techbold

BACKUP-STRATEGIE: LEITFADEN FÜR UNTERNEHMEN

EDITORIAL

Datensicherung ist Chefsache!

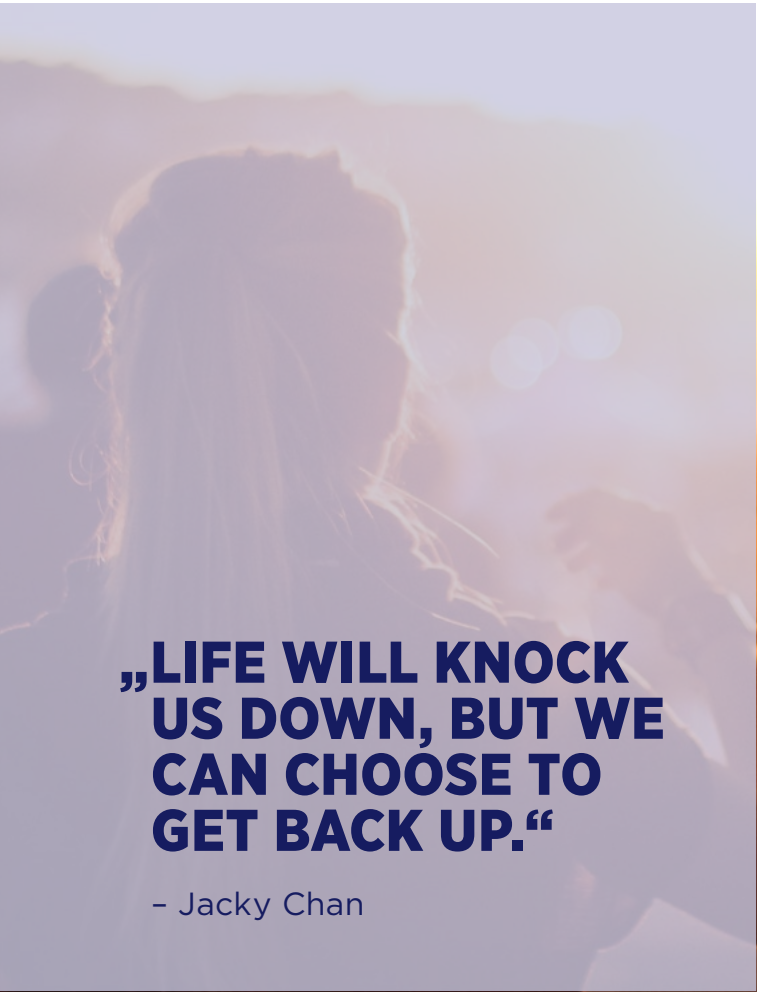
Professionelle Datensicherung ist für fast alle Unternehmen überlebenswichtig. Der Verlust von Daten kann schnell zum existenziellen Problem für jede Firma werden. Jeder Unternehmer muss wissen, welche Daten wichtig sind und wie schnell diese Daten im Worst Case wiederherstellbar sein müssen. Dieser Leitfaden bietet dir einen kompakten Überblick über die Grundlagen der Datensicherung und einen Einblick in die damit verbundenen Strategien sowie Methoden zu erhalten. So können weitere Entscheidungen, mit ausreichend Expertise untermauert werden.

Beste Grüße,

Damian Izdebski
techbold Gründer & CEO

INHALT

EINLEITUNG



Ein falscher Mausklick und weg ist sie – die Arbeit von mehreren Wochen oder gar Monaten. Alle Konzepte, Pläne, Rechnungen und Kundendaten verschwunden, irgendwo im virtuellen Nirvana. Gerade für kleinere und mittlere Unternehmen beginnt danach oft der Kampf ums blanke Überleben.

Cyber Crime macht Backups zum Muss

Regelmäßige Datensicherungen, genauer Backups, sind für alle Unternehmen ein Muss. Zu zahlreich sind die Möglichkeiten, (über-) lebenswichtige Unternehmens- und Kundendaten für immer zu verlieren. Hier ein bereits gekündigter Mitarbeiter, der „versehentlich“ einen wichtigen Ordner löscht, dort ein ausgewachsener Festplattencrash, der die komplette Firmen-IT in den Untergrund befördert.

