

DIGITALE TRANSFORMATIE

Back-up en veerkracht

Back-up en veerkracht



Als je eenmaal vertrouwd bent met de verschillende interne en cloudproducten en -services die eerder zijn besproken, is het essentieel om te bepalen hoe je die gegevens gaat beschermen in het geval van een ramp of een ander incident dat je gegevens in gevaar brengt. Het bouwen van een veerkrachtig bedrijf begint bij je informatiesystemen.

Back-ups moeten worden beschouwd als onderdeel van je algemene cyberbeveiligings- en veerkrachtstrategie. Te vaak denken bedrijven niet genoeg na over robuuste gegevensbescherming door middel van back-ups, terwijl back-ups de meest fundamentele manier zijn waarop bedrijven hun informatiesystemen en gegevens kunnen beschermen.

Bij een ramp is je laatste verdedigingslinie je back-up! Of dat nu gebeurt door een natuurramp zoals een orkaan of een vulkaanuitbarsting of door een menselijk incident waarbij je gegevens in gevaar komen of op een andere manier ontoegankelijk worden, je back-up voorziet je van nature van een losstaande kopie van je gegevens die je kunt gebruiken om je activiteiten opnieuw op te starten.

Dit wordt steeds belangrijker nu de wereld evolueert naar een meer mobiel of thuiswerktijdperk, wat betekent dat bedrijven cloudapplicaties inzetten voor productiviteit en bedrijfsprocessen.

Cloudgebaseerde software as-a-service-producten worden meestal over het hoofd gezien, omdat ze vaak op streng beveiligde locaties draaien en niet onderhevig zijn aan de natuurlijke risico's die we meestal in het Caribisch gebied hebben. Dit is niet het geval, zoals de volgende grafiek van Microsoft laat zien:

Back-up en veerkracht

	Verantwoordelijkheid	SaaS	PaaS	IaaS	Op locatie
De verantwoordelijkheid blijft altijd bij de klant	Informatie en gegevens	Microsoft	Klant	Klant	Klant
	Apparaten (mobiel en pc's)	Microsoft	Klant	Klant	Klant
	Accounts en identiteiten	Microsoft	Klant	Klant	Klant
De verantwoordelijkheid verschilt per type	Infrastructuur voor identiteit en directory	Gedeelde	Gedeelde	Klant	Klant
	Toepassingen	Microsoft	Gedeelde	Klant	Klant
	Netwerkbesturing	Microsoft	Gedeelde	Klant	Klant
	Besturingssysteem	Microsoft	Klant	Klant	Klant
Verantwoordelijkheid gaat over naar cloudprovider	Fysieke hosts	Microsoft	Klant	Klant	Klant
	Fysiek netwerk	Microsoft	Klant	Klant	Klant
	Fysiek datacenter	Microsoft	Klant	Klant	Klant

	Microsoft		Klant		Gedeelde
---	-----------	---	-------	---	----------

Bron: [Microsoft](#)

Gegevens, apparaten (pc's en smartphones) en accounts zijn volledig je verantwoordelijkheid. Bij gegevens betekent dit ook dat het je verantwoordelijkheid is om ervoor te zorgen dat de gegevens beschermd zijn tegen verlies.

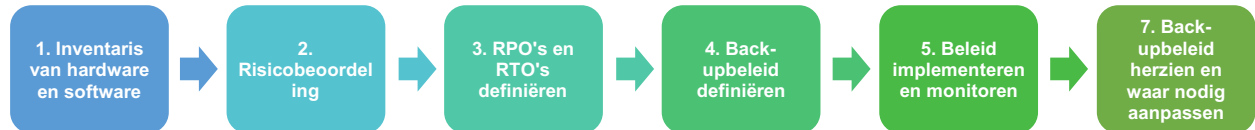
Voor gegevens die lokaal worden opgeslagen, wordt de volgende regel als beste praktijk beschouwd:

De 3-2-1 regel:

Drie kopieën van gegevens moeten worden opgeslagen op **twee** soorten media, waarvan ten minste **één** op een externe locatie.

Praat met je IT-specialisten op locatie die je kunnen voorzien van de hardware en expertise die nodig is om een veilige back-up te maken van je gegevens.

Back-up en veerkracht



Volg de bovenstaande stappen om een veerkrachtig back-upplan op te stellen en te implementeren.

