

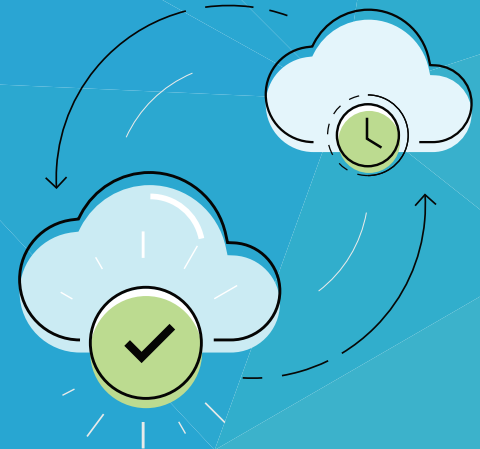
EBOOK

---

datto

# Backup vs. Business-Continuity

Gezielte Sicherheitsplanung  
für Ihr Unternehmen





**Datenschutzlösungen sind heutzutage für alle Unternehmen aller Arten unerlässlich, unabhängig von Größe, Standort und Industrie. In diesem White Paper wollen wir die Wichtigkeit von Business Continuity verglichen mit herkömmlichen Backups erörtern. Außerdem zeigen wir hier auf, wie Sie Ihre internen Recovery-Prozesse und Ihre Downtime-Kosten rasch evaluieren können, um die für Ihren Bedarf am besten geeignete Lösung zu finden.**

## Einführung

Downtime ist stets ärgerlich und teuer. Doch wie teuer ist sie wirklich? Je nach Größe der Organisation kann Downtime zwischen 7.000 und 700.000 Euro pro Stunde kosten. Deutsche Unternehmen verzeichnen im Durchschnitt 23,5 Stunden Downtime pro Jahr. Dies kostet die deutsche Wirtschaft Milliarden von Euros jährlich. Diese Zahlen sprechen für sich selbst.

Wodurch werden Ausfallzeiten verursacht? Netzwerkauswahl und menschliches Fehlverhalten sind für 50 % bzw. 45 % der Ausfälle verantwortlich. Naturkatastrophen verursachen hingegen nur 10 % Downtime. In den letzten Jahren hört man auch zunehmend von Malware und Ransomware, die durch die „Geiselnahme“ von Unternehmensdaten deren Freigabe erpressen.

In Bezug auf das betroffene Datenvolumen ist der Hauptgrund für Ausfallzeiten erneut menschliches Fehlversagen mit 58 Prozent. Die eigenen Mitarbeiter könnten einem Unternehmen also mehr Schaden zufügen als Naturkatastrophen.

Wenn Sie sich bisher noch nicht mit dem Schutz Ihrer Daten befasst haben, weil Ihr Unternehmen nicht in der Nähe eines Überschwemmungsgebiets ansässig ist, dürfen Sie nicht vergessen: Die größte Bedrohung Ihrer Daten kommt nicht außen, sondern von Ihrem Unternehmen.

## Was ist in Gefahr?



Täglich werden 2,5 Quintillionen Daten erzeugt. 90 % der derzeit existierenden Daten wurden in den letzten Jahren erzeugt, und ein signifikanter Anteil von kleinen und mittelständischen Unternehmen (KMU). Wenn man sämtliche Server, Desktops und Laptops bedenkt, die ein typisches KMU betreibt, resultiert dies in einer großen Datenmenge, die es zu schützen gilt.

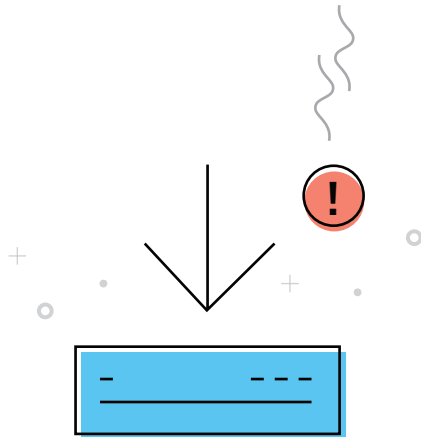
Trotzdem arbeiten fast 75 % aller KMU ohne Business-Contiuity und Disaster Recovery-Plan und nur 25 % sind „äußerst zuversichtlich“, dass sie kompromittierte Daten wiederherstellen könnten. Nur 50 % der KMU sichern weniger als 60 % ihrer Daten. Und die verbleibenden 40 %? Werden überhaupt nicht geschützt!

Wie viel kostet das? In den letzten Jahren kosteten Ausfallzeiten im Durchschnitt 35 % der befragten KMU bis zu 300.000 Euros. 3 Prozent der Befragten hatten sogar Einbußen von über 750.000 Euros.

