Disaster Recovery

= Planung, Vorbereitung und Implementierung ausfallsicherer Geschäftssysteme, um gegen unvorhergesehene Ausfallzeiten gewappnet zu sein

Ist meine Business Continuity solide genug?

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

Disaster Recovery

= Planung, Vorbereitung und Implementierung ausfallsicherer Geschäftssysteme, um gegen unvorhergesehene Ausfallzeiten gewappnet zu sein

---

Wenn Sie auf eine dieser Fragen mit **Nein** geantwortet haben, bzw. die Ausfallzeiten zu lange sind, 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.

Top 10 Tips, um Sie in Ihrer Planung und Entscheidungsfindung bei ihrem DSP zu unterstützen.

Disaster Recovery

= Planung, Vorbereitung und Implementierung ausfallsicherer Geschäftssysteme, um gegen unvorhergesehene Ausfallzeiten gewappnet zu sein

1. Das Geschäft im Mittelpunkt – und nicht die Technologie

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.

Disaster Recovery

= Planung, Vorbereitung und Implementierung ausfallsicherer Geschäftssysteme, um gegen unvorhergesehene Ausfallzeiten gewappnet zu sein

2. Es kann eine Katastrophe sein – muss es aber nicht

Bei Ihrer Planung müssen Sie alle Eventualitäten berücksichtigen – vom alltäglichen bis zum katastrophalen Ereignis.

Wirbelstürme, Überschwemmungen, Terrorangriff sind eher unwahrscheinlich

Hardwarefehler in einer kritischen Komponente wie RAID-Controller oder Firmware schon eher

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

Das finanzielle Risiko von Ausfallzeiten und Datenverlusten für das Unternehmen/Kanzlei vorab ermitteln und erst dann Budget zuweisen. 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.

4. Thema Risikobewertung

Stellen Sie sich unbedingt folgende Fragen?

Was als Katastrophenfall bzw. Disaster gilt, kann in anderen Unternehmen und selbst von anderer Abteilung andere Risikobewertung haben.

Wogegen sollen wir uns schützen? Übersehen Sie auch das augenscheinlich Banale nicht. Geringfügige Verluste aufgrund alltäglicher Probleme können sich schnell summieren.

Disaster Recovery

= Planung, Vorbereitung und Implementierung ausfallsicherer Geschäftssysteme, um gegen unvorhergesehene Ausfallzeiten gewappnet zu sein

5. Haben Sie einen Plan?

Ist Ihr Systemadministrator derjenige welcher den Recovery-Plan als

„Postit unter seinem Bett auf Ihren Sicherungsbändern“ kennt?

Wer und vor allem wie viele ist/sind in diesen Prozess involviert?

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

Den Plan unter simulierten Notfallbedingungen zu testen, ist zwar wichtig, kann aber auch eine Herausforderung darstellen.

Disaster Recovery-Tests sind oft teuer 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.**

7. Wer ist für was verantwortlich?

Wenn die Zuständigkeiten der „wichtigen“ Mitarbeiter nicht geklärt sind und sie im Notfall nicht wissen was Sie zu tun 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**. Die Personen sollten außerdem an den Tests Ihres Disaster Recovery-Plans beteiligt werden.

8. Was ist RPO? Und was ist RTO?

RPO = **R**ecovery **P**oint **O**bjective ist ein Messwert für Datenverlust.

Je größer der RPO, desto mehr Datenverlust wird von jeder Anwendung toleriert, bevor es für das Unternehmen problematisch wird.

RTO = **R**ecovery **T**ime **O**bjective ist ein Messwert für die Zeitdauer.
Zeit der Wiederherstellung. Je geringer der RTO, desto schneller muß die Anwendung wiederhergestellt sein, bevor das Unternehmen bedeutende Verluste erleidet.

Kennen Sie <u>Ihre</u> RPO und Ihre RTO für <u>Ihre</u> Anwendungen?

9. Wiederherstellung der Anwendungen bzw. Daten dauert länger als Sie denken

Haben Sie bei Ihrem Plan berücksichtigt, dass es einen Unterschied zwischen Anwendungs-und Datenwiederherstellung geben kann?

Bedenken Sie, dass bei OnlineBackup Lösungen Ihre dazu verfügbare Bandbreite.

Wenn Sie wissen, wie lange die Wiederherstellung von Anwendungen dauert und welche Folgen der Ausfall für das Unternehmen hat, entscheiden Sie sich vielleicht doch für eine andere bzw. zusätzliche Technologie.

10. Zurück zur Normalität

Die Fähigkeit des Failback (zurück zum Produktivsystem) zu den Produktionssystemen ist ebenso wichtig wie die Fähigkeit zum Failover. Sofern es nicht sorgfältig geplant wurde, verfügt ein Backup-Rechenzentrum ein Backup Server (z.B. Replica) voraussichtlich nicht über dieselbe Kapazität oder Performance wie der Produktionsstandort.

OhneFailback-Plan führen Sie zwar vielleicht einen erfolgreichen ersten Failover durch, Wolle Sie Ihr Unternehmen wochenlang auf der Basis eines unzulänglich provisionierten Backup-Standorts bzw. Backup-Systems aufrechterhalten?

Disaster Recovery

= Planung, Vorbereitung und Implementierung ausfallsicherer Geschäftssysteme, um gegen unvorhergesehene Ausfallzeiten gewappnet zu sein

Eine allzeit gültige Regel, mit der Sie in beliebigen Ausfallszenarios vor Datenverlust geschützt sind, ist die **3-2-1-Regel** der Datensicherung. Sie liefert zugleich auch die Antwort auf zwei wichtige Fragen:

Wie viele Backup-Dateien sollten erstellt und wo sollten diese aufbewahrt werden?

Disaster Recovery

= Planung, Vorbereitung und Implementierung ausfallsicherer Geschäftssysteme, um gegen unvorhergesehene Ausfallzeiten gewappnet zu sein

Die 3-2-1-Regel wurde von dem bekannten Fotografen Peter Krogh geprägt, demzufolge es zwei Gruppen von Menschen gibt: Menschen, die bereits von einem Speicherausfall betroffen waren, und Menschen, denen ein solcher Ausfall noch bevorsteht.

Die 3-2-1-Regel der Datensicherung besagt:

+ es sollten mindestens **drei** Kopien Ihrer Daten vorhanden sein

+ speichern Sie die Kopien auf **zwei** unterschiedlichen Medien

+ bewahren Sie **eine Backup-Kopie an einem externen Speicherort**