



WHITEPAPER

BACK-UP

Uitleg over en de weg naar een goed doordachte
back-up-strategie.

INLEIDING

Wat gebeurt als je een belangrijk bestand kwijt bent? Of nog erger, wat als alle documenten weg of stuk zijn? In hoeverre ben je in staat om daarvan te herstellen? En welke impact heeft het op je business? Geen leuke vragen om over na te denken maar het hebben van een goede back-up-inrichting is belangrijker dan ooit.

Bedrijven zijn in toenemende mate afhankelijk van digitale gegevens om hun dagelijkse activiteiten te ondersteunen. Het verlies of de beschadiging van deze gegevens kan aanzienlijke gevolgen hebben, variërend van financiële verliezen tot reputatieschade. Daarom is het zo belangrijk dat organisaties een goed doordachte back-up-strategie implementeren en onderhouden.

Dit document heeft één doel: jou hierbij helpen. Stapsgewijs nemen we je mee naar het uitgangspunt van een back-up, de integratie van back-up binnen goed IT-beheer en het verkennen van verschillende back-up-oplossingen.

INHOUD

- Hoofdstuk 1: Begrijpen van back-ups.
 - Waarom is een back-up zo belangrijk?
 - Wat is een back-up-strategie?
- Hoofdstuk 2: Soorten back-up-oplossingen.
 - Onsite back-up.
 - Offsite back-up.
 - Back-up in de cloud.
 - Hybride back-up.
 - Immutable back-up.
 - Air-gapped back-up.
 - Archiefback-up.
- Hoofdstuk 3: De juiste strategie is maatwerk, hoe kies je die?
 - Back-up-selectie | wat.
 - Back-up-media | waarop.
 - Back-up-redundantie | waar.
 - Back-up-typen | hoe.
 - Back-up frequentie | hoe vaak.
 - Back-up-retentie | hoe ver terug.
 - Back-up-schema
- Hoofdstuk 4: Best practices, hoe wij het doen.
 - Wat vinden wij een goede back-up-methode.
 - Implementatie.
 - Beveiliging en toegang van back-ups.
 - Monitoring en periodieke controles.
 - Herstellen wanneer het mis gaat.
 - Back-ups en de toekomst.
- Conclusie.

Hoofdstuk 1: Begrijpen van back-ups

Een back-up is een reservekopie van gegevens die wordt bewaard op een gescheiden gegevensdrager, zoals een tape, NAS of opslag in de cloud. Deze kopieën worden preventief gemaakt om belangrijke gegevens veilig te stellen om, indien nodig, teruggezet te worden.

Een back-up is anders dan een bestandreplicatie, zoals het kopiëren van een bestand van een laptop naar OneDrive. Van back-ups zijn meerdere versies beschikbaar. Een replicatie is één enkele kopie.

Waarom is een back-up zo belangrijk?

Gegevens vormen de kern van een organisatie. Of het nu gaat om gevoelige bedrijfsgegevens, klantinformatie of projectdata, deze informatie is van grote waarde. Een back-up beschermt tegen verlies als we een document per ongeluk weggooien, als een laptop of server stuk gaat, bij een cyberaanval of misschien zelfs een brand.

Wanneer er gegevens verloren gaan of beschadigd raken, kunnen ze vanaf de back-ups worden hersteld. Zie het als een soort verzekering.

Daarom zijn back-ups essentieel voor elk bedrijf. Met goede en recente kopieën van je bedrijfsgegevens beperk je mogelijke schade en verhoog je de cybersecurity van je onderneming.

Wat is een back-up-strategie?

Een back-up-strategie is een plan dat beschrijft hoe kopieën van alle bedrijfsgegevens worden ingericht. Van welke gegevens wil je hoe vaak op welke locatie en op welke media een kopie. Het beschrijft ook wat de maximale hersteltijd mag zijn en welke hoeveelheid dataverlies acceptabel is. Hier hoort ook een disaster recovery-plan bij. Daarin worden rampenscenario's beschreven.

