Die Gefahr eines Datenverlusts betrifft jedes Unternehmen!

So bauen Sie sich ein Sicherheitsnetz für Ihre Daten.

KEYWEB

Server. Cloud. Domains.

Vorwort

Ob ein Unternehmen erfolgreich ist, oder nach wenigen Monaten bis Jahren wieder von der Bildfläche verschwindet, hängt von vielen Faktoren ab.

Einer der wichtigsten ist die Tatsache, dass sich Entscheidungen und Prozesse im Unternehmen optimal am Markt ausrichten. Zwei weitere Faktoren sind Schnelligkeit und Effizienz – in Reaktionen, Prozessen und in der Entwicklung.

Moderne Technologien sind hierfür häufig die Lösung. Sie ermöglichen eine beachtliche Zeit- und Kostenersparnis. Auch die Vernetzung, welche über das Internet möglich ist, befähigt Unternehmen zu einem Grad an Effizienz, welcher vor ein paar Jahrzehnten noch pure Science Fiction war. Doch all dies hat eine riesige Kehrseite. Wenn Sie diese nicht kennen, setzen Sie Ihr komplettes Business aufs Spiel.

Redaktionsteam
der Keyweb AG

Inhalt

Impressum

Keyweb AG

Neuwerkstraße 45/46
D-99084 Erfurt
Tel.: +49 (0) 361 / 6 58 53-0

info@keyweb.de
keyweb.de

Das Risiko von Digitalisierung, Cloud, KI & Co.

Überall dort, wo Prozesse schnell und automatisiert laufen und viele – wahrscheinlich auch sehr sensible Daten – auf elektronischem Weg übermittelt und gespeichert werden, herrscht eine **unsichtbare Gefahr für genau diese Daten.**

Datendiebstahl und -manipulation.
Sicherheitslücken – durch menschliche Fehler, fehlende Updates oder heimtückische Cyberkriminelle.

Einflüsse höherer Gewalt wie Umweltkatastrophen.

Diese und andere Gefahren sind leider niemals komplett auszuschließen.

Somit lauert eine große **Gefahr für Unternehmen direkt in modernen Technologien** sowie interner, aber auch cloud-basierter und externer Speicherung von Daten.

Sind Ihnen diese Gefahren bewusst, können Sie passende Schutzmaßnahmen ergreifen. Doch sind Ihnen diese nicht oder nur unzureichend bewusst, kann es zu **verheerenden Folgen** kommen. Für Sie, für Ihr Unternehmen und für Ihre Kundinnen und Kunden.

Die verheerenden Folgen eines Datenverlusts

In der Vergangenheit kam es auch bei großen, bekannten Unternehmen zu einem Totalausfall durch Cyberattacken, Brand oder Umwelteinflüsse. Derartige Vorfälle können das **Image eines Unternehmens nachhaltig schädigen**.

Daten sind häufig das Fundament für alle Geschäftsabläufe. Sie sind das Rückgrat eines Unternehmens. Dies wird vielen Verantwortlichen leider oft erst dann schmerzlichst bewusst, wenn die wertvolle Datenbasis ganz ohne Vorankündigung von heute auf morgen verschwunden ist oder durch Kriminelle verändert oder verschlüsselt wurde.

Datenverlust oder die Nicht-Verfügbarkeit der IT-Struktur können nicht nur zu **erheblichen finanziellen Einbußen** durch Umsatzeinbrüche, Betriebsunterbrechungen und Wiederherstellungskosten führen – auch das Vertrauen der Kunden, Geschäftspartner und Mitarbeiter kann hierdurch nachhaltig geschmälert werden.

Die Folgen: Kündigungen und vermutlich auch noch rechtliche Konsequenzen. In extremen Fällen und bei unwiederbringlichen Datenverlusten kommt es zur **temporären oder vollständigen Betriebsschließung**.

Würde Ihr Unternehmen einen solchen Datenverlust überleben?

> *Unternehmen jeder Größe, deren Geschäftsprozesse auf digitalen Daten basieren, müssen sich **vor diesen Risiken schützen**, wenn sie langfristig bestehen möchten.*

Ursachen von Datenverlust

Cyberangriffe

Hardwarefehler

Softwarefehler

menschliche Fehler

Naturkatastrophen

Stromausfall

Einbruch oder Diebstahl

fehlerhafte Migration

Das nahezu unzerstörbare Sicherheitsnetz

Es gibt viele hilfreiche Sicherheitsmaßnahmen, die Sie ergreifen können, um Ihre IT und die hier gespeicherten Daten effektiv zu schützen. Jedoch gibt es nur eine, welche Ihnen als ein nahezu unzerstörbares Sicherheitsnetz dient.

Ein Backup ist ein extrem wichtiger Bestandteil eines umfassenden Datensicherheitskonzepts für Unternehmen.

Genau genommen ist es die wichtigste Sicherheits-Maßnahme, die Sie ergreifen können, um einen relevanten oder kompletten Datenverlust langfristig zu verhindern.

Es bietet das Sicherheitsnetz, was auch nach dem größten Datenunglück Ihre verlorenen oder beschädigten Geschäftsdaten wiederherstellen kann – sodass Ihr Geschäft nahezu unterbrechungsfrei weiterlaufen wird.

Was wirklich zählt ist, dass diese Daten nach einem Datenverlust vollständig und schnell wieder zur Verfügung stehen. Daher sollte das Backup regelmäßig durchgeführt, überprüft und aktualisiert werden.

Warum ein Backup hochindividuell sein muss

Um durch ein Backup im Ernstfall wirklich abgesichert zu sein, reicht es nicht aus, die Daten irgendwie, irgendwo und irgendwann zu sichern. Sie benötigen eine klare, bis ins Detail geplante Backup-Strategie.

Kein Unternehmen ist wie ein anderes. Auch Ihr Unternehmen ist absolut individuell - und somit auch die Art und Weise, wie die Unternehmensdaten in regelmäßigen Abständen gesichert werden müssen.

*Damit das Backup die nötigen Sicherheitsanforderungen erfüllt, sollte es **hochgradig auf Ihr Unternehmen** und die hier **vorherrschenden Abläufe und Gegebenheiten abgestimmt sein**.*

Für Unternehmen ist es besonders relevant, **verschiedene Backup-Methoden und Technologien so zu kombinieren**, dass eine für sie hocheffiziente und effektive Sicherungsmethode entsteht.

Mit einem **umfassenden und auf Sie abgestimmten Backup-Plan** minimieren Sie die Risiken und stellen sicher, dass im Ernstfall eine schnelle Wiederherstellung der Daten möglich ist.

Mit einem individuellen Backup können Sie:

» nach einem Cyberangriff oder anderen IT-Notfällen die verlorenen oder beschädigten Daten schnell und vollständig wiederherstellen.

» die Geschäftskontinuität auch im Fall eines solchen Vorfalls sicherstellen, indem Sie den Datenzugriff sowie den Geschäftsbetrieb schnell wieder ermöglichen.

» rechtliche Anforderungen an Datenverarbeitung und -sicherung erfüllen.

» Daten vor Upgrades oder Migrationen sichern, sodass auch bei einem Fehler die Daten wiederhergestellt werden können.

» sich vor Ransomware und der damit einhergehenden Forderung nach Lösegeld schützen.

Wir möchten Ihnen zeigen, was Sie beachten müssen, **um Katastrophenszenarien aufgrund von Datenverlust von vornherein vermeiden** zu können.

Sie werden erfahren, welche Methoden sich bewährt haben und wie Sie selbst Ihre Backup-Strategien entwickeln und optimieren können, um auf **maximale Datensicherheit** vertrauen zu können.

Sie erhalten einen **umfassenden Leitfaden** an die Hand, der Sie dabei unterstützen wird, **die besten Backup-Lösungen für Ihr Unternehmen** zu **identifizieren** und zu **realisieren**.

> *Wenn Ihre IT hohe Sicherheitsstandards erfüllt, wird sich dies auch direkt oder indirekt positiv auf das Vertrauen und die Zufriedenheit Ihrer Kundinnen und Kunden sowie Mitarbeiterinnen und Mitarbeiter auswirken.*

Erste initiale Fragen für ein sicheres Backup

Wenn Sie eine **wirklich sichere Backup-Strategie** für sich erstellen möchten, müssen Sie zuvor grundsätzliche Überlegungen treffen. Die folgenden Seiten werden Ihnen dabei helfen.