Oder noch viel schlimmer (und vor allem auch wahrscheinlicher): Der vermehrt auftretende Verschlüsselungstrojaner Locky, welcher Daten verschlüsselt und somit unbrauchbar macht. Der Trojaner verbreitet sich durch Microsoft Office-Dokumente im Anhang von E-Mails, die meist in Form von Rechnungen verschickt werden. Nach dem Öffnen der angehängten Datei wird der User aufgefordert, einen im Dokument enthaltenen Makro-Code auszuführen, um die Rechnung zu sehen.

Bestätigt er dies vorschnell, ist’s auch schon passiert. Der Trojaner verschlüsselt alle Dateien auf den infizierten PCs. Eine Nachricht auf dem Bildschirm informiert den User über die soeben vorgenommene Verschlüsselung und weist darauf hin, dass man gegen Zahlung eines bestimmten Betrages, eine Software zum Entschlüsseln der Dateien erwerben könne. Entschließt man sich das „Lösegeld“ zu zahlen, ist freilich damit nicht garantiert, dass die Entschlüsselung auch klappt. Nicht vergessen darf man in diesem Sinne aber auch auf Elementarereignisse wie Hochwasser und Feuer, oder auf Einbrüche mit Diebstahl und Vandalismus.

GRUNDLAGEN DER BACKUP-STRATEGIE

Kosten-Nutzen-Rechnung für Backups

Besonders kleine und mittelständische Betriebe schrecken vor dem vermeintlichen Aufwand zurück, eine durchgehende Backup-Strategie zu entwerfen. Dabei lassen sie leider außer Acht, dass Aufwand und Kosten nach einem Daten-Verlust um ein Vielfaches größer sind, als eine kontinuierliche Speicherung. Im Grunde muss man sich nur zwei Fragen stellen und danach eine einfach Kosten-Nutzen-Rechnung anstellen.

> Wie lange ist es für mein Unternehmen vertretbar, dass die Firmen IT ausfällt?

> Wie relevant sind die elektronschen Daten für die Aufrechterhaltung des Betriebs?

Die Antworten unterscheiden sich von Unternehmen zu Unternehmen erheblich. Eine Tischlerei mit fünf Mitarbeitern und einem Chef, der fast alle seine Kunden und Lieferanten persönlich kennt, kann einen IT-Ausfall klarerweise leichter (und länger) verkraften als eine Steuerberatungskanzlei mit hunderten Kunden, sensiblen Daten und verbindlich vorgegebenen Terminen (Umsatzsteuermeldungen an das Finanzamt, Jahresabschlüsse usw.).

Achtung Aufbewahrungspflicht!

Zu beachten ist, dass (Finanz-) Aufzeichnungen, die dazugehörigen Belege sowie die für die Abgabenerhebung bedeutsamen Geschäftspapiere und sonstigen Unterlagen von Gesetzes wegen für mindestens sieben Jahre aufzubewahren sind. Auch alle elektronischen Aufzeichnungen einer Registrierkasse unterliegen dieser Aufbewahrungspflicht. Und man darf eigentlich davon ausgehen, dass sich das Finanzamt hier nicht mit dem „Erinnerungsvermögen“ des Unternehmers zufriedengeben wird. Professionelle Backup-Lösungen können solche Anforderungen selbstverständlich im Vorhinein berücksichtigen.

Die Experten-Faustregel zur Backup-Strategie

Überhaupt muss sich jede sinnvolle Backup-Strategie an den Erfordernissen des jeweiligen Unternehmens orientieren, um den Aufwand und die Kosten zu optimieren. Als generelle Experten -Faustregel gilt:

Einmal wöchentlich ein komplettes Backup.

Täglich ein Backup der tagesaktuell veränderten Daten.

Je nach Unternehmens-Anforderung lassen sich die Zeiträume verlängern oder verkürzen. Hier stellt man sich die Frage: „Welchen Datenverlust (in Arbeitstagen) kann ich problemlos verkraften?“. Hinzu kommt – wenn im Unternehmen benötigt – ein Backup des Mailservers, wobei dieses im Regelfall mehrmals täglich abläuft.