Ransomware alleine kostete deutsche Unternehmen in 2016 über 4,5 Mio. Euros. Und 25 % derjenigen, die das Erpressungsgeld bezahlt hatten, erhielten ihre Daten dennoch nicht zurück.

Was geschieht im Katastrophenfall? Die Unternehmen müssen so schnell wie möglich versuchen, ihre wichtigen Daten wieder herzustellen. Laut IDG dauert es rund 7 Stunden, bis der Normalbetrieb nach einem Datenverlust wieder aufgenommen werden kann, und 18 % der befragten IT-Manager geben an, dass es 11-24 Stunden und sogar noch länger dauern kann.





In den letzten Jahren  
kosteten Ausfallzeiten  
35 % kleiner und  
mittelständischer  
Unternehmen bis zu  
300.000 Euro.

Die Aberdeen Group ermittelte vergleichbare Zahlen für Ausfallzeiten und Wiederherstellung bei einem Vergleich der Klassenbesten mit durchschnittlichen oder unterdurchschnittlichen Unternehmen. Wenn man die Durchschnittszeit der Wiederherstellung nach einer Ausfallzeit (5,18 Stunden) mit den durchschnittlichen Downtime-Kosten multipliziert, erhält man in jedem Fall eine hohe Rechnung.

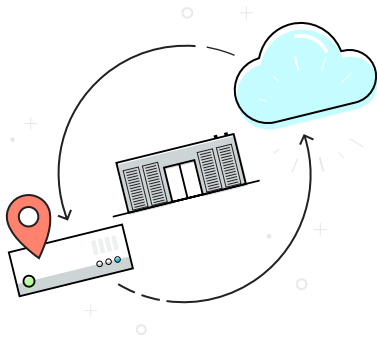
Diese Kosten entstehen durch verlorene Arbeitszeit, gesenkte Produktivität, die Kosten der Wiederherstellung, Verlust vorhandener und potenzieller Kunden, Rufschädigung sowie abgelenkte oder frustrierte Mitarbeiter und andere Stakeholder.

Was tun KMUs, um sich zu schützen? Über 60 % von ihnen schicken noch immer Tape Backups in ein Lager oder eine andere Niederlassung - eine erstaunliche Anzahl in Anbetracht dessen, dass diese Technologie mittlerweile über vier Jahrzehnte alt und die Lagerungs- und Wiederherstellungsprozesse extrem aufwendig sind. Mittlerweile nutzen fast 20 % eine Cloud-basierte Datensicherung.

## Datensicherung – lokal oder in der Cloud? Die Antwort lautet: beides.

Lokale Datensicherung erleichtert Business-Continuity durch rasche Wiederherstellung. Da sich die Daten vor Ort befinden, können sie rasch und leicht an ihrem Ursprungsort wiederhergestellt und der Betrieb kann möglichst rasch wieder aufgenommen werden. Doch was geschieht bei

Mehr als  
90 % kleiner  
Unternehmen gehen  
innerhalb von zwei  
Jahren nach einem  
schwerwiegenden  
Datenverlust  
in Konkurs.



einem Stromausfall? Oder wenn das Gerät ausfällt? Oder wenn es gestohlen, beschädigt oder durch eine Naturkatastrophe vernichtet wird? Man könnte annehmen, diese Gründe sprächen für eine Datensicherung in der Cloud. Die ausschließliche Datensicherung in der Cloud ist jedoch riskant, da man die Bandbreite nicht kontrollieren kann. Daher ist das Wiederherstellen der Daten manchmal schwierig und zeitaufwendig. Letztendlich kann auch die Cloud ausfallen.

Wie funktioniert eine hybride Cloud-Lösung? Hier werden die Daten zuerst kopiert und auf einem lokalen Speichermedium gesichert. Auf diese Weise können die Daten im Notfall rasch und leicht von diesem Gerät wiederhergestellt werden. Zusätzlich werden die Daten auch in der Cloud gespeichert. Falls also auch das Speichergerät ausfällt, gibt es eine ausgelagerte zweite Sicherungskopie der Daten in der Cloud und Sie brauchen sich nicht die Mühe zu machen, Ihre Daten physisch an einem anderen Ort aufzubewahren.

## Data Backup vs Business Continuity: Was ist der Unterschied?

Data Backup beantwortet die Frage: Sind meine Daten sicher? Kann ich sie bei einem Ausfall wiederherstellen?

Business-Continuity bedeutet hingegen, die Sicherheit des Unternehmens im Grossen und Ganzen zu betrachten und zu fragen: Wie schnell ist mein Unternehmen nach einem Systemausfall wieder einsatzbereit?



