BACKUP UND RECOVERY

DATA RECOVERY LEITFADEN

Übungen, Best Practices und schrittweise Anleitungen zum Schutz Ihrer kritischen Unternehmensdaten.

IRON MOUNTAIN®

AUF DEN SCHLIMMSTEN FALL BEREITET MAN SICH AM BESTEN IM VORAUS VOR

Niemand durchdenkt gerne alle Worst-Case-Szenarien. Aber eines ist sicher: Hinterher ist es dazu zu spät.

Unternehmen, die auf den Verlust wichtiger Daten nicht richtig vorbereitet sind, stehen im Ernstfall oft vor schwerwiegenden Konsequenzen. Eine Untersuchung der London Chamber of Commerce hat ergeben, dass 90 % der Unternehmen, die einen solchen Datenverlust zu verkraften haben, innerhalb von zwei Jahren ihr Geschäft aufgeben. Eine gründliche Vorbereitung zahlt sich also aus.

Natürlich führen nicht alle Notfallsituationen zwangsläufig zu großen und langfristigen Problemen. Doch der Verlust eines Laptops oder eine gelöschte Datei können die Unternehmensabläufe zumindest für eine gewisse Zeit beeinträchtigen.

AUF DEN SCHLIMMSTEN FALL BEREITET MAN SICH AM BESTEN IM VORAUS VOR

Was bringt Ihnen dieser Leitfaden? Und was nicht?

In diesem Leitfaden erklären wir Ihnen die Grundlagen eines Notfallplans, mit dem Sie Ihre Daten für den Ernstfall schützen können.

Dabei gehen wir nicht ins Detail, denn Themen wie Sicherung von Gebäuden und Gelände, alternative Einrichtungen oder Benutzerwiederherstellung würden den Rahmen dieses Leitfadens sprengen.

Weniger Theorie, mehr Praxis

Der Schwerpunkt liegt auf praxisorientierten Vorgehensweisen und Übungen.

In diesem Leitfaden stellen wir Ihnen fünf wichtige Schritte für den Schutz Ihrer Geschäftsdaten vor:

1. Einbinden des Managements
2. Risikoeinschätzung für Ihr Unternehmen
3. Die Auswirkungen von Datenverlust analysieren
4. Erstellen eines Datenwiederherstellungsplans
5. Testen dieses Plans

Fangen wir also an.

/01 EINBINDEN DES MANAGEMENTS

Sie wissen es auch: Das Pech kann jeden erwischen. Meistens geht es ja glimpflich aus. Aber manchmal entsteht daraus auch ein großes Problem.

Die Erfahrung anderer Unternehmen zeigt deutlich, dass ein zuverlässiger Notfallplan der beste Schutz für Ihr Geschäft ist. Untersuchungen der Aberdeen Group haben ergeben, dass branchenweit führende Unternehmen Daten 6,5 Mal schneller wiederherstellen und der finanzielle Verlust aufgrund von Ausfällen 40 Mal niedriger ist.

Doch es kostet Zeit und Geld, einen effektiven Plan zu entwickeln und umzusetzen. Bis zu einem gewissen Umfang werden sich dadurch möglicherweise auch die Geschäftsprozesse und Abläufe ändern. Deshalb müssen Sie die Führungskräfte in Ihrem Unternehmen überzeugen und in den Prozess einbinden. Das geschieht am besten, indem Sie klar zeigen, was es kosten würde, wenn nichts geschieht, und zwar noch bevor Sie den Zeit- und Kostenaufwand präzisieren.

Gehen Sie folgendermaßen vor, um die finanzielle Auswirkung verschiedener Notfallszenarien aufzuzeigen:

Jahresumsatz: _____ dividiert durch die Anzahl der Mitarbeiter: _____ = _____ dividiert durch 52 = _____ dividiert durch 40 = _____

Das kostet Sie eine Geschäftsunterbrechung pro Stunde und Mitarbeiter.

Und wie sieht es mit den Kosten bei speziellen Szenarien aus?

BEISPIELSZENARIO:

Ein Unternehmensserver, auf dem Ihre Kundendatenbank gespeichert ist, fällt aus und muss wiederhergestellt werden.