Neben der Anzahl und der Frequenz der Datensicherung ist es wichtig, **welche Daten gesichert werden sollen**.

Dies ist für jedes Unternehmen sehr individuell, da in Abhängigkeit der Tätigkeit und des Digitalisierungsgrades hier ganz unterschiedliche Anforderungen bestehen können.

Für manche Unternehmen genügt es, ein- oder zweimal in der Woche eine Sicherung aller Daten vorzunehmen, andere wiederum müssen Teile ihrer Daten mehrmals am Tag – wenn nicht sogar stündlich oder in noch kürzeren Intervallen – in Form eines Backups sichern.

Es macht beispielsweise einen großen Unterschied, ob an Ihrer Website zweimal im Monat Änderungen vorgenommen werden, oder ob dies sogar mehrmals in der Woche geschieht.

In welchen Intervallen Sie Ihre Datensicherungen vornehmen sollten, hängt von Ihren Anforderungen ab!

Ebenso wichtig ist es, zu entscheiden, welche Daten häufiger und welche seltener gesichert werden müssen.

5 Fragen für Ihre individuelle Backup-Strategie

Für Ihre individuelle Backup-Strategie setzen Sie sich bitte mit den folgenden Fragen auseinander. Diese helfen Ihnen später, abzuschätzen, wo Sie Schwerpunkte bei der Datensicherung setzen sollten.

1. Welche Daten müssen gesichert werden, damit nach einem Datenverlust alles schnell wieder reibungslos laufen kann?

Die Antwort auf diese Frage hängt vor allem damit zusammen, welche Daten Sie regelmäßig nutzen und ändern. Denken Sie hierbei nicht zu oberflächlich!

Wenn Sie zum Beispiel einen gut besuchten Onlineshop betreiben und hier regelmäßig Bestellungen eingehen, reicht es nicht aus, wenn Sie lediglich das Bestellsystem an sich sichern. Die Datenbank mit allen Kundendaten sowie aktuelle Bestellungen müssen ebenso schnell wieder zur Verfügung stehen, wenn das Geschäft nach einem Datenausfall zeitnah weiterlaufen soll.

Notizen:

2. Welche Arten von Daten müssen Sie für Ihre Datensicherung berücksichtigen?

Pauschal lässt sich das natürlich nicht beantworten – wir möchten Ihnen jedoch eine grobe und generelle Übersicht geben, an der Sie sich orientieren können:

- **Domain-Daten:** Alle Daten, die zu einer bestimmten Domain zählen
- **E-Mails**, welche sich beispielsweise auf einem separaten E-Mail-Server befinden
- **Dateiserver:** Server, auf denen verschiedenste Unternehmensdaten gespeichert sein können
- **Anwendungen:** Programme, welche in Ihrem Unternehmen verwendet werden und ggf. hiermit verbundene Daten
- **Datenbanken:** für unterschiedlichste Zwecke gespeicherte Daten in Form von Datenbanken
- **Netzwerke:** sämtliche Netzwerke, über welche innerhalb Ihres Unternehmens Daten übermittelt werden
- **Betriebssystem-Daten** und **Konfigurationen**

All diese Systeme können von einem Datenverlust betroffen sein. **Web- und Datenbankserver sind beispielsweise sehr häufige Ziele von Cyberangriffen.** Regelmäßige Backups der Systeme stellen sicher, dass Websites und Datenbanken im Falle eines Angriffs schnell wiederhergestellt werden können.

Auch **Kommunikationsdaten** können für Unternehmen essentiell sein. Damit diese nicht verloren gehen, müssen E-Mail-Server, Chat-Plattformen und andere Kommunikationstools mit ihren Inhalten gesichert werden.

Notizen:

3. In welchen Intervallen sind welche Daten zu sichern?

Die Antwort auf diese Frage hängt in hohem Maß mit Ihren **regelmäßigen Geschäftsabläufen** zusammen. Genau genommen: **in welcher Regelmäßigkeit und in welchen Zeitabständen** welche Abläufe erfolgen. Website ist nicht gleich Website, Shop nicht gleich Shop und Unternehmen nicht gleich Unternehmen.

Bei einem Online Shop ist es beispielsweise auch wichtig, entsprechende Datenbanken in den notwendigen und passenden Zeitintervallen zu sichern. Es macht einen Unterschied, ob Ihre Daten stündlich geändert werden, einmal am Tag oder einmal in der Woche. Beim zuvor genannten Shop ist es auch wichtig, entsprechende Datenbanken in den notwendigen und passenden Zeitintervallen zu sichern.

Angenommen, es gehen stündlich mehrere Bestellungen in Ihrem Shop ein. Sollten Ihre Daten heute verloren gehen, bringt es Ihnen nichts, wenn Sie den gestrigen Stand der Bestellungen wiederherstellen. Je nach Höhe Ihrer Produktpreise könnten Ihnen damit mehrere Tausend Euro verloren gehen – und bisher zufriedene Kunden gleich mit.

Notizen:

4. Welchen Speicherplatz benötigen die zu sichernden Daten?

Aus dieser Frage heraus können Sie später ableiten, welche Sicherungsmethode für Sie besonders effizient ist.

Gerade wenn die Zeitintervalle zwischen den einzelnen Sicherungen eher gering sind, sollten Sie darauf achten, dass die einzelne Sicherung an sich nicht zu viel Zeit und Speicherplatz in Anspruch nimmt. Sie können verschiedenen Backup-Methoden optimal miteinander kombinieren, sodass ein sehr gutes Kosten-Nutzen-Verhältnis in Bezug auf Ihr Backup entsteht. Hierzu erfahren Sie auf den folgenden Seiten mehr.

Notizen:

5. Gibt es ganz bestimmte Zeitpunkte, zu denen Ihre Unternehmensdaten auf jeden Fall immer noch einmal gesichert werden müssen?

Auch dieser Punkt ist sehr individuell. Beispielsweise kann ein Backup immer sinnvoll sein, kurz bevor Sie bestimmte Updates vornehmen.

Machen Sie sich bitte auch zu diesem Punkt Notizen.

Notizen:

Mehr als trockene Theorie

Backup-Arten und ihre Eigenschaften

Sie können kein gutes Backup-Konzept erstellen, wenn Sie nicht die verschiedenen Backup-Arten kennen. Wenn Sie grundsätzlich wissen, wie Sie diese für die Sicherung Ihrer Daten einsetzen können, können Sie das Backup optimal auf die Sicherheitsbedürfnisse Ihres Unternehmens ausrichten.

Lokale Backups – direkt bei Ihnen vor Ort

Lokale Backups befinden sich in der Regel direkt in Ihrem Unternehmen auf physischen Geräten – also auf unternehmensinternen Servern und Festplatten. Dies hat Vor- und Nachteile.

Dadurch, dass die Daten sich direkt bei Ihnen vor Ort befinden, kann ein **höheres Sicherheitsgefühl** entstehen.

> *Kleiner Hinweis:*
> *Je nach örtlichen Gegebenheiten muss das subjektive Sicherheitsgefühl nicht der Realität entsprechen, da auf die Sicherheit viele Faktoren einzahlen.*

Lokale Backups auf eigenen Servern zeichnen sich durch **schnelle Wiederherstellungszeiten** aus.

Die Daten befinden sich am gleichen Standort wie die Primärdaten und **können somit bei einem IT-Notfall ebenfalls betroffen sein**, insbesondere wenn es sich um Diebstahl oder Umwelteinflüsse handelt.

Die Herausforderung kann darin bestehen, dass die Geräte **regelmäßig gewartet werden müssen** und auch sehr **anfällig für physische Schäden** wie Feuer, Hardware-Ausfälle oder Diebstahl sind.

Entsprechende Sicherheitsmaßnahmen müssen Sie selbst im Unternehmen vornehmen. **Sie tragen also eine sehr große Verantwortung** für den Betrieb und die Sicherheit der Geräte sowie die Funktionsfähigkeit des Backups.

Die **Wiederherstellung** der Daten liegt in der Regel **in Ihrer Hand**.

Cloud Backups – Datensicherung an einem externen Ort

Cloud-Backups werden auf externen Servern gespeichert - in der Regel bei einem Cloud-Anbieter. Hierbei gibt es Dienstleister, welche ihr eigenes Rechenzentrum betreiben und welche, die wiederum Rechenzentren anderer Anbieter nutzen.

Der Cloud- bzw. Hosting-Anbieter ist verantwortlich für die Funktionalität der Hardware und somit für die Verfügbarkeit Ihrer Daten.

