Die 3-2-1-Regel für Backups ist fast schon Gesetz. Sie soll sicherstellen, dass durch eine effiziente Datensicherung keine Unternehmensdaten verloren gehen. Und das ist unwahrscheinlich wichtig – immerhin hängen ganze Existenzen von diesen Daten ab.

Kein Backup? Kein Mitleid!

Daten können immer irgendwie verloren gehen. Speichermedien können nach einer längeren Nutzungsdauer versagen; ein Blitzeinschlag oder ein Kurzschluss können die Hardware unbrauchbar machen; ein Hochwasser kann das gesamte IT-Netzwerk zerstören; sämtliche Daten können durch einen Hackerangriff verschlüsselt oder sogar zerstört werden; und auch so mancher falsche Klick hat schon zu massiven **Datenverlusten** geführt.
Und sind die Daten einmal weg, ist der Schaden unter Umständen gewaltig. Möglicherweise lassen sich Kundendaten, E-Mails und Termine nicht mehr aufrufen. Vielleicht sind auch sämtliche Rechnungen, Bestellungen oder Personalunterlagen weg. In vielen Fällen bedeutet das, dass wichtige – wenn nicht sogar alle – **Geschäftsprozesse zum Erliegen kommen**. Und das kostet Zeit und Geld und in ganz gravierenden Fällen sogar die Existenz des gesamten Unternehmens.
Dabei könnte alles so einfach sein. Schließlich gibt es umfassende Möglichkeiten zur Datensicherung. Eine ganz **bestimmte Backup-Strategie** sollten Sie sich dabei besonders dick hinter die Ohren schreiben – und deren Implementierung am besten schon heute in Angriff nehmen. Ihr Name: **3-2-1-Regel**.

Was ist die 3-2-1-Regel?

Die **3-2-1-Regel** gilt heute als **goldene Regel der Datensicherheit**. Im Grunde genommen ist die Formel sehr einfach: Es sollen **drei** Kopien oder Versionen aller Unternehmensdaten existieren, die auf **zwei** verschiedenen Speichermedien gesichert sind, von denen sich wiederum **eines** fern des Unternehmenssitzes befindet.
Das **3-2-1-Prinzip** geht dabei keineswegs auf einen IT-Fachmann zurück, sondern auf einen **Betroffenen**: Der Fotograph Peter Krogh sah sich selbst mit einem Verlust seiner Daten konfrontiert, entwickelte daraufhin die **3-2-1-Strategie** und machte sie 2009 in einem Buch öffentlich. Dass seine Strategie in

der Unternehmenswelt einmal zur goldenen Regel der Datensicherung aufsteigen würde, hätte er damals vermutlich nicht erwartet.
Inzwischen hat die 3-2-1-Regel schon sehr viele Unternehmen vor existenzbedrohenden Datenverlusten bewahrt. Bevor wir darauf eingehen, warum die 3-2-1-Regel für die Verfügbarkeit und den Schutz von Daten so wichtig ist, wollen wir aber noch einmal etwas genauer ins Detail gehen.

3 Kopien sind ein Muss

Die „3“ in dem Begriff 3-2-1-Regel steht dafür, dass drei Kopien aller Unternehmensdaten existieren sollten. Dabei ist es nicht ganz zutreffend, wenn von „Kopien“ die Rede ist, denn eigentlich handelt es sich einmal um **die Original-Daten** (auch **primäre Daten** genannt), die als Produktionsdaten in der täglichen Arbeit genutzt werden, und **zwei Kopien als Backups**.
Die Idee hinter dieser dreifachen Ausführung: Sollte eines der verwendeten Speichermedien beispielsweise einen Defekt aufweisen, wären immer noch zwei weitere Kopien vorhanden, sodass sich das defekte Gerät leicht ersetzen und mit den vorhandenen Daten aus einer der beiden übrigen Ausführungen bespielen lässt.
Mit jeder Backup-Kopie sinkt das **Ausfallrisiko** enorm: Mit der 3-2-1-Regel liegt das Risiko eines Datenverlusts bei 1:10.000. Im Vergleich dazu: Bei nur einer einzigen Version beträgt dieses Risiko 1:100. Sogar im Worst-Case-Szenario, in dem zwei Speichermedien parallel ausfallen, garantiert die dritte Kopie die Datensicherheit.

2 Speichermedien sichern ab

Es ist bereits angeklungen: Die verschiedenen Backups sollten auf **zwei unterschiedlichen Speichermedien** beziehungsweise Datenträgern hinterlegt sein – dafür steht die „2“ in 3-2-1-Regel. Es kann sich dabei beispielsweise um ein internes Festplattenlaufwerk und einen Wechseldatenträger (externe Festplatten, USB-Laufwerke, SD-Karten, Blueray etc.) handeln oder um zwei interne Festplattenlaufwerke an unterschiedlichen Speicherorten. Die Rede ist hier auch von einem ganz **bewussten „Medienbruch“**.
Aber warum ist dieser Punkt für die 3-2-1-Regel so entscheidend? Ganz einfach: Liegen die primären Daten und Backups an demselben Speicherort, können sie auch von demselben technischen Fehler ereilt werden. Und fällt eine Festplatte aus, kann es durchaus sein, dass kurz darauf eine weitere Festplatte desselben Speichersystems aussetzt.

