/// Beleid rond back-ups en recovery

1 INTRODUCTIE

'Back-up en recovery' is een belangrijke beschikbaarheidsmaatregel die ervoor zorgt dat corrupte, verloren of vernietigde bedrijfsinformatie hersteld kan worden. Hierdoor kan er bij een incident of calamiteit snel geschakeld worden en wordt de continuïteit van de dienstverlening naar de medewerkers en burgers van uw lokaal bestuur beter gewaarborgd.

Back-ups en recovery worden niet enkel gedaan om de impact van potentiële cyberincidenten te minimalisere, maar ook om de impact van fouten in software, menselijke vergissingen of corruptie van data te verkleinen.

Gezien het belang van back-ups en recovery (vaak het laatste redmiddel in noodsituaties) dient niet alleen bedrijfsinformatie meegenomen te worden in een back-up, maar ook systeeminstellingen, zoals bijvoorbeeld Active Directory. Voor systeeminstellingen, applicaties en databases kunnen andere back-up mechanismen nodig zijn dan voor de gebruikelijke (bestands) back-ups. Een goede back-up in een passend schema en format, zorgt ervoor dat een recovery ook daadwerkelijk succesvol kan zijn.

Een beleid rond het beheer van back-ups en recovery is essentieel omdat het duidelijke kaders zet en medewerkers instructies biedt om met de verschillende soorten back-ups aan de slag te gaan. Om een succesvol beleid te implementeren is het belangrijk dat het toezicht van dit beleid wordt toegewezen aan een beleidsmedewerker. Deze persoon heeft de verantwoordelijkheid en de bevoegdheid om de toepassing en naleving van het beleid op te volgen en te rapporteren.

2 WET- EN REGELGEVING

Het kan noodzakelijk zijn om een back-up te maken van belangrijke systemen en bestanden om te kunnen voldoen aan Vlaamse en federale wetgeving. Vlaamse lokale besturen zijn verplicht om na een noodgeval de kritische dienstverlening en eventueel andere belangrijke systemen zo snel mogelijk operationeel te hebben, al dan niet op een alternatieve locatie.

Verder zit er op bepaalde soorten data een wettelijke verplichtte bewaartermijn. Denk hierbij aan bijv. de financiële informatie van een lokaal bestuur of de administratie van het departement burgerzaken. Afhankelijk van de bewaartermijn moeten lokalen besturen ervoor zorgen dat zij deze informatie veilig bewaren op een back-up medium.

Bij het maken van back-ups houdt u het best ook de algemene verordening persoonsgegevens (AVG) in de gaten. Met het back-uppen van systemen en bestanden worden vaak ook persoonsgegevens geback-upt, waardoor uw

back-ups onder de AVG-wetgeving vallen. Dit houdt in dat u in bepaalde gevallen verplicht bent om iemands gegevens te verwijderen als deze persoon hierom vraagt. Bijvoorbeeld als de gegevens niet meer nodig zijn of op het moment dat er geen wettelijke basis meer is om iemands gegevens te bewaren (bijv. intrekken van toestemming).

Houd hierbij zeker in de gaten dat een verwijderverzoek van gegevens alsnog opnieuw kan worden uitgevoerd, indien een oudere back-up, inclusief de oude gegevens, wordt teruggeplaatst. Verder is het verplicht om persoonsgegevens te versleutelen, dus ook op het back-up medium.

3 BACK-UP EN RECOVERY

In de context van back-ups en recovery zijn de termen recovery point objective (RPO) en recovery time objective (RTO) van groot belang. RPO verwijst naar een calculatie die aanduidt hoeveel data een organisatie kan verliezen tijdens het meest kritieke moment van de dienstverlening voordat de dienstverlening ernstig beschadigd raakt.

Deze tijdsinterval duidt dus aan hoe vaak u voor een back-up moet kiezen. Met andere woorden: als u maximaal 4 uur werk kwijt kan zijn, moet u om de 4 uur een veilige back-up maken van uw IT-assets.

RTO refereert aan de tijdsduur dat een applicatie, systeem of proces onbeschikbaar kan zijn zonder dat er significante schade wordt aangericht aan de dienstverlening en de tijd die het neemt om de IT-asset die onbeschikbaar is te herstellen zodat de dienstverlening weer normaal functioneert. Deze tijdsinterval drukt uit hoelang het maximaal mag duren voordat uw dienstverlening weer up-and-running is na een calamiteit. Praktisch refereert dit aan hoelang het maximaal mag duren voordat een (disaster) recovery succesvol kan worden uitgevoerd.

