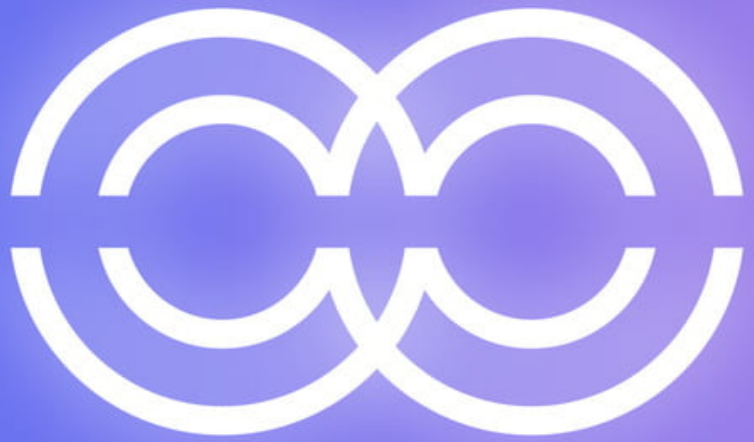
EKCO



# Disaster Recovery

# 01
# Het belang van disaster recovery

## Het belang van disaster recovery

In een steeds digitaler wordende wereld zijn bescherming van data en beschikbaarheid cruciaal. Bedrijven worden steeds afhankelijker van IT en daardoor kan een korte onderbreking al grote gevolgen hebben.

Storingen kunnen een infrastructurele oorzaak hebben (zoals uitval van hardware, stroom of brand), maar veel vaker is een onderbreking het gevolg van cyberaanvallen (zoals ransomware en hacks) of gewoonweg het gevolg van een menselijke fout.

## De oorzaken en kosten van dataverlies

Moderne bedrijven kunnen zich niet veroorloven om data te verliezen. Wat de oorzaak ook is, dataverlies is kostbaar en risicovol. De verwachting is dat dataverlies én de kosten ervan elk jaar toenemen.

Een Disaster Recovery oplossing die uptime garandeert, dataverlies minimaliseert en productiviteit maximaliseert bij elke compromitterende situatie, vormt een broodnodige digitale verzekering voor ieder bedrijf. Want het is niet langer de vraag of een ramp jou overkomt, maar wanneer.

