datto

WHITEPAPER

Backups und Business Continuity: erfolgreiche Notfallpläne im Fokus

Eine optimale Datensicherheit ist überlebensnotwendig für jedes Unternehmen – unabhängig von dessen Größe und Branchenzugehörigkeit. In diesem Whitepaper erläutern wir die Notwendigkeit einer Business Continuity-Lösung gegenüber einem simplen Backup im Katastrophenfall. Zudem zeigen wir Ihnen, wie Sie die Tauglichkeit Ihres Notfallprogramms prüfen und potenzielle Downtime-Kosten abschätzen lernen.

Einleitung

Ein Ausfall Ihres Unternehmenssystems kommt Sie teuer zu stehen: Je nach Größe der Organisation betragen die stündlichen Kosten zwischen 9.000 und 700.000 US-Dollar. Durchschnittlich entspricht das pro Stunde einem Geschäftsverlust in Höhe von 164.000 US-Dollar.[1] Die Zahlen sprechen für sich.

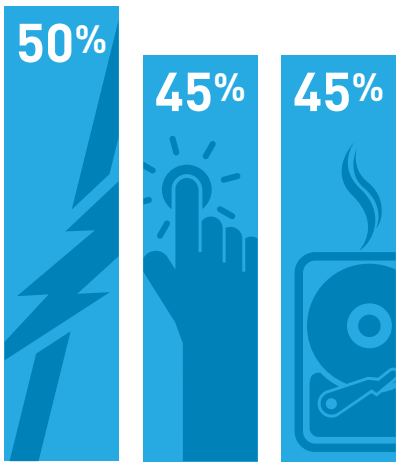


Abbildung 1: Ausfallursachen

Wie kommt es zur Downtime? Netzwerkstörungen und menschliches Versagen sind für 50 bzw. 45 Prozent aller Ausfallzeiten verantwortlich. Nur 10 Prozent der Ausfälle sind auf Naturkatastrophen zurückzuführen (siehe Abbildung 1).[2]

Schlüsselt man Ursachen von Ausfällen nach dem betroffenen Datenvolumen auf, steht wiederum menschliches Versagen mit 58 Prozent an erster Stelle (siehe Abbildung 2).[2] Wie sich herausstellt, sollten Unternehmen den Fokus nicht auf Naturkatastrophen, sondern ihre eigenen Mitarbeiter legen.

Wenn Sie Datensicherheit keine hohe Priorität beimessen, da an Ihrem Standort keine Wetterkapriolen zu befürchten sind, dann seien Sie gewarnt: Die größte Gefahr für Ihre Daten sind keineswegs äußere Einflüsse – die größte Gefahr kommt aus Ihrem Unternehmen selbst.

	Hohes Datenvolumen	Sonstige
Netzwerkstörungen	42%	53%
Menschl. Versagen	58%	44%
Serverausfälle	44%	46%
Speicherversagen	45%	44%
Anwendungsfehler	37%	33%
Stromausfälle	13%	28%
Lastspitzen	19%	15%

Abbildung 2: Ausfallzeiten, aufgeschlüsselt nach betroffenem Datenvolume

Was auf dem Spiel steht

IN JÜNGERER VERGANGENHEIT VERURSACHTEN AUSFALLZEITEN BEI 35 % DER KMU VERLUSTE IN HÖHE VON 500.000 $.

Weltweit wird täglich ein Datenvolumen von 2,5 Quintillionen Byte generiert. Rund 90 Prozent des vorhandenen Datenbestands wurde innerhalb der letzten Jahre angehäuft, ein bedeutender Teil davon von kleinen und mittelgroßen Unternehmen (KMU).[3] Wenn man bedenkt, wie viele Server, Desktop-PCs und Laptops typische KMU verwalten müssen, kann man erahnen, welche enormen Datenmengen zu schützen sind.

Dennoch verzichten knapp 75 Prozent der KMU auf einen Disaster-Recovery-Plan. Nur 25 Prozent geben an, kompromittierte Daten wiederherstellen zu können.[4] Gerade einmal 50 Prozent der KMU sichern weniger als 60 Prozent ihrer Datenbestände. Die verbliebenen 40 Prozent? Datensicherung – Fehlanzeige.[5]

Wie hoch ist der Preis für diese Nachlässigkeit? In jüngerer Vergangenheit verursachten Ausfallzeiten bei 35 Prozent der KMU Verluste in Höhe von 500.000 US-Dollar. 3 Prozent hatten mit Schäden in Millionenhöhe zu kämpfen (siehe Abbildung 3).[6]

	<1,000	1.000 bis 10.000	>10,000
Keine Kosten	17%	20%	8%
<$5000,000	35%	39%	29%
Zwischen $500.000 und $1 Million	5%	9%	8%
>$1 Million	3%	3%	10%
Weiß nicht/unsicher	24%	29%	46%