RTO en RPO wegen de meest kritieke IT-assets af tegen de worst-case scenario's en geven beiden verschillende inzichten en tijdsintervallen op de respectieve back-up en recovery strategieën. Om RTO en RPO te berekenen heeft u in eerste instantie inzicht nodig in de mate waarin bepaalde toepassingen of data kritisch zijn voor de dienstverlening van uw lokaal bestuur. Dit bepaalt u door een business impact analyse uit te voeren per toepassing of onderdeel van uw dienstverlening.

Back-ups

Back-ups zijn noodzakelijk om gegevens, applicaties en systemen te kunnen herstellen na verlies, vernietiging of manipulatie van gegevens en software. In principe kan van alle data, systemen en applicaties, een back-up gemaakt worden maar vaak wordt enkel een back-up gemaakt van de kritische assets. Om te bepalen wat kritisch voor uw lokaal bestuur is, is een risicoafweging nodig. Zo kunt u er bijvoorbeeld voor kiezen om enkel een back-up te maken van de systemen en data die nodig zijn om de werking van uw kritische dienstverlening te waarborgen.

Back-ups kunnen zowel op offline disks gemaakt worden als in de Cloud, maar idealiter houdt u de 3-2-1 regel aan.

Deze regel voldoet aan de volgende eisen:

- Bewaar 3 exemplaren van de gegevens: het origineel en ten minste twee kopieën
- Gebruik 2 verschillende soorten media voor de opslag. Dit kan helpen de impact te verminderen die aan een specifieke soort opslagmedia kan worden toegeschreven. U bepaalt zelf welk opslagmedium de originele gegevens bevat en op welke u de extra kopieën opslaat (bijv. disk bevat origineel en tape bevat kopie).
- Bewaar 1 exemplaar op een andere locatie (kluis, cloud, etc.) om te voorkomen dat gegevens verloren gaan als gevolg van een site gebonden storing.

Cloud back-ups zijn over het algemeen iets gebruiksvriendelijker (de back-up kan automatisch gemaakt worden) maar brengen meer risico's met zich mee. U zal daarom bij Cloud leveranciers een aantal kritische vragen moeten stellen over de instellingen van de back-up omgeving (bijv. back-ups in meerdere geografische zones), de versleuteling en het sleutelbeheer. Het is aanbevolen om uw team de juiste training en technische maatregelen aan te reiken zodat zij uw back-ups en back-up omgeving goed kunnen beheren.

De bewaartermijn van eigen beheerde online en offline back-ups wordt bepaald door de roulatie van de back-up media. Er dient een roulatie schema te zijn op basis van een veilige marge ten opzichte van de gemiddelde tijd die tussen systeem-malfuncties of mechanische-systeem-problemen zit (MTBF).

Tegelijk is het bewaren van back-ups belangrijk zodat u kunt terugvallen op oudere back-ups wanneer de laatste versie van uw back-up corrupt of gecompromitteerd is. Bij back-ups in de Cloud bent u vaker afhankelijk van hoe de Cloud leverancier dat heeft geregeld en hoe dit binnen lokale besturen wordt ingesteld. Zolang de Cloud leverancier maar kan voldoen aan de eisen die gesteld zijn aan o.a. de back-up en recovery.

Beveiliging van back-ups

Er is niets vervelender dan een corrupte of onleesbare back-up, zeker op het moment dat een noodgeval zich voordoet. Het is daarom belangrijk om ervoor te zorgen dat uw back-ups veilig worden opgeslagen en de inhoud van de back-ups geëncrypteerd wordt.