Sie als Unternehmen und Cloud-Nutzer kümmern sich um die Funktionalität des Backups selbst. Sie stellen also sicher, dass dies korrekt eingerichtet ist und auch entsprechend funktioniert. Möchten Sie bei einem Cloud-Backup nicht selbst dafür verantwortlich sein, können Sie bei den Anbietern auch so genannte Managed Services nutzen, was eine große Erleichterung sein kann, wenn Sie beim Thema Backup (noch) unsicher sind.

Backups in der Cloud bieten neben einer **hohen Flexibilität und Skalierbarkeit auch eine hohe Ausfallsicherheit** – vorausgesetzt der Anbieter setzt entsprechende Sicherheitsmaßnahmen ordnungsgemäß um.

Die **Daten sind von überall aus verfügbar** – daher bieten sich diese Backups auch besonders für Unternehmen mit geografisch verteilten Standorten an.

Weiterhin bieten sie den Vorteil, dass die Daten **standortgetrennt von den Originaldaten gespeichert** werden – ein zusätzlicher und wichtiger Sicherheitsaspekt.

Werden die Daten nur unzureichend verschlüsselt, kann sich die Standort-Trennung und geografische Verteilung der Daten wiederum als Nachteil erweisen. **Backup-Sicherheit sollte die wichtigste Voraussetzung sein.**

Hybride Backups – die Backup-Kombination

Hybrid-Backups verbinden lokale Datensicherung und Cloud-Backups – und somit auch die Eigenschaften dieser Backup-Varianten.

Diese Strategie bietet **zusätzliche Sicherheit und Flexibilität**, indem sie zahlreiche Sicherheitskriterien für Backups erfüllt.

Durch die Kombination von lokalen Speichermedien und der Datensicherung in der Cloud erleichtert diese Methode die Einhaltung der 3-2-1-Backup-Regel. Die **Cloud bietet eine zusätzliche Redundanz**.

Besonders Unternehmen mit einem hohem Bedarf an Speicherkapazitäten oder mehreren Standorten profitieren von einem Cloud-Speicher, welcher lokale Sicherungen ergänzt.

Das hybride Backup ist allerdings **komplexer als andere Varianten**. Die Implementierung und Verwaltung dieser Lösung ist somit **aufwendiger**.

Damit einher gehen auch **höhere Kosten für die nötige Infrastruktur** sowie die Einrichtung und Wartung dieser.

Kombinieren Sie diese Backup-Typen

zu einem hocheffizienten Backup-Konzept

Ein wichtiges Ziel für Unternehmen sollte es sein, Prozesse so zu gestalten, dass der Ressourceneinsatz möglichst gering ist – bei gleichzeitig optimiertem Output. Auch Ihr Backup muss nicht nur sicher sein, sondern sollte auch so angelegt werden, dass es **möglichst effizient gespeichert und gegebenenfalls auch wiederhergestellt werden** kann.

Um dies realisieren zu können, müssen Sie verschiedene Backup-Strategien in Kombination einsetzen: das **vollständige Backup, das differenzielle Backup und das inkrementelle Backup**! Je nach Backup-Typ beansprucht ein Backup mehr oder weniger Speicherplatz und ist langsamer oder schneller in der Datensicherung oder in der Wiederherstellung. Wir erklären Ihnen die Backup-Typen hier im Detail.

Vollbackup für die schnelle & einfache Wiederherstellung

Ein vollständiges Backup **sichert jede Datei auf einem System** und kann je nach Backup-Software entweder in einer einzelnen Backup-Datei oder in mehreren Dateien gespeichert werden. Da dabei das gesamte Dateisystem gesichert wird, **nimmt diese Backup-Art in der Regel viel Zeit in Anspruch**.

Eine alleinige Verwendung dieser Backup-Methode würde auf Dauer zu einer sehr **hohen Speicherbelastung** für Ihr gewähltes Speichermedium führen. Vollständige Backups werden deshalb gern **in Kombination mit dem differenziellen oder dem inkrementellen Backup** eingesetzt, welche in den nächsten Abschnitten erklärt werden. Sie sind sozusagen die Grundlage für weitere Sicherungen.

Dauer der Datensicherung: Sicherung dauert verhältnismäßig lange

Dauer der Wiederherstellung: schnellste und einfachste Backup-Art in der Wiederherstellung

Speicherplatzverbrauch: Speichern von Duplikaten verbraucht viel Speicherplatz

Besonders effizient: das synthetische Vollbackup

Eine besondere Form des Vollbackups ist das synthetische Vollbackup. Es erstellt ein **vollständiges Backup, ohne alle Daten bei jedem Mal neu zu sichern**. Es kombiniert ein früheres vollständiges Backup mit mehreren inkrementellen Backups, um eine aktuelle, vollständige Sicherung zu generieren.

Dadurch werden **nur die geänderten Daten** seit dem letzten vollständigen Backup **hinzugefügt**, **ohne dass alle Daten erneut kopiert werden müssen**.

Im Vergleich zum normalen vollständigen Backup, bei dem jedes Mal die gesamte Datenmenge gesichert wird, **spart** das synthetische Backup **sowohl Zeit als auch Speicherplatz**. Das normale vollständige Backup erfasst hingegen jedes Mal alle Daten von Grund auf, was zu längeren Sicherungszeiten und höherem Speicherverbrauch führt.

Differenzielles Backup – die Ergänzung zum Vollbackup

Ein differenzielles Backup baut auf einem vollständigen Backup auf. Von dieser Backup-Art ist immer dann die Rede, wenn die **Differenz zum letzten Vollbackup** gesichert wird. Das heißt: **Alle Daten, die sich seit dem letzten vollständigen Backup geändert haben** oder neu hinzugekommen sind, werden in einer Backup-Datei zusammengefasst.

Stellen Sie sich vor, Sie machen jeden Sonntag ein Vollbackup und von Montag bis Samstag jeweils ein differenzielles Backup. Am Donnerstagmorgen kommt es zu einem Datenverlust.

Um Ihren aktuellen Datensatz wieder zu erhalten, müssen Sie zwei Backup-Dateien wiederherstellen:

1. das Vollbackup vom Sonntag und

2. das differenzielle Backup vom Mittwoch, d.h.: eine Zusammenfassung aus allen Änderungen, die am Montag, Dienstag und Mittwoch stattgefunden haben.

Dauer der Datensicherung: schneller als die Vollsicherung, langsamer als die inkrementelle Sicherung

Dauer der Wiederherstellung: schneller als die inkrementelle Sicherung, langsamer als die Vollsicherung

Speicherplatzverbrauch: weniger Speicherplatzbedarf als bei einer Vollsicherung

Inkrementelles Backup

Ein **inkrementelles Backup** setzt ein Vollbackup voraus und **sichert** nur die **Daten,** die sich **seit dem jeweils letzten Backup** geändert haben.

Im Gegensatz zum differenziellen Backup werden die **Änderungen vom Vortag nicht auf den aktuellen Tag übertragen**. Dadurch, dass bei einem inkrementellen Backup **immer nur die Daten gesichert werden, die sich innerhalb eines Tages geändert haben, verbraucht** diese Backup-Art **am wenigsten Speicherplatz**.

Gehen wir davon aus, dass Sie jeden Sonntag ein Vollbackup durchführen möchten und von Montag bis Samstag jeweils ein inkrementelles Backup.

*Um Ihre Daten nach einem Datenverlust am Samstagmorgen wieder komplett zu erhalten, müssen Sie die **gesamte Sicherungskette wiederherstellen**. Dazu gehören: das Vollbackup vom Sonntag und jedes einzelne inkrementelle Backup vom Montag, Dienstag, Mittwoch, Donnerstag und Freitag. **Der Prozess der Wiederherstellung ist also deutlich aufwendiger als bei den anderen Backup-Typen.***

Dauer der Datensicherung: der Sicherungsvorgang nimmt von allen Varianten am wenigsten Zeit in Anspruch

Dauer der Wiederherstellung: aufwendigste Backup-Art in der Wiederherstellung

Speicherplatzverbrauch: pro Backup wird am wenigsten Speicherplatz beansprucht

Das System-Backup

Neben den drei Datei-Backup-Typen gibt es auch das System-Backup. Dieses bezieht sich nicht nur auf ein bestimmtes Dateisystem oder eine Datenbank, sondern auf ein komplettes System. **Hierbei wird ein Systemabbild des installierten Betriebssystems erstellt, inkl. aller Systemdateien, installierten Programme und Konfigurationen**. Man erhält einen **Snapshot aller Laufwerke, die zum Ausführen des jeweiligen Betriebssystems relevant sind**.