Abbildung 3: Gesamtkosten von Ausfällen

Was passiert im Katastrophenfall? Unternehmen müssen möglichst schnell die Kontrolle über wichtige Daten zurückerlangen. Laut IDG kann der normale Betrieb durchschnittlich sieben Stunden nach Auftreten eines Datenverlusts wieder aufgenommen werden. 18 Prozent der IT-Manager berichten von Ausfallzeiten zwischen elf und 24 Stunden oder darüber hinaus.[7]

Auf ähnliche Zahlen kamen die Marktforscher der Aberdeen Group, die vorbildlich reagierende Unternehmen mit solchen verglich, die im Falle eines Datenverlusts mit schwerwiegenden Problemen zu kämpfen hatten. Multiplizieren Sie die durchschnittliche Zeitdauer bis zur Wiederaufnahme des normalen Betriebs (5,18 Stunden) mit den stündlichen Kosten eines Ausfalls, erhalten Sie eine schwindelerregende Rechnung (siehe Abbildung 4).

	Führend	Durchschnitt	Nachzügler
Zahl der Ausfälle in den letzten 12 Monaten	0.56	2.26	3.92
Durchschnittliche Ausfallzeit pro Vorfall in den letzten 12 Monaten	0.16 Std.	1.49 Std.	17.82 Std.
Längster Ausfall	0.21 Std.	4.78 Std.	43.71 Std.
Verfügbarkeit kritischer Anwendungen	99.90%	99.62%	99.58%
Wiederherstellungszeit nach dem letzten Ausfall	1.13 Std.	5.18 Std.	27.11 Std.

Abbildung 4: Ausfallstatistiken für kleine und mittelgroße Unternehmen[1]

ÜBER 90 % ALLER UNTERNEHMEN STELLTEN 2 JAHRE NACH EINEM AUSFALL DEN GESCHÄFTSBETRIEB EIN.

Angesichts dieser Zahlen verwundert es kaum, dass 40 Prozent aller Unternehmen infolge eines Ausfalls den Geschäftsbetrieb einstellen mussten, wie die US-Bundesagentur für Katastrophenschutz FEMA vermeldet. Studien der US-Behörde SBA (Small Business Administration) zufolge mussten innerhalb von zwei Jahren nach einem Ausfall sogar über 90 Prozent der betroffenen Unternehmen ihre Türen schließen.

Was tun kleine und mittelgroße Unternehmen, um sich vor dieser existenziellen Bedrohung zu schützen? Über 60 Prozent setzen bei der Sicherung geschäftskritischer Daten immer noch auf Magnetbandtechnologie. Eine erstaunliche Zahl, wenn man bedenkt, dass die Technologie vier Jahrzehnte alt und die Handhabung höchst umständlich ist. Zudem müssen die physischen Datenträger nach der Sicherung an einen Verwahrungsort oder zu einem anderen Büro transportiert werden. Knapp 20 Prozent verwenden hingegen bereits Daten-Backups in der Cloud (siehe Abbildung 5).[8]

1. "Downtime and Data Loss: How Much Can You Afford?" Aberdeen Group, 2013.
2. "Enterprise Data and the Cost of Downtime," Independent Oracle User Group, July 2012.
3. "Small Business? Look to Big Data," Curt Finch, The International Community for Project Managers, Jan. 2014.
4. Symantec 2012 SMB Disaster Preparedness Survey, 2012.
5. Symantec 2011 SMB Disaster Preparedness Survey, 2011.
6. "Enterprise Data and the Cost of Downtime," Independent Oracle User Group, July 2012.
7. "Wanted: Better Backup," IDG Research Services, May 2012
8. "IT Trends: Disaster Recovery," InformationWeek, July 2013.

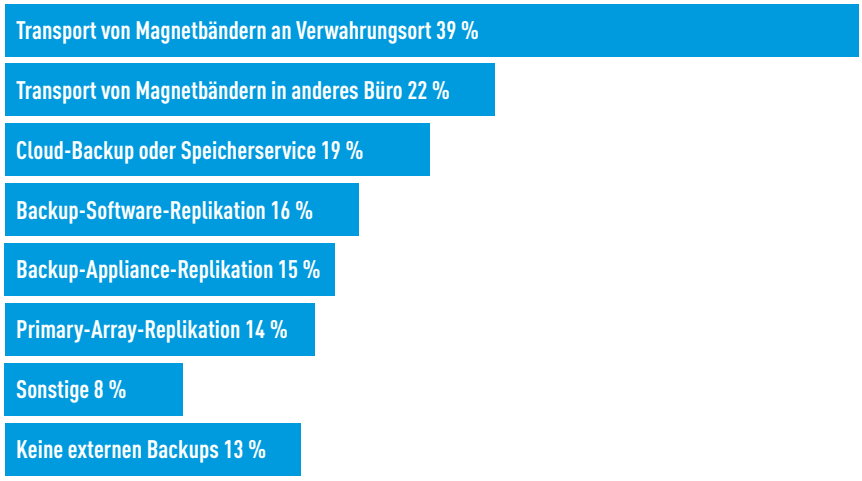
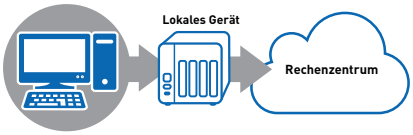


