Geschäftsbetriebs führte.

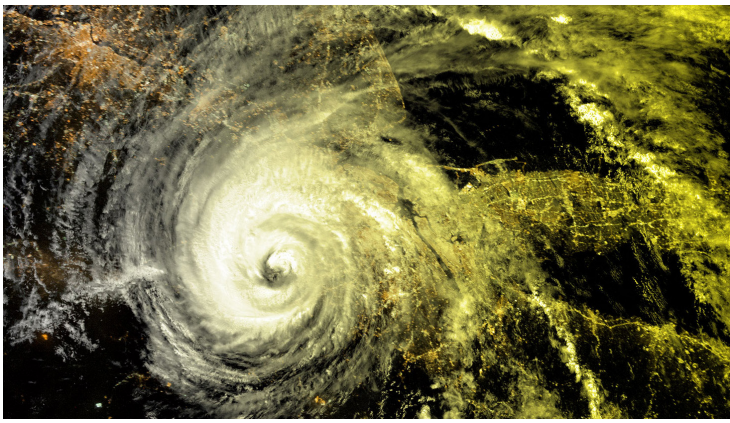
Bei solchen Missgeschicken ist es keine Überraschung, dass die Wiederherstellungsbemühungen einen so großen Teil Ihrer Zeit in Anspruch nehmen. Es ist auch klar, warum es für Sie und Ihre IT-Kollegen so schwierig ist, Verantwortung zu übernehmen und mehrere Brände gleichzeitig zu löschen. Wie können Sie effektiv planen oder arbeiten, wenn ein wichtiger Teil der Hardware kaputt geht und Sie in die improvisierten Zeitpläne des “Recovery-Modus” zwingen, während Sie Ihre dünnen Ressourcen noch mehr strecken?

7 Zu guter Letzt, wird es eine Naturkatastrophe das Ereignis sein, das Ihren Business Continuity-Plan zerstören wird?

Sprechen wir über Ängste - eine Naturkatastrophe ist ein Ereignis, das viele Formen annehmen kann: Hurrikan, Tornado, Erdbeben, Feuer, Überschwemmung oder Erdrutsch(12). Aber in welcher Form auch immer, eine Naturkatastrophe kann Ihre Systeme auslöschen, Ihre Daten unter einer Masse von verdrehten Trümmern vergraben und Ihrem Unternehmen und der lokalen/regionalen Infrastruktur so großen Schaden zufügen, dass eine Wiederherstellung fast unmöglich erscheint.

Schauen Sie sich an, was 2017 geschah, mit dem brutalen Rundschlag der Hurrikane Harvey, Irma und Maria. Oder die lodernden Waldbrände im Westen der USA. Es gibt allen Grund zu der Annahme, dass sich Naturkatastrophen dieser Größenordnung in den kommenden Jahren fortsetzen werden, was es umso dringlicher macht, dass Ihr Unternehmen über einen praktikablen, getesteten Business Continuity-Plan verfügt.

Das Problem ist, dass laut unserer jüngsten Umfrage unter IT-Entscheidern auf der ganzen Welt, mehr als die Hälfte der Befragten keine dieser Pläne haben(14). Und wenn sie einen DR-Plan haben, testen 50% von ihnen ihn viel zu selten - nur einmal im Jahr oder weniger(15). Da ist es kein Wunder, dass weniger als 15% dieser Entscheidungsträger sagten, sie hätten keinerlei Vertrauen in die Wiederherstellung ihrer Daten im Falle eines katastrophalen Datenverlustes(16).



Das ist beängstigend, wenn man bedenkt, dass die nächste Naturkatastrophe die schlimmste von allen sein könnte, die alles auf ihrem Weg zerstört, einschließlich Ihres Plans, es sei denn, Sie sind in der Lage, Abwehrmaßnahmen zu ergreifen, die die Natur selbst überwinden.

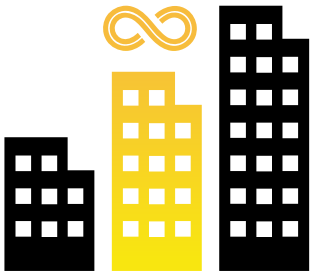
IHRE ANTWORT UM DATENVERLUST ZU BESIEGEN? ALLE SEINE AUSWIRKUNGEN VERMEIDEN.

Fügen Sie “Business, IT und Data Center Retter” zu Ihren beruflichen Erfolgen hinzu.