Het best past u de volgende beveiligingsmaatregelen toe op uw back-ups:

- Toegangscontrole tot back-ups (bijv. wachtwoorden en MFA)
- Encryptie van data op de back-ups
- Logging van activiteit op back-up medium
- Air-gapped back-ups (opslaan van back-ups op geïsoleerde en beveiligde apparaten)
- Anomaliedetectie (detectie van grote mutaties in de back-up data)

Recovery

Recovery is het herstellen van gegevens, een applicatie of omgeving naar de staat van vóór een incident. Dit wordt gedaan door middel van gemaakte back-ups. Het terugplaatsen van data, systemen en applicaties wordt niet enkel gedaan na grote incidenten zoals een ransomware aanval maar bijvoorbeeld ook om een verloren bestand of e-mail terug te zetten. Waar deze kleinere recoveries deel uitmaken van de standaard dienstverlening van uw IT-team, vergen grotere terugplaatsingen meer aanwijzingen en instellingen. Deze staan idealiter beschreven in handleidingen (zorg dat u hier ook back-ups van hebt) die aanwijzingen geven hoe applicaties en systemen weer opgestart kunnen worden. Tegelijkertijd dienen alle recoveries gelogd te worden zodat er een goed overzicht is welke gegevens, systemen en data gerecovered zijn en wanneer.

Disaster recovery wordt vaak uitgevoerd in het kader van een Business Continuity Management (BCM) proces, dewelk wordt opgestart wanneer één of meerdere kritische systemen of applicaties niet meer beschikbaar zijn. Dit proces zorgt ervoor dat in het geval van een aanzienlijk cyberveiligheidsincident de (kritische)dienstverlening stap-voor-stap terug wordt opgestart. Een veilige en complete disaster recovery is essentieel voor de uitvoering van dit proces omdat dit ervoor zorgt dat de IT-systemen (vaak het hart van een lokaal bestuur) snel hersteld kunnen worden en er data beschikbaar zijn.

Gezien het belang van recoveries wordt het aangeraden om op regelmatige termijn real-life scenario oefeningen te doen. Het best oefent uw lokaal bestuur met het terugzetten van meerdere systemen om zo potentiële complicaties en problemen op te sporen en te vermijden in het geval van een echte noodsituatie.

4 AANBEVELINGEN

Hieronder vindt u een aantal aanbevelingen die het Cyber Response Team voor Lokale Besturen (Vo-CRT) geeft met betrekking tot een beleid rond back-ups en recovery:

Organisatorische maatregelen

- Integreer (disaster) recovery processen in uw Business Continuity Management (BCM) en zorg ervoor dat u ook in kaart brengt hoelang het duurt om een (disaster) recovery uit te voeren
- Zorg ervoor dat uw back-ups en back-up gerelateerde processen voldoen aan de AVG-wetgeving (check bijv. wanneer er data van de back-ups verwijderd moet worden)
- Indien u het maken van back-ups of het opslaan van back-ups uitbesteedt (bijv. in de cloud), zorg er dan voor dat u afspraken maakt die de betrouwbaarheid en kwaliteit van uw back-ups waarborgen
- Recovery's worden altijd gedaan in samenspraak met de systeem/applicatie/data eigenaar
- Zorg dat de back-up frequentie is afgestemd met de noden van de business (via een business impact analyse)

Technische maatregelen

- Controleer het liefst dagelijks de integriteit en kwaliteit van uw back-ups
- Hanteer de 3-2-1 regel bij het opslaan van back-ups

- Zorg op elk moment voor een veilig bewaarde offline back-up
- Zorg dat uw back-up omgeving onderworpen is aan de nodige security controls zoals immutability, encryptie en isolatie
- Recovery wordt altijd gedaan in samenspraak met de systeem/applicatie/data eigenaar
- Voer regelmatig real-life scenario recovery oefeningen uit

Mensgerichte maatregelen

- Zorg ervoor dat het personeel dat verantwoordelijk is voor het maken van back-ups en het uitvoeren van recovery activiteiten voldoende getraind is en de juiste middelen ter beschikking hebben

5 VERKLARENDE WOORDENLIJST

Term	Verduidelijking	Link naar meer informatie
AVG/ GDPR	De Algemene Verordening Gegevensbescherming (AVG) of de General Data Protection Regulation (GDPR) is een Europese wetgeving met als doel om de privacy van burgers beter te beschermen	AVG (GDPR) en de Vlaamse Toezichtcommissie (VTC) | Vlaanderen Intern
1-2-3 regel	De 1-2-3 regel stelt bepaalde eisen aan het maken en opslaan van back-ups	What is the 3-2-1 Backup Rule? (uschamber.com)

REFERENTIES

- CCB – Cyberfundamentals Framework – Recovery
  - https://ccb.belgium.be/nl/cyberfundamentals-framework
- IDB – Handreiking back-ups en recovery
  - https://www.informatiebeveiligingsdienst.nl/product/back-up-en-recovery-gemeente/