Hoofdstuk 2: Soorten back-up-oplossingen



Onsite back-up

Met een on-site back-up bewaar je een kopie van bedrijfsgegevens lokaal, zoals op kantoor. De gegevens worden op een schijf op tape geplaatst niet ver van waar de originele gegevens staan. Omdat het makkelijk bereikbaar is kunnen gegevens snel worden teruggezetz, mocht dat nodig zijn.



Offsite back-up

Een offsite back-up is een back-up die op een andere plek staat dan waar de primaire data staat. Offsite kan in de cloud zijn maar ook op een andere vestiging, een naast gelegen pand of ergens anders bijvoorbeeld.



Back-up in de cloud

De meest gangbare reden om een back-up in de cloud te plaatsen is om een back-up ook ergens anders te hebben dan op kantoor of bedrijfslocatie. Een back-up in de cloud is het plaatsen van een kopie van je documenten en bestanden in de cloud. Niet te verwarren met een back-up van bestanden die al in de cloud staan.



Hybride back-up

Met een hybride back-up benadering combineer je lokale en cloudopslag. Voor deze oplossing kan bijvoorbeeld gekozen worden wanneer specifieke applicaties niet in de cloud kunnen of wanneer er problemen zijn met het internet.

**Immutable back-up**

Om je te beschermen tegen een ransomware-infectie kun je voor een immutable back-up kiezen. Dit houdt in dat je data voor een ingestelde periode 'op slot' zet. Je kan het niet veranderen en niet deleten. Het is onmogelijk om daar online bij te komen.

**Air-gapped back-up**

In het geval van air-gapped staat de back-up op een volledig geïsoleerd systeem. Zoals een kluis. Net als de immutable back-up is het onmogelijk om er online bij te komen.

**Archiefback-up**

Stel je hebt een juridische bewaartermijn of data die je niet per se direct voor handen hoeft te hebben. Deze data wil je niet meer op je actieve systemen opslaan, maar wel voor langere tijd bewaren. Het terugzetten van documenten en bestanden gaat minder snel, want minder urgent maar door bulksopslag goedkoper.

Hoofdstuk 3: De juiste strategie is maatwerk, hoe kies je die?

Door de verschillende media, typen en soorten back-up bij elkaar te voegen verstevig je je back-up-strategie. We lichten elk onderdeel toe dat hierin thuishoort zodat het duidelijk wordt welke keuzes het beste bij (de IT-inrichting van) je organisatie passen.

Back-up-selectie | wat

In de back-up-selectie bepaal je wat je gaat back-uppen. Aan de hand van een lijst van alle systemen en bedrijfsgegevens kun je gaan bepalen wat onmisbaar is en prioriteit moet krijgen bij herstel en wat minder. Sommige gegevens hebben wellicht helemaal geen back-up nodig, terwijl bedrijfskritische gegevens bij voorkeur continue beschikbaar moeten zijn.

Back-up-media | waarop

Bij back-up-media kan je denken aan een harddisk, tape of NAS, maar ook de cloud. Het type media kan helpen bij het bepalen van de locatie, maar heeft vaak te maken met de hoeveelheid data die opgeslagen moet worden. Bedenk dat de ruimte die een back-up nodig heeft meestal groeit in de loop van tijd. Dit is sterk afhankelijk van hoe vaak je een back-up wilt maken en hoe lang je ze wilt bewaren.

Back-up-redundantie | waar

Redundantie in back-ups verwijst naar het hebben van meerdere kopieën van gegevens op verschillende locaties, fysiek of in de cloud. Hiermee dek je het risico af van fouten of beschadigingen van een enkele kopie. Daarnaast biedt het hebben van kopieën op afgelegen locaties bescherming tegen grootschalige rampen, zoals brand of overstromingen.

Back-up-type | hoe

Het back-up-type verwijst naar de kenmerken en het doel van de back-up-gegevens zelf. Het beschrijft wat er wordt opgeslagen en hoe de gegevens worden bewaard. Dit zijn de drie back-up-types:

1

VOLLEDIGE BACK-UP

Bij een volledige back-up wordt een exacte kopie van alle geselecteerde gegevens gemaakt. Dit omvat alle bestanden en mappen, zonder uitzonderingen.

Hoewel volledige back-ups grondig zijn, nemen ze vaak veel opslagruimte in beslag en vereisen ze meer tijd om te maken.