1. **Inventaris** de computers en andere apparaten die op het netwerk zijn aangesloten (printers, schijven, routers, enz.). Inventariseer alle gebruikte software, zoals Office, Photoshop, Quickbooks, enz. of andere software die wordt gebruikt bij de activiteiten van je bedrijf. Noteer de leverancier, de aankoopdatum, de einddatum van de garantie, de kosten en de verwachte levensduur.
2. Voer een **risicobeoordeling** uit met behulp van het sjabloon in de bronnensectie op deze site. De beoordeling zal bepalen welke delen van de IT het meest kwetsbaar zijn en dus het belangrijkste om een back-up voor veerkracht te maken.
3. **Definieer de doelen voor herstelpunten en voor hersteltijd** (zie kader Definities). Denk eraan dat kortere doelen complexer en duurder zijn om te implementeren!
4. **Stel je back-upbeleid op**, met het sjabloon in de bronnensectie op deze site als uitgangspunt.
5. **Implementeer je back-upstrategie** volgens je gedefinieerde beleid. Aarzel niet om een plaatselijke expert in te schakelen om je te helpen dit zo goed mogelijk op te zetten. Controleer regelmatig je back-ups om er zeker van te zijn dat ze correct worden uitgevoerd.
6. Voer **elke 6 maanden een herziening uit** van je back-upbeleid of als je een grote wijziging aanbrengt in de software of hardware die in het bedrijf wordt gebruikt. Als je bijvoorbeeld van boekhoudsoftware verandert, moet je je beleid herzien als onderdeel van de kansprocedure voor software om ervoor te zorgen dat je back-ups veerkracht bieden.

Gebruik het meegeleverde sjabloon voor het back-upplan voor gegevens in de bronnen om je plan te ontwikkelen. Aangepast van [deze site](#) die verdere instructies bevat.

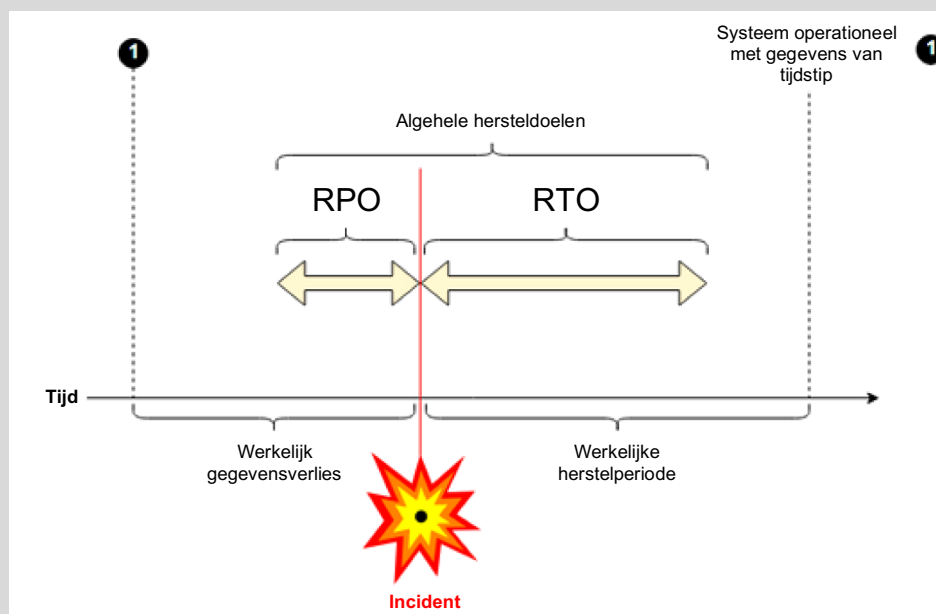
Back-up en veerkracht

BOX 1: Definities

Back-upbeleid: De procedures en regels om ervoor te zorgen dat bedrijfsgegevens voldoende worden gback-upt en beveiligd. Dit definieert het type back-ups, de frequentie en de toegang tot de back-upgeschiedenis in geval van een ramp.

Herstelpuntdoelstelling (RPO): De RPO is het maximaal aanvaardbare punt waarop gegevens verloren mogen gaan. Als er bijvoorbeeld gegevens van één dag verloren kunnen gaan, maar niet van twee dagen, dan moet de RPO worden ingesteld op één dag.

Hersteltijddoelstelling (RTO): De RTO is de maximale tijd die acceptabel is om het herstelproces uit te voeren om ervoor te zorgen dat het bedrijf operationeel is na een ramp.



Bron: [Wikipedia](#)

Incrementele back-up: Dit back-uptype bevat alleen de bestanden die sinds de meest recente incrementele of volledige back-up zijn gewijzigd. Deze biedt snellere back-ups, maar kan meer tijd nodig hebben bij een herstelbewerking.

Volledige back-up: Een enkele back-up die alle gegevens bevat die voor back-up zijn geselecteerd.

Differentiële back-up: Een cumulatieve back-up van gewijzigde gegevens sinds de laatste volledige back-up. Wordt gebruikt voor snellere back-ups, maar het kan langer duren om de gegevens volledig te herstellen.