Backup Verantwortlicher?

Auch sollte verbindlich geklärt werden, wer für das Datenbackup verantwortlich ist und über welchen Zeitraum die Backup-Dateien dann aufbewahrt werden sollten. Experten empfehlen hier mindestens einen Monat, aber je länger desto besser – und sicherer.

DIE UNTERSCHIEDLICHEN BACKUP-METHODEN

Um die beste Backup-Strategie für das eigene Unternehmen zu entwickeln, muss auch die richtige Technik gewählt werden. Grundsätzlich unterscheidet man drei unterschiedliche Methoden des Backups: Die Volldatensicherung und die differentielle sowie die inkrementelle Sicherung.

Volldatensicherung

Alle zu sichernden Daten werden zu einem vorgeschriebenen Zeitpunkt auf einen Zieldatenträger geschrieben. Bei der nächsten Sicherung werden dann erneut sämtliche Dateien gesichert. Damit die Vollständigkeit aller Datenbestände nicht von einem einzigen Backup abhängt, sollten immer mehrere Generationen der Sicherungen aufgehoben werden. Im Regelfall wird einmal pro Woche (vorzugsweise an den Wochenenden) ein Vollbackup durchgeführt. Sehr vorteilhaft ist, dass alle Daten vollständig vorliegen und bei Bedarf schnell gefunden werden können. Als nachteilig erweist sich die Tatsache, dass diese Volldatensicherung viel Zeit und Speicherplatz in Anspruch nimmt.

Inkrementelle Sicherung

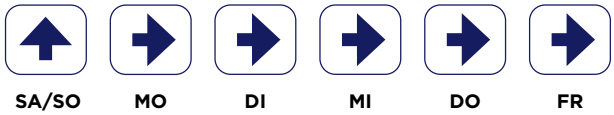
Auf Basis einer zuvor durchgeführten Volldatensicherung, werden anschließend nur noch jene Daten gesichert, die sich seit der letzten Sicherung verändert haben oder hinzugefügt wurden. Hier wird vergleichsweise wenig Speicherplatz gebraucht und das Backup ist schnell erledigt. Im Ernstfall ist der Aufwand, die Daten wiederherzustellen, aber ungleich höher als bei einer Volldatensicherung. Es werden nämlich alle Dateien einer „Sicherungskette“ zur Wiederherstellung benötigt.

Differentielle Sicherung

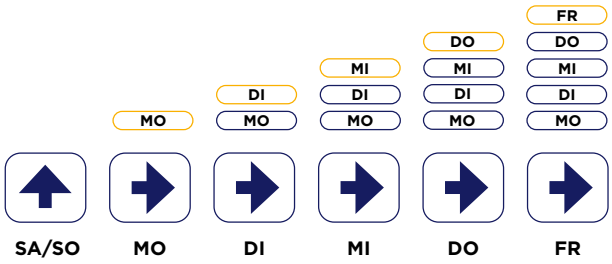
Wie die inkrementelle basiert auch diese Methode auf einem vorherigen Volldaten-Backup. Anschließend werden bei jeder Folgesicherung die Daten gespeichert, die sich seitdem verändert haben. Für eine Wiederherstellung werden demnach zwei Dateien, also die Basis-Vollsicherung und die letzte differentielle Backup-Datei benötigt. Eine differentielle Sicherung benötigt weniger Speicherplatz als eine Volldatensicherung, allerdings mehr, als ein inkrementelles Backup.

Schnellübersicht der Backup-Methoden

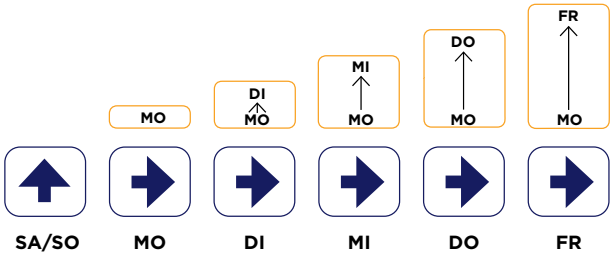
Volldatensicherung: Einmal pro Woche, bevozugt am Wochenende, wird ein komplettes Backup aller Daten gemacht.



