WHITEPAPER

Disaster Recovery-Planung: Best Practices und Mustervorlage

Auf den ersten Blick scheint die Disaster Recovery-Planung einfach nur darin zu bestehen, eine grundlegende Zusammenfassung zu erstellen, wie man Daten und Infrastruktur nach einem Notfall wiederherstellt.

In der Realität erfordert eine effektive Disaster Recovery-Planung jedoch viel mehr. Sie umfasst die Erstellung detaillierter, schrittweiser Verfahren zur Wiederherstellung von Daten und Infrastruktur. In diesen Plänen sollten nicht nur die Schritte zur Wiederherstellung beschrieben, sondern auch Folgendes behandelt werden:

- Welches Personal welche Disaster Recovery-Aufgaben ausführen wird.
- Wie schnell Wiederherstellungsaufgaben ausgeführt werden müssen, um die RTO- und RPO-Anforderungen zu erfüllen.
- Wie die Disaster Recovery-Verfahren zwischen verschiedenen Einrichtungen oder Standorten variieren können.
- Ob Disaster Recovery-Aktivitäten für Hardware unabhängig von Disaster Recovery für Software ausgeführt werden müssen.

In diesem Handbuch gehen wir auf diese und weitere Punkte ein, während wir die Best Practices für die Entwicklung eines Disaster Recovery-Plans erläutern.

Best Practices für Disaster Recovery

Bevor wir uns mit der Erstellung eines Disaster Recovery-Plans befassen, wollen wir zunächst einen Überblick über Best Practices für die Wiederherstellung nach einem Notfall geben, die Sie bei der Entwicklung und Aktualisierung Ihres Plans berücksichtigen sollten.

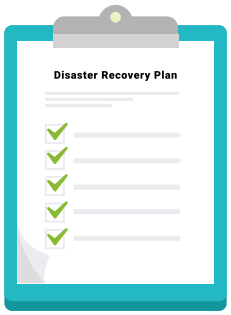
Betrachten Sie die wahrscheinlichste Ursache von Notfällen

Abhängig vom Standort (oder den Standorten) Ihrer Infrastruktur, können die Arten von Notfällen, die am wahrscheinlichsten auftreten, stark variieren. Wenn Sie beispielsweise ein Rechenzentrum in Südkalifornien betreiben, sind Erdbeben wahrscheinlich eines der wichtigsten Ereignisse, für die Sie planen müssen. In Neuengland können Hurrikane wahrscheinlicher sein. Wenn Sie ein Rechenzentrum an einem entfernten Standort haben, sind Stromausfälle möglicherweise Ihre größte Bedrohung.

Es ist wichtig, die Arten von Notfällen, die sich mit der höchsten Wahrscheinlichkeit auf Ihre Infrastruktur auswirken, zu identifizieren, da der Schweregrad, die Häufigkeit und die Vorhersagbarkeit von Notfällen je nach Art variieren. Erdbeben ereignen sich beispielsweise praktisch ohne Vorwarnung. Wenn im Gegensatz dazu ein schwerer Hurrikan die Küste der Vereinigten Staaten entlang zieht, haben Sie wahrscheinlich einige Tage Zeit, um sich auf das Ereignis vorzubereiten. Stromausfälle können plötzlich auftreten oder auch nicht, aber es ist einfach, einen Notfallplan zu erstellen, um mit ihnen umzugehen.

Wenn Sie wissen, mit welchen Notfällen Sie am wahrscheinlichsten konfrontiert sind, können Sie entsprechend planen. Sie können sogar ein statistisches Modell erstellen, um vorherzusagen, wie oft und in welchem Ausmaß Ihre Infrastruktur von Katastrophen heimgesucht wird.

Mitarbeiter müssen in der Lage sein, auf Notfallpläne zuzugreifen



Der beste Disaster Recovery-Plan ist nutzlos, wenn Ihre Mitarbeiter während eines Notfalls nicht darauf zugreifen können. Aus diesem Grund müssen Sie sicherstellen, dass die Mitarbeiter auch dann Zugang zu dem Plan haben, wenn Ihre Hauptinfrastruktur oder Ihr Netzwerk ausfällt. Ziehen Sie in Betracht, Kopien auf USB-Sticks zu speichern oder sogar auszudrucken.