Kosten der Unterbrechung pro Stunde: **z.B. 270 EUR**

multipliziert mit der Anzahl der betroffenen Mitarbeiter:
500 = 135.000

multipliziert mit dem Prozentsatz der Produktivitätseinbuße:
10 % = 13.500 EUR (Kosten der Unterbrechung für Ihr Unternehmen pro Stunde)

/01 EINBINDEN DES MANAGEMENTS

Um die Kosten verschiedener Szenarien auf die Situation in Ihrem Unternehmen zu übertragen, kopieren Sie die folgende Vorlage und füllen Sie sie aus.

Diese Zahlen sollten Ihnen helfen, der Unternehmensführung einige Anhaltspunkte für die möglichen finanziellen Folgen unterschiedlichster Notfallsituationen zu liefern. Davon ausgehend können Sie dann rational darüber diskutieren, mit welchem Budget solche Situationen vermieden werden können.

SZENARIO:

Kosten der Unterbrechung pro Stunde:

multipliziert mit der Anzahl der betroffenen Mitarbeiter:

=

multipliziert mit dem Prozentsatz der Produktivitätseinbuße:

= (Kosten der Unterbrechung für Ihr Unternehmen pro Stunde)

/02 RISIKOBEWERTUNG

Im zweiten Schritt wird ermittelt, welche Risiken tatsächlich bestehen.

Gefahren lassen sich in verschiedene Kategorien einteilen. Sie können dann einfach ermitteln, wie sich die einzelnen Kategorien auf Ihr Unternehmen auswirken und was Sie tun müssen, um die geschäftsrelevanten Daten zu schützen.

Die Fragen auf der folgenden Seite sollen Ihnen helfen, die Auswirkung der verschiedenen Notfallkategorien auf Ihr Unternehmen richtig einzuschätzen. Sie können natürlich auch eigene Fragen entwickeln. Diese sollten jedoch folgende Punkte berücksichtigen:

- Umwelt (z.B. Überschwemmungen, Feuer, Sturm und andere Situationen höherer Gewalt)
- Menschliches Versagen (z.B. versehentliches Löschen von Daten, Beschädigen von Hardware, Ändern von Zugangsrechten)
- Mobilität (z.B. Verlust von Hardware, Diebstahl von Laptops, Beschädigen von Datensicherungsbändern beim Transport)
- IT-Notfälle/Energieversorgungsunterbrechungen (z.B. beschädigte Kabel, Stromausfall, Streik)
- Juristisches/Audits (z.B. Auflagen, interne Prüfungen, Bereitstellen von Beweismitteln bei Gerichtsverfahren)

NATUR-KATASTROPHEN STELLEN MIT 40% DIE GRÖSSTE EINZELBEDROHUNG FÜR DATEN DAR.

/02 RISIKOBEWERTUNG

Arbeitsblatt zur Risikobewertung: Beispielantworten

Notfallart: Umwelt	Beispielantworten
Welche Notfälle könnten sich an diesem Standort ereignen: Feuer, Überschwemmung, Stromausfall, Serverabsturz, Virenangriffe, Streiks, Aufstände, Terroranschläge usw.?	Möglich wäre der Ausbruch eines Feuers, das sich auf verschiedene Teile des Gebäudes ausbreitet. Bei einem Brand des gesamten Bürogebäudes könnten wir allerdings das Gebäude nicht mehr betreten.
Welche Auswirkungen hätte dies auf Ihr Unternehmen und Ihre Daten (Verlust von Sachanlagen/Infrastruktur, kein Zugang möglich, längerer Stromausfall usw.)?	Die Stromversorgung auf dem Gelände könnte unterbrochen werden. Möglicherweise wäre der Zugang nur eingeschränkt möglich.
Wie schwerwiegend wäre der Ausfall?	Wichtige Server könnten beschädigt oder abgeschaltet werden. Möglicherweise wäre der Zugang für einige Tage nicht möglich. Schwere Schäden am Gebäude könnten den Zugang zum Gebäude verhindern.
Wie viele Mitarbeiter wären betroffen?	70% der Mitarbeiter verfügen über Laptops und könnten gegebenenfalls von einem anderen Ort aus arbeiten. Die E-Mail-Kommunikation wäre möglicherweise beeinträchtigt, da sie über die Zentrale läuft (könnte jedoch, falls nötig, auf Hosts umgeschaltet werden). CRM ist Cloud-basiert und wäre verfügbar. Unser Finanzverwaltungssystem wird jedoch vor Ort geführt und wäre nicht verfügbar.
Wie groß wäre die Beeinträchtigung?	In den meisten Abteilungen würde die Produktivität um ca. 50% sinken. Es würden jedoch finanzielle Einbußen von bis zu 90% entstehen.