# 02
# Disaster recovery

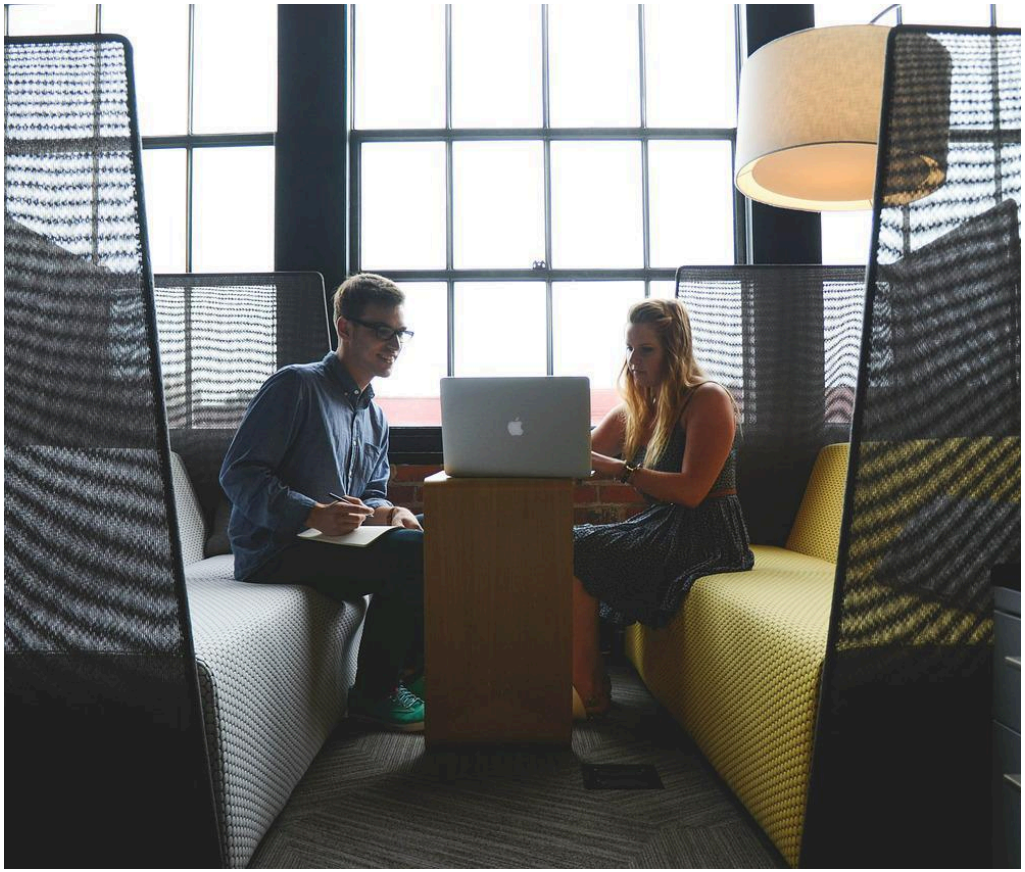
het concept

## Wat is Disaster Recovery eigenlijk?

Letterlijk betekent het: herstel na een ramp, ofwel de tijd en het werk die nodig zijn om systemen weer up & running te krijgen na dataverlies of downtime. Disaster Recovery draait niet alleen om de tijd dat systemen en medewerkers niet kunnen werken, het gaat ook om de hoeveelheid data die verloren is gegaan als een bedrijf moet terugvallen op een vorige versie van haar data.

Organisaties zouden zichzelf moeten afvragen hoeveel een uur downtime kost. En vooral: is het mogelijk om het werk dat medewerkers en systemen de afgelopen uren hebben gedaan te reproduceren? 95% van alle bedrijven kunnen deze vraag niet beantwoorden...

Om jouw IT omgeving tegen alle scenario's te beschermen, biedt Ekco Disaster Recovery oplossingen aan. Met deze diensten kun je jouw infrastructuur, applicaties en data beschermen door ze op een andere locatie op te slaan.



