Data back-ups in an SME environment

Back-ups to provide for quick and ideally complete recovery of your data in case of loss due to malicious, accidental or coincidental scenarios are one of the crucial basic protection measures an SME should take. This requires the implementation of a refined data back-up process.

The most important points for companies to remember:

- Draw up an inventory of your IT systems and data, and establish the maximum tolerable loss or outage for each item.
- Based on this information, create protection categories for objects with the same risk, and define a data back-up concept for each respective protection category.
- Define and implement a data back-up process in your SME.
- Regularly check that your data have been backed up correctly and can be recovered in accordance with your data back-up concept.

The data back-up process

With increasing digitalisation, the number of IT systems used and the quantities of data processed is continuously rising in SMEs, too. This means that an SME's reliance on the unlimited availability of its IT systems and data increases as well.

Extensive data loss, for instance due to malicious cyber-attacks, technical defects, force majeure or accidental deletion, can pose an existential threat to SMEs. The ability to recover company data quickly and ideally completely from a data back-up is therefore part of their vital basic protection.

To this end, a data back-up process should be established which safeguards that back-ups are carried out properly in accordance with a data back-up concept. And it is just as important to also check that data recovery works properly as part of this process, too.

Protection classes

Not every IT system run by an SME is equally vital for its business processes. A differentiated assessment of the respective need for protection for all IT systems and data is therefore needed. An extensive and up-to-date inventory of all IT systems and data is the basis for gaining an overview and to allocating all items listed to an appropriate protection class.

Example protection class allocation based on criteria

PC	Description	Risk	Max. tolerable outage/loss	Recovery time	Retention period
I	Standard need for protection	Small	> 1 day	< 1 week	> 1 week
II	High need for protection	Medium	1 day	1 day	> 1 month
III	Very high need for protection	High	< ½ day	< 1 day	> 1 year

Next to the threat posed by the harmful influences mentioned, there are additional criteria to be considered. This includes the maximum tolerable duration of any temporary outage of IT systems or quantitative loss of data on the one hand and the retention periods required on the other.

Such an assessment makes it possible to combine IT systems and data with a similar need for protection into protection classes. Subsequently, the requirements for a suitable data back-up concept are then established for every protection class.

Data back-up concept

The data back-up concept determines organisational and technical back-up details for every protection class. In particular, the following organisational details count amongst them:

1. Extent of data back-up (scope)
2. Frequency of data back-up (daily, weekly, monthly, ...)
3. Time of data back-up (end of the day, week-end, month end, ...)
4. Retention period of back-up versions (generation principle)
5. Required recovery times (maximum tolerable outage)

From this, the following technical details of implementation can then be deduced, in particular:

1. Data back-up process (complete, differential, incremental)
2. Back-up medium (hard drive, tape, ...)
3. Storage of data back-up media (on premise, physical external storage, cloud, ...)

Extensive data loss – for instance due to malicious cyber-attacks, technical defects, force majeure or accidental deletion – can pose an existential threat to SMEs.

Using a clever data back-up concept, such risk scenarios can be minimised by achieving a quick and ideally complete recovery of any data lost.

Further information

The **data back-up scope** serves to establish which data (sources) will actually be included in the data back-up. A well thought-out and structured data filing system can to a great extent ensure that no important data are overlooked. In addition, you should check whether the data (sources) for back-up are actually available at the time of the data back-up run (for instance with regard to devices which might be switched off over the week-end)

If you create a **data back-up** at **short intervals**, this does safeguard against any minor data losses. On the other hand, it also increases the effort required for data back-ups. In particular, this could lead to bottlenecks on the network, if you back up large data quantities every day. In this case, it is recommended you carefully assess your needs for protection.

The **time of your data back-up** depends on your business processes. Here you should assess the risk evolution of any potential data loss inside the time period between your individual data back-ups. A frequent practice is therefore to run back-ups at the end of every day, so not to disrupt daily operations and use the resources available at night for data back-ups.

In case of data loss, you generally restore the version of the last available data back-up. For various reasons, it might also be necessary though to be able to recover older historical data from further back at times. For such data, you should determine a **retention period for your back-ups**. With the help of a well thought-out rotation schedule (generation principle) geared towards data volumes and protection needs, such retention periods can be safeguarded with a minimum of data back-up media. When backing up data daily for instance (Mo to Fr), it only takes 20 data back-up media to be able to recover the back-up versions of the last four weekdays (Mo to Th), the last 13 weekends (Fr), the last two month ends and the last year end.

The term **required recovery times** denotes the period of time between the discovery of any data loss up to the time access is reinstated. The shorter this maximum tolerable outage period is set, the higher the organisational and technical requirements with regard to your data back-ups. Things to be considered here are the required time for identifying data to be recovered, locating such data on their respective data back-up copies, access to the required data back-up media and the actual data restoring process.

Sometimes, the time available (e. g. during the night) is not sufficient to completely back up data from a certain protection class at the required frequency. You can mitigate this problem by carefully choosing the type of data back-up method you use (complete, differential, incremental). With a **complete** data back-up, a complete copy of all data inside the scope is created on your data back-up medium. This method requires most space on your data back-up medium and the most time. With the **differential** method however, only the data changed since the last complete data back-up are backed up (those different from the last complete back-up). This considerably reduces the data volume, since unchanging data in particular only ever have to be backed up once. Recovery of a data back-up version takes place in two stages with this method: First, you will need to restore the last complete back-up you have, and then restore the required differential data back-up. The **incremental** method reduces the data volume to be backed up even further. Here, only changes compared to the last data back-up (no matter of what type) are backed up. If there is a need to recover data, you will therefore have to restore the last complete data back-up, the last differential data back-up as well as all subsequent incremental data back-ups.

The term **data back-up medium** denotes the container used to record a certain data back-up version. In its sim-

plest form, this could involve a simple file with a specific file format, or a physical data carrier (hard drive, optical medium, magnetic tape,) on a dedicated back-up system. The choice of a suitable data back-up medium primarily depends on the organisational requirements (extent, frequency, retention periods and recovery times). In particular for long-term retention (archiving) of large data volumes, magnetic tapes have become the medium of choice.

Data back-up media and their **storage** are of absolutely vital importance for the whole data back-up process. As far as risk assessments are concerned, factors such as physical protection, storage conditions, availability, accessibility etc. must be considered. Generally, data back-ups should be insulated against external influences to the maximum extent possible. In connection with ransomware for instance, you have to ensure that data back-ups are stored in such a way they are completely out of reach of any attacker. It is therefore vital to store them offline.