/02 RISIKOBEWERTUNG

Arbeitsblatt zur Risikobewertung: Beispielantworten

Notfallart: Umwelt	Beispielantworten
Wie lange?	Bei nur leichten Brandschäden des Gebäudes müssten wir mit einer Geschäftsunterbrechung von 5 Tagen rechnen.
Sind die Backup-Daten sicher?	Ja. Die Bandsicherungen werden an einem sicheren Ort in 20 km Entfernung vom Hauptbüro gelagert.
Wie schnell sind sie verfügbar?	Die Sicherungsbänder sind innerhalb von vier Stunden verfügbar (sofern das Betriebsgelände und die Gebäude zugänglich sind).
Wie schnell lassen sich die Daten im Bedarfsfall wiederherstellen?	Sofern das Gebäude zugänglich und die Stromversorgung gewährleistet ist, können wir innerhalb von vier Stunden nach Eintritt des Notfalls mit der Datenwiederherstellung beginnen.

/02 RISIKOBEWERTUNG

Arbeitsblatt zur Risikobewertung: Ihre Antworten

Notfallart: Umwelt	Ihre Antwort
Welche Notfälle könnten sich an diesem Standort ereignen: Feuer, Überschwemmung, Stromausfall, Serverabsturz, Virenangriffe, Streiks, Aufstände, Terroranschläge usw.?	
Welche Auswirkungen hätte dies auf Ihr Unternehmen und Ihre Daten (Verlust von Sachanlagen/Infrastruktur, kein Zugang möglich, längerer Stromausfall usw.)?	
Wie schwerwiegend wäre der Ausfall?	
Wie viele Mitarbeiter wären betroffen?	
Wie groß wäre die Beeinträchtigung?	

/02 RISIKOBEWERTUNG

Arbeitsblatt zur Risikobewertung: Ihre Antworten

Notfallart: Umwelt	Ihre Antwort
Wie lange?	
Sind die Backup-Daten sicher?	
Wie schnell sind sie verfügbar?	
Wie schnell lassen sich die Daten im Bedarfsfall wiederherstellen?	

/02 FALLLBEISPIEL SSB WIND SYSTEMS

Viele Ereignisse können dazu führen, dass ein Unternehmen die Risiken, denen die eigenen Daten ausgesetzt sind, neu bewertet. Für SSB Wind Systems, ein Hersteller von Systemen zur Steuerung von Rotorblättern, war dies die Übernahme durch das US-amerikanische Fertigungs- und Technologieunternehmen Emerson Electric.

Vor der Übernahme hatte SSB seine Datensätze immer selber verwaltet. Das vormals deutsche Unternehmen musste dafür lediglich die Vorgaben des Handelsgesetzbuchs einhalten.

Doch als Teil eines multinationalen Unternehmens mit Hauptsitz in den USA mussten nun plötzlich Anforderungen für interne Audits sowie die Vorschriften des Sarbanes-Oxley Acts erfüllt werden. In diesem Zusammenhang mussten auch die möglichen Geschäftsrisiken neu bewertet werden. Hierbei spielten wesentlich mehr Risikofaktoren eine Rolle, darunter beispielsweise:

- Wasserschäden durch Sprinkleranlagen
- Brandrisiko für die Gebäude
- Diebstahlrisiko auf dem Firmengelände

In der Folge konnte SSB einen zuverlässigen Maßnahmenkatalog entwickeln, der alle Anforderungen erfüllte und zu einem besseren Schutz der Unternehmensaktivitäten beitrug.

/03 DIE AUSWIRKUNGEN VON DATENVERLUST ANALYSIEREN

Unternehmen müssen in der heutigen Zeit auf ihr Budget achten und aus diesem Grund Prioritäten setzen.