Denken Sie auch daran, dass Mitarbeiter möglicherweise auf Kennwörter zugreifen müssen, um einen Disaster Recovery-Plan ausführen zu können. Stellen Sie sicher, dass auf diese Kennwörter zugegriffen werden kann, auch wenn Ihre Hauptinfrastruktur ausfällt.

Auch ist die Kommunikation zwischen den Mitarbeitern kritisch. Stellen Sie sicher, dass Sie einen Plan haben, wie Mitarbeiter miteinander reden und Informationen austauschen können, auch wenn dies über eine altmodische Telefonkette geschieht.

Notfallpläne müssen aktualisiert werden

Infrastrukturen ändern sich ständig. Ihr Disaster Recovery-Plan muss sich ebenfalls ändern, um Schritt zu halten. Überprüfen Sie zu diesem Zweck regelmäßig Ihren Disaster Recovery-Plan. Nehmen Sie sich vielleicht ein oder zwei Mal im Jahr Zeit, um durchzugehen, wie Sie den aktuellen Plan anwenden würden, um auf eine bestimmte Art von Notfall zu reagieren. Mithilfe dieser Übung können Sie Lücken identifizieren, die behoben werden müssen.

Schritte zum Erstellen eines Disaster Recovery-Plans

Lassen Sie uns nun die Schritte besprechen, die Sie zur Entwicklung Ihres speziellen Disaster Recovery-Plans durchlaufen sollten.

Der genaue Inhalt eines Disaster Recovery-Plans ist natürlich von Unternehmen zu Unternehmen unterschiedlich. Im Folgenden werden die Hauptschwerpunkte hervorgehoben, auf die sich ein typisches Unternehmen im Rahmen seines Disaster Recovery-Plans konzentrieren muss.

Analyse der Geschäftsauswirkungen und Risikobewertung

Der erste Schritt bei der Erstellung eines Disaster Recovery-Plans besteht darin, die Auswirkungen eines Notfalls auf verschiedene Bereiche des Unternehmens zu bewerten und zu ermitteln, wie schnell eine Wiederherstellung abgeschlossen werden müsste, um ein kritisches Problem zu vermeiden.

In den meisten Situationen können einige Abteilungen oder Prozesse länger unterbrochen werden als andere, ohne das Unternehmen kritisch zu schädigen. Zum Beispiel könnte Ihr Unternehmen ohne eine funktionierende Gehaltsabrechnung ein oder zwei Wochen überleben, da das Personal in der Regel nur alle paar Wochen bezahlt wird. Wenn Ihr Verkaufsteam hingegen eine Woche lang nicht arbeiten kann, weil die Software nicht verfügbar ist, kann dies das Unternehmen aufgrund von Umsatz- und Kundenverlusten viel Geld kosten.

Um die geschäftlichen Auswirkungen eines Notfalls auf verschiedene Bereiche Ihres Unternehmens zu ermitteln, müssen Sie eng mit Abteilungsleitern und Schlüsselpersonen zusammenarbeiten. Eine Möglichkeit dazu besteht darin, einen Fragebogen zu verteilen, in dem Sie abfragen, wie lange die jeweiligen Abteilungen ohne funktionierende IT-Infrastruktur arbeiten könnten und welche Konsequenzen es für das Unternehmen hätte, wenn die Abteilung ihren Betrieb einstellen müsste. Wenn der Fragebogen nicht genügend Informationen enthält, können Sie persönliche Interviews durchführen.

Nachdem Sie die Auswirkungen eines Notfalls bewertet haben, können Sie RTO- und RPO-Ziele für die verschiedenen Komponenten Ihrer Infrastruktur und Daten entwickeln, die den Anforderungen der einzelnen Abteilungen entsprechen.

Mit der Definition von RTOs und RPOs wissen Sie, was wiederhergestellt werden muss und wie schnell die Wiederherstellung nach einem Notfall erfolgen muss.

