INFRADAX

E-BOOK

HOW A GOOD BACKUP PROTECTS YOUR DATA FROM HACKERS AND DISASTERS

The rise of disruption

Cyber attacks, power outages and fires increasingly cause organizations to suffer from unplanned downtime and data loss. This is called "the rise of disruption '. In many cases, data is permanently lost, which can cause major problems. It is therefore increasingly important to protect data against "disasters" and hackers. In this e-book we help to explain how to keep data safe and what is required when determining your backup strategy.

At a time where organizations are generating more and more data, it is logical that data loss has a major impact. Dell estimates that the failure of systems costs large organizations (250+ employees) on average more than 700,000 euros per year. The recovery of business-critical applications takes an average of eight hours.[1] This downtime affects productivity and the speed at which new products and services are brought to the market. In the event of a data breach, you also run the risk of reputation damage, a fine or even a damage claim.[2]

Hybrid cloud frequently chosen option for data protection

According to Dell, few affected organizations are confident that they can keep threats permanently at bay.[3] The majority therefore intends to invest in new technologies better suited for data protection. The choice increasingly falls on the hybrid cloud. Mission critical workloads are then housed in both public and private clouds.

The main reasons for this are:

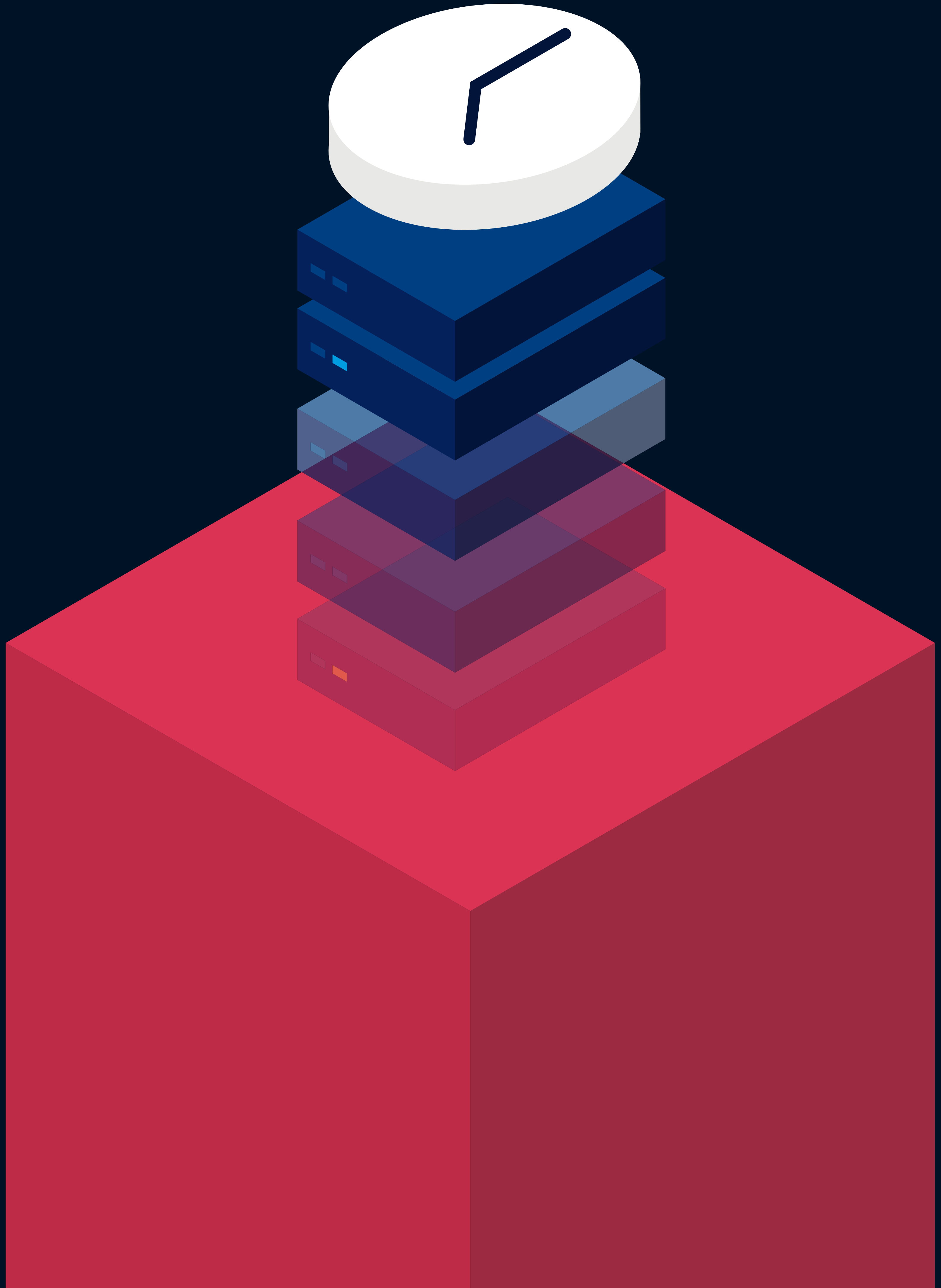
- ✓ Better performance
- ✓ Better security
- ✓ More reliable data protection
- ✓ Scalability
- ✓ Lower costs
- ✓ Faster time to market

Dell says many organizations are struggling to implement a data protection solution. An important reason for this is that they have to take into account privacy legislation (AVG). Concerns about compliance, "disasters" and cybercrime are forcing them to consider a complete data protection plan.

