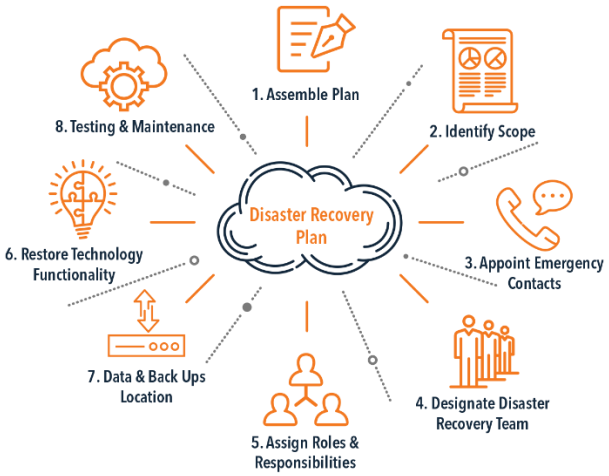

Version 1.4
5. März 2021

conus

www.conus.at

DISASTER RECOVERY IM IT BEREICH AND BUSINESS CONTINUITY

EIN GRUNDSÄTZLICHER LEITFADEN FÜR UNTERNEHMEN, ADMINISTRATOREN UND MITARBEITER

Herangehensweise vor dem Fall der Fälle

PRODUKTLINK: http://www.conus.at/index_htm_files/disaster_recovery.pdf

CONUS GmbH.
Kirchstetterngasse 47
1160 Wien
info@conus.at
+41 (0) 1 617 51 44 - 0

DEFINITIONEN

„**Disaster Recovery**“ (DSR) bezeichnet Maßnahmen, die nach einem Ausfall von Komponenten in der IT eingeleitet werden. Dazu zählt sowohl die Datenwiederherstellung als auch das Ersetzen nicht mehr benutzbarer Infrastruktur, Hardware und Organisation. Umfassender als *Disaster Recovery* ist der Begriff Business Continuity, der nicht die Wiederherstellung der IT-Dienste, sondern unterbrechungsfreie Geschäftsabläufe in den Vordergrund stellt.

Bei der Beurteilung einer Disaster-Recovery-Lösung sind folgende Punkte einer Business Impact Analyse zu beachten:

1. **Recovery Time Objective (RTO):** Wie lange darf ein Geschäftsprozess/System ausfallen? Bei der Recovery Time Objective handelt es sich um die Zeit, die vom Zeitpunkt des Schadens bis zur vollständigen Wiederherstellung der Geschäftsprozesse (Wiederherstellung von: Infrastruktur – Daten – Nacharbeitung von Daten – Wiederaufnahme der Aktivitäten) vergehen darf. Der Zeitraum kann hier von 0 Minuten (Systeme müssen sofort verfügbar sein), bis mehrere Tage (in Einzelfällen Wochen) betragen.
2. **Recovery Point Objective (RPO):** Wie viel Datenverlust kann in Kauf genommen werden? Bei der Recovery Point Objective handelt es sich um den Zeitraum, der zwischen zwei Datensicherungen liegen darf, das heißt, wie viele Daten/Transaktionen dürfen zwischen der letzten Sicherung und dem Systemausfall höchstens verloren gehen. Wenn kein Datenverlust hinnehmbar ist, beträgt die *RPO* 0 Sekunden.

Die Planung und Umsetzung eines funktionierender DSR ist je nach Größe der IT aufwändig und mit erheblichen Kosten verbunden. Somit sollte er im IT Budget vorgesehen werden.

Das **Business Continuity Management** ist die Organisationseinheit eines Unternehmens, die den Aufbau und Betrieb eines leistungsfähigen Notfall- und Krisenmanagements zwecks systematischer Vorbereitung auf die Bewältigung von Schadenereignissen bearbeitet. Dadurch soll erreicht werden, dass wichtige Geschäftsprozesse selbst in kritischen Situationen und in Notfällen nicht oder nur temporär unterbrochen werden und die wirtschaftliche Existenz des Unternehmens trotz Schadenereignis gesichert bleibt.

Ziel des Business-Continuity-Managements ist die Generierung und Proklamation von Prozessdefinitionen und Dokumentation eines betriebsbereiten und dokumentierten Notfallvorsorgeplans, der exakt auf das individuelle Unternehmen abgestimmt ist, sowie die Sensibilisierung aller Mitarbeiter auf das Thema „wirtschaftliche Existenzsicherung bei einer unternehmenskritischen Notfallsituation“.

