WHITEPAPER

Entwicklung eines effektiven IT-Disaster Recovery-Plans

Prozesse, Richtlinien und Maßnahmen zur Vermeidung von Geschäftsunterbrechungen

Mit einem guten IT-Disaster Recovery-Plan kann Ihr Unternehmen verlorene Daten wiederherstellen und die Zeit bis zur Wiederaufnahme der normalen betrieblichen Abläufe verkürzen. Außerdem stellen Sie damit sicher, dass Ihr Unternehmen bei einer Katastrophe keine schwerwiegenden Geschäftsunterbrechungen oder finanziellen Verluste erleidet.

Unternehmen sind in hohem Maße von Technologie abhängig. Ein tagelanger oder auch nur stundenweiser Ausfall dieser Technologie kann daher zu erheblichen finanziellen Verlusten führen. Bei einer Umfrage des ITIC (Intelligence and Terrorism Information Center) gaben über 98 % der Großunternehmen mit mehr als 1.000 Mitarbeitern an, dass eine einzige Ausfallstunde sie pro Jahr im Schnitt über 100.000 US-Dollar kostet.[1]

Eine weitere Untersuchung des Uptime Institute zeigte, dass bei 78 % der befragten Unternehmen in den letzten drei Jahren ein IT-Service ausgefallen war. Dies ist ein höherer Wert als in vergangenen Jahren. Von schwerwiegenden Ausfällen, die erhebliche Finanz- und Rufschäden nach sich ziehen können, waren 31 % betroffen.[2]

Für kleinere oder mittlere Unternehmen ohne großes Datenzentrum ist das Risiko möglicherweise noch größer. Laut dem IBHS (Institute for Business and Home Safety) können ca. 25 % der Unternehmen, die ein schweres Daten-Desaster erlebt haben, ihr Geschäft nicht mehr fortsetzen.[3]

OHNE EINEN EFFEKTIVEN DISASTER RECOVERY-PLAN KANN IHR UNTERNEHMEN SCHNELL GESCHICHTE SEIN.

Mit der Entwicklung eines umfassenden Plans zur Vorbereitung auf potentielle Katastrophen können Sie Unterbrechungen minimieren und den regulären Geschäftsbetrieb aufrechterhalten.

Dieses Whitepaper führt Sie durch alle Schritte der Entwicklung eines Disaster Recovery-Plans für Ihre IT-Umgebung – von der Risikoanalyse über die Umsetzung, die Durchführung von Tests bis hin zur kontinuierlichen Pflege. Wir geben Antworten auf folgende Fragen:

- **Warum benötigen Sie** einen Disaster Recovery-Plan?
- **Was ist ein Disaster Recovery-Plan** und was unterscheidet ihn von einem Business Continuity-Plan?
- **Wie erstellen Sie** einen erfolgreichen Plan?
- **Welche Komponenten umfasst** ein effektiver Disaster Recovery-Plan?
- **Wie vermeiden Sie** fünf häufige Fehler bei der Disaster Recovery?

SCHÜTZEN SIE IHR UNTERNEHMEN – UND IHREN ARBEITSPLATZ – MIT EINEM EFFEKTIVEN DISASTER RECOVERY-PLAN.

Copyright © 2002-2021 Acronis International GmbH.

Disaster Recovery und Business Continuity im Vergleich

Ein Business Continuity-Plan ist ein strategischer Plan, der „Prozesse und Maßnahmen beschreibt, die ein Unternehmen umsetzen muss, um geschäftskritische Funktionen während und nach einer Katastrophe aufrechterhalten zu können".[4] Ein Business Continuity-Plan tritt nicht nur bei Katastrophen in Kraft, sondern auch bei unvorhergesehenen Ereignissen wie Kompromittierungen, Krankheit oder Tod einer hochrangigen Führungskraft, Pandemien, Aufständen usw.

Ein Disaster Recovery-Plan ist ein Teil Ihres Business Continuity-Plans. Er führt die Prozesse, Richtlinien und Maßnahmen auf, die benötigt werden, um die Geschäftsprozesse sowie den Infrastrukturbetrieb bei Stromausfällen, Geräteausfällen, Feuer, Überschwemmungen oder anderen Störungen wiederherzustellen und weiterzuführen.