Wiederherstellungsstrategien

Mit diesen Informationen sind Sie bereit, Ihre eigentlichen Wiederherstellungsstrategien zu entwickeln. Dazu müssen Sie beurteilen, ob die derzeit vorhandenen Ressourcen ausreichen, um die verschiedenen von Ihnen festgelegten RTO- und RPO-Ziele zu erreichen. Haben Sie genug Personal, um auf einen Notfall zu reagieren und diese Ziele zu erreichen? Haben Sie genügend Backup-Infrastruktur und Netzwerkbandbreite? Werden Sie in der Lage sein, bei Bedarf schnell genug neue Hardware oder Software zu erwerben?

Durch Beantwortung dieser Fragen können Sie die allgemeinen Wiederherstellungsstrategien entwickeln, welche die Grundlage für Ihren Disaster Recovery-Plan bilden. Wenn Sie feststellen, dass Sie zu wenig Ressourcen haben, um die Strategien umzusetzen, besprechen Sie dies mit dem Management, um zu ermitteln, was Sie benötigen. Wenn Sie über mehr Ressourcen verfügen, als für die Wiederherstellung nach einem Notfall erforderlich sind, könnte dies eine Gelegenheit sein, diesen Teil Ihres Budgets zu reduzieren (was für das Management immer ein Gewinn ist).

Entwicklung eines Disaster Recovery-Plans

Sobald Sie Ihre Wiederherstellungsstrategie entwickelt und die Unterstützung des Managements erhalten haben, können Sie die Details für die Umsetzung der Strategien angehen.

Dazu ist es notwendig, dass Sie:

- Ein Gesamtplan-Framework entwickeln, das die verschiedenen Komponenten Ihres Plans definiert. Zum Beispiel wird Ihr Plan möglicherweise in verschiedene Unterpläne unterteilt, von denen jeder eine andere Abteilung im Unternehmen oder ein anderes Rechenzentrum betrifft.
- Das Personal identifizieren, das für die Ausführung des Plans (oder der Unterpläne) verantwortlich ist.
- Pläne zur Verlagerung von Hardware, Software oder Daten nach einem Notfall entwickeln.
- Die spezifischen Verfahren zur Wiederherstellung im Notfall zusammen mit den Schritten für den Zugriff auf spezielle Informationen, die zur Ausführung der Verfahren erforderlich sind, aufschreiben.
- Manuelle Workarounds dokumentieren, die Ihr Team befolgen muss, falls der Haupt-Wiederherstellungsplan nach einem Notfall fehlschlägt.
- Den Plan zusammenstellen und ihn dem Management zur Genehmigung vorlegen.

Testen des Plans

Nachdem der Plan erstellt worden ist, ist es Zeit, ihn zu testen. Führen Sie einen Testlauf der Disaster Recovery-Verfahren durch, um sicherzustellen, dass alles wie erwartet funktioniert. Stellen Sie sicher, dass alle Mitarbeiter, die an den Disaster Recovery-Verfahren beteiligt sind, wissen, welche Rollen sie haben und wie sie ausgeführt werden sollen, und wie sie während eines Notfalls auf die erforderlichen Informationen zugreifen können.

Stellen Sie sicher, dass Sie die Ergebnisse dieser Tests dokumentieren und überprüfen, um Lücken zu identifizieren, die behoben werden müssen, bevor ein tatsächlicher Notfall eintritt.

Mustervorlage für Disaster Recovery-Pläne

Wie bereits erwähnt, wird der Disaster Recovery-Plan jedes Unternehmens unterschiedlich sein. Um Ihnen bei der Erstellung Ihres Plans zu helfen, finden Sie hier eine grundlegende Vorlage, die Ihnen bei der Strukturierung Ihres Plans nützlich sein könnte..

1. Ziele
Ihr Plan kann mit einer Definition der allgemeinen Ziele der Disaster Recovery-Verfahren beginnen.

2. Personal
Erstellen Sie eine Tabelle, die den Namen, die Position und die Kontaktinformationen aller Mitarbeiter enthält, die an der Notfallwiederherstellung teilnehmen, sowie die Rolle, die sie spielen werden.

Dieser Abschnitt kann auch eine Telefonkette für interne und externe Kontakte enthalten, mit denen Sie Informationen während einer Katastrophe austauschen können.

