The Risk of Data Loss Is a Concern For Every Business!

How to Create a Safety Net for Your Data.

KEYWEB

Server. Cloud. Domains.

Foreword

Many factors determine whether a company is successful or disappears after a few months or years.

One of the most important is whether the company's decisions and processes are optimally aligned with the market. Two other factors are speed and efficiency – in responses, processes and development.

Modern technology is often the answer. They offer significant time and cost savings. Networking via the Internet also enables companies to achieve levels of efficiency that were the stuff of science fiction a few decades ago. But there is a huge downside. If you don't realise this, you are putting your entire business at risk.

Keyweb
Editorial Team

Contents

The Risk of Digitalisation, Cloud, AI & Co. 4

The Devastating Consequences of Data Loss 5

Causes of Data Loss 6

The Almost Indestructible Safety Net 7

Why a Backup Needs to Be Highly Customised 8

Getting Started With a Secure Backup 9

5 Questions to Ask for Your Individual Backup Strategy 10

Types of Backups and Their Characteristics 12

Combine These Backup Types
to Create a Highly Efficient Backup Concept 14

These Backup Principles Make Your Backup –
As Secure As a High-Security Safe 16

Backup Solutions & Tools for the Realisation of Your Backup 18

Backup Services: So Your Backup Doesn't Get Out Of Hand 20

Checklist: The 8 Security Criteria Your Backup Should Meet 22

Use Cases & Best Practices 24

Is it Worth Investing in Backup Infrastructure? 26

Customised Backup Solutions from Keyweb 28

Imprint

Keyweb AG

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

info@keyweb.de
keyweb.de

The Risk of Digitalisation, Cloud, AI & Co.

Wherever processes are fast and automated, and where a lot of data – possibly very sensitive data – is transmitted and stored electronically, there is an invisible threat to that very data.

Theft and manipulation. Security breaches – whether due to human error, lack of updates or insidious cyber criminals, or force majeure such as environmental disasters. Unfortunately, these risks can never be completely eliminated today and will be even more so in a few years' time.

This means that **modern technologies** and internal, cloud based and external data storage **pose a major threat to businesses**.

If you are aware of these dangers, you can take appropriate protective measures. But if you are unaware, or not fully aware, the **consequences can be devastating**. For you, for your business and for your customers.

The Devastating Consequences of Data Loss

In the past, even large, well-known companies have been forced to shut down due to cyber-attacks, fire or environmental disasters. Such incidents can cause lasting **damage to a company's image**.

Data is often the foundation of all business processes. It is the backbone of a business. Unfortunately, many managers are only made painfully aware of this when their valuable database disappears overnight without warning, or is altered or encrypted by criminals.

Data loss or IT unavailability can not only result in **significant financial losses** due to lost revenue, business interruption and recovery costs – it can also permanently damage the trust of customers, business partners and employees.

The consequences: Cancellations and potentially legal consequences. In extreme cases, where data is irretrievably lost, the **company may have to shut down temporarily or completely**.

Would your business survive such a data loss?

> *Companies of all sizes whose business processes are based on digital data must **protect themselves against these risks** if they are to survive in the long term.*

Causes of Data Loss

cyber attacks

hardware failures

software errors

human error

natural disasters

power failure

burglary or theft

faulty migration

The Almost Indestructible Safety Net

There are many helpful security measures you can take to effectively protect your IT and the data it stores. But there is only one that provides an almost indestructible safety net.

A backup is an extremely important part of a comprehensive data security plan for businesses.

In fact, it is the single most important security measure you can take to prevent significant or complete data loss in the long term.

It provides the safety net that can recover your lost or corrupted business data even after the most catastrophic data loss – so your business can continue to operate virtually uninterrupted.

What really matters is that this data is quickly and completely available again in the event of a data loss. Therefore, backups should be performed, reviewed and updated on a regular basis.

Why a Backup Needs to Be Highly Customised

To be truly protected by a backup in an emergency, it is not enough to back up the data somehow, somewhere and at some point. You need a clear backup strategy that is planned down to the last detail.

No two companies are the same. Your business is unique – and so is the way you need to back up your data on a regular basis.

*To ensure that your backup meets the necessary security requirements, it should be **highly tailored to your business, its processes and circumstances**.*

It is **particularly important for companies** to combine different **backup methods and technologies to create a highly efficient and effective backup method**.

With a **comprehensive and tailored backup plan**, you can minimise risks and ensure that data can be recovered quickly in the event of an emergency.

With a customised backup, you can:

- recover lost or damaged data quickly and completely after a cyberattack or other IT emergency.
- ensure business continuity even in the event of such an incident by quickly restoring data access and business operations.
- comply with legal requirements for data processing and backup.
- back up data before upgrades or migrations so that it can be recovered in the event of a failure.
- protect yourself from ransomware and the associated ransom demands.

We want to show you what you need to consider to avoid data loss disasters in the first place.

You will learn which methods have proven themselves and how you can develop and optimise your own backup strategies to ensure maximum data security.

You will receive a comprehensive guide to help you identify and implement the best backup solutions for your business.

> *When your IT meets high security standards, it also has a direct or indirect positive impact on the trust and satisfaction of your customers and employees.*

Getting Started With a Secure Backup

If you want to create a **truly secure backup strategy** for yourself, there are some basic considerations you need to make. The following pages will help you do this.

In addition to the number and frequency of backups, it is important to consider **what data should be backed up**.

This is very individual for each company, as there can be very different requirements depending on the activity and degree of digitisation.

For some businesses, backing up all of their data once or twice a week is sufficient, while others need to back up parts of their data several times a day – if not hourly or even more frequently.

For example, it makes a big difference whether changes are made to your website twice a month or several times a week.

How often you should back up your data depends on your needs!

It is also important to decide which data needs to be backed up more often and which less often.

