

E-BOOK

HOE EEN GOEDE BACK-UP JE DATA BESCHERMT TEGEN HACKERS EN RAMPEN



The rise of disruption

Door cyber attacks, stroomuitval en brand hebben organisaties steeds vaker last van ongeplande downtime en dataverlies. Dit wordt ook wel 'the rise of disruption' genoemd. In veel gevallen gaat data definitief verloren, wat voor grote problemen kan zorgen. Het is dus steeds belangrijker om data te beschermen tegen 'disasters' en hackers. In dit e-book vertellen we hoe je data veilig bewaart, en waar je op moet letten bij het bepalen van je back-up strategie.

In een tijd dat organisaties steeds meer data genereren, is het logisch dat dataverlies grote impact heeft. Dell schat dat de uitval van systemen grote organisaties (+250 werknemers) gemiddeld ruim 700.000 euro per jaar kost. Het herstel van bedrijfskritische applicaties duurt gemiddeld acht uur.¹ Die downtime heeft gevolgen voor de productiviteit en de snelheid waarmee nieuwe producten en diensten naar de markt worden gebracht. Bij een datalek loop je ook het risico van reputatieschade, een boete of zelfs een schadeclaim.²



Hybrid cloud veelgekozen optie voor dataprotectie

Volgens Dell hebben maar weinig getroffen organisaties er vertrouwen in dat ze bedreigingen definitief buiten de deur kunnen houden.³ Het merendeel is daarom van plan te investeren in nieuwe technologieën voor betere databescherming. De keuze valt daarbij steeds vaker op de hybrid cloud. Mission critical workloads worden dan zowel in public als private clouds ondergebracht.

Drijfveren daarvoor zijn:

- ✓ Betere performance
- ✓ Betere security
- ✓ Betrouwbardere dataprotectie
- ✓ Schaalbaarheid
- ✓ Lagere kosten
- ✓ Snellere time to market

Dell zegt dat veel organisaties worstelen met het implementeren van een oplossing voor dataprotectie. Een belangrijke reden daarvoor is dat ze rekening moeten houden met privacywetgeving (AVG). Zorgen over compliancy, 'disasters' en cybercriminaliteit, dwingt hen tot nadenken over een compleet dataprotectieplan.

Back-up belangrijk onderdeel dataprotectie

Een back-up is een belangrijk onderdeel van zo'n plan. De korte definitie van een back-up is 'een kopie van je data'. Daar val je op terug na een incident, zodat je weer aan de slag kunt. Maar er komt meer bij kijken.