3. Hardware- und Softwarelisten

Dieser Abschnitt des Plans enthält Tabellen oder Listen der Hardware und Software, auf die sich der Plan bezieht. Identifizieren Sie, welche Komponenten geschäftskritisch sind und welche Abteilungen von ihnen abhängen. Definieren Sie außerdem das RPO und RTO für jedes System und halten Sie die Abhängigkeiten zwischen den Systemen fest.

4. Backup- und Disaster Recovery-Verfahren

Dieser Abschnitt ist das Kernstück Ihres Disaster Recovery-Plans. Es werden die erforderlichen Verfahren zum Wiederherstellen der im vorherigen Abschnitt angegebenen Hardware- oder Softwaresysteme ausführlich beschrieben. Außerdem wird erläutert, wer für die Ausführung der einzelnen Schritte verantwortlich ist.

Offensichtlich müssen Sie abwägen, wie detailliert die Schritte in den Verfahren beschrieben werden. Wahrscheinlich brauchen Sie einen Schritt wie „Öffnen Sie Ihren Laptop“ nicht als ersten Schritt aufschreiben, den ein Mitarbeiter befolgen würde, um sich bei einem Remote-System anzumelden. Sie sollten jedoch sicherstellen, dass alle nicht trivialen technischen Schritte und Informationen im Plan klar dargelegt sind. Wenn der Plan beispielsweise das Hochfahren virtueller Server in der Cloud als Ersatz für ausgefallene physische Server beinhaltet, sollten Sie sich vergewissern, dass das Verfahren die Mitarbeiter durch die Verwendung der Konsole oder der CLI des Cloud-Anbieters führt, um eine neue Serverinstanz zu erstellen. Sie wollen nicht, dass Ihr Personal diese Dinge während eines Notfalls selbst herausfinden muss.

Die Disaster Recovery-Verfahren sollten auch Schritte zur Dokumentation des Fortschritts während der Ausführung des Plans durch Ihr Team enthalten. Diese Informationen sind wichtig für den Fall, dass eine neue Gruppe übernehmen muss; sie sind auch für Audit-Zwecke nach dem Ereignis hilfreich.

Wenn Sie mehrere Standorte unterstützen möchten, benötigen Sie möglicherweise einen Unterplan für die Anforderungen der einzelnen Disaster Recovery-Standorte.

5. Prüfverfahren

In diesem Abschnitt werden Verfahren zum Testen des Disaster Recovery-Plans sowie zur Dokumentation und Überprüfung der Testergebnisse beschrieben.

6. Unkritische Wiederherstellungsprozesse

Hier erläutert Ihr Plan, wie nicht kritische Hardware- oder Softwaresysteme nach Wiederherstellung kritischer Dienste behandelt werden. Beispielsweise verfügt Ihr Unternehmen möglicherweise über ein internes Online-Forum, in dem Mitarbeiter Informationen über soziale Aktivitäten veröffentlichen können. Möglicherweise ist die Webseite für das Unternehmen in keiner Weise kritisch, Sie sollten jedoch trotzdem dokumentieren, wie sie wiederhergestellt wird, sobald die RPO- und RTO-Ziele für wichtige Komponenten erfüllt wurden.

Notfallwiederherstellung mit MSP360 Managed Backup

MSP360 ist eine führende plattformübergreifende Cloud-Backup- und Disaster-Recovery-Lösung. MSP360 Backup ist mit den wichtigsten öffentlichen Cloud-Diensten wie Amazon Web Services, Microsoft Azure und Google Cloud Platform integriert. MSP360 Backup bietet leistungsstarke, benutzerfreundliche Backup- und Disaster Recovery-Funktionen, einschließlich Backups auf Dateiebene und Image-Basis, Disaster Recovery

auf virtuellen Maschinen in der Cloud, Datenkomprimierung und Verschlüsselung auf Militärniveau mit kundengesteuerten Schlüsseln. Kunden können MSP360 Backup auf Windows-, Mac- und Linux-Betriebssystemen ausführen.

MSP360 bietet Tausenden von VARs und MSPs einen schlüsselfertigen White-Label-Datenschutzdienst, mit dem sie ihre Marke im Cloud-Backup-Markt stärken können.