SCENARIEN UND INCIDENTS

Grundsätzlich lässt sich die Art von Ereignissen (Incidents) in folgende Sparten unterteilen:

- IT/System-Ausfall
- Gebäudeausfall
- Ausfall von Personal (bspw. Pandemie)
- Ausfall von Lieferanten/Partnern

Je nach Ereignis, wird das Unternehmen mit einem spezifischen Katastrophenszenario reagieren. Um die Kontinuität des Unternehmens sicherzustellen, ist bei einem Systemausfall anders zu reagieren als bei einem starken Anstieg von erkranktem Personal. Für den ersten Fall wird sich das Unternehmen parallele IT-Systeme beschaffen, um den Ausfall eines Systems über alternative Ressourcen zu überbrücken.

DER DISASTER RECOVERY PLAN

Bedrohungen, welche auch auf die IT und Business Continuity eines Unternehmen Einfluss haben, nehmen massiv zu! Mögliche Bedrohungszenarien, welche die IT eines Unternehmens innerhalb von Sekunden zerstören und deren Auftreten als sicher gilt, und nur die Frage besteht, wann es soweit ist (im Detail wird in diesem Papier nicht darauf eingegangen):

- Stromausfall / Black Out
- Zerstörung durch Feuer
- Falsche Bedienung / Mitarbeiterverhalten
- Pandemien bzw. Seuchenausbruch
- Terroranschläge
- Gezielte oder allgemeine Angriffe auf IT-Systeme durch Social Engineering, Hacking oder Viren
- Umweltkatastrophen
- Soziale Unruhen
- Physischer Einbruch und Zerstörung von IT-Systemen
- Ausfall zentraler Provider und Leitungen

Unternehmen sollten mit ihrem IT- oder Managed-Service-Provider-Team zusammenarbeiten, um einen DSR-Plan zu erstellen, der die notwendigen Schritte zur Wiederherstellung von Netzwerken, Servern, Laptops/Desktops, Daten und Konnektivität auflistet. Die Erstellung eines DSR Planes sollte „generalstabsmäßig“ im Zuge eines alleinstehenden Projektes durchgeführt werden.

- **Datenschutz**: Unternehmen sollten gemeinsam mit ihrer IT-Abteilung oder ihrem Lösungsanbieter sicherstellen, dass Offsite-Backups erfolgreich ausgeführt werden – einschließlich Überwachungsdiensten und der Möglichkeit, eine VM (virtuelle Maschine) so schnell wie möglich offsite zu starten. Daher sollte der DSR-Plan die Server mit den wertvollsten Daten identifizieren, denn deren Backup hat höchste Priorität.

- **Robuste redundante VPN-Lösungen**: Viele Szenarien machen es Mitarbeitern unmöglich, ihr Büro zu benutzen oder zu erreichen. In solchen Fällen können die Mitarbeiter jedoch von zu Hause aus mit einer zuverlässigen VPN-Verbindung weiterarbeiten. Daher gehört eine robuste VPN-Lösung zu den wichtigsten Diensten, die ein kleines Unternehmen unbedingt haben sollte. Bei der Erstellung eines DSR-Plans muss deshalb festgehalten werden, wer im Notfall auf das VPN zugreifen darf.

- **Überprüfung der Data-Disaster-Recovery-/Business-Continuity-Pläne**: Ein guter erster Schritt ist die Durchführung einer sogenannten „Tabletop-Übung“ mit Vertretern der IT-Abteilung, des Lösungsanbieters, Abteilungsleitern und Kommunikationsteams. Hier geht es darum, Pläne, Prozesse und Verfahren zu überprüfen.

- **Testen der IT-Systeme & Infrastrukturen**: Umsetzung eines Probelaufs zur Überprüfung der Leistung der wichtigsten Elemente der DSR-Pläne. Es muss sichergestellt sein, dass alle Unternehmensdaten in regelmäßigen Abständen gesichert werden, damit nach einer Krise geschäftskritische Informationen verfügbar sind. Klassische Listen von Geräten, Anwendungen und anderen kritischen Systemen sind hilfreich, weil diese im Krisenfall voraussichtlich nicht funktionieren.