Ein IT-Disaster Recovery-Plan ist ein wichtiger Teil Ihres Business Continuity- und Disaster Recovery-Plans. In diesem Plan werden die Schritte zur Aufrechterhaltung des IT-Betriebs sowie zur Wiederinbetriebnahme der IT-Systeme (einschließlich Netzwerk, Server, PCs, Datenbanken, Anwendungen und andere Bestandteile der IT-Infrastruktur) definiert.

IHR DISASTER RECOVERY-PLAN SOLLTE FOLGENDE SCHRITTE UMFASSEN:

- Einrichtung einer Planungsgruppe
- Durchführung einer Risikoanalyse und Vorbereitung der Inventarisierung der IT-Ressourcen
- Festlegung der Prioritäten
- Entwicklung von Wiederherstellungsstrategien
- Entwicklung von Dokumentation, Verifizierungskriterien und Maßnahmen
- Durchführung von Tests
- Umsetzung des Plans
- Wartung der IT-Infrastruktur

IHR PLAN SOLLTE ALLE ASPEKTE IHRER INFRASTRUKTUR BERÜCKSICHTIGEN UND DIE REAKTIONSMASSNAHMEN SCHRITT FÜR SCHRITT NENNEN.

Copyright © 2002-2020 Acronis International GmbH.

Jedes Unternehmen benötigt einen IT-Disaster Recovery-Plan

Da sich Katastrophen nicht ankündigen, sollten Sie so schnell wie möglich einen IT-Disaster Recovery-Plan erstellen und umsetzen. Ein gut funktionierender Plan minimiert Risiken, reduziert Unterbrechungen und gewährleistet wirtschaftliche Stabilität. Zudem verringert er Versicherungsprämien und potentielle Haftungsrisiken. Vor allem erspart ein gut durchdachter Plan Ihrem Unternehmen im Fall einer Katastrophe tausende, wenn nicht gar hunderttausende Euro an Verlusten.

Um herauszufinden, welche Kosten Ihrem Unternehmen durch eine Katastrophe entstehen können, sollten Sie die Kosten eines Systemausfalls berücksichtigen: die Folgen für die Mitarbeiterproduktivität, der Verlust abrechenbarer Stunden, entgangene Verkäufe durch eine ausgefallene E-Commerce-Webseite sowie Strafen für Verstöße gegen gesetzliche Bestimmungen.

Daten sind eine wertvolle Ressource. Kunden-, Finanz- und Personaldaten, Forschungs- und Entwicklungsdokumente sowie E-Mails sind unersetzlich. Da in jedem Dokument eine bestimmte Menge an Arbeitszeit steckt, ist eine Wiederherstellung dieser Daten unerlässlich. In einem Worst-Case-Szenario kann Ihr Disaster Recovery-Plan die Rettung für Ihr Unternehmen sein.

Der Planungsprozess für die IT-Disaster Recovery

Mit den nachfolgenden Schritten für die Planung der Disaster Recovery können Sie während und nach einer Katastrophe für die nötige geschäftliche Stabilität sorgen.

1 EINRICHTUNG EINER PLANUNGSGRUPPE

Wenden Sie sich an die Führungskräfte verschiedener Abteilungen und nehmen Sie sie in Ihre Planungsgruppe auf. Beziehen Sie Entscheidungsträger aus verschiedenen Abteilungen und auch Kollegen aus der Buchhaltung, dem Kundenservice und der IT-Abteilung mit ein. Ihr Disaster Recovery-Plan muss eine Liste aller Gruppenmitglieder und deren Kontaktdaten, Funktionen im Unternehmen sowie deren Zuständigkeiten im Disaster Recovery-Plan enthalten, denn diese Personen müssen beim Eintreten einer Katastrophe erreichbar sein.

Copyright © 2002-2021 Acronis International GmbH.

