Plan zur Aufrechterhaltung des

Betriebs (DRP)

Beispiel Label Cyber-Safe

Hinweis: Dieses Dokument wird im Rahmen der Cyber-Safe-Labelisierung zur Verfügung gestellt und muss an Ihre Situation angepasst werden. Seine Verwendung garantiert nicht, dass die Anforderungen des Labels erfüllt werden.

1 Einleitung

Zwischen Ausfällen, Bränden, Überschwemmungen, Computerviren oder Epidemien gibt es viele potenzielle Risiken und Vorfälle, die das Leben (und Überleben) eines Unternehmens beeinträchtigen können.

Da Unternehmen zunehmend digitalisiert werden, können die Folgen der Nichtverfügbarkeit eines Computersystems und des Datenverlusts katastrophal sein.

1.1 Definition

Der **DRP (Disaster Recovery Plan)** ist ein Verfahren zur Reaktion auf unerwartete Ereignisse, um die Kontinuität des Betriebs der Organisation sicherzustellen.

Das **RPO (Recovery Point Objective)** ist der Zeitpunkt der letzten vollständigen Sicherung. Je weiter es von dem Vorfall entfernt ist, desto wahrscheinlicher ist es, dass Daten verloren gehen. Dies ist daher das Datensicherungsintervall, das Ihr Unternehmen tolerieren kann.

Das RTO (Recovery Time Objective) ist die Zeit, die Sie benötigen, um Ihre Systeme wiederherzustellen und nach einem größeren Vorfall zur normalen Aktivität zurückzukehren.

Je mehr Sie die potenziellen Auswirkungen eines Vorfalls mit dem richtigen Notfallwiederherstellungsplan minimieren können, desto eher können Sie den Betrieb wieder aufnehmen. Diese Indikatoren (RPO/RTO) helfen Ihnen, Ihre Anforderungen an die Sicherung Ihrer Daten und Infrastruktur zu definieren.

Um das Thema weiter zu untersuchen, finden Sie Links zu Artikeln zum Abschließen dieses Verfahrens in Anlage 1.

1.2 Umfang

Jeder Disaster-Recovery-Plan ist insofern einzigartig, als er sich an Ihr Unternehmen und seine Besonderheiten anpasst. Es gibt daher kein perfektes Modell: Es geht darum, alle Risiken zu antizipieren und eine vollständige und erschöpfende Vision zu erhalten, um das Unerwartete kontrollieren zu können.

Anhang 1 ist ein Beispiel für einen Notfallwiederherstellungsplan für Cyber-Safe. Dieses Dokument kann ein Beispiel für Ihren Ansatz sein, aber Sie müssen zuerst über Ihre Situation im Besonderen nachdenken.

1.3 Objektiv

Um mit wirtschaftlichen Unsicherheiten und Risiken (ob wirtschaftlich, finanziell oder gesundheitlich) umzugehen, basiert der Konjunkturplan auf Antizipation.

Es besteht darin, eine agile Haltung einzunehmen, um sich an ein sich veränderndes Umfeld anzupassen. Die Einsätze sind wichtig und vielfältig für die Gesellschaft:

- Gewährleistung eines Mindestumsatzniveaus durch die Wiederaufnahme einer (auch teilweisen) Tätigkeit und Sicherstellung des Überlebens des Unternehmens;
- seine Kunden auch in Krisenzeiten zufrieden zu stellen und sie zu binden, um sein Image zu verbessern;
- Halten Sie Mitarbeiter und rationalisieren Sie die interne Organisation des Unternehmens, indem Sie das gute Management und das ordnungsgemäße Funktionieren der Struktur garantieren.

2 Rollen und Verantwortlichkeiten

Für die Entwicklung, Wartung, Prüfung und Ausführung der DRP müssen Verantwortlichkeiten definiert werden.

Eine Liste der Akteure im Sanierungsplan definiert die Rollen und Verantwortlichkeiten sowie die Informationen, die für die Kontaktaufnahme mit ihnen erforderlich sind.

Eine DRP muss jederzeit aktiviert werden können, daher ist es wichtig, dass:

- Der Zugang zum Dokument ist gewährleistet;
- Die Liste enthält die Kontaktdaten (ggf. privat), die notwendig sind, um die Information der Verantwortlichen zu gewährleisten;

3 Kritische Ressourcen und Aktivitäten

Systeme werden immer komplexer und vernetzter, daher müssen Prioritäten entsprechend der Kritikalität von Daten und Aktivitäten genau definiert werden.

RTO-Metriken, die maximale Ausfallzeit, die Ihr Unternehmen ertragen kann, bevor die Situation kritisch wird, und RPO, die maximal zulässige Datenverlustzeit des Unternehmens, sollten für jede Aktivität bewertet werden, um die Tool- und Datenwiederherstellung zu priorisieren.

Um dies zu tun, ist es notwendig aufzulisten:

- Die für den reibungslosen Betrieb des Unternehmens erforderlichen Tools (ERP, CRM, Website, Kundenschnittstelle, ...);
- Daten, ihr Standort und ihre Kritikalität;

4 Szenarien

Unabhängig von Ihrer beruflichen Tätigkeit ist es wichtig, sich der Risiken bewusst zu werden und sie abzubilden. Dann können Sie die Dienstleistungen und Aktionen klassifizieren, die für das optimale Funktionieren Ihres Unternehmens unerlässlich sind.