Wie wir gerade gesehen haben, kann es schwierig sein, mit den heutigen Datenschutzmethoden gegen Datenverlust vorzugehen, insbesondere angesichts der gestiegenen Komplexität, der verschärften Budgetbeschränkungen und der höheren Erwartungen, die Sie auf Schritt und Tritt vorfinden.

Wie setzen Sie in diesem Umfeld effektiv einen Business Continuity-Plan um? Nun, ein wichtiger Schritt ist die Erkenntnis, dass es bei der Lösung nicht unbedingt darum geht, sich von einer Katastrophe zu erholen - es geht darum, die Katastrophe ganz zu verhindern. Sie denken, das ist nicht möglich? Überlegen Sie es sich noch einmal. Erwägen Sie Folgendes:

Geschäfts Kontinuität auf Enterprise-Level ohne Enterpise-Budgets.



Dies ist einer der wichtigsten Bestandteile dieses eBooks. Wir müssen zuerst das Konzept der Vermeidung von IT-Katastrophe verstehen. Anstatt das sprichwörtliche Durcheinander, das Ausfallzeiten mit sich bringen, zu beseitigen, geht es bei der Vermeidung eines IT-Desasters darum, die Auswirkungen von Ausfallzeiten oder Ausfällen aus der Sicht Ihrer Endbenutzer auf eine bloße Störung zu reduzieren - mit völlig vernachlässigbaren Auswirkungen auf Ihr Unternehmen.

Das gute daran, Sie müssen kein riesiges Unternehmen sein, um dies zu erreichen. Während sich früher nur die wohlhabendsten Unternehmen Lösungen mit ununterbrochener Verfügbarkeit und sofortiger Wiederherstellung leisten konnten, kann heute praktisch jede Unternehmensgröße ein IT-Desaster verhindern. Genau richtig, Ihr mittelständisches Unternehmen kann das gleiche Maß an Kontinuität erreichen, ohne das Budget eines Großunternehmens zu haben.

Tatsache ist, dass die richtige Business Continuity-Lösung die Aufgabe für Sie kostengünstig erledigt, indem sie einen Ausfall auf einen harmlose Störung reduziert, ohne dass Sie für komplexe Lösungen zu viel Geld ausgeben müssen und die möglicherweise nicht einmal Ihre SLAs für spezifische Systeme und Anwendungen erfüllen.

Dies ist ein wichtiger Wendepunkt bei der Wiederherstellung, von dem Ihr Unternehmen profitieren kann - und sollte. Wie ist das möglich?

Wir empfehlen einen dreistufige Vorgehensweise, um Katastrophen in Ihrem Unternehmen erfolgreich zu verhindern:

Bereiten Sie sich vor:

Arbeiten Sie mit Ihren verschiedenen Geschäftsbereichen zusammen, um Risikoprofile zu entwickeln.

Die Verhinderung eines IT-Desasters liegt nicht nur in der Verantwortung Ihres IT-Teams. IT-Mitarbeiter müssen mit jedem LOB-Team (Line of Business) zusammenarbeiten, um festzustellen, wo RTOs und RPOs straff kalkuliert sein müssen oder wo es zulässig ist, ältere Backups von Anwendungen wiederherzustellen. Sie sollten so eng wie möglich mit den Geschäftsbereichen zusammenarbeiten , weil eine heutige Investition Probleme später vermeidet.

Konkret müssen Sie Risikoprofile entwickeln, die das Risikoniveau beschreiben, das die verschiedenen Geschäftsbereiche (und Ihr Unternehmen als Ganzes) tolerieren können. Welche Daten sind unternehmenskritisch und müssen sofort wiederhergestellt werden? Was folgt als nächstes? Und darauf? Nur wenn Sie diese Profile erstellen und Systeme und Daten in Prioritätsebenen klassifizieren, werden Sie erkennen welche Wiederherstellung wichtig ist und wie sich das auf Ihren Betrieb auswirkt. Wenn Sie das versäumen kann es die Belastbarkeit Ihres Unternehmens überschreiten.

Während des gesamten Prozesses sollten Sie darauf vorbereitet sein, dass die Geschäftsbereiche unterschiedliche Vorstellungen darüber haben, welche Daten wichtig sind. Tatsächlich kann es zu Konflikten zwischen verschiedenen Geschäftsbereichen kommen, denn es wird Ihnen nur möglich sein es einem Teil davon gleichzeitig recht zu machen - und nur einem Teil von Systemen und Anwendungen gleichzeitig höchste Priorität einzuräumen. Deshalb müssen Sie einen strategischen, übergreifenden Blick auf Ihren Plan werfen, um konkurrierende RTO- und RPO-Anforderungen zu lösen.