Backup important data protection component

A backup is an important part of a disaster recovery plan. The short definition of a backup is "a copy of your data". You fall back on that after an incident, so that you can get back to work. But there is more to it.

1. **Step 1: Determine how long you want to keep data**
2. **Step 2: Choose the correct backup medium**
3. **Step 3: Choose the correct backup method**



1

Step 1: Determine how long you want to keep data

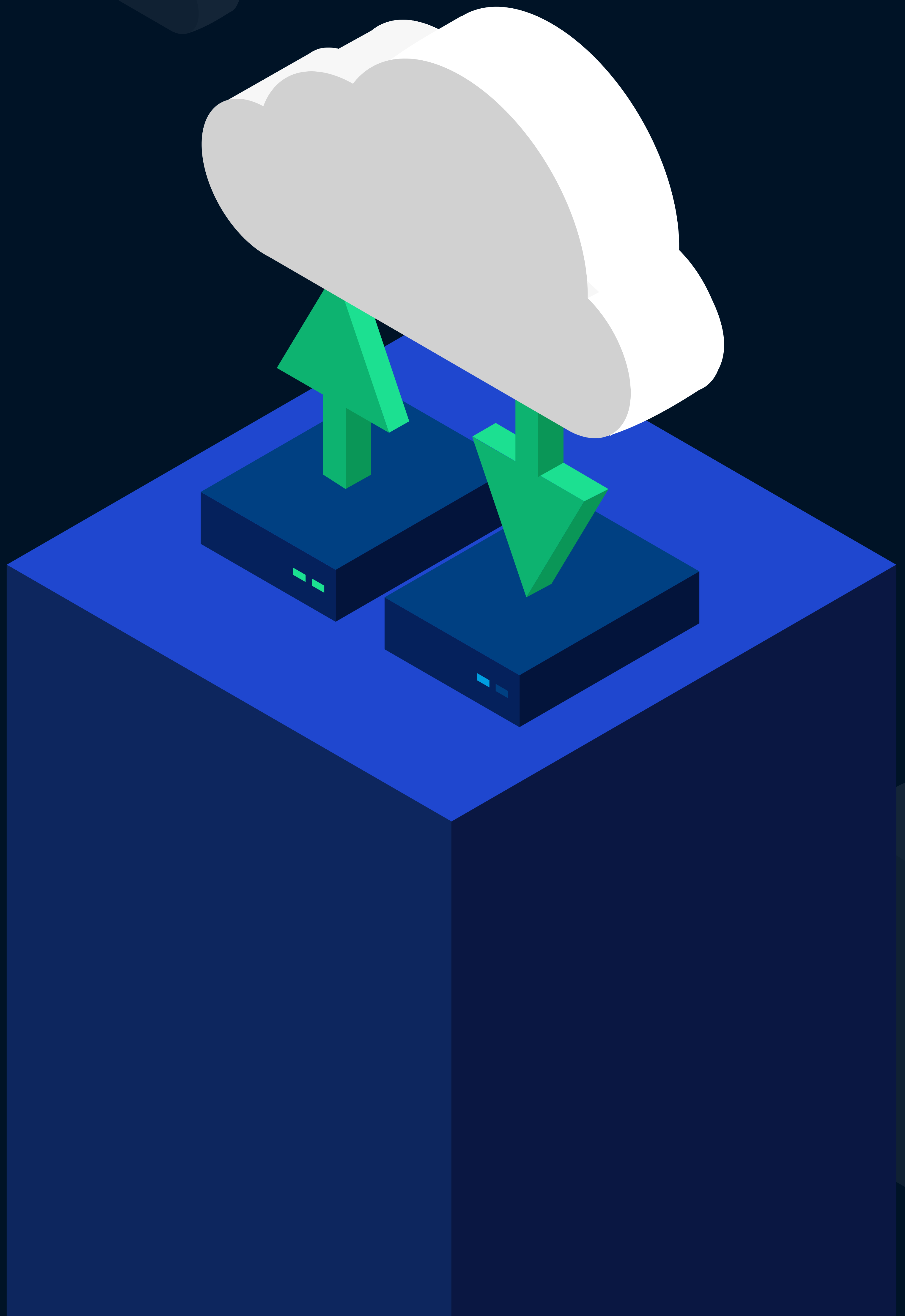
Because in general, costs increase as recovery time is shorter and the amount of data loss is lower, determining your backup strategy starts with questions about RTO and RPO times: how fast data must be restored and how much data can be lost. to go? The answer differs per company and per application. A webshop can probably not afford a minute of downtime, because otherwise customers will go directly to the competitor. For a production company, a somewhat longer recovery time may be less of a problem, for example because it can also process invoices in the evening.