MSP360 Backup bietet Ihnen einen schnellen und einfachen Bare-Metal-Wiederherstellungsprozess. Es ermöglicht damit Image-basierte Backups auf einem beliebigen Cloud- oder lokalen Backup-Ziel, wodurch Image-basierte Backups als virtuelle VMware-Maschinen oder virtuelle Azure-Maschinen wiederhergestellt werden können.

Sicherung auf Dateiebene, Systemstatus und Systemabbild

MSP360 Backup bietet Backup und Wiederherstellung von:

- Sicherungen auf Dateiebene
- Systemstatussicherungen: Nur das Betriebssystem und die Konfiguration
- Systemabbildsicherung: Vollständige Kopie des erforderlichen Computers oder Servers

Cloud und lokal

Mit MSP360 Backup können Sie Ihre Systemabbilder im lokalen Speicher oder bei einem der über 30 Cloud-Speicheranbieter Ihrer Wahl speichern, einschließlich Amazon S3 und Amazon Glacier, BackBlaze B2, Wasabi Hot Storage, Microsoft Azure, Amazon Cloud-Laufwerk, Microsoft OneDrive, Google Drive.

Bootfähiges USB für Bare-Metal-Wiederherstellung

Erstellen Sie auf einfache Weise ein Wiederherstellungs-USB-Laufwerk oder eine startfähige ISO-Datei für die Notfallwiederherstellung im Fall eines System- oder Hardware-Absturzes. Installieren Sie zusätzliche Treiber für eine Hardwarekonfiguration, die unterschiedlich von der aktuellen Maschine ist.

Flexible Aufbewahrung und Wiederherstellung

Warum nur die neueste Version wiederherstellen? MSP360 Backup ermöglicht die Bare-Metal-Wiederherstellung auf den von Ihnen gewählten Zeitpunkt. Speichern Sie mit Hilfe von flexiblen Aufbewahrung Einstellungen so viele Versionen wie Sie benötigen, für so lange Sie möchten.

Komprimierung und Verschlüsselung

MSP360 unterstützt On-Point-Komprimierung und -Verschlüsselung. Durch die Komprimierung können Sie Platz (und damit Geld) auf dem Speicher Ihrer Wahl und Zeit bei der Durchführung eines Backups sparen. Mit der AES256-Verschlüsselung und den verschlüsselten Upload-Kanälen können Sie sicher sein, dass alle Ihre Dateien sicher sind.

Fazit

Die Planung einer Notfallwiederherstellung scheint etwas zu sein, das Sie immer bis morgen verschieben können. Aber erliegen Sie nicht dem Irrglauben, dass eine erfolgreiche Notfallwiederherstellung während einer ernsthaften Störung ohne Vorbereitung Durchgeführt werden kann. Es gibt zu viele sich bewegende Elemente - in Bezug auf verschiedene Hardware- und Softwaresysteme, Personal und Geschäftsprozesse -, um eine Notfallwiederherstellung einfach so nebenbei durchzuführen. Aus diesem Grund ist es wichtig, einen detaillierten Disaster Recovery-Plan zu haben, lange bevor es zu einem Notfall kommt.

Über MSP360

MSP360TM wurde 2011 von einer Gruppe erfahrener IT-Experten gegründet und bietet Cloud-basierte Backup- und Dateiverwaltungsdienste für kleine und mittlere Unternehmen (KMUs). Das Angebot von MSP360 umfasst leistungsstarke, benutzerfreundliche Backup-Management-Funktionen und eine Verschlüsselung nach Militärstandard mit vom Kunden kontrollierten Schlüsseln.

Kunden können ihre Backupdaten bei mehr als 20 Online-Speicheranbietern speichern, darunter Amazon S3 und Amazon Glacier. MSP360 arbeitet auch mit Tausenden von VARs und MSPs zusammen, um diesen einen schlüsselfertigen White-Label-Datenschutzdienst anzubieten. Es ist seit 2012 ein Advanced Technology Partner von Amazon Web Services. MSP360 hat außerdem den Status eines Storage Competency Partners im AWS Partner Network erhalten. Weitere Informationen finden Sie unter www.MSP360.com. Folgen Sie uns auf Twitter unter @MSP360.