Bei der Entwicklung eines effektiven Plans zum Schutz der Unternehmensdaten muss Folgendes bedacht werden:

- Was ist für das Überleben des Unternehmens unverzichtbar?
- Was muss auf jeden Fall sofort wiederhergestellt werden, sobald die geschäftskritischen Systeme wieder funktionsfähig sind?
- Was kann warten?

Indem Sie analysieren, wie sich ein Datenverlust auf Ihr Unternehmen auswirkt, erkennen Sie, welche ersten Maßnahmen im Ernstfall greifen müssen. Sie sehen, welche Schwerpunkte Sie bei einer Investition in den Schutz Ihrer Daten setzen sollten. Und wenn es Probleme gibt, können Sie sich auf das Wesentliche konzentrieren, anstatt spontan und unkoordiniert zu reagieren.

/03 DIE AUSWIRKUNGEN VON DATENVERLUST ANALYSIEREN

Diese Fragen sollten Sie stellen.

Für jede Analyse müssen zunächst die notwendigen Fragen ermittelt werden. Hier sind einige typische Fragen, die Sie für jeden Datentyp beantworten sollten:

Wie überlebenswichtig ist dieser Datentyp für das Unternehmen? Hierfür eignet sich eine Skala (z.B. 1 bis 5, wobei 1 für „Absolut überlebenswichtig" steht) oder eine Klassifizierung (z.B. geschäftskritisch, wichtig, nicht so wichtig).

Was kostet der Verlust dieser Daten das Unternehmen pro Stunde, pro halbem Tag oder pro Tag, und zwar in finanzieller als auch in nicht-finanzieller Hinsicht? (Umsatzeinbußen, Strafzahlungen, Sanierungskosten, Schädigung des Ansehens, Compliance, fortgesetzter Auftragsrückstau usw.)

Welche Ressourcen werden für die Wiederherstellung der Daten benötigt? (z.B. Mitarbeiter, Fachwissen, Hardware, Anlagen usw.)

Wie hoch ist ihre maximal tolerierbare Ausfallzeit (MTA)?

Wenn der Verlust bestimmter Datentypen nicht rechtzeitig behoben wird, verursacht er einen irreparablen Schaden für Ihr Unternehmen. Dazu gehören beispielsweise Rechnungs- und Kontodaten, Systeme zur Lagerkontrolle und Bestellverwaltung sowie ERP-Daten. Es lohnt sich also, eine grundlegende Frage zu beantworten: Wie schnell wird aus einem einzelnen Datenverlust eine Katastrophe für das gesamte Unternehmen?

Dies ist die maximal verfügbare Zeit für die Datenwiederherstellung. Notfallstrategien, die diesen Zeitrahmen nicht erfüllen, sind also keine realistische Option. Um die maximale Zeit für die Datenwiederherstellung zu ermitteln, müssen Sie die Kosten für die einzelnen Datentypen und Systeme auf Stunden- oder Tagesbasis hochrechnen, bis der Wert die Summe übersteigt, die das Unternehmen noch tragen kann.

/03 DIE AUSWIRKUNGEN VON DATENVERLUST ANALYSIEREN

Ermitteln der Wiederanlaufdauer (RTO)

Nachdem Sie jetzt die maximal tolerierbare Ausfallzeit für Ihr Unternehmen ermittelt haben, sollten Sie festlegen, bis wann die Systeme und Prozesse wieder funktionieren müssen. Hierfür ermitteln Sie zunächst, wie schnell zerstörte oder verlorene Daten wiederhergestellt werden sollen. Das ist die sogenannte Wiederanlaufzeit (Recovery Time Objective, RTO). Für jeden Datentyp gibt es eine eigene RTO.

Jede RTO sollte basierend darauf ermittelt werden, welche Auswirkungen und Kosten der Datenverlust verursacht. Ein Systemausfall, durch den das halbe Unternehmen zum Stillstand kommt und der Tausende Euro pro Stunde kostet, hat also eine wesentlich niedrigere RTO als eine kleine Störung, die leicht behoben werden kann.

Es kostet wesentlich mehr, sich auf einen Vorfall mit niedriger RTO vorzubereiten. Sie müssen also Kompromisse eingehen, um eine akzeptable Balance zu finden.