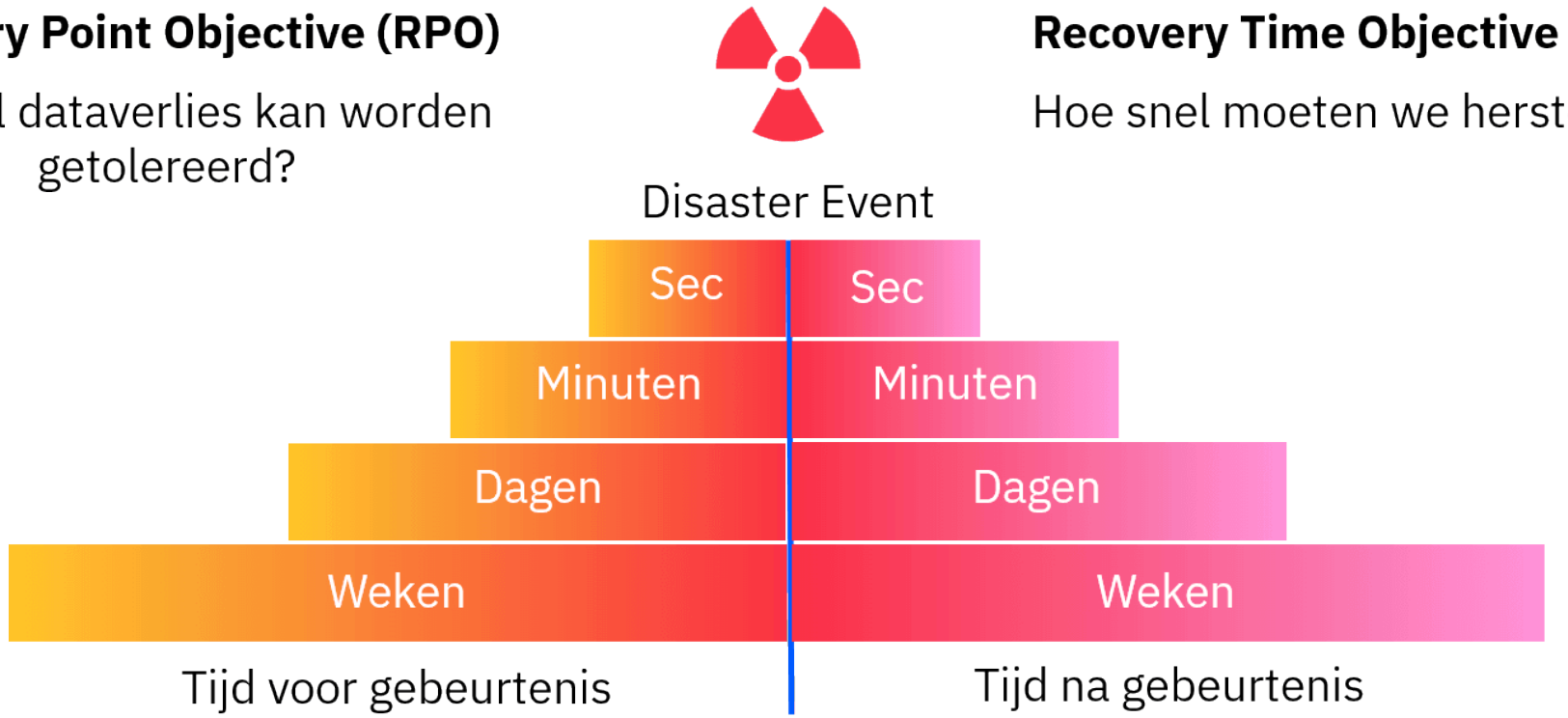
Een backup zonder oplossing voor Disaster Recovery is bij incidenten een leeg concept voor het herstellen van bestanden, software en functionaliteit. Dit heeft meestal meer om het lijf dan alleen het herstellen van data naar het oorspronkelijke systeem. Als een server down gaat, moet deze opnieuw worden geïnstalleerd, geconfigureerd en misschien zelfs vervangen. Dat maakt een backup geen echte DR-oplossing. Met alleen een backup moeten VM’s compleet opnieuw opgebouwd worden, omdat er geen automatisch herstel is ingebouwd in het backupproces.

