Tip sheet

BACK UP YOUR DATA SAFELY

Data is a vital element and a valuable asset of modern society. Their loss can not only cause significant damage, for example in financial terms, but also disrupt business operations or trade.

Backing up your data – that is, copying or archiving data to restore it if it is lost or damaged – is therefore essential for both businesses and individuals, who are also facing storage challenges.

Definition of successful backup

Successful data backup combines reliability, protection against security threats and resource optimization. This combination ensures accurate and fast recovery of data in the event of loss.

1 Reliable backup

Backed up data is recoverable consistently and accurately. Regular backups, one or several duplications from a primary source to one or several locations and secondary storage media are required.

2 Secure backup

The backed-up data is protected against unauthorized access, its integrity is guaranteed, and encryption and access controls are used to prevent data breaches and data leaks.

3 Efficient backup

Storage space, processing power during backup or restore, and network bandwidth all need to be optimized.

RELIABILITY + **SECURITY** + **EFFICIENCY** = **SUCCESSFUL BACKUP**

Why backup?

Backing up means solving four problems that companies or organizations – just as individuals – face in their day-to-day activities:

- Any computer or its components – such as hard drives – may fail (software or hardware failure).
- Anyone can make mistakes (mishandling or accidental deletion of files, etc.)
- Anyone can be a victim of a cyber-attack (security threats).
- Disasters always occur at a time when they are least expected (disasters or natural disasters).

→ ***If your data is lost, deleted or corrupted, backup is your only ally.***

restena
réseau · sécurité · .lu

Tips on how to implement efficient backup

A successful backup relies on the establishment of clear backup objectives based on an evaluation of the data and the establishment of a backup strategy that answers a set of key questions. In companies, policies and obligations can influence this strategy. For example, some of them do not allow data to be backed up to a public cloud. So make sure you ask yourself the right questions before considering a backup.

What data should be backed up?

Not all the data you have is equally important. Think about each type of data and decide if they deserve to be backed up: are they critical and/or do regulatory data retention requirements apply to them?

How often do I back up data?

Once you have identified the data to be backed up, define how often the backup should be performed: on a weekly, monthly, or yearly basis? It is up to you to decide the pace, but it must be consistent, regular, and constant.

Tip!

To reduce the risk of human error, consider automating your backups with automated backup software or scripts.

How long shall I keep data?

The retention time of the data depends on the nature of the data. Personal data, for example, is subject to the General Data Protection Regulation (GDPR). Business-related general documents also meet legal retention requirements that must be complied with.

Where shall I store data?

There are two main types of media – local backup and cloud backup. It's up to you to choose the one that suits you best.

LOCAL BACKUP

Local backup is physical storage, such as external hard drives, magnetic tapes, or network storage.

Specifications

The data is stored at the main site of a company or organization. Backups are frequently performed on internal or external hard drives.

Strengths

- Fast data recovery
- Data control
- Guaranteed confidentiality

CLOUD BACKUP

Cloud backup uses cloud-based solutions such as public cloud, private cloud or cloud to cloud (C2C).

Specifications

The data is stored on an off-site server or storage system, typically hosted by an outsourced backup provider.

Strengths

- Off-site storage
- Better disaster recovery capabilities

The 3-2-1 backup policy

To ensure optimal backup, keep multiple backup copies.

- **3** copies of your original data (including original data)
- **2** backup copies on different media
- **1** copy stored 'off-site', i.e., in another location (another building, another IT environment, such as the cloud, etc.)

The 'off-site' copy is used primarily to guard against physical disasters – such as fires, floods or theft – that could occur on the main data storage site.

→ ***Don't wait for your data to disappear before setting up your backup plan !***

Protect your backups from cyber attacks

Even if it is the best solution to ransomware attacks (attacks that take the data present on their victims' computer hostage for a monetary ransom); backup is also the target of this technique used by cybercriminals.

Physically isolate storage media

Physical isolation is the process of disconnecting storage media from the network. Since the storage medium is completely offline, it remains protected against malware, viruses or ransomware that could spread across connected systems.

Ensure the immutability of backups

An immutable backup is a copy of data that cannot be altered, deleted or modified in any way. In such a case, even the system administrators, users, applications or systems that created the data cannot alter it.

Encrypt data

Encrypting data protects against misuse and leak of exfiltrated data (data exfiltration/data leaks). While this does not offer protection against ransomware (re)encryption, it ensures that your data is unusable. With encryption, data is converted from a readable format to an encrypted format and can only be read by the owner of the data with the correct encryption key.

Example: the vulnerability of research and education

The diverse nature of data, the variety of systems used and the need for robust protection of sensitive information pose unique challenges to the research and education sector. This sector is particularly vulnerable because of its distributed data sources, the type of sensitive and proprietary information – ranging from student records to cutting-edge research results – it processes, the diversity and complexity of the data structures and technology platforms and systems it faces.

These challenges need to be addressed with tailored solutions that include robust backup plans, best practice training, investment in user-friendly backup tools, appropriate encryption methods, and a comprehensive recovery plan following data loss.

Recommendation and responsibility

Define clear and documented strategies.

Identify your data protection needs and document your backup strategy and any associated procedures to ensure a clear understanding of processes and responsibilities.

Be in line with data security and regulatory compliance.

Ensure that your backup practices comply with applicable data protection and privacy regulations and that they comply with any security policies in place in your organization.

Regularly review, test, and improve your backup plan.

Review your backup plan periodically or whenever changes occur in data structure, technology advances, storage needs and obligations. And also make sure you test the data recovery process and make adjustments if needed.

→ ***Your backups must be reliable and functional at all times. When in doubt, review and adapt your backup plan.***

Service offer

Thanks to its Computer Security Incident Response Team (Restena-CSIRT), the Restena Foundation assists the Luxembourg's research and education community encountering computer security incidents. It also conducts tailor-made phishing and awareness-raising campaigns on hot topics and jointly organises conferences such as CyberDay.lu and Data Privacy Day.

For more information on this service, please visit www.restena.lu/csirt

Co-funded by the European Union

This tip sheet is one of the awareness-raising activities set up as part of the European LuCySe4RE project that has received funding from the European Union’s Digital Europe programme (DIGITAL) under grant agreement No. 101127864.

restena
réseau · sécurité · .lu