**Backup – lokal oder in der Cloud?**  
**Die Antwort ist eine kombinierte Lösung. Eine Hybrid Cloud verbindet die Vorteile der lokalen Datensicherung mit der Sicherheit der Cloud.**

Deshalb ist Backup im allgemeiner einer guter erster Gedanke. Business-Continuity ist ebenso wichtig, denn sie sorgt dafür, dass Ihre Organisation im Katastrophenfall zeitnah wieder einsatzfähig ist. Fällt beispielsweise Ihr Server aus, so könnten Sie nicht rasch weiterarbeiten, wenn Sie Ihre Daten nur lokal gespeichert haben. Der Server müsste ersetzt, Software und Daten erneut installiert und das gesamte System für Ihre bevorzugten Einstellungen konfiguriert werden. Dies könnte Tage in Anspruch nehmen. Kann sich Ihr Unternehmen leisten, so viel Zeit zu verlieren?

Wenn wir über Business-Continuity sprechen, denken wir an die angestrebten RTO- (Recovery Time Objective) und RPO- (Recovery Point Objective) Zeiten.

RTO: Recovery Time Objective oder RTO ist die Zeit, innerhalb der ein Unternehmen nach einer Störung wieder betriebsfähig sein muss, um inakzeptable Folgen zu vermeiden.

RPO: Recovery Point Objective oder RPO ist die maximal verträgliche Zeit, für die man im Katastrophenfall auf Daten verzichten kann.

Bei der Berechnung Ihres angestrebten RTO müssen Sie ermitteln, wie lange Sie ohne Ihre Daten auskommen, bevor Ihr Unternehmen gefährdet ist. Aus Ihrem RPO können Sie andererseits erkennen, wie häufig Backups durchgeführt werden müssen. Je nach den geschäftlichen Anforderungen kann Ihr RTO einen Tag und Ihr RPO eine Stunde betragen. Anhand dieser Kennzahlen können Sie ermitteln, welche Art von Lösung Sie zur Sicherung Ihrer Daten benötigen. (Siehe Abbildung 6).

Nach der Bestimmung von RPO und RTO sollten Sie berechnen, wie viel die Ausfallzeiten und der Datenverlust Sie tatsächlich kosten könnten. Fügen Sie

Die Berechnung der tatsächlichen Kosten eines Datenverlustes liefert Ihnen die finanzielle Rechtfertigung für Investitionen in eine Business-Continuity-Lösung.



dazu einfach den durchschnittlichen Stundenlohn, Ihre durchschnittlichen stündlichen Betriebskosten und die stündlichen Einnahmen, die Ihnen verloren gingen, dann wissen Sie, was der Datenverlust Sie kosten würde.

Alternativ dazu können Sie RPO, RTO und Downtime-Kosten rasch und leicht mit unserem kostenlosen, einfachen Online-RTO-Rechner berechnen.

Da die meisten Unternehmen mit einem beschränkten Budget auskommen müssen, rechtfertigen diese Kosten den Erwerb und die Nutzung einer Business-Continuity-Lösung.

## Image oder lediglich Datei-Backup

Zur Datensicherung gibt es zwei verbreitete Lösungen: Datei- oder Image-basiert, d. h., eine Abbildung des Systems.

Die dateibasierte Datensicherung funktioniert genauso, wie sie sich anhört: Sie wählen die Dateien, die gesichert werden sollen, und diese Dateien werden dann entsprechend der Lösung, die Sie gewählt haben, auf einem lokalen Speichergerät oder in der Cloud gesichert. In diesem Fall werden jedoch nur die ausgewählten Dateien gespeichert. Was wäre, wenn Sie eine wichtige Datei vergessen?

Bei der Image-basierten Datensicherung wird jedoch eine Abbildung Ihrer Daten in deren Umfeld erzeugt. Auf diese Weise können Sie genau replizieren, was auf Ihrem Server gespeichert ist, einschließlich Betriebssystem, Konfigurationen, Einstellungen und Präferenzen. Falls der Server abstürzt, können Sie ihn in Minutenschnelle wiederherstellen, anstatt Stunden oder sogar Tage damit zu verbringen, einen neuen Server zu erwerben, das Betriebssystem zu installieren und zu konfigurieren.

# Über Datto

Datto ist ein innovativer Anbieter umfassender Backup-, Recovery- und Business Continuity-Lösungen, die weltweit bereits von Tausenden von Managed Service Providern genutzt werden. Datto bietet Unternehmen jeder Größe über 300+ PB zweckgerichteter Cloud-, Software- und Hardware-Leistungen für den kompletten Datenschutz - immer und überall.

**Für mehr Informationen - [www.datto.com/de](http://www.datto.com/de)**

**datto**