arcserve®

WHITE PAPER

Zehn Tipps bei der Planung von Disaster Recovery und Business Continuity

Business Continuity – also die Planung, Vorbereitung und Implementierung ausfallsicherer Geschäftssysteme, um gegen unvorhergesehene Ausfallzeiten gewappnet zu sein, wird häufig als IT-Problem betrachtet. Deshalb überlassen es die meisten Unternehmen auch der IT-Abteilung, eine Lösung dafür zu finden. Das führt zwangsläufig zum Einsatz verschiedener taktischer Lösungen ohne eine maßgebliche Gesamtstrategie, die eine gemeinsame Richtung vorgibt. In Wirklichkeit ist die Business Continuity, so wie es der Begriff schon andeutet, ein Problem, das das gesamte Unternehmen betrifft und daher auch als Ganzes und von allen Benutzern und nicht nur von den Systemadministratoren angegangen werden sollte.

Wie können Sie herausfinden, ob Ihr aktueller Plan für die Business Continuity solide ist? Hier ist eine kleine Checkliste für Sie.

- Erfordert Ihr Plan erhebliches manuelles Eingreifen?
- Nehmen Sie bei Ihrem Plan einen Datenverlust bei kritischen Systemen von mehr als ein paar Sekunden in Kauf?
- Kann der Zugang zu kritischen Systemen in wenigen Minuten wiederhergestellt werden?
- Setzen Sie eine aktuelle Technologie bei Ihren Backup- und Wiederherstellungslösungen ein, die Ihren Plan für die Business Continuity unterstützen?

Wenn Sie auf eine dieser Fragen mit Nein geantwortet haben, ist das Risiko hoch, dass Datenverluste und Ausfallzeiten für das Unternehmen drohen.

Alle sprechen darüber, wie Disaster Recovery richtig geht. Aber man sollte auch ein Auge darauf haben, was passieren kann, wenn Disaster Recovery nicht richtig durchgeführt wird. Deshalb haben wir die Top 10 Tips zusammengestellt, um Sie in Ihrer Planung und Entscheidungsfindung zu unterstützen.

1. Das Geschäft im Mittelpunkt – und nicht die Technologie

Sie sollten immer im Blick behalten, dass es bei der Disaster Recovery darum geht, eine geschäftliche Anforderung zu erfüllen. Deshalb müssen den Überlegungen auch geschäftliche Anforderungen zugrunde gelegt werden. Bevor Sie versuchen herauszufinden, wie Sie Disaster Recovery implementieren sollten, müssen Sie nach dem „Warum" fragen. Sprechen Sie mit Führungsverantwortlichen in Ihrem Unternehmen, um zu verstehen, was für sie wichtig ist. Sie können nur wissen, welche Systeme die wichtigsten sind, wenn Sie die Anwender im Unternehmen fragen. Wenn Sie die Anforderungen des Unternehmens verstehen, können Sie entsprechende Prioritäten festlegen, die Sie zudem bei der Auswahl der Technologie unterstützen.

2. Es kann eine Katastrophe sein – muss aber nicht

Wenn Sie an Disaster Recovery denken, haben Sie wahrscheinlich Wirbelstürme, Überschwemmungen, Terrorangriffe und Ähnliches vor Augen, nicht aber, dass ein Software-Upgrade schief geht oder dass ein Hardwarefehler in einer kritischen Netzwerkkomponente auftritt. Normalerweise wird für ein Worst-Case-Szenario geplant, aber man stolpert über die trivialen alltäglichen Fehler. Bei Ihrer Planung müssen Sie alle Eventualitäten berücksichtigen – vom alltäglichen bis zum katastrophalen Ereignis.

3. Wie können Sie Budgets verteilen, ohne die Kosten für Ausfälle zu kennen?

Allzu oft weisen Unternehmen ein Budget für die Disaster Recovery-Planung zu, bevor sie überhaupt das finanzielle Risiko von Ausfallzeiten und Datenverlusten für das Unternehmen ermittelt haben. Beziffern Sie zuerst, wie viel Geld Sie durch einen Ausfall kritischer Systeme verlieren würden, erst dann können Sie ermitteln, wie viel Sie ausgeben sollten, um diese Verluste zu verhindern. Ihr Budget richtet sich also nach den potentiellen Kosten eines Ausfalls. Denken Sie daran, bei Ihren Kostenberechnungen für Ausfallzeiten auch die Einhaltung von rechtlichen Vorschriften zu berücksichtigen. Oft wird die Nichterfüllung gesetzlicher Verpflichtungen mit Geldstrafen belegt.