1

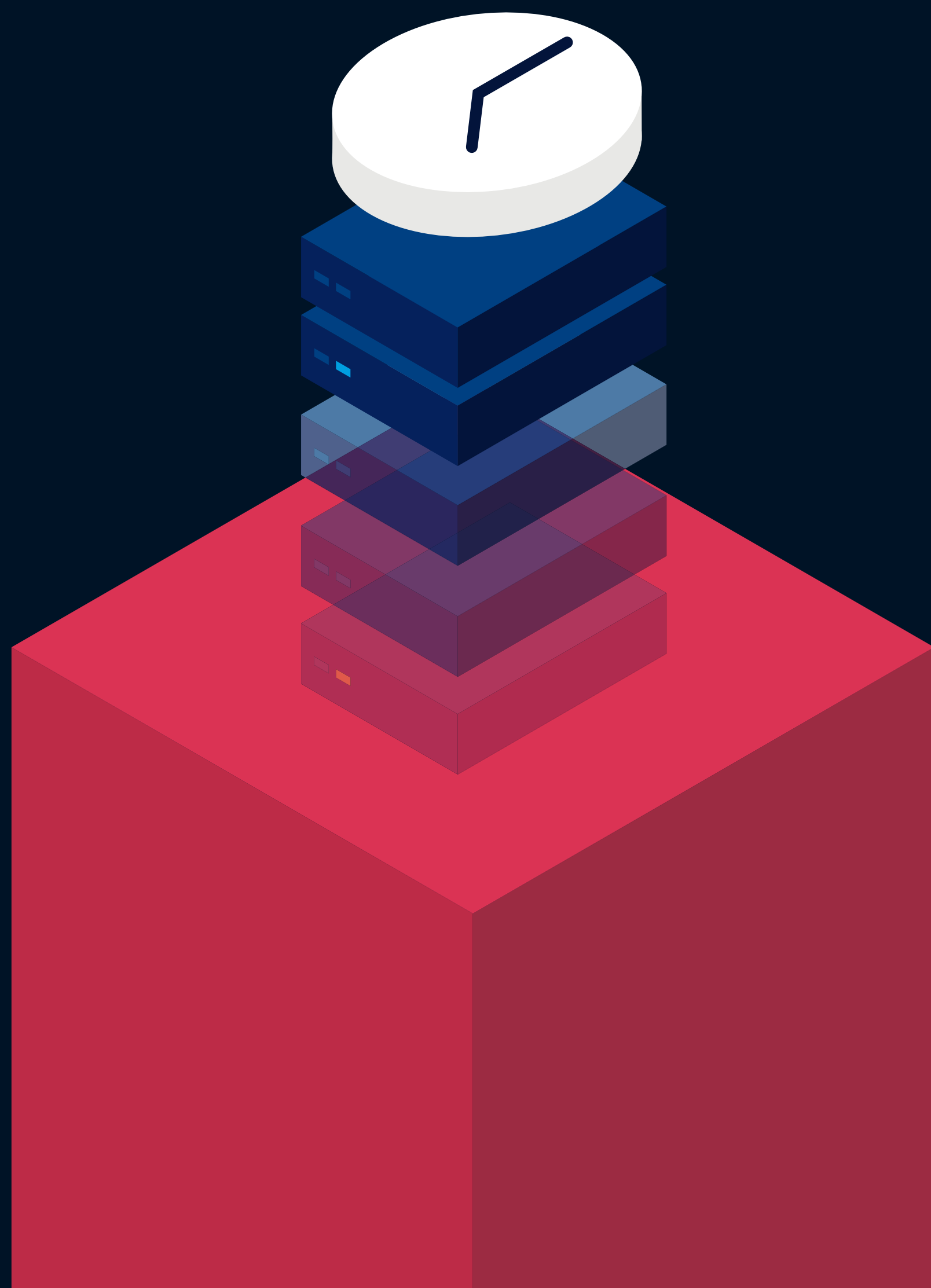
Stap 1: Bepaal hoe lang je data wilt bewaren

2

Stap 2: Kies het juiste back-up medium

3

Stap 3: Kies de juiste back-up methode



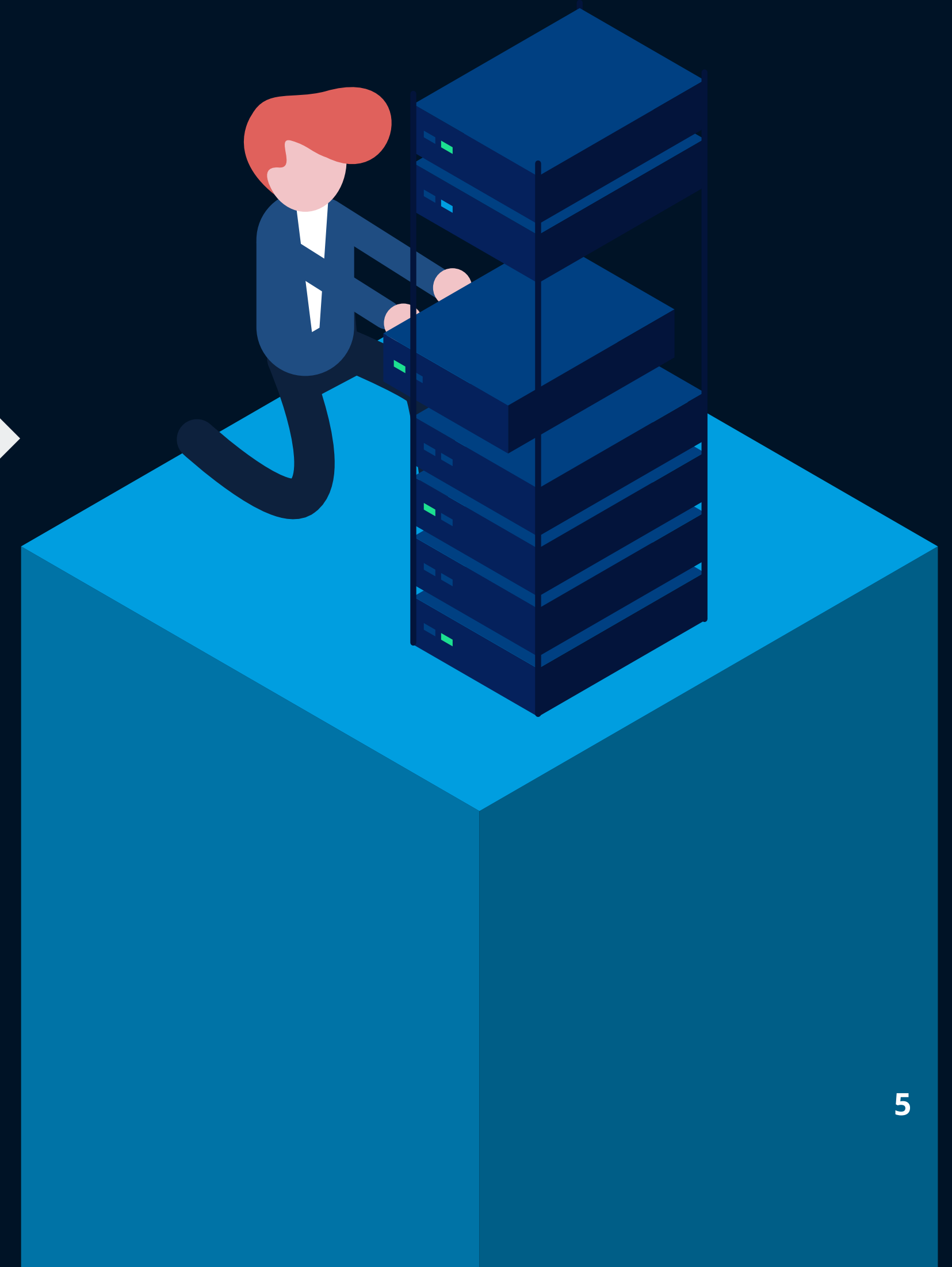
Stap 1: Bepaal hoe lang je data wilt bewaren