2

INCREMENTELE BACK-UP

Incrementele back-ups richten zich alleen op gewijzigde gegevens sinds de laatste back-up. Dit bespaart opslagruimte en verkort de back-up-tijd.

Ze zijn efficiënt, maar vereisen dat je zowel de laatste volledige back-up als alle incrementele back-ups nodig hebt om gegevens te herstellen.

3

DIFFERENTIËLE BACK-UP

Net als een incrementele back-up, begint een differentiële back-up ook met een volledige back-up.

Hierna worden kopieën gemaakt van alles dat sinds de laatste volledige back-up is veranderd, dus niet zoals bij een incrementele back-up alleen de wijzigingen.

Hij is groter dan een incrementele back-up en kleiner dan een volledige.

Voor het maken van een back-up schema wordt er vaak een combinatie gemaakt van 1 en 2 of 1 en 3.

Back-up-frequentie | hoe vaak

Voor dit deel bepaal je hoe vaak je van een bepaalde bron een bepaald type back-up wilt maken. De hoeveelheid gegevensverlies is van invloed bij het bepalen van de frequentie van de back-up. Het verhogen van de frequentie zou kunnen helpen bij het verkleinen van het aantal uur aan werk dat mogelijk verloren gaat bij een incident.

Een hogere frequentie van de back-up is niet altijd mogelijk vanwege de tijd die het kost om de back-up te maken. Een gangbaar uitgangspunt is dan bijvoorbeeld om in het weekend een volledige back-up te draaien en dagelijks een incrementele.

Back-up-retentie | hoe ver terug

De zogenoemde retentie van een back-up geeft aan hoe ver je terug kan in de geschiedenis van een back-up. Dit kan belangrijk zijn wanneer je bijvoorbeeld een bestand terug wil zetten wat een half jaar geleden is verwijderd. Een back-up met een retentie van een maand biedt in dat geval geen oplossing.

Back-up-schema

Alle bovenstaande punten komt samen in een back-up-schema. Elk onderdeel dat je wilt back-uppen krijgt zo'n schema. In een back-up schema staat dus wat, hoe, waarop, waar, hoe vaak en hoe ver terug je wilt back-uppen.



Hoofdstuk 4: Best practices, hoe wij het doen

Een doordachte back-up-strategie en back-ups zijn pas effectief als ze naadloos worden geïntegreerd in IT-beheer. En laat dat nou een mooi deel van ons werk zijn.

Wij regelen de back-up-inrichting, stellen back-up-schema's in, zorgen voor de beveiliging van de back-ups, monitoren de back-up-processen en voeren herstelacties uit als dat nodig is.

Wat vinden wij een goede back-up-methode

Onderdeel van een goed doordachte back-up-strategie is de 3-2-1 methode. Hiermee bewaar je drie kopieën van je data op (minstens) twee verschillende media waarvan minimaal één off-site, op een andere locatie.

Eén stapje beter is de 3-2-1-1. Die laatste 1 staat in ons geval voor het toevoegen van een air-gapped- of immutable back-up-oplossing (zie hoofdstuk 2). Beide oplossingen werken als een kluis. Het is onmogelijk om er online bij te komen waardoor deze strategie ook geschikt is tegen cyberaanvallen zoals ransomware.



Om de strategie compleet te maken hanteren wij een standaard back-up en retentiebeleid. Hierin hebben we voor de systemen die we kunnen back-uppen vastgesteld hoe vaak we een back-up maken, welk type het meest geschikt is en hoe lang iets bewaard moet worden.

Back-ups implementeren

Zodra er een back-up-strategie is opgesteld, zal het moeten worden geïmplementeerd. Dit is de technische uitwerking van de inrichting. Wij zien het adviseren over de keuze van welke types hardware, software en bijvoorbeeld welke clouddienst het meest geschikt is als onderdeel van de implementatie. Ook de beveiliging nemen we hierin mee.

Beveiliging en toegang van back-ups

Net als alles binnen de IT moeten ook de back-ups beveiligd worden. Het is belangrijk om na te denken wie binnen je organisatie toegang mag hebben tot de back-ups, zowel fysiek als de back-up-software.