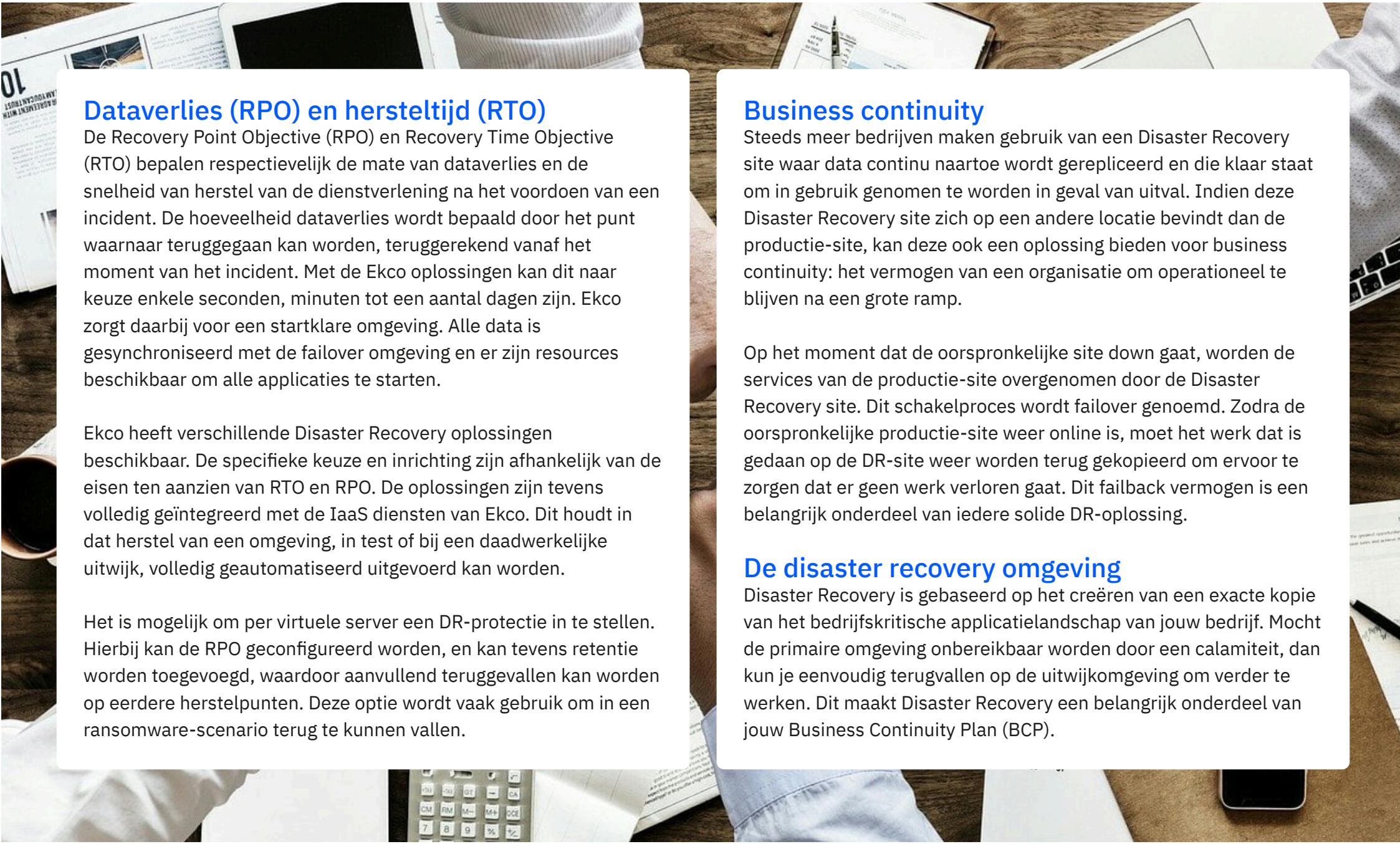
**Recovery Point Objective (RPO)**

Hoeveel dataverlies kan worden getolereerd?

**Recovery Time Objective (RTO)**

Hoe snel moeten we herstellen?





## Dataverlies (RPO) en hersteltijd (RTO)

De Recovery Point Objective (RPO) en Recovery Time Objective (RTO) bepalen respectievelijk de mate van dataverlies en de snelheid van herstel van de dienstverlening na het voordoen van een incident. De hoeveelheid dataverlies wordt bepaald door het punt waarnaar teruggegaan kan worden, teruggerekend vanaf het moment van het incident. Met de Ekco oplossingen kan dit naar keuze enkele seconden, minuten tot een aantal dagen zijn. Ekco zorgt daarbij voor een startklare omgeving. Alle data is gesynchroniseerd met de failover omgeving en er zijn resources beschikbaar om alle applicaties te starten.

Ekco heeft verschillende Disaster Recovery oplossingen beschikbaar. De specifieke keuze en inrichting zijn afhankelijk van de eisen ten aanzien van RTO en RPO. De oplossingen zijn tevens volledig geïntegreerd met de IaaS diensten van Ekco. Dit houdt in dat herstel van een omgeving, in test of bij een daadwerkelijke uitwijk, volledig geautomatiseerd uitgevoerd kan worden.