Abbildung 5: Methoden zur Auslagerung von Backup-Daten (mehrere Antworten möglich)

LOKALES BACKUP ODER CLOUD? DIE WAHRHEIT LIEGT IN DER MITTE. EINE HYBRIDE LÖSUNG VEREINT DIE VORTEILE LOKALER BACKUPS MIT DER SICHERHEIT DER CLOUD.



Lokales Backup oder Cloud? Die Wahrheit liegt in der Mitte

Mit rein lokalen Backups können zumindest kleinere Ausfälle oft bewältigt werden. Dank sofortiger Verfügbarkeit gelingt die Datenwiederherstellung am ursprünglichen Standort innerhalb kurzer Zeit – ohne größere Einschränkungen des Geschäftsbetriebs. Doch was passiert, wenn der Strom ausfällt? Wenn die Hardware den Dienst versagt? Oder wenn die Daten von Mitarbeitern gestohlen oder vernichtet werden? Die Cloud erscheint als nächstliegende Antwort auf diese Probleme. Eine reine Datensicherung über die Cloud ist aufgrund der schwankenden Bandbreite jedoch riskant. Die Wiederherstellung von Daten gestaltet sich häufig kompliziert und zeitaufwändig. Auch die Cloud ist zudem nicht immun gegen Ausfälle.

Wie funktioniert eine hybride Cloud-Lösung? Ihre Daten werden zunächst kopiert und auf einem lokalen Gerät gespeichert. Im Ernstfall können Sie eine schnelle und einfache Wiederherstellung über dieses Gerät vornehmen. Zusätzlich werden Ihre Daten jedoch auch in der Cloud gespeichert. Fällt das Gerät aus, verfügen Sie noch über externe Cloud-Kopien Ihrer Daten. Gleichzeitig entfällt der Aufwand, physische Datenkopien auszulagern.

Datei-Backups versus Business Continuity

Beim Backup steht die Datensicherheit im Vordergrund und somit die Frage: Sind Ihre Geschäftsdaten in guten Händen? Können Sie die Daten bei einem Ausfall wiederherstellen?

Business Continuity berührt hingegen Fragen auf Unternehmensebene: Wie schnell können Sie den Geschäftsbetrieb nach einem Systemausfall wieder aufnehmen?

Datei-Backups sind eine unerlässliche Grundlage. Sie müssen sich jedoch auch um die Business Continuity Gedanken machen, damit Ihr Unternehmen im Katastrophenfall schnell wieder einsatzfähig wird. Fällt beispielsweise Ihr Server aus, genügt kein reines Datei-Backup, um in möglichst kurzer Zeit den Normalzustand wiederherzustellen.

Der Server müsste ausgetauscht, Software und Daten müssten neu installiert und das gesamte System mit den Ausgangseinstellungen konfiguriert werden. Dieser Prozess kann Tage in Anspruch nehmen. Kann sich Ihr Unternehmen das wirklich leisten?

Für eine effektive Business Continuity müssen folgende Kennzahlen kalkuliert werden: Recovery Time Objective (RTO) und Recovery Point Objective (RPO).

RTO: Bei der Recovery Time Objective handelt es sich um den Zeitraum, der vom Zeitpunkt des Schadens bis zur vollständigen Wiederherstellung der Geschäftsprozesse vergehen darf.

RPO: Bei der Recovery Point Objective handelt es sich um den maximal zumutbaren Zeitraum, der zwischen zwei Datensicherungen liegen darf.

BERECHNEN SIE DIE TATSÄCHLICHEN KOSTEN EINES DATENVERLUSTS, UM DIE INVESTITION IN EINE BUSINESS CONTINUITY-LÖSUNG ZU RECHTFERTIGEN.

Durch die Berechnung der RTO ermitteln Sie die maximale Zeitdauer, die Sie auf Ihre Daten verzichten können, ohne Ihr Geschäft ernsthaft zu gefährden.