Legen Sie Ihre Mission fest:

Etablieren und verstehen Sie Ihre Meßgrößen zur Gewährleistung der Geschäftskontinuität.

Zuerst müssen Sie realistisch gegenüber Ihren SLAs sein. Ihre SLAs können nicht verhindern, dass eine Naturkatastrophe eintritt oder ein besonders cleverer Hacker Ihre Sicherheit knackt. Aber sie stellen eine Richtlinie für Anbieter dar, um einen angemessenen Service anzubieten, und können als Rechtsmittel für Sie dienen, wenn die Leistung unzureichend ist.

Wenn Ihr Team SLAs aushandelt, sollten Sie sich an Ihren Risikoprofilen orientieren. Es ist wichtig zu verstehen, wie Störungen Ihrem Unternehmen schaden können, damit Sie die SLAs nicht über- oder unterbewerten.

Achten Sie als nächstes besonders auf Ihre RPOs. Sie werden in der heutigen IT-Welt oft von den RTOs überschattet, aber sie sind absolut entscheidend für Ihren Erfolg. Wie wir wissen, ist eine schnelle Wiederherstellung immer wünschenswert, aber wenn die Daten zuletzt vor 24 Stunden gesichert wurden, kann das für die Benutzer Ihrer wichtigsten Systeme und Anwendungen wertlos sein.

Angenommen, Sie erwägen eine Business Continuity-Lösung, die eine Wiederherstellung in 15 Minuten garantiert. Alles gut und schön. Aber welche Art von RPO kann erreicht werden um diesen strikten RTO einzuhalten? Können Sie auch 15-Minuten-Recovery-points erreichen, und wenn ja, wie komplex und kostspielig wird es sein, diese zu sichern?

Neue Möglichkeiten erkennen:

Schauen Sie in die Cloud.

Sechzig Prozent aller IT-Arbeitslasten werden bis 2019 (1) in der Cloud laufen, und bis 2020 wird eine unternehmensweite “No-Cloud”-Politik so selten sein wie eine “No-Internet”-Politik heute (2). Wie wir jedoch gesehen haben, verwenden viele Unternehmen weiterhin Non-x86-Plattformen, einschließlich UNIX, HP/UX, AIX, Solaris und andere, um ihre Legacy-Anwendungen zu unterstützen.

Mit diesen multi-generationellen IT-Umgebungen sind Unternehmen mit einem erhöhten Risiko von Datenverlust und längeren Ausfallzeiten konfrontiert, die durch die Lücken im Labyrinth der primären und sekundären Rechenzentren, Cloud-Workloads, Betriebsumgebungen, Disaster Recovery (DR)-Pläne und Kolocationseinrichtungen verursacht werden. Die Einhaltung von SLAs ist oft schwierig und der Schutz jenseits geschäftskritische Anwendungen und Daten wird unrealistisch.

Um diese Risiken zu reduzieren, braucht man mehr als mutige Aussagen über eine neue Ära. Sie benötigen eine Lösung, die speziell dafür entwickelt wurde, Unternehmen dabei zu unterstützen, IT-Katastrophen an jedem Ort, von Ihren Systemen und Ihren Anwendungen, in ihren Gebäuden und in Ihren Clouds zu verhindern.

Zu diesem Zweck sollten Sie Cloud-fähige Lösungen nutzen, die die Benutzerfreundlichkeit eines einzelnen Dienstes mit einer vollständigen Palette von Funktionen kombinieren, um SLAs zu erfüllen und jedes einzelne Byte in Ihrer Infrastruktur vollständig zu schützen. Auf diese Weise können Sie endlich den Knoten der IT des 21. Jahrhunderts entwirren und gleichzeitig RTOs und RPOs unterstützen - von Sekunden bis Stunden.

DER UNTERSCHIED ZWISCHEN IT-KATASTROPHEN UND NEAR-ZERO-DATENVERLUST

Wie bereits erwähnt, besteht der entscheidende Unterschied zwischen der Verhinderung einer IT-Katastrophe und den Aufräumarbeiten danach darin, dass Sie Ihre Risikoprofile bestimmen, Ihre Business Continuity Metriken genau festlegen und alle Prozesse in Ihrer dezentralen, multi-generationellen Infrastruktur mit einer einzigen Lösung optimieren, die flexible RTOs, RPOs und SLAs erfüllen kann.