Het is mogelijk om per virtuele server een DR-protectie in te stellen. Hierbij kan de RPO geconfigureerd worden, en kan tevens retentie worden toegevoegd, waardoor aanvullend teruggevallen kan worden op eerdere herstelpunten. Deze optie wordt vaak gebruik om in een ransomware-scenario terug te kunnen vallen.

## Business continuity

Steeds meer bedrijven maken gebruik van een Disaster Recovery site waar data continu naartoe wordt gerepliceerd en die klaar staat om in gebruik genomen te worden in geval van uitval. Indien deze Disaster Recovery site zich op een andere locatie bevindt dan de productie-site, kan deze ook een oplossing bieden voor business continuity: het vermogen van een organisatie om operationeel te blijven na een grote ramp.

Op het moment dat de oorspronkelijke site down gaat, worden de services van de productie-site overgenomen door de Disaster Recovery site. Dit schakelproces wordt failover genoemd. Zodra de oorspronkelijke productie-site weer online is, moet het werk dat is gedaan op de DR-site weer worden terug gekopieerd om ervoor te zorgen dat er geen werk verloren gaat. Dit failback vermogen is een belangrijk onderdeel van iedere solide DR-oplossing.

## De disaster recovery omgeving

Disaster Recovery is gebaseerd op het creëren van een exacte kopie van het bedrijfskritische applicatielandschap van jouw bedrijf. Mocht de primaire omgeving onbereikbaar worden door een calamiteit, dan kun je eenvoudig terugvallen op de uitwijkomgeving om verder te werken. Dit maakt Disaster Recovery een belangrijk onderdeel van jouw Business Continuity Plan (BCP).

# 03
# Disaster recovery

## Waarom is disaster recovery essentieel?

# Waarom is disaster recovery essentieel?

Een ramp kan elk bedrijf overkomen. De vraag is niet of, maar wanneer je te maken krijgt met een disaster. Je 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

Eindklanten eisen een steeds hogere beschikbaarheid van een bedrijf, nu we steeds meer richting een 24-uurs economie gaan. Bij een langdurige downtime of veel dataverlies door een disaster, wordt het vertrouwen van de eindklant geschonden en loopt het bedrijf risico. 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.

# 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 te 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.

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. Daarnaast zorgt het verlies van ontevreden klanten ook voor verlies aan inkomsten op de langere termijn. Met Disaster Recovery wordt de hersteltijd verkort en kunnen verliezen worden beperkt.

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. Jouw bedrijf leidt niet alleen omzetverlies, maar ontvangt mogelijk ook boetes omdat er niet voldaan kan worden aan de wettelijke rapportage verplichtingen.

## 4

### Voldoen aan de AVG

Wekelijks backups maken van bedrijfsdata is niet langer voldoende om te voldoen aan de AVG. De AVG 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

