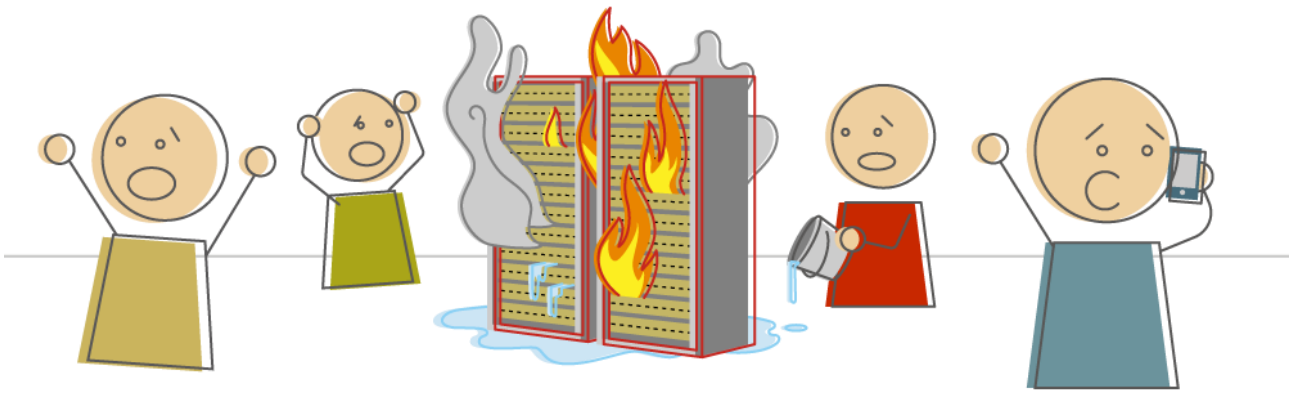
Richtlinien für Disaster Recovery

UNTERNEHMENSKRITISCHE PROZESSE SCHÜTZEN

Wien, im September 2021

Ausfallzeiten und Datenverluste gehören für jedes Unternehmen zum Geschäftsrisiko. Dieses Risiko muss mit der richtigen Technologie abgefangen werden, egal in welcher Form eine Organisation Informationstechnologie einsetzt. Ein wichtiger Begriff dabei lautet Disaster Recovery. Wie dieser Begriff mit der sogenannten Business Continuity zusammenhängt und was bei der der Vorbereitung von Disaster Recovery zu beachten ist, fassen wir in diesem Dokument zusammen.



Disaster Recovery bezeichnet jene Maßnahmen, die nach einem Ausfall von kritischen IT-Komponenten eingeleitet werden. Dazu zählt sowohl die Datenwiederherstellung als auch das Ersetzen nicht mehr benutzbarer Infrastruktur. Die Ursache, das „Disaster", kann vielfältiger Natur sein – ein Brand, ein Erdbeben, ein Wasserschaden, ein Terroranschlag bis hin zu technischen Gebrechen, menschlichem Versagen oder Verschlüsselungen durch Ransomware.

Die Wiederherstellung durch Disaster Recovery ist eine zentrale Grundlage für die reibungslose Fortsetzung des Geschäftsbetriebs, also der Business Continuity. Allerdings stammt daher die häufige Fehleinschätzung, dass auch Business Continuity als reines IT-Problem betrachtet wird. Man geht davon aus, dass es Sache der IT-Abteilung ist, sich um die Planung, Vorbereitung und Implementierung ausfallsicherer Geschäftssysteme zu kümmern. Deshalb überlassen es die meisten Unternehmen der IT-Abteilung, Maßnahmen gegen unvorhergesehene Ausfallzeiten zu setzen. Das führt zwangsläufig zu verschiedenen taktischen Ansätzen ohne eine maßgebliche Gesamtstrategie. Eine gemeinsame, unternehmensweite Richtung fehlt. Das Ergebnis ist dann oft unbefriedigend, denn Business Continuity ist eine Anforderung, die das gesamte Unternehmen betrifft.

Business Continuity muss ganzheitlich, also von allen Beteiligten und nicht nur von Systemadministratoren angegangen werden.