2 RISIKOANALYSE

Nachdem Sie die Planungsgruppe für die Disaster Recovery definiert haben, müssen Sie eine Risikoanalyse und -prüfung durchführen.

a. Erstellen Sie ein Inventar aller Positionen, Bürogeräte, Anwendungen, Systeme, Server und Software im Unternehmen.

b. Ermitteln Sie die geschäftskritischen Anforderungen für Ihr Unternehmen und legen Sie fest, welche Anwendungen und Systeme geschäftskritisch, wichtig, notwendig und nicht kritisch sind.

c. Schätzen Sie ein, wie wahrscheinlich der Eintritt einer Katastrophe ist und wie sie sich auf diese Anwendungen und Systeme auswirken könnte. Dazu müssen Sie nicht nur Naturkatastrophen wie Orkane, Überschwemmungen und Feuer in Betracht ziehen, sondern auch vom Menschen verursachte Bedrohungen wie Viren-Angriffe, Infrastrukturausfälle und Fehler von Mitarbeitern (z. B. versehentliches Löschen von Daten).

d. Führen Sie eventuell auch eine Analyse der geschäftlichen Auswirkungen durch, um die Recovery Time Objectives (RTOs) und Recovery Point Objectives (RPOs) für alle geschäftskritischen Aktivitäten im Unternehmen festzulegen.

3 FESTLEGUNG DER PRIORITÄTEN FÜR ANWENDUNGEN UND SYSTEME

Nachdem Sie die geschäftskritischen Anwendungen und Systeme definiert haben, müssen Sie diese nach Prioritäten ordnen. Stellen Sie sich folgende Fragen:

a. Wie viele Daten darf Ihr Unternehmen höchstens verlieren?

b. Wie lange können Sie auf diese Daten verzichten?

c. Wie aktuell müssen die wiederhergestellten Daten sein?

d. Was muss lokal und was außerhalb des Firmenstandorts gespeichert werden?

e. Welches Risiko ist noch tragbar?

f. Welche Kosten entstehen dem Unternehmen durch Ausfälle?

g. Wie viel kostet die erneute Erstellung bzw. Zusammenstellung der Daten?

h. Wie viel kostet ein Serverausfall stündlich, einschließlich Personalkosten?

i. Was übernimmt Ihre Betriebsversicherung, wenn es um das Ersetzen von Daten geht?

j. Wie viel kostet eine Auslagerung der Disaster Recovery?

Das Ziel dieses Schritts ist die **Minimierung des Risikos** zusätzlicher Verluste und Unterbrechungen.

4 ENTWICKLUNG VON WIEDERHERSTELLUNGSSTRATEGIEN

ISO/IEC 27031, der weltweite Standard für IT Disaster Recovery, besagt: „Mit Strategien werden die Ansätze definiert, die zur Implementierung der erforderlichen Resilienz sowie zur Umsetzung der Grundsätze für Zwischenfall-Prävention, -Erkennung, -Reaktion, Recovery und Wiederherstellung nötig sind.“[5] Bei der Entwicklung Ihrer Strategien sollten Sie alle Aspekte Ihres Unternehmens berücksichtigen, einschließlich Budget, Ressourcen, Lieferanten, physische Anlagen, Personalbeschränkungen, technische Beschränkungen, gesetzliche Verpflichtungen und Risiken. Entwickeln Sie Strategien sowohl für automatische als auch manuelle Maßnahmen.

5 DOKUMENTATION IHRES PLANS

Nachdem Sie die Risiken analysiert, die Prioritäten gesetzt und die erforderlichen Disaster Recovery-Strategien entwickelt haben, wird es Zeit, diese Informationen zu dokumentieren. Legen Sie die nötigen Regeln, Prozesse und Aufgaben fest, die im Falle einer Störung die Aufrechterhaltung der geschäftskritischen Prozesse Ihres Unternehmens gewährleisten sollen.

6 DURCHFÜHRUNG VON TESTS

Definieren Sie klare Testziele und Erfolgskriterien, einschließlich der RTOs und RPOs. Testen Sie alle Funktionen wie Datenwiederherstellung, Failover (Ausfallsicherung), Zugriff auf Remote-Daten und Stresstests. Dokumentieren Sie alle Verifizierungskriterien und Maßnahmen in Ihrem Plan.

Copyright © 2002-2021 Acronis International GmbH.

7 UMSETZUNG DES PLANS

Stellen Sie den Plan den Mitarbeitern aus allen Unternehmensabteilungen zur Verfügung und bewahren Sie mindestens eine Kopie außerhalb des Firmenstandorts auf. Dadurch ist sichergestellt, dass der Plan im Katastrophenfall schnell auffindbar ist. Dokumentieren Sie alle Empfänger, Weitergabezeitpunkte und Standorte.