Ermitteln des Wiederanlaufpunkts (RPO)

Bei größeren Katastrophen kommt es unweigerlich zu Datenverlust. Das sind meistens die Daten, die seit der letzten Datensicherung (sofern diese erfolgt ist) erstellt oder geändert wurden. Mit dem Wiederanlaufpunkt (Recovery Point Objective, RPO) legen Sie fest, wie viele Daten über einen Zeitraum wiederhergestellt werden müssen, wenn es zu einem notfallbedingten Ausfall kommt.

Das hat direkte Auswirkungen auf Ihre Datensicherungsstrategie. Wenn Sie eine RTO von vier Stunden festlegen, müssen Sie die relevanten Daten alle vier Stunden sichern, um diese RTO zu erreichen. Wenn Sie eine effektive RTO von Null festlegen, müssen Sie in ein vollgespiegeltes Echtzeit- Backupsystem investieren.

/03 DIE AUSWIRKUNGEN VON DATENVERLUST ANALYSIEREN

Arbeitsblatt zur Risikobewertung

Daten/System	Wie wichtig?	MTA	RTO	RPO

/04 DATA RECOVERY PLAN ERSTELLEN

Sie kennen nun die Risiken, denen Ihr Unternehmen ausgesetzt ist, die Auswirkungen, die der Verlust unterschiedlicher Daten haben kann, und die maximale Ausfallzeit, die Ihr Unternehmen meistern kann.

Sie wissen, wie schnell die wichtigen Datentypen wiederhergestellt werden müssen und wie viele Daten Sie verlieren können, ohne Ihr Unternehmen ernsthaft zu gefährden.

Jetzt müssen Sie einen Plan zum Schutz der geschäftskritischen Daten entwickeln.

/04 DATA RECOVERY PLAN ERSTELLEN

Einen Schritt nach dem anderen.

Sortieren Sie zunächst die Datentypen, die Sie bei der Analyse der Auswirkungen eines Datenverlusts als kritisch ermittelt haben. Beginnen Sie dabei mit den Datentypen, die für das Überleben des Unternehmens unverzichtbar sind.

Ermitteln Sie für jeden dieser Datentypen die entsprechenden Daten und stellen Sie fest, wo sie sich befinden. Manchmal sind sie nicht sofort ersichtlich.

Berechnen Sie dann, was es kosten würde, RTO und RPO der einzelnen Datentypen mittels eines mehrschichtigen Backupsystems zu realisieren.

Für geschäftskritische Daten, die so schnell wie möglich wiederhergestellt werden müssen, eignet sich beispielsweise eine vollständige Remote-Replikation oder andere Datensicherungsoptionen. Für den Großteil der täglich erzeugten Daten genügt eine professionelle Banddatensicherung, wobei die Bänder an einem anderen Ort aufbewahrt werden. Dabei muss gewährleistet sein, dass sie im Notfall schnell zur Verfügung stehen. Diese Lösung ist bei der Wiederherstellung großer Datenmengen oft schneller. Andere Daten wiederum können einfach archiviert werden, auch hier meist auf Sicherungsbändern.

Für alle Backup-Daten müssen Sie außerdem Richtlinien zur Aufbewahrung dieser Daten entwickeln, um Ihre RPO-Ziele zu erreichen und die Rechtsvorschriften zu erfüllen. Diese Richtlinien sind oft Teil von Compliance-Audits.

Aufschreiben, bekannt machen.

Ihr Plan zum Schutz von geschäftsrelevanten Daten muss klar verständlich sein und allen, die ihn benötigen, leicht zugänglich gemacht werden. Selbst der beste Plan nützt nichts, wenn er auf einem Server gespeichert ist, der im Ernstfall ausfällt – oder wenn ihn nur eine Person kennt, die gerade dann im Urlaub ist, wenn der Notfall eintritt. Aber es geht nicht nur um dieses letztgenannte Szenario. Aktuelle, von PwC durchgeführte Studien haben ergeben, dass 60% der Unternehmen nicht davon überzeugt sind, dass ihre Mitarbeiter über die notwendigen Tools verfügen, um das Unternehmen vor Datenrisiken zu schützen. Sie sollten Ihren Plan zum Schutz der Unternehmensdaten also:

Aufschreiben | Ausdrucken | Anderen zugänglich machen | An einem anderen Ort aufbewahren

/04 DATA RECOVERY PLAN ERSTELLEN

Was sollte ein Datensicherungsplan enthalten?