5 Questions to Ask for Your Individual Backup Strategy

For your individual backup strategy, please consider the following questions. They will help you to assess where to prioritise your backups.

1. What data needs to be backed up so that you can get back up and running quickly after a data loss?

The answer depends on what data you use and change regularly. Don't think too superficially here!

For example, if you run a busy online shop and regularly receive orders, it is not enough to simply back up the ordering system itself. The database containing all customer information and current orders must be available just as quickly if business is to continue promptly after a data loss.

Notes:

2. What types of data do you need to consider for your data backup?

Of course, there is no general answer to this question – but we would like to give you a rough and general overview that you can use as a guide:

- **Domain data:** all data belonging to a specific domain
- **Emails** that are stored on a separate email server, for example
- **File server:** server on which a wide range of corporate data can be stored
- **Applications:** software used in your organisation and all associated data
- **Databases:** data stored in the form of databases for a variety of purposes
- **Networks:** all networks via which data is transmitted within your company
- **Operating system information** and **configurations**

All of these systems can be affected by data loss. **Web and database servers**, for example, are often the **target of cyber attacks**. Regular system backups ensure that websites and databases can be quickly restored in the event of an attack.

Communication data can also be essential for companies. To prevent this from being lost, email servers, chat platforms and other communication tools and their content need to be backed up.

Notes:

3. At what intervals should which data be backed up?

The answer to this question depends largely on your **regular business processes**. More specifically, the **regularity and frequency** of which processes take place. Not all websites are the same, not all shops are the same, not all businesses are the same.

For an online shop, for example, it is important to back up the relevant databases at the necessary and appropriate intervals. It makes a difference whether your data is changed every hour, once a day or once a week. For the shop mentioned above, it is also important to back up the relevant databases at the necessary and appropriate intervals.

Let's say your shop receives several orders every hour. If your data is lost today, there is no point in restoring yesterday's order status. Depending on the value of your product prices, you could lose several thousand euros – and previously satisfied customers with it.

Notes:

4. How much storage space is required for the data to be backed up?

Based on this question, you can later determine which backup method is particularly efficient for you.

Especially if the intervals between backups are very short, you should make sure that the backup itself does not take up too much time and storage space. You can use a combination of backup methods to get the best value for your money. Read more about this on the following pages.

Notes:

5. Are there specific times when your business data needs to be backed up again?

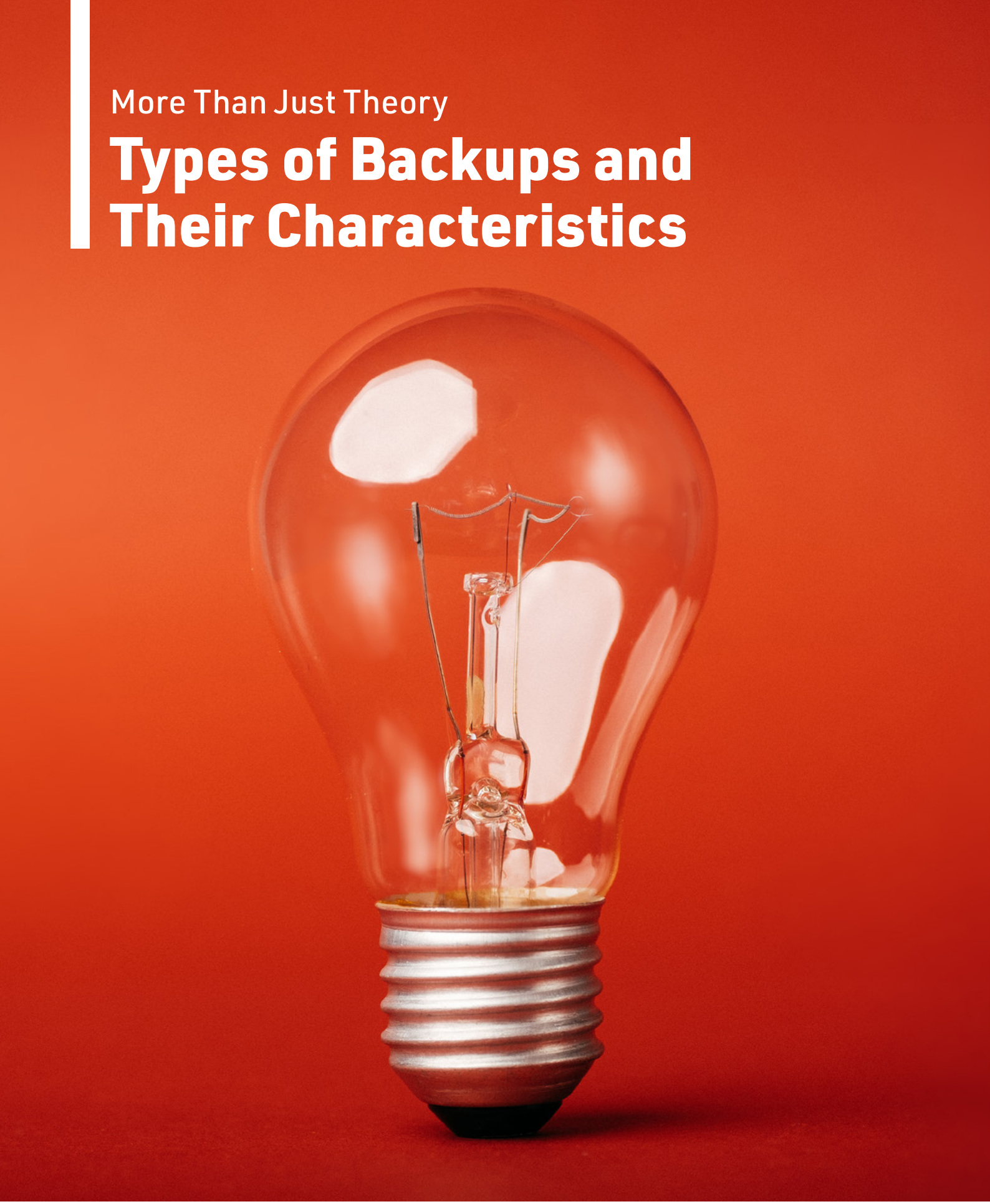
Again, this is very individual. For example, it may be useful to make a backup just before you perform certain updates.