8 PFLEGE DES PLANS

Die Pflege Ihres Disaster Recovery-Plans trägt entscheidend zu einer erfolgreichen Wiederherstellung des Betriebs bei. Überarbeiten Sie den Plan regelmäßig, damit alle Veränderungen bei Lieferanten, Anlagen, Geräten, Anwendungen, Software, Backup-Verfahren sowie bei Budget und Personal (einschließlich aktuelle Kontaktinformationen und Kompetenzen) aufgenommen werden. Überprüfen Sie den Plan ein oder zwei Mal jährlich und führen Sie in diesem Zuge auch IT-Disaster Recovery-Tests durch.

Komponenten Ihres Plans

Nachfolgend finden Sie eine Vorlage für einen Disaster Recovery-Plan. Jeder Plan ist individuell. Dieser Beispielplan enthält daher nur die wichtigsten Informationen zur Erstellung eines Plans.

1 EINLEITUNG

Am Anfang Ihres Disaster Recovery-Plans sollten die Zielsetzung, eine Zusammenfassung sowie Angaben zum Umfang des Plans stehen. Nennen Sie alle Voraussetzungen und Kriterien zur Aktivierung des Plans. Geben Sie zudem an, wer den Plan erstellt hat, wer ihn genehmigt hat und wer zur Aktivierung des Plans autorisiert ist.

2 AUFGABEN UND VERANTWORTUNGSBEREICHE

Listen Sie alle Mitglieder des Disaster Recovery-Teams auf, einschließlich der Verantwortlichen für die Geschäftsprozesse, das Netzwerk und die Anlagen. Folgende Informationen sollten enthalten sein:

a. Kontaktdaten

b. Die Aufgabe der Mitglieder im Katastrophenfall

c. Verantwortungsbereich(e) im Unternehmen

d. Ausgabenobergrenzen (z. B. wie viel Geld steht jedem Teammitglied zum Kauf von Geräten zur Verfügung)

e. Andere Befugnisbeschränkungen

Es ist ratsam, auch die Nummer der Polizei und andere Notrufnummern mitaufzunehmen.

3 WEITERE KONTAKTINFORMATIONEN

Erstellen Sie eine Liste der primären und sekundären Ansprechpartner für die folgenden Bereiche:

a. Hardware

b. Betriebssysteme

c. Software, Anwendungen und Datenbanken

d. Kommunikation

e. Räumlichkeiten

f. Lieferanten

Copyright © 2002-2021 Acronis International GmbH.

4 REAKTION AUF ZWISCHENFÄLLE

Dokumentieren Sie den Plan für die Bewertung von Schäden am Standort und die ersten Schritte des Disaster Recovery-Prozesses. Beschreiben Sie die folgenden Punkte:

a. Wichtige Indikatoren für geringe, schwerwiegende und katastrophale Schäden

b. Vorgehensweise für die Benachrichtigung der Teammitglieder

c. Erste Schritte und Standard-Notfallmaßnahmen für alle Teammitglieder

5 AKTIVIERUNG DES PLANS

Listen Sie alle Maßnahmen für den Betrieb im Notfallmodus auf:

a. Definieren Sie die Kriterien für die Aktivierung des Plans, einschließlich der Mindestvoraussetzungen.

b. Definieren Sie Prozessbezeichnungen und -anweisungen für alle Teammitglieder.

c. Legen Sie Kategorien für wichtige Daten fest.

6 RÜCKKEHR ZUM NORMALEN BETRIEBSMODUS

Legen Sie die Kriterien und Maßnahmen für eine Rückkehr zum normalen Betriebsmodus fest, einschließlich der folgenden Schritte:

a. Austausch von Geräten und Materialien nach Bedarf

b. Wiederherstellung oder Neustart von Systemen nach Bedarf

c. Überprüfung von Systemfunktionen und Arbeitsergebnissen

d. Benachrichtigung des Personals über die Rückkehr zum normalen Betriebsmodus

7 DOKUMENTATION DES VERLAUFS

Protokollieren Sie das Datum für jedes Dokument und jede Änderung an Ihrem Disaster Recovery-Plan. Halten Sie die Namen und die Positionen der Personen oder fest, die Änderungen am Plan vorgenommen und den Plan genehmigt haben.

