HOE ZEKER WEET JIJ DAT HET HERSTEL VAN EEN BACKUP OOK ECHT WERKT?

Het belang van een Backup & Recovery-oplossing is bekend bij bedrijven en consumenten. Vrijwel elk bedrijf gebruikt een backup-oplossing die met regelmaat: elke week, dag of uur automatisch een backup maakt van alle digitale systemen en bedrijfsdata. Deze backup wordt extern op een fysieke en digitale plek opgeslagen, zodat bij een 'disaster': een cyberaanval of fysieke vernieling, zoals brand, de systemen en bedrijfsdata kunnen worden hersteld.

Wat zijn de gevolgen wanneer een systeem en bedrijfsdata niet kan worden hersteld?

Wat nog niet alle bedrijven beseffen is dat het kunnen herstellen van een disaster net zo belangrijk is als het maken van een backup. Een backup dient snel en juist te worden hersteld, zodat een bedrijf na een disaster direct verder kan werken. Ten slotte is een backup zonder het juiste herstel niets waard…

Hoe zeker weet jij dat de backup en het herstel ook echt werkt?

Met het gebruik van disaster recovery kun je op elk moment checken of het herstel van een backup ook echt werkt. Zo ben je voorbereid op een disaster en kun je de bedrijfscontinuïteit waarborgen, omdat je weet dat het herstel van een backup ook echt werkt. In dit whitepaper geven we 5 redenen om disaster recovery te activeren.

90% van bedrijven met dataverlies door een disaster gaan binnen twee jaar failliet.

Bron: Acronis

> **Werken de backups? Zorg dat je zeker bent van je zaak en bij een disaster direct kunt schakelen om weer up-and-running te krijgen. Test periodiek of een backup werkt op de uitwijkplek, dan ben jij ten alle tijden voorbereid op een disaster.**
>
> Stan Laurijssen, DSD Europe

5 x waarom disaster recovery activeren

Dataverlies kan komen door een natuurramp: een brand, storm of overstroming, een menselijk voorval: ransomeware-aanval of per ongeluk verwijderen of beschadigen van data en een software of hardware storing, wat kan resulteren in dataverlies. Een disaster kan elk bedrijf overkomen. De vraag is niet of maar wanneer u te maken krijgt met een disaster...

U moet voorbereid zijn op een disaster met een backup en de zekerheid dat de backup ook (snel) hersteld kan worden. Lees hieronder hoe disaster recovery hierbij helpt:

1. Een bedrijf zonder data heeft geen business

Een eindklant neemt een bedrijf in vertrouwen wanneer zij een aankoop doen of een samenwerking aangaan. Daarbij komt dat eindklanten een hogere beschikbaarheid verwachten van een bedrijf, nu we steeds maar richting een 24-uurseconomie gaan. Bij een langdurige downtime of veel dataverlies door een disaster, wordt het vertrouwen van de eindklant geschonden en loopt het bedrijf risico de klant aan de concurrent te verliezen. Het verlies aan business en bijkomende imagoschade kan uiteindelijk leiden tot faillissement.

Disaster recovery verlaagt RTO en RPO

Het vertrouwen terugwinnen van een klant na een disaster kost veel meer tijd, energie en geld dan dat je hebt geïnvesteerd in het opbouwen van een klantrelatie. Met disaster recovery is een bedrijf na een disaster vrijwel direct weer up-and-running, waardoor een eindklant geen last heeft van downtime, betrouwbaarheid van een bedrijf niet wordt geschonden en de klantrelatie behouden blijft.

Recovery Time Objective (RTO)

Hoe lang mag een bedrijf uit de lucht zijn na een disaster? Hoe lang kun je werken zonder IT systemen? En hoeveel business mis je, wanneer de systemen niet werken?

Recovery Point Objective (RPO)

Hoeveel dataverlies is acceptabel? Ben je relatief weinig werk kwijt wanneer een backup van één dag of langer geleden wordt gebruikt? Of is het al een ramp als je alle data van afgelopen uur kwijt bent?