Please make a note of this point as well.

Notes:

More Than Just Theory

Types of Backups and Their Characteristics



You cannot create a good backup strategy if you do not understand the different types of backups. Once you know the basics of how to use them to back up your data, you can optimise your backup to meet your company's security requirements.

Local Backups – Right At Your Site

Local backups are typically stored on physical devices within your company, such as internal servers and hard drives. This has both advantages and disadvantages:

The fact that the data is on your premises can provide a **greater sense of security**.

> *A word of caution:*
> *depending on local conditions, the subjective feeling of safety may not necessarily correspond to reality, as many factors contribute to safety.*

Local backups on your own servers offer **fast recovery times**.

The data is stored at the same location as the primary data and **can therefore also be affected in the event of an IT emergency**, in particular in the event of theft or environmental influences.

The challenge can be that the equipment requires **regular maintenance** and is also **highly susceptible to physical damage** such as fire, hardware failure or theft.

You must take the appropriate security measures within your organisation. **This means that you have a great deal of responsibility** for the operation and security of the equipment and the functionality of the backup.

Data **recovery** is usually **in your hands**.

Cloud Backups – Data Backup to an Off-site Location

Cloud backups are stored on external servers – usually by a cloud provider. There are service providers that operate their own data center and others that use the data centers of other providers.

The cloud or hosting provider is responsible for the functionality of the hardware and therefore the availability of your data.

As a business and cloud user, you are responsible for the functionality of the backup. You are responsible for ensuring that it is set up and working properly. If you do not want to be responsible for a cloud backup yourself, you can also use so-called Managed Services from the providers, which can be a great relief if you are (still) unsure about backups.

Backups in the cloud offer **high levels of flexibility, scalability and reliability** – as long as the provider properly implements appropriate security measures.

The **data is available from anywhere**, making these backup variants particularly suitable for businesses with geographically spread locations.

They also have the advantage that the data is **stored separately from the original data** – an additional and important aspect of security.

If the data is insufficiently encrypted, the separation of sites and the geographical distribution of the data can prove to be a disadvantage. **Backup security should be the most important requirement**.

Hybrid Backups – The Backup Combination

Hybrid backups combine local and cloud backups – and the characteristics of each.

This strategy provides **additional security and flexibility** by meeting a number of backup security criteria.

The combination of local storage and cloud backup makes it easier to comply with the 3-2-1 backup rule. The **cloud provides additional redundancy**.

Businesses with large storage needs or multiple locations can benefit from cloud storage to complement local backups.

However, hybrid backup is **more complex than other backup types**. As a result, it is more complex to implement and manage.

This also means **higher costs for the necessary infrastructure** and its installation and maintenance.

Combine These Backup Types

To Create a Highly Efficient Backup Concept

An important goal for businesses should be to design processes that minimise the use of resources while optimising output. Your backup must not only be secure, it must also be created in a way that allows it to be **stored as efficiently as possible and restored quickly when needed**.

To achieve this, you need to use a combination of different backup strategies: **full, differential and incremental**! Depending on the type of backup, a backup will use more or less storage space and will be slower or faster when backing up or restoring data. We explain backup types in detail here.

Full Backup for Fast & Easy Recovery

A **full backup** combines every single file on a system into a single backup file. Because the **entire file system** is backed up, this type of backup takes a **long time to create**.

However, using this backup method alone would, in the long run, place a very heavy load on your chosen storage medium. Full backups are therefore often used in combination with differential or incremental backups, which are explained in the next sections. They form the basis for further backups.

Backup Duration: backup takes relatively long

Recovery Duration: fastest and easiest backup type to restore

Storage Space Consumption: storing duplicates takes up a lot of storage space

Particularly Efficient: The Synthetic Full Backup

A special type of full backup is a synthetic full backup. This creates a complete backup without having to back up all the data each time. It combines a previous **full backup** with several incremental backups to **create a current full backup**.

This means that **only the data that has changed** since the last full backup is added, **without having to copy everything again**.

Compared to a normal full backup, which backs up the entire amount of data each time, a synthetic backup **saves both time and storage space**. The normal full backup, on the other hand, backs up all the data from scratch each time, resulting in longer backup times and higher storage usage.

Differential Backup – the Complement To the Full Backup

A differential backup is based on a full backup. This type of backup is used whenever the **difference from the last full backup** is being backed up. This means that **any data that has changed or been added since the last full backup** is collected in one backup file

> *Suppose you make a full backup every Sunday and a differential backup from Monday to Saturday.*
>
> *To recover your current data set, you need to **restore two backup files**:*
>
> *1. the full backup from Sunday, and*
>
> *2. the differential backup from Wednesday, i.e. a summary of all the changes that occurred on Monday, Tuesday and Wednesday.*

Backup Duration: faster than the full backup, slower than the incremental backup

Recovery Duration: faster than the incremental backup, slower than the full backup

Storage Space Consumption: requires less storage space than a full backup

Incremental Backup

An **incremental backup** requires a full backup and **only backs up data that has changed since the last backup**.

Unlike a differential backup, the changes from the previous day are not transferred to the current day. Because an incremental backup only backs up data that has changed during the day, this type of backup **uses the least amount of storage space**.