8 VORGEHENSWEISEN

Nach der Aktivierung des Plans sollten die Mitglieder des Disaster Recovery-Teams die jeweiligen Reaktions- und Wiederherstellungsmaßnahmen mit den Materialien vornehmen, die ihnen zugewiesenen wurden. Je ausführlicher Ihr Plan ist, desto wahrscheinlicher ist es, dass die betroffenen Daten, Systeme oder Anwendungen wiederhergestellt und in den normalen Betriebsmodus versetzt werden können. Nehmen Sie alle von Systemanbietern stammenden relevanten Informationen und Maßnahmen zur Wiederherstellung mit auf. Treten Sie während der Entwicklung des Plans mit Ihren Lieferanten in Kontakt und finden Sie heraus, welche Notfalldokumentation diese Ihnen geben können.

9 TESTS

Dokumentieren Sie alle Tests und halten Sie den Zeitpunkt der Tests sowie die Ressourcen fest, mit denen die Tests verwaltet und durchgeführt werden. Je nach Größe Ihres Unternehmens und etwaigen branchenspezifischen Compliance-Vorgaben sollten Sie jeden Monat, einmal im Quartal oder zumindest einmal im Jahr Tests durchführen. Mit einer isolierten Disaster Recovery-Testumgebung können Sie Tests so oft wie nötig durchführen, ohne andere Produktionsumgebungen zu beeinträchtigen.

Copyright © 2002-2021 Acronis International GmbH.

10 ANHÄNGE

Ergänzen Sie Ihren Disaster Recovery-Plan mit den wichtigsten Dokumenten Ihres Unternehmens, einschließlich:

a. Inventur- und Berichtsformulare

b. Wartungsformulare

c. Hardware-Listen und Seriennummern

d. Software-Listen und Lizenznummern

e. Kontaktliste der Lieferanten

f. Kontaktliste der Mitarbeiter mit privaten und geschäftlichen Telefonnummern

g. Kontaktliste für andere relevante Abteilungen

h. Abbildungen von Netzwerkplänen

i. Grundriss des Technikraums

j. Verträge und Maintenance-Vereinbarungen

k. Besondere Betriebsanweisungen für empfindliche Geräte

l. Verzeichnis der Mobiltelefone und dazugehörige Verträge

m. Test-Szenarien

n. Versicherungspolicen

o. Mietverträge und Informationen über Gebäude

p. Kaufbelege für Technikkäufe

q. Inventuraufnahmebelege bzw. Bestandsverzeichnis

r. Personalakten

s. Standortkarten

t. Informationen zur Lagerung von Gefahrenstoffen

Fügen Sie diese Dokumente Ihrem Plan als Anhang hinzu.

So vermeiden Sie fünf häufige Fehler bei der Disaster Recovery

Der Wiederaufbau nach einer Katastrophe ist niemals leicht. Doch mit dem richtigen Plan schaffen Sie es, Ihre Systeme mit möglichst wenigen Fehlern wiederherzustellen und Ihr Geschäft wieder in Ruhe betreiben zu können. Vermeiden Sie diese fünf häufigen Fehler und sorgen Sie für den Erfolg Ihrer Disaster Recovery-Lösung.

1 SAN-TO-SAN-REPLIKATION

Die Replikation von Daten von einem Ort zum anderen ist nur eine von mehreren Funktionen einer effektiven Disaster Recovery-Lösung. Folgende Aspekte sollte außerdem berücksichtigt werden:

a. Virtualisierungsumgebungen

b. Applikationsspezifische Agenten

c. Anforderungen an Snapshot-Storage

d. Serveraktivierung und Dokumentation

e. Backup und Recovery

Copyright © 2002-2021 Acronis International GmbH.