Es geht letztlich also darum, **verschiedene Speichertechnologien** mit unterschiedlichen Ausfallwahrscheinlichkeiten einzusetzen und durch ihre Kombination das Risiko eines kompletten Datenverlusts massiv zu verringern – wenn nicht sogar vollkommen auszuschalten.

1 externer Aufbewahrungsort als Notnagel

Die „1“ in der 3-2-1-Regel bezieht sich auf einen unbedingt notwendigen **externen Aufbewahrungsort** für die dritte Version der Original-Daten. Der Grund für diese Notwendigkeit besteht in möglichen äußeren Einflüssen. Ein Hochwasser, ein Brand oder ein Kurzschluss können die Technik am Firmenstandort beschädigen oder gar zerstören. Und dann nützt es auch nichts, wenn es vor Ort eine, zwei, drei oder mehr Kopien der Unternehmensdaten gibt – die **physischen Speichermedien** wären in solchen Fällen gleichermaßen betroffen.
Daher ist es unabdingbar, dass ein Backup **fern des eigentlichen Firmenstandorts** liegt. Möglich ist, dass hier ein externer Datenträger zum Einsatz kommt, den der Geschäftsführer oder die Geschäftsführerin bei sich zuhause aufbewahrt – natürlich gut verschlüsselt und genauso gut abgeschlossen. Inzwischen ist aber immer mehr die Private Cloud als externer Aufbewahrungsort für Backups gefragt.
Hier stellt sich aber eine besondere Herausforderung: Das Firmennetzwerk und das Cloud-Backup müssen so gut wie möglich voneinander abgeschottet sein. Im Falle eines Cyberangriffs verschlüsseln die Angreifenden das Cloud-Backup ansonsten einfach mit – und die **Umsetzung der 3-2-1-Backup-Regel** wäre damit für die Katz.

Warum ist die 3-2-1-Regel so wichtig?

Es gibt viele Gründe dafür, dass die 3-2-1-Regel für Unternehmen unglaublich wichtig ist. Die drei wichtigsten Gründe stellen wir Ihnen in einer Auswahl vor:

1. **Ohne Daten geht es nicht**
   In vielen Unternehmen lässt es sich heute schlicht nicht mehr arbeiten, wenn der Zugriff auf die Unternehmensdaten nicht möglich ist. Das bedeutet, dass der Geschäftserfolg immer stärker von der **dauerhaften Datenverfügbarkeit** abhängt. Jeder Ausfall wird teuer, ein kompletter Datenverlust kann sogar die Existenz bedrohen.

2. **Daten sind zunehmend gefährdet**
   Auf der einen Seite entwickeln Cyberkriminelle täglich neue Schädlinge und Strategien, mit denen sie Unternehmensdaten massiv in Gefahr bringen. Auf der anderen Seite verfestigt sich die Vorhersage immer mehr, dass **Klimakatastrophen** wie das Hochwasser im Sommer 2021 künftig immer häufiger werden könnten. Und dadurch steigt auch die Gefahr für Unternehmensdaten durch äußere Einflüsse.
3. **Datenschutz gibt den Ton an**
   Der Schutz von (personenbezogenen) Daten ist inzwischen ein Muss für jedes Unternehmen. Datenschutzbehörden greifen immer härter durch und verhängen bei Verstößen saftige Strafen. Dass Unternehmen zu jeder Zeit die **Datenverfügbarkeit gewährleisten** müssen, ist Teil der mannigfaltigen Forderungen für einen umfassenden Datenschutz.

Sie sehen: Davor, dass die Umsetzung der 3-2-1-Regel unbedingt notwendig ist, sollte kein Unternehmen die Augen verschließen. Aber wie lässt sich so eine **3-2-1-Backup-Regel** am besten einführen?

IT-Fachleute setzen 3-2-1-Regel um

Am besten holen Sie sich für die Einführung der 3-2-1-Backup-Regel Fachleute an die Seite – sie lässt sich nämlich nicht von heute auf morgen erledigen. Stattdessen gehen ihr meist einige Überlegungen voraus und es gilt einige **Fragen** zu klären. Auf welchen Speichermedien sollen die drei Versionen hinterlegt sein? Wie häufig sollen die Backups der Original-Daten aktualisiert werden? Wer ist dafür verantwortlich, dass die Backups zuverlässig laufen? Und wie lässt sich die 3-2-1-Regel technisch umsetzen?

SET up Computersysteme GmbH ist Ihr Ansprechpartner in allen Fragen rund um Ihre Datensicherung !