> *Let's say you want to make a full backup every Sunday and an incremental back-up from Monday to Saturday.*
>
> *To fully recover your data, you need to **restore the entire backup chain**. This includes the full backup from Sunday and each incremental backup from Monday, Tuesday, Wednesday, Thursday and Friday. The restore process is therefore much more complex than for the other types of backups.*

Backup Duration: of all variants, the backup process takes the least time

Recovery Duration: most complex backup type in the recovery process

Storage Space Consumption: least amount of disk space used per backup

The System Backup

In addition to the three types of file backups, there is also a system backup. This is not just a specific file system or database, but an entire system. **This creates a system image of the installed operating system, including all system files, installed programs and configurations.** The result is a **snapshot of all the drives relevant to the operating system**.

In the event of a serious software problem, a **fully functional system can be restored**, rather than having to restore each file individually. **This saves a lot of time compared to a fresh installation**. The downside is the relatively large amount of storage space that may be required, depending on the frequency and size of the snapshot.

The exact combination of backup types will depend on your business requirements. Again, it depends on when, how often and what data is changed.

These Backup Principles Make

Your Backup – As Secure As a High-Security Safe

In order for your backup to be secure enough to protect you from current threats and typical failures and errors, it needs to meet very specific criteria.

Some of these criteria are easier to meet if you follow backup rules and methods. By following these principles, you can be confident about your backups. Although the most important rules are no secret, they are often ignored. We would like to share them with you here - so you can do better.

The principle is to always have different versions of the data available for backup.

Determine the Optimal Number of Backups – With the 3-2-1 Backup Rule

This rule covers the three most important basic principles for your backup, and if you follow all three, you will be able to protect your data very reliably.

3

You should make at least **three copies**, or backups. This may sound like a lot, but once you understand the other principles, the reason becomes clear.

2

The backups should be stored on at least **two different media**, e.g. locally on a backup server, on network attached storage (NAS) or cloud storage.

1

At least **one copy** of your data should be stored in a separate location, e.g. online in the cloud of **certified German data center**.

Useful Backup Routines: With the Multi-Generation Backup Method

By **backing up your data regularly**, you minimise the risk of data loss. This is because an up-to-date copy of your data is only available in the event of an emergency if your regularly changing business data is frequently backed up. Unfortunately, this is still far too rarely considered. Do it better!

A popular backup method that will optimise your data backup is the grandfather-father-son backup. The aim of this method is to **perform a complete backup as efficiently as possible**.

The principle is to always have different versions of the data available for backup.

For example, each week there are 4 daily backups (son backups), which are overwritten one at a time with each new week.

In addition, there are 4 weekly backups (father backups) which are kept until the end of the month and then overwritten week by week in the following month.

There are also usually up to 12 monthly backups, which are also overwritten with new monthly backups after a maximum of 12 months (grandfather backups).

No More Backup Procrastination: With Backup Automation

If you had to constantly think about when to run another backup – or if something else was more important – this would be an unnecessary risk factor for your data – and an additional stress factor for you! **Make it easier for yourself!**

The solution is **automated backups**. These **minimise the likelihood of human error** and ensure that your data backups are **carried out reliably and consistently**.

- **Time Efficiency:** Automated backups save time and reduce the workload for IT teams.
- **Consistency:** Regular and consistent backups minimise the risk of data loss.
- **Reducing Human Error**: Automated processes reduce the risk of human error that can occur with manual backups.
- **Notifications and Reports:** Automated systems often provide notifications and reports that inform IT teams about the status of backups and allow them to recognise potential problems at an early stage.

In this context, it is important to clarify **which processes can be automated** and which, for various reasons, are better handled manually.

There are several technologies available for automating your backups, which we will discuss in more detail later.

Encryption Of Your Data: Your Backup Needs To Be Protected Too

Just like your original data, your backup probably contains a lot of sensitive information that should not be tampered with or spied on.

Encryption techniques protect your backups from unauthorised access and cyberattacks, for example during data transfer. Of course, it is important to maintain a **high standard of encryption** to prevent unauthorised access to your data. This should be accompanied by **internal access security**. Not everyone in the company should have access to sensitive data – including access to backups!

Protect your backups from unauthorised access with encryption!

One of the most commonly used methods is **AES (Advanced Encryption Standard) encryption**, especially the **256-bit version**, which offers high levels of security and efficiency. It is an internationally recognised standard.

Public key encryption is often used to securely transmit and store data, using methods such as **RSA** to enable secure communication between different parties.

In addition, **end-to-end encryption** ensures that data is fully protected both in transmission and at rest. **Hashing algorithms**, such as **SHA-256**, are also used to ensure the integrity of the secured data, which can detect and prevent data manipulation.

Only a Working Backup Is a Good Backup!

You back up regularly and feel safe, but then it happens: a complete loss of data. But you have your backup, which – shock – doesn't work.

Such a situation must be avoided at all costs. One way to do this is to run a **regular backup restore test**. These tests verify that the backed up data can be restored completely and accurately in the event of a disaster. It evaluates not only the integrity of the backups, but also the efficiency of the recovery processes.

You should regularly incorporate testing into your IT security strategy to ensure that all data is quickly and fully available in the event of a power outage, cyber attack or other incident. This will allow you to identify and remediate vulnerabilities early on, which will greatly enhance business continuity and data security.

Regular checks of the restore processes are at least as important as the backup itself.

Backup Solutions & Tools for the Realisation of Your Backup

Implementing all of these backup strategies and methods in a disciplined manner can be quite challenging – especially if you want to do it manually and on your own.

This is where **backup software solutions** come into play, helping businesses to make **regular and, more importantly, secure copies of their data**. This means they can be quickly and completely restored in the event of an emergency.

With the right solutions, backups can be performed automatically and regularly at the desired and defined intervals. These tools also take care of the necessary data encryption during data transfer and storage.