Um die Szenarien zu definieren, müssen die Risiken, denen die Organisation ausgesetzt ist, anhand der nicht erschöpfenden Liste der folgenden Kriterien bewertet werden:

- Menschliches Risiko: Streik oder Unfall eines Arbeitnehmers.
- Naturgefahren: schlechtes Wetter oder eine Pandemie.
- Logistisches Risiko: eine Lieferzeit oder der Konkurs eines Lieferanten.
- Technisches Risiko: Strom-, Internet- oder Maschinenausfall.
- Datensicherheitsrisiko: ein Hack, ein Datendiebstahl oder ein Bug.
- Materialgefahr: Diebstahl oder Feuer.
- Kundenrisiko: eine Zahlungsverzögerung oder ein Forderungsausfall.

Die DRP hilft Ihnen, sich schnell an die Arbeitsorganisation (Teiltätigkeit, Telearbeit etc.) anzupassen: Sie garantiert die Widerstandsfähigkeit und Nachhaltigkeit Ihres Unternehmens angesichts dieser Szenarien. Die Auswirkungen der Krise, wie auch immer sie aussehen mag, werden so gemildert.

5 Verfahren

Berücksichtigen Sie für jeden Datentyp und/oder Servertyp die Schritte, um zu einem eingeschränkten (minimalen) Betriebsmodus und einem voll funktionsfähigen Modus zurückzukehren.

5.1 Beispiel: Wiederaufnahme von Verwaltungsdateien im Falle von Ransomware

Benötigte Zeit (mit den Testergebnissen zu verfeinern): 6 Stunden für den Farbverlauf und 15 Stunden für den Funktionsumfang.

1. Bestimmen Sie das Datum der Infektion: X
2. Erstellen Sie eine neue Umgebung, die vollständig von der aktuellen Arbeitsumgebung isoliert ist, und führen Sie alle folgenden Aktionen in dieser neuen Umgebung aus.
3. Erneutes Aktivieren der vsphere-VM auf ein früheres Datum als X
4. Erneutes Aktivieren der veeam-VM auf ein früheres Datum als X
5. Veeam starten und AD auf ein Datum vor X zurücksetzen
6. Überprüfen Sie einige Elemente im AD
7. Stellen Sie die "Fileserver"-VM auf ein Datum vor X zurück
8. Stellen Sie die PCs der folgenden Mitarbeiter auf ein Datum vor X zurück
9. ======== ABBAUMODUS ERREICHT ==========
10. Wiederherstellen anderer PCs
11. Überwachung wiederherstellen
12. ....
13. ======== FUNKTIONSMODUS ERREICHT ========

5.2 ERP-Datenrettung bei Festplattenausfall

Zeitaufwand (zu verfeinern mit den Ergebnissen der Tests): 10h für Steigung und 20h für funktional.

1. Erkennung von nicht funktionierenden ERP-Funktionen
2. Validierung des generalisierten Scheiterns, Information der Mitarbeiter
3. Intervention des IT-Dienstleisters für Diagnosefestplatten zum Austausch→
4. Hardware-Ersatz (SLA)
5. Wiederherstellung der letzten verfügbaren Medien
6. Überprüfen der Integrität der SQL-Datenbank
7. Intervention des ERP-Dienstleisters
8. Wiederherstellen des letzten verfügbaren ERP-Backups
9. ======== ABBAUMODUS ERREICHT ==========
10. Wiederaufnahme der Finanztätigkeit
11. Inventarisierung verlorener Daten
12. Manuelles Fortsetzen fehlender Daten
13. ...
14. ======== FUNKTIONSMODUS ERREICHT ========

6 Prioritäten

Setzen Sie sie für jedes Element in Punkt 5 in die Reihenfolge der Rückforderung entsprechend den Bedürfnissen des Unternehmens:

- 5,1 im Gefälle (6h)
- 5,3 in Steigung (4h)
- 5.4 in funktional (9h)
- 5,2 in Steigung (10h)
- ....

7 Prüfung und Häufigkeit

Definieren Sie, wie oft das Verfahren getestet werden soll und welche Punkte unbedingt überprüft werden müssen.

Um die wirtschaftlichen Auswirkungen von Tests zu reduzieren, nutzen Sie regelmäßige oder auferlegte Ereignisse, um Ihren Wiederherstellungsprozess zu definieren und zu testen, zum Beispiel:

- Ein Serverwechsel
- Gefangenschaft während der COVID-Krise
- ERP-Software aktualisieren

Die Simulation eines Szenarios mit den Akteuren des Sanierungsplans ermöglicht den Austausch über die Verantwortlichkeiten der einzelnen Szenarien. Dieser Ansatz, der durch einen PV oder einen Bericht dokumentiert wird, ist sehr effektiv und einfacher einzurichten als vollständige Tests.

8 Physische Passwörter und Zugriff

Überprüfen Sie während der Tests, ob Sie die wichtigsten Dienste neu starten können und dass Sie auch ohne die Informationen (Papier im Safe, USB-Stick ...) Zugriff auf Codes und Passwörter haben.

Ebenso muss ein physischer Zugriff möglich sein.

9 Anhänge

9.1 Anhang I

Deutsch Bank - Management der Geschäftskontinuität

9.2 Anlagen

Wikipedia - Plan zur Wiederaufnahme des Geschäftsbetriebs

https://de.wikipedia.org/wiki/Disaster_Recovery

https://fr.wikipedia.org/wiki/Plan_de_reprise_d%27activité

Wikipedia – Kontinuitätsplan

https://de.wikipedia.org/wiki/Betriebliches_Kontinuitätsmanagement
https://fr.wikipedia.org/wiki/Plan_de_continuité

Infomaniak News – Disaster Recovery Plan (DRP)

https://news.infomaniak.com/de/loesungen-cyberangriffen/