2. Hoe langer een systeem plat ligt, hoe meer schade

Een veelvoorkomend disaster is een cyberaanval, waarbij cybercriminelen uit zijn op gevoelige bedrijfsdata. Hoe langer de bedrijfssystemen plat liggen, hoe meer tijd cybercriminelen hebben om gevoelige data van werknemers én eindklanten te stelen en misbruiken. Bedenk eens hoeveel schade er in een paar uur tijd kan worden aangericht bij jouw klant. En wat de gevolgen zijn voor een bedrijf, wanneer bedrijfs- en klantdata worden gelekt.

Vergelijk de kosten van disaster recovery met de kosten bij downtime:

Verlies van omzet	+	Verlies van productiviteit	+	Kosten voor herstel	+	Immateriële kosten	=	Downtime kosten (per uur)

Disaster recovery voorkomt verlies door beperken van (ongeplande) downtime

Een lange downtime kan veel schade aanrichten in de vorm van dataverlies, maar daarnaast ook inkomstenverlies. Gedurende de downtime heeft een bedrijf geen inkomsten, daarnaast kan de lange downtime veel kosten tot gevolg hebben en zorgt uiteindelijk het verlies van klanten ook voor verlies aan inkomsten op de langere termijn.

Met disaster recovery wordt de hersteltijd verkort en kunnen verliezen worden beperkt: niet alleen qua inkomsten, maar ook qua kosten voor mogelijke schade als gevolg van downtime en uitgaven om de dagelijkse bedrijfsfuncties weer te herstellen.

Disaster recovery minimaliseert onderbreking van kritieke processen

Een bedrijf kan ook te maken hebben met kritieke processen die altijd actief moeten zijn, omdat ze cruciaal zijn voor de bedrijfscontinuïteit. Door middel van disaster recovery worden mogelijke onderbrekingen geminimaliseerd en zijn kritieke processen na een disaster vrijwel direct weer actief.

3. Wettelijke aansprakelijkheid voorkomen

Een inconsistente database door dataverlies heeft voor elk bedrijf dat financiële data verwerkt, impact op de bedrijfscontinuïteit. Het missen van data leidt tot financieel verlies, doordat je geen volledige data kunt aanleveren bij bijvoorbeeld de belastingdienst of KvK. Je leidt niet alleen omzetverlies, maar ontvangt mogelijk ook boetes omdat je niet kunt voldoen aan je wettelijke rapportage verplichtingen.

43% van bedrijven zonder disaster recovery plan gaan failliet in de nasleep van een groot dataverlies.

Bron: Veritis

4. Voldoen aan de GDPR

Wekelijkse backups maken van bedrijfsdata is niet langer voldoende om te voldoen aan de GDPR. Zo staan er in artikel 32 de volgende twee oorwaarden:

1. Het vermogen om bij een fysiek of technisch incident de beschikbaarheid van en de toegang tot de persoonsgegevens tijdig te herstellen
2. Een procedure voor het op gezette tijdstippen testen, beoordelen en evalueren van de doeltreffendheid van de technische en organisatorische maatregelen ter beveiliging van de verwerking.

De GDPR vereist niet alleen een wekelijkse backup, maar ook dat data tijdig hersteld kan worden en dat bij een disaster de juiste stappen worden ondernomen. Personeel moet weten wie zij moeten benaderen bij een disaster en er moet een plan zijn om systemen en processen in de juiste volgorde te herstellen en data op de juiste locatie terug te plaatsen. Om te voldoen aan de GDPR heeft een bedrijf dus een disaster recovery plan nodig.

Voldoet een bedrijf niet aan de GDPR of leidt een bedrijf dataverlies van gevoelige data, zoals bank- en persoonsgegevens, dan heeft dit juridische gevolgen. Denk aan boetes, maar ook aan reputatieschade.

5. Vertrouw niet op het onwaarschijnlijke

Ondanks dat de technologie zich continu ontwikkelt en geavanceerder wordt kun je er niet vanuit gaan dat hardware en software 100% waterdicht is. Je kunt maatregelen treffen om hardware te beschermen met bijvoorbeeld koelsystemen en piekstroombeveiliging en software en personeel beschermen met security-oplossingen, maar dan nog is je data niet beveiligd tegen alle mogelijke disasters.