Omdat over het algemeen geldt dat kosten stijgen naarmate de hersteltijd korter is en de hoeveelheid dataverlies lager is, begint het bepalen van je back-up strategie met vragen over RTO- en RPO-tijden: hoe snel moet data hersteld zijn en hoeveel data mag verloren gaan? Het antwoord verschilt per bedrijf en per applicatie. Een webshop kan zich waarschijnlijk nog geen minuut downtime veroorloven, omdat klanten anders direct naar de concurrent gaan. Voor een productiebedrijf is een wat langere hersteltijd mogelijk een minder groot probleem, bijvoorbeeld omdat het facturen ook 's avonds nog kan verwerken.

Stap 2: Kies het juiste back-up medium

Kosten zijn ook bepalend voor de keus van het back-up medium. Er zijn grofweg drie opties⁴:

- **Hard disk drives:** Disks worden veel gebruikt voor back-ups omdat deduplicatie mogelijk is oftewel gegevensontdubbeling. Dat maakt veel schijfruimte vrij, wat handig is bij voortdurende groei van data. Daarnaast kunnen disks anders dan tape meerdere taken tegelijk uitvoeren, dus ook gelijktijdig honderden back-ups uitvoeren.⁵
- **Back-up servers:** Je systeem is als het ware dubbel uitgevoerd, met een server speciaal voor het bewaren van kopieën. Een nadeel kan zijn dat wanneer de server on-site staat, je bij brand nog steeds data verliest. Daarom kiezen veel organisaties voor de cloud: je beschikt dan over een back-up server in een extern datacenter. Als deze eigendom is van een provider, heeft dat als voordeel dat je gemakkelijk kunt opschalen en alleen betaalt voor gebruik. Een mogelijk nadeel is dat je afhankelijk bent van de snelheid van je verbinding. Er kunnen ook bezwaren leven op het gebied van veiligheid en privacy, maar aanbieders stellen daar het gebruik van de nieuwste technologieën tegenover.
- **Tape drives:** Een oud en vertrouwd medium dat veel opslagcapaciteit biedt. De lage kosten maken tape interessant. Dat geldt met name voor organisaties die te maken hebben met lange bewaartermijnen, maar niet per se snel bij opgeslagen gegevens hoeven te kunnen.



Stap 3: Kies de juiste back-up methode

Behalve over het opslagmedium moet je ook nadenken over de back-up methode.