Anstatt alle Dateien einzeln wiederherzustellen, kann im Fall eines schwerwiegenden Softwareproblems ein **komplett betriebsbereites System wiederhergestellt werden (Restore)**. **Das spart im Vergleich zu einer Neuinstallation jede Menge Zeit**. Der Nachteil besteht in der relativ hohen Speicherkapazität, welche benötigt werden könnte – abhängig von der Frequenz und der Größe des Snapshots.

Wie genau die Backup-Arten miteinander kombiniert werden, wird sich ganz individuell und in Abhängigkeit von den Anforderungen Ihres Unternehmens gestalten. Hier spielt es wieder eine Rolle, wann, wie oft und welche Daten geändert werden.

Mit diesen Backup-Prinzipien wird

Ihr Backup – so sicher wie ein Hochsicherheitstresor

Damit Ihr Backup so sicher ist, dass es wirklich vor aktuellen Bedrohungen und typischen Fehlen sowie Defekten geschützt ist, muss es ganz bestimmte Kriterien erfüllen.

Einige dieser Kriterien lassen sich leichter abdecken, wenn man Backup-Regeln und -Methoden einhält. Die wichtigsten Regeln sind zwar kein Geheimnis, werden aber immer noch gern ignoriert. Wir möchten Ihnen diese hier an die Hand geben – damit Sie es besser machen.

Mithilfe dieser Prinzipien können Sie sich beim Thema Backup wirklich sicher sein.

Die optimale Anzahl der Backups festlegen – mit der 3-2-1 Backup-Regel

Diese Regel umfasst die drei wichtigsten Grundprinzipien für Ihr Backup, mit denen Sie – wenn Sie alle drei einhalten, Ihre Daten bereits sehr zuverlässig schützen können.

3

Sie sollten mindestens **drei Kopien**, also Backups, erstellen. Das klingt eventuell erst einmal viel, aber wenn Sie die weiteren Prinzipien kennen, wird der Grund hierfür verständlich.

2

Die Datensicherungen sollten sich auf mindestens **zwei verschiedenen Datenträgern** befinden, z.B. lokal auf einem Backup-Server, auf einem Netzwerkspeicher (NAS) oder Cloud Storage.

1

Mindestens eine Kopie Ihrer Daten sollte sich an einem separaten Ort befinden, z.B. online in der Cloud eines **deutschen zertifizierten Rechenzentrums.**

Sinnvolle Backup-Routinen: mit der Mehrgenerationen Backup-Methode

Indem Sie Ihre **Daten regelmäßig sichern**, minimieren Sie das Risiko von Datenverlusten enorm. Denn nur wenn die sich **regelmäßig verändernden Unternehmensdaten auch entsprechend häufig gesichert** werden, kann auch eine aktuelle Kopie der Daten im Notfall zu Verfügung stehen. Leider wird dieser Punkt dennoch noch viel zu selten berücksichtigt. Machen Sie es besser!

Eine beliebte Backup-Methode, welche Ihre Datensicherung optimieren wird, ist das **Großvater-Vater-Sohn-Backup**. Ziel ist es, hiermit eine **lückenlose Datensicherung so effizient wie möglich durchzuführen**.

Das Prinzip beruht darauf, stets unterschiedliche Versionen der Daten für die Datensicherung bereitzuhalten.

Es gibt in jeder Woche z.B. jeweils vier Tagessicherungen (Sohn-Backups), die mit jeder neuen Woche einzeln überschrieben werden.

Weiterhin gibt es 4 Wochensicherungen (Vater-Backups), die bis zum Monatsende erhalten bleiben und wochenweise im nächsten Monat überschrieben werden.

Außerdem gibt es in der Regel bis zu 12 Monatssicherungen, die auch nach spätestens 12 Monaten einzeln von neuen Monatssicherungen überschrieben werden (Großvater-Backups).

Keine Backup-Prokrastination: mit der Automatisierung von Backups

Wenn Sie von nun an ständig überlegen müssten, wann Sie wieder ein Backup durchführen sollten – oder wenn ständig etwas anderes wichtiger wäre, wäre dies ein unnötiger Risikofaktor für Ihre Daten – und ein zusätzlicher Stressfaktor für Sie! **Machen Sie es sich einfacher!**

Die Lösung sind **automatisierte Backups**. Diese **reduzieren die Wahrscheinlichkeit von menschlichen Fehlern** auf ein Minimum und gewährleisten, dass Ihre Datensicherungen **zuverlässig und konsistent durchgeführt** werden.

- **Zeiteffizienz:** Automatisierte Backups sparen Zeit und reduzieren den Arbeitsaufwand für IT-Teams.
- **Konsistenz:** Regelmäßige und konsistente Backups minimieren das Risiko von Datenverlusten.
- **Reduktion menschlicher Fehler:** Automatisierte Prozesse reduzieren das Risiko menschlicher Fehler, die bei manuellen Backups auftreten können.
- **Benachrichtigungen und Berichte:** Automatisierte Systeme bieten oft Benachrichtigungen und Berichte, die IT-Teams über den Status der Backups informieren und mögliche Probleme frühzeitig erkennen lassen.

In diesem Zusammenhang ist es wichtig zu klären, **welche Vorgänge automatisiert durchgeführt werden können** und welche aus diversen Gründen doch besser manuell ausgeführt werden sollen.

Zur Automatisierung Ihrer Backups stehen Ihnen verschiedenste Technologien zur Verfügung, auf die wir später genauer eingehen werden.

Verschlüsselung Ihrer Daten: Auch Ihr Backup muss geschützt sein

Ihr Backup enthält genau wie Ihre Originaldaten vermutlich viele sensible Informationen, welche weder manipuliert noch ausspioniert werden sollten.

Mit **Verschlüsselungstechniken** schützen Sie Ihre Backups z.B. bei der Datenübertragung vor unbefugtem Zugriff und Cyberangriffen. Hierbei ist natürlich wichtig, dass ein **hoher Verschlüsselungsstandard** eingehalten wird, damit Unbefugte keinen Zugriff auf Ihre Daten haben. Hiermit sollte eine **interne Zugriffssicherung** einhergehen. Nicht jeder im Unternehmen darf Zugriff auf sensible Daten bekommen – das gilt natürlich auch für den Zugriff auf Backups!

Eine der am häufigsten eingesetzten Methoden ist die **AES-Verschlüsselung (Advanced Encryption Standard)**, insbesondere in der **256-Bit-Variante**, die sich durch ihre hohe Sicherheit und Effizienz auszeichnet. Sie ist international als Standard anerkannt.

Für die sichere Übertragung und Speicherung von Daten kommt häufig die **Public-Key-Verschlüsselung** zum Einsatz, bei der Verfahren wie **RSA** verwendet werden, um eine gesicherte Kommunikation zwischen verschiedenen Parteien zu ermöglichen.

Darüber hinaus sorgt eine **End-to-End-Verschlüsselung** dafür, dass Daten sowohl während der Übertragung als auch im Ruhezustand umfassend geschützt sind. Um die Integrität der gesicherten Daten zu gewährleisten, werden zusätzlich **Hashing-Algorithmen wie SHA-256** genutzt, die eine Manipulation der Daten erkennen und verhindern können.

Nur ein funktionierendes Backup ist ein gutes Backup!

Sie erstellen regelmäßig Backups und wiegen sich in Sicherheit und dann passiert es: ein kompletter Datenverlust. Aber Sie haben ja Ihr Backup, das – Schock! Nicht funktioniert.

Eine solche Situation gilt es unbedingt zu vermeiden. Möglich ist das mit einem **regelmäßigen Backup-Wiederherstellungstest**. Dieser überprüft, ob die gesicherten Daten im Ernstfall vollständig und fehlerfrei wiederhergestellt werden können. Dabei werden nicht nur die Integrität der Backups, sondern auch die Effizienz der Wiederherstellungsprozesse bewertet.

Sie sollten entsprechende Tests regelmäßig in Ihre IT-Sicherheitsstrategie integrieren, um sicherzustellen, dass alle Daten im Falle eines Ausfalls, einer Cyber-Attacke oder anderer Zwischenfälle schnell und vollständig wieder verfügbar sind. So lassen sich Schwachstellen frühzeitig erkennen und beheben, was die Betriebskontinuität und Datensicherheit erheblich stärkt.