Jedes Unternehmen ist einzigartig. Es gibt jedoch einige Kernelemente, die in keinem Datensicherungsplan fehlen sollten. Zu diesen zählen:

Wann und wie soll der Plan greifen? Legen Sie fest, was ein Notfall genau ist und wer die entsprechenden Abläufe auslösen soll.

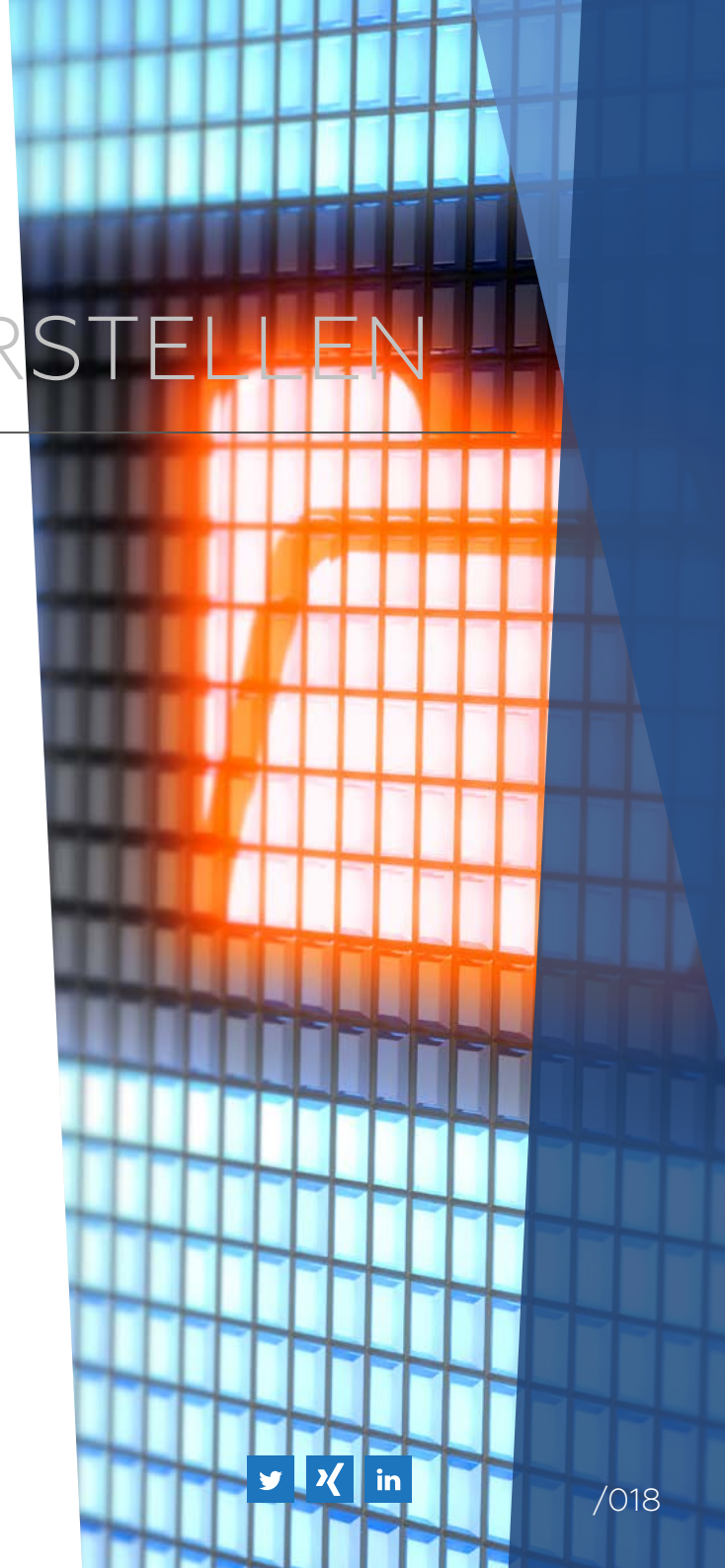
Wer soll als erstes informiert werden und wie?

Eine Vorgehensweise für die Bewertung der Auswirkungen eines Datenverlusts: Orientieren Sie sich an der Logik, die Sie in der Analyse der Auswirkungen von Datenverlust ermittelt haben.