Veel voorkomende soorten zijn:

- **Full back-up:** Dit is een complete kopie van de databron, die met regelmatige intervallen wordt gemaakt. De hersteloperatie verloopt relatief snel. Het kopiëren vergt daarentegen vrij veel tijd en opslagruimte.
- **Incremental back-up:** Je back-up bevat alleen de bestanden die gewijzigd zijn sinds de laatste full back-up. Dit bespaart tijd en opslagruimte. Het nadeel is dat bij herstel elke incremental back-up in de juiste volgorde moet worden verwerkt, wat lang kan duren.
- **Differential back-up:** Deze methode gaat ook uit van de laatste wijzigingen na een full back-up, maar is cumulatief van aard. Dat betekent dat telkens alle back-ups die sinds de full back-up zijn gemaakt, mee worden gekopieerd. Dit proces kost minder tijd dan het maken van een full back-up, maar meer dan een incremental back-up. De hersteltijd is wel korter dan bij incremental back-ups.

Een andere populaire methode is de continue back-up (datareplicatie). Wijzigingen in het bronsysteem worden dan doorlopend binnen enkele seconden verplaatst naar een doelsysteem. Dat resulteert in een lage RTO. Het tweede systeem neemt het direct over als het eerste crasht. Verder worden snapshots wel gebruikt om data snel te kunnen herstellen. Er wordt dan op een bepaald moment als het ware een foto gemaakt van je systeem. Als je systeem crasht, zet je het terug naar dat tijdstip. Dit zorgt voor een lage RPO.

Hou je aan de 3-2-1-regel

Het is niet zo dat er maar één ideale methode of strategie is. Het hangt van jouw specifieke situatie af wat de beste oplossing is. Wel is er een basisregel voor een goede back-up: de 3-2-1-regel. Die houdt in dat je drie kopieën moet maken, één is niet voldoende. Daarvoor gebruik je minstens twee verschillende media. En één kopie bewaar je buiten de deur.

In ieder geval zijn er vier uitgangspunten om in het achterhoofd te houden bij het bepalen van jouw back-up strategie:

- 1 **Automatiseer:** Computers zijn goed in repeterende taken. Automatiseren vermindert de kans op menselijke fouten en spaart tijd. Cloud tiering is hiervan een voorbeeld. Bestanden die lange tijd niet meer zijn gebruikt, worden automatisch gearchiveerd in de cloud.
- 2 **Reguleer:** Bepaal je RTO- en RPO-tijden.
- 3 **Kopieer:** Kies je methode, media en infrastructuur. Trend is om functies samen te voegen in één appliance, zoals de Dell IDPA. Dat is hard- en software ineen, die door compressie veel data kan opslaan. Taken voor beheer, monitoring en rapportering verlopen geautomatiseerd. IDPA is bovendien een schaalbare oplossing, die ook beschermt tegen ransomware.
- 4 **Test:** door je back-up oplossing regelmatig te testen, kom je niet voor verrassingen te staan als zich werkelijk een disaster voordoet.

Dell zegt dat veel organisaties worstelen met het implementeren van een oplossing voor dataprotectie. Een belangrijke reden daarvoor is dat ze rekening moeten houden met privacywetgeving (AVG). Zorgen over compliancy, 'disasters' en cybercriminaliteit, dwingt hen tot nadenken over een compleet dataprotectieplan.

Infradax ontzorgt met Back-up as a Service

Infradax is een gecertificeerd back-up specialist, die jou kan adviseren over de beste strategie en de IT-infrastructuur die daarbij hoort. We ontwerpen, implementeren en beheren complete dataprotectie oplossingen. Doordat we jouw oude apparatuur kunnen opkopen en afvoeren, houden we de TCO laag. Je kunt ook kiezen voor Back-up as a Service (BaaS). Dat heeft veel voordelen: zo betaal je enkel voor data die je daadwerkelijk opslaat. Je data staat veilig opgeslagen in een Nederlands datacenter en jij bepaalt zelf de balans tussen regie en totale ontzorging. Met Infradax ben je altijd beschermd tegen verlies van bedrijfskritische data.



**Wil je meer weten
over back-up strategieën?**

Neem dan gerust contact op.

hello@infradax.com

DELLTechnologies

¹<https://www.delltechnologies.com/en-us/data-protection/gdpr/index.htm#overlay=//www.dell.com/en-us/collaterals/unauth/presentations/products/data-protection/dell-gdpr-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>



Fortranweg 8
3821 BK, Amersfoort

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