4. Thema Risikobewertung

Was als Katastrophenfall bzw. Disaster gilt, kann von Unternehmen zu Unternehmen und selbst von Abteilung zu Abteilung variieren. Einige Ereignisse, beispielsweise Erdbeben, können so katastrophale Folgen haben, dass sich das Unternehmen ganz offensichtlich schützen muss. Andere Ereignisse scheinen zunächst nichts Besonderes zu sein, z. B. eine ausgefallene Netzwerkhardware. Dennoch können sie enorme finanzielle Auswirkungen haben. Wenn Sie an Disaster Recovery denken, sollten Sie sich unbedingt folgende Fragen stellen: Wogegen sollen wir uns schützen? Übersehen Sie auch das augenscheinlich Banale nicht. Geringfügige Verluste aufgrund alltäglicher Probleme können sich schnell summieren.

5. Haben Sie einen Plan?

Wenn Ihr Disaster Recovery-Plan nichts weiter als eine Haftnotiz auf den Backup-Bändern unter dem Bett Ihres Systemadministrators ist, haben Sie ein Problem. Es klingt zwar erstaunlich, aber eine überraschend große Anzahl Unternehmen verfügt über gar keinen Disaster Recovery-Plan. Wichtig ist, dass Sie ein formales Dokument ausarbeiten, in dem alle Anwendungen, Hardware, Anlagen, Service Provider, Mitarbeiter und Prioritäten aufgeführt sind. Und Sie müssen von allen Stakeholdern im Unternehmen entsprechende Unterstützung einholen. Der Plan muss alle funktionalen Bereiche umfassen und klare Richtlinien dahingehend enthalten, was vor, während und nach einem Notfall zu geschehen hat.

6. Wir haben einen Plan, aber den haben wir nie getestet

Ein Disaster Recovery-Plan ist nur dann sinnvoll, wenn er auch funktioniert. Und dies lässt sich nur sicherstellen, indem Sie ihn testen. Den Plan unter simulierten Notfallbedingungen zu testen, ist zwar wichtig, kann aber auch eine Herausforderung darstellen. Disaster Recovery-Tests sind kostspielig und ziehen wichtige Zeit- und Personalressourcen aus dem Tagesbetrieb ab. Es bleibt aber dabei: Ohne vollständig auf Anwendungsebene getestete Wiederherstellung stehen Sie bei einem echten Notfall vor einem Problem. Halten Sie Ausschau nach Datensicherungslösungen, die es Ihnen ermöglichen, Umgebungen für unterbrechungsfreies Testing Ihrer Disaster Recovery-Pläne einzurichten.

7. Wer ist für was verantwortlich?

Ein echtes Notfallereignis läuft immer chaotisch ab und stiftet viel Verwirrung. Wenn die wichtigen Mitarbeiter nicht wissen, welche Zuständigkeiten sie im Notfall haben, dauert die Wiederherstellung unnötig lange und geht mit zahlreichen Schwierigkeiten einher. In Ihrem Disaster Recovery-Plan müssen die Rollen und Verantwortlichkeiten jeder beteiligten Person klar dargelegt sein. Dies beinhaltet auch, was zu tun ist, wenn die zuständigen Mitarbeiter nicht verfügbar sind. Diese Personen sollten außerdem an den Tests Ihres Disaster Recovery-Plans beteiligt werden.

8. Was ist RPO? Und was ist RTO?

Es werden zwei Messgrößen verwendet, um die Toleranz einer Anwendung bezüglich Ausfallzeit und Datenverlust zu messen: Recovery Point Objective (RPO) und Recovery Time Objective (RTO). RPO ist ein Messwert für Datenverlust. Je größer der RPO, desto mehr Datenverlust wird von jeder Anwendung toleriert, bevor es für das Unternehmen problematisch wird. Stellen Sie ihn sich als Zeitpunkt vor, bis zu dem Sie Daten erfolgreich wiederherstellen können. Alle Daten zwischen diesem Punkt und dem Eintritt des Notfalls sind verloren. RTO ist ein Messwert für die Zeitdauer

der Wiederherstellung. Je geringer der RTO, desto schneller muß die Anwendung wiederhergestellt sein, bevor das Unternehmen bedeutende Verluste erleidet. Wenn Sie RPO und RTO nicht für jede Anwendung kennen, werden Sie bei der Disaster Recovery im Dunkeln tappen. Mit RPO und RTO können Sie Service Level definieren, an denen Sie gemessen werden können.