Regelmäßige Überprüfungen der Wiederherstellungsprozesse sind mindestens genauso wichtig wie Ihr Backup selbst.

Backup-Lösungen & Tools für die Umsetzung Ihres Backups

All die genannten Backup-Strategien und -Methoden diszipliniert durchzuführen, kann durchaus herausfordernd sein – insbesondere, wenn man sie manuell und selbst umsetzen möchte.

Hier kommen **Backup-Software-Lösungen** ins Spiel, die Unternehmen dabei unterstützen, **regelmäßig und vor allem sicher Kopien ihrer Daten zu erstellen**. So können diese im Ernstfall schnell und vollständig wiederhergestellt werden.

Mit entsprechenden Lösungen ist es möglich, Backups automatisiert und regelmäßig in den gewünschten und definierten Intervallen durchzuführen. Diese Tools übernehmen auch die nötige Datenverschlüsselung bei der Übertragung und Speicherung der Daten.

Typen von Backup-Lösungen

Es gibt verschiedene **Typen von Backup-Software**, die jeweils unterschiedliche Bedürfnisse abdecken:

1. **On-Premise-Backup-Lösungen:** Diese Lösungen werden auf unternehmenseigenen Servern installiert und ermöglichen eine hohe Kontrolle über den Backup-Prozess. Sie sind besonders für Unternehmen geeignet, die strenge Compliance-Anforderungen erfüllen müssen und ihre Daten nicht extern speichern möchten.

2. **Cloudbasierte Backup-Lösungen:** Diese Lösungen speichern Backups in der Cloud, was vor allem für Unternehmen mit verteilten Standorten oder dezentralen Arbeitskräften attraktiv ist.

3. **Hybrid-Backup-Lösungen:** Eine Kombination aus On-Premise und cloudbasierten Lösungen, die das Beste aus beiden Welten vereint. Unternehmen können so eine flexible Backup-Strategie entwickeln, die sowohl lokalen Speicher als auch die Sicherheit und Skalierbarkeit der Cloud nutzt.

Es gibt eine Vielzahl von Backup-Softwarelösungen, die unterschiedliche Funktionen und Sicherheitsoptionen bieten.

Bei der Auswahl der passenden Backup-Software sollten Sie **darauf achten, dass die Lösung eine einfache Verwaltung und Wiederherstellung der Daten ermöglicht**, insbesondere bei der Bewältigung großer Datenmengen und komplexer IT-Infrastrukturen.

Damit Sie bei der Auswahl einer passenden Backup-Software eine gute Entscheidung treffen können, sollten Sie sich an den folgenden Kriterien orientieren.

Kriterien für gute Backup-Lösungen

1. **Automatisierung und Zeitplanung:** Die Software sollte automatische Backups nach einem festgelegten Zeitplan durchführen können, um menschliche Fehler zu minimieren.

2. **Verschlüsselung:** Sowohl die Datenübertragung als auch die Speicherung der Backups sollten mit starken Verschlüsselungsalgorithmen geschützt werden.

3. **Skalierbarkeit:** Die Lösung muss in der Lage sein, mit dem Wachstum des Unternehmens und der Menge der zu sichernden Daten Schritt zu halten.

4. **Wiederherstellungsoptionen:** Eine gute Backup-Software bietet flexible und schnelle Wiederherstellungsoptionen, sowohl für komplette Systeme als auch für einzelne Dateien.

5. **Speicheroptionen:** Es sollte die Möglichkeit bestehen, Backups an mehreren Orten zu speichern, inklusive lokaler Speicher, externer Rechenzentren und Cloud-Dienste.

6. **Benutzerfreundlichkeit:** Eine intuitive Benutzeroberfläche und einfache Verwaltung sind entscheidend, um den Aufwand für das IT-Team zu minimieren.

7. **Compliance und Sicherheit:** Die Software sollte die Einhaltung relevanter rechtlicher und regulatorischer Anforderungen unterstützen, einschließlich der DSGVO.

8. **Support und Updates:** Regelmäßige Software-Updates und ein zuverlässiger Support sind unerlässlich, um die langfristige Sicherheit und Funktionalität der Lösung sicherzustellen.

Durch die sorgfältige Auswahl einer Backup-Software, die diese Kriterien erfüllt, können Unternehmen ihre Daten effektiv sichern und sich vor den verheerenden Folgen eines Datenverlusts schützen.

Wir möchten an dieser Stelle noch betonen, dass Sie die Verantwortung für Ihr sicheres Backup an kein Tool komplett abgeben dürfen. Sie selbst müssen immer wieder den Sinn und den Erfolg Ihrer Backups überprüfen.

Proxmox Backup-Server für besondere Anforderungen

Der Proxmox Backup-Server (PBS) ist eine **besonders leistungsstarke und effiziente Lösung** für die Sicherung und Wiederherstellung Ihrer Unternehmensdaten.

Er bietet Ihnen die Möglichkeit, **virtuelle Maschinen und Container, die auf Proxmox VE basieren, schnell und effektiv zu sichern** und wiederherzustellen.

Auch georedundante Backups lassen sich mit PBS umsetzen. Mit der benutzerfreundlichen Oberfläche gestaltet sich das Backup Ihrer IT-Struktur **effizient und übersichtlich**.

Effiziente Sicherung

Dank der verwendeten Sicherungstechnologie werden **nur die geänderten Datenblöcke gesichert**, was viel Speicherplatz spart und Ihre Backup-Zeiten verkürzt. Die inkrementellen Backups sorgen dafür, dass **nur die Änderungen seit dem letzten Backup** gesichert werden. Dies reduziert die Netzwerklast und beschleunigt den Backup-Prozess.

Starke Verschlüsselung

Ihre Daten sind dank der **integrierten Verschlüsselungsfunktion** jederzeit sicher. So können Sie darauf vertrauen, dass nur autorisierte Personen Zugriff auf Ihre wertvollen gesicherten Daten haben.

- Planen Sie mit dem Client im Proxmox Backup-Server **ganz einfach regelmäßige Backups** nach Ihren Bedürfnissen und **automatisieren Sie somit den gesamten Prozess**, um menschliche Fehler zu minimieren. Hierbei können Sie ganz individuell **Zeitpläne für Ihre Datensicherung** erstellen. In diesem Zusammenhang können Sie auch eine Verifizierung Ihrer Daten einrichten, sodass deren Integrität, also Korrektheit, sichergestellt ist.

- Dank integrierter **Monitoring- und Reporting-Funktionen** behalten Sie den Überblick über Ihre Backup-Prozesse einschließlich detaillierter Einblicke und Benachrichtigungen bei Auffälligkeiten.

- Im Falle eines Systemausfalls profitieren Sie von den **umfassenden Wiederherstellungsfunktionen des Proxmox Backup-Servers**. Sie können Ihre Daten so wiederherstellen, dass diese dem **Stand eines gewünschten Zeitpunkts** entsprechen. **Ausfallzeiten werden minimiert und die Geschäftskontinuität gewahrt.**

*Backup-Software dient dazu, die nötigen **Schritte der Datensicherung automatisiert durchzuführen.***

Sie bietet verschiedenste Funktionen, die weit über das bloße Kopieren von Dateien hinausgehen.

*Die verschiedenen Backup-Arten wie differenzielle oder inkrementelle Backups können planmäßig erstellt werden, wodurch nur geänderte oder neue Daten gesichert werden und die **Datensicherung hocheffizient** geschehen kann.*

*Backup-Tools bieten die nötigen Verschlüsselungsoptionen, um die Daten **während der Übertragung und Speicherung** vor unbefugtem Zugriff zu **schützen**.*

Backup-Service:

Damit Ihnen Ihr Backup nicht über den Kopf wächst

Wie Sie an dieser Stelle sicher schon erkannt haben, ist „Backup" so viel mehr als nur ein kleiner Server in einem Serverraum, auf den einmal in der Woche alle Daten Ihres Unternehmens übertragen werden.

Ein gutes Backup erfordert vor allem eine **gute Planung und eine bewusste und individuelle Auswahl geeigneter Strategien**. Hinzu kommt die regelmäßige **korrekte Durchführung** und **Überprüfung** der Backup-Prozesse.