Een disaster kan veroorzaakt worden door verschillende aspecten: de natuur, technologie en mensen. Hoewel sommige disasters onwaarschijnlijk lijken is het van cruciaal belang dat een bedrijf is voorbereid op alle soorten disasters, zodat ook bij zeldzame gevallen de dagelijkse bedrijfsfuncties snel hersteld kunnen worden.

Bereid je voor op een disaster door failovers te testen

Zorg ervoor dat u voorbereid bent op een disaster door periodiek te testen of de backup ook daadwerkelijk werkt op de uitwijklocatie. Zo biedt de Disaster Recovery tool van Acronis de mogelijkheid om de backup te testen door deze te starten in de Acronis managed cloud recovery site.

Zorg er daarnaast voor dat u een Disaster Recovery Scenarios-plan hebben liggen, zodat elke partij weet welke handelingen, wanneer moeten worden verricht ten tijden van een disaster. Test ook dit plan periodiek!

> **Als 2020 ons iets heeft geleerd, dan is het wel dat bedrijfsomgevingen kunnen veranderen. Bedrijven worden voortdurend geconfronteerd met nieuwe problemen - een mobiele wereld met een groeiend aantal remote endpoint devices, toenemende ransomware en de noodzaak om kritische data zo snel mogelijk te herstellen om een bedrijf draaiende te houden.**
>
> Mathijs Theunissen, Acronis

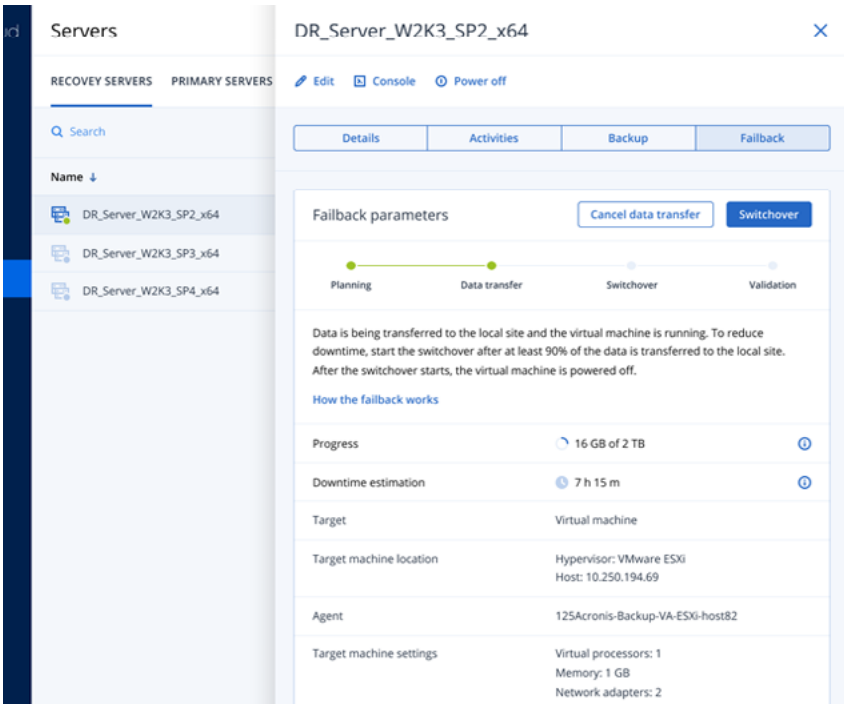
Acronis (Advanced) Disaster Recovery

Acronis Cyber Protect Cloud is een uitgebreide backup & recovery oplossing, die tevens cybersecurity gebruikt om endpoints, systemen en data te beschermen tegen disasters. Onderdeel van Cyber Protect Cloud is Disaster Recovery, waarmee je onder andere een failover kan testen in de Acronis Cloud omgeving, zodat je zeker bent dat een backup ook daadwerkelijk werkt.

Kunt u geen downtime permitteren?

Tevens biedt Acronis een advanced-versie van Disaster Recovery als add-on op Acronis Cyber Protect Cloud. Met deze add-on kun je niet alleen een failover en failback testen, maar kun je binnen enkele minuten verder werken door de IT-systemen over te zetten op virtuele machines in de Acronis Cloud omgeving.