Wo befinden sich die Backup-Daten und wie wird darauf zugegriffen?

Wie werden die betroffenen Systeme und Daten wiederhergestellt?
(wichtigste Systeme zuerst)

Wann gilt ein Notfall als beendet und wann kann der normale Geschäftsbetrieb wiederaufgenommen werden?



/04 DATA RECOVERY PLAN ERSTELLEN

Mehrschichtiger Schutz: das richtige Backup für die richtigen Daten!

Daten sind nicht gleich Daten. Da gilt auch für Backups. Backups von geschäftskritischen Daten sollten nach Möglichkeit sofort zur Verfügung stehen. Daten für den täglichen Geschäftsablauf oder archivierte Daten lassen sich auch mit einer gewissen Verzögerung wiederherstellen.

Für die meisten Unternehmen gilt: Es ist einfach zu teuer, alle Daten-Backups immer sofort zur Verfügung zu haben. Untersuchungen der Association for Information and Image Management (AIIM) haben ergeben, dass ca. 80% der Daten nach 90 Tagen nicht mehr benötigt werden. Es ist also wenig sinnvoll, in kostspielige Ressourcen zu investieren, um diese Daten sofort verfügbar zu machen.

Stattdessen sollten Sie ein mehrschichtiges System zur Datensicherung einsetzen. Dabei werden hochverfügbare, teure Optionen für unternehmenskritische Daten (z.B. Echtzeit-Vertriebsdaten) mit kostengünstigeren, aber langsameren Alternativen für weniger wichtige Daten (z.B. E-Mails, Vorjahresdaten, Auditdaten) kombiniert.

Ein Beispiel:

Der Iron Mountain-Kunde Teleperformance España, ein Spezialist für Kundenmanagement, muss aus rechtlichen und unternehmensspezifischen Gründen alle Ton- und Schriftdatensätze speichern, um sie wieder aufrufen zu können. Je nach Zeitspanne müssen unterschiedliche Daten aufbewahrt werden, die wiederum in unterschiedlichen Zeitspannen wieder abrufbar sein müssen. Diese Daten befinden sich auf Sicherungsbändern, CDs oder DVDs oder auf Papier.

Iron Mountain erfasst diese Daten wöchentlich und archiviert sie. Dabei hat jedes Element seine eigene Aufbewahrungsfrist. Nach Ablauf dieser Frist vernichtet Iron Mountain die Daten sicher und ohne weitere Mitwirkung von Teleperformance España. Das bedeutet also: Die jeweiligen Daten werden über die für sie erforderliche Zeit kosteneffizient aufbewahrt.

/05 DEN PLAN TESTEN

In der Theorie sieht jeder Plan gut aus. Doch erst in der Praxis zeigt sich, ob Sie wirklich so gut vorbereitet sind, wie Sie glauben.

Wenn Ihre Server jedoch bereits einen Meter unter Wasser stehen, ist es zu spät, Schwächen im Plan aufzudecken.

/05 DEN PLAN TESTEN

Was soll getestet werden?

Natürlich können Sie nicht jedes Szenario vorhersehen, aber Sie können testen, wie gut der Plan in den am häufigsten eintretenden Situationen funktioniert:

Ein typisches Szenario: Der Serverausfall, bei dem ein einzelner Server beschädigt wird und wiederhergestellt werden muss.

Ein Stromausfall im gesamten Gebäude

Überschwemmungen/Feuer, durch die Teile des Bürogebäudes zerstört werden

Ein beschädigtes Kabel, das den Zugang zu Internet, Cloud und WAN verhindert

Aufgrund von Evakuierungsmaßnahmen oder ähnlichen Maßnahmen der Sicherheitsdienste ist kein Zugang zu Gebäuden möglich.

Wie oft soll gestestet werden?

Die Dinge ändern sich. Menschen kommen und gehen. Neue Systeme werden eingeführt, alte ausgemustert. Um den Plan immer auf dem neuesten Stand zu halten, müssen Sie ihn regelmäßig testen und überarbeiten. Idealerweise sollte ein solcher Test alle sechs Monate (oder zumindest einmal jährlich) durchgeführt werden.