9. Die Wiederherstellung dauert länger als Sie denken

Es ist wichtig zu wissen, wie lange die Wiederherstellung grundlegender Geschäftssysteme dauern wird. Auch wenn Sie auf ausgelagerte Backup-Kopien zugreifen können, heißt dies nicht, dass Sie die Anwendungen rechtzeitig wiederherstellen können. Können Sie Daten schnell genug wiederherstellen und Systeme schnell genug wieder bereitstellen, um den Anforderungen der Anwender in Unternehmen gerecht zu werden? Verfügen Sie über ausreichend Bandbreite, um Daten von einem Cloud Service Provider zurückzuspielen? Wenn Sie wissen, wie lange die Wiederherstellung von Anwendungen dauert und welche Folgen der Ausfall für das Unternehmen hat, entscheiden Sie sich vielleicht für eine andere Technologie.

10. Zurück zur Normalität

Bei der Disaster Recovery-Planung wird eine Komponente häufig vernachlässigt: die Rückkehr zum Produktionssystem nach einem Failover zu einem Notfallstandort. Der Grund liegt auf der Hand. Wenn wir an einen Notfall denken, geht es uns dabei primär darum, unsere wertvollen Assets zu schützen. Wenig Gedanken machen wir uns darüber, was mit diesen Assets passiert, nachdem das Notfallereignis vorbei ist. Die Fähigkeit des Failback zu den Produktionssystemen ist ebenso wichtig wie die Fähigkeit zum Failover. Sofern es nicht sorgfältig geplant wurde, verfügt ein Backup-Rechenzentrum voraussichtlich nicht über dieselbe Kapazität oder Performance wie der Produktionsstandort. Ohne Failback-Plan führen Sie zwar vielleicht einen erfolgreichen ersten Failover durch, fahren dann aber zunehmend Verluste ein, wenn Ihr Unternehmen seinen Betrieb wochenlang auf der Basis eines unzulänglich provisionierten Backup-Standorts aufrechterhalten muss.

Ausfallzeiten und Datenverluste gehören für jedes Unternehmen, das sich auf IT stützt, zum Geschäftsrisiko dazu. Wie dieses Risiko mit der richtigen Technologie abgefangen werden kann, sollte bereits ganz früh in der Softwareentwicklung- und bei der Bereitstellung überlegt werden. Wenn Sie das von jeder Anwendung benötigte Schutzlevel kennen, können Sie auch die entsprechenden Ressourcen zuweisen. Sobald eine Anwendung von den Anwendern im Unternehmen produktiv genutzt wird, müssen die zugehörigen RPO- und RTO-Werte klar identifiziert und die richtigen Business Continuity-Lösungen implementiert werden, um im Falle eines Ausfalls eine Wiederherstellung garantieren zu können.

Arcserve® Unified Data Protection

Seit über 20 Jahren bietet Arcserve Unternehmen in aller Welt Schutz mit null Ausfallzeit. Mit Arcserve Unified Data Protection (UDP) steht eine Komplettlösung für all Ihre Anforderungen im Bereich Datensicherung und Hochverfügbarkeit bereit. Mit einer zentralisierten Steuerung vereinheitlicht Arcserve UDP Backup, Snapshot, Replikation und Deduplikation für Ihre virtuellen und physischen Anwendungen sowie für On-Premise- und Cloud-basierte Anwendungen. Arcserve UDP Assured Recovery™ bietet einen umfassenden Testprozess zur Vorbereitung auf den Notfall in Echtzeit, mit dem Sie Business Continuity-Pläne prüfen können, ohne dass Ihr Geschäftsbetrieb unterbrochen wird. Weitere Informationen finden Sie unter **www.arcserve.com/de**.

arcserve®
assured recovery™

Copyright© 2015 Arcserve (USA), LLC sowie Tochtergesellschaften und Niederlassungen. Alle Rechte vorbehalten. Alle erwähnten Markenzeichen, Markennamen, Dienstleistungsmarken und Firmenlogos, auf die hier verwiesen wird, sind Eigentum der jeweiligen Inhaber. Dieses Dokument dient ausschließlich zu Informationszwecken. Arcserve übernimmt keine Haftung für die Richtigkeit oder Vollständigkeit der Informationen. Soweit nach anwendbarem Recht erlaubt, stellt Arcserve dieses Dokument im vorliegenden Zustand ohne jegliche Gewährleistung zur Verfügung; dazu gehören insbesondere stillschweigende Gewährleistungen der Marktauglichkeit, der Eignung für einen bestimmten Zweck und der Nichtverletzung von Rechten Dritter. In keinem Fall haftet Arcserve für Verluste oder unmittelbare oder mittelbare Schäden, die aus der Verwendung dieses Dokuments entstehen; dazu gehören insbesondere entgangene Gewinne, Betriebsunterbrechung, Verlust von Goodwill oder Daten, selbst wenn Arcserve über die Möglichkeit solcher Schäden im Voraus informiert wurde.