

Back-up en recovery beleid

Back-up en recovery beleid

2021

Eveline Mosterd
Nick Henriët

Ebbehout 31
1507 EA Zaandam

Eveline.mosterd@odnzk.nl

www.odnzk.nl

...

Inleiding

Een goed back-up en recovery proces zorgt ervoor dat na een incident/calamiteit de juiste informatie/gegevens teruggeplaatst kunnen worden binnen de afgesproken tijdsduur en het datapunt waardoor er zin mogelijk informatie/gegevens verloren gaan, waardoor de normale werkzaamheden weer hervat kunnen worden. Een goed back-up en recovery proces is ook een zeer belangrijke maatregel tegen ransomware.

Back-up en recovery is een belangrijke beschikbaarheids- en continuïteit maatregel die ervoor zorgt dat corrupte, verloren of vernietigde bedrijfsinformatie hersteld kan worden. Alle informatie/gegevens dienen meegenomen in de back-up. Back-up en recovery is essentieel bij calamiteiten en uitwijk.

Doelstelling is het herstellen van gegevens en/of programmatuur bij verlies of beschadiging door bijvoorbeeld:

- Fouten in software;
- Menselijke fouten, zoals bedienfouten (bewust en onbewust);
- Corruptie van data of programmatuur;
- Herstellen van dienst in geval incident of calamiteit. Bijvoorbeeld bij een brand of een crash.

1 Back-up en recovery beleid

Ten behoeve van de beveiliging van de informatie is er back-up en recovery beleid voor alle voorzieningen van de OD NZKG. Het doel van dit beleid is te voorkomen dat in geval van gedeeltelijk of geheel verlies of beschadiging van data en/of programmatuur de dienstverlening van de OD NZKG hier hinder van ondervindt.

De OD NZKG hanteert de volgende beleidsuitgangspunten. De beleidsuitgangspunten zijn ontleend aan de Baseline Informatiebeveiliging Overheid (BIO) en aanvullend op het strategisch informatiebeleid van de OD NZKG.

Artikel 1: Uitgangspunten

1. In opdracht van de eigenaar van de data maakt de systeembeheerder reservekopieën van alle essentiële bedrijfsgegevens, programmatuur en het systeem (bijvoorbeeld de AD) die op lokale servers en cloud locaties staan, zodat de continuïteit van gegevensverwerking kan worden gegarandeerd.
2. De omvang en frequentie van de back-ups is in overeenstemming met het belang van de data voor de continuïteit van de dienstverlening en de interne bedrijfsvoering.
3. Dit back-up- en recovery beleid heeft betrekking op de servers, die wel en niet onder beheer staan van de OD NZKG. Ook is dit beleid van toepassing op data die in de cloud staan wel of niet beheerd door de OD NZKG.
4. De OD NZKG gebruikt de back-up en recovery om de gevolgen van de uitval en/of het verlies van informatie te minimaliseren. Dit kan worden bereikt met behulp van een combinatie van kopieën, incrementele back-ups, differentiële back-ups en transactielogboeken en systeem baselines.
5. Alle informatie/gegevens van de OD NZKG moet op een dusdanige wijze door de OD NZKG dan wel de leverancier worden opgeslagen dat een back-up maken mogelijk is.
6. De back-uplocatie is gescheiden van de omgeving waar de data vandaan komt.
7. Er is back-up documentatie aanwezig. Deze documenten bevatten de identificatie van alle belangrijke gegevens, programma's, documentatie en support items die nodig zijn om essentiële taken tijdens een herstelperiode uit te voeren. Documentatie van het recoveryproces bevat procedures voor het herstel van single-systeem of applicatiestoringen, alsmede voor een totale datacenter ramp.
8. Er zijn geteste ICT-procedures voor back-up en recovery.
9. Het testen/simuleren van grootschalige recovery acties dienen jaarlijks worden uitgevoerd middels het Business Continuity Management (BCM) proces.
10. De back-up data worden vernietigd in overeenstemming met het beleid omtrent behandeling van digitale media van de OD NZKG.

Artikel 2 Verantwoordelijkheid

Het team Proces en Informatie (P&I) is belast met het uitvoeren van dit beleid. Het team P&I wordt daarbij ondersteund door de ICT-dienstverleners.

Artikel 3: Dataverlies en hersteltijd (BBN 2)

1. Het maximale dataverlies is vastgesteld op 28 uur.
2. De maximale hersteltijd is vastgesteld op 16 werkuren bij (minimaal) 85% van de incidenten.

Artikel: Dataverlies en hersteltijd (BBN2+)

1. Het maximale dataverlies is vastgesteld op 24 uur.
2. De maximale hersteltijd is vastgesteld op max 4 tot 8 uur (minimaal) 85% van de incidenten.

Artikel 4: Frequentie van de back-up

1. De backs-ups op BBN 2 en BBN2+ niveau dient voor de OD NZKG en zijn leveranciers minimaal 1 jaar aan informatie/gegevens te bevatten.
2. De leveranciers dient aan te tonen dat de back-up op basis van een cyclus wordt gemaakt.
3. De OD NZKG hanteert een back-up cyclus en bewaartermijn volgens het onderstaande schema.

Back-up frequentie	Bewaartermijn back-up
Dagback-up	Week
Week back-up	Maand
Vier-wekelijks back-up (maand)	Kwartaal
Kwartaal back-up	Jaar
Jaar back-up	3 jaar

Artikel 5: Locatie van de back-ups

1. Het back-upproces voorziet in opslag van de back-up op een locatie, waarbij een incident op de ene locatie niet kan leiden tot schade op de andere.
2. Minstens drie versies van een back-up moeten worden bewaard, op tenminste twee verschillende opslagmedia.
3. Een back-up dient op een opslagmedium geplaatst te worden, die in een brandwerende kluis bewaard kan worden.

Artikel 6: Recovery

1. Voor grootschalige recovery acties van het systeem of de informatie/ gegevens is toestemming nodig van de systeemeigenaar of indien deze niet benoemd of aanwezig is, de directeur Bedrijfsvoering. Voor gerichte individuele verzoeken bijvoorbeeld om document of email terug te halen dient de Servicemanager te worden geïnformeerd.
2. Bij grote calamiteiten (ransomware of corrupte database) is altijd overleg nodig met de systeemeigenaar of indien deze niet is benoemd of niet aanwezig, is de directeur Bedrijfsvoering. De systeemeigenaar of de directeur Bedrijfsvoering bepaalt en de ICT-beheerder heeft een adviserende/uitvoerende rol.

Artikel 7: Logging

Van back-up en recovery activiteiten en de verblijfplaats van de media wordt een logboek bijgehouden.

Artikel 8: Controle

1. De back-ups worden dagelijks gecontroleerd.
2. Met vaste regelmaat (tenminste 1 x per jaar) wordt de back-upprocedure en herstelprocedures getest om de betrouwbaarheid ervan vast te stellen. Van deze test wordt een verslag gemaakt.
3. De back-up en recovery procedures moeten worden getest conform de documentatie en deze moet regelmatig worden bijgewerkt om rekening te houden met nieuwe technologie, veranderingen in het bedrijf, en de migratie van applicaties naar alternatieve platforms.

Artikel 9: Encryptie

Alle back-ups moeten worden encrypt. De data wordt hiermee versleutelt.

Het uitlezen, oftewel de decryptie van de data gaat alleen met behulp van de encryptie-sleutel, waardoor de data alleen voor de eigenaar van de data toegankelijk is.