IST IHR BUSINESS CONTINUITY MANAGEMENT SOLIDE?

Bevor wir näher auf Disaster Recovery eingehen, möchten wir hier ganz deutlich auf dessen Zweck, nämlich Business Continuity, hinweisen. Unter Business Continuity versteht man die unterbrechungsfreie Weiterführung des Geschäftsbetriebs auch im Krisenfall. Manche Unternehmen beschäftigen sich überhaupt nicht mit diesem Thema, andere haben zumindest einen Plan und im Enterprise-Bereich gibt es so gut wie immer ein Konzept dafür. Um zu überprüfen, ob das Business Continuity Management Ihres Betriebs nicht nur etabliert, sondern auch solide ist, beantworten Sie einfach die folgenden Fragen:

- *Gibt es in Ihrem Unternehmen ein definiertes Business Continuity Management (BCM)?*
- *Erfordert Ihr BCM erhebliches manuelles Eingreifen?*
- *Nehmen Sie mit Ihrem BCM bei kritischen IT-Systemen einen Datenverlust von mehr als ein paar Sekunden in Kauf?*
- *Gewährleistet Ihr BCM, dass der Zugang zu kritischen IT-Systemen in wenigen Minuten wiederhergestellt wird?*
- *Beinhaltet Ihr BCM den Einsatz von aktueller Technologie bei Ihren Backup- und Recovery-Lösungen?*

Wenn Sie auch nur eine dieser Fragen mit „Nein“ beantworten, ist das Risiko Ihres Unternehmens hoch. Im Krisenfall drohen teure Ausfallzeiten und empfindliche Datenverluste.

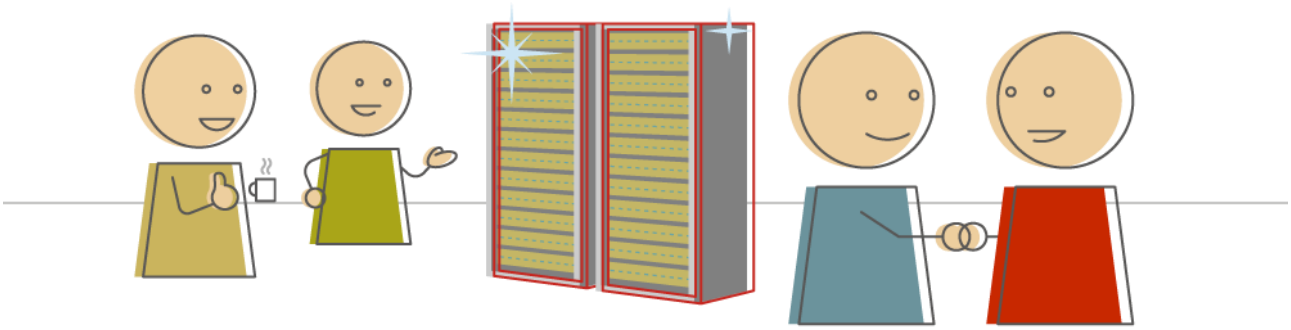
RICHTLINIEN FÜR WIRKUNGSVOLLES DISASTER RECOVERY

Wie im vorangehenden Abschnitt ausgeführt, ist Business Continuity kein reines IT-Problem. Daher kann auch Disaster Recovery nicht als isoliertes IT-Problem betrachtet werden. Obwohl sich Disaster Recovery auf die Wiederherstellung von IT-Infrastruktur bezieht, muss es den Anforderungen der Business Continuity gerecht werden. Dieser Grundgedanke kommt in den nachfolgenden Richtlinien für die Vorbereitung eines wirkungsvollen Disaster Recovery zum Ausdruck.

1. Das Business steht im Mittelpunkt, nicht die Technologie

Sie sollten immer im Blick behalten, dass es bei 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, nach den Anforderungen aus der Business Continuity. 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 Stakeholder im Unternehmen einbeziehen. Erst wenn Sie die Anforderungen aus kommerzieller Sicht verstehen, können Sie entsprechende Prioritäten festlegen. In der Folge wird es auch einfacher, die passenden Technologien auszuwählen.