Types of Backup Solutions

There are different **types of backup software**, each designed to meet different needs:

1. **On-Premise Backup Solutions:** These solutions are installed on your own servers and provide a high level of control over the backup process. They are particularly suitable for companies that have strict compliance requirements and do not want to store their data off-site.
2. **Cloud-Based Backup Solutions:** These solutions store backups in the cloud, which is particularly attractive for companies with distributed locations or a decentralised workforce.
3. **Hybrid Backup Solutions:** A combination of on-premises and cloud-based solutions that offer the best of both worlds. This allows companies to develop a flexible back-up strategy that utilises both local storage and the security and scalability of the cloud.

There are a variety of backup software solutions available, each offering different features and security options.

When choosing the right backup software, it is important to make sure that the solution allows you to easily manage and restore data, especially if you have large amounts of data and complex IT infrastructures.

To help you make a good decision when choosing backup software, you should consider the following criteria.

Criteria for Good Backup Solutions

1. **Automation and Scheduling:** The software should be able to perform automatic backups on a set schedule to minimise human error.
2. **Encryption:** Both data transfer and backup storage should be protected with strong encryption algorithms.
3. **Scalability:** The solution must be able to keep pace with the growth of the business and the amount of data that needs to be backed up.
4. **Restore Options:** A good backup software offers flexible and fast restore options for both complete systems and individual files.
5. **Storage Options:** It should be possible to store backups in multiple locations, including local storage, off-site data centers and cloud services.
6. **User Friendliness:** An intuitive user interface and easy administration are essential to minimise the workload for the IT team.
7. **Compliance and Security:** The software should support compliance with relevant legal and regulatory requirements, including GDPR.
8. **Support and Updates:** Regular software updates and reliable support are essential to ensure the long-term security and functionality of the solution.

By carefully selecting backup software that meets these criteria, businesses can effectively back up their data and protect themselves from the devastating consequences of data loss.

We would like to emphasise that you should not hand over the responsibility for your secure backup to any tool. You must constantly monitor the purpose and success of your backups.

Proxmox Backup Server For Special Requirements

The Proxmox Backup Server (PBS) is a **powerful and efficient solution** for backing up and restoring your business data.

It enables you to back up and **restore virtual machines and containers based on Proxmox VE quickly and effectively**.

Geo-redundant backups are also possible with PBS. The user-friendly interface makes backing up your IT structure **efficient and straightforward**.

Efficient Backup

The backup technology used **backs up only the changed blocks of data**, saving a lot of storage space and reducing your backup times. Incremental backups ensure that **only changes since the last backup** are backed up. This reduces network load and speeds up the backup process.

Strong Encryption

Your data is secure at all times thanks to the **integrated encryption function**. So you can be confident that only authorised persons have access to your valuable, secure data.

- Using the Proxmox Backup Server client, you can **easily schedule regular backups** according to your needs and **automate the entire process** to minimise human error. You can create customised **schedules for your data backups**. You can also set up verification of your data to ensure its integrity.
- Thanks to integrated **monitoring and reporting functions**, you can maintain an overview of your backup processes, including detailed insights and notifications in the event of anomalies.
- In the event of a system failure, the **Proxmox Backup Server** provides **comprehensive recovery capabilities**. You can **restore your data to a specific point in time**. **Downtime is minimised and business continuity is maintained.**

*Backup software is used to **automate the necessary data backup steps**.*

It offers a wide range of functions that go far beyond simply copying files.

*The different types of backup, such as differential or incremental, can be scheduled to ensure that only changed or new data is backed up, making **data protection highly efficient**.*

*Backup tools provide the necessary encryption options to **protect data** from unauthorised access **during transmission and storage**.*

Backup Services:

So Your Backup Doesn‘t Get Out Of Hand

As you will have realised by now, ‚backup' is so much more than a small server in a server room to which all your company's data is transferred once a week.

Above all, good backup requires **good planning and a conscious and individual choice of suitable strategies**. In addition, the backup processes must be **carried out and checked regularly and correctly**.

When you want to focus on your core business, it can be overwhelming - after all, all you want is a backup. **If you do not have the resources or knowledge to run an efficient backup in your business, backup services can be the solution.**

In addition to the storage location, a backup service also includes the backup, management and restoration of your data by the service provider. This gives you a number of benefits:

» **Schedule and Automate Backups:**
Backup copies of your data are created without the need for manual intervention. This minimises the risk of human error and ensures that your data is backed up regularly.

» **Monitoring and Notifications:**
Your backups are constantly monitored and you are notified if any errors or problems occur. This allows you to identify and fix potential problems before they cause data loss.

» **Restore Options:**
The backup service usually offers options for restoring your data if necessary.

*A Managed Service Provider (MSP) can support you in the provision, management and monitoring of backup and recovery solutions. Instead of you as a company setting up and operating your own backup systems, the MSP takes over this task as a **managed service**.*

The **decision between backup storage and backup service** depends on several criteria, including the size and complexity of your company, your data management requirements, budget and internal resources.

If you have **internal IT resources** and the **expertise** to **manage the backup process yourself**, you can **choose a backup storage**. You **may need to invest additional time and resources** to plan, perform and monitor backups - but it can be a more cost-effective solution.