2 REMOTE-KOLLOKATION/AUSWAHL DES SPEICHERORTS

Die Wahl des Disaster Recovery-Speicherorts ist für den Erfolg eines solchen Projekts von entscheidender Bedeutung. Achten Sie darauf, dass der Speicherort nicht zu nah an Ihrem Firmenstandort liegt und sich im Notfall aus der Ferne aktivieren lässt. Es gibt unterschiedliche Anlagen, deshalb sollten Sie sich vergewissern, dass die von Ihnen gewählte Einrichtung alle Governance-, Risiko- und Compliance-Standards erfüllt. In den USA sollte sie beispielsweise mit dem Standard SSAE-16 SOC 2 Typ II zertifiziert sein und in Großbritannien mit dem Standard ISO/IEC 24762.

3 ABWEICHUNGEN BEI HARDWARE UND SOFTWARE

Ihr Disaster Recovery-Standort stellt ein funktionierendes Abbild Ihrer Produktionsumgebung dar und muss daher kontinuierlich gepflegt werden. Sorgen Sie dafür, dass Software-Lizenzen, Patches und Upgrades auf dem neuesten Stand sind. Wenn Sie sich dazu entscheiden, alte Hardware zu verwenden, sollten Sie die zusätzlichen Maintenance-Kosten miteinberechnen, die nötig sind, um die Disaster Recovery-Hardware aktuell und zu Ihren Firmenstandort parallel zu halten.

4 FEHLGESCHLAGENE TESTS

Der Entwurf eines Disaster Recovery-Testszenarios kann ein Projekt für sich sein. Schlägt Ihr Test fehl, benötigen Sie zusätzliche Zeit, um die Fehler zu analysieren und eine Lösung zu entwickeln. Dies sollten Sie unbedingt berücksichtigen. Beziehen Sie diese Kosten in die Entscheidung mit ein, ob Sie Ihre Disaster Recovery-Lösung intern entwickeln oder an einen Disaster Recovery-Anbieter auslagern möchten.

5 UNTERSCHÄTZUNG DER RESSOURCEN

Selbst wenn Sie über kompetentes IT-Personal und genügend Ressourcen verfügen, um einen Disaster Recovery-Plan umzusetzen, stellt sich die Frage, ob diese Ressourcen bei Bedarf auch wirklich zur Verfügung stehen. Mit sorgfältiger Planung und regelmäßigen Meetings sorgen Sie dafür, dass Ihre Ressourcen bei Eintritt einer Katastrophe verfügbar sind.

Ein Disaster Recovery-Plan kann darüber entscheiden, ob Ihr Unternehmen in Insolvenz gehen muss oder überlebt. Bedenken Sie die zahlreichen Argumente, die für einen Disaster Recovery-Plan sprechen: die Minimierung entgangener Verkäufe, verlorener Umsätze und Geschäftsunterbrechungen, die Beschränkung von Haftungsrisiken, die Senkung von Versicherungsprämien und der Schutz Ihrer Unternehmensressourcen. Die Erstellung eines Disaster Recovery-Plans ist die erste Maßnahme für den Schutz Ihres Unternehmens vor natürlichen und vom Menschen verursachten Katastrophen.

REFERENZEN

„2020 Hourly Cost of Downtime Survey“, ITIC, https://itic-corp.com/blog/2020/06/forty-percent-of-enterprises-say-hourly-downtime-costs-top-1million/

„2020 Data Center Industry Survey“, Uptime Institute, https://uptimeinstitute.com/2020-data-center-industry-survey-results

„Emergency Preparedness“, U.S. Small Business Administration, http://www.sba.gov/content/disaster-planning

„What is BCDR? Business continuity and disaster recovery guide“, Tech Target, http://searchstorage.techtarget.com/definition/Business-Continuity-and-Disaster-Recovery-BCDR

„Information technology — Security techniques — Guidelines for information and communication technology readiness for business continuity“, ISO, https://www.iso.org/obp/ui/#iso:std:iso-iec:27031:ed-1:v1:en

Acronis

Weitere Informationen unter
www.acronis.com

Copyright © 2002-2021 Acronis International GmbH. Alle Rechte vorbehalten. Acronis und das Acronis Logo sind eingetragene Markenzeichen der Acronis International GmbH, in den Vereinigten Staaten und/oder in anderen Ländern. Alle anderen Marken oder eingetragenen Marken sind das Eigentum ihrer jeweiligen Inhaber. Technische Änderungen, Abweichungen bei den Abbildungen sowie Irrtümer sind vorbehalten. 2021-02