2. Auch kleine Fehler können in Katastrophen münden

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. Die Erfahrung zeigt: Geplant wird für Worst-Case-Szenarios, tatsächlich gestolpert wird über triviale, alltägliche Fehler. Bei Ihrer Planung müssen Sie daher alle Eventualitäten berücksichtigen – vom alltäglichen bis zum monumentalen Ereignis.

3. Das finanzielle Risiko sollte das Budget bestimmen

Allzu oft wird der Disaster Recovery-Planung ein Budget zugewiesen, noch bevor überhaupt das finanzielle Risiko von Ausfallzeiten und Datenverlusten für das Unternehmen ermittelt wurde. Beziffern Sie also zuerst, was ein Ausfall kritischer Systeme Ihrem Unternehmen kosten würde. Dann können Sie ermitteln, wie viel Sie ausgeben sollten, um diese Verluste zu verhindern. Kurz gesagt, Ihr Budget sollte sich nach den potenziellen Kosten eines Ausfalls richten. 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. Führen Sie eine Risikobewertung durch

Was als Katastrophenfall gilt, kann von Unternehmen zu Unternehmen und selbst von Abteilung zu Abteilung variieren. Einige Ereignisse, beispielsweise Erdbeben, können so katastrophale Folgen haben, dass sich die Organisation ganz offensichtlich davor schützen muss. Andere Ereignisse scheinen zunächst nichts Besonderes zu sein, wie zum Beispiel eine ausgefallene Netzwerkkomponente. Dennoch können sie enorme finanzielle Auswirkungen haben. Wenn Sie an Disaster Recovery denken, sollten Sie sich unbedingt folgende Frage stellen:

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

5. Erstellen 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 und deren Anforderungen an die Business Continuity erfüllen. Der Plan muss alle funktionalen Bereiche umfassen und klare Richtlinien dahingehend enthalten, was vor, während und nach einem Notfall zu geschehen hat. Beziehen Sie in Ihren Plan auch externe Dienstleister ein, wie zum Beispiel Ihren Cloud-Service Provider.

6. Testen Sie Ihren Plan

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. Falls Sie Ihre Backups in einer Private Cloud angelegt haben, muss auch das Cloud-Service unbedingt in die Tests einbezogen werden. Ein Tipp am Rande: Halten Sie Ausschau nach Datensicherungslösungen, die es Ihnen ermöglichen, Umgebungen für unterbrechungsfreies Testing Ihrer Disaster Recovery-Pläne einzurichten.

7. Definieren Sie die Verantwortungen

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 in die Tests Ihres Disaster Recovery-Plans eingebunden werden.

8. Definieren Sie die Messgrößen RPO und RTO

In der Praxis 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 den 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. Bedenken Sie, dass der RTO bei einer Cloud Backup Lösung durch die verfügbaren Bandbreiten limitiert sein kann. 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 die Wirksamkeit Ihrer Maßnahmen gemessen werden kann.

9. Gehen Sie von realistischen Recovery-Zeiten aus

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. Stellen Sie sich folgende Fragen: Können Sie die Daten schnell genug wiederherstellen? Können Sie die Systeme schnell genug wieder bereitstellen, um den Anforderungen der Anwender im Unternehmen gerecht zu werden? Verfügen Sie über ausreichend Bandbreite, um die Daten von einem Cloud Service Provider zurückzuspielen? Wenn Sie herausfinden, dass die Wiederherstellung von Anwendungen zu lange dauert, können Sie ggf. die eingesetzte Technologie erneuern.