- **Upgrade/Fix Equipment/Anwendungen und mehr**: Während einer Testsimulation lässt sich feststellen, welche Systeme nicht mit voller Kapazität arbeiten oder Abweichungen aufweisen. Es müssen effektive Mittel gefunden werden, die im Notfall einen Zugriff auf kritische Systeme ermöglichen. Dabei sollten das IT-Team und der Lösungsanbieter eng zusammenarbeiten, um die bestehende IT-Infrastruktur ausfallsicher zu gestalten.

Ein Business-Continuity-Plan (BC-Plan) kann Teil eines DR-Plans sein. Es handelt sich aber eigentlich um eine Ergänzung des DSR-Plans, denn er umfasst die Wiederherstellung des gesamten Betriebs und nicht nur der IT-Systeme.

Ein solider BC-Plan beinhaltet zudem eine Reihe von Grundsätzen für das Risikomanagement. Das bedeutet, dass alle möglichen Bedrohungen hinsichtlich des Wertes und der Erträge eines Unternehmens identifiziert werden müssen, damit im nächsten Schritt die Risiken minimiert werden können. Dazu zählen beispielsweise:

- Namen der Notfallteams und Kontaktinformationen
- Listen mit geschäftskritischen Geräten
- Listen der Lieferanten
- Listen mit wichtigen Dokumenten und kritischen Geschäftsdokumenten
- Listen mit minimalen betrieblichen Anforderungen für die Wiederaufnahme des Geschäftsbetriebs
- Kommunikationspläne für wichtige Interessengruppen des Unternehmens, einschließlich Mitarbeiter, Vorstand, Kunden und mehr.

TYPISCHE STOLPERSTEINE

Alles alleine machen

Die Aufstellung einer Disaster Recovery Konzepts wird in der Regel der IT-Abteilung aufgetragen. Allerdings ist keine Einzelabteilung alleine zur Bewältigung dieser Aufgabe in der Lage: In die Wiederherstellung des Geschäftsbetriebs nach einem Störfall muss das ganze Unternehmen einbezogen werden. Ein wirksamer Disaster Recovery Plan muss die Perspektiven der Systemnutzer, Abteilungsleiter, Finanzverantwortlichen und Rechtsexperten berücksichtigen, denn nur sie wissen, welche Anwendungen und Daten für den Geschäftsbetrieb kritisch sind und Priorität haben. Es empfiehlt sich, bei der Ausarbeitung des Plans externe Experten zu Rate zu ziehen. Eine kompetente Beratung hilft festzustellen, welche IT- und geschäftlichen Ressourcen besonders geschützt werden müssen.

Mangelnde Schulung des Disaster Recovery Konzepts

Natürlich geht es bei der Disaster Recovery vorwiegend um IT-Systeme, Archive und Daten. Aber die physische Umgebung, die Stromversorgung, die Kommunikation und die betroffenen Menschen dürfen nicht außer Acht gelassen werden. Die Mitarbeiter müssen in der Ausführung des Disaster Recovery Plans geschult werden, damit sie wissen, wie der Geschäftsbetrieb schnell wiederhergestellt werden kann.

Ein effektiver Plan muss alternative Möglichkeiten vorsehen, falls manche Mitarbeiter keinen Standortzugang haben. In diesem Fall sollten andere Mitarbeiter in der Lage sein einzuspringen. Im schlimmsten Fall sollten Zeitarbeitskräfte an einem alternativen Standort eingesetzt werden können. Daher sollte man ein Handbuch für die Wiederherstellung des Geschäftsbetriebs mit schrittweisen Disaster Recovery Anweisungen (einschließlich Passwörtern) und Zugangsinformationen für alle Systemressourcen erstellen. Diese Anweisungen müssen regelmäßig aktualisiert und an mehreren geografisch verteilten, gut zugänglichen, aber auch gut gesicherten Orten aufbewahrt werden.

Unzureichende Tests unterschiedlicher Szenarien

Wenn Sie gemeinsam mit Ihrem externen Beratungspartner den Disaster Recovery Plan aufgestellt und bekannt gemacht und geschult haben, sind Sie in der Lage, den Geschäftsbetrieb im Katastrophenfall wieder herzustellen – zumindest theoretisch. Ob der Plan jedoch in der Praxis und unter extremem Druck tatsächlich funktioniert, lässt sich nur feststellen, wenn man ihn regelmäßig in unterschiedlichen angenommenen Katastrophenszenarien testet. Durch geplante und unangekündigte Notfalltests lassen sich Schwächen im Disaster Recovery Konzept ermitteln und beseitigen und die Reaktionsfähigkeit des Teams steigern.