Wenn Sie sich auf Ihr Kerngeschäft konzentrieren möchten, kann dies unter Umständen auch sehr überfordernd sein – denn schließlich wollen Sie doch einfach nur ein Backup. **Sollten Ihnen die Ressourcen oder das Wissen für ein effizientes Backup im Unternehmen fehlen, können Backup-Services die Lösung sein.**

Planung **Datenspeicher** **Software** **Durchführung** **Überprüfung**

Ein Backup-Service umfasst neben dem Speicherort auch die Sicherung, Verwaltung und Wiederherstellung Ihrer Daten durch den Service-Anbieter. Diese Variante bietet Ihnen somit einige Vorteile:

» **Planung und automatisierte Ausführung von Backups**: Es werden Sicherungskopien Ihrer Daten erstellt, ohne dass manuelle Eingriffe erforderlich sind. Dies minimiert von Anfang an das Risiko menschlicher Fehler und garantiert Ihnen, dass Ihre Daten regelmäßig gesichert werden.

» **Überwachung und Benachrichtigungen:** Ihre Sicherungskopien werden kontinuierlich überwacht und Sie werden benachrichtigt, wenn Fehler oder Probleme auftreten. Dadurch können potenzielle Probleme frühzeitig erkannt und behoben werden, bevor sie zu Datenverlust führen.

» **Wiederherstellungsoptionen:** Der Backup-Service bietet in der Regel Optionen für die Wiederherstellung Ihrer Daten, wenn dies einmal nötig ist.

> *Ein sogenannter Managed Service Provider (MSP) kann Sie bei der Bereitstellung, Verwaltung und Überwachung von Backup- und Wiederherstellungslösungen unterstützen. Anstatt Sie als Unternehmen Ihre eigenen Backup-Systeme aufbauen und betreiben, übernimmt der MSP diese Aufgabe als **Managed Service**.*

Die **Entscheidung zwischen Backup-Storage und Backup-Service** hängt von mehreren Kriterien ab, darunter die Größe und Komplexität Ihres Unternehmens, Ihre Datenmanagementanforderungen, das Budget und die internen Ressourcen.

Wenn Sie über **interne IT-Ressourcen** verfügen und die **erforderliche Expertise** haben, um den **Backup-Prozess selbst zu verwalten**, können Sie sich **für ein Backup-Storage entscheiden**. Sie müssen **möglicherweise zusätzlich Zeit und Ressourcen investieren**, um Backups zu planen, durchzuführen und zu überwachen – aber es kann eine kostengünstigere Lösung für Sie sein.

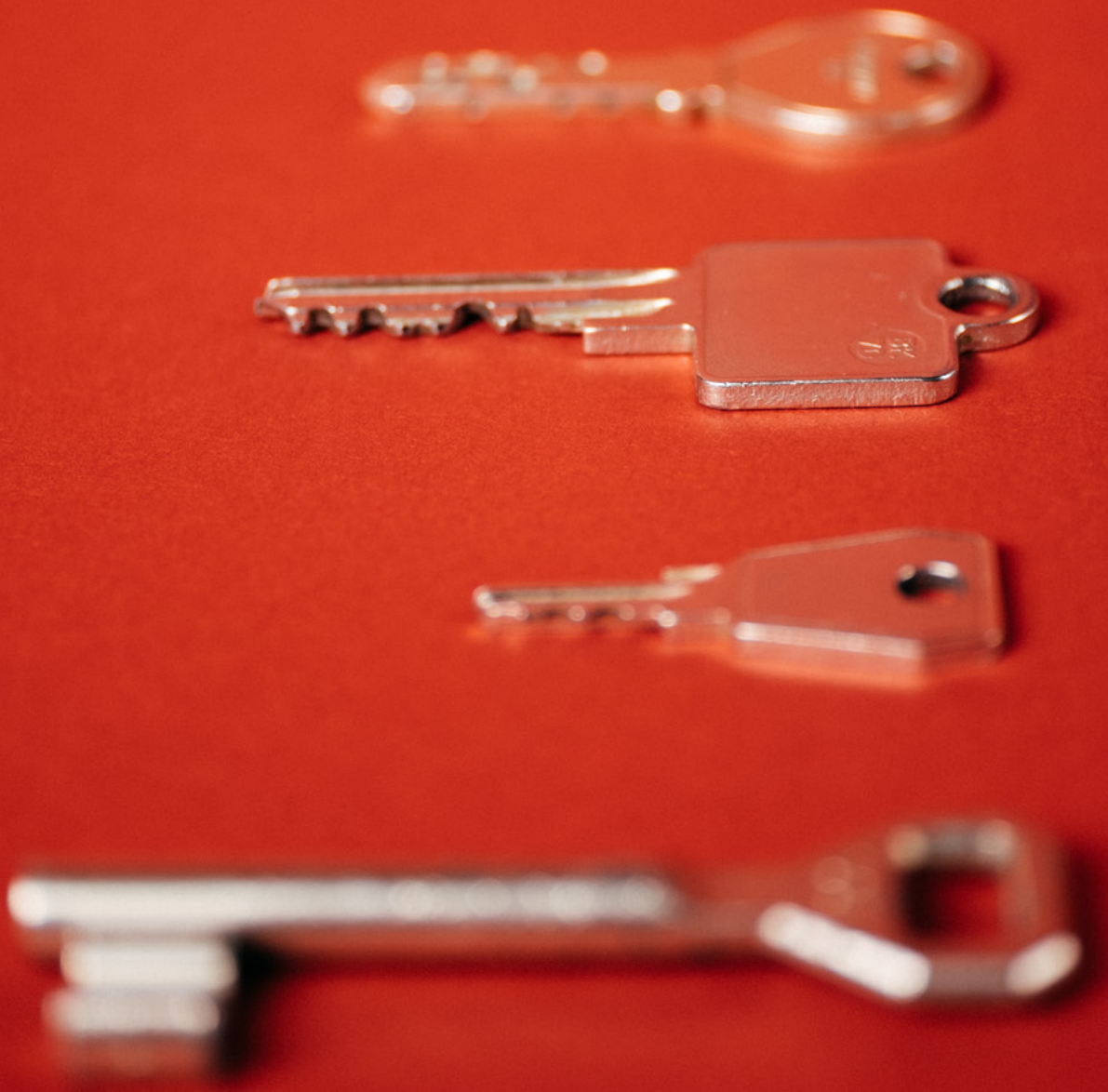
Auch bei einfachen IT-Infrastrukturen oder wenn es Ihnen wichtig ist, die **komplette Kontrolle über den gesamten Backup-Prozess** zu behalten, kann diese Lösung Vorteile für Sie bieten.

Wenn Ihr Unternehmen über eine **komplexe IT-Infrastruktur mit umfangreichen Datenmanagementanforderungen** verfügt, die zum Beispiel mehrere Standorte, verschiedene Betriebssysteme oder spezielle Anwendungen umfassen, kann ein Backup-Service die bessere Option sein – insbesondere dann, wenn Sie für die Erstellung nicht die eigenen Ressourcen beanspruchen möchten.

Auch wenn Ihr Unternehmen nicht über die erforderlichen IT-Ressourcen oder das Fachwissen verfügt, um den Backup-Prozess intern zu verwalten, ist ein Backup-Service die richtige Lösung. Sie können **von den Fachkenntnissen und Erfahrungen des Dienstleisters profitieren**, um den **Backup-Prozess effizient zu verwalten** und sicherzustellen, dass Ihre Daten **sicher und zuverlässig in Ihrem Backup-Storage gespeichert** werden.

Checkliste:

Diese 8 Sicherheitskriterien sollte Ihr Backup erfüllen



Die Sicherheit und Zuverlässigkeit Ihres Backups entscheidet letztendlich über dessen Nutzen im Ernstfall. Damit Ihr **Backup-Prozess von Anfang an sicher** ist, haben wir für Sie an dieser Stelle eine **hilfreiche Checkliste** zusammengestellt, die Sie im Prozess der Backup-Planung unterstützen wird.

Verantwortlichkeiten festlegen

» Sie sollten einen **zuverlässigen und vertrauenswürdigen Verantwortlichen für das Thema Datensicherung** festlegen. In der Regel handelt es sich um den IT-Administrator, welcher weitere Verantwortliche mit den Prozessen vertraut macht und alles überwacht. Sollte dies intern nicht möglich sein, können und sollten Sie sich durch Dienstleister unterstützen lassen.