10. Zurück zur Normalität

Ein Faktor wird bei der Disaster Recovery-Planung häufig vernachlässigt, nämlich die Rückkehr zum Produktionssystem nach einem Failover zu einem Notfallstandort. Der Grund liegt auf der Hand: Wer an einen Notfall denkt, möchte primär wertvolle Assets schützen. Wenig Gedanken macht man sich darüber, was mit diesen Assets passiert, nachdem das Notfallereignis vorbei ist. Dabei ist die Fähigkeit des Failback zu den Produktionssystemen ebenso wichtig wie die Fähigkeit zum Failover. Backup-Rechenzentren verfügen nur selten über dieselbe Kapazität oder Performance wie der Produktionsstandort. Ohne Failback-Plan führen Sie zwar vielleicht ein erfolgreiches erstes Failover durch. Anschließend fahren Sie aber empfindliche Verluste ein, wenn Ihr Unternehmen seinen Betrieb wochenlang auf der Basis eines unterdimensionierten Backup-Standorts aufrechterhalten muss.

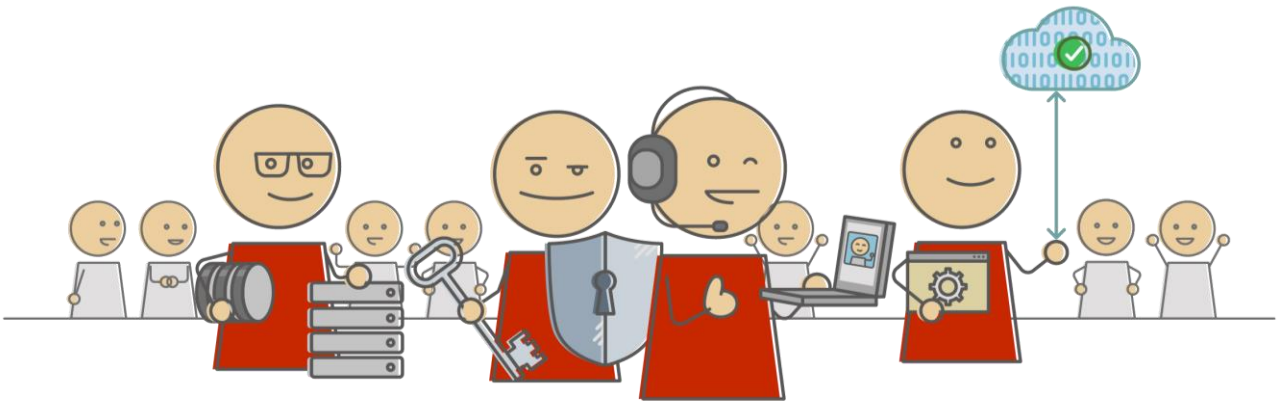
NÜTZEN SIE UNSERE ERFAHRUNGEN

Wenn Disaster Recovery in Ihrem Unternehmen noch nicht ausreichend vorbereitet ist, brauchen Sie das Rad nicht neu zu erfinden. Wir teilen mit Ihnen gerne die langjährigen Erfahrungen, die wir mit unseren Auftraggebern in zahlreichen Projekten sammeln konnten. Bitte wenden Sie sich bei Interesse an den Autor dieses Dokuments oder an einen der d-con.net Systems Engineers. Wir helfen Ihnen gerne weiter.

Zum Autor: *Günther Klement ist CSO bei d-con.net und verfügt über jahrzehntelange technisch-organisatorische Erfahrungen im IT-Sektor. Der Aufbau von IT-Teams und Lösungen sowie die Etablierung von Services gehören beruflich seit vielen Jahren zu seinem täglichen Brot. Günther Klement berät die Kunden von d-con.net unter anderem bei der Definition passender IT-Services.*

guenther.klement@d-con.net
d-con.net GmbH
Johannesstraße 50, AT-2371 Hinterbrühl
+43 (1) 616 32 17 – 0

d-con.net ist ein strategisches Asset



d-con.net ist ein strategischer Dienstleistungspartner. Wir arbeiten laufend daran, unseren Auftraggebern Hochtechnologie zu erschließen und in Best Practices IT-Lösungen verfügbar zu machen. Bei uns erhält man hochmoderne Systeme und leistungsfähige Managed Services, immer am Puls der Zeit. Da unsere Auftraggeber oft international agierende Unternehmen sind, werden unsere Kunden rund um den Globus in ihren Landesniederlassungen auf allen Kontinenten unterstützt.