Inkrementelle Sicherung: Aufbauend auf Volldatensicherung, werden jeweils alle Daten gesichert, die sich seit der letzten Sicherung verändert haben. Für eine wiederherstellung benötigt man die volle „Sicherungskette“.

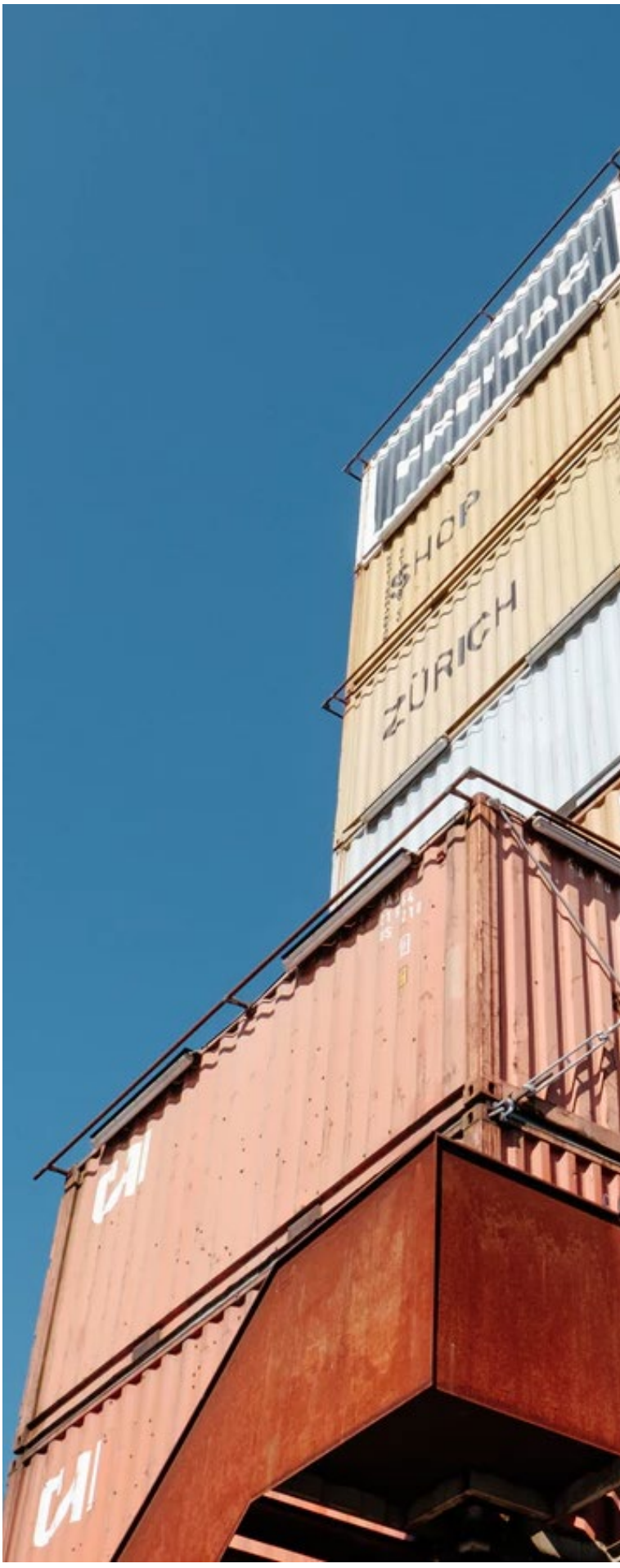


Differentielle Sicherung: Im Gegensatz zu der inkrementellen Sicherung werden aufbauend auf Volldatensicherung, an jedem Sicherungspunkt alle Daten gesichert, die sich seit dem Vollbackup verändert haben. Zur Wiederherstellung braucht man also nur die aktuellste differentielle Sicherung und das Vollbackup.



Fazit

Welche dieser Variante für ein Unternehmen am sinnvollsten ist, kommt auf die Menge an Daten an und darauf, wie häufig diese Daten geändert werden. Für die meisten kleineren und mittleren Unternehmen hat sich ein tägliches (inkrementelles oder differentielles Backup), sowie eine wöchentliche Volldatensicherung als guter Kompromiss zwischen Aufwand und Datensicherheit erwiesen. Im schlimmsten Fall bedeutet das nämlich, dass „nur“ die Arbeit eines Tages verloren geht.