Met Acronis disaster recovery technologie garanderen zij een RPO en RTO onder de 15 minuten, ongeacht de soort disaster: een natuurramp, cyberaanval of een menselijke fout.



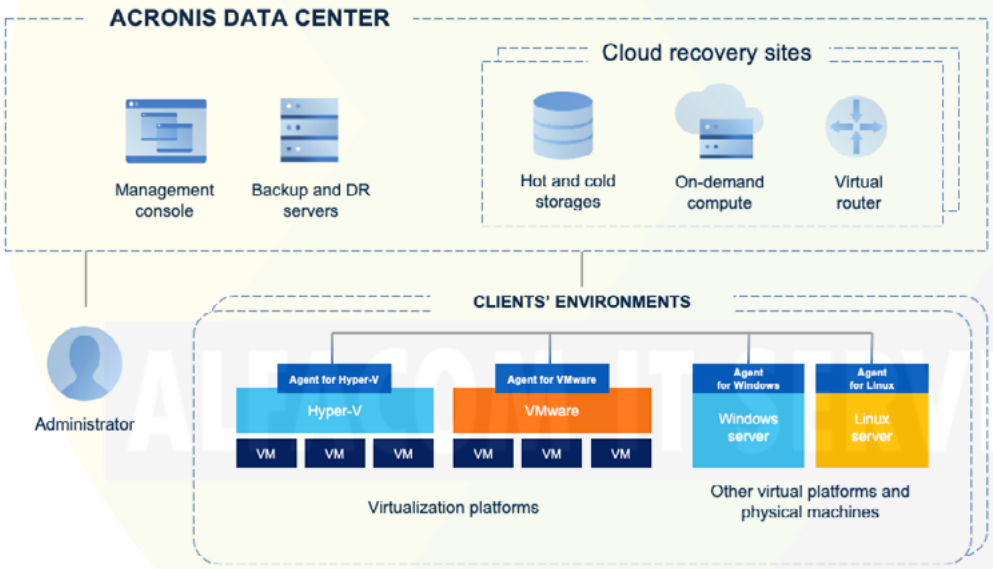
Automatiseer disaster recovery voor belangrijke processen

Met Advanced Disaster Recovery is het mogelijk om 'key disaster recovery scenarios' te automatiseren met runbooks - instructies hoe de bedrijfsprocessen van je klanten in de cloud moeten worden opgestart. Zo zorg je ervoor dat belangrijke systemen en applicaties automatisch en in de juiste volgorde worden hersteld, zodat kritieke bedrijfsprocessen bij een disaster binnen no time weer zijn opgestart.

Waarom wij Acronis Disaster Recovery aanbieden?

Minder downtime en betere security

Met Advanced Disaster Recovery garanderen wij bedrijfscontinuïteit voor onze klanten. In welke omgevingen zij ook werken: fysiek, virtueel, on-premise of in de cloud. Bij een disaster beperk je de downtime naar enkele minuten, omdat zij binnen enkele minuten verder kunnen werken met hun IT-systemen in de
Acronis Cloud omgeving.



Alles in één beheerplatform

Acronis gebruikt één beheerplatform voor backup, recovery, security én disaster recovery. Alle beheerfuncties bevinden zich in dezelfde omgeving, zo kun je eenvoudig serverlijsten configureren, connectiviteitsinstellingen testen, disaster recovery runbooks configureren én herstellen op meerdere netwerken. Dat allemaal zonder te hoeven schakelen tussen meerdere beheersomgevingen.

Met Acronis Cyber Protect Cloud kunnen wij onze klanten een complete cybersecurity, backup en recovery service bieden, welke wij volledig kunnen implementeren, beheren en monitoren vanuit één beheerplatform.

Wat kunnen wij

Een complete backup- en security service, aangepast op de wensen van onze klanten.

Meer weten over Acronis Disaster Recovery?

Neem contact op dan beantwoord wij al uw vragen.

+31 (0)10 413 05 03

info@alfacom.nl

Onze Cloud partner DSD Europe biedt een uniek platform voor digitale distributie van cloud services en software, voor inmiddels meer dan 5.500 MSP's en IT- resellers in Europa.

Opzoek naar een Office365 disaster recovery klik **Acronis Office365 Recovery**