Die Business Continuity Cloud von Arcserve, die auf einer einheitlichen, Cloud-basierten Verwaltungsoberfläche basiert, ermöglicht es, diese Realität zu erreichen, ohne unerschwinglich oder schwer zu verwalten zu sein. Es wurde für hybride Multi-Cloud-Infrastrukturen entwickelt und umfasst Backup, Disaster Recovery, Hochverfügbarkeit und E-Mail-Archivierung, um Ihre RTOs, RPOs und SLAs zu erfüllen, ohne die Komplexität mit mehreren Anbietern, Tools und Schnittstellen arbeiten zu müssen. Gewinnen Sie Ihre Zeit, die Sie mit der Verwaltung von Backups verbracht haben zurück, mit einer einzigen Lösung, die es Ihnen das ermöglicht:

- **Verhindern Sie Ausfallzeiten** und Datenverluste durch komplexe, generationsübergreifende IT-Infrastrukturen mit integrierten Cloud-nativen, Cloud-basierten und Cloud-fähigen Technologien.
- **Wiederherstellung von SLAs** und Unterstützung von RTOs und RPOs, von Sekunden bis Stunden.
- **Erhöhen Sie die Transparenz** für die Interessenvertreter und gewährleisten Sie die Systemverfügbarkeit durch integrierte erweiterte Tests und Berichte.
- **Sichere Übertragung großer Datenmengen** in die und aus der Cloud ohne Bandbreitenverlust
- **Einfache Skalierung** und Bezahlung nach dem Prinzip des Pay-as-you-grow ohne zusätzliche Tools oder Verwaltungsoberflächen.
- **Unterstützung der Einhaltung von Unternehmens**- und Regulierungsvorschriften durch Vereinfachung der gesetzlichen Offenlegung und Prüfung.
- **Sichern Sie Ihre IT-Transformation** mit Multi-Cloud und Cross-Cloud-Datenschutz.

Als “Backup your back up” bietet Arcserve ein ausgedehntes weltweites Vertriebs- und Supportnetzwerk mit dem Know-how, dem Support und den Ressourcen, die Sie benötigen, um Ihr Unternehmen vollständig vor Daten- und Finanzkatastrophen zu schützen.

Für weitere Informationen besuchen Sie bitte - **arcserve.com/de**.

QUELLEN

[1] http://itic-corp.com/blog/2017/05/hourly-downtime-tops-300k-for-81-of-firms-33-of-enterprises-say-downtime-costs-1m/

[2] http://itic-corp.com/blog/2017/05/hourly-downtime-tops-300k-for-81-of-firms-33-of-enterprises-say-downtime-costs-1m/

[3] https://www.zdnet.com/article/the-nasty-future-of-ransomware-four-ways-the-nightmare-is-about-to-get-even-worse/

[4] https://cybersecurityventures.com/ransomware-damage-report-2017-part-2/

[5] https://businessinsights.bitdefender.com/cyber-attacks-how-much-they-will-cost-you

[6] https://cybersecurityventures.com/ransomware-damage-report-2017-part-2/

[7] https://www.corero.com/blog/846-theft-and-ddos-attacks-go-hand-in-hand.html

[8] https://ehrintelligence.com/news/jones-memorial-recovers-from-ehr-downtime-due-to-cyberattack

[9] https://www.healthcareitnews.com/news/patient-safety-jeopardized-ehr-downtime-jamia-says#gs.9vbtaEQ

[10] https://switchon.eaton.com/blackout-tracker

[11] https://switchon.eaton.com/blackout-tracker

[12] http://outlookpower.com/article/my-thirteen-days-in-exchange-hell/

[13] https://www.zdnet.com/article/diy-it-guide-to-disaster-preparedness-because-its-always-something/

[14] https://s13937.pcdn.co/wp-content/uploads/2018/03/WBD-Survey-Results-Infographic-v2.pdf

[15] https://s13937.pcdn.co/wp-content/uploads/2018/03/WBD-Survey-Results-Infographic-v2.pdf

[16] https://s13937.pcdn.co/wp-content/uploads/2018/03/WBD-Survey-Results-Infographic-v2.pdf