DIE UNTERSCHIEDLICHEN SPEICHER MEDIEN

Backup auf externe Festplatten

Externe Festplatten gibt es inzwischen mit sehr hohen Speicherkapazitäten von bis zu mehreren Terabytes. Sie sind mobil und haben eine recht hohe Lebensdauer.

Cloud-Backup

Immer beliebter wird auch die Datensicherung in der so genannten Cloud, zumal das Angebot in diesem Bereich immer breiter wird. Das Backup in der Cloud sollte aber immer nur ein zusätzlicher Speicherort sein, keinesfalls der einzige. Außerdem musst du darauf achten, dass die Übertragung verschlüsselt passiert und zudem gut überlegen, wem du deine sensiblen Firmendaten anvertraust. Anbieter, die auf österreichische Rechenzentren setzen, solltest du bevorzugen, da hierzulande strenge Datenschutz- und Sicherheitsbestimmungen gelten. Bei internationalen Anbietern (auch wenn sie klingende Namen haben) kann man sich nie ganz sicher sein, wo die Daten schlussendlich wirklich landen. Vor allem wenn auch Kundendaten gesichert werden, kann man da schnell in einen Konflikt mit den österreichischen Datenschutz-Richtlinien und der EU-DSGVO geraten.

NAS-Backup

Bei einem NAS (Network Attached Storage) handelt es sich um eine zentrale Netzwerkfestplatte mit PC-ähnlichen Funktionen. Sie eignet sich für kleine und große Unternehmen. Zusammen mit der richtigen Backup-Software hat man ohne großen Aufwand einen zentralen Datenspeicher, der die Daten von allen PCs nach festen Zeitschemen oder via Knopfdruck sichert.

RAID-Backup

Bei diesem System werden mehrere Festplatten zu einem Laufwerk organisiert. Das sorgt für mehr Schutz, da dieses Laufwerk eine deutlich höhere Sicherheit beim Ausfall einzelner Festplatten als eine normale Festplatte erreicht. Das heißt: Ein System ist weiter einsatzfähig, auch wenn eine Festplatte kaputtgeht. Gleiches gilt auch für die Arbeitsdaten darauf, da diese auf einer zweiten Platte gespiegelt sind.

ACHTUNG!

Bei einem RAID-System handelt es sich um keine richtige Datensicherung im Sinne eines Backups, sondern nur um einen Minimalschutz vor einem kompletten Systemstillstand. Das wird von vielen Unternehmen leider nach wie vor falsch verstanden bzw. falsch eingeschätzt.

Streamer-Backup

Bei Streamern handelt es sich um eine recht alte, aber nach wie vor bewährte Speichermöglichkeit. Hierzu werden Backups auf Magnetbändern gespeichert – vergleichbar mit Kassetten- oder Videorekordern. Eine Wiederherstellung nach einem Datenverlust ist allerdings recht langwierig und auch das Handling der Magnetbänder ist umständlich und zeitaufwändig.

IN 8 SCHRITTEN ZUM EFFEKTIVEN BACKUP

1

Die 3-2-1 Daten-Backup-Regel

Mit dieser einfachen Methode kannst du die Wahrscheinlichkeit eines Datenverlusts stark minimieren. Konkret bedeutet das, dass eine 3-fache Kopie der Daten (auch der „Live-Daten“ an denen gearbeitet wird) mit zwei verschiedenen Technologien (Festplatte, NAS, Cloud …) anzufertigen, wobei dann eine Kopie immer außer Haus sein muss. Funktioniert ein Backup (oder ein Datenträger) nicht, kann auf das zweite zurückgegriffen werden. Sehr wichtig ist vor allem, dass man ein Backup außer Haus aufbewahrt (etwa in der Cloud) – denke hier beispielsweise an die Möglichkeit eines Brandes der das komplette Firmengebäude zerstört.