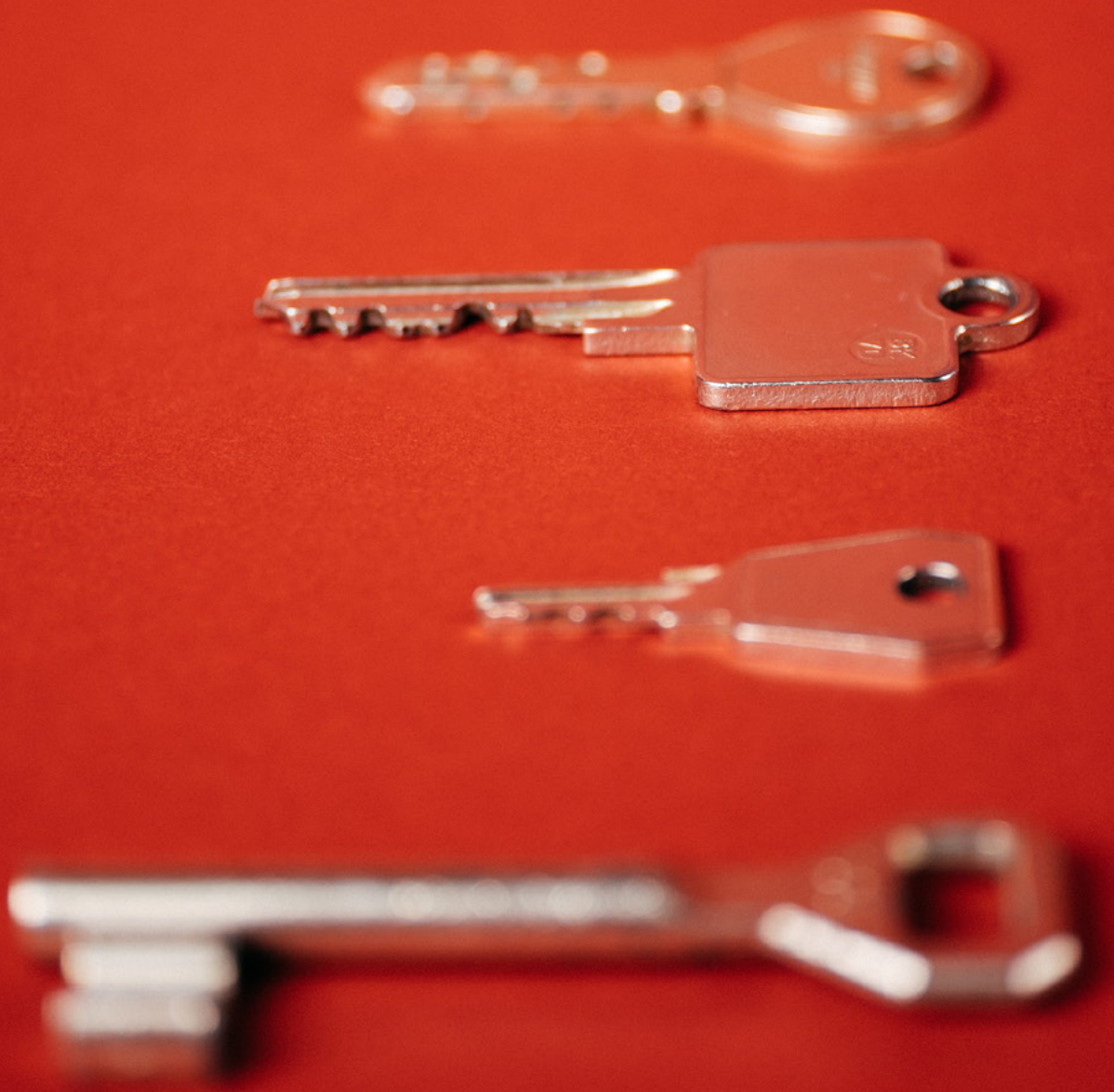
Even if your IT infrastructure is simple, or if it is important for you to retain **complete control over the entire backup process**, this solution can still offer you benefits.

If your company has a **complex IT infrastructure with extensive data management requirements**, such as multiple sites, different operating systems or specific applications, **a backup service may be a better option** – especially if you don't want to use your own resources to create it.

Even if your organisation does not have the IT resources or expertise to manage the backup process in-house, a backup service is the right solution. You can **benefit from the service provider's expertise and experience** to **manage the backup process efficiently** and ensure that your data is **stored safely and reliably in your backup storage**.

Checklist:

The 8 Security Criteria Your Backup Should Meet



The security and reliability of your backup will ultimately determine its usefulness in an emergency. To ensure that your **backup process is secure from the start**, we have put together a **helpful checklist** to help you plan your backup.

Define Responsibilities

» You should appoint a **reliable and trustworthy person to be responsible for the backup**. This is usually the IT administrator, who will train other responsible people in the procedures and monitor everything. If this is not possible internally, you can and should seek support from service providers.

Notes:

Data to be Backed Up and Security Standards

» Data and systems to be backed up need to be **defined and classified** by your company **before they are backed up**. Business-critical and personal data must always be backed up to a higher standard. You need to be aware of the standards you need to meet.

Notes:

Backup Locations

» Backup data should be stored redundantly – ideally in multiple geographically separated locations to avoid failures due to disasters or hardware problems. **Follow the 3-2-1 backup method**! When choosing a hosting service provider, make sure that they also offer you the option to store your **backups in different locations** – ideally within the EU.

Notes:

Backup Types

» Implementing different types of backups such as full, differential and incremental backups can increase the efficiency of your data protection and improve recovery time. **Define such an efficient backup strategy!** It is important to keep the specific needs of your business in mind.

Notes:

Backup Plan

» A **well-thought-out backup plan** that defines the frequency of backups, retention periods, and recovery goals is essential. It should also take into account the specific needs of your business.

Notes:

Automation of Your Backups

» Backup processes should be performed regularly and as automated as possible to minimise human error and **ensure that backups are actually created successfully**. Use the right software and, if in doubt, get help from a service provider!

Notes:

Checking Your Backup Processes

» The success of your backups needs to be checked regularly. There is no point in relying on your backup if it is not being made at the required intervals. **Run regular restore tests!**

Notes:

Recovery Plan

» A clear **disaster recovery plan** should be in place so that you can **act quickly in the event of an emergency**. This is critical to maintaining your business continuity.

Notes:

Comply With Legal Requirements

» The backup system should comply with **applicable legal requirements** and industry-specific regulations, such as the General Data Protection Regulation (GDPR).