Notizen:

Zu sichernde Daten und Sicherheitsstandards

» Zu sichernde Daten und Systeme müssen **vor der Sicherung** durch Ihr Unternehmen **definiert und klassifiziert werden**. Für geschäftskritische und personenbezogene Daten sind grundsätzlich höhere Sicherheitsstandards einzuhalten. Über die einzuhaltenden Standards müssen Sie sich unbedingt im Vorfeld informieren.

Notizen:

Backup-Standorte

» Backup-Daten sollten redundant gespeichert werden – idealerweise an mehreren geografisch verteilten Standorten, um Ausfälle aufgrund von Katastrophen oder Hardwareproblemen zu vermeiden. **Beachten Sie die 3-2-1-Backup-Methode**! Sollten Sie einen Hosting-Dienstleister wählen, so ist unbedingt darauf zu achten, dass Ihnen dieser auch die Möglichkeit bietet, Ihr **Backup an unterschiedlichen Standorten** – bestenfalls innerhalb der EU – zu speichern.

Notizen:

Backup-Typen

» Die Implementierung verschiedener Backup-Typen wie Voll-, Differential- und inkrementelle Backups kann die Effizienz Ihrer Datensicherung erhöhen sowie die Wiederherstellungszeit verbessern. **Legen Sie eine solche effiziente Backup-Strategie fest!** Hierbei ist es wichtig, die spezifischen Anforderungen Ihres Unternehmens jederzeit zu beachten.

Notizen:

Backup-Plan

» Ein **gut durchdachter Backup-Plan**, der die Häufigkeit der Backups, die Aufbewahrungsfristen und die Wiederherstellungsziele definiert, ist essentiell. Auch hier sind die individuellen Anforderungen Ihres Unternehmens zu berücksichtigen.

Notizen:

Automatisierung Ihrer Backups

» Die Backup-Prozesse sollten regelmäßig sowie weitgehend automatisiert ablaufen, um menschliche Fehler zu minimieren und **sicherzustellen**, **dass Backups wirklich erfolgreich** erstellt werden. Nutzen Sie hierfür die passende Software und lassen Sie sich im Zweifel durch einen Dienstleister unterstützen!

Notizen:

Überprüfung Ihrer Backup-Prozesse

» Die erfolgreiche Durchführung Ihrer Backups muss regelmäßig überprüft werden. Es bringt Ihnen nichts, wenn Sie auf Ihr Backup vertrauen – dieses aber nicht in den gewünschten Intervallen erstellt wird. **Führen Sie regelmäßige Wiederherstellungstests durch!**

Notizen:

Wiederherstellungsplan

» Es sollte ein klarer **Notfallwiederherstellungsplan** vorhanden sein, damit **im Ernstfall schnell gehandelt** werden kann. Dies ist entscheidend für die Aufrechterhaltung Ihrer Geschäftskontinuität.

Notizen:

Rechtliche Anforderungen einhalten

» Das Backup-System sollte den **geltenden rechtlichen Anforderungen** und branchenspezifischen Vorschriften entsprechen, wie z. B. der Datenschutz-Grundverordnung (DSGVO).

Notizen:

Physische Sicherheit

» Die physische Sicherheit der Backup-Speicherorte ist genauso wichtig wie die Sicherheit der Daten selbst. Dies umfasst den **Schutz vor Diebstahl**, **Brand**, **Wasser und anderen potenziellen Gefahren**. Backup-Speicherorte sollten daher sicher und vor unbefugtem Zugriff geschützt sein. Sollte sich Ihr Backup in einem externen Rechenzentrum befinden – was wir Ihnen immer empfehlen würden – sollten Sie unbedingt auf diesen **umfassenden Schutz** achten!

Notizen:

*Auch **wenn sich Ihre Geschäftsabläufe und Anforderungen einmal ändern**, ist es wichtig, dass Sie Ihre **Backup-Pläne und Prozesse aktualisieren.** Wie Sie gesehen haben, gibt es viele Aspekte, die von der ganz individuellen Situation Ihres Unternehmens abhängen. **Pauschale Lösungen und Ignoranz sind hier komplett fehl am Platz.***

Wenn Sie das falsche Backup haben, haben Sie im Zweifel gar kein Backup!

Anwendungsfälle & Best Practices

Zum Schluss möchten wir Ihnen noch ein paar typische Anwendungsfälle und dazu hilfreiche Backup-Szenarien an die Hand geben. Aber bedenken Sie bitte auch hier – Sie wissen es sicher schon: **Es kommt immer auf den individuellen Fall an.**

Die beschriebenen Szenarien dienen nur als Orientierung, aber niemals als ausgefeilte Backup-Strategie für Ihr Unternehmen!

Nextcloud: Kein richtiges Backup – aber doch ein Sicherheitsnetz für Ihre Dateien in kritischen Fällen

Nextcloud ist eine **Plattform mit vielerlei Funktionen**. Neben Kalender, Chat und anderen nützlichen Tools ist die wichtigste Funktion das Datei- und Ordnersystem, in dem Sie Ihre wichtigen Dateien ablegen und mit anderen Personen teilen können. Das Praktische: Die Daten und Funktionen können Sie über verschiedenste Endgeräte aufrufen und bearbeiten.

Dem liegt eine **Datensynchronisation auf allen Systemen** zugrunde, was man bereits als eine Form der Datensicherung betrachten könnte. Liegt beispielsweise der Defekt eines Endgeräts vor, mit dem die Nextcloud verbunden ist, so sind die Daten niemals verloren, sondern **können von einem anderen Endgerät aufgerufen und nach Reparatur auch wieder auf diesem Gerät genutzt werden**. Befindet sich die Nextcloud also auf einem sicheren Server, kann das Nutzen einer Nextcloud bereits an sich schon eine gute Datensicherung darstellen.

Zusätzlich sollten jedoch die unterschiedlichen Bereiche der Nextcloud in Form eines Backups gesichert werden. Der Backup-Prozess umfasst verschiedene Ebenen und Prozesse:

- **Dateisicherung:** Regelmäßige Backups der Dateien und Ordner in Nextcloud.
- **Datenbank-Backups:** Sicherung der Datenbank, welche die Konfigurations- und Metadaten von Nextcloud beinhaltet.
- **Konfigurations-Backup:** Sicherung der Konfigurationsdateien und -einstellungen von Nextcloud.

Möchte man Nextcloud effektiv sichern, sollte man sich wie in allen Fällen darüber Gedanken machen, **wie man selbst die Plattform im Unternehmen einsetzt**.

Um regelmäßig vollständige und differenzielle Backups der Nextcloud zu erstellen und diese auf separaten Servern zu speichern, können Skripte und Tools genutzt werden.

Auch hier ist das **regelmäßige Testen der Wiederherstellungsprozesse notwendig**, um sicherzustellen, dass im Ernstfall eine schnelle und vollständige Wiederherstellung möglich ist.

Backup von virtuellen Maschinen und Containern:

Um **virtuelle Server** bzw. sogenannte Container zu sichern, können Tools wie VMware, vShere oder Hyper-V genutzt werden. Das sind die Hypervisoren zum Erstellen der virtuellen Systeme. Diese verfügen in der Regel über eine Lösung zum Sichern der VMs. Hier kommt dann z.B. der Proxmox Backup Server zum Einsatz.

Somit können vollständige und inkrementelle Backups erstellt werden.

Container-Backups: Tools wie Docker Backup oder Kubernetes Backup-Lösungen können verwendet werden, um Container-Images und deren Daten zu sichern.

Auch hier stellen automatisierte Backup-Prozesse sicher, dass VMs und Container regelmäßig gesichert werden, ohne dass manuelle Eingriffe erforderlich sind.

Sicherung einer Website

Bei einer Website muss nicht unbedingt das komplette System ständig gesichert werden – im Gegensatz zur Datenbank und zu den E-Mails.

Zur Sicherung einer Website sind natürlich erst einmal **die Daten, aus denen die Darstellung der Seite besteht** – also HTML-Dateien oder PHP mit Text sowie Bilder – relevant. Handelt es sich um ein CMS wie beispielsweise Wordpress, ist es unumgänglich, die **Datenbank zu sichern,** da diese die eigentlichen Inhalte, bis auf die Medien, enthält.

Ein Beispiel zur Veranschaulichung ist die Firmenseite eines Malerbetriebs: Hier werden oft lediglich die Kontaktinformationen zu finden sein. Somit müssen die Seitendaten selten gesichert werden. Jedoch ist es hier wichtiger, die **E-Mails regelmäßig zu sichern,** damit diese nicht verloren gehen.