2

Selbst erzeugte Daten sichern

Alle Daten, die man im Unternehmen selbst erzeugt, müssen auch gesichert werden – egal, ob Geschäftsbriefe, Präsentationen, Buchhaltungs- oder Produktinformationen. Programminstallationsdateien müssen nicht gesichert werden, da diese durch eine Neuinstallation wiederhergestellt werden können.

3

Verantwortlichkeiten klären

Bestimme einen Mitarbeiter der für die Datensicherung zuständig ist bzw. als Ansprechpartner für einen eventuellen IT-Dienstleister fungiert. Damit können Kompetenzkonflikte und die Tatsache, dass man sich gerne auf andere verlässt („Der Kollege wird die Daten schon gesichert haben“), vermieden werden.

4

Backup-Software

Automatisiere deine Backup-Routinen. Manuelle Sicherungsprozesse sind sehr fehleranfällig. Überprüfe täglich, ob der Backup-Job wirklich ausgeführt wurde (Protokolldateien).

5

Von der Firmen-IT abkoppeln

Trenne das Backup von der Firmen-IT. Ein doppeltes Speichern auf einem Server reicht nicht aus, um Datensicherheit zu gewährleisten. Nutze beispielsweise Cloud-Computing.

6

Wichtige Dokumente zusätzlich sichern

Eine zusätzliche Kopie von Daten, die im Geschäftsalltag nicht mehr geändert werden (etwa Verträge oder Patente), sollte auf einem Datenträger in einem Safe verwahrt werden.

7

Backups überprüfen

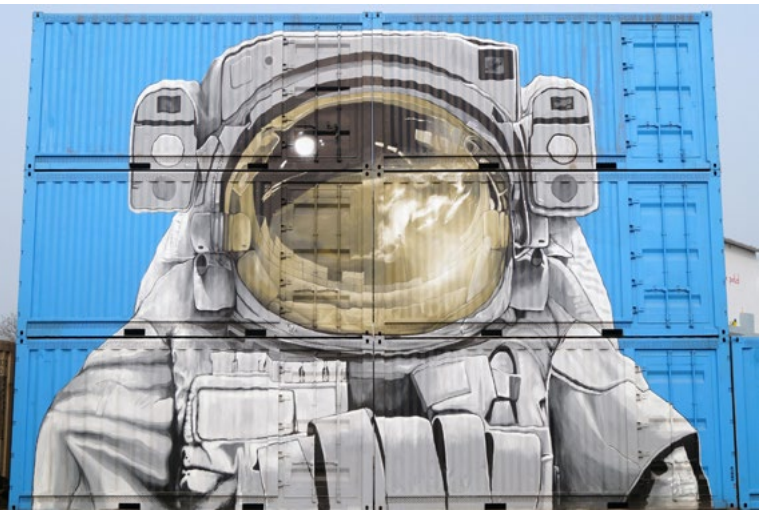
Prüfe regelmäßig (viertel- oder halbjährlich), ob sich die Backup-Dateien aufrufen und wiederherstellen lassen.

8

Systeme Anpassen

Wechselt das Unternehmen auf ein neues Betriebssystem, muss auch die Datensicherung entsprechend angepasst werden.

PRÜFUNG DER EIGENEN BACKUP-ROUTINE



Auch wenn du bereits eine laufende Datensicherungsroutine hast, gibt es noch einiges zu erkunden – z. B. ob sie funktionstüchtig ist.

Routine bedeutet nicht immer Sicherheit

Den meisten Unternehmen ist völlig klar, dass eine regelmäßige Datensicherung der Geschäftsdaten absolut essentiell ist. Jedoch laufen oft automatisierte Backups ab, die aber allesamt ein großes Problem haben: Seit ihrer Implementierung wurden sie nie mehr beachtet und die Backup-Dateien schon gar nicht auf ihre Funktionalität überprüft. Umso schlimmer ist die Überraschung, wenn sich die vermeintliche Datensicherung im Ernstfall als wertlos erweist und du herausfindest, dass Teile des Backups unvollständig sind, oder es gar leer ist. Oftmals ist es der Fall, dass zwar täglich ein Speichermedium angeschlossen wird, aber auf dem Datenträger selbst gar nichts drauf ist.