Überprüfen Sie nach jedem Test, was funktioniert hat und was nicht, und überlegen Sie, was überarbeitet oder verbessert werden könnte. Diese Änderungen sollten in den neuen Plan übernommen und jedem Mitarbeiter des Datenwiederherstellungsteams mitgeteilt werden.

/05 DEN PLAN TESTEN

Unterschiedliche Tests

Es gibt Tests mit unterschiedlicher Prüftiefe:

Walkthrough-Test:
Das Datenwiederherstellungsteam bespricht die einzelnen Schritte und Phasen des Wiederherstellungsplans. Dadurch lassen sich spezielle Probleme und fehlende Schritte ermitteln und Sie können erkennen, ob weitere Schulungen erforderlich sind.

Simulationen:
Das Datenwiederherstellungsteam konzentriert sich auf ein spezielles Szenario und geht den Wiederherstellungsplan so durch, wie er in diesem Fall anzuwenden wäre. Dabei wird auch überprüft, wie gut die einzelnen Elemente und Beteiligten unter diesen Umständen agieren.

Paralleltest:
Das Datenwiederherstellungsteam führt eine tatsächliche Datenüberprüfung auf einem Parallelsystem durch (also Systeme, die parallel mit den tatsächlich genutzten Systemen geschaltet werden).

Unterbrechungstest:
Der Datenwiederherstellungsplan wird tatsächlich durchgeführt, es werden Backup-Systeme erstellt und das Wiederherstellungsteam organisiert eine vollständige Umstellung auf die Backup-Daten.

WARNUNG: Dies ist ein hochriskanter Test, der die normalen Geschäftsabläufe beeinträchtigen kann. Er sollte mit größter Vorsicht und außerhalb der normalen Geschäftszeiten durchgeführt werden.

/06 ABSCHLIESSENDES

Katastrophen, ob große oder kleine, gehören zu den traurigen Tatsachen im Leben. Sie können nicht bis ins Detail vorhersagen, was passieren wird, und erst recht nicht, wann es passiert. Aber Sie können sich vorbereiten.

Die Entwicklung eines realistischen, robusten und mehrschichtigen Plans zur Datensicherung ist einer der grundlegenden Schritte, um das langfristige Überleben Ihres Unternehmens zu sichern. Dabei sollten Cloud- und Bandsicherungsoptionen kombiniert werden, um die richtige Mischung aus Verfügbarkeit, Zuverlässigkeit und Preis-Leistungsverhältnis zu finden.

Wenn Sie das richtige Verhältnis gefunden haben, lässt sich der Datenverlust im Katastrophenfall auf ein Minimum reduzieren und Sie können so schnell wie möglich wieder zum Alltagsgeschäft zurückkehren. Außerdem können Sie fundierte Entscheidungen darüber treffen, wie viel Sie in welche Optionen investieren möchten.

Die Empfehlungen in diesem E-Book sollen Ihnen bei den ersten Schritten zur Erstellung eines Datensicherungsplans helfen. So können Sie die wichtigsten Systeme und kritische Daten im Ernstfall schnell wiederherstellen. Wir hoffen natürlich, dass Sie diesen Plan nie wirklich brauchen werden.

Alles Gute!

FOLGEN SIE UNS:

0800 408 0000 | IRONMOUNTAIN.DE
0800 00 24 24 | IRONMOUNTAIN.CH
+43 (0) 2287 30 544 | IRONMOUNTAIN.CO.AT

ÜBER IRON MOUNTAIN

Iron Mountain Inc (NYSE: IRM) Ist ein global führender Dienstleister für Lösungen im Bereich Archivierung und Informationsmanagement. Das Unternehmen bietet den mehr als 220.000 Firmenkunden, die weltweit auf Iron Mountain vertrauen, eine Archivinfrastruktur von über 7,9 Millionen Quadratmetern, verteilt auf mehr als 1.400 Einrichtungen in 52 Ländern, um das zu schützen, was den Kunden am wichtigsten ist. 1951 gegründet, schützt Iron Mountain Milliarden von Informationen, darunter kritische Geschäftsdokumente, elektronische Informationen, medizinische Daten sowie kulturelle und historische Gegenstände
Weitere Informationen finden Sie auf www.ironmountain.de

IRON MOUNTAIN®