Notes:

Physical Security

» The physical security of backup locations is just as important as the security of the data itself. This includes **protection against theft, fire, water and other potential threats**. Backup locations should therefore be secure and protected from unauthorised access. If your backup is stored in an offsite data center – which we always recommend – you should make sure you have this **comprehensive protection**!

Notes:

*Even **as your business processes and requirements change**, it is important that you **update your backup plans and processes.** As you have seen, there are many aspects that depend on your organisation's unique situation. **There is no room for one-size-fits-all solutions or ignorance.***

If you have the wrong backup, you may not have a backup at all!

Notes:

Use Cases & Best Practices

Finally, we would like to provide you with some typical use cases and helpful backup scenarios. But remember, as you probably already know: **It always depends on the individual case**.

The scenarios described are intended as a guide, not as a sophisticated backup strategy for your business!

Nextcloud: Not a Real Backup – But a Safety Net for Your Files When You Need It

Nextcloud is a **platform with many different features**. As well as a calendar, chat and other useful tools, the most important feature is the file and folder system, where you can store your important files and share them with other people. The great thing is that you can access and edit the data and functions on a wide range of devices.

This is based on **data synchronisation across all systems**, which could be considered a form of data backup. For example, if a device to which the Nextcloud is connected fails, the data is never lost, but **can be accessed from another device and used on the device again once it has been repaired**. So if the Nextcloud is on a secure server, using a Nextcloud can be a good backup in itself.

However, the various areas of Nextcloud should also be backed up. The backup process has several levels and processes:

- **File Backup:** Regular backups of files and folders in Nextcloud.
- **Database Backup:** Backup of the database, which contains the configuration and metadata of Nextcloud.
- **Configuration Backup:** Backup of Nextcloud configuration files and settings.

If you want to secure Nextcloud effectively, you should, as in all cases, think about how you use the platform in your company.

Scripts and tools can be used to regularly create full and differential backups of Nextcloud and store them on separate servers.

Again, regular testing of recovery processes is required to ensure that a quick and complete recovery is possible in the event of an emergency.

Backup of Virtual Machines & Containers:

Tools such as VMware, vShere or Hyper-V can be used to secure **virtual servers** or containers. These are the hypervisors used to create virtual systems. They usually have a solution for backing up the VMs. For example, the Proxmox Backup Server is used here.

This allows complete and incremental backups to be created.

Container backups: Tools such as Docker Backup or Kubernetes backup solutions can be used to back up container images and their data.

Again, automated backup processes ensure that VMs and containers are backed up regularly without the need for manual intervention.

Backing Up a Website

A website does not necessarily require the entire system to be backed up all the time, unlike the database and emails.

When backing up a website, **the data that makes up the presentation of the page** – i.e. HTML files or PHP with text and images – is obviously the first thing that needs to be backed up. If it is a CMS such as Wordpress, it is essential to **back up the database**. This contains the actual content, except for the media.

An example of this is the company website of a painting company: often only the contact information can be found here. This means that the page data rarely needs to be backed up. However, it is more important to **regularly back up the emails** to ensure they are not lost.

File Level Backup
(pure page elements php/html/etc.)

Database Backup

Email Backup

Backup of an Online Shop

If you want to back up an online shop that is heavily frequented, you should do this several times a day. For example, your **database will need to be backed up more often**. The shop's images, which usually do not change as often, need to be backed up less often. If you have a shop, always remember the **emails you have exchanged with your (potential) customers**.

Another useful scenario would be to only back up the databases at short intervals, where frequent changes are made. This could relate to stock and order information.

> *If a large number of orders are placed in a short period of time, it may also make sense to set up what is known as **live replication of the database**. In this case, even an hourly backup might not be sufficient in the event of data loss and could cause significant problems.*
>
> *However, this would not be a backup in the true sense of the word.*

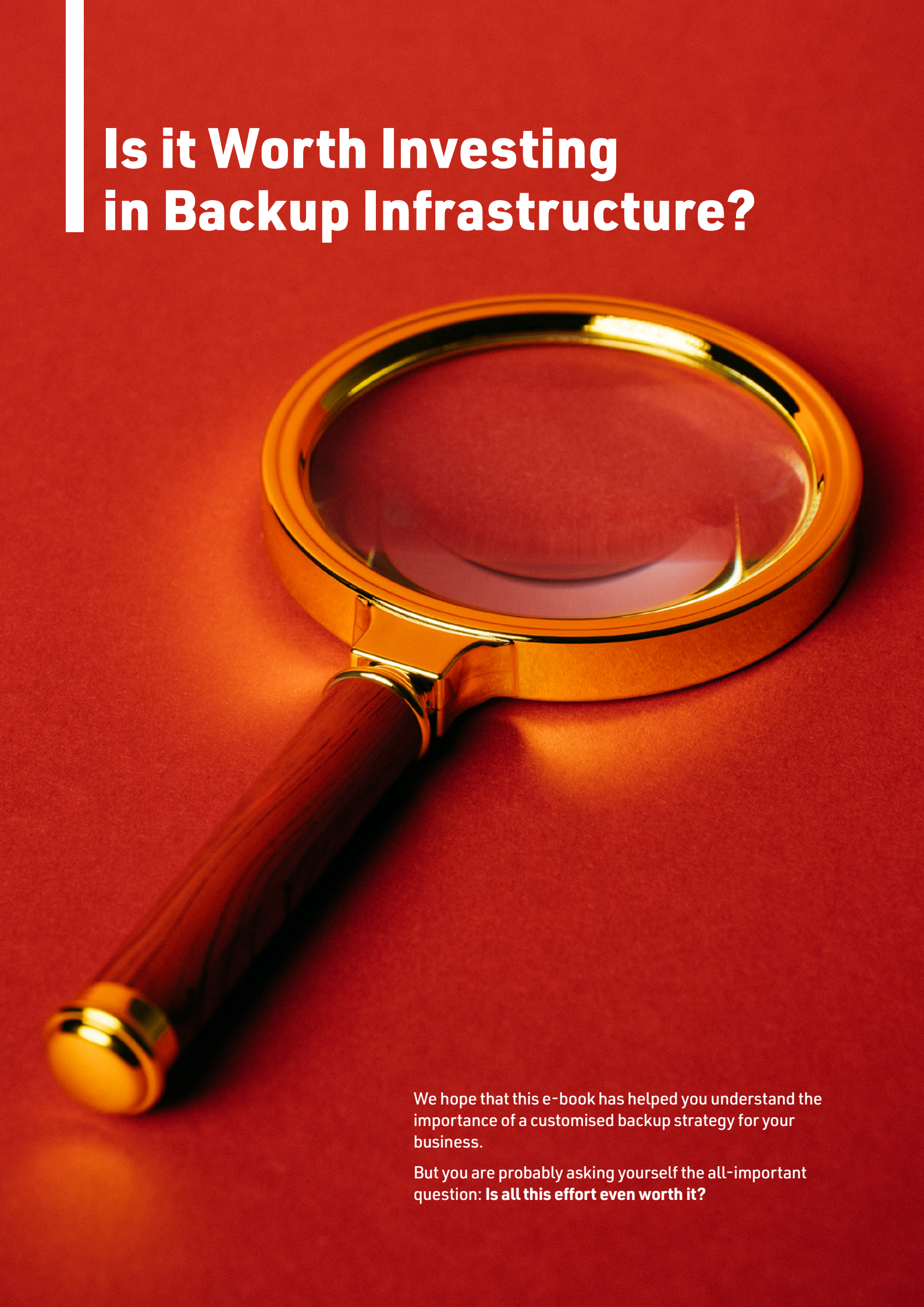
Securing a Server or Cloud Infrastructure