Sicherung auf Dateiebene
(reine Seiten-Elemente php/html/etc.)

Backup der Datenbank

Backup der E-Mails

Sicherung eines Online-Shops

Wenn Sie einen Online-Shop sichern möchten, welcher stark frequentiert ist, sollten Sie dies mehrfach am Tag tun. Hierbei muss zum Beispiel Ihre **Datenbank häufiger gesichert werden**. Die Bilder des Shops, welche sich in der Regel nicht so häufig ändern, müssen Sie seltener sichern. Denken Sie bei einem Shop auch immer an die **E-Mails, welche Sie mit Ihren (potentiellen) Kunden ausgetauscht haben**.

Ein weiteres sinnvolles Szenario wäre es, nur die Datenbanken in einem kurzem Intervall zu sichern, wenn hier häufige Änderungen erfolgen. Dies könnte Informationen zum Lager und zu Bestellungen betreffen.

> ***Bei sehr vielen Bestellungen*** *in einem kurzen Zeitraum kann es auch sinnvoll sein, eine so genannte* ***Live Replikation der Datenbank*** *einzurichten. Denn in diesem Fall könnte schon ein stündliches Backup im Fall eines Datenverlusts nicht ausreichen und erhebliche Probleme mit sich ziehen.*
>
> *Dies wäre jedoch kein Backup im eigentlichen Sinne.*

Sicherung einer Server- oder Cloud-Infrastruktur

Betreiben Sie eine Umgebung für virtuelle Maschinen, ist in der Regel nicht jede Instanz gleich wichtig und es ändern sich Daten unterschiedlich schnell.

Je nach Größe kann in kurzen Abständen regelmäßig eine Sicherung erfolgen. Im Fall einer Proxmox-Umgebung können kleine Instanzen direkt und einfach via Proxmox gesichert werden.

Hier bietet sich der Einsatz eines zusätzlichen Proxmox-Backup-Servers an. Dieser muss sich nicht direkt am selben Standort befinden. Man sollte in diesem Fall nach dem ersten initialen Backup die Variante das Backup ändern (beschleunigen) und nur die letzten Änderungen sichern.

Lohnt sich die Investition in Backup-Infrastrukturen für Sie?

Wir hoffen, dass es uns mit diesem E-Book gelungen ist, Ihnen zu verdeutlichen, wie wichtig ein individuelles Backup-Konzept für Ihr Unternehmen ist.

Doch vermutlich taucht in Ihrem Kopf die alles entscheidende Frage auf: **Lohnt sich der ganze Aufwand überhaupt?**

Die Implementierung von Backup-Lösungen verursacht natürlich initiale Kosten, die durch Hardware, Software und Dienstleistungen entstehen. **Eine sorgfältige Planung und Budgetierung im Vorfeld ist daher unerlässlich, um sicherzustellen, dass die gewählten Lösungen sowohl kosteneffizient als auch effektiv sind.**

Investitionen in skalierbare Backup-Lösungen ermöglichen es, das System an das Unternehmenswachstum anzupassen. Außerdem sollten laufende Kosten für Support und Wartung in die Budgetplanung einbezogen werden.

Langfristige Einsparungen durch ein effektives Backup-System

Durch die Prävention von Datenverlusten können langfristig **erhebliche Kosten eingespart werden**, welche durch Ausfallzeiten und Datenwiederherstellung entstehen würden.

- **Vermeidung von Betriebsunterbrechungen:** Regelmäßige Backups sorgen dafür, dass im Falle eines Datenverlusts eine schnelle Wiederherstellung möglich ist, wodurch Betriebsunterbrechungen minimiert werden.
- **Reputation und Kundenvertrauen:** Die Vermeidung von Datenverlusten trägt zur Erhaltung der Unternehmensreputation und des Kundenvertrauens bei.
- **Rechtskonformität:** Die Einhaltung gesetzlicher Vorgaben bezüglich der Datensicherung schützt das Unternehmen vor rechtlichen Konsequenzen und möglichen Bußgeldern.

Wir stellen also an dieser Stelle noch einmal die Gegenfrage(n):

- Was sind Ihnen Ihre Daten wert?
- Was ist Ihnen die Geschäftskontinuität wert?
- Und: Was ist Ihnen das Vertrauen Ihrer Kunden wert?

Und jetzt fragen wir Sie:

Lohnt es sich, in effiziente und effektive Backup-Prozesse zu investieren?

Sie möchten sich von uns zu passenden Backup-Lösungen beraten lassen?

Kontaktieren Sie uns noch heute für eine kostenlose Beratung und erfahren Sie, wie wir Ihnen helfen können, Ihre Daten zu schützen und Ihre Geschäftskontinuität zu wahren.

Montag bis Freitag
8.00 bis 17.00 Uhr

Tel.: 0361/6 58 53-55
sales@keyweb.de

Keyweb AG
Neuwerkstraße 45/46
99084 Erfurt

Individuelle Backup-Lösungen von Keyweb

Sie suchen eine optimal auf Ihre Bedürfnisse ausgerichtete Backup-Lösung? Wir helfen Ihnen, auch beim Thema Datensicherheit entspannt zu bleiben!

- professionelle und individuelle Backup-Beratung
- DSGVO-konformes Hosting für besonderen Datenschutz
- umfassende Datensicherheits-Maßnahmen
- serverseitiger DDoS-Schutz
- TÜV-zertifiziertes redundantes Rechenzentrum in Deutschland
- standortgetrenntes Backup dank verteilter Rechenzentren möglich

Unsere Backup-Lösungen für Unternehmen

Backup-Storage KeyDisc Pro

» Online-Backup-Speicher

» mit nutzerfreundlicher Oberfläche

» ideal für Daten- & Konfigurationsbackups

» Software KeyHelp Pro kostenfrei

Sichern Sie Ihre Daten auf der KeyDisc Pro.

Backup-Speicher wählen

KeyDisc Pro mit Managed Service

» Backup Storage KeyDisc Pro

» inkl. Einrichtung Ihres regelmäßigen Backups – optimiert auf Ihre Anforderungen

» regelmäßige Funktions-überprüfung Ihres Backups

» Restore einmal monatlich inklusive

Als Backup-Lösung für Keyweb-Server buchbar.

KeyDisc Managed entdecken

Proxmox Backup Server

» die ideale Datensicherung für Ihre Cloud-Umgebung

» ideal, wenn Sie eine Proxmox-Umgebung nutzen

» Sie sparen Lizenzkosten für Backup-Software

Kann direkt bei Bestellung der Cloud gebucht werden oder später per Ticket.

per Ticket anfragen

Mit dem Managed Backup halten wir Ihnen komplett den Rücken frei. Wir sorgen dafür, dass Ihr Backup optimal eingerichtet wird und funktionsfähig ist. – Sie kümmern sich einfach weiter um Ihr Geschäft.

1. Gemeinsam mit Ihnen wählen wir die **passende Backup-Software** aus und richten diese für Sie ein.
2. Nach Abstimmung mit Ihnen richten wir Ihre **individuell sinnvollen und gewünschten Backup-Intervalle** sowie die **Vorhaltezeiten für Ihre Daten** ein.
3. Wir setzen Ihre gewählte Backup-Strategie um.
4. Einmal monatlich kann eine **kostenfreie Wiederherstellung Ihrer Daten** erfolgen.
5. Wir **überprüfen**, **ob Ihr Backup wie geplant erstellt worden ist**. Sollte dies nicht der Fall sein, stoßen wir dieses erneut an oder teilen Ihnen das mit.

Wann ist der Managed Backup Service für Sie geeignet?

- ✔ wenn es für Sie zu aufwendig ist, regelmäßig den Erfolg Ihres Backups zu überprüfen
- ✔ wenn Ihr Backup sehr häufig und in kurzen Intervallen laufen muss, da schon nach kurzer Zeit viele Daten auf Ihren Systemen verändert wurden
- ✔ wenn Sie sich zeitweise nicht um Ihr Backup kümmern können, beispielsweise in Urlaubszeiten oder bei Personalengpässen

Mehr Informationen zu unseren Backup-Lösungen finden Sie unter:

keyweb.de/backup

Interessiert an maßgeschneiderten Backup-Lösungen für Ihr Unternehmen?

Kontaktieren Sie uns noch heute für eine kostenlose Beratung und erfahren Sie, wie wir Ihnen helfen können, Ihre Daten zu schützen und Ihre Geschäftskontinuität zu wahren.