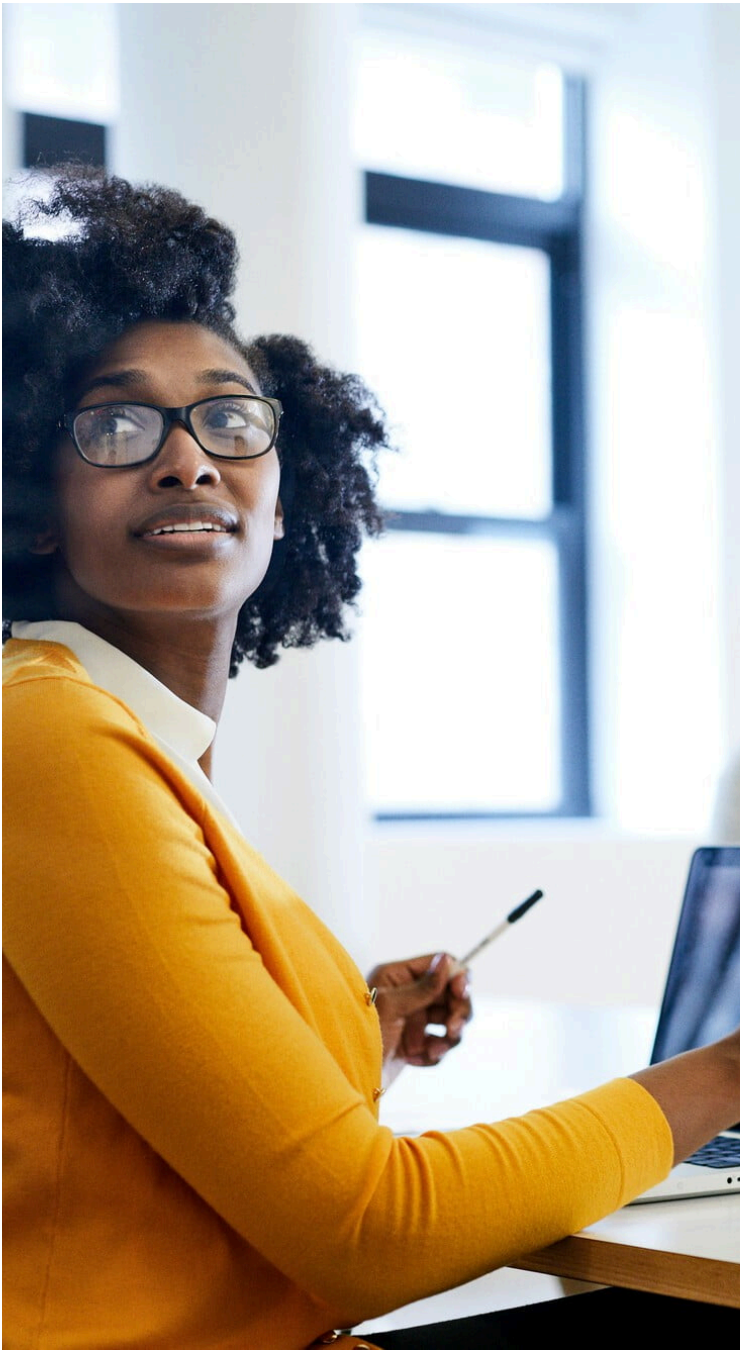
## Vertrouw niet op het onwaarschijnlijke

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 securityoplossingen, 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.

# 04
# Disaster recovery oplossing

Welke disaster recovery oplossing past het beste?



## Welke disaster recovery oplossing past het beste?

Met Disaster Recovery borg je de continuïteit van jouw organisatie in geval van een calamiteit. Doordat er een kopie van jouw complete virtuele omgeving (data, systemen, netwerken en applicaties) wordt opgeslagen op een andere locatie, ben je binnen no-time weer online zonder dat er bedrijfsgegevens verloren gaan.

Ekco adviseert bij een implementatie welke oplossing het beste past, afhankelijk van de RPO en RTO eisen, of wanneer er sprake is van een verschil in virtualisatietechniek tussen bron- en uitwijkplatform.

De Disaster Recovery dienst van Ekco kan in meerdere scenario's worden toegepast: de meest gebruikte is waarbij zowel de bron-, als ook de failover omgeving zijn ondergebracht bij Ekco. Een ander veel gebruikt scenario is een uitwijk vanaf een kantoorlocatie naar het Ekco Disaster Recovery platform. Dit biedt de mogelijkheid voor Disaster Recovery zonder grote investeringen in eigen hardware. Ekco maakt hierbij gebruik van hoogwaardige datacenters in Nederland.

Ontdek de mogelijkheden van Disaster Recovery oplossingen van Ekco en kies voor continuïteit, veiligheid en zekerheid.

# Het begint allemaal met een gesprek...

Kom vandaag nog in contact met ons team.

sales@ek.co
www.ek.co
NL: +31 85 822 7900
IE: +353 1 699 4540
UK: +44 (0) 330 135 8792