If you operate an environment for virtual machines, not every instance is usually equally important and data changes at different rates.

Depending on the size, a backup can be performed regularly in a quick cycle. In the case of a Proxmox environment, small instances can be backed up directly and easily via Proxmox.

The use of an additional Proxmox backup server is recommended. This does not have to be at the same site. In this case, you should speed up the backup after the first initial backup and only back up the most recent changes.

Is it Worth Investing in Backup Infrastructure?



We hope that this e-book has helped you understand the importance of a customised backup strategy for your business.

But you are probably asking yourself the all-important question: **Is all this effort even worth it?**

Implementing backup solutions naturally involves upfront costs for hardware, software and services. **Careful planning and budgeting in advance is therefore essential to ensure that the chosen solutions are both cost-efficient and effective**.

Investing in scalable backup solutions allows the system to grow with the business. Ongoing support and maintenance costs should also be included in the budget planning.

Long-Term Savings Thanks to an Effective Backup System

Preventing data loss can save significant costs in the long run that would otherwise be spent on downtime and data recovery.

- Avoiding Business Interruptions: Regular backups ensure quick recovery in the event of data loss, minimising business disruption.
- Reputation and Customer Trust: Preventing data loss helps to maintain a company's reputation and customer trust.
- Legal Compliance: Complying with legal requirements for data protection protects the company from legal consequences and possible fines.

So at this point we ask the question(s) again:

- What is your data worth to you?
- What is business continuity worth to you?
- And: What is your customers' trust worth to you?

And now we ask you:

Is it worth investing in efficient and effective backup processes?

Do you need help finding the right backup solution?

Our experts will provide you with attentive, personalised and expert advice.

Monday to Friday
8 am to 5 pm

Phone: +49 361/6 58 53-55
sales@keyweb.de

Keyweb AG
Neuwerkstraße 45/46
99084 Erfurt
Germany

Customised Backup Solutions from Keyweb

Are you looking for a backup solution that is optimally tailored to your needs? We help you to stay relaxed when it comes to data security!

- professional and customised backup advice
- GDPR-compliant hosting for specialised data protection
- comprehensive data security measures
- server-side DDoS protection
- TÜV certified redundant data center in Germany
- off-site backup possible thanks to distributed data centers

Customised Backup Solutions from Keyweb

Backup Storage KeyDisc Pro

» online backup storage

» with user-friendly interface

» deal for data & c onfiguration backup

» KeyHelp Pro software free of charge

Back up your data on the KeyDisc Pro

Select backup storage

KeyDisc Pro with Managed Service

» backup storage KeyDisc Pro

» incl. setup of your regular backup – optimised to your requirements

» regular functional check of your backup

» restore once a month included

Bookable as a backup solution for Keyweb servers.

Discover KeyDisc Managed

Proxmox backup server

» the ideal data backup for your cloud environment

» ideal if you use a Proxmox environment

» you save licence costs for backup software

Can be booked directly when ordering the cloud or later by ticket

Request by ticket

With managed backup, we have your back. We ensure that your backup is optimally set up and functional. – You just get on with your business.

1. We work with you to choose the **right backup software** and set it up for you.
2. In consultation with you, we will set up your **customised and desired backup** intervals and the **retention times for your data**.
3. We implement your chosen backup strategy.
4. Your data can be **restored free of charge** once a month.
5. We will **check that your backup has been created as planned**. If it has not, we will initiate it again or let you know.

When is the Managed Backup Service Right for You?

- ✔ if it is too time-consuming to regularly check the success of your backup
- ✔ if your backup needs to run very frequently and at short intervals, as a lot of data on your systems will have changed after a short time
- ✔ if you are temporarily unable to take care of your backups, for example during holidays or staff shortages

You can find more information about our backup solutions at:

keyweb.de/backup

Interested in customised backup solutions for your business?

Contact us today for a free consultation to find out how we can help you protect your data and ensure business continuity.