Backups per Schnelltest prüfen

Stell deine IT-Abteilung oder deinen IT-Dienstleister (falls du die Datensicherung ausgelagert hast) einfach Mal auf die Probe. Bitte darum, die Datei X und das Mail Y (beide müssen wirklich existieren bzw. existiert haben) von voriger Woche wiederherzustellen, da du sie „versehentlich“ gelöscht hast. Wenn du die beiden Dateien nicht spätestens am nächsten Tag vorliegen hast, dürfte es wohl ein paar Probleme mit deiner Datensicherung geben. Ist das der Fall musst du dem unbedingt nachgehen. Natürlich kannst du die Verantwortlichen auch um eine komplette Wiederherstellung eines Backups bitten, allerdings sind der Aufwand und die Kosten in diesem Fall weitaus höher.

Backups im Detail prüfen

In diesem Fall, ist es am besten das Backup einmal komplett zurück zu spielen. Nun gilt es zu prüfen, ob der Server und alle Dienste wie gewünscht funktionieren und in weiterer Folge das konkrete Vorhandensein der Dateien zu testen. Die Durchführung eines solchen „Disaster Recovery Kompletttests“ ist jedoch sehr kompliziert und zeitintensiv. Zu aller erst muss man die Festplatte des getesteten Servers komplett löschen. Stellt man an diesem Punkt fest, dass das Backup nicht erfolgreich war, bleibt nichts als ein defektes System zurück. Daher empfiehlt es sich den Test auf einem identischen, aber nicht im Einsatz befindlichen, Gerät durchzuführen. In weiterer Folge muss mit Hilfe eines „Rescue-Mediums“ (spezielle Boot-CD oder bootbarer Wechselträger) der Backup-Test gestartet und alle Daten zurückgespielt werden. Der ganze Vorgang ist nicht ungefährlich und sollte am besten von einem professionellen IT Dienstleister durchgeführt werden.

Vereinfachte Prüfung durch Virtualisierung

Professionelle IT-Dienstleister setzen heute auf Virtualisierung. “Virtuelle Maschinen“, sozusagen virtuelle Abbilder deiner Computer und Server, erleichtern unter anderem sowohl die Datensicherung als auch ihre Überprüfung. So lässt sich ein Desaster Recovery Kompletttest durch das Duplizieren der virtuellen Abbilder nicht nur sicher, sondern auch aus der Ferne durchführen.

ÜBER TECHBOLD

Von IT-Consulting bis IT-Betrieb

Alles aus einer Hand. Mit der stetig zunehmenden Komplexität von IT-Systemen gilt es das „große Ganze“ im Blick zu behalten. IT-Themen können nicht isoliert betrachtet werden. Sie greifen ineinander, bauen aufeinander auf und ergänzen sich. Unser Ziel ist eine funktionierende, zukunftsfähige und skalierbare Unternehmens-IT zu schaffen.

Deshalb bietet techbold IT-Lösungen aus einer Hand.

Unsere techbold IT-Experten analysieren deinen Bedarf und beraten herstellerunabhängig. Wir gewährleisten die zuverlässige Umsetzung jedes Projekts mit sicheren, effizienten und zukunftsfähigen IT-Lösungen.

LERNE UNS KENNEN

Wir von techbold sind ein langjährig erfahrenes Team von IT & Computer Experten und Pionieren. Uns verbindet die gemeinsame Leidenschaft für Technologie und für die Vernetzung der Menschen untereinander. Wir sind überzeugt, dass uns Mut und Leidenschaft sowohl als Mensch, als auch als Unternehmen besser und erfolgreicher macht.

JOCHEN JASCH
Head of Sales

+43 660 562 4361
+43 59 555 719
jja@techbold.at

TECHBOLD IT-SOLUTIONS WIEN
techbold secure IT GmbH
Dresdner Straße 89, 1200 Wien
+43 59 555 | office@techbold.at

TECHBOLD IT-SOLUTIONS OBERÖSTERREICH
techbold secure IT GmbH
Business Center Plus City, Plus-Kauf-Straße 7,
4061 Pasching, Oberösterreich
+43 59 555 | office@techbold.at

TECHBOLD IT-SOLUTIONS BURGENLAND
techbold secure IT GmbH
Werner von Siemens-Straße 1, 7343 Neutal
+43 59 555 | office@techbold.at