De manier van het beveiligen van alle onderdelen die worden ingezet bij de gekozen back-up-inrichting zijn -als het goed is - vastgelegd in de strategie. Dit nemen we tijdens de implementatie en de inrichting van de monitoring mee.

Monitoring en periodieke controles

Het werk is niet klaar na het maken van back-ups. Monitoring en herstelprocessen moeten worden ingericht. Monitoring helpt bij het identificeren van fouten in het back-up-proces, zoals mislukte back-ups of corrupte gegevens. Het biedt ook inzicht in de prestaties en maakt het mogelijk om processen te optimaliseren.

Veel van dit werk automatiseren we met de juiste back-up-software, maar periodieke controles op geautomatiseerde processen zullen nog wel uitgevoerd moeten worden. We kijken of selecties nog kloppen, wat er in quarantaine is gezet en of daar actie op moet worden ondernomen. Noem het proactieve monitoring.

Herstellen wanneer iets misgaat

Het opzetten van een herstelprocedure zorgt ervoor dat mensen weten wat er moet gebeuren wanneer er onverhoopt toch iets misgaat. Om zo ver niet te komen voeren we met regelmaat herstel oefeningen uit. Ook hierbij kan veel ondervangen worden met de juiste software maar zeker niet alles. Bij grotere problemen acteren we natuurlijk direct.



Back-ups en de toekomst

Wat recent een trend was, is nu al razendsnel in ontwikkeling. Zo zien we hoe bijvoorbeeld machine learning, de AI-techniek waarbij algoritmen kunnen leren van data en voorspellingen kunnen doen, al zeer succesvol is geïntegreerd in diverse monitoring- en beveiligingssoftware.

En niet voor niets want de huidige tijd van cyberdreigingen vraagt om constante beschermingsaanpassingen. Om die reden zien we ook dat de markt hier vol op inzet. Wij blijven onszelf in ieder geval op de hoogte houden van de nieuwste ontwikkelingen en hoe deze toegepast kunnen worden in een goed doordachte back-up-strategie.

Conclusie

Lang verhaal kort. We zetten nog even de stappen voor het opzetten, implementeren en onderhouden van een goed doordachte back-up-strategie op een rijtje. Deze vullen we aan met nog een aantal tips.

- Maak een lijst van alle systemen en bedrijfsgegevens. Classificeer alle gegevens zodat je precies weet wat kritiek is, dit helpt bij het prioriteren bij herstel.
- Bepaal wat de maximale hersteltijd mag zijn.
- Welke hoeveelheid dataverlies acceptabel is.
- Hoe vaak een back-up van welke gegevens gemaakt worden.
- Hoe de back-ups opgeslagen en waar ze bewaard worden.
- Hoe lang de retentie is.
- Verwerk de vergaarde informatie in back-up-schema's.
- Bepaal hoe de beveiliging moet worden geregeld.
- Leg vast wie, waar verantwoordelijk voor is.
- En waar het back-up-beheer uit bestaat. Maak ook afspraken over de frequentie van controles, tests en oefeningen.
- Zet al deze informatie in een document.

Het document dat hieruit voortkomt is de perfecte basis voor het opstellen van een disaster recovery-plan, waarin scenario's worden omschreven wat er bij een ramp moet gebeuren. En laat dat nou precies het thema zijn voor de volgende whitepaper.

Mocht je behoefte hebben aan een IT-partner die je kan helpen met het inrichten en uitwerken van een back-up-strategie of ondersteuning kan bieden bij het back-up-beheer, schroom niet om contact op te nemen. We zijn zeer benaderbaar.

088-990 40 00 | info@meos.nl

www.meos.nl



Wij houden van IT

MEOS is een no-nonsense IT-bedrijf.

Wij regelen dat computers het gewoon doen, altijd en overal, zonder zorgen.

Samen met onze klanten zorgen we voor stabiele, efficiënte en veilige IT-infrastructuren.

Het is ons streven om het beste IT-servicebedrijf van Nederland te zijn, en dat lukt al vrij aardig. We zijn altijd op zoek naar hoe iets beter kan, innovatiever en slimmer.

Daar hebben we een woord voor:

me·os.it (aka meositeren)

to improve *it*, to make *it* better.