Die RPO hingegen besagt, wie oft Sie Backups durchführen müssen. Je nach Geschäftsanforderungen kann die RTO beispielsweise einen Tag betragen und die RPO eine Stunde. Die jeweils erforderlichen Zeitfenster geben Aufschluss darüber, welche Art der Backup-Lösung Sie tatsächlich benötigen (siehe Abbildung 6).

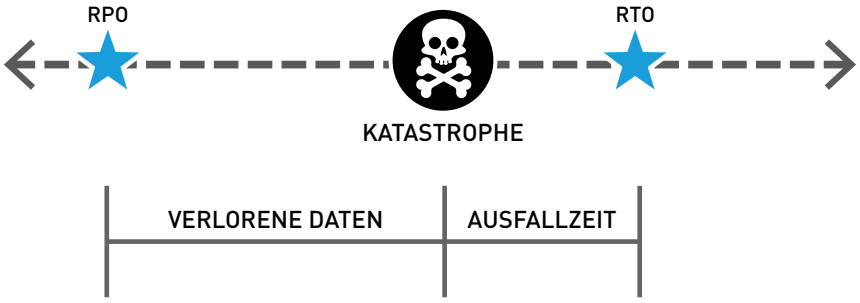


Abbildung 6: Unterschied zwischen RPO und RTO

Sobald Sie RPO und RTO ermittelt haben, sollten Sie die Kosten eines Ausfalls sowie des daraus resultierenden Datenverlusts kalkulieren. Addieren Sie hierzu einfach den Durchschnittslohn, die Betriebskosten und die Durchschnittseinnahmen pro Stunde.

Alternativ können Sie RPO, RTO und Ausfallkosten bequem mit diesem kostenlosen Online-Downtime-Rechner ermitteln.

Da viele Unternehmen mit einem knappen Budget zu kämpfen haben, können diese Zahlen die Investition in eine Business Continuity-Lösung rechtfertigen.[11]

Image-Backups versus Datei-Backups

Es gibt zwei bekannte Arten von Backup-Lösungen: datei- und image-basiert. Ein Datei-Backup macht exakt, was der Name verspricht: Sie bestimmen, welche Dateien zu sichern sind, und diese Dateien werden lokal oder in der Cloud gespeichert. In Sicherheit ist jedoch nur, was Sie ausgewählt haben. Was, wenn Sie eine zentrale Datei vergessen haben?

Image-Backups erstellen hingegen ein Abbild Ihrer Daten innerhalb der jeweiligen Umgebung. Es handelt sich um eine exakte Replikation des Servers – inklusive Betriebssystem, Konfiguration und Einstellungen. Fällt ein Server aus, können Sie ihn innerhalb von Minuten wieder in Betrieb nehmen – statt den Stunden oder Tagen, die es dauern würde, einen neuen Server anzufordern und das Betriebssystem zu installieren und zu konfigurieren.

IM KATASTROPHENFALL HANDLUNGSFÄHIG ZU BLEIBEN, IST FÜR KLEINE UNTERNEHMEN UND GROSSKONZERNE GLEICHERMASSEN WICHTIG.

Wichtige Bestandteile einer Business Continuity-Lösung

Nachfolgend sind die essenziellen Anforderungen an eine Business Continuity-Lösung aufgelistet:

- Hybrides Cloud-Backup: Ein hybrider Ansatz behebt die Schwachstellen einer reinen Cloud- oder lokalen Lösung.
- Optimale RTO und RPO: Achten Sie auf Business Continuity statt auf bloße Datensicherung. Berechnen Sie, wie viel Ausfallzeit Ihr Unternehmen standhält (RTO) und wie viel Datenverlust noch tolerabel ist (RPO).
- Image-basierte Backups: Sorgen Sie dafür, dass die Backup-Lösung ein Image aller Daten und Systeme statt lediglich von einer Auswahl an Dateien erstellt.

Fazit

Kleinere Unternehmen verfügen zwar über ein geringeres IT-Budget als Großkonzerne, ihre Daten aber sind denselben Risiken ausgesetzt. Der Markt für Datensicherungslösungen ist riesig. Egal für welche Lösung Sie sich auch entscheiden – Datensicherheit und Business Continuity sollten in Ihrem Unternehmen stets höchste Priorität genießen.

Über Datto

Datto wurde 2007 gegründet und ist einer der führenden Anbieter für Business Continuity-Lösungen weltweit. Mit innovativen, auf dem Markt einzigartigen Lösungen für jegliche Unternehmensgrößen und seiner mehr als 160 Petabyte großen Cloud bietet Datto bereits tausenden Managed Service Providern die Gewissheit, zuverlässig vor Datenverlust und dem Ausfall geschäftskritischer Systeme und Netzwerke geschützt zu sein.