Keine doppelte Sicherung des Disaster Recovery Plans

Was tun im Fall der Fälle? Viele Unternehmen kommen nach einem größeren Störfall auch deshalb ins Straucheln, weil der Datensicherungsstandort ebenfalls betroffen ist – oder weil die Sicherungsdateien teilweise beschädigt oder nicht auf dem neuesten Stand sind.

Um ganz sicher zu gehen, schaffen Sie für Ihre Daten eine zusätzliche Sicherungsebene, indem Sie mehrere Sicherungskopien in einem standortfernen Tape-Tresorraum aufbewahren. Eine ausreichende Redundanz des primären Datensicherungssystems verbessert die Chancen auf eine erfolgreiche, vollständige und schnelle Disaster Recovery.

Disaster Recovery Plan wird nicht weiter entwickelt

Ihr Unternehmen und die Regeln und Vorschriften, denen es unterliegt, verändern sich. Mit diesen Veränderungen muss das Disaster Recovery Konzept Schritt halten. Planen Sie, Ihren Disaster Recovery Plan mindestens einmal pro Quartal zu überprüfen und zu aktualisieren. Dabei muss auch ermittelt werden, ob sich wichtige Aspekte verändert haben, die berücksichtigt werden müssen – zum Beispiel, ob die Standorte wichtiger Mitarbeiter verlegt oder neue IT-Systeme angeschafft wurden.

Große Datenmengen in einer Anwendung

Sämtliche Herausforderungen der Sicherung und Wiederherstellung potenzieren sich zusätzlich bei sehr großen Datenbanken. Die darin vorgehaltenen Datensätze sind typischerweise für den Geschäftsbetrieb kritisch. So können die Auswirkungen langer Backup-Fenster und langwieriger Wiederherstellungen für den Geschäftsbetrieb erheblich sein.

Fazit

Vielleicht ist ein wirklich *perfekter* Disaster-Recovery-Plan unmöglich, aber ein effektiver Plan ist auf jeden Fall realisierbar. Mit sorgfältiger Planung sowie regelmäßigen Tests und Überarbeitungen Ihres Disaster Recovery Plans können Sie dem Fall der Fälle Ihren Geschäftsbetrieb schnell wieder auf die Beine bringen.

OPERATIONAL INCIDENTS

Die folgenden Punkte stellen typische incidents im IT-Bereich dar. Jeder mögliche incident löst folgende Tätigkeiten aus:

- Bewertung der Priorität
- Errichtung einer To-Do Liste oder eines Handbuchs zur Behebung des incidents
- Operational Test und seine Auswertung

Power	Serverroom(s) power outage | Duration | 30 minutes
	Serverroom(s) power outage | Duration 1 day
	Serverroom(s) power outage | Duration non forseeable
	Power peak from provider
	Break of local power distribution
Hardware	Hardwarefailure - Server outage for each server
	Hardwarefailure - Storage outage for each storage
	Hardwarefailure - Switch outage for each switch
	Hardwarefailure – Outage Firewall for each firewall
	Hardwarefailure – Outage Internetline for each line
	Hardwarefailure of several components
	Break of primary air conditioner
	Break of backup air conditioner
Software	Damage of server due to software upgrade
	Loss of several data because of operator errors or sabotage
	Complete loss of data because of maleware, virus, sabotage, …
	Softwarefailure - Server outage for each virtual server
	Damage of network(s) because of maleware, virus or sabotage
Layer 2	Damage and failure of cluster and/or storage connections
	Damage and failure of primary network
	Damage and failure of secondary network
	Damage and failure of tertiary network
General	Damage of one network location due to fire, sabotage, environmental disaster, war, …
	Damage of the complete network due to fire, sabotage environmental disaster, war, …
	Temporary ban of local access (f.i. epidemic or pandemic consequences, social disorder, …)
Prevention	Emergency hardware material
	Actual list of contact companies and persons
	Actual list of credentials and passwords
	Monitoring environment server rooms and cabinets
	Redundancy to internet access and VPN
	Check and Backups and test of restore process