2

Step 2: Choose the correct backup medium

Costs also determine the choice of the backup medium. There are roughly three options[4]:

- **Hard disk drives:** Disks are widely used for backups because of the possibility of data deduplication. That frees up a lot of disk space, which is helpful with continued growth of data. In addition, disks in contrast to tape, can perform multiple tasks at the same time, including hundreds of backups at the same time.[5]
- **Back-up servers:** Your system is, as it were, redundant, with a server especially for storing copies. A disadvantage may be that when your server is on-site, you will still lose data in the event of a fire. That is why many organizations opt for the cloud: you then have a backup server in an external data center. If it is owned by a provider, it has the advantage that you can easily scale up and only pay for use. A possible disadvantage is that you are dependent on the speed of your connection. There may also be objections in the field of security and privacy, but providers often use of the latest technologies. In order to stay relevant and to strengthen their distinctiveness.
- **Tape drives:** An old and trusted medium that offers a lot of storage capacity. The low cost makes tape interesting. This is especially true for organizations that have to deal with long retention periods, but do not necessarily need to be able to quickly access stored data.



3

Stap 3: Choose the correct backup method

In addition to the storage medium, you should also consider the backup method.

Common types are:

- **Full back-up:** This is a complete copy of the data source, which is created at regular intervals. The recovery operation proceeds relatively quickly. Copying, requires quite a lot of time and storage space.
- **Incremental back-up:** Your backup only contains the files that have changed since the last full backup. This saves time and storage space. The downside is that each incremental backup has to be processed in the correct order when restoring, which can take a long time.
- **Differential back-up:** This method is based on the latest changes after a full backup, but is cumulative in nature. This means that all backups that have been made since the full backup are copied. This process takes less time than making a full backup, but more than an incremental backup. The recovery time is shorter than with incremental backups.

Another popular method is continuous backup (data replication). Changes to the source system are then continuously moved to a target system within seconds. This results in a low RTO. The second system takes over immediately if the first crashes. Furthermore, snapshots are used to quickly restore data. At a certain moment, a picture is taken of your system, as it were. If your system crashes, it reverts to that point in time. This ensures a low RPO.

Stick to the 3-2-1 rule

It is not that there is only one ideal method or strategy. The best solution depends on your specific situation. There is, however, a basic rule for a good backup: the 3-2-1 rule. This means that you have to make three copies, one is not enough. You use at least two different media for this. And you keep one copy outside the door.

In any case, there are four principles to keep in mind when determining your backup strategy:

1. **Automate:** Computers are good at repetitive tasks. Automation reduces the risk of human error and saves time. Cloud tiering is an example of this. Files that have not been used for a long time are automatically archived in the cloud.
2. **Regulate:** Determine your RTO and RPO times.
3. **Copy:** Choose your method, media and infrastructure. The trend is to merge functions in one appliance, such as the Dell IDPA. That is hardware and software in one, which can store a lot of data through compression. Tasks for management, monitoring and reporting are automated. IDPA is also a scalable solution, which also protects against ransomware.
4. **Test:** by regularly testing your backup solution, you will not be faced with surprises if a disaster actually occurs.

Dell says many organizations are struggling to implement a data protection solution. An important reason for this is that they have to take into account privacy legislation (AVG). Concerns about compliance, "disasters" and cybercrime are forcing them to consider a complete data protection plan.

Infradax relieves you with Backup as a Service

Infradax is a certified backup specialist, who can advise you on the best strategy and IT infrastructure in order to create a safe and comprehensible IT environment. We design, implement and manage complete data protection solutions. Because we can buy back and dispose of your old IT hardware, we keep the TCO low. You can also choose Back-up as a Service (BaaS). This has many advantages: you only pay for data that you actually store. Your data is safely stored in a Dutch data center and you determine the balance between management and total unburdening. With Infradax you are always protected against loss of business-critical data.

INFRADAX

Want to know more about backup strategies?

Contact our specialists
hello@infradax.com

DELL Technologies

[1] https://www.delltechnologies.com/en-us/data-protection/gdpi/index.htm#overlay=//www.dellemc.com/en-us/collaterals/unauth/presentations/products/data-protection/dell-gdpi-2019-key-findings-deck-dell-branding.pdf
[2] https://wire19.com/reasons-for-data-backup-and-recovery/
[3] https://corporate.delltechnologies.com/en-us/newsroom/announcements/2019/03/20190321-01.htm
[4] https://www.ibm.com/cloud/learn/backup-and-restore
[5] https://www2.computerworld.nl/it-beheer/107708-waarom-tape-soms-beter-is-dan-een-hdd

INFRADAX

Fortranweg 8
3821 BK, Amersfoort

✉ hello@infradax.com
☎ +31 (0) 33 789 00 33